Web Security Help

Websense® TRITON™ Web Security ソリューション

v7.8

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2014
アメリカ合衆国およびアイルランドにて印刷

商標について

目次

1 使用開始にあたって

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense® Web Security ソリューションの使用方法を学習し、質問に対する回答を見つけるには、本ガイドを閲覧するか、または出発点として以下のトピックのどれかを使用してください。

最初のステップ	開始時のソリューション
• *TRITON コンソールの使用方法* • *サブスクリプション* • *Web Security Dashboard*	• *インストールとサブスクリプションの問題* • *マスタ データベースの問題* • *トラブルシューティングのヒントとツール*
ポリシーの作成	**フィルタリングソリューション**
• *カテゴリおよびプロトコルへのアクセスの管理* • *クライアントの追加* • *ポリシーの使用* • *1 つのポリシーを複数のクライアントに割り当てる*	• *ポリシー実施の問題* • *ユーザー設定およびユーザー識別の問題* • *ブロック メッセージの問題*
レポートの使用	**レポーティングソリューション**
• *プレゼンテーション レポート* • *調査レポート* • *Real-Time Monitor* • *ツールボックスによるポリシーの実施動作の確認*	• *ログ、ステータス メッセージ、およびアラートの問題* • *Log Server と Log Database の問題* • *調査レポートとプレゼンテーション レポートの問題*
高度なツール	**他のソリューション**
• *ポリシーの例外* • *特定の URL の再分類* • *代理管理およびレポート作成*	• *指定済み管理の問題* • *相互運用性の問題* • *トラブルシューティングのヒントとツール*

概要

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Web Security ソリューションはインターネット アクセス ポリシーを作成、適用、レポートするために使用します。それと合わせて、一連の Websense コンポーネント（*Websense Web Security コンポーネント、444 ページ*を参照）は、インターネット セキュリティおよび管理、ユーザーの特定、アラート、レポート、およびトラブルシューティングの機能を提供します。

このバージョンに含まれる新しい機能の概要は、Websense Technical Library から入手できるリリース ノートに記載しています。

Websense Web Security は、インストールした後、**デフォルト** ポリシーを適用して、要求をブロックしないでインタネット使用状況をモニタします。

- このデフォルト ポリシーは、ユーザーの組織が独自のポリシーを指定し、それをクライアントに割り当てるまでの間、ネットワーク内のすべてのクライアントのインターネット アクセスを管理します。
- デフォルト ポリシーを編集して、それをモニタのためだけでなく、適用のためにも使用できるようにできます。
- カスタム ポリシーを作成した後、デフォルト ポリシーが他のポリシーによって管理されていない要求に適用されます。

詳細は、*Default ポリシー、112 ページ*を参照してください。

ポリシーの適用を開始するには、下記を参照してください。

1. *インターネット使用状況のフィルタ、57 ページ*
2. *クライアント、87 ページ*
3. *インターネット アクセスのポリシー、111 ページ*

単一のブラウザ ベースのツールである TRITON® Unified Security Center は、Websense Web Security、Data Security および Email Security ソリューションの全般的設定、ポリシー管理、およびレポート機能のための集中的なグラフィカル インターフェースを提供します。詳細は、*TRITON コンソールの使用方法、21 ページ*を参照してください。

TRITON Unified Security Center へのアクセスのレベルを指定することによって、特定の管理者が 1 つ以上の TRITON モジュールを管理できるようにすることができます。Web Security モジュール内でアクセス許可をさらに詳細に設定することによって、管理者がポリシーを管理し、レポーティング タスクなどを実行することができるように設定できます。詳細は、*代理管理およびレポート作成、405 ページ*を参照してください。

TRITON コンソールの使用方法

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Web Security manager のナビゲート*、23 ページ
- *Web Security Dashboard*、39 ページ

TRITON Unified Security Center は、Websense Web Security、Email Security および Data Security ソリューションを管理するために使用する集中化された設定インターフェースです。これは、インターネット アクティビティのポリシーのカスタマイズ、インターネット使用状況のモニタ、インターネット使用状況レポートの作成、Websense Web Security の構成および設定の管理のために使用する Web Security モジュール（Web Security manager）を含んでいます。

重要

TRITON コンソールでは Internet Explorer Compatibility View を使用してはいけません。Internet Explorer で不適切な動作やページ レイアウトが発生した場合、[Compatibility View（互換性表示）] ボタン（ブラウザのアドレス バーの URL と [Refresh（リフレッシュ）] ボタンの間）が選択されていないことを確認してください。

インストール時に、TRITON Unified Security Center は、1 つの管理者アカウント **admin** に対して、すべての TRITON モジュールおよび TRITON の設定への完全なアクセスを許可するように構成されます。このアカウントのパスワードは、インストール時に設定されます。

サブスクリプション キーが入力されるまで、admin ユーザー（またはユーザーが作成する他の優先管理者）が Web Security manager にログオンし、接続した時、**[Initial Setup Checklist（初期設定チェックリスト）]** が表示されます。このチェックリストを使用して、サブスクリプション キーを入力し、基本的な初期設定タスクを実行します。

キーが入力され、確認された後、Web Security manager にログオンしている管理者には **[Status（ステータス）] > [Dashboard（ダッシュボード）]** ページが表示されます。

- 初めて Web Security manager を使用する、またはこのバージョンを使用する管理者はクイック チュートリアルを利用できます。**[Help（ヘルプ）]** をクリックし、続いて **[Getting Started（使用開始にあたって）]** をクリックし、その後下記のどちらかのチュートリアルを選択します。
  - 新しい管理者のためのチュートリアル
  - アップグレードする管理者のためのチュートリアル
- 最初のログオン時に、管理者がダッシュボードから移動したとき、**[Save and Deploy（保存と配備）]** ボタンがオンになります。それによって最初のデフォルト ダッシュボード設定をその管理者アカウントに保存できます。（最初のデフォルトが保存された後は、チャートが追加、削除、または編集されたときのみ、ダッシュボードから移動したときに [Save and Deploy] ボタンがオンになります）。
- 複数の TRITON モジュールへのアクセス許可を持つアカウントを使用している場合は、TRITON ツールバーを使用してモジュール間を切り替えます。*Web Security manager のナビゲート、23 ページ*を参照してください。
- 指定済み管理を使用していて、すでに管理ロールを作成している場合は、管理するロールを選択するように求められることがあります。*代理管理およびレポート作成、405 ページ*を参照してください。

TRITON コンソールにログオンした時、Web Security モジュールは、インストール時に指定したデフォルト（ベース）Policy Server に接続します。別のポリシー サーバーを管理するには、Web Security ツールバーの [Policy Server（ポリシー サーバー）] ドロップダウン リストからそのポリシー サーバーの IP アドレスを選択します。

TRITON コンソール セッションは、ユーザー インターフェースでの最後のアクション（ページの移動のためのクリック、情報の入力、変更のキャッシング、変更の保存など）から 30 分を経過した時に終了します。セッション終了の 5 分前に警告メッセージが表示されます。

- ページ上にキャッシュされていない変更、またはキャッシュされているが保存されていない変更がある場合、それらの変更はセッション終了時に失われます。必ず **[OK]** をクリックして変更をキャッシュし、**[Save and Deploy]** をクリックして、これらの変更を記録し適用してください。
- 同じブラウザ ウィンドウの複数のタブで TRITON コンソールが開かれている場合、すべてのインスタンスで同じセッションが共有されます。いずれかのタブでセッションがタイムアウトすると、セッションはすべてのタブでタイムアウトします。

- 同じコンピュータ上の複数のブラウザ ウィンドウで TRITON コンソールが開かれている場合、**下記の事柄を行わない限り**インスタンスで同じセッションが共有されます。
  - 複数の Internet Explorer ウィンドウを別々に開く。
  - [File] > [New Session] コマンドを使って、新しい Internet Explorer のウィンドウを開く。
  - Internet Explorer を使って TRITON コンソールとの接続を開き、次に Firefox または Chrome を使って別の接続を開く。

TRITON Unified Security Center からログオフせずにブラウザを閉じるか、または TRITON モジュールにアクセスするために使用しているリモート コンピュータが突然にシャットダウンすると、ユーザは一時的に TRITON コンソールからロックアウトされます。管理コンポーネントは、通常、この問題を約 2 分以内に検出し、中断されたセッションを終了し、ユーザーは再度ログオンできるようになります。

Web Security manager のナビゲート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

TRITON コンソールの Web Security モジュールには、6 つのメイン エリアがあります。

1. バナー
2. TRITON ツールバー
3. Web Security ツールバー
4. 左側のナビゲーション ペイン
5. 右側のショートカット ペイン
6. コンテンツ ペイン

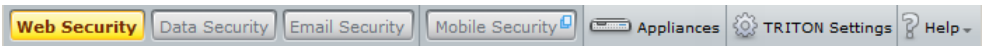
このガイドは、**admin** アカウントが使用できるオプションを示しています。指定済み管理者には、ここに示す機能のサブセットが表示されます。詳細は、*代理管理およびレポート作成*、405 ページを参照してください。

バナー

バナーは、ブラウザ ページの上部にあり、下記の情報を表示します。

- 管理ログオン アカウントに関連付けられている **ユーザー名**
- 管理者セッションを終了するときに使用する **[Log Off（ログオフ）]** ボタン。

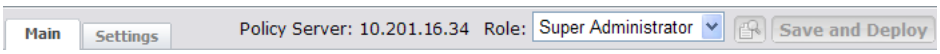
TRITON ツールバー



TRITON ツールバーは、バナーの下にあり、以下の機能を提供します。

- TRITON Unified Security Center のモジュール間の移動。
- ネットワークに配備されている V シリーズ **アプライアンス** の Appliance Manager への接続。
- インストールされているすべてのモジュールに影響を及ぼすグローバル **TRITON 設定**の構成。
- **ヘルプ情報**、チュートリアル、製品情報、および Websense テクニカル サポート リソースへのアクセス。

Web Security ツールバー



Web Security ツールバーは、TRITON ツールバーの下にあり、下記の操作に使用します。

- 左側のナビゲーション ペインの **[Main（メイン）]** タブと **[Settings（設定）]** タブを切り替える。

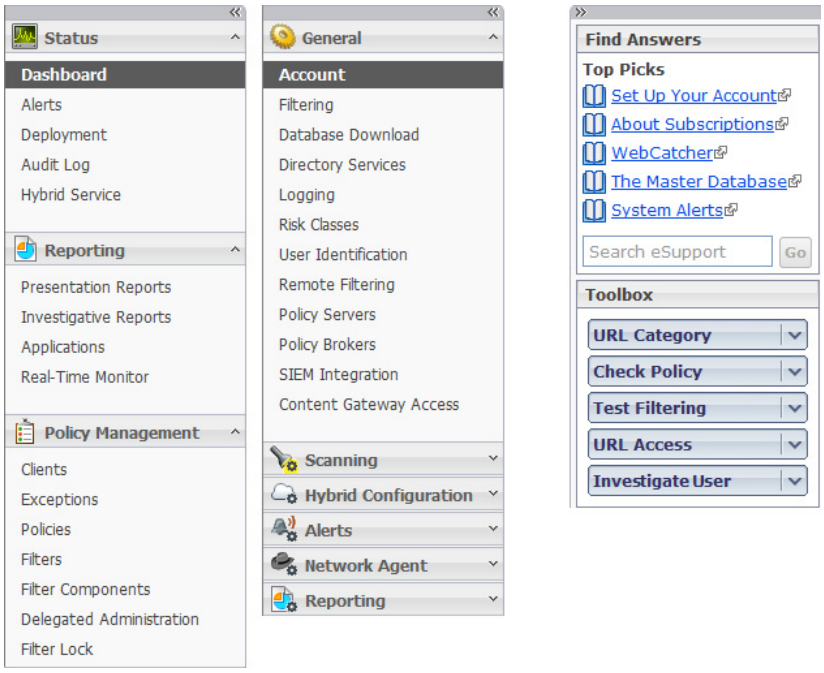
- 現在接続されているポリシー サーバーを確認し、ポリシー サーバーの複数のインスタンス（もしあれば）の間で切り替える（*Policy Server の動作、458 ページ*を参照）。
- 管理**ロール**を表示する、ロールを切り替える、または現在のロールのポリシー許可を発行する。

> **ヒント**
> ポリシー管理許可とレポーティング許可があるのにレポーティング機能だけが表示されている場合、別の管理者がそのロールにログオンしている可能性があります。一度に 1 人の管理者だけが各ロールのポリシー管理機能にアクセスできます。

- **未反映の変更を表示し**（小さな虫メガネ アイコンを使用する）、未反映の変更を **[Save and Deploy（保存および配備）]** する。キャッシュされている未保存の変更がない場合、これらのボタンは無効化されています。

  詳細は、*変更の確認、保存、および廃棄、26 ページ*を参照してください。

左側および右側のナビゲーション ペイン



左側のナビゲーション ペインには下記の 2 つのタブがあります。**[Main]** と **[Settings]** です。**[Main]** タブは、ステータス、レポーティング、およびポリシー管理機能にアクセスするために使用します。**[Settings]** タブは、Websense アカウントを管理し、グローバル システム管理タスクを実行するために使用します。（[Settings] タブは、サブスクリプション レベルに応じて異なるオプションを表示します）。

右側のショートカット ペインには、便利なツールと情報へのリンクが含まれています。

- **[Find Answers（回答の検索）]** は、タスクを完了するのに役立つ関連記事、ウェビナー、ビデオ、ワークシート、およびチュートリアルへのリンクを提供します。Websense eSupport Knowledge Base にある詳細な情報を検索するには、[Search（検索）] ボックスを使用します。
- **[Toolbox（ツールボックス）]** には、設定を確認できるクイック検索ツールが含まれています。詳細は、*ツールボックスによるポリシーの実施動作の確認、356 ページ*を参照してください。

どちらのナビゲーション ペインも、ペインの上部の二重矢印アイコン（<< または >>）をクリックすることによって最小化できます。ペインを通常に表示に戻すには、逆向きの矢印のアイコン（>> または <<）をクリックします。

ペインを最大化せずに関連機能のメニューを表示するには、最小化した左のナビゲーション ペインのショートカット アイコンにマウスを置きます。

変更の確認、保存、および廃棄

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Web Security manager で変更を行った場合、通常、ページの下部の **[OK]** をクリックして変更をキャッシュし、次に **[Save and Deploy（保存と配備）]** をクリックして変更を Policy Database に保存する必要があります。それによって変更が有効になります。

- Web Security manager の一部のフィールドまたはセクションには、別個の **[Save（保存）]** ボタンまたは **[Save Now（すぐに保存）]** ボタンがあります。これらの機能への変更はキャッシュされた後で保存されるのではなく、すぐに保存され、反映されます。
- 変更のタイプによっては、変更をキャッシュするために下位ページとメイン ページの両方で [OK] をクリックしなければならない場合があります。

重要

{OK} ボタンをダブルクリックまたはトリプルクリックしないように注意してください。同じボタンへを複数回のすばやくクリックすると、表示に問題が起こる可能性があります。この問題は、ブラウザを終了して、もう一度開くことによってのみ解決できます。

[View Pending Pending Changes（未反映の変更を表示）] ページを使用してキャッシュされた変更を確認します。1 つの領域の機能への複数の変更は、通常、キャッシュ リストの中では 1 つのエントリにグループ化されます。たとえば、6 つのクライアントを追加し、2 つのクライアントを削除した場合、キャッシュ リストにはクライアントに変更が行われたことだけが示されます。1 つの [Settings] ページへの複数の変更は、クライアント リストの中では複数のエントリとして示されます。これは、1 つの [Settings] ページで複数の機能を設定した場合に起こります。

- キャッシュされた変更をすべて保存するには、**[Save All Changes（すべての変更を保存）]** をクリックします。
- キャッシュされた変更をすべて廃棄するには、**[Cancel All Changes（すべての変更をキャンセル）]** をクリックします。

[Save All Changes] または [Cancel All Changes] を選択した後、選択した最後のページに戻ります。どちらのオプションも取り消しできません。

監査ログを使用して Web Security manager で行われた変更の詳細を確認します。詳細は、*監査ログの表示とエクスポート、475 ページ*を参照してください。

サブスクリプション

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense のは、クライアント（ユーザーまたは IP アドレス）ごとにサブスクリプションを発行します。

ソフトウェアを起動するために、有効なサブスクリプション キーを入力します（*アカウント情報の設定、29 ページ*を参照）。それによってマスタ データベース（*Websense マスタ データベース、32 ページ*を参照）をダウンロードしてポリシー適用を有効化できるようになります。

最初のデータベースが正常にダウンロードされた後、Web Security manager は、サブスクリプションに含まれているクライアントの数およびサブスクリプション タイプ（Web Filter、Web Security、Web Security Gateway、または Web Security Gateway Anywhere）を表示します。

Websense Filtering Service という名前のコンポーネントが毎日、インターネット要求を生成するクライアントのサブスクリプション テーブルを保持します。サブスクリプション テーブルは、毎夜クリアされます。テーブルがクリアされた後、クライアントから初めてインターネット要求が行われたとき、その IP アドレスがテーブルに含められます。

テーブルにリストされているクライアントの数がサブスクリプション レベルに達したとき、まだリストされていないクライアントからインターネット アクセスが要求されると、サブスクリプションの制限を超過します。バージョン 7.8.1 では、サブスクリプション レベルを超えたクライアントは、ユーザーの設定によって、インターネットから完全にブロックされるか、または制約なしのアクセスを許可されます 7.8.1 および 7.8.2 において、この設定は、またサブスクリプションが失効したとき、すべての要求を許可するか、またはブロックするかを決定します。

- サブスクリプションが超過するか、または期限切れになったとき、インターネット要求の処理方法を設定するには、*アカウント情報の設定*、29 ページを参照してください。
- サブスクリプションの期限が近づいた、または期限が切れたときにアラート メッセージを送信するように設定するには、*システム アラートの設定*、484 ページを参照してください。

MyWebsense ポータルによるアカウントの管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense, Inc., が保持するカスタマ ポータル mywebsense.com では、製品更新、パッチおよびホットフィックス、製品ニュース、評価、テクニカル サポート リソースにアクセスできます。

アカウントを作成すると、アカウントはお客様の Websense サブスクリプション キーに関連付けられます。これによって、ご使用の Websense 製品およびバージョンについての情報、警告およびパッチに確実にアクセスすることができます。

組織の複数のユーザーのために、同じサブスクリプション キーに関連付けられた MyWebsense アカウントを作成することができます。

アカウント情報の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *サブスクリプション、27 ページ*
- *データベースのダウンロードの設定、34 ページ*
- *プロトコルの使用、335 ページ*

[Settings（設定）] > [General（一般）] > [Account（アカウント）] ページを使用して、サブスクリプション情報を入力または確認し、またサブスクリプションが期限切れになったとき、またはバージョン 7.8.1 でサブスクリプション レベルが超過したとき Websense Web Security ソリューションが応答する方法を決定します。

また、ページを使用して Web セキュリティ コンポーネントがカテゴリおよびプロトコル使用状況データを Websense, Inc., に匿名で送信するように指定します。この情報は Websense Master Database を最適化してフィルタリングをより効率的に行うために使用し（*Websense マスタ データベース、32 ページ* を参照）、また Websense ThreatSeeker® Intelligence Cloud（websense.com/content/Threatseeker.aspx を参照）で使用されます。

インストールした後、または新しいサブスクリプション キーを受け取ったときはいつでも、**[Subscription key（サブスクリプション キー）]** フィールドを使用してキーを入力し、**[Apply（適用）]** をクリックします。キー構文を確認するためのチェックが行われ、次に Filtering Service がマスター データベースのダウンロードを試みます。

- キーは表示されるが、[Subscription key] が表示されない場合、二次 Policy Server に接続されています。この場合、Policy Server インスタンスはそのキー情報を一次 Policy Server から取得し、その IP アドレスはサブスクリプション登録済みのユーザーの数の下に表示されます。
- 複数の Policy Server 環境で複数のサブスクリプション キーを管理するには、**[Settings] > [General] > [Policy Servers（ポリシー サーバー）]** ページを使用します（*複数 Policy Server 環境での動作*、462 ページを参照）。
- キー構文は正しいが、キーが無効かまたは期限切れであるためにマスター データベースのダウンロードが失敗した場合、[Status（ステータス）] > [Alerts（アラート）] ページにヘルス アラート メッセージが表示されます。デフォルトでは、このメッセージは、[Status] > [Dashboard] ページの [System（システム）] タブにも表示されます。

最初にマスター データベースのダウンロードが正常に完了した後、[Account] ページに下記の情報が表示されます。

Key expires（キーの期限切れ）	現在のサブスクリプションの終了日この日の後、マスター データベースのダウンロードとインターネット ポリシーの適用を継続するためにサブスクリプションを更新する必要があります。
Subscribed users（サブスクリプション登録済みユーザー）	*Web Security Gateway Anywhere*：オンプレマイス コンポーネント、ハイブリッド サービス、およびリモート フィルタリング ソフトウェアによって管理されたユーザーの合計
Subscribed network users（サブスクリプション登録されたネットワーク ユーザーの数）	インターネット要求を管理できるネットワーク内ユーザーの数
Subscribed remote users（サブスクリプション登録されたリモート ユーザの数）	ネットワークの外側にいるとき要求を処理できるユーザーの数（オプションのリモート フィルタリング コンポーネントが必要です）。
Primary Policy Server（一次 Policy Server）	Policy Server インスタンスの IP アドレス、この Policy Server がサブスクリプション キー情報を受け取ります。 二次 Policy Server の情報を確認するときのみ表示されます。

1. 下記の場合に、**[Block users when subscription expires or is exceeded:（サブスクリプションの有効期限切れ、または規定数を超えた場合ユーザをブロックする）]**（バージョン 7.8.1）または **[Block users when subscription expires（サブスクリプションの有効期限切れの場合ユーザをブロックする）]**（バージョン 7.8.2）を選択します。

- サブスクリプションが有効期限切れになったときすべてのユーザーのインターネット アクセスをすべてブロックする（バージョン 7.8.1 および 7.8.2）。
- サブスクリプション登録済みユーザーの数を超過したユーザーのインターネット アクセスをすべてブロックする（バージョン 7.8.1）。

このオプションを選択しないままにしておくと、上記の場合にユーザーに制約なしのインターネットアクセスを提供します。

2. **[Send category and protocol data to Websense, Inc.（Websense, Inc. にカテゴリおよびプロトコル データを送信する）]** をオンにして、Web セキュリティ コンポーネントが Websense 定義のカテゴリおよびプロトコルに関する使用状況データを収集し、それを自動的に Websense, Inc. に送信するように設定します。

   この使用状況データは、Websense, Inc., による Web セキュリティ機能の絶え間ない向上に役立ちます。

3. Under [WebCatcher] の下の **[Send URL information to Websense（URL 情報を Websense に送信 ）]** をオンにすると、Websense, Inc. による URL の分類およびセキュリティ効果の向上に役立ちます。このツールの詳細については、*WebCatcher とは、36 ページ*を参照してください。

   - 分類のために評価する未分類の URL を送信するには、**[Send uncategorized URLs to improve URL categorization（URL の分類を改良するために未分離の URL を送信）]** をオンにします。
   - 不正な Web サイト アクティビティの追跡を支援するためにセキュリティ関連の URL を送信するには、**[Send security URLs to improve security effectiveness（セキュリティの効果を改良するためにセキュリティ URL を送信）]** をオンにします。
   - 検討のために Websense, Inc. に送信した情報のローカル コピーを保持するには、**[Save a copy of the data being sent to Websense（Websense に送信するデータのコピーを保存）]** をオンにします。

     このオプションが有効化されているとき、WebCatcher は、データを Log Server コンピュータの **Websense\Web Security\bin** ディレクトリに、暗号化されていない XML ファイルとして保存します。これらのファイルには日付と時刻のスタンプが付加されます。
   - 組織の **[Country of origin（国）]** を選択します。インターネット アクティビティの大部分がログ記録されている国を選択します。
   - **[Maximum upload file size（アップロード ファイルの最大サイズ）]** を指定します。最大サイズに到達したとき、収集された WebCatcher データが自動的に送信され、新しいファイルが開始されます。
   - **[Daily start time（毎日の開始時刻）]** フィールドを使用して、最大ファイル サイズに到達しなかった場合に、WebCatcher が収集したデータを送信する毎日の時刻を指定します。

4. （*Websense Web Security Gateway Anywhere*）ソフトウェアのオンプレマイス部分とハイブリッド部分の間の接続をアクティブ化または更新するため、下記のどちらかの手順を実行します。
   - Web セキュリティ管理者の **[Contact email address（コンタクト電子メール アドレス）]** を入力する。これは、通常、頻繁にモニタされるグループ電子メール エイリアスです。ハイブリッド サービスの問題に関するアラートがこのアドレスに送信されます。アラートに適切に応答できなかった場合、ハイブリッド サービスが一時的に切断されることがあります。
   - 管理者がいる **[Country（国）]** および **[Time zone（タイム ゾーン）]** を入力します。

   この情報が提供され検証されるまで、ユーザーの要求はハイブリッド サービスによって管理されません。詳細については、*ハイブリッド サービス の設定*、261 ページを参照してください。
5. 変更を完了したとき、**[OK]** をクリックします。**[Save and Deploy]** をクリックするまで、変更は適用されません。

Websense マスタ データベース

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *リアルタイムのデータベースの更新*、33 ページ
- *Real-Time Security Updates™*、33 ページ
- *データベースのダウンロードの設定*、34 ページ
- *Master Database ダウンロード ステータスの確認*、467 ページ
- *Master Database ダウンロードの再開*、468 ページ

Websense マスター データベースにはインターネット・コンテンツの管理のベースを提供するカテゴリとプロトコル定義があります（*カテゴリおよびプロトコルへのアクセスの管理*、59 ページを参照）。

- **[Categories（カテゴリ）]** を使用して、類似するコンテンツをもつウェブサイト（URL および IP アドレスによって識別される）を分類します。
- **[Protocol（プロトコル）]** 定義は、ファイルの転送やインスタント メッセージの送信など類似する目的に使用するインターネット通信プロトコルを分類します。

URL データベースの限定的なバージョンが Websense Filtering Service のインストール時にインストールされますが、完全なインターネット管理機能を有効化するために、できるだけ早く完全なマスター データベースをダウンロー

ドしてください。はじめてマスター データベースをダウンロードするには下記の手順を実行します。

- Web Security manager の **[Initial Setup Checklist]** にサブスクリプション キーを入力します。
- Filtering Service がプロキシを通じてダウンロードをおこなわなければならない場合は、このチェックリストでプロキシの設定値も設定します。

データベースをすべてのダウンロードするプロセスには数分から 60 分以上かかることがあります。インターネット接続速度、帯域幅、使用可能なメモリ、空き容量などにより異なります。

最初のダウンロードの後、Filtering Service は設定したスケジュールに従ってデータベースの変更をダウンロードします（*データベースのダウンロードの設定、34 ページ*を参照）。マスター データベースは頻繁に更新されますから、デフォルトでは、データベースのダウンロードが毎日行われるようにスケジュール設定されています。

マスター データベースが 15 日以上更新されなかった場合、Websense Web Security ソリューションはポリシー適用を停止します。

いつでもデータベースのダウンロードを開始するために、または最後のデータベースのダウンロードのステータス。最後のダウンロードの日付、または現在のデータベースのバージョン番号を確認には、Web Security Dashboard の **[System]** タブに移動し、コンテンツ ペインの上部のツールバーにある **[Database Download（データベースのダウンロード）]** をクリックします。

リアルタイムのデータベースの更新

完全なデータベースのスケジュール設定されたダウンロードのほかに、必要に応じてより小さな、部分的な更新が行われます。リアルタイム 更新は、たとえば、一時的に誤って分類れていたサイトを再分類するとき使用することがあります。これらの更新により、サイトとプロトコルが適切に管理されるようにします。

Websense Filtering Service がデータベース更新を 1 時間ごとにチェックします。

最新の更新は、**[Status] > [Alerts（アラート）]** ページにリストされます（*現在のシステム ステータスの確認、490 ページ*を参照）。

Real-Time Security Updates™

標準のリアルタイムのデータベースの更新を受け取ることのほかに、Websense Web Security、Web Security Gateway、Web Security Gateway Anywhere サブスクリプションをもつ組織は、Real-Time Security Updates を有効化して、Websense, Inc によってマスター データベースへのセキュリティ関連の更新が発行されるとすぐにそれらの更新を受け取ることができます。

Real-Time Security Updates は、インターネットベースのセキュリティの脅威に対する追加された保護のレイヤを提供します。更新が発行されるとすぐにそれらの更新をインストールすると、新たなフィッシング（身元詐称）詐欺、犯罪的なアプリケーション、およびメインストリームのウェブサイトまたはアプリケーションに感染する悪意のあるコードの脅威に対する脆弱性が軽減されます。

Filtering Service は、5 分ごとにセキュリティの更新をチェックします。更新は一般的には容量が小さいので、通常のネットワーク アクティビティを妨げません。

[Settings] > [General] > [Database Download（データベースのダウンロード）] ページを使用して、Real-Time Security Updates を有効化します（*データベースのダウンロードの設定、34 ページ*を参照）。

データベースのダウンロードの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *アカウント情報の設定、29 ページ*
- *Websense マスタ データベース、32 ページ*
- *Master Database ダウンロード ステータスの確認、467 ページ*

[Settings] > [General] > [Database Download（データベースのダウンロード）] ページを使用して、自動マスター データベースのダウンロードのスケジュールを設定します。[Initial Setup Checklist] にまだ情報を入力していない場合、このページを使用して Websense Filtering Service がデータベースをダウンロードするのに使用するプロキシ サーバーまたはファイアウォールの設定値を設定できます。

1. （*Websense Web Security*、*Web Security Gateway*、*Web Security Gateway Anywhere*）**[Enable real-time security updates（real-time security updates を有効化）する]**（デフォルト）を選択し、Websense Filtering Service が 5 分ごとにマスター データベースへのセキュリティの更新をチェックするようにします。セキュリティの更新が検出されたとき、その更新がすぐにダウンロードされます。

   リアルタイムのセキュリティの更新は、ネットワークを新たなフィッシング（身元詐称）詐欺、犯罪的なアプリケーション、またはメインストリームのウェブサイトまたはアプリケーションに感染する悪意のあるコードの脅威に対する脆弱性からすばやく保護します。
2. 自動ダウンロードの場合 **[Download days（指定ダウンロード日）]** を選択します。

- [Real-Time Security Updates] が有効化されている場合は、すべてのダウンロード日が選択されます。ダウンロードは毎日自動的に実行され、セキュリティの更新のために最新の標準データベースが使用できるようにします。
- ポリシーの適用を中断されず継続するためには、マスター データベースを少なくとも 2 週間ごとにダウンロードする必要があります。
- すべてのダウンロード日を選択解除した場合、Filtering Service は、データベースが *7 日間経過した*とき、ダウンロードを自動的に試みます。

3. **[Download between（ダウンロード開始 / 終了時刻）]** で、Filtering Service がマスター データベースの更新のダウンロードを試みる開始時刻と終了時刻を選択します。デフォルトでは、ダウンロードは、Filtering Service コンピュータの時刻に従って、21:00（9 p.m.）と 06:00（6 a.m.）の間に行われます。
   - Filtering Service は、この期間の任意の時刻に Master Database サーバに接続します。ダウンロードが失敗した場合のアラートを設定するには、*システム アラートの設定*、484 ページを参照してください。
   - いつでも Websense が再起動され、利用可能なマスター データベースの更新をチェックします。更新は、指定した時間待機するのではなく、すぐに開始します。

   > **注意**
   > マスター データベースをダウンロードした後、またはそれを更新した後、CPU 使用率が 90% に達することがありますが、データベースはローカル メモリにロードされます。

4. Filtering Service がマスター データベースをダウンロードするためにプロキシ サーバーまたはプロキシイング ファイアウォールを通過してインターネットにアクセスしなければならない場合、**[Use proxy server or firewall（プロキシ サーバーまたはファイアウォールを使用）]** を選択します。次に下記の項目に入力します。
   - プロキシ サーバーまたはファイアウォールの **[IPv4 address or hostname（IPv4 アドレスまたはホスト名）]**。
   - データベース ダウンロードが通過しなければならない **[Port（ポート）]**（デフォルトでは 8080）。

5. 上記で設定したプロキシ サーバーまたはファイアウォールがインターネットに到達するための認証を必要とする場合、**[Use authentication（認証を使用）]** を選択し、次に Filtering Service がインターネットアクセス権を得るために使用する **[User name（ユーザー名）]** と **[Password（パスワード）]** を入力します。

> **注意**
> [Use authentication] を選択した場合、マスター データベースのダウンロードを有効化するために、サーバーまたはファイアウォールをクリア テキストまたは基本認証を受け入れるように設定する必要があります。

デフォルトでは、ユーザー名およびパスワードは、Policy Server コンピュータのロケールの文字セットに対応するように暗号化されます。この暗号化を **[Settings] > [General] > [Directory Services（ディレクトリ サービス）]** ページを通じて手動で設定できます（*拡張ディレクトリ設定*、98 ページを参照）。

WebCatcher とは

Web Security Help | Web Security ソリューション | バージョン 7.8.x

WebCatcher は、認識されていない、セキュリティー関連の URL を収集し、それらを Websense Security Lab に送信するオプションの機能です。未分類の URL が分類のために検討され、セキュリティ関連 URL については、それがインターネットへのアクティブな脅威に関してどんな情報を提供するかが分析されます。（WebCatcher の処理では完全な URL ロギングを必要としません）。分析の結果は、マスター データベースの更新に使用され、それによってパフォーマンスが向上します。

> **注意**
> 複数の Web Security Log Server インスタンスがある環境では、WebCatcher は、Web Security manager の **[Settings] > [General] > [Accounts]** ページで一度だけ有効化されます。

Websense Security Lab に送信された情報は、URL だけを含み、ユーザー情報は含みません。例：

```
<URL HREF="http://www.ack.com/uncategorized/" CATEGORY="153"
IP_ADDR="200.102.53.105" NUM_HITS="1" />
```

この例の IP アドレスは、要求者の IP アドレスではなく、URL をホストしているコンピュータのアドレスを反映しています。

> **注意**
> イントラネット サイトは、WebCatcher によって送信されません。イントラネット・サイトには、10.xxx.xxx.xxx、172.16.xxx.xxx、192.168.xxx.xxx の範囲の IP アドレスをもつすべてのサイトが含まれます。

WebCatcher データは、HTTP ポストを経由して Websense, Inc. に送信されます。HTTP トラフィックの送信を許可するために、プロキシ サーバーまたはファイアウォールでロールを作成するか、または他の変更を行う必要がある場合があります。

Websense テクニカル サポート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense ソフトウェアおよびサービスに関する下記のような技術情報に support.websense.com で 1 日 24 時間いつでもアクセスできます。

- 検索可能な Websense Knowledge Base（Solution Center、Technical Library、カスタマ フォーラムで構成されている）
- ウェビナー と show-me ビデオ
- 製品マニュアルと詳細な技術ペーパー
- よくある質問に対する回答

その他の質問については、このページの上部にある **[Contact Support（サポートの問い合わせ）]** タブをクリックしてください。

問い合わせページは、ソリューションを見つける、オンライン サポート 事例を開く、および Websense Technical Support への連絡のための情報が含まれています。

速やかな電話応答のために、MyWebsense の [Profile（プロファイル）] セクションにある **[Support Account ID（サポート アカウント ID）]** を利用することができます。

電話でのサポートの場合、次の準備が必要です。

- Websense のサブスクリプション キー
- ソリューションのための管理コンソールへのアクセス（例、TRITON コンソール、Appliance manager、Content Gateway manager）

- レポーティング ツールを実行しているコンピュータおよびデータベース サーバー（Microsoft SQL Server または SQL Server Express）へのアクセス
- ネットワークのアーキテクチャに精通しているか、専門家に連絡できること

2 Web Security Dashboard

Web Security Help | Web Security ソリューション | バージョン 7.8.x

TRITON コンソールにログ オンし、Web Security manager に接続したとき、最初に **[Status（ステータス）] > [Dashboard（ダッシュボード）]** ページの **[Threats（脅威）]** タブが表示されます。このタブは、マルウェア脅威と関連している可能性があるネットワーク上の疑わしいアクティビティに関する情報を表示します。

表示される情報のタイプおよび詳細のレベルはサブスクリプション レベルによって異なります。たとえば、アウトバウンド脅威に関する情報を表示し、その脅威についてフォレンシックな詳細情報を入手するには、Web Security Gateway または Web Security Gateway Anywhere が必要です。*Threats ダッシュボード*、41 ページを参照してください。

ダッシュボードの要素は、スーパー管理者および Web Security Dashboard でレポートを表示する権限がある指定済み管理者に表示されます（*ロールの編集*、423 ページを参照）。

- 指定済み管理者の Risks（リスク）、Usage（使用状況）、および System（システム）ダッシュボードへのアクセスは、Threats ダッシュボードへのアクセスとは別に設定されます。
- Threats ダッシュボードへのアクセス権限をもつ指定済み管理者はまた、新型の高度なマルウェア脅威と関連するフォレンシックな詳細情報を表示する許可が与えられることもあります。*脅威に関連するフォレンシック データの検討*、49 ページを参照してください。

最初に管理者が Web Security manager にログ オンし、次にダッシュボードから移動したとき **[Save and Deploy（保存と配備）]** ボタンがオンになります。これは、各管理者アカントのデフォルト ダッシュボードの設定を保存するために変更が行われたか否かに関わらず行われます。

最初のデフォルトが保存された後、ダッシュボードから移動すると、チャートが追加、削除、または編集されたときのみ [Save and Deploy] ボタンがオンにされます。

このダッシュボードには、以下のような 3 つの追加的タブがあります：

- **Risks（リスク）**では、Security Risk クラスに属する URL へのブロックおよび許可された要求についての情報が示されます。この情報の程度はお客様のサブスクリプション レベルによって異なります。*Risks ダッシュボード、50 ページ*を参照してください。
- **Usage（使用状況）**は、帯域情報およびブロックされた要求と許可された要求の要約など、ネットワーク内のトラフィック パターンに関する情報を示します。*Usage ダッシュボード、51 ページ*を参照してください。
- **System（システム）**ではアラート メッセージとステータス情報、そして配備の現在の状態を示すグラフが表示され、ネットワーク中のインターネット アクティビティに焦点が当てられています。*System ダッシュボード、52 ページ*を参照してください。

Risks、Usage、および System のダッシュボードでは同時にそれぞれ最大 12 個の要素（グラフ、ステータスの要約、またはカウンタ）を表示することができます。ほとんどのダッシュボードのグラフは、それらの時間（本日、最後の 7 日間、最後の 30 日間など）およびそれらの表示形式（積み上げ棒グラフ、積み上げ面グラフ、複数折れ線グラフなど）を変更するためにカスタマイズできます。タブに同じぐファルの複数のバージョンを含めることができます（例、種々の時間を表示する）。

- ダッシュボードの要素は、2 分ごとに更新されます。

  タブ譲歩いずれかの要素が変更された場合、タブ上のすべての要素も更新されます。たとえば、あるグラフの時間が変わった場合、ページ上のすべての要素でデータが更新されます。
- ダッシュボード要素の利用可能なセットは、サブスクリプション タイプによって異なります。たとえば、ハイブリッド フィルタリングに関するグラフは、Web Security Gateway Anywhere でのみ利用できます。
- タブに要素を追加するには、**[Add Charts（チャートを追加）]** をクリックし、次に手順について *ダッシュボード タブに要素を追加する、53 ページ*を参照します。
- タブから要素を削除するには、要素タイトル バーに含まれている [Options（オプション）] アイコン（  ）をクリックし、次に **[Remove（削除）]** を選択します。
- 要素のすべての編集オプションにアクセスするには、要素タイトル バーに含まれている [Options（オプション）] アイコンをクリックし、つづいて **[Edit（編集）]** を選択します。
- 一般的に、円グラフ、棒グラフ、または折れ線グラフをクリックすると、より詳細な情報を示す調査レポートが表示されます。一部のセキュリティ関連のグラフはそうではなく Threats ダッシュボードにリンクします。

ダッシュボード ツールバーには下記の最大 4 つのボタンが表示されます。

- **[Database Download（データベースのダウンロード）]**、スーパー管理者のみ利用でき、マスター データベースのステータスを表示し、ダウンロードを開始または中断するオプションを提供します（*Master Database ダウンロード ステータスの確認*、467 ページを参照してください）。
- **[Status Monitor（ステータス モニタ）]** は、現在の管理者のポリシー許可を解除し、タイムアウトなしに下記のページにアクセスできるモニタリング モードになります。
  - Status > Dashboard
  - Status > Alerts
  - Reporting > Real-Time Monitor

  Web Security Status Monitor（ステータス モニタ）モード、56 ページを参照してください。
- **[Add Charts（チャートを追加）]** は、管理者がページ上で要素を追加することによって、選択したサッシュボードのビューをカスタマイズできるようにします。*ダッシュボード タブに要素を追加する*、53 ページを参照してください。
- **[Print（印刷）]** は、ページに表示されたチャートの印刷用バージョンをもつ二次ウィンドウを開きます。ブラウザのオプションを使用してページを印刷します。

Threats ダッシュボード

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Web Security Dashboard*、39 ページ
- *脅威イベントの詳細の調査*、45 ページ
- *疑わしいアクティビティに重大度を関連付ける方法*、47 ページ
- *脅威インシデントの詳細情報の検討*、47 ページ
- *脅威に関連するフォレンシック データの検討*、49 ページ

Web Security Dashboard の **[Threats]** タブを使用して、ネットワーク内の疑わしいアクティビティをモニタし、調査します。

- アウトバウンド脅威に関する情報を表示し、その脅威についてフォレンシックな詳細情報を入手するには、Web Security Gateway または Web Security Gateway Anywhere が必要です。
- Threats ダッシュボードの要素の追加または削除はできません。

Threats ダッシュボードの最初のビューは、下記の項目を示します。

- **[Top Security Destinations（上位セキュリティ宛先）**では、疑わしい トラフィックが送信される、または疑わしいアクティビティに関連するサイトがホストされている上位 10 カ国が示されます。
- **[Security Events by Type（タイプ別のセキュリティ イベント）]** では、マルウェア脅威と関連する上位セキュリティ カテゴリ中のサイト（宛先）へのブロックされた要求、許可された要求、またはその両方の要求の数を示します。
- **[Suspicious Event Summary（疑わしいイベントの要約）**ではネットワーク内の脅威に関連するイベントに関する情報を示します。

タブの右上隅の **[Status]** コントロールは、脅威のデータが自動的に更新されるか否かを示します。

- ステータスが **[Running（実行中）]** である場合は、**[Pause（一時停止）]** をクリックして、現在の結果を調べている間、データが更新されないようにします。
- ステータスが **[Paused（一時停止中）]** である場合、**[Start（開始）]** をクリックしてダッシュボードを更新が中断されていた間に収集された新しいデータによって更新します。

タブの上部の追加的なコントロールによって、チャートおよび要約テーブルに含められる情報を下記の指定の項目に制限できます。

- 期間（本日、7 日間、30 日間など）
  - ドロップダウン リストの下の日付の詳細情報は、選択した期間を計算するために使用する開始日および時刻を示します。
  - 利用可能な最大時間を [Settings] > [Reporting（レポーティング）] > [Dashboard] ページで設定します（*ダッシュボードのレポーティング データの設定、531 ページ*を参照）。

    Microsoft SQL Server Express の場合、最大期間は、30 日間で、変更できません。
- 重大度（Critical（危険）、High（高位）、Medium（中位）、または Low（低位））

  各重大度レベルに関連する分類の詳細については、**[Severity Mapping（重大度マッピング）]** リンクをクリックします。
- アクション（All（すべて）、Permitted（許可）、または Blocked（ブロック））
- 方向（All（すべて）、Inbound（インバウンド）、または Outbound（アウトバウンド））

また、[Top Event Destinations（上位イベント宛先）] マップおよび [Security Events by Category（カテゴリ別セキュリティ イベント）] チャートを使用して、ページの下部の要約テーブルに表示される情報をさらに絞り込むことができます。

- [Suspicious Event Summary（疑わしいイベント要約）] テーブルにある国に関連するトラフィックのみを表示するにはマップ上のドットをクリックします。

  ドットのサイズは、その国に関連するインシデントの数を反映します。ドットの上でマウスを動かすと、国名を示すツールチップが表示されます（ドットのない青のエリアの上でマウスを動かすと、大陸名が表示されます）。
- テーブル内のそのカテゴリに関連するトラフィックだけを表示するには、チャート内のカテゴリをクリックします。

  チャート内では各カテゴリは異なる色で表示されます。チャート内のバーまたはセグメントの上でマウスを動かすと、カテゴリ名を示すツールチップが表示されます。

デフォルトでは：

- [Top Event Destinations] マップは、疑わしいアクティビティの発信元または疑わしいトラフィックの送信先の上位 20 カ国を示します。
- [Security Events By Category] チャートは、ネットワーク内の疑わしいアクティビティに関連する上位 5 つのカテゴリを積み上げ棒グラフ形式で示します。

マップまたはチャートの情報を変更するには、下記の手順を実行します。

- **[Options（オプション）]** アイコンをクリックし、次に **[Edit（編集）]** を選択します。
- **[Top（上位）]** リスト（両方の要素）または **[Chart type（チャート タイプ）]** リスト（[Security Events by Category] チャート）を使用して表示を更新します。

  [上位] 値またはチャート タイプの変更は、要約テーブルに表示される情報に影響を与えません。

[Suspicious Event Summary] テーブルは、調査対象の特定のイベントを特定するために役立つ種々のオプションを提供します。

- [Search（検索）] ボックスを使用して、ユーザー名、IP アドレス、またはホスト名（もしあれば、Content Gateway が必要です）のイベントを見つけます。

  [Search] ボックスの条件に基づくテーブルのフィルタリングを停止するには、**[Clear（クリア）]** をクリックします。

- 要約テーブルに現在適用されている各フィルター（期間、重大度、アクション、方向、国、カテゴリ）が示されます。フィルターをクリアしてテーブルに表示 s あれる情報を拡大するには、フィルターの隣のチェック ボックスをクリアします。
- 詳細レポートを表示するには、ユーザー名、IP アドレス またはホスト名（もしあれば）をクリックします。*脅威イベントの詳細の調査、45 ページ*を参照してください。

[Suspicious Event Summary] をカスタマイズして、下記の列のいずれかを表示または非表示にすることができます。デフォルトで表示される列には、アスタリスク（*）が付いています。

列	説明
Severity*（重大度）	青い背景の [S] アイコン（S）によって示されます。イベントに関連する重大度（Critical、High、Medium、または Low）を示します。
Forensics* （フォレンシック）	虫メガネ アイコン（）によって示されます。イベントがファイルを送信する試みを含んでいるかどうかを示します。 Web Security Gateway または Gateway Anywhere のみ。
User*（ユーザー）	アクティビティに関連するユーザー名（もしあれば）。
IP address（IP アドレス）	アクティビティが行われたコンピュータの IP アドレス。
Device*（デバイス）	アクティビティが行われたコンピュータの名前。 Web Security Gateway または Gateway Anywhere のみ。
Category*（カテゴリ）	アクティビティに関連するマスター データベース カテゴリ
Last Attempt* （最後の試行）	行に表示された特性のすべてを共有する最新のイベントのタイムスタンプ。
Country*（国）	（国コードの）略語 [CC] によって示されます。イベントの宛先（ターゲット）の 2 文字の国コードを示します。複数の宛先が 1 つのイベントと関連付けられている場合、[Multiple（複数）] が表示されます。
Direction（方向）	疑わしいアクティビティがインバウンド トラフィックに関係しているのか、またはアウトバウンド トラフィックに関係しているのかを示します。 アウトバンド脅威検出は、Web Security Gateway または Gateway Anywhere を必要とします。
Incidents* （インシデント）	[Last Attempt] を除く、行に表示されるすべての特性を共有するインシデントの数。

チャートで列を追加するか、または列を削除するには、テーブルの上の **[Customize（カスタマイズ）]** リンクをクリックします。テーブルで列を追加するには列名の隣のチェック ボックスをオンし、またはテーブルから列を削除するには、そのチェックボックスをオフにします。

テーブルのコンテンツを CSV ファイルにエクスポートするには、**[Export to CSV（CSV へのエクスポート）]** をクリックします。イベント データをエクスポートする時刻を選択し、**[Export（エクスポート）]** をクリックします。

脅威イベントの詳細の調査

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Dashboard] > [Threats] > [Event Details（イベントの詳細）] ページを使用して、疑わしいアクティビティのインシデントを調査します。ページは下記に関連するインシデントを表示できます。

- Threats ダッシュボードの [Suspicious Event Summary] テーブルから選択した特定のユーザー名、IP アドレス、またはデバイス（デバイス名情報は、Content Gateway によって提供され、また他の統合製品が使用されている場合は利用できません）。
- 疑わしいアクティビティ アラート電子メール通知内のリンクをクリックすることによって選択された特定の重大度レベル（*疑わしいアクティビティ アラートの設定、489 ページ*を参照）。

ページの上部で、テーブルは選択したユーザー、IP アドレス、ホスト名、または重大度レベルに関連する各インシデントを示します。テーブルは、ページあたり 10 行のデータを示します。

- 特定のインシデントまたは関連するインシデントのグループに結果を絞るには、[Search] フィールドを使用します。検索フィルタを削除するには **[Clear]** をクリックします。
- テーブルに含まれる期間、およびテーブルが最後に更新された時刻を確認するには、ページの右上部分の情報を参照します。
- テーブルに表示されている列を変更するには、コンテンツ ペインの上部のツールバーに含まれている **[Customize]** をクリックしあ m す。詳細テーブルには Threats ダッシュボードの要約テーブルと同じ列のオプションがあります。
- 選択したインシデント、それに関連する脅威、使用している検出方法に関するそのほかの詳細情報によってページの下部を更新するにはテーブル内の行をクリックします（*脅威インシデントの詳細情報の検討、47 ページ*を参照）

  インシデントの詳細セクションは、Websense ACEInsight へのリンクを含んでいます。このリンクを使用して、そのインシデントに関連する URL および脅威に関する現在の情報を確認します。
- 11 個以上のインシデントがある場合、テーブルの下部のページングのコントロールを使用してデータ検索します。

Web Security Gateway 環境と Gateway Anywhere 環境では、ネットワークに感染する目的、またはネットワークの外側に機密データを送る目的の試行に関連するファイルを捕捉できます。ファイルに関連するデータを総称して**フォレンシック データ**と言い、このファイルは**フォレンシック リポジトリ**と言う特別なデータベースに保存されます。

- デフォルトでは、フォレンシックの捕捉およびストレージが有効化されます。
- フォレンシック捕捉およびストレージを [Settings] > [Reporting] > [Dashboard] ページで設定します（*ダッシュボードのレポーティング データの設定、531 ページ*を参照）。

フォレンシックの捕捉が有効化され、インシデントと関連するファイル（例、スプレッドシート、ドキュメント、または圧縮ファイル）がある場合、[Event Details（イベントの詳細）] テーブルのフォレンシックの列にアイコンが示されます。フォレンシック データを含むインシデントを選択したとき、インシデントに関連するファイルに関する情報が、そのページの [Forensic Data（フォレンシック データ）] セクションに表示されます（*脅威に関連するフォレンシック データの検討、49 ページ*を参照）。

警告

脅威インシデントに関連するファイルを開くときは注意してください。ファイルがマルウェアに感染している場合、インシデントを調査するために使用するコンピュータに感染する可能性あります。

また、捕捉したファイルが高い機密データを含んでいることがあります。

インシデントのユーザー エージェント ヘッダーがキャプチャされた場合、[User Agent String（ユーザー エージェント文字列）] フィールドに含まれるリンクを使ってユーザー エージェントの **他のインスタンスを検索する**ことができます。このリンクをクリックすると、[Reporting] > [Applications] ページの [Search] タブに検索結果が表示されます。アプリケーション レポートおよびユーザー エージェントに関する詳細については、*アプリケーション レポートの作成、216 ページ*を参照してください。

イベント情報を CSV ファイルにエクスポートするには、コンテンツ ペインの上部のツールバーの **[Export]** をクリックします。ページに現在表示されているユーザー、IP アドレス、ホスト名、または重大度レベルだけではなく、選択した**期間**にログされたすべての脅威関連のイベントがエクスポートされます。

疑わしいアクティビティに重大度を関連付ける方法

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense マスター データベースは、要求に割り当てられたカテゴリに基づき、脅威に関連するイベントに重大度レベルを割り当てます。

- 重大度レベルは Websense マスター データベースでカテゴリにマップされ、Websense データベースが更新されたとき変更されることがあります。
- Websense Web Filter および Websense Web Security のサブスクリプションは、高位および危険の重大度レベルがある一部またはすべてのカテゴリを含みません。これらのカテゴリは、Threats ダッシュボードに表示されることがありますが、カテゴリ フィルタでは管理できません。

関連する重大度レベルがあるカテゴリの現在にリストを表示するには、Threats ダッシュボードの上部の近くにある **[Severity Mapping（重大度マッピング）]** リンクをクリックします。リストは、サブスクリプションを使ったフィルタリングに利用できないカテゴリを表示します。

脅威インシデントの詳細情報の検討

Web Security Help | Web Security ソリューション | バージョン 7.8.x

管理者が、[Threats] > [Event Details] ページの上部のテーブルにあるインシデントを選択したとき、テーブルの下のエリアに、そのインシデントに関する利用可能なすべての詳細情報が取り込まれます。利用可能な詳細情報は下記の条件によって異なる場合があります。

- 発生したインシデントのタイプ。例：
  - マスター データベースによってブロックされたカテゴリに割り当てられた URL の アウトバンド要求は、脅威名、目的、またはタイプを含む可能性は低いです。なぜなら Content Gateway の分析が行われる前に要求がブロックされているからです。
  - 試行されたファイル転送を含まない要求は、フォレンシック データを含みません
- 統合製品がインターネット要求情報を Filtering Service に提供する。例：
  - Content Gateway だけが、ホスト名、脅威名、脅威の目的、脅威のタイプ、およびスキャン中のカテゴリ情報だけを渡します。
  - すべての統合製品がプロトコル、メソッド、またはコンテンツ タイプ情報を渡すわけではありません。
- ファイル転送試行がインシデントに関連付けられているかいなか（Content Gateway だけがこのタイプのフォレンシック データを提供します）。*脅威に関連するフォレンシック データの検討、49 ページ*を参照してください。

下記のインシデントの詳細情報がページに表示される場合があります。

フィールド	説明
Severity（重大度）	危険、高位、中位、または低位。 *疑わしいアクティビティに重大度を関連付ける方法、47 ページ*を参照してください。
Category（カテゴリ）	宛先 URL に割り当てられたマスター データベースまたはカスタム カテゴリ
Threat Name（脅威名）	不正なソフトウェア、ボット トラフィック、または他の脅威アクティビティ（もしあれば）に関連する名前。
Threat Intent（脅威の目的）	脅威が試みようとしていること（キー操作のログ、ネットワークに侵入する裏口を開くなど）。
Platform（プラットフォーム）	脅威がターゲットにしているオペレーティング システム（Windows、Android など）。
Threat Type（脅威のタイプ）	不正なソフトウェアの分類（トロイ、ワーム、新型のしつこい脅威など）。
Action（アクション）	要求に割り当てられるアクション（許可またはブロック）
Reason（理由）	許可またはブロック アクションが適用される理由（例、当該の URL にカテゴリが割り当てられている）。
Incident Time（インシデント時刻）	インシデントが発生した日付および時刻
ACEInsight Link（ACEInsight リンク）	ACEInsight.com へのリンクで URL または脅威に関するさらなる調査を有効化します。
User（ユーザー）	URL を要求しているユーザー（ユーザーが特定されている場合）。
Source IP address（送信元 IP アドレス）	要求が発信された IP アドレス
Device（デバイス）	要求が発信されたコンピュータの名前（Content Gateway を必要とします。ホスト名が入手できない場合、発信 IP アドレスが繰り返されます）。
Destination IP address（宛先 IP アドレス）	要求された URL の IP アドレス。
Port（ポート）	要求された URL との通信に使用するポート。
Protocol（プロトコル）	要求された URL に使用するプロトコル。
Direction（方向）	インシデントがインバウンド接続に関連しているか、アウトバウンド接続に関連しているか。
Method（メソッド）	要求が GET であったか、POST であったか。

フィールド	説明
Content Type（コンテンツ タイプ）	要求に関連する HTTP ヘッダーの [Content-Type] フィールドに報告される値（例、text/html、image/gif、または application/javascript）
Bytes Sent（送信バイト数）	送信元コンピュータから送信されるバイトの数。
Bytes Received（受信バイト数）	ターゲット（宛先）URL によって返されるバイトの数。 要求がブロックされた場合、この数は 0 です。
Country（国）	宛先 URL をホストしている国。
Full URL（完全 URL）	ターゲット サイトの完全 URL（ドメイン、パス、CGI ストリング、およびファイル）。
Active Policy（アクティブ ポリシー）	要求を管理するために使用するポリシー。
Database Category（データベース カテゴリ）	Websense マスタ データベースによって要求に割り当てられているカテゴリ。
Scanning Category（スキャン中のカテゴリ）	Content Gateway 分析によって要求に割り当てられたカテゴリ（Master Database カテゴリと一致する場合があります）。
Role（ロール）	指定済み管理者ロールは、要求を管理するために使用するポリシーとして機能します。

脅威に関連するフォレンシック データの検討

Web Security Help | Web Security ソリューション | バージョン 7.8.x

管理者が、フォレンシック データを含む [Threats] > [Event Details（イベントの詳細）] ページでインシデントを選択したとき、テーブルの下のデータ エリアに試行されたファイル転送に関する詳細情報が取り込まれます。フォレンシックの詳細情報は以下の内容を含みます。

フィールド	説明
Source（送信元）	要求を行っているユーザーまたは IP アドレス。
Destination（宛先）	ターゲット コンピュータの IP アドレス。
Data Security Incident ID（Data Security インシデント ID）	インシデントに関連する Websense Data Security の ID 番号。Data Security manager でインシデントをさらに調査するために使用できます（Web Security Gateway Anywhere または Websense Data Security ソリューションが必要です）。

フィールド	説明
Files（ファイル）	インシデントに関連するファイルの名前およびサイズ。ファイル名は、実際のファイルを開くために使用できるリンクです。 **警告**：捕捉されたファイルを開くときは注意してください。ファイルは、調査に使用するコンピュータを感染させるマルウェアを含んでいることがあります。ファイルはまた、機密データを含んでいることもあります。
Parameters and Body（パラメータと本文）	ファイルの送信または検索に使用した HTTP 要求について CGI パラメータおよび HTML 本文の詳細情報を示します。 要求の本文に含まれるパラメータおよび詳細情報の数は、インシデントによって大きく異なります。

Risks ダッシュボード

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *System ダッシュボード*、52 ページ
- *Threats ダッシュボード*、41 ページ
- *Usage ダッシュボード*、51 ページ
- *ダッシュボード タブに要素を追加する*、53 ページ

Web Security Dashboard の **[Risks]** タブを使用して、[セキュリティ リスク] クラスに含まれる URL に対する許可された要求とブロックされた要求をモニタします。デフォルトでは、下記のチャートが表示されます。

- **[30-Day Risk Trends（30 日リスク傾向）]** は、本日を含む 30 日を超える特定のセキュリティおよび法的責任カテゴリのブロックされた要求の傾向を表示します。明るく表示されている行をクリックすると、下記のどちらかの情報が表示されます。
  - セキュリティ関連カテゴリ（例、不正な）の場合、Threats ダッシュボード表示し、そこからさらに詳しく調査できます。
  - 他のカテゴリ（例、アダルト）の場合、より詳細な情報を含む調査レポートを表示します。
- **[Clients with Security Risks（セキュリティ リスクがあるクライアント）]** は、Security Risk サイトに関連するコンピュータを表示します。これらのコンピュータがウィルスやスパイウェアに感染していないかチェックすることができます。

- **[Top Security Risk Categories（上位セキュリティ リスク カテゴリ）]** は、セキュリティ リスク カテゴリの中で最も多くの要求を受け取ったカテゴリを表示します。この情報は現在のポリシーがネットワークに適した保護を提供しているかどうか判断するのに役立ちます。
- **[Risk Classes（リスク クラス）]** は、各リスク クラスへの要求が許可またはブロックされた数を表示します（*リスク クラス、64 ページ*を参照）。この情報は、現在のポリシーが有効かどうか判断するのに役立ちます。
- **Top Uncategorized（上位未分類）]** は、Websense マスタ データベースで分類されていない URL のうち、アクセス回数が多いものを表示します。**[Filter Components（フィルター コンポーネント）] > [Edit Categories（カテゴリーの編集]** を順に選択し、URL をカテゴリに割り当てます。
- （*Web Security Gateway および Gateway Anywhere*）**[Analytics:Security Risks（分析：セキュリティ リスク）]** は、コンテンツが変更されたか、サイトのセキュリティが弱くなったために Content Gateway の分析によって新しいカテゴリに割り当てられた要求の数を表示します。

ページの任意のチャートをクリックすると、より詳細な情報を含む調査レポートが開きます。

Usage ダッシュボード

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *System ダッシュボード、52 ページ*
- *Risks ダッシュボード、50 ページ*
- *Threats ダッシュボード、41 ページ*
- *ダッシュボード タブに要素を追加する、53 ページ*

Web Security ダッシュボードの **[Usage（使用状況）]** タブを使用して、組織の一般的なインターネット アクティビティの傾向をモニタできます。デフォルトでは、下記のチャートが表示されます。

- **[Top Blocked Users（ブロックされた上位ユーザ）]** は、要求したサイトがブロックされた回数が多いユーザーを表示します。
- **[Top Requested Categories（要求された上位カテゴリ）]** は、最もアクセス回数が多いカテゴリを表示して、セキュリティ、帯域幅、生産性に関して予想される問題の概要を提供します。より詳細な情報を含む調査レポートを表示するには、チャートをクリックします。
- **[Enforcement Summary（強制の要約）]** は、セキュリティ リスク クラスに含まれるサイトに対する最近の許可された要求とブロックされた要求、および他のブロックされた要求の概要を表示します。

- （*Web Security Gateway および Gateway Anywhere*）**[Web 2.0 Categories（Web 2.0 カテゴリ）]** は、要求された Web 2.0 URL に割り当てられているカテゴリのうちの要求回数が多いものを表示します。
- （*Web Security Gateway および Gateway Anywhere*）**[Web 2.0 URL Bandwidth（Web 2.0 帯域幅）]** は、帯域幅を最も多く使用している Web 2.0 URL を表示します。
- （*Web Security Gateway および Gateway Anywhere*）**[Analytics: Top Categories（分析：上位カテゴリ）]** は、スキャンによって URL が元のカテゴリに適合しないと判断された後に、要求された URL が割り当てられた回数が多いカテゴリを表示します。

任意のチャートまたは要素（30-Day Activity Summary を除く）をクリックして、より詳細な情報が含む調査レポートを開きます。

System ダッシュボード

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Threats ダッシュボード、41 ページ*
- *Risks ダッシュボード、50 ページ*
- *Usage ダッシュボード、51 ページ*
- *ダッシュボード タブに要素を追加する、53 ページ*

Web Security Dashboard の **[System]** タブを使用して、環境のステータスをモニタします。デフォルトでは、以下のダッシュボードの要素が表示されます。

- **[Health Alert Summary（ヘルス アラートの要約）]** は、コンポーネントのアラート メッセージとステータス メッセージを表示します。要約にエラーまたは警告が表示された場合、アラート メッセージをクリックして [Alerts（アラート）] ページを開きます。ここでより詳細な情報を入手できます（*現在のシステム ステータスの確認、490 ページ*を参照）。

  [Health Alert Summary] の情報は、30 秒ごとに更新されます。
- **[User Activity:Zoom Trend（ユーザーのアクティビティ：傾向をズーム）]** は、選択された期間中ログ データベースに登録されているインターネット要求の数を表示します。
  - カーソルをクリックし、ドラッグして、チャートの中の詳しく検討するセクションを選択します。この動作を繰り返すことによって、より短い時間帯を選択し、詳しく検討することができます。
  - 最大ズームでは、データ ポイントが 10 分ごとに表示されます（例、12:00:00、12:10:00、12:20:00）。

チャートのデフォルト（マクロ）ビューが表示されている場合、各データ ポイントは、チャートの選択したエリア内での複数の 10 分間隔のデータ ポイントのサンプリングをベースに作成されます。そのため、マクロ ビューに表示される数は、チャートが拡大されたときに表示される数と正確には対応しない場合があります。

- **[Zoom Out（縮小）]** をクリックして、前のフォーカス レベルに戻ります。
- **[Reset Chart（チャートをリセット）]** をクリックしてデフォルトの詳細レベルに戻ります。

- **[Protocol Bandwidth Use（プロトコルの帯域幅使用）]** は、ネットワークで最も多くの帯域幅を使っているプロトコルを表示します。
- **[Filtering Service Status（Filtering Service のステータス）]** は、現在の Policy Server に関連する各 Filtering Service のステータスを表示します。

  Filtering Service IP アドレスをクリックして、Network Agent および Content Gateway との接続ステータスを含むその Filtering Service インスタンスに関するより詳細な情報を確認します。*Filtering Service 詳細の確認*、466 ページを参照してください。
- （*Web Security Gateway Anywhere*）**[Hybrid Bandwidth Summary（ハイブリッド帯域幅の要約）]** は、ハイブリッド サービスによって管理されているインターネット要求によって消費された帯域幅を表示します。
- （*Web Security Gateway Anywhere*）**[Hybrid Requests（ハイブリッド要求）]** は、ハイブリッド サービスによって許可およびブロックされた組織のユーザーによる要求数を表示します。

ダッシュボード タブに要素を追加する

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Status] > [Dashboard] > [Add Chart（チャートを追加）] ページを使用して Risk、Usage、または System ダッシュボードに要素を追加します。

Threats ダッシュボードの要素の追加または削除はできません。

最初に、**[Add elements to tab（タブに要素を追加）]** ドロップダウン リストを使用してタブを選択し、次に **[Dashboard Elements（ダッシュボードの要素）]** リストから追加する要素を選択します。

- どのタブにも要素を追加できます。
- 各タブには最大 12 個の要素を表示できます。
- 選択したタブに現在表示されている要素は、青い丸のアイコンで示されます。
- 同じ要素の複数のコピーをタブに追加できます（例、要素のそれぞれのコピーが異なる時間を示すようにする）。

リストで要素を選択したとき、**[Preview（プレビュー）]** ペインにサンプルが表示されます。プレビュー ペインを使用して、チャートの **[Name（名前）]**、もしあれば、**[Chart type（チャートのタイプ）]**、**[Time period（期間）]**、および **[Top（上位）]** の値（例、上位 1 ～ 5 のカテゴリ、または上位 16 ～ 20 のユーザー）への変更を行うことができます。

- **[Chart type]**：多くのチャートは、複数折れ線グラフ、棒グラフ、折れ線グラフ、積み上げ面グラフ、または積み上げ棒グラフとして表示できます。一部のチャートは、棒グラフ、折れ線グラフ、または円グラフとして表示できます。使用できるグラフのタイプは、表示されるデータによって異なります。
- **Time period**：ほとんどのチャートでは、表示対象の期間を変更できます。たとえば、本日（現在の日の午前 0 時以降の時間）、最後の 7 日間、または最後の 30 日間などです。ダッシュボードのチャートの最大期間を延長した場合、チャートも最後の 180 日間、または 365 日間を表示できるようになります。
  - Microsoft SQL Server Express の場合、ダッシュボード チャートの最大期間は、30 日間で、変更できません。
  - デフォルトの最大期間（30 日間）を使用するとダッシュボードのパフォーマンスが向上します。

  ダッシュボードのチャートの期間延長の詳細については、*ダッシュボードのレポーティング データの設定、531 ページ*を参照してください。
- **[Top]**：上位のユーザー、カテゴリ、URL などに関する情報を表示するチャートは、最大 5 つの値を表示できます。上位 5 つの値、6 ～ 10 位の値、11 ～ 15 位の値、16 ～ 20 位の値のどれを表示するか選択します。

変更を完了したとき、**[OK]** をクリックします。ダッシュボード タブがすぐに更新されます。

チャートの編集をしていたが、初めからやり直したい場合は、**[Restore Defaults（デフォルトの復元）]** をクリックして、チャートをそのデフォルトの期間、タイプ、および上位の値（もしあれば）にリセットします。

デフォルトでは 2 つのダッシュボードの要素がタブに表示されませんが、それらの要素を追加することができます。

- **[30-Day Value Estimates（30 日間の推定値）]** は、本日を含む 30 日間に Web セキュリティ ソフトウェアによって得られる時間および帯域幅の節約を推定する方法を提供します。

  推定値の計算方法の説明を表示するには、マウスを **[Time（時間）]** または **[Bandwidth（帯域幅）]** の項目（[Saved（節約）の下）の上に置きます（*節約される時間と帯域幅、55 ページ*を参照）。計算は [Add Charts（チャートを追加）] ページでカスタマイズできます。

- **[Activity Today（本日のアクティビティ）]** は、Web セキュリティ ソフトウェアが本日どのようにネットワークを保護していたかを示す例を示します。サブスクリプション タイプに従って、ブロックされた不正なサイト、アダルト サイト、スパイウェア サイトおよび Content Gateway によってスキャンされたまたはスキャンされ再分類されたサイトに関する情報を表示します。

  この要素はまた、本日のこれまでに処理したインターネット要求の合計数、ブロックした要求の合計数、および処理したリアルタイム データーベース更新の数も示します。

節約される時間と帯域幅

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense web セキュリティ ソリューションは、無駄な時間と帯域幅の損失を最小限に抑えるのに役立ちます。

[Value Estimates（推定値）] はデフォルトでは表示されませんが、Web Security Dashboard に追加してこれらの時間および帯域幅の節約の推定値を示すことができます。これらの値は下記のように計算されます。

- 節約した時間：**閲覧あたりにかかった一般的な時間**に**ブロックされたサイト**の数をかけます。最初に、ユーザーが要求したウェブサイトの閲覧に消費した平均時間（秒）としてデフォルト値が使用されます。ブロックされたサイトの数の値は、利用可能な期間中（[Settings] > [Reporting] > [Dashboard] ページで設定された最大期間まで）にブロックされた要求の合計数を表します。
- 節約した帯域幅：**閲覧あたりの一般的な時間**に**ブロックされたサイト**の数をかけます。最初に、平均ウェブサイトによって消費した平均バイト数としてデフォルト値が使用されます。ブロックされたサイトの数の値は、利用可能な期間中（[Settings] > [Reporting] > [Dashboard] ページで設定された最大期間まで）にブロックされた要求の合計数を表します。

チャートにダッシュボードを追加した後、マウスをカウンタの上で動かし、値が現在計算される方法を確認します。

計算された値を変更するには、マウスをチャートのツールバーに含まれている **[Options]** アイコンの上で動かし、**[Edit]** を選択します。[Edit] ページで、

下記のオプションを使用して計算の基礎として使用する新しい平均的時間および帯域幅の測定値を入力します。

オプション	説明
ブロック ページごとに節約された平均時間（秒）	ユーザーが個別のページを閲覧するのに費やすと組織が推定する平均時間（秒）を入力します。 この値とブロックされたページの数の積を計算し、その値が節約された時間として表示されます。
ブロック ページごとに節約された平均帯域幅 [KB]	閲覧されるページの平均サイズを単位キロバイト（KB）で入力します。 この値とブロックされたページの数の積を計算し、その値が節約された帯域幅として表示します。

変更を完了したとき、**[OK]** をクリックしてダッシュボードに戻ります。

Web Security Status Monitor（ステータス モニタ）モード

Web Security Help | Web Security ソリューション | バージョン 7.8.x

セキュリティ上の理由で、TRITON コンソール セッションは、30 分間非アクティブになると終了します。しかし、Status Monitor モードにして、タイムアウトせずにインターネット アクティビティおよびアラート データをモニタできます。

- Web Security manager で Status Monitor モードにするには、他の TRITON 管理モジュールをログ オフする必要があります。
- Status Monitor モードの場合、[Status] > [Dashboard, Status（ダッシュボード、ステータス）] > [Alerts, Status（アラート、ステータス）] > [Deployment, and Reporting（配備およびレポーティング）] > [Real-Time Monitor（リアルタイム モニタ）] ページの情報は、ブラウザを閉じるかログ オフするまで通常通り、継続的に更新されます。

Status Monitor モードを開始するには、最初に未反映の変更を保存するか、または破棄します。次に下記の手順を実行します。

- [Web Security] ツールバーの **[Role（ロール）]** から **[Status Monitor]** モードを選択します。
- [Status] > [Dashboard] または [Status] > [Alerts] ページの上部のツールバーの **[Status Monitor]** ボタンをクリックします。

Web Security のステータスのモニタを停止するには、TRITON コンソールをログ オフするか、またはブラウザを閉じます。

3 インターネット使用状況のフィルタ

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリおよびプロトコルへのアクセスの管理*、59 ページ
- *フィルタの使用*、71 ページ
- *フィルタリング設定値の設定*、81 ページ
- *インターネット アクセスのポリシー*、111 ページ
- *Web Security ポリシーの調整*、313 ページ

ポリシーはユーザーのインターネット アクセスを管理します。ポリシーとは、いつ、どのようにウェブサイトとインターネット アプリケーションをフィルタするべきかを決定するスケジュールのことです。もっとも単純なポリシーは、下記の要素から成ります。

- **カテゴリ フィルタ**、ウェブサイト カテゴリに処置（[許可]または[ブロック]）を適用するために使用します。
- **プロトコル フィルタ**。インターネット アプリケーションおよび非 HTTP プロトコルに処置を適用するために使用します。

> **注意**
> Websense Web Security Gateway Anywhere 環境の場合、ハイブリッド サービスは、プロトコル フィルタリングを適用しません。

- 各フィルタをいつ適用するかを決定するスケジュール

ポリシーによって、クライアント（例、ユーザー、グループ、ネットワーク内の IP アドレス）に種々のレベルのインターネット アクセスを割り当てることができます。最初に、インターネット アクセスの制限を具体的に定義するフィルタを作成し、次にフィルタを使用してポリシーを作成します。

最初にインストールする場合、サブスクリプション キーが入力されたとき、即座にそのポリシーを使用してインターネット要求のモニタリングを開始するために **Default（デフォルト）**ポリシーが使用されます（*Default ポリシー、112 ページ*を参照）。最初に、Default ポリシーはすべての要求を許可します。

> **注意**
> Websense Web Security の以前のバージョンからアップグレードするとき、既存のポリシー設定は保存されます。アップグレード後にポリシーを調べてそれらが今でも適切であることを確認します。

種々のクライアントに異なるアクセスのレベルを適用するには、カテゴリ フィルタの定義から開始します。下記のフィルターを定義できます。

- [ビジネス & 経済]、[教育]、および[ニュース & メディア]のカテゴリに含まれているウェブサイト以外のすべてのウェブサイトへのアクセスをブロックする 1 番目のカテゴリ フィルター。
- セキュリティ リスクを表すウェブサイトとアダルト マテリアルを含んでいるウェブサイト以外のすべてのウェブサイトを許可する 2 番目のカテゴリ フィルター。
- ウェブサイトをブロックしないでウェブサイトへのアクセスをモニタする 3 番目のカテゴリ フィルタ（*カテゴリ フィルタの作成、72 ページ*を参照）

これらのカテゴリ フィルタに加えて、下記のフィルタを定義できます。

- インスタント メッセージ & チャット、P2P ファイル共有、プロキシ回避、およびストリーミング メディアのプロトコル グループへのアクセスをブロックする 1 番目のプロトコル フィルタ
- セキュリティ リスクおよびプロキシ回避に関連する非 HTTP プロトコル以外のすべての非 HTTP プロトコルを許可する 2 番目のプロトコル フィルター
- すべての非 HTTP プロトコルを許可する 3 番目のプロトコル フィルター（*プロトコル フィルタの作成、76 ページ*を参照）

組織のインターネット アクセス規制に対応するフィルタのセットを定義した後、それらをポリシーに追加して、クライアントに適用できます（*インターネット アクセスのポリシー、111 ページ*を参照）。

カテゴリおよびプロトコルへのアクセスの管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリまたはプロトコルがブロックされる場合、61 ページ*
- *新しいマスター データベースのカテゴリおよびプロトコル、61 ページ*
- *特別なカテゴリ、62 ページ*
- *リスク クラス、64 ページ*
- *セキュリティ プロトコル グループ、67 ページ*

Websense マスタ データベースは、類似するウェブサイト（URL および IP アドレスによって特定される）を **カテゴリ**別に編成します。各カテゴリは、[アダルト マテリアル]、[ギャンブル]、[ピアツーピア共有ファイル] などの記述名が付いています。また、組織にとって特に関心があるグループサイトにユーザー独自のカスタム カテゴリを作成することもできます（*カスタム カテゴリの作成、326 ページ*を参照）。マスター データベースのカテゴリとユーザー定義のカテゴリは共に、インターネット アクセス管理の基準になります。

Websense, Inc. は、マスター データベースの中のカテゴリまたはサイトについて価値を判断しません。カテゴリは、購読している顧客に関係するサイトの便利なグループ化を作成ができるように設計されています。それらは任意のサイト、サイトのグループ、サイトの発行者や営利団体を特徴付けることを目的としていません。また、そうすることはできないようになっています。同様に Websense カテゴリに添付してあるラベルは、便利な速記式になっており、いかなる意見や態度、賛同や反対を、それぞれに分類された主題やサイトに対して提示するようには作成していません。

最新のマスター データベースのカテゴリのリストは、下記の URL から入手できます。

websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php

サイトをマスター データベースに追加する、またはサイトをカテゴリ間で移動するよう指示するには、**support.websense.com** に移動し、**[Site Lookup Tool（サイト検索ツール）]** をクリックします。MyWebsense にログオンするように求められ、次にこのツールへのアクセスが許可されます。ここでサイトに割り当てられている現在のカテゴリを確認し、新しいカテゴリを要求することができます。

カテゴリ フィルタを作成するとき、ブロックするカテゴリと許可するカテゴリを選択します。

URL カテゴリの格納のほかに、Websense マスター データベースは、非 HTTP インターネット トラフィックを管理するために使用するプロトコル グループを含んでいます。各プロトコル グループは、インターネット プロトコル（FTP、IRC など）およびアプリケーション（MSN Messenger、BitTorrent など）のインターネット プロトコルの類似するタイプを定義します。定義は、毎夜のように頻繁に確認および更新されます。

カテゴリと同じく、カスタム プロトコルをポリシーで使用するように定義できます。

最新のマスター データベースのプロトコルのリストは、下記の URL から入手できます。

websense.com/global/en/ProductsServices/MasterDatabase/ProtocolCategories.php

プロトコル フィルタを作成するとき、ブロックするプロトコルと許可するプロトコルを選択します。

注意

Websense Web Filter および Web Security 環境では、プロトコルベースのポリシー適用を有効化するために Network Agent をインストールする必要があります。

Websense Web Security Gateway および Gateway Anywhere の場合は、Network Agent を使用せずに HTTP ポートをトンネリングする非 HTTP プロトコルをフィルタリングできます。詳細は、*トンネリング プロトコルの検出*、235 ページを参照してください。

Websense Web Security Gateway Anywhere のハイブリッド サービスは、プロトコルのフィルタを適用しません。

一部の Websense 定義プロトコルは、外部サーバー、たとえば特殊なインスタント メッセージング サーバーを宛先とするアウトバウンド インターネット トラフィックのブロックを可能にします。ダイナミックに割り当てたポート番号を持つ Websense が定義したプロトコルだけが、外部トラフィックとしてブロックされます。

カテゴリまたはプロトコルがブロックされる場合

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ユーザーがブロックされているカテゴリに含まれている URL を要求したとき、ブラウザは、要求されたサイトではなく、**ブロック ページ**を表示します。ブロック ページは要求された URL がブロックされた理由を示す簡単な説明を示すカスタマイズ可能な HTML ページです。

ブロック ページの詳細、およびブロック ページのカスタマイズの詳細については、*ブロック ページ*、143 ページを参照してください。

ユーザーがブロックされたプロトコルに依存しているアプリケーション（例、チャット プログラム、トーレント プログラム）を使用しようとしたとき、ブロック メッセージは表示されません。アプリケーションはエラー メッセージを表示するか、または単にハングしたようになります。

ブロックされたプロトコルへのアクセスを試みているユーザーからのエラー レポートを減らすために、ユーザーが組織の機器上でどのアプリケーションの使用が許可または禁止されているかを理解していることが重要です。

新しいマスター データベースのカテゴリおよびプロトコル

Web Security Help | Web Security ソリューション | バージョン 7.8.x

新しいカテゴリおよびプロトコルをマスター データベースに追加したとき、それらの各カテゴリおよびプロトコルには **[Permit（許可）]** や **[Block（ブロック）]** などのデフォルトの処置が割り当てられます（*処置*、68 ページを参照）。

- デフォルトの処置は、すべてのアクティブなカテゴリ フィルタおよびプロトコルのフィルタに適用されます（*フィルタの使用*、71 ページを参照）。カテゴリまたはプロトコルがフィルタリングされる方法を変更するには、下記のどちらかの手順を実行します。
  - アクティブな各フィルターを別個に編集します。クライアントの種々のグループにカテゴリまたはプロトコルへの種々のレベルのアクセス権限を与える場合は、このオプションを使用します。
  - 全てのフィルタで同じ処置を適用するには、カテゴリまたはプロトコルの属性を編集します。*グローバル カテゴリの変更 [グローバル カテゴリのへんこう]*、324 ページおよび *グローバル カテゴリの変更 [グローバル カテゴリのへんこう]*、339 ページを参照してください。
- デフォルトの処置は、当該のサイトまたはプロトコルが一般的にビジネスに適していると見なされるかどうかに関するフィードバックを基準にしています。

新しいカテゴリまたは プロトコルがマスター データベースに新しいカテゴリまたはプロトコルが追加されたときは常にシステム アラートを生成させるように設定できます。詳細は、*警告*、481 ページを参照してください。

特別なカテゴリ

Web Security Help | Web Security ソリューション | バージョン 7.8.x

マスター データベースは、特定のタイプのインターネット使用状況を管理するために役立つ特別なカテゴリを含んでいます。以下のカテゴリは、すべての Websense Web Security ソリューションで使用できます。

- **[Special Events（スペシャル イベント）]** カテゴリは、ホット トピックと見なされるサイトを分類するために使用します。これは特別のイベントに関連するインターネット トラフィックの急増を管理するのに役立ちます。たとえば、公式の [World Cup（ワールド カップ）] サイトは、一般的には [Sports（スポーツ）] カテゴリに示されますが、World Cup Finals（ワールドカップ決勝戦）時には [Special Events（スペシャル イベント）] カテゴリに移動されます。

  [Special Events] カテゴリへの更新は、スケジュール設定されたダウンロード中にマスター データベースに追加されます。サイトは短時間でこのカテゴリに追加され、その後別のカテゴリに移動されるか、またはマスター データベースから削除されます。
- **[Productivity（生産性）]** カテゴリは、時間を無駄にする動作がないようにすることに重点を置いています。
  - 広告宣伝
  - アプリケーション / ソフトウェアのダウンロード
  - インスタント メッセージ
  - 掲示板 & フォーラム
  - オンライン委託販売 & トレーディング
  - 報酬サイト
- **[Bandwidth（帯域幅）]** カテゴリは、ネットワーク帯域幅の節約に重点を置いています。
  - 教育ビデオ
  - 娯楽ビデオ
  - インターネット ラジオ / テレビ
  - インターネット電話
  - ピアツーピア ファイル共有
  - 個人用ネットワーク・ファイル保存 / バックアップ
  - ストリーミング メディア
  - 監視
  - ウイルス性ビデオ

Websense Web Security、Web Security Gateway、および Web Security Gateway Anywhere には、下記に示すそのほかのセキュリティ カテゴリが含まれています。

- **[Security（セキュリティ）]** は、ウィルス検出ソフトウェア プログラムをバイパスする可能性がある不正なコードを含んでいるインターネット サイトに重点を置いています。
  - 新型のマルウェア コマンドおよびコントロール（Content Gateway が必要）
  - 新型のマルウェア ペイロード（Content Gateway が必要）
  - ボット ネットワーク
  - カスタム暗号化アップロード（Content Gateway が必要）
  - パスワードを含んでいるファイル（Content Gateway が必要）
  - キーロガー
  - 不正な埋め込まれた i フレーム
  - 不正な埋め込まれたリンク
  - 不正な Web サイト
  - フィッシングとその他詐欺サイト
  - エクスプロイトされる可能性が高いドキュメント（Content Gateway が必要）
  - 不要になる可能性が高いフトウェア
  - スパイウェア
  - 疑わしい埋め込まれたリンク
- **[Extended Protection（拡張保護）]** は、不正の可能性の高い Web サイトに重点を置いています。
  - **[Dynamic DNS（ダイナミック DNS）]** は、ダイナミック DNS サービスを使って ID をマスクするサイトを含みます。これらのサイトは多くの場合、精巧で持続的な脅威に関連しています。
  - **[Elevated Exposure（高度のエクスポージャー）]** は、本当の性質や ID をカモフラージュするサイトや、悪意が含まれることを示唆する要素を含むサイトを含みます。
  - **[Emerging Exploits（新種のエクスプロイト）]** は、既知のまたは潜在的なエクスプロイト コードをホストしていることが判明したサイトを含みます。
  - **[Suspicious Content（疑わしいコンテンツ）]** は、有用なコンテンツをほとんど、または全く含まないと考えられるサイトを含みます。

[Extended Protection] グループは、*定評*をベースに、不正な可能性の高いウェブサイトをフィルタします。サイトの定評は、不正な可能性のあるアクティビティの初期の兆候を基にしています。アタッカーは、たとえば、一般的な誤ったつづりを含む URL や正しいつづりの URL に類似する URL を標的とすることがあります。そのようなサイトは、従来のフィルターが更新されこれらのサイトが不正として反映される前にユーザーにマルウェアを配信ために使用される可能性があります。

When Websense のセキュリティ研究者が潜在的な脅威を含むサイトを検出したとき、研究者がそのサイトの最終のカテゴリ化を 100 % 確信するまで、そのサイトは [Extended Protection] カテゴリに入れられます。

リスク クラス

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリのリスク クラスへの割り当て、502 ページ*
- *プレゼンテーション レポート、161 ページ*
- *調査レポート、187 ページ*

Websense マスター データベース はカテゴリを**リスク クラス**に分類します。リスク クラスは、カテゴリのグループに含まれているサイトによってもたらされる可能性がある脆弱性のタイプまたはレベルを提案します。

リスク クラスは主にレポーティングで使用されます。Web Security Dashboard は、インターネット アクティビティがリスク クラス別に表示されるグラフを含んでおり、またリスク クラス別に編成されたプレゼンテーション レポートまたは調査レポートを作成できます。

リスク クラスはまた、カテゴリ フィルタの作成にも役立ちます。たとえば、最初に、[Basic Security（基本セキュリティ）] カテゴリ フィルタが [Security Risk（セキュリティ リスク）] クラスに含まれているすべてのデフォルトのカテゴリをブロックします。独自のカテゴリ フィルタを作成するときガイドラインとしてリスク クラスのグループ化を使用することができます。これはカテゴリを何らかの方法で許可するか、ブロックするか、制限するかを判断するのに役立ちます。

5 つのリスク クラスがあります。デフォルトでは、各リスク クラスは下記にリストしているカテゴリを含みます。

- カテゴリは複数のリスク クラスに示されることがあり、またどのリスク クラスにも割り当てられないことがあります。
- マスター データベースではグループ化が定期的に変更されます。新しいカテゴリがマスター データベースに追加されたという通知を受け取ったとき、デフォルト リスク クラスの割り当てを確認することをお勧めします。

Legal Liability（法的責任）

アダルト マテリアル（アダルト コンテンツ、ランジェリー、水着、ヌード、セックスを含む）
帯域幅 > ピアツーピア ファイル共有
ギャンブル
違法行為または不審な行為

Legal Liability（法的責任）

IT（情報技術）> ハッキングおよびプリキシ回避
不寛容
過激派グループ
悪趣味
暴力
武器

Network Bandwidth Loss（ネットワーク帯域幅損失）

帯域幅（教育ビデオ、娯楽ビデオ、インターネット ラジオ / テレビ、インターネット電話、
娯楽 > メディアファイル ダウンロード サービス
生産性 > 広告宣伝、アプリケーションおよびソフトウェア ダウンロード
ソーシャル Web コントロール - フェイスブック > フェイスブック ビデオ アップロード
ソーシャル Web コントロール - ユーチューブ > ユーチューブ ビデオ アップロード

Business Usage（業務関連の使用）

帯域幅 > 教育ビデオ
ビジネスおよび経済（金融情報＆サービス、ホストされている業務用アプリケーションを含む）
教育 > 教材、参考資料
政府（軍隊を含む）
ソーシャル Web のコントロール - LinkedIn（includes LinkedIn のつながり、LinkedIn のジョブ、LinkedIn メール、LinkedIn の更新を含む）
IT（コンピュータ セキュリティ情報、検索エンジンおよびポータル、WebCollaboration および URL 翻訳サイトを含む）
旅行
乗物

Security Risk（セキュリティ リスク）

帯域幅 > ピアツーピア ファイル共有
拡張保護（ダイナミック DNS、高い暴露、新たなエクスプロイト、新規に登録された Web ウェブサイト、疑わしいコンテンツを含みます）[*Websense Web Security*]
IT > ハッキング、プロキシ回避、Web および電子メール スパム
パーク ドメイン
生産性 > アプリケーション / ソフトウェアのダウンロード

Security Risk（セキュリティ リスク）

セキュリティ（ボット ネットワーク、安全でない Web サイト、キーロガー、不正な埋め込まれた i フレーム、不正な埋め込まれたリンク、不正な Web サイト、フィッシングとその他詐欺サイト、不要になる可能性が高いフトウェア、スパイウェア、疑わしい埋め込まれたリンクを含む）[*Websense Web Security*]

Web Security Gateway および Gateway Anywhere の場合は、最新のマルウェア コマンドおよびコントロール、最新のマルウェア ペイロード、カスタム暗号化アップロード、パスワードを含んでいるファイル、および エクスプロイトされる可能性が高いドキュメント も含みます。

Productivity Loss（生産性の損失）

妊娠中絶（妊娠中絶賛成論、妊娠中絶反対論を含む）

アダルト マテリアル > 性教育

権利擁護団体

帯域幅 > 娯楽ビデオ、インターネット ラジオ / テレビ、ピアツーピア ファイル共有、ストリーミング メディア、監視、ウィルス性ビデオ

ドラッグ（薬物乱用、マリファナ、処方薬、栄養補助食品、および規制されていない化合物を含む）

教育（文化団体、教育機関を含む）

娯楽（メディアファイル ダウンロード サービスを含む）

ギャンブル

ゲーム

政府 > 政治組織

健康

IT > Web および電子メール スパム、Web ホスティング

インターネット通信（一般的な電子メール、組織の電子メール、テキストおよびメディア メッセージング、Web チャットを含む）

求人情報

ニュースおよびメディア（オルタナティブ ジャーナルを含む）

パーク ドメイン

生産性（アプリケーション / ソフトウェアのダウンロード、インスタント メッセージング、掲示板 & フォーラム、オンライン委託販売 & トレーディング、報酬サイトを含む）

宗教（新興宗教、伝統的宗教を含む）

ショッピング（インターネット オークション、不動産を含む）

社会組織（専門家・従業員団体、奉仕・慈善事業団体、および友好団体を含む）

ソーシャル Web コントロール - フェイスブック（フェイスブック アプリ、フェイスブック チャット、フェイスブック コメンティング、フェイスブック イベント、フェイスブック フレンド、フェイスブック ゲーム、フェイスブック グループ、フェイスブック メール、フェイスブック写真のアップロード、フェイスブック ポスティング、フェイスブック質問、フェイスブック ビデオのアップロードを含む ）

ソーシャル Web のコントロール - LinkedIn（includes LinkedIn のつながり、LinkedIn のジョブ、LinkedIn メール、LinkedIn の更新を含む）

Productivity Loss（生産性の損失）

ソーシャル Web のコントロール - ツイッター（ツイッター フォロー、ツイッター メール、ツイッター ポスティングを含む）

ソーシャル Web のコントロール - 各種（Blog コメンティング、Blog ポスティング、Classifieds ポスティングを含む）

ソーシャル Web のコントロール - ユーチューブ（ユーチューブ コメンティング、ユーチューブ共有、ユーチューブ ビデオのアップロードを含む）

社会 & ライフスタイル（アルコールおよびタバコ、ブログおよび個人サイト、ゲイまたはレズビアンまたはバイセクシュアル関連、出会い系＆結婚 / お見合いサービス

スペシャル イベント

スポーツ（スポーツハンティング / 射撃クラブを含む）

旅行

乗物

優先管理者は、各リンクに割り当てられているカテゴリを **[Settings] > [General] > [Risk Class（リスク クラス）]** ページで変更できます（*カテゴリのリスク クラスへの割り当て、502 ページ*を参照）。

セキュリティ プロトコル グループ

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Security] および [Extended Protection] のカテゴリのほかに、Websense Web Security は、インターネット上で送信されたスパイウェアおよび不正なコードまたはコンテンツの検出しそれらからの保護に役立てるために 2 つの プロトコル グループを含んでいます。

- **[Malicious Traffic（不正なトラヒック）]** プロトコル グループは、**[Bot Networks（ボット ネットワーク）]** プロトコルを含み、このプロトコルは不正目的でボットネットによって接続を試みるボットによって生成されたコマンド & コントロール トラフィックをブロックすることを目的としています。
- The **[Malicious Traffic（Cannot block）（不正なトラフィック（ブロック不能））]** プロトコル グループは、不正なソフトウェアに関連する可能性があるトラフィックを特定するために使用されます。
  - **[Email-Borne Worms（電子メールに含まれているワーム）]** は、電子メールベースのワーム攻撃によって生成された可能性があるアウトバウンド SMTP トラヒックを追跡します。
  - **[Other（その他）]** は、不正なアプリケーションとの接続の疑いがあるインバウンドおよびアウトバウンド トラフィックを追跡します。

[Malicious Traffic] プロトコル グループは、デフォルトではブロックされ、またこれはプロトコル フィルタ内部で設定できます（*プロトコル フィルタの編集、77 ページ*を参照）。[Malicious Traffic（Cannot block）] プロトコルは、レポーティングのためにログに記録できますが、他の処置を適用できません。

処置

Web Security Help | Web Security ソリューション | バージョン 7.8.x

カテゴリおよびプロトコル フィルターは、各カテゴリまたはフィルタに**処置**を割り当てます。これは、クライアントのインターネット要求の際に Websense フィルタリング ソフトウェアが行う処置です。下記の処置がカテゴリとプロトコルの両方に適用します。

- 要求を **[Block（ブロック）]**。ユーザーはブロック ページまたはブロック メッセージを受け取り、サイトの表示やインターネット アプリケーションの使用ができなくなります。
- 要求を**[Permit（許可）]**。ユーザーはサイトを表示したりインターネット アプリケーションを使用したりできます。
- 要求をブロックするまたは許可する前に、現在の **[Bandwidth（帯域幅）]** 使用量を評価します。この処置が有効化されており、帯域幅が指定したしきい値に到達したとき、特定のカテゴリまたはプロトコルのこれ以上のインターネット要求がブロックされます。*Bandwidth Optimizer による帯域幅の管理*、342 ページを参照してください。

カテゴリにだけその他の処置を割り当てることができます。

- **[Confirm（確認）]**- ユーザーはブロック ページを受け取り、そこでサイトを業務目的のためにアクセスしているのかユーザーに尋ねます。ユーザーが **[Continue（続行）]** をクリックした場合は、そのサイトを表示できます。

  [Continue] をクリックするとタイマーが起動します。設定した時間の間（デフォルトでは 60 秒）、ユーザが [Confirm] カテゴリに含まれる別のサイトにアクセスしても、別のブロック ページは表示されません。設定時間が終了した後、他の [Confirm] サイトを閲覧すると、別のブロック ページが表示されます。

  デフォルト時間は、**[Settings] > [General] > [Filtering]** ページで変更できます。

- **[Quota（割り当て）]**- ユーザーはブロック ページを受け取り、サイトを表示するために割り当て時間を使用するかどうかユーザーに尋ねます。ユーザーが **[Use Quota Time（割り当て時間を使用）]** をクリックした場合は、そのサイトを表示できます。

  [Use Quota Time] をクリックすると下記の 2 つのタイマーが起動します。割り当てセッション タイマーと合計の割り当て配分タイマーです。

  - ユーザーがデフォルトの**セッション**時間（デフォルトでは 10 分）中に他の割り当てサイトを要求した場合は、別のブロック ページを受け取らずにこれらのサイトにアクセスできます。

- **合計**の割り当て時間は毎日配分されます。割り当て時間がなくなると、各クライアントは翌日にならないと割り当て時間カテゴリにあるサイトにアクセスできません。デフォルトの毎日の割り当て配分（デフォルトでは 60 分）は、**[Settings] > [General] > [Filtering]** ページで設定します。毎日の割り当て配分は、クライアントごとに個別に配分することもできます。詳細は、*割り当て時間を使ってインターネット アクセスを制限する、69 ページ*を参照してください。

> **重要**
> 複数の Filtering Service が配備されている環境では、Websense State Server は [Confirm] および [Quota] 処置を正しく適用することを求められます。詳細は、*Policy Server、Filtering Service、および State Server、469 ページ*を参照してください。

- **Block Keywords（キーワードをブロック）**：キーワードを指定し、キーワードのブロックを有効化したとき、ユーザーが要求するサイトの URL にブロックされているキーワードが含まれる場合、そのサイトにアクセスできません。*キーワードベースのポリシーの実施、327 ページ*を参照してください。
- **Block File Types（ファイル タイプをブロック）**：ファイル タイプのブロックが有効化されたとき、ユーザーがブロックされているタイプのファイルをダウンロードしようとすると、ブロック ページを受け取り、そのファイルをダウンロードできません。*ファイル タイプに基づくトラフィックの管理、345 ページ*を参照してください。

割り当て時間を使ってインターネット アクセスを制限する

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ユーザーが [Use Quota Time（割り当て時間の使用）]、をクリックしたとき、割り当てセッションが終了するまで、割り当てカテゴリに含まれているサイトを表示できます。デフォルトの割り当てセッション時間（**[Settings] > [General] > [Filtering]** ページから）は 10 分です。

割り当てセッションが終了したあと、割り当てサイトを要求すると、別の割り当てブロック メッセージが表示されます。毎日の割り当て配分を使い切っていないユーザーは、新しい割り当てセッションを開始できます。

割り当て時間が設定されると、ユーザーが割り当て時間カテゴリにあるサイトを要求した時に、Filtering Service は優先順位リストを使用して、対処方法を決定します。それによって下記に設定された割り当て時間を検索します。

1. ユーザー
2. コンピュータまたはネットワーク クライアント

3. ユーザーが所属するグループ

   ユーザーが複数のグループのメンバーである場合、割り当て時間は、**[Settings] > [General] > [Filtering]** ページの **[Use more restrictive blocking（より厳密なブロック基準を使用する）]** の設定に従って割り当てられます（*フィルタリング設定値の設定、81 ページ*を参照）。

4. デフォルトの割り当て時間

Java または Flash アプレットなどのインターネット アプレットは、割り当て時間の制約どおりに反応しない場合があります。ブラウザ内で動作するアプレットが割り当て時間制約サイトからアクセスされたとしても、そのアプレットは設定した割り当てセッション時間を超えて継続することができます。

これは、そのようなアプレットはクライアント コンピュータに完全にダウンロードされ、発信もとのホスト サーバーへ応答することなくアプリケーションのように動作することが原因です。ただし、ユーザがブラウザの [Refresh（リフレッシュ）] ボタンをクリックすると、Filtering Service は通信を l 確認して、適用される割り当て制約に従ってその要求をブロックします。

検索フィルタリング

Web Security Help | Web Security ソリューション | バージョン 7.8.x

検索フィルタリングは、一部の検索エンジンによって提供される機能であり、この機能はユーザーに表示される不適切な検索結果の数を制限するのに役立ちます。

通常、インターネット検索エンジンの検索結果は 検索基準と一致したサイトと関連するサムネイル イメージを含む場合があります。それらのサムネールがブロックされたサイトに関連付けられている場合、Websense Web Security ソリューションはユーザーが完全なサイトにアクセスしないようにしますが、検索エンジンがイメージを表示するのは防止しません。

検索フィルタリングを有効化したとき、検索エンジン機能は、ブロックされているサイトに関連付けられているサムネイル イメージを検索結果の中に表示しないようにします。検索フィルタリングを有効化すると、ローカルとリモートの両方のフィルタリング クライアントに影響を与えます。

Websense, Inc. は、検索フィルタリングの機能を備えた検索エンジンのデータベースを保持しています。データベースから検索エンジンが追加または削除された場合、アラートを発生します（*警告、481 ページ*を参照）。

検索エンジンは、**[Settings] > [General] > [Filtering]** ページを通じてアクティブ化します。詳細は、*フィルタリング設定値の設定、81 ページ*を参照してください。

フィルタの使用

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリおよびプロトコルへのアクセスの管理、59 ページ*
- *インターネット アクセスのポリシー、111 ページ*
- *カテゴリ フィルタの作成、72 ページ*
- *プロトコル フィルタの作成、76 ページ*
- *制限付きアクセス フィルタの作成、316 ページ*

カテゴリ、プロトコル、制限付きアクセス フィルタを表示、作成、および変更するには **[Policy Management] > [Filters]** ページを使用します。

[Filters] ページは下記の主な 3 つのセクションに分割されています。

- **[Category Filters（カテゴリ フィルタ）]** は、ブロックおよび許可するカテゴリを決定します。
- **[Protocol Filters（プロトコル フィルタ）]** は、ブロックおよび許可する非 HTTP プロトコルを決定します。

  完全なプロトコルベースのポリシーの適用を有効化するために、Network Agent をインストールする必要があります。

  Websense Web Security Gateway の場合は、Network Agent を使用せずに HTTP ポートをトンネリングする非 HTTP プロトコルをフィルタリングできます。詳細は、*トンネリング プロトコルの検出、235 ページ*を参照してください。

  Websense Web Security Gateway Anywhere 環境の場合、ハイブリッド サービスは、プロトコルベースのポリシーの適用を提供しません。
- **[Limited Access Filters（制限付きアクセス フィルター）]** は、許可されたウェブサイトの限定リストを定義します（*ユーザーのアクセスを、指定した URL のリストに制限する、314 ページ*を参照）。

カテゴリ フィルタ、プロトコル フィルタ、および制限付きアクセス フィルタは**ポリシー**の構築ブロックを形成します。各ポリシーは少なくとも 1 つのカテゴリ フィルタまたは制限付きアクセス フィルタ、および 1 つのプロトコル フィルタで構成されており、特定のスケジュールで選択したクライアントに適用されます。

- 既存のカテゴリ フィルタ、プロトコル フィルタ、または制限付きアクセス フィルタを検討または編集するには、フィルタ名をクリックします。詳細については、下記の項目を参照してください：
  - *カテゴリ フィルタの編集、73 ページ*
  - *プロトコル フィルタの編集、77 ページ*
  - *制限付きアクセス フィルタの編集、317 ページ*

- 新しいカテゴリ フィルタ、プロトコル フィルタ、または制限付きアクセス フィルタを作成するには、**[Add（追加）]** をクリックします。詳細については、下記の項目を参照してください：
  - *カテゴリ フィルタの作成、72 ページ*
  - *プロトコル フィルタの作成、76 ページ*
  - *制限付きアクセス フィルタの作成、316 ページ*

既存のフィルタをコピーするには、フィルター名の隣のチェック ボックスをオンにして、**[Copy（コピー）]** をクリックします。コピーには、一意な数字が付いた元のフィルタの名前がつけられ、次にフィルタのリストに加えられます。他のフィルターの編集と同じようにコピーを編集します。

指定済み管理者ロール（*代理管理およびレポート作成、405 ページ*を参照）を作成した場合、優先管理者は、他のロールに対して作成したフィルタを指定済み管理者が使用できるようにコピーすることができます。

フィルタを他のロールにコピーするには、フィルタ名の横のチェックボックスをオンにし、**[Copy to Role（ロールにコピー）]** をクリックします。詳細は、*ロールへのフィルタおよびポリシーのコピー、319 ページ*を参照してください。

カテゴリ フィルタの作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *フィルタの使用、71 ページ*
- *カテゴリ フィルタの編集、73 ページ*
- *カテゴリまたはプロトコルがブロックされる場合、61 ページ*

新しいカテゴリ フィルタを作成するには、**[Policy Management（ポリシー管理）] > [Filters] > [Add Category Filter（カテゴリ フィルタを追加）]** ページを使用します。事前定義したテンプレートを使用するか、または既存のカテゴリ フィルターをコピーして、新しいフィルタのベースとして使用できます。

1. 一意な**フィルタ名**を入力します。名前は 1 ～ 50 文字でなければならず、また下記の文字を含むことはできません。

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   フィルタ名にはスペース、ダッシュ、アポストロフィーを含めることができます。
2. フィルタの短い**説明**を入力します。この説明は、[Filters]ページの [Category Filters（カテゴリ フィルタ）] セクションのフィルタ名の隣に表示されます。またこの説明にはフィルターの目的を示す必要があます。

フィルタ名に適用される使用文字の制限は、説明にも適用されますが、2つの例外があります。説明にはピリオド（.）およびカンマ（,）を使用できます。

3. テンプレートを使用するか、既存のフィルタをコピーするかを決めるためドロップダウン リストからにエントリを選択します。テンプレートの詳細については、*カテゴリ フィルタおよびプロトコル フィルタのテンプレート、80 ページ*を参照してください。
4. 新しいフィルタを確認および編集するには、**[OK]** をクリックします。フィルターは、[Filters] ページの **[Category Filters]** リストに追加されます。

フィルタをカスタマイズするには、フィルタ名をクリックし、次に*カテゴリ フィルタの編集*に進みます。

カテゴリ フィルタの編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリおよびプロトコルへのアクセスの管理、59 ページ*
- *処置、68 ページ*
- *割り当て時間を使ってインターネット アクセスを制限する、69 ページ*
- *フィルタの使用、71 ページ*
- *カテゴリの使用、322 ページ*

既存のカテゴリ フィルタの変更を行うには、**[Policy Management] > [Filters] > [Edit Category Filter（カテゴリ フィルタを編集）]** ページを使用します。

重要

カテゴリ フィルタを編集したとき、変更はそのフィルタを適用する各ポリシーに反映されます。

別の指定済み管理ロールで同じ名前をもつカテゴリ フィルタを適用するポリシーには反映されません。

フィルタ名および説明は、ページの上部に表示されます。

- フィルタ名を変更するには、**[Rename（名前の変更）]** をクリックします。
- フィルタの説明を変更するには、**[Description]** フィールドに入力します。

[Policies using this filter（このフィルタを使用しているポリシー）] の隣の数値は、選択したフィルターを現在使用しているポリシーの数を表します。カテゴリ フィルタがアクティブな場合、フィルタを適用するポリシーのリストを参照するには、**[View Policies（ポリシーを表示）]** をクリックします。

このページの下部にカテゴリのリストと現在各カテゴリに適用されいる処置が表示されます。

1. カテゴリ情報を表示するか、または選択したカテゴリに関連する処置を変更するには、**[Categories（カテゴリ）]** リストからエントリを選択します。
2. カテゴリに適用される処置の変更を行う前に、詳細情報セクション（[Categories] の右側）を使用して、そのカテゴリに関連する特別な属性を確認します。
   - カテゴリに割り当てられた再分類された URL（もしあれば）のリストを表示するには、**[See custom URLs in this category（このカテゴリのカスタム URL を参照）]** をクリックします。*特定の URL の再分類、330 ページ*を参照してください。
   - カテゴリに割り当てられたキーワードのリストを表示するには、**[See keywords in this category（このカテゴリのキーワードを参照）]** をクリックします。*キーワードベースのポリシーの実施、327 ページ*を参照してください。
   - カテゴリのカスタム URL またはキーワードを定義するために使用する正規表現のリストを表示するには、**[See regular expressions in this category（このカテゴリの正規表現を参照）]** をクリックします。
3. 選択したカテゴリに適用される処置を変更するには、カテゴリ リストの右のボタンを使用します。利用可能な処置の詳細については、*処置、68 ページ*を参照してください。

   指定済み管理者は、優先管理者によってロックされているカテゴリに割り当てられた処置を変更できません。
4. 選択したカテゴリに高度な処置を適用するには、[Categories] リストの右側のチェック ボックスを使用します。
   - キーワードが選択したカテゴリへの要求の割り当てに使用される方法を変更するには、**[Block keywords（キーワードをブロック）]** をオンまたはオフにします。*キーワードベースのポリシーの実施、327 ページ*
   - 選択したカテゴリのサイトからユーザーが特定のタイプのファイルにアクセスできるかどうかを決定するには、**[Block file types（ファイル タイプをブロック）]** をオンまたはオフにします。*ファイル タイプに基づくトラフィックの管理、345 ページ*を参照してください。

ファイル タイプをブロックすることを選択した場合は、ブロックする 1 つ以上のファイル タイプを選択します。

選択した ファイル タイプの設定をフィルタに含まれているすべての許可したカテゴリに適用するには、**[Apply to All Categories（すべてのカテゴリに適用）]** をクリックします。

警告

Websense Web Security Gateway および Gateway Anywhere の場合、ファイル タイプのブロックをすべてのカテゴリに適用すると、パフォーマンスに重大な影響を及ぼすことがあります。

ブロックされたタイプに一致しない拡張子をもつすべてのファイルは、HTML ファイルや CSS ファイルなどテキスト ファイルを含む真のファイル タイプを見つけるためにスキャンされます。

- カテゴリのサイトへのアクセスを特定の帯域幅しきい値を基準に制限するかどうかを指定するには、**[Block with Bandwidth Optimizer（Bandwidth Optimizer でブロック）]** をオンまたはオフにします。*Bandwidth Optimizer による帯域幅の管理*、342 ページを参照してください。

  帯域幅を基準にブロックすることを選択した場合、使用するしきい値制限を指定します。

  選択した帯域幅の設定をフィルタに含まれているすべての許可したカテゴリに適用するには、**[Apply to All Categories]** をクリックします。

5. 他のカテゴリに適用した処置を変更するには、ステップ 1 ～ 3 を繰り返します。
6. フィルタを編集した後、**[OK]** をクリックして変更をキャッシュし、[Filters] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

新しいカテゴリ フィルタをアクティブ化するには、それをポリシーに追加し、そのポリシーをクライアントに割り当てます。*インターネット アクセスのポリシー*、111 ページを参照してください。

プロトコル フィルタの作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリおよびプロトコルへのアクセスの管理、59 ページ*
- *処置、68 ページ*
- *プロトコル フィルタの編集、77 ページ*
- *プロトコルの使用、335 ページ*
- *カテゴリまたはプロトコルがブロックされる場合、61 ページ*

新しいプロトコル フィルタを定義するには、**[Policy Management] > [Filters] > [Add Protocol Filter（プロトコル フィルタを追加）]** ページを使用します。新しいフィルタの基準として、事前定義したテンプレートを使用するか、または既存のプロトコル フィルタをコピーして使用します。

1. 一意な**フィルタ名**を入力します。名前は 1 ～ 50 文字でなければならず、また下記の文字を含むことはできません。

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   フィルタ名にはスペース、ダッシュ、アポストロフィーを含めることができます。
2. フィルタの短い**説明**を入力します。この説明は、[Filters] ページの [Protocol Filters（プロトコル フィルタ）] セクションのフィルタ名の隣に表示されます。またこの説明にはフィルターの目的を示す必要があります。

   フィルタ名に適用される使用文字の制限は、説明にも適用されますが、2 つの例外があります。説明では、ピリオド（.）とカンマ（,）が使用できます。
3. 新しいフィルターの基準として、テンプレートを使用する（*カテゴリ フィルタおよびプロトコル フィルタのテンプレート、80 ページ*を参照）か、既存のフィルタをコピーするかを決めるためにドロップダウン リストからエントリを選択します。
4. 新しいフィルタを確認および編集するには、**[OK]** をクリックします。フィルターは、[Filters] ページの **[Protocol Filters（プロトコル フィルタ）]** リストに追加されます。

新しいフィルタのカスタマイズを完了するために、*プロトコル フィルタの編集*に進みます。

プロトコル フィルタの編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリおよびプロトコルへのアクセスの管理、59 ページ*
- *プロトコル フィルタの作成、76 ページ*
- *処置、68 ページ*
- *プロトコルの使用、335 ページ*
- *Bandwidth Optimizer による帯域幅の管理、342 ページ*

既存のプロトコル フィルタの変更を行うには、**[Policy Management] > [Filters] > [Edit Protocol Filter（プロトコル フィルタを変更）]** ページを使用します。

重要

ここでの変更内容は、このフィルタが適用されるすべてのポリシーに反映されます。

別の指定済み管理ロールで同じ名前をもつプロトコル フィルタを適用するポリシーには反映されません。

フィルタ名および説明は、ページの上部に表示されます。

- フィルタ名を変更するには、**[Rename]** をクリックします。
- フィルタの説明を変更するには、**[Description]** フィールドに入力します。

[Policies using this filter（このフィルタを使用しているポリシー）] の隣の数値は、選択したフィルターを現在使用しているポリシーの数を表します。プロトコル フィルタがアクティブな場合、フィルタを適用するポリシーのリストを参照するには、**[View Policies]** をクリックします。

このページの下部にプロトコルのリストと現在各カテゴリに適用されいる処置が表示されます。

プロトコルがフィルタされログ記録される方法を変更するには、下記の手順を実行します。

1. **[Protocols（プロトコル）]** リストからプロトコルを選択します。選択したプロトコルの高度な処置がリストに右側に表示されます。
2. 選択したプロトコルに適用される処置を変更するには、[Protocols] リストの下部の **[Permit]** ボタンと **[Block]** ボタンを使用します。

注意

Websense ソフトウェアは、TCP ベースのプロトコル要求をブロックできますが、UDP ベースのプロトコル要求をブロックできません。

一部のアプリケーションは、TCP ベースと UDP ベースの両方のメッセージを使用します。アプリケーションの元のネットワーク要求が TCP を経由して行われ、後のデータが UDP 経由で送信された場合、Websense ソフトウェアは最初の TCP 要求をブロックし、それによってその後の UDP トラフィックをブロックします。

UDP 要求は許可されている場合でも、[ブロックされた] とログ記録される場合があります。

同じ処置を選択したプロトコル グループの他のプロトコルに適用するには、**[Apply to Group（グループに提供）]** をクリックします。

3. アラートおよびレポーティングに使用できる選択したプロトコルの使用に関する情報がいる場合は、**[Log protocol data（ロトコル データをログに記録）]** をオンにします。
4. これらのプロトコルの使用に帯域幅を制限するには、**[Block with Bandwidth Optimizer]** をクリックし、使用する帯域幅しきい値を指定します。詳細は、*Bandwidth Optimizer による帯域幅の管理*、342 ページを参照してください。
5. フィルタを編集した後、**[OK]** をクリックして変更をキャッシュし、[Filters] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

新しいプロトコル フィルタをアクティブ化するには、それをポリシーに追加し、そのポリシーをクライアントに割り当てます（*インターネット アクセスのポリシー*、111 ページを参照）。

注意

特定の時刻にプロトコル フィルタの適用を開始するポリシーを作成できます。ユーザーがそのフィルターが有効になる前に、プロトコル セッションを開始した場合、フィルタがそのプロトコルをブロックしていてもそのセッションが続く限り、ユーザーはそのプロトコルに引き続きアクセスできます。ユーザーがそのセッションを終了したあと、そのプロトコルの追加の要求がブロックされます。

Websense 定義のカテゴリ フィルタとプロトコル フィルタ

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Web Security ソリューションは、複数のサンプルのカテゴリ フィルタとプロトコル フィルタを含んでいます。これらのフィルタをそのまま使用するか、変更することができます。事前定義のフィルターが必要でない場合は、それらのフィルタを多数削除できます、

下記の事前定義のカテゴリ フィルタがあります。

- Basic（基本）
- Basic Security（基本セキュリティ）
- Block All（すべてブロック）
- Default（デフォルト）
- Monitor Only（モニタのみ）
- Permit All（すべて許可）
- Strict Security（厳格なセキュリティ）

[Block All] および [Permit All] カテゴリ フィルタは、[Filters] ページにはリストされませんが、それらをポリシーに追加できます。これらのフィルターは他のフィルターとは異なって処理され、削除または編集することができません。Filtering Service がインターネット要求を受け取ったとき、Filtering Service は、その他のチェックを行う前に、最初に [Block All] または [Permit All] フィルタが適用するかどうか確認するためにチェックします（*URL 要求への応答*、122 ページを参照）。

下記の事前定義のプロトコル フィルタがあります。

- Basic Security（基本セキュリティ）
- Default（デフォルト）
- Monitor Only（モニタのみ）
- Permit All（すべて許可）

[Permit All] プロトコル フィルタは、カテゴリ フィルターと同様に、[フィルタ ページ] に示されず、編集も削除もできません。またこのプロトコル フィルタは、ポリシー適用プロセス中に優先順位が付けられます。

[Default] カテゴリおよびプロトコル フィルタは、編集できますが、削除できません。アップグレード環境でデフォルト ポリシーにギャップがある場合は、他に適用するフィルタがないとき、期間中 [Default] フィルタを使って要求をフィルタリングします。

カテゴリ フィルタおよびプロトコル フィルタのテンプレート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

新しいカテゴリまたはプロトコル フィルタを作成するとき、[Filters] ページで既存のフィルターのコピーを作成するか、[Add Filter（フィルタを追加）] ページでもでるとして既存のフィルターとして既存のフィルタを選択するか、フィルタの**テンプレート**を使用できます。

Websense Web Security ソリューションは、下記の 5 つのカテゴリ フィルタのテンプレートを含んでいます。

- **[Monitor Only（モニタのみ）]** および **[Permit All（すべて許可）]** は、すべてのカテゴリを許可します。
- **[Block All（すべてブロック）]** は、すべてカテゴリをブロックします。
- **[Basic（基本）]** は最も頻繁にブロックされるカテゴリをブロックし、残りのカテゴリを許可します。
- **[Default（デフォルト）]** は、Block（ブロック）、Permit（許可）、Continue（続行）、および Quota（割り当て）処理をカテゴリに適用します。
- **[Strict Security（厳格なセキュリティ]**）は、2 つのその他のセキュリティ カテゴリをブロックし、実行可能ファイルのタイプファイルタイプ ブロックを 3 番目のカテゴリに追加することによって [Default] テンプレートを拡張します。
- **[Basic Security（基本セキュリティ）]**は、[セキュリティ リスク]クラス内のデフォルト カテゴリだけをブロックします（*リスク クラス、64 ページ*を参照）。

Websense Web Security ソリューションは、下記の 3 つのプロトコル フィルタのテンプレートを含んでいます。

- **[Monitor Only]** および **[Permit All]** は、すべてのプロトコルを許可します。
- **[Basic Security]** は、P2P ファイル共有プロトコル、プロキシ回避プロトコル、インスタント メッセージング ファイル アタッチメント（取得している場合）、および不正なトラフィック（Websense Web Security）をブロックします。
- **[Default]** は、インスタント メッセージング / チャット プロトコル、P2P ファイル共有、プロキシ回避プロトコル、インスタント メッセージング ファイル アタッチメント（取得している場合）、および不正なトラフィック（Websense Web Security）をブロックします。

Websense 定義のほとんどのカテゴリおよびプロトコル フィルタを変更または削除できますが、テンプレートの編集や削除はできません。同様に、必要に応じて多くの数のカスタム ファイルを作成できますが、新しいテンプレートは作成できません。

テンプレートは変更できませんから、いつでもテンプレートに戻ることによって、Websense 定義のフィルタによって適用された元の処置を参照することができます。たとえば、[Default] カテゴリおよびプロトコル フィルタ テンプレートは、元の [Default] カテゴリおよびプロトコル フィルタと同じ処置を適用します。つまり、テンプレートのデフォルトを使用するフィルタを作成することによって常に元の Websense ポリシー設定を復元できます。

たとえば、テンプレートを使用して新しいフィルターを作成するには、*カテゴリ フィルタの作成、72 ページ*または*プロトコル フィルタの作成、76 ページ*を参照してください。

フィルタリング設定値の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリおよびプロトコルへのアクセスの管理、59 ページ*
- *ブロック ページ、143 ページ*
- *パスワード無効化、105 ページ*
- *アカウントの無効化、106 ページ*
- *Bandwidth Optimizer による帯域幅の管理、342 ページ*
- *キーワードベースのポリシーの実施、327 ページ*

インターネット要求が処理される方法の基本設定を行うには、**[Settings] > [General] > [Filtering]** ページを使用します。

複数のグループ ポリシーが適用するときポリシーがユーザーに適用される方法を決定するには、**[General Filtering（一般的なフィルタリング）]** を使用し、キーワード検索オプションを指定し、次にパスワード無効化、アカウント無効化、継続、および割り当てセッションの動作を設定します。

1. 複数のグループ ポリシーが適用するときユーザーの要求が処理される方法を決定ために、**[Use most restrictive group policy（最も厳しいグループ ポリシーを使用）]** をオンまたはオフにします（*適用順序、119 ページ*を参照）。
   - オプションを選択 j したとき、最も厳しい設定に適用するポリシーが使用されます。つまり、ある適用可能なグループ ポリシーがカテゴリへのアクセスをブロックし、他の適用可能なグループ ポリシーがそのカテゴリへのアクセスを許可した場合、そのカテゴリに含まれているサイトへのユーザーの要求はブロックされます。
   - このオプションが選択されていない場合、最も寛大な設定が使用されます。

2. 下記の**キーワード検索オプション**からいずれかを選択します（*キーワードベースのポリシーの実施、327 ページ*を参照）。

CGI のみ	CGI クエリ文字列（Web アドレスの [?] の後）にキーワードがある場合、サイトをブロックします。 例：**search.yahoo.com/search?p=test** このオプションが選択されている場合、Filtering Service は、[?] の前のキーワードは検索しません。
URL のみ	キーワードが URL に示されている場合、サイトをブロックします。要求されたアドレスが CGI クエリ文字列を含んでいる場合、Filtering Service は [?] までのキーワードを検索します。
URL および CGI	アドレスのどこでもキーワードが示されている場合、サイトをブロックします。CGI クエリ文字列が存在する場合、Filtering Service は [?] の前後のキーワードを検索します。
キーワード ブロックの無効化	注意して使用してください。**[キーワード ブロックの無効化]** を選択すると、カテゴリ フィルタで **[キーワードをブロック]** が選択されている場合でも、すべてのキーワード ブロックがオフになります。

3. **[Password override timeout（パスワード無効化タイムアウト）]** フィールドに、パスワードの無効化を選択した後、ユーザーがすべてのカテゴリに含まれているサイトにアクセスできる最大時間（秒）（最大 3600、デフォルト 60）を入力します（*パスワード無効化、105 ページ*を参照）。
4. **[Continue timeout（継続のタイムアウト）]** フィールドに [Continue（継続）] をクリックしたユーザーが [Comfirm（確認）] 処置によって管理されるカテゴリに含まれているサイトにアクセスできる最大時間（秒）（最大 3600、デフォルト 60）を入力します（*処置、68 ページ*を参照）。
5. **[Account override timeout（アカウント無効タイムアウト）]** フィールドに、ユーザーが無効アカウントに割り当てられているポリシーによってフィルタリングされる最大時間（分（最大 3600、デフォルト 5）を入力します（*アカウントの無効化、106 ページ*を参照）。
6. **[Quota session length（割り当てセッション時間）** フィールドにユーザーが割り当て制限付きカテゴリに含まれているサイトを閲覧できる時間を入力します（最大 60 分、デフォルト 10 分）（*割り当て時間を使ってインターネット アクセスを制限する、69 ページ*を参照）。

   ユーザーが [Use Quota Time（割り当て時間の使用）] ボタンをクリックした後、セッションが開始します。

7. すべてのユーザーに対して **[Default quota time per day（1 日当たりのデフォルトの割り当て時間）]**（最大 240 秒、デフォルト 60 秒）を入力します。

   個々のユーザーの割り当て時間を変更するには、**[Policies（ポリシー）] > [Clients（クライアント）]** ページに移動します。

   割り当てセッション時間および 1 日当たりのデフォルトの割り当て時間への変更を行った後、**[Default quota sessions per day]** が計算され、表示されます。

[State Server（ステート サーバー）] で、下記の場合に **[IPv4 address or hostname（IPv4 アドレスまたはホスト名）]** および **[Port（ポート）]** の情報を提供します。

- 環境に、複数の Websense Filtering Service インスタンスがふくまれており、また
- [Quota] 処置、[Confirm] 処置、パスワード無効化、またはアカウント無効化を使用する場合。

State Server は、クライアントの割り当て、確認、パスワード無効化、およびアカウント無効化のセッションを追跡して、セッション時間が複数の Filtering Service インスタンスに正しく割り当てられていることを確認します（*Policy Server、Filtering Service、および State Server、469 ページ*を参照）。

State Server 接続の詳細情報を入力した後、**[Check Status（ステータスを確認）]** をクリックして接続を確認します。環境にある各 Policy Server インスタンスについて State Server 接続情報を設定します。

[Bandwidth Optimizer] で、利用可能な帯域幅に基づくインターネット使用状況をフィルタリングするために必要な情報を入力します。帯域幅ベースのインターネット アクセスの適用の詳細については、*Bandwidth Optimizer による帯域幅の管理、342 ページ*を参照してください。

注意

Websense Web Security Gateway Anywhere 環境では、どの帯域幅ベースの制限もハイブリッド サービスを通過する要求には適用されません。

1. **[Internet connection speed インターネット接続速度]** を指定するために、下記のどちらかの手順を実行します。
   - ドロップダウン リストから標準速度を選択する。
   - テキスト フィールドに秒あたりのネットワーク速度（単位キロビット）を入力する。
2. 帯域幅ベースの処置が適用されたときに使用するデフォルトのしきい値を入力します。しきい値を設定したが、カテゴリまたはプロトコル フィルタが帯域幅ベースの処置を含まない場合、帯域幅の使用量の制限は行われません。
   - **ネットワーク**：合計のネットワーク トラフィックが合計の利用可能な帯域幅のこの割合（%）に到達したとき、アクティブな フィルタで設定されたように、帯域幅ベースのアクセスの制限を開始します。
   - **プロトコル**：特定のプロトコル（HTTP、MSN Messenger nado）のトラフィックが合計の利用可能な帯域幅のこの割合（%）に到達したとき、アクティブな フィルタで設定されたように、そのプロトコルへのアクセスの制限を開始します。
3. （*Websense Web Security Gateway*）Content Gateway は、レポーティングで使用するために、HTTP トラフィックおよび HTTP をトネリングするプロトコルによって使用された帯域幅に関する情報を収集できます。このオプションを有効化するには、**[Include bandwidth data collected by Websense Content Gateway（Websense Content Gateway によって収集された帯域幅データを含む）]** をオンにします。

[Block Messages（ブロック メッセージ）] セクションを使用して、URL またはブラウザベースのブロック メッセージの上部フレームで作成した代替の HTML ブロックページへのパス を入力する（*代替ブロック メッセージの作成*、154 ページを参照）か、またはブロック ページに ACEInsight へのリンクを含めるように Websense Web Security Gateway Anywhere を設定します。

- 下記のような異なるプロトコルに別個のページを使用できます。**FTP**、**HTTP**（**HTTPS** を含む）、および **Gopher**。

  デフォルトのブロック メッセージを使用するには、これらのフィールドを空白のままにしておきます。

  カスタム ブロック ページを作成した後、これらのブロック ページをすべてのプロトコルに対して使用する場合、このセクションのフィールドを空白にしておくこともできます（*ブロック メッセージのカスタマイズ*、149 ページを参照）。

- Websense Web Security Gateway Anywhere 環境の場合
  - 上記のフィールドで指定されたカスタム ブロック メッセージは、ハイブリッド サービスによって処理された要求には適用されません。

    代わりに、[Settings] > [Hybrid Configuration（ハイブリッド設定）] > [User Access（ユーザー アクセス）] ページを使用してハイブリッド ブロック ページをカスタマイズします（*ハイブリッド ブロック ページのカスタマイズ、276 ページ*を参照）。
  - ユーザーが [ACEInsight] リンクをクリックしたとき、ユーザーがアクセスを試みた URL は、ACEInsight に送信され、ACEInsight の分析を示すウェブ ページが表示されます。

    ACEInsight に送信された URL は切り捨てられ、CGI 文字列（ユーザー名またはパスワードを含む場合があります）が省略されます。そのため、ACEInsight はパスワード保護されたコンテンツを分析せず、Content Gateway 以外の別の結果を返すことがあります。

    ハイブリッド ブロック ページには、[ACEInsight] リンクは表示されません。

特定の検索エンジンに組み込まれている設定を有効化させることによって、ブロックされているサイトに関連するサムネール イメージおよび他の明示的コンテンツが検索結果に表示されないようにするには、**[Search Filtering（検索フィルタリング）]** から、**[Enable search filtering（検索フィルタリングを有効にする）]** を選択します（*検索フィルタリング、70 ページ*を参照）。

この機能がサポートされている検索エンジンは、チェック ボックスの下に表示されます。

このページの設定値の設定を完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy（保存と配備）]** をクリックするまで変更は適用されません。

4 クライアント

Web Security Help | Web Security ソリューション | バージョン 7.8.x

特定のユーザーまたはコンピュータを Web Security manager の**クライアント**として追加することによって、Websense Web Security ソリューションがそれらのユーザーまたはコンピュータからの要求をフィルタする方法をカスタマイズできます。クライアントとは、以下のようなものです：

- **コンピュータ**：IP アドレスで定義された、ネットワーク上の個々のコンピュータ
- **ネットワーク**：IP アドレスの範囲で集合的に定義された、コンピュータのグループ
- **ディレクトリ**クライアント：サポートされているディレクトリ サービスに含まれるユーザー、グループ、またはドメイン（OU）アカウント

> **注意**
>
> Websense Web Security Gateway Anywhere 環境では、ハイブリッド サービスは、ポリシーをユーザーまたグループ、またはフィルタリングされている場所に適用できます。ただし、個々のクライアントまたはネットワークには適用できません。*ハイブリッド サービス クライアントの処理*、109 ページを参照してください。

最初に、すべてのクライアント要求は、**デフォルト** ポリシーによって管理されます（*Default ポリシー*、112 ページを参照）。Web Security manager の [Clients] ページにクライアントを追加した後、そのクライアントに特定のポリシーを割り当てることができます。

複数のポリシーが適用可能である場合、たとえば、1 つのポリシーがユーザーに割り当てられ、別のポリシーがコンピュータに割り当てられている場合、デフォルトでは、Websense Filtering Service はポリシーを下記の優先順で適用します。

1. 要求を発行した**ユーザー**に割り当てられているポリシーを適用します。そのポリシーに要求時にスケジュールされているフィルタがない場合、適用できる次のポリシーを使用します。
2. ユーザー固有のポリシーがない場合、またはポリシーに要求時にアクティブなフィルタがない場合、要求を作成した**コンピュータ**（最初）または**ネットワーク**（2 番目）に割り当てられているポリシーを探します。
3. コンピュータまたはネットワークに固有のポリシーがない場合、またはポリシーに要求時にアクティブなフィルタがない場合、ユーザーが所属する**グループ**に割り当てられているポリシーを探します。ユーザーが複数のグループに属する場合、Websense Filtering Service はすべての適用されるすべてのグループ ポリシーを検討します（*適用順序、119 ページ*を参照）。
4. グループ ポリシーがない場合は、ユーザーの**ドメイン**（OU）に割り当てられているポリシーを探します。
5. 適用されるポリシーが見つからなかった場合、または要求時にポリシーがカテゴリ フィルタを適用しなかった場合、そのクライアントが割り当てられているロールに **[デフォルト]** ポリシーを適用します。

Filtering Service が要求を処理する方法の詳細については、*URL 要求への応答、122 ページ*を参照してください。

Filtering Service がグループまたはドメイン ベースを IP アドレス ベース（コンピュータおよびネットワーク）のポリシーよりも優先させるように設定する方法については、*グループおよびドメイン ポリシーの優先度設定、121 ページ*を参照してください。

ハイブリッド サービスがポリシーをクライアントに適用する方法については、*適用順序、119 ページ*を参照してください。

クライアントの処理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *クライアント、87 ページ*
- *コンピュータとネットワークの処理、91 ページ*
- *ユーザーおよびグループの処理、92 ページ*
- *クライアントの追加、102 ページ*
- *クライアントの設定の変更、104 ページ*

[Policy Management（ポリシー管理）] > [Clients（クライアント）] ページは、既存のクライアントに関する情報を表示したり、指定済み管理ロールのクライアントを追加、編集、または削除するために使用します。

指定済み管理者である場合、管理対象のクライアントのリストから [Clients] ページにクライアントを追加します。それによってポリシーをそれらのクライアントに適用できます。手順については、*クライアントの追加、102 ページ*を参照してください。

くらい後は、以下の 3 つのグループに分けられています。

- **ディレクトリ**、ディレクトリ サービスからのユーザー、グループ、およびドメイン（OU）を含みす（*ユーザーおよびグループの処理、92 ページ*を参照）。
- **ネットワーク**、単一のポリシーによって管理できるフィルタ対象のネットワーク内の IPv4 または IPv6 アドレス範囲（*コンピュータとネットワークの処理、91 ページ*を参照）。
- **コンピュータ**、フィルタ対象のネットワーク内の、IPv4 または IPv6 アドレスによって識別される個々のコンピュータ（*コンピュータとネットワークの処理、91 ページ*を参照）。

選択したタイプの既存のクライアントのリストを表示するうには、そのクライアント タイプの隣のプラス記号（+）をクリックします。各クライアント リストには下記の情報が含まれます。

- クライアント名、IP アドレス、または IP アドレス範囲。
- 現在クライアントに割り当てられている**ポリシー**。他のクライアントを割り当てるまで、**[デフォルト]** ポリシーが使用されます（*インターネット アクセスのポリシー、111 ページ*を参照）。
- クライアントが、ブロックされたサイトを表示またはその表示を試みるために**パスワード無効化**（*パスワード無効化、105 ページ*を参照）オプション、または**アカウント無効化**（*アカウントの無効化、106 ページ*を参照）オプションを使用できるかどうか。
- クライアントにカスタムの**割り当て時間**が割り当てられているかどうか（*割り当て時間を使ってインターネット アクセスを制限する、69 ページ*を参照）。

特定のクライアントを見つけるには、ツリー内の適切なノードを参照します。

クライアント ポリシー、パスワード無効化、割り当て時間、および認証の設定を変更するには、リストから 1 つ以上のクライアントを選択し、**[Edit（編集）]** をクリックします。詳細は、*クライアントの設定の変更、104 ページ*を参照してください。

クライアントを追加するか、または現在 [Clients] ページに表示されていない管理対象のクライアントにポリシーを適用するには、**[Add（追加）]** をクリックします。詳細については、*クライアントの追加、102 ページ*を参照してください。

指定済み管理ロールを作成している場合（*代理管理およびレポート作成、405 ページ*を参照）、優先管理者は、それらのクライアントを他のロールに移動できます。最初にクライアント エントリの隣のチェック ボックスをオンにし、次に **[Move to Role（ロールに移動）]** をクリックします。クライアントが指定済み管理ロールへ移動したとき、クライアントに適用されたポリシーおよびフィルタはそのロールにコピーされます。詳細は、*クライアントをロールに移動、108 ページ*を参照してください。

Websense User Service を LDAP ベースのディレクトリ サービスと通信するように設定している場合、このページの上部のツールバーに **[Manage Custom LDAP Groups（カスタム LDAP グループを管理）]** ボタンが表示されます。LDAP 属性に基づくグループを追加または編集するには、このボタンをクリックします（*カスタム LDAP グループの処理、100 ページ*を参照）。

[Clients] ページからクライアントを削除するには、削除対象のクライアントを選択し、**[Delete（削除）]** をクリックします。

コンピュータとネットワークの処理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *クライアントの処理*、89 ページ
- *ユーザーおよびグループの処理*、92 ページ
- *クライアントの追加*、102 ページ
- *1 つのポリシーを複数のクライアントに割り当てる*、119 ページ

Web Security manager では、**コンピュータ**は、フィルタリング対象のコンピュータに関連する IP アドレス（例、10.201.3.1、fd3a:918a:71a1:bcaa::0011）です。**ネットワーク**は、フィルタリング対象のコンピュータのグループに対応する IP アドレス範囲（例、10.201.3.2 ～ 10.201.3.44、fd3a:918a:71a1:bcaa::1111 ～ fd3a:918a:71a1:bcaa::1211）です。

- Websense Web Security Gateway Anywhere 環境では、ハイブリット サービスは、ポリシーを個別のコンピュータおよびネットワーク クライアントに適用しません。フィルタ対象の場所へのポリシーの適用の詳細については、*ハイブリッド サービス クライアントの処理*、109 ページを参照してください。
- ポリシーを IPv6 コンピュータおよびネットワーク クライアントに適用する前に、影響を受けるコンピュータ上の一時的な IP v 6 アドレスを無効化します。詳細については、support.websense.com を参照してください。

ポリシーをユーザー、グループ、またはドメイン、クライアントに割り当てるのと同じようにコンピュータおよびネットワークに割り当てることができます。

- たとえば、ユーザーがログオンする必要がない、またはゲスト アカウントをもつユーザーがアクセスできるというポリシーを**コンピュータ**に割り当てます。
- 一度複数のコンピュータに同じポリシーを適用するために、ポリシーを**ネットワーク**に割り当てます。

ポリシーをコンピュータまたはネットワークに割り当てた場合、フィルタ対象のコンピュータに誰がログオンしているかに関係なく、ポリシーをログオンしているユーザーに割り当てていない**限り**、そのポリシーが適用されます。オンプレマイズ Web Security コンポーネントを使用している場合、コンピュータまたはネットワーク ポリシーがユーザーに適用されるグループ ポリシーよりも優先されます（Websense Web Security Gateway Anywhere 環境では、コンピュータまたはネットワーク ポリシーの適用の前にハイブリッド サービスによってグループ ポリシーが適用されます*ハイブリッド サービス クライアントの処理*、109 ページを参照してください。）

ユーザーおよびグループの処理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *クライアントの処理*、89 ページ
- *ディレクトリ サービス*、93 ページ
- *カスタム LDAP グループの処理*、100 ページ
- *コンピュータとネットワークの処理*、91 ページ
- *クライアントの追加*、102 ページ
- *1 つのポリシーを複数のクライアントに割り当てる*、119 ページ

ネットワーク内の個々のユーザーおよびグループにポリシーを適用するために、Websense User Service がディレクトリ サービスにアクセスして、ディレクトリ オブジェクト（ユーザー、グループおよびドメイン [OU]）情報を取得するように設定します。

User Service は、混合モードまたはネイティブ モードで Windows Active Directory と通信でき、また Lightweight Directory Access Protocol（LDAP）経由でアクセスした Novell eDirectory、または Oracle（旧 Sun Java）Directory Server Enterprise Edition と通信できます。

- LDAP ベースのディレクトリ サービスを使用するとき、重複するユーザー名はサポートされません。同一のユーザー名が複数のドメインで使用されないようにしてください。
- Active Directory または Oracle Directory Service を使用する場合、パスワードが空白のユーザー名はサポートされません。パスワードをすべてのユーザーに割り当てます。

User Service は、ポリシーの適用に使用するために情報をディレクトリ サービスから Filtering Service に伝達します。最良の方法として、User Service を Windows コンピュータにインストールすることを推奨します（Linux コンピュータにインストールすることもできます）。

ディレクトリ サービス通信を設定するには、*ディレクトリ サービス*を参照してください。

ディレクトリ サービス

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ディレクトリ サービスは、ネットワークのユーザーとリソースに関する情報を格納するツールです。Web Security manager でユーザーのクライアント（ユーザー、グループ、ドメイン、または組織単位）を追加する前に、Websense User Service がディレクトリ サービスから情報を取得するように設定する必要があります。

ネットワークで使用しているディレクトリ サービスを特定するには、**[Settings（設定）] > [General（一般）] > [Directory Services（ディレクトリ サービス）]** ページを使用します。1 つの Policy Server につき 1 つのタイプのディレクトリ サービスの設定だけを指定できます。

注意

Websense Web Security Gateway Anywhere 環境では、[Directory Services（ディレクトリ サービス）] ページからの情報は、[Hybrid Configuration（ハイブリッド設定）] > [Shared User Data（共有ユーザー データ）] ページに供給ためにも使用されます。この情報によって、ハイブリッド サービスがユーザーベースおよびグループベースのポリシーを適用できます。*ユーザーおよびグループ データをハイブリッド サービスに送信、280 ページ*を参照してください。

最初に [Directories（ディレクトリ）] リストからディレクトリ サービスを選択します。ここでの選択内容が、ページにどの設定を表示するかを決定します。

設定の手順については下記の該当するセクションを参照してください。

- *Windows Active Directory（混在モード）、94 ページ*
- *Windows Active Directory（ネイティブ モード）、95 ページ*
- *Novell eDirectory および Oracle（Sun Java）Directory Server、97 ページ*

警告

Websense Web Security Gateway Anywhere 環境では、ハイブリッド サービスは、Windows Active Directory（ネイティブ モード）、Oracle Directory Server、および Novell eDirectory をサポートします。

設定が完了した後、User Service はディレクトリ サービスと通信して、ユーザーおよびグループ ベースのポリシーの適用を有効化します。User Service は、収集したユーザーおよびグループ情報を最大 3 時間キャッシュします。ディレクトリ サービス内のユーザー、グループ、または OU エントリに変更を行っている場合、User Service がそのユーザーおよびグループのマッピングを即座に更新するように強制するには、**[User Service Cache（ユーザー サービス キャッシュ）]** の下の [Clear Cache（キャッシュをクリア）] ボタンを使用します。ユーザー ベースのポリシーの適用は、キャッシュが再作成される間短期間速度を低下させることがあります。

管理者がそれらのネットワーク アカウントを使用して TRITON コンソールにログオンできるようにする場合は、[TRITON Settings（TRITON の設定）] > [User Directory（ユーザー ディレクトリ）] ページでディレクトリ サービス通信を設定する必要もあります。すべての管理ユーザーの認証に同じディレクトリを使用しなければなりません。詳細については、TRITON Settings Help を参照してください。

Windows Active Directory（混在モード）

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ディレクトリ サービスが混在モードの Active Directory である場合、一般的にはこれ以上の設定は必要ありません。

Websense User Service が Linux サーバーの Websense アプライアンス上に配備されており、下記のいずれかの条件が満たされている場合は、この画面で追加の情報を提供してください。

- 透過的識別に使用される DC Agent（*DC Agent、373 ページ*を参照）
- Active Directory による透過的識別のために Logon Agent が**ネーティブ**モードで使用されている。

上記の設定が使用している設定と一致する場合、ドメイン名をドメイン コントローラ IP アドレスに解決するために、User Service および DC Agent または Logon Agent は、Windows Internet Name Server（WINS）と通信する必要があります（*Websense アプライアンスまたは Linux サーバーに配備された User Service、585 ページ*を参照）。

その通信を有効化するために、Windows Active Directory（混在モード）のフィールドを使用して下記の情報を入力します。

1. ディレクトリ サービスにアクセスできる**管理ユーザー**のアカウント名。
2. アカウントの**パスワード**。
3. アカウントの**ドメイン**情報。
4. ネットワーク内の **WINS サーバー**の IP アドレスまたはホスト名

以下のことにご注意ください：

- DC Agent を使用している場合、DC Agent インスタンスを設定しているときに、これらのステップを [Settings] > [User Identification（ユーザー ID）] > [DC Agent] ページでも実行できます。両方の場所で設定を実行する必要はありません。
- Logon Agent を使用している場合、ネーティブモードでディレクトリに接続している場合でも、[Windows Active Directory（Mixed Mode）（Windows Active Directory（混在モード））] ページでこれらのステップを（変更のキャッシュおよび保存を含めて）実行する必要があります。その後、WINS 接続の設定が完了した時、[Windows Active Directory（Native Mode）（Windows Active Directory（ネイティブ モード））] ページ上でディレクトリ サービスの設定を完了できます。

インストールでこの設定を使用しなかった場合、管理資格情報のフィールドが無効化されます。

Windows Active Directory（ネイティブ モード）

Web Security Help | Web Security ソリューション | バージョン 7.8.x

重要

User Service が Websense アプライアンスまたは Linux サーバーに配備されていて、Logon Agent を使用してユーザーを特定する場合は、最初に [Active Directory（Mixed Mode）（Active Directory（混在モード））] ページで WINS サーバーの接続を設定します。その後、[Windows Active Directory（Native Mode）] ページに戻り、ディレクトリ サービスの接続を設定します。

Windows Active Directory は、ユーザー情報を 1 つ以上のグローバル カテゴリに保存します。グローバル カテゴリによって、個人およびアプリケーションが Active Directory ドメインにあるオブジェクト（ユーザー、グループなど）を見つけることができます。

Websense User Service がネイティブ モードの Active Directory と通信するためには、ネットワーク内のグローバル カタログ サーバーに関する情報を提供する必要があります。

1. [グローバル] カテゴリ サーバーのリストの横の **[Add]** をクリックします。[Add Global Catalog Server（グローバル カタログ サーバーを追加）] ページが表示されます。

2. グローバル カタログ サーバーの **IPv4 アドレスまたはホスト名**を入力します。
   - フェイルオーバー用に複数のグローバル カタログ サーバーを構成している場合、DNS ドメイン名を入力します。
   - グローバル カタログ サーバーがフェイルオーバー用に構成されていない場合、追加するサーバーの IPv4 アドレスまたはホスト名（ネットワーク内で名前解決が有効化されている場合）を入力します。
3. User Service がグローバル カタログとの通信で使用する**ポート**（デフォルトでは、**3268**）を入力します。
4. オプションとして、User Service がユーザーおよびグループ情報をインターネット要求に関連付けるときに使用する**ルート コンテクスト**を入力します。このコンテクストはポリシー管理に使用し、Web Security manager でクライアントを追加するためには使用しないことに注意してください。
   - 値を入力する場合、それは組織のドメインで有効なコンテクストでなければなりません。
   - 指定した通信ポートが 3268 または 3269 である場合は、ルート コンテクストを入力する必要はありません。ルート コンテクストがない場合、User Service は、ディレクトリ サービスの最高レベルで検索を始めます。
   - 指定したポートが 389 または 636 である場合は、ルート コンテクストを入力する必要があります。

   注意
   複数のドメインに同じユーザ名が存在しないようにしてください。User Service が 1 つのユーザに対して重複アカウント名を見つけると、ユーザを透過的に識別できません。

5. User Service がディレクトリ サービスからユーザー名およびパス情報を取得するために使用する管理アカウントを指定します。このアカウントは、ディレクトリ サービスのクエリーおよび読み取りを実行できる必要がありますが、ディレクトリ サービスを変更する必要はなく、またドメイン管理者である必要もありません。

   アカウント情報を入力する方法を指定するために、**[Distinguished name by components（コンポーネント別の識別名）]** または **[Full distinguished name（完全識別名）]** を選択します。

- [Distinguished name by components] を選択した場合、管理アカウントの**表示名**、アカウント **パスワード**、**アカウント フォルダ**、および **DNS ドメイン名** を入力します。管理者ユーザー名の一般名（cn）を使用します。ユーザ ID（uid）は使用しないでください。

> **注意**
>
> **[Account folder（アカウント フォルダ）]** フィールドは組織の単位（ou）タグ（例、*ou= 財務*）を持つ値をサポートしません。管理アカウント名に ou タグが含まれている場合は、その管理アカウントの完全識別名を入力します。

- [Full distinguished name] を選択した場合、**[User distinguished name（ユーザー識別名）]** フィールドに識別名を単一の文字列（例、*cn=Admin*、*cn=Users*、*ou=InfoSystems*、*dc=company*、*dc=net*）として入力し、次にそのアカウントの**パスワード** を入力します。

6. **[Test Connection（テスト接続）]** をクリックして、User Service が入力したアカウント情報を使用しているディレクトリと接続できないことを確認します。
7. **[OK]** をクリックして、[Directory Services] ページに戻ります。
8. 各グローバル カタログ サーバーについて上記の手順を繰り返します。
9. **[Advanced Directory Settings（ディレクトリの詳細設定）]** をクリックし、*拡張ディレクトリ設定、98 ページ* に進みます。

Novell eDirectory および Oracle（Sun Java）Directory Server

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ディレクトリから情報を取得するために、User Service では管理権限を持つユーザー アカウントの識別名、ルート コンテクスト、パスワードを必要とします。

1. ディレクトリ サーバーの **IPv4 アドレスまたはホスト名**を入力します。
2. User Service がディレクトリとの通信で使用する**ポート**番号を入力します。デフォルトは 389 です。
3. ディレクトリがリードオンリー アクセスのための管理者権限を必要とする場合、**管理者識別名**を入力します。
4. User Service がユーザー情報を検索するときに使用する**ルート コンテクスト**を入力します。例、*o=domain.com*。
   - ルート コンテクストの入力は、Oracle Directory Server の場合は必須ですが、Novell eDirectory の場合はオプションです。
   - コンテクストを絞り込むと、ユーザー情報の検索の速度と効率が高まります。

- User Service はこのコンテクストを、ポリシーの実施を支援するためにユーザーおよびグループ情報を検索するときに使用します。これは Web Security manager にクライアントを追加する時には使用しません。

> **注意**
> 複数のドメインに同じユーザ名が存在しないようにしてください。User Service が 1 つのユーザに対して重複アカウント名を見つけると、ユーザを透過的に識別できません。

5. 上記で入力した管理者の**パスワード**を入力します。
6. **[Test Connection（テスト接続）]** をクリックして、User Service が入力した情報を使用しているディレクトリと接続できないことを確認します。
7. **[Advanced Directory Settings（ディレクトリの詳細設定）]** をクリックし、*拡張ディレクトリ設定、98 ページ*に進みます。

拡張ディレクトリ設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Windows Active Directory（ネイティブ モード）、95 ページ*
- *Novell eDirectory および Oracle（Sun Java）Directory Server、97 ページ*

これらの設定は下記の事柄を定義するために使用します。

- Websense User Service がユーザー、グループ、ドメイン情報を検索するためにディレクトリ サービスを検索する方法
- User Service がディレクトリ サービスと通信するために暗号化された接続を使用するかどうか
- LDAP 情報を符号化するために User Service がどの文字セットを使用するのか

いずれかの LDAP ベースのディレクトリ サービスの必要に応じてこれらの設定を行います。

1. ディレクトリ サービスでカスタム オブジェクト クラス タイプ（属性名）を使用する場合は、**[Use custom filters（カスタム フィルタを使用する）]** をオンにします。デフォルト フィルタ の設定は、チェック ボックスの下にリストされます。
2. 既存のフィルタ文字列を編集して、ディレクトリ専用のオブジェクト クラス タイプに入れ替えます。例えば、ディレクトリが [**o u**] の代わりに [**dept**] などのオブジェクト クラス タイプを使用する場合は、新しい値を [Domain search filter（ドメイン検索フィルタ）] フィールドに挿入します。

   属性は常に、ディレクトリ サービス コンテンツの検索に使用される文字列です。カスタム フィルタは下記の機能を提供します。

属性	説明
ユーザー ログオン ID 属性	ユーザー ログオン名を識別します
ファースト ネーム属性	ユーザーのファースト ネームを識別します
姓属性	ユーザーの姓を識別します
グループ属性	グループの名前を識別します
MemberOf 属性	ユーザーまたはグループが他のグループのメンバーであることを指定します。 Novell eDirectory を使用している場合は、この属性は、**groupMembership** 属性に該当します。
ユーザ検索フィルタ	User Service がユーザーを検索する方法を決定します
グループ検索フィルタ	User Service がグループを検索する方法を決定します
ドメイン検索フィルタ	User Service がドメインおよび組織単位を検索する方法を決定します
ユーザのグループ検索フィルタ	User Service がユーザーをグループに関連付ける方法を決定します。

3. User Service と使用しているディレクトリ サーバーとの間で確実に通信されるようにするために、**[Use SSL（SSL を使用する）]** をオンにします。
4. User Service が LDAP 情報を符号化するために使用する文字セットを決定するために、**[UTF-8]** または **[MBCS]** を選択します。

   MBCS、またはマルチバイトの文字セットは、つ状は、中国語、日本語、韓国語など東アジアの言語を符号化するために使用します。
5. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

カスタム LDAP グループの処理

関連項目：

- *ユーザーおよびグループの処理、92 ページ*
- *ディレクトリ サービス、93 ページ*
- *カスタム LDAP グループの追加および編集、101 ページ*

ディレクトリ サービスで定義されている属性を基にカスタム グループを管理するには、**[Manage Custom LDAP Groups（カスタム LDAP グループを管理）]** ページを使用します。このオプションは、User Service が LDAP ベースのディレクトリ サービスと通信するように設定している場合にだけ利用できます。

重要

カスタム LDAP グループを追加した場合、グループ定義はアクティブな Policy Server に格納され、他の Policy Server のインスタンスには影響を与えません。カスタム LDAP グループを複数の Policy Servers に追加するには、順に各 Policy Server に接続して、情報を入力します。

カスタム LDAP グループを追加した後、ディレクトリ サービスを変更するか、またはディレクトリ サーバーの場所を変更した場合、既存のグループは無効になります。グループをもう一度追加してから、各グループをクライアントとして定義する必要があります。

- グループを追加するには、**[Add]** をクリックします（*カスタム LDAP グループの追加および編集、101 ページ*を参照）。
- リストに含まれているエントリを変更するには、そのグループ名をクリックします。（*カスタム LDAP グループの追加および編集*を参照）。
- エントリを削除するには、エントリを選択し **[Delete（削除）]** をクリックします。

カスタム LDAP グループへの変更が終わったら、**[OK]** をクリックして変更をキャッシュし、前のページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

カスタム LDAP グループの追加および編集

ディレクトリ サービスに定義されている属性に基づいてグループを定義するには、**[Add Custom LDAP Group（カスタム LDAP グループの追加）]** ページを使用します。既存の定義の変更を行うには、**[Edit Custom LDAP Group（カスタム LDAP グループを編集）]** ページを使用します。

重要

カスタム LDAP グループを追加した後、ディレクトリ サービスを変更するか、またはディレクトリ サーバーの場所を変更した場合、既存のグループは無効になります。グループをもう一度追加してから、各グループをクライアントとして定義する必要があります。

1. **グループ名**を入力または編集します。LDAP グループの目的を明確に示すわかりやすい名前を入力します。

   グループ名は大文字と小文字を区別し、一意な名前でなければなりません。
2. ディレクトリ サービスでこのグループを定義する説明を入力または変更します。例：

   ```
   (WorkStatus=parttime)
   ```

   この例では **WorkStatus** は雇用状況を示すユーザ属性であり、**parttime** はこのユーザーがパートタイム従業員であることを示す変数です。
3. **[OK]** をクリックして、[Manage Custom LDAP Groups]ページに戻ります。リストに新しいまたは変更したエントリが示されます。
4. その他のエントリを追加または編集するか、または **[OK]** をクリックして変更をキャッシュし、前のページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

クライアントの追加

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *クライアントの処理*、89 ページ
- *コンピュータとネットワークの処理*、91 ページ
- *ユーザーおよびグループの処理*、92 ページ
- *ディレクトリ サービスの検索*、103 ページ
- *クライアントの設定の変更*、104 ページ

このページを使用して下記のどちらかにユーザー、グループ、およびネットワーク クライアントを追加します。

- [Clients（クライアント）] ページ。それによってそれらにポリシーを割り当てることができます（**[Clients] > [Add Clients（クライアントの追加）]**）
- 特定の URL をブロックまたは許可するポリシーの例外（**[Exceptions] > [Add Other Clients to Exception（例外に他のクライアントを追加）]**）

指定済み管理ロールにログオンされている場合は、管理対象のクライアントリストに表示されるクライアントだけを [Clients] ページまたは例外に追加できます。

ポリシー管理およびレポーティング ロールの場合は、[Clients] ページに管理対象のクライアントを追加するプロセスでそれらのクライアントに 1 つのポリシーを割り当てる必要があります。（調査レポーティング ロールの場合はこの要件がありません）。

1. 1 つ以上のクライアントを特定します。
   - ユーザー、グループ、またはドメイン（OU）クライアントを追加するには、**ディレクトリ** ツリーを参照して、ディレクトリ サービスに含まれているエントリを見つけます。LDAP ベースのディレクトリ サービスを使用している場合は、**[Search（検索）]** をクリックして、ディレクトリ検索ツールを有効化することもできます（*ディレクトリ サービスの検索*、103 ページを参照）。
   - コンピュータまたはネットワーク クライアントを追加するには、**IP アドレス**または **IP アドレス範囲**を IPv4 または IPv6 形式で入力します。

     2 つのネットワーク定義が重複しないが、ネットワーク クライアントは、コンピュータ クライアントとして別個に識別された IP アドレスを含む場合があります。そのような重複がある場合、コンピュータに割り当てられたポリシーがネットワークに割り当てられたポリシーよりも優先されます。

2. **[Selected Clients（選択したクライアント）]** リストに各クライアントを追加するには矢印ボタン（>）をクリックします。

   [Selected Clients] リストからエントリを削除するには、クライアントを選択し、**[Remove（削除）]** をクリックします。

3. [Clients] ページに複数のクライアントを追加している場合、**ポリシー**を選択し、[Selected Clients] リストのすべてのクライアントに割り当てます。
4. 完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

選択したクライアントは、[Clients] ページまたは例外に表示されます。

複数のクライアントを [Clients] ページに追加した後、1 つ以上のクライアント エントリを選択し、**[Edit]** をクリックして、ポリシー割り当ておよび他のクライアント設定の設定値を変更できます。詳細は、*クライアントの設定の変更、104 ページ*を参照してください。

ディレクトリ サービスの検索

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense User Service を LDAP ベースのディレクトリ サービスと通信するように設定している場合は、検索機能を使用して、ポリシーまたは例外割り当てのために特定するディレクトリ クライアントを検索できます。

ディレクトリ サービスを検索してユーザー、グループ および OU 情報を取得するには、下記の手順を実行します。

1. **[Search（検索）]** をクリックします。
2. ユーザー、グループ、または OU の**名前**のすべてまたは一部を入力します。
3. **[Type（タイプ）]** リストを使用して、検索するディレクトリ エントリのタイプ（ユーザー、グループ、OU、またはすべて）を指定します。

   大きなディレクトリ サービスの場合、**[All（すべて）]** を選択すると検索時間が長くかかることがります。

4. **[Search for（検索対象）]** リストを使用して、検索を実行する方法を指定します。
   - 入力した検索条件を含むすべてのディレクトリ エントリを検索するには、**[Entries containing search string（検索文字列を含むエントリ）]** を選択します。
   - 検索条件と正確に一致するディレクトリ エントリだけを検索するには **[Exact search string only（正確な検索文字列のみ）]** を選択します。
5. **[Search Context（検索コンテクスト）]** ツリーを参照して、検索するディレクトリの部分を指定します。コンテクストが正確であればあるほど検索の速度が速くなります。

6. **[Go（実行）]** をクリックします。
   検索結果のリストが表示されます。
7. 検索結果から 1 つ以上のエントリを選択し、右矢印（> をクリックすることによって、選択したエントリをクライアントまたは管理者として追加します。
   - 検索基準の別のセットを入力するには **[New Search（新規検索）]** をクリックします。
   - 検索機能の使用を停止し、代わりにディレクトリ ツリーを検索してユーザーを特定するには、**[Browse（参照）]** をクリックします。
8. 変更を完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

クライアントの設定の変更

Web Security Help | Web Security ソリューション | バージョン 7.8.x

1 つ以上のクライアントのポリシーおよび認証の設定を変更するには、**[Policy Management] > [Clients] > [Edit Client（クライアントを編集）]** ページを使用します。[Edit] をクリックする前に、複数のクライアントを選択した場合、[Edit Client] ページで行った設定の変更が選択したすべてのクライアントに適用されます。

1. 選択したクライアントに適用する 1 つの **ポリシー**を選択します。別のポリシーが割り当てられるまでデフォルト ポリシーがクライアントを管理します。
2. **[Block Page Override Options（ブロック ページ無効化オプション）]** で、このクライアントに要求したサイトを閲覧するためにブロックページを無効にするオプションがあるかどうかを指定します。
   - （*優先管理者のみ*）[Settings] > [General] > [Filtering（フィルタリング）] ページで設定した時間（デフォルトでは 60 秒）の間ブロックしたサイトにアクセスできるように指定するパスワードを選択したクライアントが入力できるようにするには、**[Enable password override（パスワード無効化を有効化）]** をオンにします。*パスワード無効化、105 ページ*を参照してください。
     また、パスワードを入力し、確認します。
     組織のアクセス可能な使用ポリシーによって一般的には許可されていないサイトに時々アクセスする必要がある特定のユーザーに対してこのオプションを有効化することができます。
     クライアントのパスワード無効化権限を削除するには、**[Off（オフ）]** をクリックします。

- **[Enable account override（アカウント無効化を有効化）]** をオンにすると、選択したクライアントがネットワーク ログオン名およびパスワードを入力したときに、要求に対して別のポリシーが適用され、ブロックされているサイトにアクセスできるようになります。要求が新しいポリシーによって許可された場合、[Settings] > [General] > [Filtering] で設定した時間（デフォルトでは 5 分）の間、ユーザーがそのサイトにアクセスできます。*アカウントの無効化*、106 ページを参照してください。

  一般的には IP アドレス ベースのポリシーによって管理されている共有コンピュータ（例、キオスク コンピュータ）- ユーザーはゲスト アカウントを使ってログオンできる - に対してこのオプションを有効化することができます。それによってユーザーは、ブロック ページに自分のネットワーク資格情報を入力して、通常のポリシーが共有コンピュータに対してブロックされているサイトへのアクセスを許可するかどうかを確認できます。

  ユーザーのポリシーもそのサイトをブロックする場合は、ユーザーは 2 番目のブロック ページを受け取ります。

3. 選択したクライアントに**割り当て時間**のカスタム時間を割り当てるには、**[Custom（カスタム）]** をクリックし、割り当てる割り当て時間（分）を入力します。

   デフォルトの割り当て設定に戻すには、**[Default（デフォルト）]** をクリックします。

4. **[OK]** をクリックして変更をキャッシュし、[Clients] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

新しいクライアントの設定は、**[Policy Management] > [Clients]** ページのクライアント リストの一部として表示されます。

パスワード無効化

Web Security Help | Web Security ソリューション | バージョン 7.8.x

パスワード無効化によって、有効なパスワードをもつ優先管理者ロールのクライアントは、ブロックされたカテゴリに含まれているサイトにアクセスできます。パスワード無効化は 個々ユーザー、グループ、コンピュータ、ネットワーク（但しドメイン [OU] は除く）に許可されます。

優先管理者がパスワード無効化オプションを有効化したとき、管理者はパスワードも作成します。パスワード無効化の権限をもつクライアントがブロックされたサイトを要求したとき、Websense ブロック ページはパスワード フィールドを含みます。そのフィールドでクライアントは限定された時間の間ブロックされたサイトにアクセスするパスワードを入力できます。

指定済み管理者はこのオプションを使用できません。なぜならこれは実質的にフィルタ ロックを無効化する方法を提供するからです（*Filter Lock（フィルタ ロック）の作成*、416 ページを参照）。

重要

複数の Filtering Service が配備されている環境では、パスワード無効化時間の正確な割り当てのためには Websense State Server が必要です。詳細は、*Policy Server*、*Filtering Service*、*および State Server*、469 ページを参照してください。

パスワード無効化権限をもつクライアントがパスワード エントリごとにブロックされているサイトにアクセスできる時間を **[Settings] > [General] > [Filtering]** ページで設定します（*フィルタリング設定値の設定*、81 ページを参照）。

[Policy Management] > [Clients] ページを使ってパスワード無効化特権を特定の特定のクライアントに許可します（*クライアントの追加*、102 ページまたは *クライアントの設定の変更*、104 ページを参照）。

アカウントの無効化

Web Security Help | Web Security ソリューション | バージョン 7.8.x

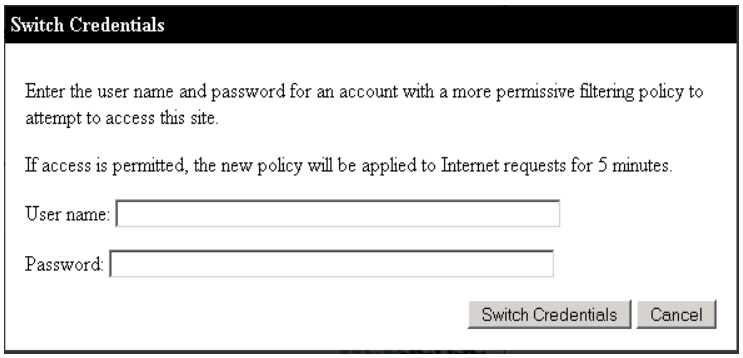
アカウントの無効化は、ユーザーが要求にポリシーを適用するために使用する資格情報を変更できるようにします。

たとえば、ユーザーがキオスク コンピュータから、またはネットワーク アカウントではなくローカル アカウントを使ってログオンしたコンピュータからインターネットにアクセスする場合、管理者はアカウント無効化許可をコンピュータまたはネットワーク（IP アドレス ベース）クライアントと関連付けることができます。

アカウント無効化許可をディレクトリ クライアント（ユーザー、グループ、ドメイン [OU]）に与えることもできます。

ユーザーの要求が現在にポリシーによってブロックされており、アカウント無効化許可がフィルタリングされるクライアント（IP アドレスまたはディレクトリ クライアント）に割り当てられている場合、ブロック ページは、

[Enter New Credentials（新しい資格情報を入力）] ボタンを含みます。そのボタンを使ってユーザーはユーザー名およびパスワードを入力できます。



ユーザーが **[Switch Credentials（資格情報を切り替え）]** をクリックした後、Websense Filtering Service は新しいアカウントに割り当てられたポリシーを特定し、そのポリシーを要求に適用します。

- 新しいポリシーが要求を許可すれば、ユーザーはそのサイトにアクセスできます。
- 新しいポリシーが要求をブロックば、ユーザーには別のブロックページが表示されます。

つまり、パスワード無効化とは異なり、アカウント無効化オプションはブロックされたサイトへのアクセスを保証していません。代わりに、要求をフィルタリングするために使用するポリシーを変更します。

[Settings] > [General] > [Filtering] ページで指定した時間（デフォルトでは 5 分）の間、そのコンピュータ上のその他の要求に新しいポリシーが適用されます。*フィルタリング設定値の設定*、81 ページを参照してください。

重要

複数の Filtering Service が配備されている環境では、アカウント無効化時間の正確な割り当てのためには Websense State Server が必要です。詳細は、*Policy Server*、*Filtering Service*、および *State Server*、469 ページを参照してください。

ユーザー資格情報を正常に切り替えた後、ユーザーがアカウント無効化時間が終了する前にコンピュータから離れる場合は、下記の URL を入力して、無効化セッションを手動で終了できます。

```
http://<Filtering_Service_IP_address> :15871/cgi-bin/
cancel_useraccount_overrider.cgi
```

アカウント無効化オプションを使用するコンピュータ上でこの URL をブラウザ ブックマークとして使用することができます。

クライアントをロールに移動

Web Security Help | Web Security ソリューション | バージョン 7.8.x

優先管理者は、**[Move Client To Role（クライアントをロールに移動）]** ページを使用して、1 つ以上のクライアントを指定済み管理ロールに移動できます。クライアントが移動した後、そのクライアントは [Managed Clients] リストとターゲット ロールの [Clients] ページに表示されます。

- 優先管理者ロールのクライアントに適用されたポリシーおよびポリシーが適用するフィルタは、指定済み管理ロールにコピーされます。
- 指定済み管理者はそれらの管理対象のクライアントに適用されているポリシーを変更できます。
- フィルタ ロック制限は、優先管理者によって管理されているクライアントには影響を及ぼしませんが、指定済み管理者ロールで管理されているクライアントに影響を及ぼします。
- グループ、ドメイン、または組織単位が管理対象のクライアントとしてロールに追加された場合、そのロールに含まれている指定済み管理者は、グループ、ドメイン、または組織単位の個々のユーザーにポリシーを割り当てることができます。
- ネットワーク（IP アドレス範囲）が管理対象のクライアントとしてロールに追加された場合、そのロールに含まれている指定済み管理者はそのネットワーク内の個々のコンピュータにポリシーを割り当てることができます。
- 同じクライアントを複数のロールに移動できません。

選択したクライアントを指定済み管理ロールに移動するには、下記の手順を実行します。

1. **[Select role（ロールを選択）]** ドロップダウン リストを使用して移動先ロールを選択します。
2. **[OK]** をクリックします。

   ポップアップ メッセージが、選択したクライアントは移動中であることを示します。移動プロセスには時間がかかります。
3. **[Save and Deploy]** をクリックするまで変更は適用されません。

移動プロセス中に選択したロールのポリシー アクセス権を持つ指定済み管理者がログオンした場合、処理対象クライアント リストの新しいクライアントを表示するには、TRITON コンソールをログアウトし、ログオンしなおさなければなりません。

ハイブリッド サービス クライアントの処理

Websense Web Security Gateway Anywhere 環境では、ハイブリッド サービスは、指定した外部 IP アドレス（場所）から発信されたインターネット要求、および不明の場所からハイブリッド サービスにログオンしているユーザー（例、オフサイトのユーザー）からのインターネット要求を管理できます。

ハイブリッド サービスは、下記のクライアントに対してポリシー（Web Security manager で作成）を適用できます。

- サポートされている LDAP ベースのディレクトリ サービスで定義されているユーザー、グループ、およびドメイン（OU）。

  そのために Websense Directory Agent をインストールし設定する必要があります（*ハイブリッド ユーザーの識別、391 ページ*を参照）。
- フィルタリング対象の場所、[Hybrid Configuration（ハイブリッド設定）] > [Filtered Locations（フィルタリング対象の場所）] ページで識別されます。場所は、外部 IP アドレス、IP アドレス範囲、または 1 つ以上のファイアウォールのサブネット、またはゲートウェイ コンピュータによって識別されます。

ハイブリット サービスは、ネットワーク内の個々のクライアント コンピュータにポリシーを適用**しません**。

ハイブリッド サービスによって管理されたディレクトリ クライアント（ユーザー、グループ、および OU）は、それらの要求がオンプレマイズ コンポーネントによって管理されるのと同様に、[Policy Management] > [Clients] ページで識別されます。

フィルタリング対象の場所へのポリシーの適用は、コンピュータまたはネットワーク クライアントへのポリシーの適用に似ています。

1. 場所を [Settings] > [Hybrid Configuration] > [Filtered Locations（フィルタリング対象の場所）] ページに追加します（*フィルタ対象の場所を定義、263 ページ*を参照）。
2. [Filtered Locations] ページに表示される IP アドレスまたは範囲をコンピュータまたはネットワーク クライアントとして [Policy Management] > [Clients] ページで追加します（*コンピュータとネットワークの処理、91 ページ*を参照）。
3. ポリシーを IP アドレスまたは範囲に適用します。

ユーザー、グループ、または場所ポリシーが適用しないときは常に、デフォルト ポリシーが使用されます。

5 インターネット アクセスのポリシー

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *インターネット使用状況のフィルタ、57 ページ*
- *クライアント、87 ページ*
- *Default ポリシー、112 ページ*
- *ポリシーの使用、113 ページ*
- *適用順序、119 ページ*

ポリシーはユーザーのインターネット アクセスを管理します。ポリシーは、下記の要素から成ります。

- カテゴリ フィルタ。URL カテゴリにアクション（許可、ブロック）を適用するために使用します（*カテゴリおよびプロトコルへのアクセスの管理、59 ページ*を参照）。
- 制限付きアクセス フィルタ。制限された URL のリストにのみアクセスを許可するために使用します（*ユーザーのアクセスを、指定した URL のリストに制限する、314 ページ*を参照）。
- プロトコル・フィルタ。インターネット プロトコルにアクションを適用するために使用します（*カテゴリおよびプロトコルへのアクセスの管理、59 ページ*を参照）。
- 各カテゴリまたは制限付きアクセス フィルタとプロトコル フィルタをいつ適用するかを設定するスケジュール。

新しい Websense Web Security インストレーションには、3 つの事前定義ポリシーが含まれています：

- **[Default（デフォルト）]** は、他のポリシーによって管理されていないすべてのクライアントのインターネット アクセスをフィルタします。このポリシーは、サブスクリプション キーを入力するとすぐにアクティブになります（*Default ポリシー、112 ページ*を参照）。
- **[Unrestricted（無制限）]** は、インターネットへの無制限のアクセスを提供します。このポリシーは、デフォルトではどのクライアントにも適用されません。
- **[Example - Standard User（例 - 標準ユーザー）]** は、1 つのポリシーで複数のカテゴリおよびプロトコル フィルタを適用して、時間帯ごとに異なるインターネット アクセスを提供する方法を示します。このポリシーは

これらのポリシーをそのまま使用するか、ユーザーの組織に適合するように編集するか、またはユーザーの組織の固有のポリシーを作成します。

Default ポリシー

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *インターネット アクセスのポリシー、111 ページ*
- *ポリシーの使用、113 ページ*
- *適用順序、119 ページ*

インストールの後、有効なサブスクリプション キーを入力したとき、**Default** ポリシーによってインターネット アクティビティのモニタリングが開始されます。使用開始直後は、Default ポリシーはすべての要求を許可します。

注意

Websense ソフトウェアの以前のバージョンからアップグレードするとき、既存のポリシー設定は維持されます。アップグレード後にポリシーを調べてそれらが今でも適切であることを確認してください。

追加的なポリシーを作成および適用するとき、Default ポリシーは引き続き、他のポリシーが割り当てられていないすべてのクライアントのインターネット アクセスを管理します。

Default ポリシーは 1 日 24 時間、週 7 日、適用範囲（カテゴリまたは制限アクセス付きフィルタとプロトコル フィルタの組み合わせを適用する）を提供しなければなりません。

重要

Websense ソフトウェアの以前のバージョンからアップグレードした場合に、継承された Default ポリシーがすべての時間帯をカバーしていない場合があります。Default ポリシーを変更することは要求されません。しかし、ポリシーを編集する場合、すべての時間帯がカバーされていない限り、変更を保存できません。

組織のニーズに応じて、Default ポリシーを編集してください。Default ポリシーは削除できません。

ポリシーの使用

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *インターネット アクセスのポリシー、111 ページ*
- *ポリシーの作成、115 ページ*
- *ポリシーの編集、116 ページ*
- *インターネット使用状況のフィルタ、57 ページ*
- *Web Security ポリシーの調整、313 ページ*

既存のポリシー情報を検討するとき、**[Policy（ポリシー）][Management（管理）] > [Policies（ポリシー）]** ページを使用します。このページはまた、ポリシーの追加、編集、削除や、指定済み管理者ロールへのポリシーのコピー（優先管理者のみ）、ポリシー設定に関する詳細情報の出力を開始するためにも使用します。

[Policies] ページには、既存のポリシーのリストが表示されます。このリストは、各ポリシーの名前と説明、およびそのポリシーが割り当てられているユーザー、ネットワーク、コンピューター クライアントの数を含みます。

- ポリシーを追加するには、**[Add（追加）]** をクリックし、次に*ポリシーの作成、115 ページ*の手順を実行します。
- ポリシーを編集するには、リストの中のポリシー名をクリックし、次に*ポリシーの編集、116 ページ*の手順を実行します。
- ポリシーを削除するには、ポリシー名の横のチェックボックスをオンにし、**[Delete（削除）]** をクリックします。
- どのクライアントがそのポリシーによってフィルタリングされているかを調べるには、[Users（ユーザー）]、[Networks（ネットワーク）] または [Computers（コンピュータ）] 列の中の番号をクリックします。ポップアップ ウィンドウにクライアント情報が表示されます。

ポリシーとそのコンポーネントについて、フィルタ、カスタム カテゴリおよびプロトコル、キーワード、カスタム URL、正規表現などの情報を含むリストをファイルに出力するには、**[Print Policies To File（ポリシーをファイルに出力）]** をクリックします。この機能では、ポリシーに関する情報の詳細なスプレッドシートが Microsoft Excel 形式で作成されます。これは HR 担当者や管理者、その他の管理者権限を持つ人がポリシーに関する情報を検討するための便利な手段となります。

指定済み管理者ロール（*代理管理およびレポート作成、405 ページ*を参照）を作成した場合、優先管理者は、他のロールに対して作成したポリシーを指定済み管理者が使用できるようにコピーすることができます。そのポリシーによって適用されるフィルタもコピーできます。

注意

指定済み管理者は [Filter Lock（フィルタ ロック）] によって管理されますから、[Permit All（すべてを許可）] フィルタがコピーされたとき、そのコピーには新しい名前が割り当てられ、[Filter Lock] による制約が適用されます。オリジナルのフィルタは編集できませんが、コピーされたフィルタは編集できます。

ポリシーを他のロールにコピーするには、ポリシー名の横のチェックボックスをオンにし、**[Copy to Role（ロールにコピー）]** をクリックします。この処理には数分かかる場合があります。詳細は、*ロールへのフィルタおよびポリシーのコピー、319 ページ*を参照してください。

ポリシーの作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *インターネット アクセスのポリシー、111 ページ*
- *ポリシーの使用、113 ページ*
- *ポリシーの編集、116 ページ*
- *フィルタの使用、71 ページ*
- *ユーザーのアクセスを、指定した URL のリストに制限する、314 ページ*

新しいカスタム ポリシーを作成するとき、**[Policy][Management] > [Policies] > [Add Policy（ポリシーを追加）]** ページを使用します。

1. 一意な**ポリシー名**を入力します。名前は 1 ～ 50 文字でなければならず、また、以下の文字を含むことはできません。

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   ポリシー名にはスペース、ダッシュ、アポストロフィーを含めることができます。

2. ポリシーの **[Description（説明）]** を入力します。説明は長期間にわたってポリシー管理に役立つように、明確で具体的な内容にしてください。

   ポリシー名に適用される使用文字の制限は、説明にも適用されますが、2 つの例外があります。説明にはピリオド（.）およびカンマ（,）を使用できます。

3. 既存のポリシーを新しいポリシーのベースとして利用する場合は、**[Base on existing policy（既存のポリシーをベースにする）]** をクリックし、次に、ドロップダウン リストでポリシーを選択します。

   空白のポリシーから開始する場合は、このチェック ボックスにマークを付けないでおきます。

4. **[OK]** をクリックして変更をキャッシュし、[Edit Policy（ポリシーの編集）] ページに進みます。

   [Edit Policy（ポリシーの編集）] ページを使って新しいポリシーの定義を完了します。*ポリシーの編集、116 ページ*を参照してください。

ポリシーの編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *インターネット アクセスのポリシー、111 ページ*
- *ポリシーの使用、113 ページ*
- *ポリシーの作成、115 ページ*
- *フィルタの使用、71 ページ*
- *ユーザーのアクセスを、指定した URL のリストに制限する、314 ページ*

[Policy Management] > [Policies] > [Edit Policy] ページを使用して既存のポリシーを変更する、または新規のポリシーの定義を終了します。

ページの上部を使用して、ポリシー名と説明を編集します。

- ポリシー名を変更するには、**[Rename（名前の変更）]** をクリックします。
- フィルタの説明を変更するには、**[Description]** フィールドに入力します。

ポリシーの説明の下の **[Clients（クライアント）]** フィールドは、現在このポリシーによってフィルタリングされている各タイプのクライアント（ディレクトリ、コンピュータ、ネットワーク）の数をリストします。このポリシーによってどのクライアントが管理されているかを調べるには、そのクライアント タイプに対応するリンクをクリックします。

このポリシーをそれ以外のクライアントに割り当てるには、画面の上部のツールバーの **[Apply to Clients（クライアントに適用）]** をクリックし、*1 つのポリシーを複数のクライアントに割り当てる、119 ページ*の手順を実行します。

[Policy Definition（ポリシーの定義）] 領域は、このポリシーが種々の時間帯にどのフィルタを適用するかを定義するために使用します。

1. スケジュールに時間ブロックを追加するには、**[Add]** をクリックします。
2. [Schedule（スケジュール）] テーブルの **[Start（開始）]** および **[End（終了）]** 列を使用して、この時間ブロックがカバーする時間を定義します。

   午前 0 時を超える時間（例、午後 5 時から午前 8 時）のフィルタを定義するためには、スケジュールに 2 つの時間ブロックを追加します。開始時から午前 0 時までの時間と、午前 0 時から終了時までの時間です。

   [Example - Standard User] ポリシーは、午前 0 時を超える時間帯を定義する方法を示します。

3. **[Days（日）]** 列は、この時間ブロックに含まれる曜日を定義します。リストから日を選択するには、列の右側の下向き矢印をクリックします。日の選択を完了したとき、上向き矢印をクリックします。
4. **[Category / Limited Access Filter（カテゴリ / 制限付きアクセス フィルタ）]** 列は、この時間ブロックで適用するフィルタを選択するために使用します。

   このポリシーで適用する新しいフィルタを追加するには、**[Create category filter（カテゴリ フィルタの作成）]** または **[Create limited access filter（制限付きアクセス フィルタの作成）]** を選択します。その方法については *カテゴリ フィルタの作成、72 ページ*または*制限付きアクセス フィルタの作成、316 ページ*を参照してください。
5. **[Protocol Filter（プロトコル フィルタ）]** 列は、この時間ブロックで適用するプロトコル フィルタを選択するために使用します。

   このポリシーで適用する新しいフィルタを追加するには、**[Create protocol filter（プロトコル フィルタの作成）]** を選択します。手順については、*プロトコル フィルタの作成、76 ページ*を参照してください。
6. スケジュールに時間ブロックを追加するには、ステップ 1 ～ 5 を繰り返します。

スケジュールの中のいずれかの時間ブロックが選択されている時、[Edit Policies] ページの下部に、その時間ブロックに適用されるフィルタが表示されます。各フィルタ リストには下記の情報が含まれます。

- フィルタ タイプ（カテゴリ フィルタ、制限つきアクセス フィルタ、またはプロトコル フィルタ）
- フィルタ名と説明
- フィルタの内容（処置が適用されるカテゴリまたはプロトコル、または許可されているサイトのリスト）
- 選択したフィルタを適用するポリシーの数
- フィルタを編集するために使用できるボタン

このページでフィルタを編集したとき、変更はそのフィルタを適用する各ポリシーに影響を及ぼします。複数のポリシーによって適用されているフィルタを編集する場合は、その前に **[Number of policies using this filter（このフィルタを使用しているポリシーの数）]** リンクをクリックして、どのポリシーが変更の影響を受けるかを正確に確認しておきます。

フィルタ リストの下に表示されるボタンは、フィルタ タイプによって異なります。

ファイル タイプ	ボタン
カテゴリ フィルタ	• 選択したカテゴリに適用する処置を変更するには、**[Permit（許可）]**, **[Block（ブロック）]**、**[Confirm（確認）]** または **[Quota（割り当て）]** ボタンをクリックします（*処置、68 ページ*を参照）。 • 親カテゴリと、そのサブカテゴリ全体に割り当てる処置を変更するには、はじめに親カテゴリに適用する処置を変更し、次に **[Apply to Subcategories（サブカテゴリに適用）]** をクリックします。 • キーワード ブロック、ファイル タイプ ブロック、または帯域幅を基にしたブロックを有効化するには、**[Advanced（詳細）]** をクリックします。
制限付き アクセス フィルタ	• **[Add Sites（サイトの追加）]** および **[Add Expressions（正規表現の追加）]** ボタンは、フィルタに許可されている URL、IP アドレス、または正規表現を追加するために使用します（*ユーザーのアクセスを、指定した URL のリストに制限する、314 ページ*を参照）。 • サイトをフィルタから削除するには、URL、IP アドレス、または正規表現の横のチェックボックスをオンにし、**[Delete]** をクリックします。
プロトコル フィルタ	• 選択したプロトコルに適用する処置を変更するには、**[Permit]** または **[Block]** ボタンを使用します（*処置、68 ページ*を参照）。 • プロトコル グループのすべてのプロトコルに適用する処置を変更するには、はじめにグループ内のいずれかのプロトコルに適用する処置を変更して、次に **[Apply to Group（グループに適用）]** をクリックします。 • 選択したプロトコルのデータをログに記録する、または帯域幅を基にしたブロックを有効化するには、**[Advanced]** をクリックします。

ポリシーの変更を完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

1 つのポリシーを複数のクライアントに割り当てる

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *インターネット アクセスのポリシー*、111 ページ
- *ポリシーの作成*、115 ページ
- *ポリシーの編集*、116 ページ
- *クライアント*、87 ページ
- *クライアントの追加*、102 ページ

選択したポリシーをクライアントに割り当てるには、**[Policies] > [Edit Policy] > [Apply Policy to Clients]** ページを使用します。

クライアント リストは、使用可能なすべてのディレクトリ、コンピュータ、ネットワーク クライアント、および各クライアントに現在割り当てられているポリシーを表示します。

1. 選択したポリシーを割り当てる各クライアントの隣のチェック ボックスをオンにします。
2. [Edit Policy] ページに戻るために、**[OK]** をクリックします。
3. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

適用順序

Web Security Help | Web Security ソリューション | バージョン 7.8.x

要求されたインターネット データを許可、ブロック、または制限するかどうかを決定するために、複数の基準が、特定の順序で使用されます。

Websense Web Security ソリューションは、受け取った各要求を下記のように処理します。

1. サブスクリプションの適合性を確認し、サブスクリプションが現在有効であり、登録されているクライアントの数が規定数を超えていないことを確認する。
2. どの例外またはポリシーを適用するかを決定する。以下の順序で検索します。
   - オンプレマイズ ソフトウェア（Websense Filtering Service）
     a. **ユーザー**に割り当てられているポリシーまたは例外
     b. 使用中のコンピュータの **IP アドレス**（コンピュータまたはネットワーク）に割り当てられているポリシーまたは例外

c. ユーザーが属している**グループ**に割り当てられているポリシーまたは例外
d. ユーザーの**ドメイン（OU）**に割り当てられているポリシーまたは例外
e. **デフォルト**ポリシー

> **注意**
> 必要ならば、Filtering Service がグループまたはドメイン ベースのポリシーを IP アドレス ベースのポリシーよりも優先させるように設定することができます。*グループおよびドメイン ポリシーの優先度設定*、121 ページを参照してください。

- （*Websense Web Security Gateway Anywhere*）要求がハイブリッドサービスによって管理されるされるユーザーの場合、
  a. **ユーザー**に割り当てられているポリシーまたは例外
  b. ユーザーが属している**グループ**に割り当てられているポリシーまたは例外
  c. ユーザーの**ドメイン（OU）**に割り当てられているポリシーまたは例外
  d. 要求の発行元の外部 **IP アドレス**（フィルタされている場所）に割り当てられているポリシーまたは例外
  e. **デフォルト**ポリシー

  最初に見つかった該当する例外またはポリシーが使用されます。

3. 要求を例外またはポリシーの制限に従ってフィルタする。

ユーザが 2 つ以上のグループまたはドメインに属していて、優先度の高いポリシーが適用されていない場合があります。この場合、Websense Web Security ソリューションは、各ユーザー グループに割り当てられたポリシーをチェックします。

- すべてのグループが同じポリシーを割り当てられている場合は、Websense ソフトウェアはそのポリシーを適用します。
- 1 つのグループに他のグループと異なるポリシーが割り当てられている場合は、Websense ソフトウェアは **[Settings（設定）] > [General（一般）] > [Filtering（フィルタリング）]** ページの **[Use more restrictive blocking（より厳格な制限でブロックをする）]** の選択を使用して、適用するポリシーを決定します。
  - **[Use more restrictive blocking]** がオンになっている場合、要求されたカテゴリへのアクセスが、適用されるいずれかのポリシーによってブロックされていれば、そのサイトはブロックされます。

- このオプションがオフになっている場合、要求されたカテゴリへのアクセスが、適用されるいずれかのポリシーによって許可されていれば、サイトはアクセスを許可されます。

適用されるいずれかのポリシーが制限付きアクセス フィルタを適用する場合、**[Use more restrictive blocking]** オプションは想定しているのと異なる結果をもたらす可能性があります。*制限付きアクセス フィルターと実施の順序*、314 ページを参照してください。

- 1 つのグループが他のグループと異なるポリシーを割り当てられていて、適用される可能性があるいずれかのポリシーがファイル タイプ ブロックを適用する場合、そのファイル タイプ ブロックの設定は無視されます。

グループおよびドメイン ポリシーの優先度設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

組織が IP アドレス（コンピューターおよびネットワーク）に適用されるポリシーよりもディレクトリ ポリシー（ユーザー、グループ、ドメインに適用される）を優先させたい場合があります。

これはたとえば、グループ ベースのポリシーが組織の中で広く使用されており、ネットワーク内の IP アドレスに [Account Override（アカウントの無効化）]（*アカウントの無効化*、106 ページを参照）が適用される場合に起こります。デフォルトの適用優先順位が使用されていて、IP アドレス ベースのポリシーがグループ ベースのポリシーを無効化するとき、アカウントの無効化の失敗が頻繁に起こる可能性があります。グループおよびドメイン ポリシーが優先されていれば、この問題は回避されます。

Websense Filtering Service がディレクトリ ポリシーを優先させるように設定する（要求に適用するポリシーを決定する際に [User] > [Group] > [Domain] > [Computer] > [Network] の順に検索する）ことができます。

Filtering Service が Windows または Linux サーバー上にインストールされている場合、

1. Filtering Service を実行しているコンピュータ上で Websense **bin** デシレクトリ（C:\Program Files または Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）に移動します。
2. **eimserver.ini** ファイルをテキストエディタで開きます。
3. ファイルの **[FilteringManager]** セクションを見つけ、下記のパラメータを追加します。

   ```
   UserGroupIpPrecedence=true
   ```

4. ファイルを保存して閉じます。

5. Filtering Service を再び起動します。
   - *Windows*: [Windows Services（Windows サービス] ツールで **Websense Filtering Service** を再起動します。
   - *Linux*: /opt/Websense/WebsenseDaemonControl コマンドを使って **Filtering Service** を再起動します。

Filtering Service が Websense アプライアンス上のある時、

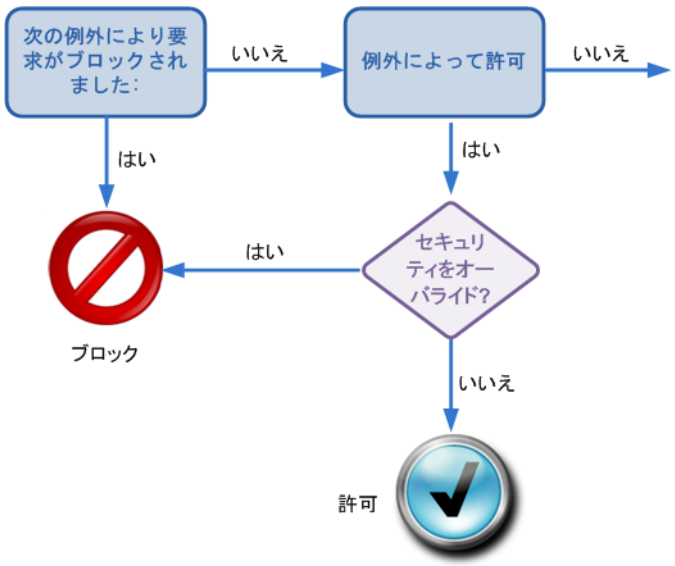
1. Content Gateway manager にログ オンします。
2. **[Administration] > [Toolbox]** ページに移動します。
3. Appliance Command Line セクションの [Command Line Utility] の下の **[Launch Utility]** をクリックします。
4. モジュールのドロップダウン リストから **Websense Web Security** を選択します。
5. [Command] フィールドに **user-group-ip-precedence** と入力します。
6. **[Action（アクション）]** フィールドで **[enable（許可）]** を選択します。

   変更を適用するために Filtering Service が停止し、自動的に再起動されます。

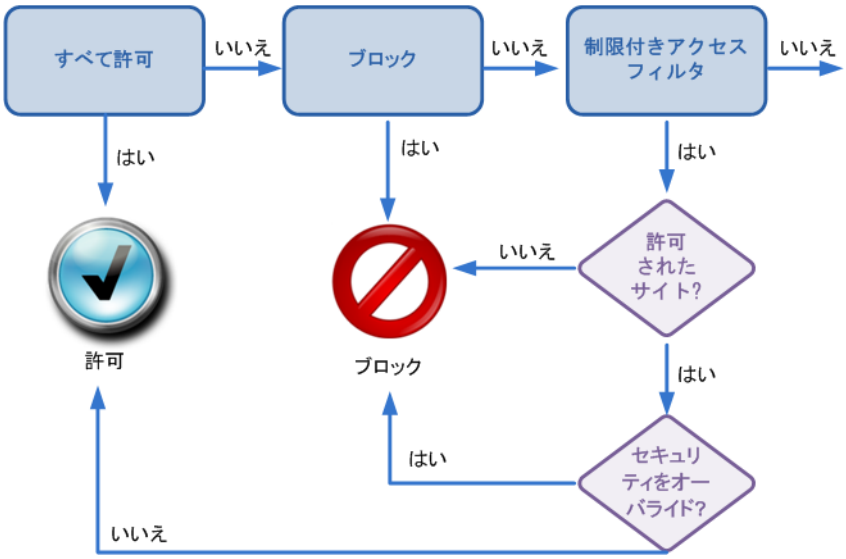
URL 要求への応答

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Filtering Service は、以下の順にポリシー制約を評価して要求されたサイトへのアクセスを許可するかブロックするかを決定します。（Websense Web Security Gateway Anywhere 環境では、ここに示すロジックはオンプレマイズ ソフトウェアには適用されますが、ハイブリッド サービスには適用されません）。



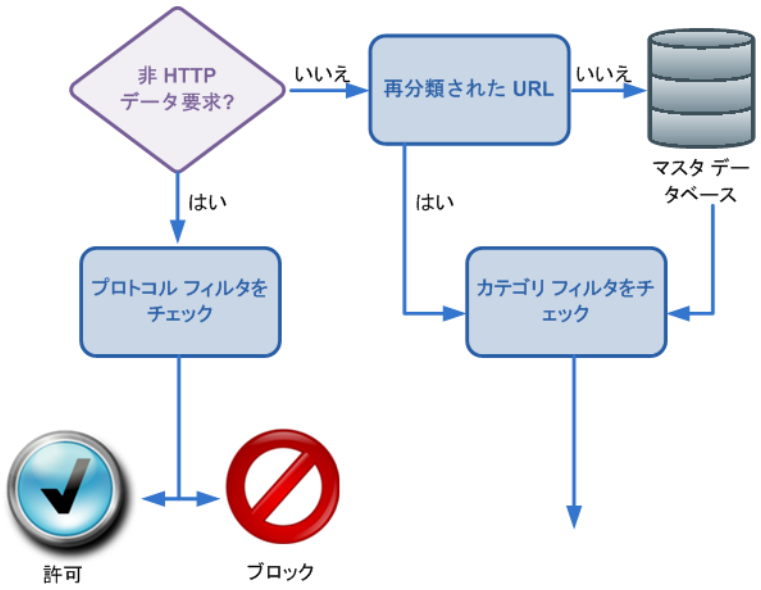
1. サイトが **exception（例外）**にリストされているかどうかをチェックします。
   - **[block exception（例外をブロック）]** が指定されている場合、サイトをブロックします。
   - **[permit exception（例外を許可）]** が指定されている場合、サイトを許可します。
   - サイトに適用される例外がなければ、手順 2 に進みます。



2. ポリシーが現在の日時にどの**カテゴリ フィルタ**または**制限つきアクセス フィルタ**を適用するかを決定します。
   - アクティブな URL カテゴリ・フィルタが **[Permit All（すべて許可）]** である場合、サイトを許可します。
   - アクティブな URL カテゴリ・フィルタが **[Block All（すべてブロック）]** である場合、サイトをブロックします。
   - フィルタが**制限つきアクセス フィルタ**である場合、フィルタがそのサイトの URL または IP アドレスを含んでいるかどうかをチェックします。その URL または IP アドレスを含んでいる場合、そのサイトを許可します。そうでない場合、そのサイトをブロックします。

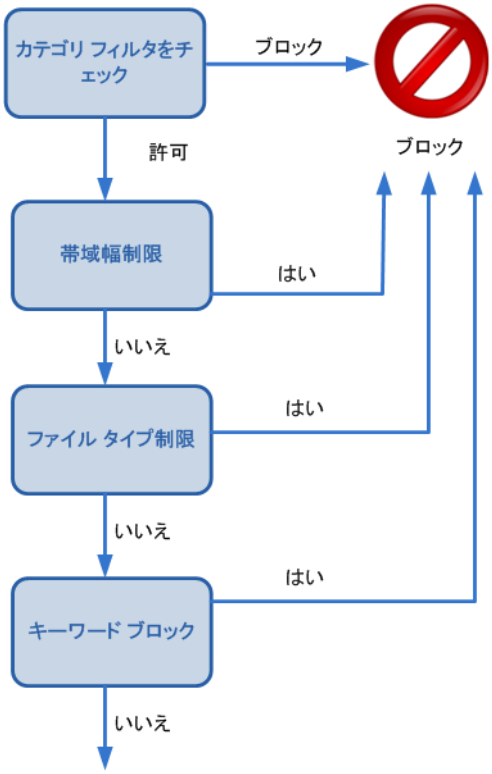
- 他のカテゴリ・フィルタが適用される場合、手順 3 に進みます。

> **注意**
> Filtering Service は、検索エンジンからアクセスした URL を他の URL と同様に処理します。それらの URL は該当するポリシーに従ってブロックまたは許可されます。キャッシュされた URL のログ レコードは、キャッシュされた URL 全体（検索エンジン パラメータを含む）を示します。



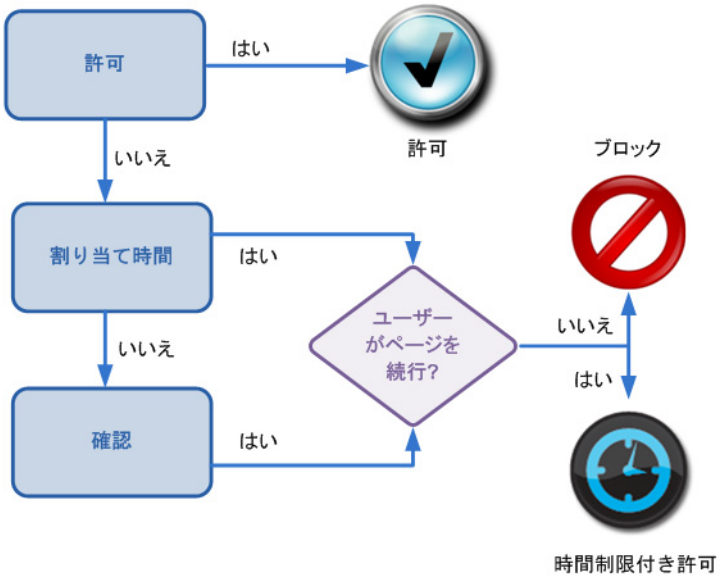
3. アクティブな**プロトコル フィルタ**をチェックし、要求に関連づけられている非 HTTP プロトコルがあるかどうかを調べます。
   - そのような 非 HTTP がある場合、プロトコル フィルタで定義されているとおり、適切なアクションを適用します。
   - そうでない場合は、手順 4 に進みます。
4. サイトを **Recategorized URLs** リストのエントリと照合します。
   - 一致するサイトがあれば、そのサイトのカテゴリを指定し、手順 6 に進みます。
   - 一致するサイトがなければ、手順 5 に進みます。

5. サイトを **Master Database** のエントリと照合します。
   - その URL が Master Database にあれば、そのサイトのカテゴリを指定し、手順 6 に進みます。
   - その URL がなければ、サイトを[Miscellaneous/Uncategorized（その他/未分類）] に分類し、手順 6 に進みます。



6. アクティブなカテゴリ フィルタをチェックし、要求されたサイトを含むカテゴリに適用される処置を指定します。
   - 処置が [**ブロック**] になっている場合、サイトをブロックします。
   - 他の処置が適用される場合、手順 7 に進みます。
7. アクティブなカテゴリ フィルタの **[Bandwidth Optimizer（帯域幅オプティマイザー）]** の設定をチェックします（*Bandwidth Optimizer による帯域幅の管理、342 ページ*を参照）。
   - 現在の帯域幅使用量が指定限界を超える場合、そのサイトをブロックします。
   - 限界を超えない場合、またはどの帯域幅ベースのフィルタリング・オプションもアクティブでない場合、手順 8 に進みます。

8. アクティブなカテゴリに適用される**ファイルの種類**制約をチェックします（*ファイル タイプに基づくトラフィックの管理、345 ページ*を参照）。
   - サイトに拡張子が[ブロック]に設定されているファイルが含まれる場合、それらのファイルへのアクセスをブロックします。サイト全体がブロックされたファイルの種類から成っている場合、そのサイトへのアクセスをブロックします。
   - サイトに拡張子が[ブロック]に設定されているファイルが含まれない場合、手順 9 に進みます。
9. キーワード ブロックが有効化されている場合、URL および CGI パスでブロックされている**キーワード**をチェックします（*キーワードベースのポリシーの実施、327 ページ*を参照）。
   - キーワードがブロックされていた場合、サイトをブロックします。
   - ブロックされたキーワードがなければ、手順 10 に進みます。



10. カテゴリに設定されたフィルタリング アクションに従って、サイトを処理します。
    - **Permit**（**許可**）サイトを許可します。
    - **Limit by Quota**（**割り当て時間で制限**）ブロック・メッセージと、割り当て時間を使用してサイトを閲覧するか、前のページに戻るかのオプションを合わせて表示します。
    - **Confirm**（**確認**）ブロック・メッセージと、業務目的でサイトを表示するオプションを合わせて表示します。

Filtering Service は、要求されたサイトがブロックされるか明示的に許可されるまで処理を続けます。サイトがブロックまたは明示的に許可された時点で、それ以上の調査は行われません。たとえば、要求されたサイトがブロックされるカテゴリに属し、ブロックされるキーワードを含んでいる場合、Filtering Service は、カテゴリ レベルでサイトをブロックし、キーワードのチェックは行いません。この場合、Log Server はブロック カテゴリに属するサイトであるために要求がブロックされたと記録し、キーワードが原因でブロックされたとは記録しません。

注意

パスワード アクセス権限を持つユーザは、サイトがブロックされた理由に関わらず、ウェブサイトにアクセスすることができます。

6 ポリシーの例外

Web Security Help | Web Security ソリューション | バージョン 7.8.x

例外により、管理者はブロック カテゴリの URL と IP アドレスを速やかに許可したり、許可カテゴリの URL と IP アドレスを速やかにブロックすることができます。

例外の作成は、URL のカテゴリの変更を必要としないし、また影響を受けるクライアントに割り当てられているポリシーを変更するようなこともありません。これにより、ユーザーの要求、企業のポリシーの変更、インターネット アクティビティのスパイク、およびその他の環境の変化に柔軟かつ迅速に対応することができます。

例：

- [Default]ポリシーによって[ショッピング]カテゴリへのアクセスが禁止されているにも関わらず、すべての従業員に、承認されたベンダーのウェブサイトへのアクセスを許可する。
- [学生]ロールのすべてのクライアントに対して、ウェブサイトの調査中に疑わしいトラフィック スパイクが起こっている未分類の URL へのアクセスをブロックする。
- [ブログ] および [パーソナル] カテゴリのサイトへの一般的アクセスをブロックしたまま、Web Marketing チームの 3 人のメンバーに、あるデザイン ブログへのアクセスを許可する。
- HR 担当者の要求により、特定のユーザーに対してリスト内の URL へのアクセスをブロックする。

一般的なタスクについての簡潔な説明は*例外のショートカット、138 ページ*に示しています。

例外に含めることができる情報に関する詳細は、*例外の処理、130 ページ*を参照してください。

例外の処理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *例外の追加または編集*、133 ページ
- *複数の例外の同時編集*、137 ページ

[Policy Management（ポリシー管理）] > [Exceptions（例外）] ページを使って既存の例外を表示、編集、削除したり、新しい例外を作成することができます。

Super Administrators は、どのロールで作成されたかに関わりなく、すべての例外を見ることができます。指定済み管理者は、当該管理者の現在のロールに影響するすべての例外を見ることができます。リストの中の例外の編成の詳細については、*例外の編成*、132 ページを参照してください。

- 例外によって 1 つの URL または正規表現がブロックまたは許可されている場合、その URL または正規表現がリストされます。そうでない場合、[URLs] 列の中のリンクをクリックすると、影響を受ける URL の完全なリストが表示されます。
- 例外の影響を受けるのが
  - 1 つのクライアントである場合、クライアントの IP アドレス、アドレス範囲、または表示名がリストされます。
  - 1 つのロールである場合、ロール名が "Role [Role_Name]" の形式で表示されます。
  - すべてのロールのすべてのクライアントである場合、"Global" という語が表示されます。

    指定済み管理者が無効化できるグローバル例外は、[Clients] 列にアイコンが表示されます（*例外の無効化*、136 ページを参照）。
  - 複数の、特定のクライアントである場合、クライアントの数が表示されます。リンクをクリックすると、影響を受ける URL の完全なリストが表示されます。

例外リストは、下記の項目も表示します。

列	説明
Type（タイプ）	例外に含まれる URL に対する処置を示すアイコンを表示します。 • ブロック（  ） • 許可（  ） • 許可、セキュリティの無効化を無効化（  ）
Last Modified（最後の更新日付）	例外が最後に編集された日付を示します。
Expires（期限）	例外に期限が設定されているかどうか、および、設定されている場合はその日付を示します。
Active（アクティブ）	例外が現在、フィルタリングで適用されている（Active）か、適用されていない（Inactive）かを示します。

[Filter] ドロップダウン リストを使って、指定した特性を持つ例外だけを表示します。下記のフィルタを利用できます。

フィルタ	説明
Permitted（許可）	URL を許可する例外
Blocked（ブロック）	URL をブロックする例外
Active（アクティブ）	現在適用されている例外。
Inactive（非アクティブ）	現在使用されていない例外。
Will Expire（期限）	期限の日付が指定されている例外
Expired（期限切れ）	期限の日付が過ぎたために非アクティブになっている例外
Never Expires（無期限）	永久的にアクティブであるように設定されている例外
Global（グローバル）	すべてのロールのすべてのクライアントに適用される例外
All Clients in a Role（ロール内のすべてのクライアント）	特定の指定済み管理者ロールのすべてのクライアント（優先管理者ロールを含む）に適用される例外。
Specific Clients（特定のクライアント）	1 つまたは複数の特定のクライアントに適用される例外

また、**[Search（検索）]** フィールドを使って、表示する例外を制限することもできます。

1. ドロップダウン リストを使って、どのテーブル列を検索するかを指定します。
2. 指定する文字列の全体または一部を入力します。
3. **[Search（検索）]** をクリックします。
4. 前のビューに戻るには、**[Clear Search Results（検索結果の消去）]** をクリックします。

新しい例外を作成するには、**[Add（追加）]** をクリックします。手順については、*例外の追加または編集*、133 ページを参照してください。

既存の例外を編集するには、例外の名前をクリックするか、1 つ以上の例外の隣のチェック ボックスをオンにし、**[Edit（編集）]** をクリックします。その方法については *例外の追加または編集*、133 ページまたは *複数の例外の同時編集*、137 ページを参照してください。

例外を削除するには、例外名の横のチェックボックスをオンにし、**[Delete（削除）]** をクリックします。

例外の編成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Policy Management] > [Exceptions] ページに例外が表示される編成は、管理者のロールによって異なります。

優先管理者の場合、例外は以下のようにグループ化されます。

1. グローバル例外（すべてのロールのすべてのクライアントに影響を及ぼす）
2. 優先管理者ロールの [Clients（クライアント）] ページの特定のクライアントに影響を及ぼす例外
3. 明示的にロールに割り当てられていない（どの [Clients] ページや [Managed Clients（処理対象クライアント）] リストにも表示されない）1 つ以上のコンピュータを含む例外
4. 優先管理者ロールの全体に適用される例外
5. 別の指定済み管理者ロールの特定のクライアントに適用される例外
6. 指定済み管理者ロールの全体に適用される例外

他のロールの指定済み管理者の場合、例外は以下のようにグループ化されます。

1. ロール内の特定のクライアントに影響を及ぼす例外
2. ロール全体に影響を及ぼす例外（[グローバル] 例外を含む）

各グループの中では、例外はアルファベット順に表示されます。

例外の追加または編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Policy Management] > [Exceptions] > [Add Exception] または **[Edit Exception]** ページを使って、特定のクライアントの特定のウェブサイトをブロックまたは許可する標準ポリシーの適用を無効化する例外を作成または更新します。

1. この例外の固有の、記述的な**名前**を入力します。名前は 1 ～ 50 文字でなければならず、また、以下の文字を含むことはできません。

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

2. **[URLs]** フィールドで、例外によって許可またはブロックする URL または IP アドレスをリストします。
   - URL を **domain.com** の形式で入力した場合、ドメインとそのサブドメイン（*www.domain.com*, *subdomain.domain.com*）の両方が照合されます。
   - URL を **www.domain.com** の形式で入力した場合、
     - http://www.domain.com は照合されます
     - http://domain.com は照合されません
     - http://subdomain.domain.com は照合されません

   1 行に 1 件、URL または IP アドレスを入力してください。
3. どの**クライアント**がこの例外の影響を受けます。

   優先管理者は、下記の例外を作成できます。
   - すべてのロールのすべてのクライアントに適用される **[グローバル]** 例外

     このオプションを選択する場合、**指定済み管理者がこの例外を無効化する例外を作成することを許可する**かどうかを指定します（*例外の無効化、136 ページ*を参照）。
   - **ロール内のすべてのクライアント**に適用される例外

     このオプションを選択した後、ドロップダウンリストから 1 つのロールを選択します。
   - **ロール内の特定のクライアント**に適用される例外

     このオプションを選択した後、2 つのリストが表示されます。左側のリストは、指定済み管理者ロールの処理対象クライアントに追加されている、またはいずれかのロールの [Clients] ページに追加されている、もしくは 1 つの例外に追加されている**定義済みの**すべてのクライアントを表示します。右側のリストは、この例外の適用対象として**選択されている**クライアントを表示します。

     各リストの上の検索ボックスは、追加または削除するクライアントをすばやく見つけるのに役立ちます

左側のリストに表示されていないクライアントを例外に追加するには、**[Add Other Clients（他のクライアントを追加）]** をクリックし、次に、ユーザー、グループ、コンピュータ（IPv4 または v6 アドレス）、またはネットワーク（IPv4 または v6 アドレス範囲）クライアントを追加します。

重要

複数のロールに属している特定のクライアントを選択した場合、例外が作成された時に、それは自動的に分割され、影響を受ける各ロールについて新しい例外が作成されます。

たとえば、[優先管理者]、[HR]、および [Facilities] ロールのクライアントに適用する [Permit Craigslist] という例外を定義した場合、[OK] をクリックしたときに 3 つの例外が作成されます。

- [HR] および [Facilities] ロールに対する例外はアイコンが付けられます。例外の影響を受けるロールを確認するには、アイコンの上にマウスを移動します。
- [優先管理者] ロールに対する例外には注釈は付けられません。

- 指定済み管理者が作成する例外は、**[All managed clients in this role（このロールのすべての処理対象クライアント）]** または **[Specific clients in this role（このロールの特定のクライアント）]** に適用できます。

  後者のオプションを選択した場合、2 つのリストが表示されます。左側のリストは、[Managed Clients（処理対象クライアント）] リストおよび [Clients（クライアント）] ページで**定義されている**すべてのクライアントを表示します。右側のリストは、この例外の適用対象として**選択されている**クライアントを表示します。

  - 各リストの上の検索ボックスは、追加するクライアントをすばやく見つけるのに役立ちます
  - クライアントが**定義されているクライアント**リストに表示されていない場合、そのクライアントはロールの処理対象クライアントとして定義されているグループ、OU、またはネットワーク（IP アドレス範囲）のメンバーであると考えられます。そのようなクライアントを追加するには、**[Add Other Clients]** をクリックし、次に、追加するユーザー、グループ、または IPv4 もしくは v6 アドレスを指定します。

4. 例外の **[Type]** を指定します。これは、指定したクライアントに対してリストされている URL を**ブロックする**か**許可する**かを決定します。

5. **[Expires]** で、例外がいつ期限切れになるかを指定します。
   - **[Never（期限なし）]** を選択した場合、例外は削除されるまで、または期限の日付が追加されるまで適用されます。
   - **[After（期限の日付）]** を選択した場合、mm/dd/yyyy 形式で日付を入力するか、カレンダー アイコンをクリックして日付を選択します。期限切れになる時刻は、選択した日の午前 0 時（Filtering Service を実行しているコンピュータ上で設定されている時刻）です。
6. 例外の **[State（状態）]** を指定します。デフォルトでは、例外は **[Active（アクティブ）]** になり、変更をキャッシュし、保存した後、即時適用されます。現時点で例外を使用しない場合、このチェックボックスをオフにします。
7. デフォルトでは、URL が [Security Risk（セキュリティ リスト）] カテゴリ（[悪質な Web サイト]、[スパイウェア] など）に関連付けられている場合、これらのサイトを許可する例外はすべての無視され、URL はアクティブなポリシーを基にフィルタリングされます（*[セキュリティ リスク] カテゴリを優先、331 ページ*を参照）。
   - カテゴリ フィルタがカテゴリをブロックする場合、要求はブロックされます。
   - カテゴリ フィルタがカテゴリを許可する場合、要求は許可されます。
   - 制限つきアクセス フィルタを使用している場合、要求はブロックされます。

   このセキュリティ機能を無効にするには、**[Advanced（詳細）]** をクリックし、次に、**[Block URLs that become a security risk, even if they are permitted by exception（例外によって許可されている場合でも、セキュリティ リスクとなる URL をブロックする）]** チェックボックスをオフにします。

   これの変更は推奨されません。
8. 例外によって許可またはブロックされる URL を定義するために正規表現を使用するには、**[Advanced]** をクリックし、次に **[Regular expressions（正規表現）]** ボックスに正規表現を 1 行に 1 つ入力します。

   作成した正規表現を検証するには、**[Test Regular Expression（正規表現のテスト）]** をクリックします。

   > **警告**
   > 使用する正規表現の数が多すぎたり、正規表現が複雑または過度に一般的である場合、処理速度が大幅に低下することがあります。

9. 変更が終わったら、**[OK]** をクリックして変更をキャッシュし、[Exceptions] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

例外の無効化

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *例外の追加または編集、133 ページ*
- *複数の例外を適用できる場合の優先順、137 ページ*

デフォルトでは、優先管理者が例外を作成したとき、その例外は指定済み管理者が作成するどの例外よりも優先されます。

例：

- 優先管理者のグローバル例外が **mysite.com** をブロックし、一部の処理対象クライアントに対する指定済み管理者の例外が **mysite.com** を許可する場合。

  デフォルトで、その URL はブロックされます。
- 優先管理者のグローバル例外が **anothersite.com** を許可し、指定済み管理者の例外が同じサイトをブロックする場合。

  デフォルトで、その URL は許可されます。

しかし、優先管理者は、例外を作成するときに、**[Allow delegated administrators to create exceptions that override this exception（指定済み管理者がこの例外を無効化する例外を作成することを許可する）]** オプションを指定できます。このオプションが選択されている場合は、指定済み管理者の例外が優先管理者の例外よりも優先されます。

例：

- 優先管理者のグローバル例外が **samplesite.com** を許可し、指定済み管理者の例外が指定済み管理者ロールに対して **samplesite.com** をブロックする場合。

  指定済み管理者ロールに対してこの URL はブロックされます。
- 優先管理者のグローバル例外が **example.com** をブロックし、指定済み管理者の例外が処理対象クライアントに対して **example.com** を許可する場合。

  指定した処理対象クライアントに対してこの URL が許可されます。

無効化できる優先管理者の例外は、[Policy Management] > [Exceptions] ページの [Clients] 列にアイコン（  ）が表示されます。

複数の例外を適用できる場合の優先順

Web Security Help | Web Security ソリューション | バージョン 7.8.x

デフォルトでは、優先管理者の例外が、指定済み管理者によって作成された例外に優先します。したがって、優先管理者の例外が URL をブロックし、指定済み管理者の例外がその URL を許可する場合、その要求は**ブロック**されます。

しかし、優先管理者の例外で指定済み管理者による無効化が許可されている場合（*例外の無効化、136 ページ*を参照）、指定済み管理者の例外が優先されます。したがって、優先管理者の例外が URL をブロックし、指定済み管理者の例外がその URL を許可する場合、その要求は**許可**されます。

1 つの要求に対して同じ優先度の複数の例外を適用できる場合（例、優先管理者の複数の例外に同じ URL が含まれる）

- Filtering Service は [ブロック] する例外を先にチェックします。したがって、[ブロック] する例外と [許可] する例外がある場合、要求は**ブロック**されます。
- 複数の[ブロック]する例外がある場合、最初に見つかったものが適用されます。
- [ブロック]する例外がなく場合、複数の[許可]する例外がある場合、最初の [許可] する例外が適用されます。

例外を作成した後、Test Filtering ツール（*フィルタリングのテスト、357 ページ*を参照）を使用して、クライアント要求が期待している通りにフィルタリングされていることを確認します。

複数の例外の同時編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Policy Management] > [Exceptions] > [Edit Exceptions] ページを使用して、複数の例外を同時に編集します。

複数の例外を編集するとき、編集できるのは例外のタイプ（[許可] または [ブロック]）、期限の設定（[期限なし] または期限の日付）、状態（[アクティブ] または [非アクティブ]）、セキュリティの無効化の設定（Websense ソフトウェアがセキュリティ リスクを検出した時に、[許可] 対象の例外の中の URL を許可するかブロックするか）だけです。

編集する例外の詳細を表示するには、ページ上部の **[View details of each selected exception（選択した各例外の詳細を表示する）]** リンクをクリックします。

1. 例外の **[Type]** を指定します（[Block] または [Permit]）。変更を行うには、**[Change]** をクリックし、次に新しい選択を行います。
2. 例外の **[Expires]** 設定を更新するには、**[Change]** をクリックし、次に、
   - **[Never（期限なし）]** を選択した場合、例外は削除されるまで、または期限の日付が追加されるまで適用されます。
   - **[After（期限の日付）]** を選択した場合、mm/dd/yyyy 形式で日付を入力するか、カレンダー アイコンをクリックして日付を選択します。
3. 例外の **[State]** を更新するには、**[Change]** をクリックし、次に、**[Active]** チェック ボックスをオンまたはオフにします。非アクティブの例外は使用されません。
4. デフォルトでは、Websense Web Security が URL にセキュリティ リスクがある（[悪質なソフトウェア]、[スパイウェア] など）と判断した場合に、その URL は例外によって許可されている場合でもブロックされます。

   許可されている例外の現在のセキュリティ設定を更新するには、**[Advanced]** をクリックし、次に **[Change]** をクリックします。**[Block URLs that become a security risk, even if they are permitted by exception（例外によって許可されている場合でも、セキュリティ リスクとなる URL をブロックする）]** チェックボックスをオンまたはオフにします。

   デフォルトのセキュリティ無効化保護を無効化することは推奨されません。
5. 変更が終わったら、**[OK]** をクリックして変更をキャッシュし、[Exceptions] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

例外のショートカット

Web Security Help | Web Security ソリューション | バージョン 7.8.x

以下のショートカットを使って、頻繁に実行するタスクを実行する最速の方法を見つけてください。

優先管理者の場合

- *1 つの URL を全員に対してブロックまたは許可する方法、139 ページ*
- *1 つの URL を 1 人のユーザーに対してブロックまたは許可する方法、139 ページ*

指定済み管理者の場合

- *自分のロール全体に対して URL をブロックまたは許可する方法*、140 ページ
- *1 つの URL を 1 つの処理対象クライアントに対してブロックまたは許可する方法*、141 ページ

すべての管理者

- *フィルタリングされない URL を作成する方法*、142 ページ

1 つの URL を全員に対してブロックまたは許可する方法

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Super Administrators は以下の手順により特定の URL をネットワーク内の全員に許可することができます。

1. **[Policy Management] > [Exceptions（例外]** ページに移動し、**[Add]** をクリックします。
2. この例外の固有の **[Name（名前）]** を入力します。
3. 許可しようとする **URL** を入力します。
4. デフォルトにより、この例外はすべてのクライアントに適用されるように設定されています（**[Global（グローバル）]** が選択されています）。
5. デフォルトにより、この例外は当該 URL を **[Block（ブロック）]** するように設定されています。これを変更するには、**[Type（タイプ）]** を **[Permit（許可）]** にします。
6. 有効期限を設定します（該当する場合）。
7. **[OK]** をクリックして変更をキャッシュし、**[Save and Deploy]** をクリックしてそれらの変更を適用します。

1 つの URL を 1 人のユーザーに対してブロックまたは許可する方法

Web Security Help | Web Security ソリューション | バージョン 7.8.x

優先管理者はは以下の手順により特定の URL をネットワーク内の 1 人のユーザーに対して、クライアントのロールに関わりなく、ブロックまたは許可することができます。

1. **[Policy Management] > [Exceptions（例外]** ページに移動し、**[Add]** をクリックします。
2. この例外の固有の **[Name（名前）]** を入力します。
3. 許可しようとする **URL** を入力します。

4. この例外の影響を受けるクライアントを指定するには、**[Specific clients in any role（任意のロールの特定のクライアント）]** を選択します。
5. **[Defined clients（定義されているクライアント）]** リストの上の検索ボックスにユーザー名または IP アドレスの全部または一部を入力し、**[Enter]** を押します。
   - 検索結果にそのクライアントが表示された場合、そのクライアントを選択し、右矢印（>）ボタンをクリックして、そのクライアントを **[Selected]** リストに入れます。
   - 検索結果にそのクライアントが表示されない場合、**[Add Other Clients]** をクリックし、
     - リストからユーザーまたはグループ名を選択するか、または **[Search]** をクリックして、ユーザー ディレクトリの中のユーザーまたはグループを検索します。
     - IP アドレスまたは範囲を IPv4 または IPv6 形式で入力します。

     追加するクライアントの指定が完了したら、適当な右矢印（>）ボタンをクリックしてクライアントを [Selected] リストに追加し、**[OK]** をクリックします。
6. デフォルトにより、この例外は当該 URL を **[Block（ブロック）]** するように設定されています。これを変更するには、**[Type（タイプ）]** を **[Permit（許可）]** にします。
7. 有効期限を設定します（該当する場合）。
8. **[OK]** をクリックして変更をキャッシュし、**[Save and Deploy]** をクリックしてそれらの変更を適用します。

自分のロール全体に対して URL をブロックまたは許可する方法

Web Security Help | Web Security ソリューション | バージョン 7.8.x

指定済み管理者は以下の手順により特定の URL を、管理下のロールのすべての処理対象クライアントに対してブロックまたは許可することができます。

重要

優先管理者によって作成された例外が、指定済み管理者によって作成された例外に優先することがあります。

作成した例外が処理対象クライアントに適用されていないと思われる場合、**Test Filtering** ツールを使用して、別の例外がその例外を無効化していないか調べます（*フィルタリングのテスト、357 ページ*を参照）。

1. **[Policy Management] > [Exceptions（例外]** ページに移動し、**[Add]** をクリックします。
2. この例外の固有の **[Name（名前）]** を入力します。
3. 許可しようとする **URL** を入力します。
4. デフォルトでは、例外は**このロールのすべての処理対象クライアント**に適用されるように設定されています。
5. デフォルトにより、この例外は当該 URL を **[Block（ブロック）]** するように設定されています。これを変更するには、**[Type（タイプ）]** を **[Permit（許可）]** にします。
6. 有効期限を設定します（該当する場合）。
7. **[OK]** をクリックして変更をキャッシュし、**[Save and Deploy]** をクリックしてそれらの変更を適用します。

1 つの URL を 1 つの処理対象クライアントに対してブロックまたは許可する方法

Web Security Help | Web Security ソリューション | バージョン 7.8.x

指定済み管理者は以下の手順により特定の URL を処理対象クライアントの 1 つに対してブロックまたは許可することができます。

> **重要**
> 優先管理者によって作成された例外が、指定済み管理者によって作成された例外に優先することがあります。
>
> 作成した例外が処理対象クライアントに適用されていないと思われる場合、**Test Filtering** ツールを使用して、別の例外がその例外を無効化していないか調べます（*フィルタリングのテスト、357 ページ*を参照）。

1. **[Policy Management] > [Exceptions（例外]** ページに移動し、**[Add]** をクリックします。
2. この例外の固有の **[Name（名前）]** を入力します。
3. 許可しようとする **URL** を入力します。
4. この例外の影響を受けるクライアントを指定するには、**[Specific clients in any role（任意のロールの特定のクライアント）]** を選択します。

5. **[Defined clients（定義されているクライアント）]** リストの上の検索ボックスにユーザー名または IP アドレスの全部または一部を入力し、**[Enter]** を押します。
   - 検索結果にそのクライアントが表示された場合、そのクライアントを選択し、右矢印（>）ボタンをクリックして、そのクライアントを **[Selected]** リストに入れます。
   - クライアントがロールの中で処理対象クライアントとして定義されているグループ、OU、またはネットワーク（IP アドレス範囲）のメンバーであるが、[Managed Clients] リストまたは [Clients] ページに表示されない場合、そのクライアントは検索結果には表示されません。

     この場合、例外の作成をキャンセルし、クライアントを [Clients] ページへ追加してから例外を作成します。それによってこのクライアントは [Add Exceptions] ページの検索結果に表示されるようになります。
6. デフォルトにより、この例外は当該 URL を **[Block（ブロック）]** するように設定されています。これを変更するには、**[Type（タイプ）]** を **[Permit（許可）]** にします。
7. 有効期限を設定します（該当する場合）。
8. **[OK]** をクリックして変更をキャッシュし、**[Save and Deploy]** をクリックしてそれらの変更を適用します。

フィルタリングされない URL を作成する方法

Web Security Help | Web Security ソリューション | バージョン 7.8.x

バージョン 7.6 またはそれ以前のバージョンからアップグレードしたとき、既存のフィルタリングされない URL は [許可] されている例外に変更されます。フィルタリングされない URL は、どの管理者によって作成されたかによって、次のように変更されます。

- 優先管理者によって作成された場合は、その URL または正規表現をすべてのロールのすべてのクライアントに対して許可するグローバル例外になります。
- 指定済み管理者によって作成された場合は、その URL または正規表現を 1 つのロールのすべてのクライアントに対して許可するロール規模の許可する例外になります。

全員に対して（優先管理者のみ）、または管理しているロールの全員に対して特定の URL を許可する方法については、下記を参照してください。

- *1 つの URL を全員に対してブロックまたは許可する方法*、139 ページ
- *自分のロール全体に対して URL をブロックまたは許可する方法*、140 ページ

7 ブロック ページ

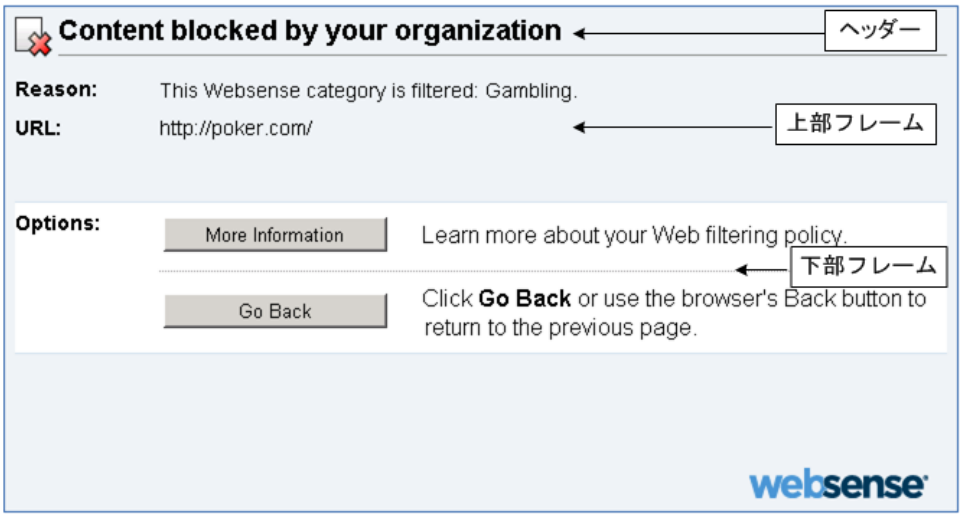
Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *グラフィック広告のブロック、145 ページ*
- *埋め込まれているページのブロック、146 ページ*
- *ブロック ページの使用、147 ページ*
- *代替ブロック メッセージの作成、154 ページ*
- *代替ブロック メッセージを他のコンピュータで使用、155 ページ*
- *要求がブロックされた理由の判別、156 ページ*

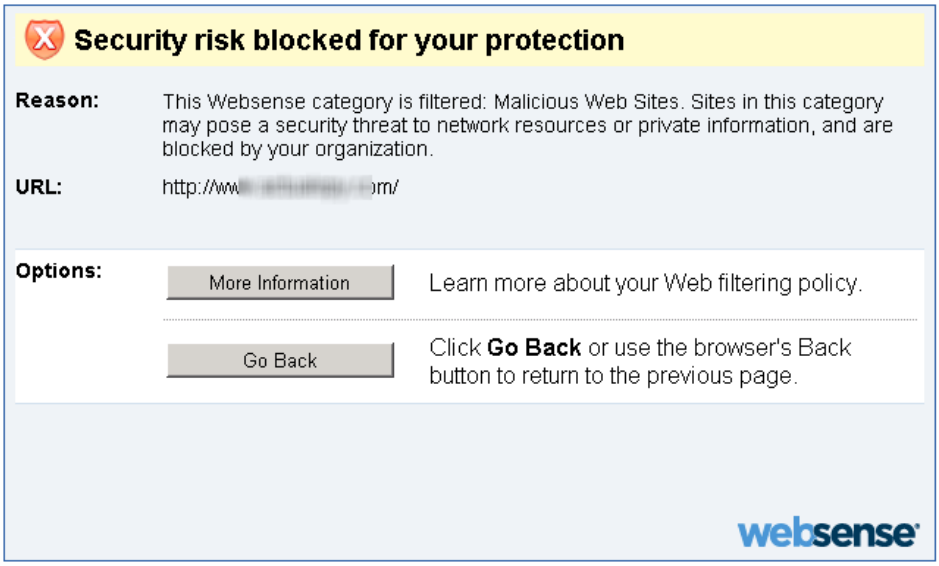
Websense Web Security がウェブサイトをブロックした時、クライアントのブラウザでブロック ページを表示します。

ブロック ページは HTML ファイルから成り、デフォルトでは 3 つの主要なセクションによって構成されます。



- **ヘッダー**は、サイトがブロックされていることを示します。
- **上側のフレーム**には、要求された URL と URL がブロックされた理由を示すブロック メッセージが含まれます。
- **下側のフレーム**には、ユーザーが利用できるオプションが示されます。たとえば、前のページに戻ったり、[Continue（継続）] または [Use Quota Time（割り当て時間の使用）] ボタンを使ってサイトを表示するオプションがあります。

サイトが [セキュリティ リスク] クラスのカテゴリに属しているためブロックされた場合（*リスク クラス*、64 ページを参照）、セキュリティ ブロック ページが表示されます。



Websense Web Security Gateway および Gateway Anywhere 環境では、優先管理者は ACEInsight へのリンクを含むブロック ページの拡張バージョンを有効化できます。

- [Settings（設定）] > [General（一般）] > [Filtering（フィルタリング）] ページのリンクを有効化します。
- ユーザーはこのリンクをクリックして、セキュリティ上の理由によってブロックされている URL に関する詳細情報を見つけることができます。

Websense ソフトウェアにはデフォルトのブロック ページ ファイルが含まれています。これらのデフォルトを使用するか、自分のカスタム バージョンを作成することができます。

注意

Websense Web Security Gateway Anywhere 環境では、オンプレマイズ ブロック ページへの変更はハイブリッド ブロック ページには影響を及ぼしません。*ハイブリッド ブロック ページのカスタマイズ*、276 ページを参照してください。

- デフォルト ファイルをカスタマイズして、ブロック メッセージを変更します（*ブロック ページの使用*、147 ページを参照）。
- Websense ソフトウェアがリモート ウェブ サーバー上にホストされているブロック メッセージ（デフォルトまたはカスタム）を使用するように設定します（*代替ブロック メッセージを他のコンピュータで使用*、155 ページを参照）。

グラフィック広告のブロック

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense ソフトウェアが標準またはセキュリティ ブロック ページの代わりに、非常に小さい、空白のイメージ ファイル（BlockImage.gif）を表示する場合があります。これは次のような時に起こります。

- [広告宣伝] カテゴリがブロックされている
- サイトが [広告宣伝] カテゴリの URL をホストしている画像（GIF ファイル、JPG ファイル）を表示しようとしている。

広告宣伝は多くの場合、広告宣伝以外の情報も表示するページのフレームまたは iframes の中に表示されます。この場合、グラフィカルな広告宣伝はページ上では一般的に、白（空白）のボックスとして表示されます。サイトの残りのコンテンツは通常通りに表示されます。

サイト全体が広告宣伝イメージから成っている場合もあります。この場合、ユーザーのブラウザには標準ブロック メッセージの代わりに空白のウェブ ページが表示されます。ユーザーには、下記のような URL のためにサイトがブロックされていることがわかります。

```
http://<Filtering Service IP address> :15871/cgi-bin/
blockpage.cgi?ws-session=<session number>
```

デフォルトの 1 ピクセルのブロック イメージ以外のイメージを表示したい場合は、単にデフォルト ファイルを置換します。

1. Filtering Service を実行しているコンピュータ上でブロック ページ ディレクトリ（デフォルトでは C:\Program Files または Program Files（x86）\Websense\Web Security\BlockPages\Images or /opt/Websense/BlockPages/Images）に移動します。
2. 元の **blockImage.gif** ファイルのバックアップのコピーを作成します。
3. イメージに **blockImage.gif** という名前をつけ、それを Images ディレクトリへコピーします（元のファイルを上書きします）。

埋め込まれているページのブロック

Web Security Help | Web Security ソリューション | バージョン 7.8.x

大部分の ウェブページは複数のソース（ad サーバー、ストリーミング ビデオ サイト、ソーシャル ネットワーキング アプリケーション、イメージ ホスティング サービスなど）からのコンテンツを含んでいます。一部のサイトはコンテンツを集積し、複数のサイトからのコンテンツを 1 つのプレゼンテーションにまとめています。

このような場合、ユーザーが許可されているコンテンツとブロックされているコンテンツが混ざっているサイトを要求する可能性があります。

ページの中のフレームまたは iframe にブロックされているコンテンツが含まれる場合、Websense ソフトウェアはそのフレームの中に標準またはセキュリティ ブロック ページを表示します。しかし、フレームが小さい場合は、エンド ユーザーにはページのごく小さな部分だけが表示され（ブロック アイコンの一部しか表示されない場合もあります）、コンテンツがブロックされている理由がわからない場合があります。

この問題に対処するために、ユーザーがブロック ページの表示されている部分の上にマウスを置くと、ツールチップ形式のポップアップに簡単なブロック メッセージが表示されます。そのメッセージをクリックすると、ブロック ページの全体が別のウィンドウに表示されます。

元のページの許可されているコンテンツの閲覧に戻るには、ユーザーはブロック ページを表示しているウィンドウを閉じなければなりません。ブラウザの制約のため、フレーム内から開いたブロック ページの [Back] ボタンをクリックしても無効です。

ブロック ページが新しいウィンドウに表示されている時、[Use Quota Time] または [Continue] オプションが表示されます。それぞれのボタンをクリックすると、次のようになります。

1. 新しい（ポップアップ）ウィンドウを閉じます。
2. 元のブラウザ ウィンドウに、前にブロックされていたコンテンツ（だけ）が表示されます。

元のページを、前にブロックされていたコンテンツを含めて表示するには、以下のいずれかを実行します。

- サイトの URL を再入力します。
- ブラウザの [Back] ボタンを使ってサイトに戻り、ページをリフレッシュします。

ブロック ページの使用

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ブロック メッセージのカスタマイズ、149 ページ*
- *代替ブロック メッセージの作成、154 ページ*
- *代替ブロック メッセージを他のコンピュータで使用、155 ページ*

Websense ブロック ページを作成するために使用したファイルは、下記のディレクトリに保存されます。

- Windows:

  ```
  C:\Program Files\Websense\Web Security\BlockPages\
  <language_code> \Default
  ```

  または

  ```
  C:\Program Files(x86)\Websense\Web Security\BlockPages\
  <language_code> \Default
  ```

- Linux:

  ```
  /opt/Websense/BlockPages/<language_code> /Default
  ```

注意

Websense Web Security Gateway Anywhere 環境では、これらのブロック ページはオンプレマイズ ソフトウェアによってフィルタリングされたユーザーにのみ適用されます。ハイブリッド サービスによって提供されたページをカスタマイズする方法については、*ハイブリッド ブロック ページのカスタマイズ、276 ページ*を参照してください。

ブロック ページを構成するために使用する 2 つのプライマリ HTML ファイルがあります。

- **master.html** はブロック ページの情報フレームを作成し、下記のいずれかのファイルを使ってボトム フレームに適切なオプションを表示します。

ファイル名	内容
blockFrame.html	ブロックされているカテゴリに含まれるサイトのテキストとボタン（[Go Back（戻る）] オプション）。
continueFrame.html	**[Confirm（確認）]** アクションが適用されるカテゴリに含まれるサイトのテキストとボタン。
quotaFrame.html	**[Quota（割り当て）]** アクションが適用されるカテゴリに含まれるサイトのテキストとボタン。
moreInfo.html	ユーザーがブロック・ページの **[More information（詳細情報）]** リンクをクリックしたときに表示されるページのコンテンツ。

- **block.html** はブロック メッセージのトップ フレームのテキストを含みます。このテキストは、アクセスが制限されていることを説明し、要求されたサイトをリストし、サイトが制限されている理由を示します。

このほかに、テキスト コンテンツ、スタイル、ブロック ページで使用するボタン機能を提供するためにいくつかの支援ファイルを使用します。

ファイル名	説明
blockStyle.css	ほとんどのブロック ページのスタイルが含まれているカスケード表示形式のスタイル シート
master.css	ブロック ページ ポップアップ（例、アカウント無効化ポップアップ）のスタイルが含まれているカスケード表示形式のスタイル シート
popup.html	埋め込まれているページがブロックされている時（*埋め込まれているページのブロック、146 ページ*を参照）、このファイルを使ってフルサイズのブロック ページ ポップアップが表示されます。
block.inl	ブロック ページのブロック フレームを作成するために使用するツールを提供します。
blockframe.inl	標準的なブロック ページの追加的情報を提供します。
continueframe.inl	ユーザーが [Continue（継続）] オプションを使用できる場合に、ブロック フレームの追加的情報を提供します。
quotaframe.inl	ユーザーが [Use Quota Time（割り当て時間を使用）] オプションを使用できる場合に、ブロック フレームの追加的情報を提供します。

ファイル名	説明
base64.js	ユーザーが [Account Override（アカウントの無効化）] オプションを使用できる場合に、資格情報暗号化をサポートするために使用する JavaScript ファイル。このファイルは変更または削除してはいけません。
master.js	標準的なブロック ページの作成に使用する JavaScript ファイル。
security.js	セキュリティ ブロック ページの作成に使用する JavaScript ファイル。
messagefile.txt	ブロック ページで使用するテキスト文字列を含みます。
WebsenseCopyright.txt	Websense ブロック ページの著作権情報
master.wml	基本的なブロック情報を含む WML ファイル

使用環境の中に Web DLP コンポーネントが含まれる場合、もう 1 つのファイル、**policyViolationDefaultPage.html** は、Websense Data Security コンポーネントがコンテンツの Web への送信または Web からのダウンロードをブロックするときのブロック ページ コンテンツを提供します。

ブロック メッセージのカスタマイズ

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *メッセージ フレームのサイズの変更*、151 ページ
- *ブロック ページに表示するロゴの変更*、151 ページ
- *ブロック ページ コンテンツ変数の使用*、152 ページ
- *デフォルト ブロック ページに戻る*、154 ページ

デフォルト ブロック ページ ファイルのコピーを作成し、次にそのコピーを使用して、ユーザーが受け取るブロック ページのトップ フレームをカスタマイズすることができます。

- 組織のロゴ、色、スタイルを使うようにブロック ページの外観を変更します。
- 組織のインターネット利用ポリシーについての情報を追加します。
- インターネット利用ポリシーについて管理者に問い合わせるための手段を提供する。

固有のカスタム ブロック ページを作成するには、以下の手順を実行します。

1. Websense ブロック ページ ディレクトリに移動します。英語：

   ```
   Websense/Web Security/BlockPages/en/Default
   ```

2. ブロック ページ ファイルをカスタム ブロック ページ ディレクトリにコピーします。英語：

   ```
   Websense/Web Security/BlockPages/en/Custom
   ```

   注意

   BlockPages\en\Default にあるオリジナルのブロック メッセージ ファイルを変更**しないでください**。それを **BlockPages/en/Custom** ディレクトリにコピーし、次に、コピーを変更します。

3. メモ帳や vi などのテキストエディタでこのファイルを開きます。

   警告

   プレーン テキスト エディタでブロック メッセージ ファイルを編集してください。HTML エディタによっては、HTML コードを変更してしまうものがあり、ファイルが壊れたりブロック・メッセージの表示に問題が生じたりします。

4. テキストを修正してください。このファイルには、変更の方法を指示するコメントが含まれています。

   トークン（$* と *$ のシンボルで囲まれている）または HTML コードの構造を変更**しないでください**。これらの部分は Websense ソフトウェアがブロック メッセージで特定の情報を表示できるようにしています。

5. 一部のブロック ページ HTML ファイルはページ作成のために使用するサポート ファイルを参照するために、ハード コード化されたパスを使用します。ブロック ページのフォーマットを指定するために使用するスタイルシート（**blockStyle.css**）またはセキュリティ ブロック ページを作成するために使用する JavaScript（**security.js**）を変更した場合、必ずカスタム HTML ファイルの中でもそれらのファイルへのパスを更新しておいてください。例：

   ```
   <link rel="stylesheet" href="/en/Custom/blockStyle.css
   type="text>
   ```

6. ファイルを保存します。

7. Websense Filtering Service を再起動します（*Websense サービスの停止と起動、477 ページ*を参照）。

メッセージ フレームのサイズの変更

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ブロック メッセージに表示する情報の内容によっては、ブロック メッセージのデフォルトの長さおよびトップ フレームの高さが適当でない場合があります。**master.html** ファイルでこれらのサイズ パラメータを変更するには、下記の手順を実行します。

1. **master.html** を **Websense/BlockPages/en/Default** ディレクトリから **Websense/BlockPages/en/Custom** ディレクトリへコピーします。
2. メモ帳や vi などのテキストエディタ（TML エディタではない）でこのファイルを開きます。
3. メッセージ フレームの幅を変更するには、下記の行を編集します。

   ```
   <div style="border:1px solid #285EA6;width:600px...">
   ```

   必要に応じて、**width** パラメータの値を変更します。
4. 追加的情報を表示するためにメッセージのトップ フレームをスクロールさせるには、下記の行を編集します。

   ```
   <iframe src="$*WS_BLOCKMESSAGE_PAGE*$*WS_SESSIONID*$" ...
      scrolling="no" style="width:100%; height:6em;">
   ```

   メッセージ テキストがフレームの高さを超えるときにスクロール バーを表示するようにするには、**scrolling** パメータの値を **auto** に変更します。

   また、**height** パラメータの値を変更して、フレームの高さを変えることもできます。
5. ファイルを保存して閉じます。
6. 変更を有効にするために、Filtering Service を再起動します（*Websense サービスの停止と起動*、477 ページを参照）。

ブロック ページに表示するロゴの変更

Web Security Help | Web Security ソリューション | バージョン 7.8.x

master.html ファイルは、ブロック ページ上に Websense ロゴを表示するために使用する HTML コードを含みます。代わりにユーザーの組織のロゴを表示するには、以下の手順を実行します。

1. ブロック ページ ファイルを **Websense/BlockPages/en/Default** ディレクトリから **Websense/BlockPages/en/Custom** ディレクトリへコピーします（まだコピーしていない場合）。
2. 組織のロゴを含んでいるイメージ ファイルを同じ場所にコピーします。

3. メモ帳や vi などのテキスト エディタ（HTML エディタでない）で **master.html** を開き、下記の行を編集して、Websense ロゴを組織のロゴに置換します。

   ```
   <img title="Websense" src="/en/Custom/wslogo_block_page.png"
   ...>
   ```

   - **wslogo_block_page.png** を組織のロゴを含んでいるイメージ ファイルの名前に置換します。
   - **title** パラメータの値を組織の名前を反映するように置換します。
4. ファイルを保存して、閉じます。
5. 変更を有効にするために、Filtering Service を再起動します（*Websense サービスの停止と起動*、477 ページを参照）。

ブロック ページ コンテンツ変数の使用

Web Security Help | Web Security ソリューション | バージョン 7.8.x

コンテンツ変数は HTML ブロック ページで表示する情報を制御します。次の変数はデフォルト ブロック メッセージ コードに含まれています。

変数名	表示されるコンテンツ
WS_DATE	現在の日付
WS_USERNAME	現在のユーザ名（ドメイン名は除く）
WS_USERDOMAIN	現在のユーザ用のドメイン名
WS_IPADDR	要求発信元コンピュータの IP アドレス
WS_WORKSTATION	ブロックされたコンピュータのコンピュータ名を表示（コンピュータ名がなければ、IP アドレスを表示）

変数を使用するには、適切な HTML タグの $* と *$ の間に変数名を入力します：

```
<p id="UserName"> $*WS_USERNAME*$</p>
```

ここで、*WS_USERNAME* は変数です。

このブロック メッセージ コードには、ほかにも下記のような変数があります。固有のカスタム ブロック メッセージを作成する際に、これらの変数を利用できます。しかし、Websense 定義のブロック メッセージ ファイルにこれらの変数が含まれる場合、それを変更しては**いけません**。Filtering Service はブロックされた要求を処理する時にこれらの変数を使用しますから、これらの変数はそのままにしておく必要があります。

変数名	目的
WS_URL	要求された URL の表示
WS_BLOCKREASON	サイトがブロックされた理由を表示（適用された処置）
WS_ISSECURITY	要求されたサイトが [セキュリティ リスク] クラスのいずれかのカテゴリに属しているかどうかを示します。[TRUE] である場合、セキュリティ ブロック ページが表示されます。
WS_PWOVERRIDECGIDATA	ブロック ページ HTML コードの入力フィールドに **[Password Override]** ボタンの使用に関する情報を入力する。
WS_QUOTA_CGIDATA	ブロック ページ HTML コードの入力フィールドに **[Use Quota Time]** ボタンの使用に関する情報を入力する。
WS_PASSWORDOVERRIDE-BEGIN, WS_PASSWORDOVERRIDE-END	パスワード無効化機能に関係します。
WS_MOREINFO	要求されたサイトがブロックされた理由について詳細を表示する（**[More information]** リンクをクリックすると表示される）。
WS_POLICYINFO	どのポリシーが要求元のクライアントに指定されているかを表示する。
WS_MOREINFOCGIDATA	Filtering Service に **[More information]** リンクの使い方に関するデータを送る。
WS_QUOTATIME	要求元クライアントに残されている割り当て時間数を表示する。
WS_QUOTAINTERVALTIME	要求元クライアントに設定された割り当てセッションの長さを表示する。
WS_QUOTABUTTONSTATE	特定の要求に対して **[Use Quota Time]** ボタンが有効化または無効化されているかどうかを指定する。
WS_SESSIONID	要求に関連する内部識別子として動作する。
WS_TOPFRAMESIZE	設定されていれば、カスタム ブロック サーバーにより送信されたブロック ページのトップ部分のサイズ（%）を指定する。
WS_BLOCKMESSAGE_PAGE	ブロック ページのトップフレームに使用するソースを指定する。
WS_CATEGORY	ブロックされた URL のカテゴリを表示する。
WS_CATEGORYID	要求された URL のカテゴリの一意な識別子

デフォルト ブロック ページに戻る

Web Security Help | Web Security ソリューション | バージョン 7.8.x

カスタマイズしたブロック メッセージを組み込んだ後にユーザーがエラーを受け取った場合は、以下の手順に従ってデフォルトのブロック メッセージを復元できます。

1. **Websense/BlockPages/en/Custom** ディレクトリのすべてのファイルを削除します。デフォルトでは、Websense ソフトウェアは元通り Default ディレクトリのファイルを使用するようになります。
2. Filtering Service を再起動します（*Websense サービスの停止と起動*、477 ページを参照）。

代替ブロック メッセージの作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ブロック ページの使用*、147 ページ
- *ブロック メッセージのカスタマイズ*、149 ページ

また、独自の HTML ファイルを作成し、ブロック・ページのトップ フレームに表示するテキストを指定することができます。既存の HTML ファイルを使用する、代替ファイルを最初から作成する、または **block.html** のコピーを作成してテンプレートとして使用することができます。

- 下記の 3 つのプロトコルのそれぞれに対して異なるブロック メッセージを作成します。HTTP、FTP、および Gopher。
- ファイルを Websense コンピュータ上、または内部の Web サーバー上にホストします（*代替ブロック メッセージを他のコンピュータで使用*、155 ページを参照）。

代替ブロック メッセージ ファイルを作成した後、Websense ソフトウェアが新しいメッセージを表示するように設定しなければなりません（*フィルタリング設定値の設定*、81 ページを参照）。このプロセスで、それぞれの設定可能なプロトコルに対してどのメッセージを使用するかを指定できます。

代替ブロック メッセージを他のコンピュータで使用

関連項目：

- *ブロック ページの使用*、147 ページ
- *ブロック メッセージのカスタマイズ*、149 ページ
- *代替ブロック メッセージの作成*、154 ページ

Websense ブロック ページを使用し、トップ フレーム内のメッセージだけをカスタマイズする代わりに、独自の HTML ブロック ページを作成して、それを内部 Web サーバー上でホストすることもできます。

注意

ブロック メッセージを外部 Web サーバー上に保存することもできます。しかし、そのサーバーがマスター データベースにリストされているサイトをホストしていて、そのサイトがブロックされているカテゴリに含まれる場合、ブロック ページ自体がブロックされます。

一部の組織では、Websense サーバー コンピュータの ID を隠すために、代替のリモート ブロック ページを使用します。

リモート ブロック ページには任意の HTML ファイルを使用できます。デフォルトの Websense ブロック ページの形式に従う必要はありません。しかし、この方法でブロック ページを作成した場合、Websense 定義のブロック ページ（デフォルトまたはカスタム）で利用できる [Continue]、[Use Quota Time]、および [Password Override] 機能を利用できません。

ファイルの準備が完了したら、**eimserver.ini** ファイルを編集して、新しいブロック ページをポイントするようにします。

1. Websense Filtering Service を停止し、次に Policy Server サービスを停止します（*Websense サービスの停止と起動*、477 ページを参照）。
2. Filtering Service を実行しているコンピュータ上で Websense **bin** ディレクトリ（デフォルトでは C:\Program Files または Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）に移動します。
3. **eimserver.ini** ファイルのバックアップのコピーを作成し、それを別のディレクトリに保存します。

4. テキスト エディタで **eimserver.ini** ファイルを開き、**[WebsenseServer]** のセクションを見つけます（ファイルの上部）。
5. ブロック ページをホストしているサーバーのホスト名または IP アドレスを、下記の形式で入力します。

   ```
   UserDefinedBlockPage=http://<hostname or IP address>
   ```

   URL のプロトコル部分（http://）は必須です。
6. ファイルを保存してテキスト エディタを閉じます。
7. Websense Policy Server を停止し、次に Filtering Service サービスを停止します。

サービスが開始したとき、ユーザーは代替コンピュータ上でホストされているブロック ページを受け取ります。

要求がブロックされた理由の判別

Web Security Help | Web Security ソリューション | バージョン 7.8.x

要求がブロックされた理由を調べたい場合、ブロック ページのソース コードの情報を活用できます。

- ブロック ページが Filtering Service によって送信された場合（アプライアンスまたはオンプラマイズ ソフトウェアによってフィルタリングされているユーザー）、**[More information（詳細）]** をクリックします。次に、メッセージ テキストのどこかを右クリックして、**[View Source（ソースを表示）]** を選択します。*Filtering Service によってブロックされた要求*、157 ページを参照してください。

  > **注意**
  > Internet Explorer 10 では、[View Source（ソースを表示）] オプションが表示されない場合があります。[View Source（ソースを表示）] オプションが表示されない場合、**[Page Tools（ページ ツール）]** をクリックし、**[View on the desktop（デスクトップに表示）]** を選択します。

- ブロック ページがハイブリッド サービスによって送信された場合（Websense Web Security Gateway Anywhere 環境）、ブロック メッセージのどこかを右クリックして、**[View Source]** を選択します。*ハイブリッド サービスによってブロックされた要求*、158 ページを参照してください。

Filtering Service によってブロックされた要求

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ブロック ページの詳細情報の HTML ソースは、サイトを要求したユーザー、および要求をフィルタするために使用した基準についての情報を示します。具体的には、以下の情報を示します。

- 要求のユーザー名およびソース IP アドレス（入手可能な場合）と要求が発行された時刻（HH:MM 形式）。
- 要求にどのポリシーが適用されているか、およびそのポリシーが割り当てられている対象がユーザー、グループ、ドメイン、コンピューター（個別の IP アドレス）、ネットワーク（IP アドレスの範囲）のいずれであるか。

  2 つ以上のグループ ポリシーが適用可能である場合、このメッセージはまた、**[Use more restrictive blocking（より厳格な制限でブロックをする）]** 設定が使用されているかどうかを示します。*フィルタリング設定値の設定、81 ページ*を参照してください。
- ポリシーのどの要素によって、要求がブロックされたか（例、カテゴリ フィルタまたは制限付きアクセス フィルタ、ファイル タイプ、キーワード、帯域幅の使用）。
- ポリシーが割り当てられたロールの名前。
- サイトの分類に使用したリソース（Websense Master Database、リアルタイム データベース更新、リアルタイム データベース更新に含まれる正規表現、カスタム URL、キーワード、Websense Web Security Gateway スキャニングなど）。

例：

ユーザー名：`WinNT://Test/tester1 Source IP Address:10.12.132.17 Current Time:15:30`

このネットワーク（`10.12.132.0 ～ 10.12.132.255`）は、ポリシー `[role-8**Default]` によってフィルタリングされます。ポリシーには現時点でのカテゴリまたは制限付きアクセス フィルタが含まれます。

このクライアントは下記のロールに関連付けられます：優先管理者。

要求は、マスタ データベースによって分類されました。

ここで、要求はユーザーのコンピュータが配置されているネットワーク（IP アドレス範囲）に適用されるポリシー（Default）によってフィルタリングされます。ポリシー割り当ては優先管理者ロールで実行され、要求されたサイトは Master データベースによって分類されました。

ハイブリッド サービスによってブロックされた要求

ハイブリッド サービスによって送信されたブロック ページの HTML ソースは、要求されたサイトの分類方法や、要求にポリシーを割り当てる方法に関する情報を示します。具体的には、以下の情報を示します。

- ポリシーが割り当てられたロールの名前。*代理管理ロール*、406 ページを参照してください。
- サイトに割り当てられているカテゴリ。
- 要求に割り当てられているポリシー（1 つまたは複数）。
- ファイル タイプ ブロッキングを使用した場合、適用したファイル タイプ。
- 要求の作成に使用したプロトコル（HTTP、HTTPS、または FTP over HTTP）。
- サイトの分類に使用したリソース（Websense Master Database、リアルタイム データベース更新、リアルタイム データベース更新に含まれる正規表現、カスタム URL、キーワード、Websense Web Security Gateway スキャニングなど）。
- 問題が発生してハイブリッド サービスが要求がブロックされた理由を報告できない場合、またはブロック ページの表示中にハイブリッド サービスにエラーが発生した場合、**[Exception reason（例外の理由）]** フィールドに説明とエラー コード（数値）が表示されます。問題が繰り返し発生する場合、Websense のテクニカル サポートは問題のトラブルシューティングにこのエラー コードを使用します。

例：

```
Role:Super Administrator
Category:Peer-to-Peer File Sharing
Policy:Default
Domain:
Group:
FileType:
Network:
Protocol:http
Category Reason String:Master database
Exception reason:
```

ここで、要求は優先管理者ロールの [Peer-to-Peer File Sharing] カテゴリをブロックするポリシーによってフィルタリングされます。要求された HTTP サイトは Master データベースによって分類されました。

8 レポートによるインターネット アクティビティの評価

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プレゼンテーション レポート*、161 ページ
- *調査レポート*、187 ページ
- *セルフレポートへのアクセス*、215 ページ
- *アプリケーション レポートの作成*、216 ページ
- *Real-Time Monitor*、224 ページ

Web Security manager は、インターネット アクセスのポリシーの効果を評価するのに役立つ一連のレポーティング ツールを提供します。（Real-Time Monitor 以外のすべてのレポーティング機能は、Windows 専用のコンポーネント Log Server がインストールされている場合にのみ有効にすることができます）。

注意
指定済み管理を使用する組織では、一部の管理者がレポーティング機能を使用できないことがあります。*代理管理およびレポート作成*、405 ページを参照してください。

- **Web Security ダッシュボードのグラフ**は、ネットワーク内でのインターネット アクティビティを瞬時に確認するのに役立つ脅威、リスク、使用状況およびシステム関連の情報を提供します。大部分のグラフで、時間、グラフの形式、表示する結果のセットをカスタマイズできます。*Web Security Dashboard*、39 ページを参照してください。
- **プレゼンテーション レポート**は、事前定義されたレポート、カスタム レポート、レポート テンプレートのリストを提供します。レポートは、棒グラフ、トレンド グラフ、表形式などの形式で取得できます。

  事前定義されているいずれかのレポートをコピーするか、独自のフィルターを適用してカスタム レポートを作成するか、またはレポート テンプレートを使用してレポートを最初から作成します。詳細については、*プレゼンテーション レポート*、161 ページを参照してください。

- **調査レポート**では、対話形式でログ データを参照できます。メイン ページは、リスク クラス別のアクティビティの要約棒グラフを表示します。ページ上の種々の要素をクリックすることによって、グラフを更新したり、データの表示方法を変更することができます。

  インターネット使用状況データを表示する種々の方法の詳細については、*調査レポート*、187 ページを参照してください。
- **アプリケーション レポート**は、インターネット要求の発信元のブラウザおよびプラットフォームに関する情報と、特定のユーザー エージェント文字列に関連するアクティビティを調査するために使用できる検索項目を提供します。

  詳細は、*アプリケーション レポートの作成*、216 ページを参照してください。
- **Real-Time Monitor** は、要求された URL と各要求に適用された処置を含む、ネットワークでの現在のインターネット アクティビティを表示します。Websense Web Security Gateway および Web Security Gateway Anywhere 環境では、このモニターはまた Content Gateway によってモニターされていたサイトを示します。サイトがスキャン結果によって動的に再分類されている場合は、元の分類と現在の分類の両方が示されます。

  詳細は、*Real-Time Monitor*、224 ページを参照してください。

重要

TRITON コンソールでは Internet Explorer Compatibility View を使用してはいけません。Internet Explorer で不適切なレポーティング動作やページ レイアウトが発生した場合、[Compatibility View（互換性表示）] ボタン（ブラウザのアドレス バーの URL と [Refresh（リフレッシュ）] ボタンの間）が選択されていないことを確認してください。

インターネット閲覧時間とは何か？

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *データベース ジョブ*、516 ページ
- *インターネット ブラウズ時間の設定*、525 ページ

インターネット閲覧時間、つまりユーザーがウェブサイトのアクセスで費やした時間の推定量を示すプレゼンテーション レポートおよび調査レポートを生成することができます。誰かが特定のサイトを開いた後、そのサイトの閲覧で費やした正確な時間を知ることができるソフトウェア プログラムはありません。サイトを開き、そのサイトを数秒間だけ閲覧し、次にビジネス コールをかけた後で別のサイトを要求しているかもしれません。また別の人はサイトを数分かけてていねいに閲覧してから、他のサイトに移動しているかもしれません。

ログ データベース ジョブ（*データベース ジョブ、516 ページ*を参照）は、設定可能なパラメータに基づいて閲覧時間を計算します。このジョブは一日に一度実行されます。したがって、閲覧時間情報と実際のログ データの間に時間差が生じることがあります。

閲覧時間の計算方法：

- インターネット セッションはユーザーがブラウザを開いた時に開始し、そのユーザーが少なくとも 3 分に 1 回（デフォルト）追加のウェブサイト要求を行っている間継続します。

  閲覧時間のしきい値を変更する場合は、*インターネット ブラウズ時間の設定、525 ページ*を参照してください。
- ユーザーが別のサイトを要求せずに 3 分間経過すると、そのインターネット セッションは終了します。
- 3 分以上経過してからユーザーが別の要求を出した場合は、新しいセッションの開始になります。一般に、ユーザーの閲覧時間は毎日の複数のセッションによって構成されています。

データベース ジョブは各セッションの総時間を、最初の要求の時刻から、最後の要求の 3 分後の時刻までの時間として計算します。

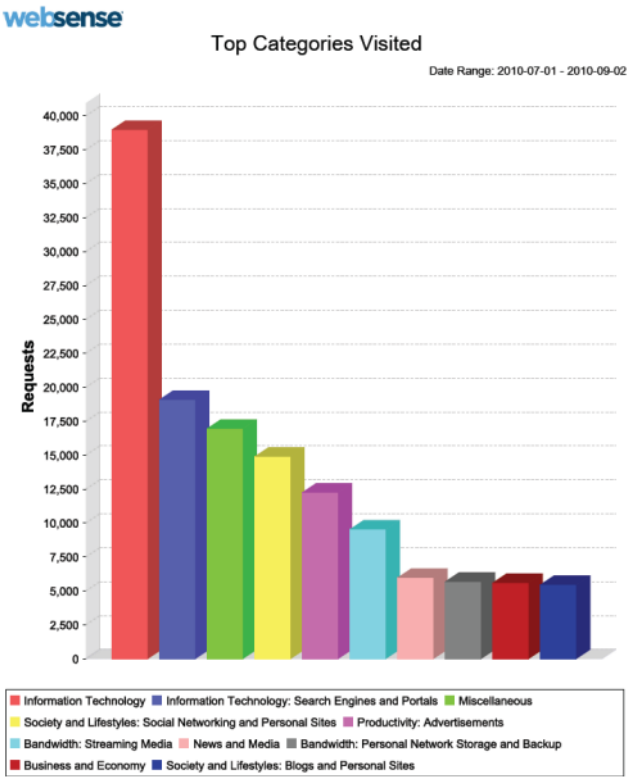
プレゼンテーション レポート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *新しいプレゼンテーション レポートの作成、164 ページ*
- *使用頻度の高いレポートの使用、175 ページ*
- *プレゼンテーション レポートの実行、175 ページ*
- *プレゼンテーション レポートのスケジュール設定、177 ページ*
- *スケジュールされたジョブのリストの表示、183 ページ*

[Reporting（レポート作成）] > [Presentation Reports（プレゼンテーション レポート）] ページで、棒グラフ、トレンド グラフ、および表形式レポートを HTML、PDF、または Microsoft Excel（XLS）形式で生成します。



利用できるレポートとテンプレートは Repot Catalog（レポート カタログ）中にあります。これは、レポートやテンプレートを関連する**レポート カテゴリ**別に編成しています。サブスクリプションによって、どのレポート カテゴリと事前定義レポートがカタログに表示されるかが決まります。例えば、[Real Time Security Threats（リアルタイム セキュリティ脅威）] や [Scanning Activity（スキャン アクティビティ）] のようなレポート カテゴリには、Websense Web Security Gateway または Gateway Anywhere のサブスクリプションが必要です。

- カテゴリを展開し、そのカテゴリのレポートまたはテンプレートを表示します。
- レポート タイトルをクリックすると、そのレポートに含まれる情報の簡単な説明が示されます。

プレゼンテーション レポートを実行するには、以下の手順を実行します：

1. カタログ中のレポートを選択し、**[Run（実行）]** をクリックします。[Run Report（レポートを実行）] ページが表示されます。
2. *プレゼンテーション レポートの実行*、175ページの説明に従って、レポートの詳細を指定します。

- レポートをフォアグラウンドで実行する（レポートの実行のスケジュール設定を行わない）場合、レポートを表示するためのアプリケーション（Web ブラウザ、Adobe Reader、Microsoft Excel など）を閉じるときに、レポートが自動的に保存されることはありません。レポートの保存は手動で行わなければなりません。
- レポートをバックグラウンドで実行する（レポートを即時実行するようにスケジュール設定する）場合、レポートが完了したときコピーが保存され、レポートへのリンクが [Review Reports（レポートの検討）] ページに表示されます。

レポート カタログ中のいずれかのテンプレート、定義済みレポート、またはカスタム レポートを新しいレポートのベースとして使用するには、以下の手順を実行します：

1. カタログ中のレポートまたはテンプレートの名前を選択します。

   レポート テンプレートを選択する場合：

   - **[New Trend Report（新トレンド レポート）]** はインターネット アクティビティの経時的トレンドを示します。
   - **[New Top N Report（新上位 N 件レポート）]** は、指定された特性が認められるインターネット アクティビティの上位を示します。
2. **[Save As（名前を付けて保存）]** をクリックします。
3. 新しいファイルの名前、タイトル、およびレポート カテゴリを提供します。

   レポート テンプレートを使用する場合、レポートのディメンション（測定対象と測定単位）も定義します。

   手順については、*新しいプレゼンテーション レポートの作成*、164 ページを参照してください。
4. レポートを改良するために、レポート フィルタを編集します。レポート フィルタは、どのユーザー、カテゴリ、プロトコル、アクションをレポートに含めるか、などの要素を制御します。

   手順については、*レポート フィルタを定義する*、166 ページを参照してください。

カスタム レポートのレポート フィルタを変更する場合は、レポートを選択し、次に **[Edit（編集）]** をクリックします。事前定義されているレポートまたはレポート テンプレートを編集または削除することはできません。

カスタム レポートを削除するには、そのレポートを選択し、次に **[Delete（削除）]** をクリックします。削除されたレポートがいずれかのスケジュール設定されているジョブに含まれる場合、そのジョブではそのレポートは引き続き生成されます。スケジュール設定されているジョブの編集および削除についての詳細は、*スケジュールされたジョブのリストの表示*、183 ページを参照してください。

使用頻度が高いレポートは、すばやく見つけることができるように、[Favorites（使用頻度の高いレポート）] というマークを付けることができます。そのためには単に、レポートを選択し、**[Favorite]** を選択します（*使用頻度の高いレポートの使用、175 ページ*を参照してください）。**[Show Favorites only（使用頻度の高いレポートだけを表示）]** にマークを付けると、レポート カタログには [favorites] というマークを付けたテンプレートだけが表示されます。

ページの上部にあるボタンを使用して、レポートを後で実行するようにスケジュール設定したり、スケジュール設定されたジョブを表示したり、スケジューラによって作成されたレポートを表示および管理します。

- **[Scheduler（スケジューラ）]** をクリックして、1 つ以上のレポートを含むジョブについて特定の日時の実行または繰り返しベースでの実行をスケジュール設定します。*プレゼンテーション レポートのスケジュール設定、177 ページ*を参照してください。
- **[Job Queue（ジョブ キュー）]** をクリックして、既存のスケジュール設定ジョブと各ジョブのステータスのリストを表示および管理します。*スケジュールされたジョブのリストの表示、183 ページ*を参照してください。
- **[Review Reports]** をクリックし、スケジュール設定され、正常に実行されたレポートのリストを表示および管理します。*スケジュール設定プレゼンテーション レポートのレビュー、185 ページ*を参照してください。

新しいプレゼンテーション レポートの作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プレゼンテーション レポート、161 ページ*
- *レポート フィルタを定義する、166 ページ*
- *プレゼンテーション レポートの実行、175 ページ*

[Save As New Report（新規レポートとして保存）] ページを使用して、以下のようなレポートを作成します：

- 事前定義レポートの編集可能なバージョン。
- 異なるレポート フィルタを適用するための既存カスタム レポートのコピー。
- レポート テンプレートに基づく新しいレポート。

このページ上で利用できるオプションは、選択されているオプションによって決まります。

事前定義またはカスタムのレポートのコピーを作成する場合は、以下のような手順になります

1. 新しいレポートを容易に識別できる名前で **Report name（レポート名）**を置き換えます。（デフォルトの名前は、元のレポート テンプレートの名前に当該コピーを示すナンバーが付加されています。）

   この名前は 1 ～ 85 文字であり、別のレポート名と重複してはなりません。
2. **Report title（レポート タイトル）**を入力します。これは、レポートが生成されるときページの最上部に表示されるタイトルです。
3. **Report category（レポート カテゴリ）**を選択します。このレポートは Report Catalog（レポート カタログ）においてこのカテゴリに基づいて仕分けられます。そのデフォルトは User-Defined Reports（ユーザー定義レポート）です。
4. 以下のいずれかを行います：
   - **[Save（保存）]** をクリックして、レポートの新しいバージョンを保存し、Report Catalog に戻ります。
   - **[Save and Edit（保存および編集）]** をクリックして、新しいレポートのためのレポート フィルタを編集します（*レポート フィルタを定義する、166 ページ*を参照してください）。
   - **[Cancel]** をクリックして、変更を破棄し、Report Catalog に戻ります。

レポート テンプレートを使用して新しいレポートを作成する場合は、以下のような手順になります

1. 一意の**Report name（レポート名）**を入力します。これは、Report Catalog で示される名前です

   この名前は 1 ～ 85 文字であり、別のレポート名と重複してはなりません。
2. **Report title（レポート タイトル）**を入力します。これは、レポートが生成されるときページの最上部に表示されるタイトルです。
3. **Report category（レポート カテゴリ）**を選択します。このレポートは Report Catalog（レポート カタログ）においてこのカテゴリに基づいて仕分けられます。そのデフォルトは User-Defined Reports（ユーザー定義レポート）です。
4. 上位 N 件レポートを作成する場合は、ステップ 5 に進みます。

   トレンド レポートを作成する場合は、トレンド レポートの X 軸の **[Time unit（期間の単位）**を指定します。日（デフォルト）、週、月、または年を単位とするトレンドを示すレポートを作成することができます。
   - トレンド レポートで必要なデータを示すために、含めるべき最初の週、月、または年の**初日**を指定期間の最初の日付に設定してください。（デフォルトでは週の初日は日曜日ですが、Microsoft SQL Server の設定とロケールによって、これと異なる場合があります。）

- ユーザー情報がディレクトリ サービスで更新されると、ユーザー グループ情報も変更されるでしょう。このために週間、月間、または年間グループ トレンド レポートが影響されることがあります。なぜなら、グループ レポートに特定のユーザーを含めるためには、そのユーザーは少なくとも選択されている期間の 1 日前に当該グループに属していなければならないからです。

  例えば、2012 年 8 月の月間グループ トレンド レポートが特定のユーザーのアクティビティを含むものであるためには、そのユーザーは 2012 年 7 月 31 日 の時点で当該グループに属していなければなりません。2012 年 8 月 23 日（水曜日）にグループに加えられるユーザーは、その翌日からの毎日のトレンド レポート、8 月 23 日後の土曜日、日曜日、または月曜日からの週間トレンド レポート（曜日は Microsoft SQL Server の設定によって異なります）、および 2012 年 9 月 01 日からの月間トレンド レポートに含まれます。

5. **Internet activity per（類別インターネット アクティビティ）**ドロップダウン リストを使用して、レポートのフォーカス領域を選択します。カテゴリ別（デフォルト）、プロトコル別、リスク クラス別、処置別（許可やブロックなど）、ユーザー別、またはグループ別のインターネット アクティビティを示すことができます。
6. **Measure by（測定基準）**ドロップダウン リストを使用して、フォーカス領域の測定基準を選択します。要求（デフォルト）、帯域幅、またはブラウズ時間を測定基準にすることができます。
7. 以下のいずれかを行います：
   - **[Save]** をクリックして、レポートを保存し、Report Catalog に戻ります。ステップ 5 で選択したレポート カテゴリで、この新しいレポートがリストされるようになります。
   - **[Save and Edit]** をクリックして、新しいレポートのためのレポート フィルタを編集します。レポート フィルタを編集するプロセスは、カスタマ レポートの場合と同じです（*レポート フィルタを定義する、166 ページ*を参照してください）。
   - **[Cancel]** をクリックして、変更を破棄し、Report Catalog に戻ります。

レポート フィルタを定義する

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *新しいプレゼンテーション レポートの作成、164 ページ*
- *プレゼンテーション レポートの実行、175 ページ*

レポート フィルタによって、プレゼンテーション レポートに含まれる情報を設定することができます。例えば、レポートを特定のクライアント、カテゴリ、リスク クラス、プロトコル、または特定の処置（許可、ブロックなど）にさえ限定することができます。また、レポートに新しい名前と説明を与え、レポートのタイトルを変更し、カスタム ログを選択し、レポート フィルタを通じてその他の一般的なオプションを設定することもできます。

> **注意**
> カスタム ロゴを使用するために、レポート フィルタを更新する前に、サポートされているフォーマットでイメージを作成し、そのファイルを適切な場所に配置しなければなりません。*レポート ロゴのカスタマイズ*、173 ページを参照してください。

利用できるオプションは以下のようになっています：

- 事前定義レポートまたは事前定義レポートに基づくカスタム レポートを編集する場合、フィルタで利用できるオプションは選択されているレポートによって異なります。

  例えば、Top Blocked Groups by Requests（要求別のブロックされた上位グループ）のようなグループ情報のレポートを選択した場合、レポートにどのグループを含めるかを指定できますが、個別のユーザを選択することはできません。
- New Top N Report（新上位 N 件レポート）または New Trend Report（新トレンド レポート）テンプレートを使用して作成されたレポートを編集する場合は、カスタム レポートに適用できなくても、**すべて**のオプションがフィルタで示されます。

  当該レポートにとって適切なオプションだけを選択するようにしてください。

事前定義されているレポートのフィルタは変更できません。[Save As New Report（新規レポートとして保存）] ページで **[Save and Edit]** を選択して作成する場合にはカスタム レポートのフィルタを編集できるし、あるいは Report Catalog でレポートを任意に選択し、**[Edit]** をクリックすることができます。

[Edit Report Filter（レポート フィルタの編集）] ページが開き、レポートの種々の要素を管理するために、各要素に対応するタブが表示されます。各タブで必要とされる項目を選択し、**[Next（次へ）]** をクリックして次のタブへ移ります。手順の詳細については、以下を参照してください：

- *レポートのクライアントの選択*、168 ページ
- *レポートのためのカテゴリの選択*、169 ページ
- *レポート対象のプロトコルの選択*、170 ページ
- *レポートのための処置の選択*、171 ページ
- *レポート オプションの設定*、172 ページ

[Confirm（確認）] タブで、レポートの実行またはスケジュール設定のどちらかを選択し、レポート フィルタを保存します。*レポート フィルタ定義の確認、174 ページ*を参照してください。

レポートのクライアントの選択

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *レポートのためのカテゴリの選択、169 ページ*
- *レポート対象のプロトコルの選択、170 ページ*
- *レポートのための処置の選択、171 ページ*
- *レポート オプションの設定、172 ページ*
- *レポート フィルタ定義の確認、174 ページ*

[Presentation Reports] > [Edit Report Filter] ページの **[Clients（クライアント）]** タブにより、レポートに含めるべきクライアントを指定することができます。各レポートに 1 つのクライアントのタイプだけを選択できます。たとえば、同じレポートでユーザとグループの組み合せを選択することはできません。

レポート定義が特定のクライアント タイプを指定している場合は、そのタイプのクライアントまたはより大きな分類グループのクライアントを選択することができます。例えば、Top Blocked Groups by Requests（要求別のブロックされた上位グループ）に基づいてレポートのフィルタを定義する場合、そのレポートのためにグループやドメイン（OU）を選択できますが、個々のユーザーを選択することはできません。

リストされているすべてのクライアントをレポートに含める場合は、このタブでは何も選択する必要はありません。

1. ドロップダウンリストからクライアント タイプを選択します。
2. **Limit search（検索の制限）** リストで検索結果の最大件数を設定します。

   組織内のトラフィックによっては、ログ データベースに多数のユーザ、グループまたはドメイン（OU）がある可能性があります。このオプションは、結果リストの長さと、検索結果を表示するために必要とされる時間を管理します。
3. 検索基準として 1 字以上の文字を入力し、**[Search（検索）]** をクリックします。

   アスタリスク（*）は、欠けている文字を表すワイルドカード文字として使用します。たとえば、[J*n] と指定すると、Jackson、Jan、Jason、Jon、John 等が返されます。

   検索文字列を定義する際に、すべての期待している結果が、検索結果の制限数の範囲内に含まれるように注意しなければなりません。

4. 結果リストで 1 つ以上のエントリを強調表示にし、右向き矢印ボタン（>）をクリックして、それらのエントリを **Selected（選択）**リストに移します。
5. 必要に応じてステップ 2 ～ 4 を繰り返して何度でも検索を実行し、さらに多くのクライアントを Selected リストに追加します。
6. クライアントの選択が終わったら、**[Next]** をクリックして Categories（カテゴリ）タブを開きます。*レポートのためのカテゴリの選択*、169 ページを参照してください。

レポートのためのカテゴリの選択

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *レポートのクライアントの選択*、168 ページ
- *レポート対象のプロトコルの選択*、170 ページ
- *レポートのための処置の選択*、171 ページ
- *レポート オプションの設定*、172 ページ
- *レポート フィルタ定義の確認*、174 ページ

[Presentation Reports] > [Edit Report Filter] ページの **[Categories]** タブにより、カテゴリまたはリスク クラスに基づくレポートに含めるべき情報を指定することができます。*リスク クラス*、64 ページを参照してください。

リストされているすべてのカテゴリまたはリスク クラスをレポートに含める場合は、このタブでは何も選択する必要はありません。

1. 次のどちらかの分類を選択します：**Category（カテゴリ）**または **Risk Class（リスク クラス）**。

   親カテゴリを展開して、サブカテゴリを表示します。リスク クラスを展開して、現在、そのリスク クラスに割り当てられているカテゴリのリストを表示します。

   関連するレポートが特定のリスク クラスに関するものである場合、選択できるのは該当するリスク クラスとそれが表すカテゴリだけです。

   注意
   レポートで指定されているリスク クラスでサブセットのカテゴリを選択する場合は、その選択を反映するようなレポート タイトルへの変更を考えてください。

2. レポートに含める各カテゴリまたはリスク クラスのチェックボックスをオンにします。

リストの下の **[Select All（すべて選択）]** および **[Clear All（すべてクリア）]** ボタンを使用して、必要とされる個別の選択操作を簡略にすることができます。

3. 右向き矢印（>）ボタンをクリックし、選択項目を **Selected** リストに追加します。

   リスク クラスにマークを付ける時、右矢印をクリックすると、すべての関連付けられているカテゴリが [Selected] リストに入れられます。

4. すべての選択が完了したら、**[Next]** をクリックして Protocols（プロトコル）タブを開きます。*レポート対象のプロトコルの選択、170 ページ*を参照してください。

レポート対象のプロトコルの選択

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *レポートのクライアントの選択、168 ページ*
- *レポートのためのカテゴリの選択、169 ページ*
- *レポートのための処置の選択、171 ページ*
- *レポート オプションの設定、172 ページ*
- *レポート フィルタ定義の確認、174 ページ*

[Presentation Reports] > [Report Filter（レポート フィルタ）] ページの **[Protocols（プロトコル）]** タブによって、レポートに含めるべきプロトコルを指定することができます。

リストされているすべてのプロトコルをレポートに含める場合は、このタブでは何も選択する必要はありません。

1. プロトコル グループ（グループ名の横にアイコンが表示される）を展開または縮小します。
2. レポートに含める各プロトコルのチェックボックスをオンにします。

   リストの下の **[Select All（すべて選択）]** および **[Clear All（すべてクリア）]** ボタンを使用して、必要とされる個別の選択操作を簡略にすることができます。

3. 右向き矢印（>）ボタンをクリックし、選択項目を **Selected** リストに追加します。
4. すべての選択が完了したら、**[Next]** をクリックして Actions（処置）タブを開きます。*レポートのための処置の選択、171 ページ*を参照してください。

レポートのための処置の選択

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *レポートのクライアントの選択*、168 ページ
- *レポートのためのカテゴリの選択*、169 ページ
- *レポート対象のプロトコルの選択*、170 ページ
- *レポート オプションの設定*、172 ページ
- *レポート フィルタ定義の確認*、174 ページ

[Presentation Reports] > [Edit Report Filter] ページの **[Actions]** タブによって、レポートに含めるべき処置（例えば、制限付きアクセス フィルタによる許可や割り当て時間によるブロックなど）を指定することができます。レポートがブロックされる要求についてのみ適用されることになっていると、選択できるのはブロック関連の処置（ファイル タイプによるブロック、キーワードによるブロック、等々）だけです。

リストされているすべてのアクションをレポートに含める場合は、このタブでは何も選択する必要はありません。

1. 処置グループ（グループ名の横にアイコンが表示される）を展開または縮小します。
2. レポートに含める各処置のチェックボックスをオンにします。

   リストの下の **[Select All（すべて選択）]** および **[Clear All（すべてクリア）]** ボタンを使用して、必要とされる個別の選択操作を簡略にすることができます。
3. 右向き矢印（>）ボタンをクリックし、選択項目を **Selected** リストに追加します。
4. すべての選択が完了したら、**[Next]** をクリックして Options（オプション）タブを開きます。*レポート オプションの設定*、172 ページを参照してください。

レポート オプションの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *レポート ロゴのカスタマイズ*、173 ページ
- *レポートのクライアントの選択*、168 ページ
- *レポートのためのカテゴリの選択*、169 ページ
- *レポート対象のプロトコルの選択*、170 ページ
- *レポートのための処置の選択*、171 ページ
- *レポート オプションの設定*、172 ページ
- *レポート フィルタ定義の確認*、174 ページ

[Presentation Reports] > [Edit Report Filter] ページの **Options** タブによって、レポートのいくつかの面を設定します。

1. オプションとして、**レポート カタログ名**を変更することもできます。名前は 1 ～ 85 字の文字列なければなりません。

   この名前はレポート自体には表示されず、レポート カタログの中でレポート フォーマットとフィルタの一意な組み合わせを識別するためにのみ使用します。
2. レポートで表示される**レポート タイトル** を変更します。タイトルの最大の長さは 85 文字です。
3. レポート カタログに表示する**説明**を変更します。説明の最大の長さは 336 文字です。

   説明は、レポート カタログの中でレポート フォーマットとフィルタの一意な組み合わせを識別するために役立ちます。
4. レポートに表示するログを選択します。

   該当するディレクトリの中のすべてのサポートされるイメージがリストされます。*レポート ロゴのカスタマイズ*、173 ページを参照してください。
5. **[Save as Favorite（使用頻度の高いレポートとして保存）]** チェックボックスをオンにして、当該レポートを [使用頻度の高いレポート] にします。

   レポート カタログには使用頻度の高いレポートの横に星印が表示されます。[Report Catalog] ページで **[Show only Favorites（使用頻度の高いレポートだけを表示）]** を選択すると、リストアップされるレポートの数が少なくなり、特定のレポートを容易に見つけることがでます。
6. **Show only top（上位のみを表示）**チェックボックスをオンにして、レポートされる項目数の上限として 1 から 20 までの数を入力します。

このオプションは、選択したレポートのフォーマットが上位 N 件レポートとして指定されている場合にのみ表示されます。このフォーマットは限られた数の項目を表示するために使用します。制限される項目はレポートによって異なります。例えば、Top Categories Visited（アクセス件数上位カテゴリ）レポートでは、このエントリは報告されるカテゴリの数を指定します。

7. すべての入力と選択が完了したら、**[Next]** をクリックして [Confirm] タブを開きます。*レポート フィルタ定義の確認*、174 ページを参照してください。

レポート ロゴのカスタマイズ

Web Security Help | Web Security ソリューション | バージョン 7.8.x

デフォルトにより、プレゼンテーション レポートの左上隅に Websense ロゴが表示されます。カスタム レポートを作成し、そのレポート フィルタを編集するとき、別のロゴを選択することができます。

1. 以下のいずれかのフォーマットのイメージ ファイルを作成します。

   - .bmp
   - .gif
   - .jfif
   - .jpe
   - .jpg
   - .jpeg
   - .png
   - .ttf

2. イメージ ファイルの名前は拡張子を含めて最大 25 文字です。
3. イメージ ファイルを **ReportTemplates\images** ディレクトリにコピーします。デフォルトのパスは次のとおりです：

   ```
   C:\Program Files(x86)\Websense\Web Security\Manager\
   ReportTemplates\images
   ```

[Edit Report Filter] ページの Options タブ上のドロップダウン リストで、このディレクトリ中のすべてのサポートされているイメージ ファイルが自動的に表示されます。イメージは自動的に、そのロゴに割り当てられているスペースに合わせて拡大または縮小されます（*レポート オプションの設定*、172 ページを参照してください。）

注意
レポート フィルタ中でアクティブなイメージを削除または移動しないでください。ロゴ ファイルが消失していると、レポートは生成されません。

レポート フィルタ定義の確認

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *レポートのクライアントの選択*、168 ページ
- *レポートのためのカテゴリの選択*、169 ページ
- *レポート対象のプロトコルの選択*、170 ページ
- *レポートのための処置の選択*、171 ページ
- *レポート オプションの設定*、172 ページ

[Presentation Reports] > [Edit Report Filter] ページの **[Confirm]** タブによって、Report Catalog で示される名前と説明を表示し、作業の進め方を選択することができます。

1. **Name（名前）**と **Description（説明）**を確認します。

   何らかの変更が必要な場合は、**[Back（戻る）]** をクリックして Options タブに戻り、そこで必要な変更を行います。（*レポート オプションの設定*、172 ページを参照してください。）
2. 処理方法を指定してください。

オプション	説明
保存	レポート フィルタを保存し、レポート カタログに戻ります。*プレゼンテーション レポート*、161 ページを参照してください。
保存して実行	レポート フィルタを保存し、[Run Report（レポートの実行）] ページを開きます。*プレゼンテーション レポートの実行*、175 ページを参照してください。
保存してスケジュール	レポート フィルタを保存し、[Schedule Report（レポートのスケジュール設定）] ページを開きます。*プレゼンテーション レポートのスケジュール設定*、177 ページを参照してください。

3. **[Finish（終了）]** をクリックして、ステップ 2 の選択を適用します。

使用頻度の高いレポートの使用

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プレゼンテーション レポート*、161 ページ
- *プレゼンテーション レポートの実行*、175 ページ
- *プレゼンテーション レポートのスケジュール設定*、177 ページ

頻繁に作成するレポートをすばやく見つけられるようにするために、プレゼンテーション レポートに [使用頻度の高いレポート] というマークを付けることができます。

1. **[Presentation Reports]**ページ上で、頻繁に生成するレポートまたは速やかに検出できるようにするレポートを強調表示にします。
2. **[Favorite]** をクリックします。

   リストの中の使用頻度の高いレポートの名前の横に星印が表示されます。それによって、多くのレポートが表示されるときに、それらのレポートをすばやく見つけることができます。
3. レポート カタログの上にある **Show only Favorites（使用頻度の高いレポートだけを表示）**チェックボックスをオンにして、使用頻度の高いレポートとしてマークされているものだけがリストアップされるようにします。レポートの完全なリストに戻すには、このチェックボックスをオフにします。

ニーズが変化し、使用頻度の高いレポートが頻繁に使用されなくなった場合、そのレポートを選択し、**[Favorite]** をクリックして星印を削除します。

プレゼンテーション レポートの実行

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プレゼンテーション レポート*、161 ページ
- *プレゼンテーション レポートのスケジュール設定*、177 ページ

[Presentation Reports] > [Run Report] ページを使用して、単一のレポートを直ちに生成します。また、1 つ以上のレポートのジョブを作成し、その 1 回だけの実行または繰り返し実行のスケジュールを設定することもできます（*プレゼンテーション レポートのスケジュール設定*、177 ページを参照してください）。

レポートを実行するには、以下の手順を実行します：

1. **Start date（開始日）**と **End date（終了日）**を選択して、レポートによってカバーされる期間を設定します。
2. レポートの **Output format（出力フォーマット）**を選択します。

フォーマット	説明
PDF	ポータブル ドキュメント フォーマット。PDF ファイルは表示用にフォーマットされていて、Adobe Reader で開くことができます。 表示するには、Adobe Reader 7.0 以降が必要です。
HTML	HyperText Markup Language.HTML ファイルは表示用にフォーマットされていて、ブラウザで開くことができます。
XLS	Excel スプレッドシート。XLS ファイルは再使用のためにフォーマットされていて、Microsoft Excel で開くことができます。 表示するには、Microsoft Excel 2003 以降が必要です。

3. **Top N（上位 N 件）**レポートを選択している場合は、レポートすべき項目数を選択します。
4. レポートを生成する方式を指定します：
   - **Schedule the report to run in the background（レポートをバックグラウンドで実行するようにスケジュール設定する）**（デフォルト）を選択すると、レポートがスケジュール設定ジョブとして直ちに実行されます。オプションとして、レポートの完了時点で通知させるための電子メール アドレスを提供することができます。また、レポートが生成できなかった場合に通知させるための電子メール アドレスを提供することもできます。（ジョブ キューをモニタして、レポートのステータスをチェックすることもできます。）
   - **Schedule the report to run in the background** の選択を解除すると、レポートはフォアグラウンドで実行されます。この場合、レポートのスケジュール設定は行われず、これは [Review Reports] ページでも表示されません。
5. **[Run]** をクリックします。
   - レポートを直ちに実行するようにスケジュール設定されていると、完了したレポートは自動的に保存され、Review Reports リストに追加されます。レポートを表示、保存、または削除するには、[Presentation Reports] ページ最上部の **[Review Reports]** をクリックします。
   - レポートをフォアグラウンドで実行すると、レポートが表示されます。完了すると、HTML レポートがブラウザ ウィンドウで表示されます。PDF または XLS フォーマットでは、レポートを開くか、またはディスクに保存するかのどちらかを選択することができます。

HTML を選択した場合、**[Presentation Reports]** をクリックして [Report Catalog] に戻ります。PDF または XLS を選択した場合、もう一度 [Run Reports] ウィンドウを使って同じレポートを作成できます。

このオプションでは、プレゼンテーション レポートはレポートのコピーを自動的に保存するようなことはありません。後で閲覧するためにレポートのコピーを保存したい場合は、レポートを開くために使用されるアプリケーションに組み込みまれている保存機能を利用します。

6. レポートを印刷するためには、レポートの表示で使用されるアプリケーションで用意されている印刷オプションを利用します。

   印刷で最良の結果を得るには、PDF フォーマットを出力し、Adobe Reader で印刷のオプションを使用します。

プレゼンテーション レポートのスケジュール設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プレゼンテーション レポート*、161 ページ
- *プレゼンテーション レポートの実行*、175 ページ
- *スケジュールされたジョブのリストの表示*、183 ページ

プレゼンテーション レポートを必要に応じて実行でき、また **[Presentation Reports] > [Scheduler（スケジューラ）]** ページを使用して、1 つまたは複数のレポートを実行するスケジュールを設定したジョブを作成することもできます。

スケジュールされたジョブによって生成されたレポートは、電子メールを通じて 1 人以上の受信者に配信されます。スケジュールされたジョブを作成する際、使用する電子メール サーバが添付されたレポート ファイルのサイズおよび数を処理できるかどうかを考慮してください。

完了したレポートはまた、[Presentation Reports] > [Review Reports] ページに追加されます（*スケジュール設定プレゼンテーション レポートのレビュー*、185 ページを参照してください）。

スケジューラにアクセスするには以下の手順を実行します。

- [Presentation Reports] ページ最上部（Report Catalog の上）の **[Scheduler]** ボタンをクリックします。
- レポート フィルタを編集する場合は、[Confirm] タブで **[Save and schedule（保存して、スケジュールを設定する）]** を選択し、つづいて **[Finish]** をクリックします（*レポート フィルタを定義する*、166 ページを参照してください）。

- [Job Queue（ジョブ キュー）] ページでジョブ名リンクをクリックして、ジョブを編集します。
- [Job Queue] ページで **[Add（追加）]** をクリックし、新しいジョブを作成します。

[Scheduler] ページには、実行すべきレポートとそれらの実行スケジュールを選択するためのタブがいくつかあります。手順の詳細については、以下を参照してください：

- *スケジュールの設定*、179 ページ
- *スケジュールするレポートの選択*、180 ページ
- *日付範囲の設定*、181 ページ
- *出力オプションの選択*、182 ページ

ジョブを作成したら、Job Queue を使用して、ジョブ ステータスやその他の有用な情報を確認します（*スケジュールされたジョブのリストの表示*、183 ページを参照してください）。

スケジュール設定されているプレゼンテーション レポートが実行されると、そのレポート ファイルが電子メール添付の **presentationreport_0** として受信者に送られます。ファイルの番号は、添付されているレポートの番号に従って大きくなります。

スケジュール設定されているレポートも、TRITON 管理サーバー コンピュータ上の **ReportingOutput** ディレクトリに自動的に保存されます（デフォルトでは C:\Program Files （x86）\Websense\Web Security\ReportingOutput）。電子メールで送られる添付ファイルの名前が ReportingOutput ディレクトリに保存されるファイルの名前と一致しないことに注意してください。特定のレポートを検出する最良の方法は [Review Reports] ページを使用することであり、このページで日付やジョブ名、あるいはレポート名により検索することができます。

[Settings（設定）] > [Reporting（レポーティング）] > [Preferences（優先設定）] ページで指定されている期間（デフォルト：5 日間）が過ぎると、レポートは [Review Reports] ページと ReportingOutput ディレクトリから自動的に削除されます。レポートをより長期に保存したい場合は、レポートをバックアップ ルーチンに含めるか、または長期にわたって格納できる場所にレポートを保存します。

[Review Reports] ページで、レポートが削除される前に一定期間（デフォルト：3 日間）にわたってアラートが表示されます。[Settings] > [Reporting] > [Preferences] ページによって、このアラート期間を変更することができます。

毎日生成されるレポートの数によっては、レポート ファイルはかなりの量のディスク スペースを使用します。TRITON 管理サーバー コンピュータで利用できる適切なサイズのディスク スペースを確保してください。ファイルが自動的に削除される前に ReportingOutput ディレクトリが大きくなりすぎた場合、ファイルを手動で削除できます。

レポートはユーザー指定のフォーマットで生成されます：PDF（Adobe Reader 7.0 以降）、XLS（Microsoft Excel 2003 以降）、または HTML。HTML フォーマットを指定すると、レポートは Web Security manager コンテンツ ペインで表示されます。コンテンツ ペインで表示されるレポートは印刷できず、またファイルとして保存することもできません。レポートを印刷またはファイルに保存する場合は、出力フォーマットに PDF または XLS を選択してください。

スケジュールの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プレゼンテーション レポートのスケジュール設定、177 ページ*
- *スケジュールするレポートの選択、180 ページ*
- *出力オプションの選択、182 ページ*
- *日付範囲の設定、181 ページ*

[Presentation Reports] > [Scheduler] ページの **[Schedule（スケジュール設定）]** タブによって、1 度だけの実行または周期的繰り返し実行のレポーティング ジョブを作成します。

注意

Log Database の過負荷を防止し、ログ記録および対話的レポーティングのパフォーマンス低下を避けるために、レポート ジョブの実行スケジュールを異なる日時に設定すべきです。

1. このスケジュールされたジョブを一意に識別する**ジョブ名**を入力します。
2. スケジュール設定ジョブの **Recurrence Pattern（繰り返しパターン）**と **Recurrence Options（繰り返しオプション）**を選択します。使用できるオプションは、選択したパターンによって異なります。

パターン	Options（オプション）
1 回	ジョブを実行する日付を入力するか、カレンダからアイコンをクリックして選択します。
毎日	追加の繰り返しオプションはありません。
毎週	ジョブを実行する各曜日のチェックボックスをオンにします。
毎月	ジョブを実行する日を入力します。日付は 1 ～ 31 の数値で指定し、コンマで区切る必要があります（1,10,20）。 毎月、連続する日付でジョブを実行するには、開始日と終了日をハイフンで区切って入力します（3-5）。

3. **[Schedule Time（スケジュール時刻）]** で、ジョブを実行する開始時刻を設定します。

   ジョブは、TRITON 管理サーバー上の時刻に従って開始します。

   > **注意**
   > スケジュールされたレポートの生成を今日開始する場合は、ジョブの開始前にジョブ定義を完了できるように十分に余裕のある時刻を選択します。

4. **[Schedule Period（スケジュール期間）]** で、ジョブを開始する日付を選択し、オプションとしてジョブを終了する日付を入力することができます。

オプション	説明
終了日の指定なし	ジョブは設定されたスケジュールに従って、無限に実行を継続します。 将来のいずれかの時点でジョブを停止するには、ジョブを編集するか、削除します。*スケジュールされたジョブのリストの表示、183 ページ*を参照してください。
次の回数後に終了	このジョブを実行する回数を選択します。その回数の後、ジョブは実行しませんが、削除するまでは [ジョブ キュー] に入ったままです。*スケジュールされたジョブのリストの表示、183 ページ*を参照してください。
次の日付で終了	ジョブの実行を停止する日付を設定します。ジョブはその日付以降実行しません。

5. **[Next]** をクリックして、Reports タブを開きます。*スケジュールするレポートの選択、180 ページ*を参照してください。

スケジュールするレポートの選択

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プレゼンテーション レポートのスケジュール設定、177 ページ*
- *スケジュールの設定、179 ページ*
- *出力オプションの選択、182 ページ*
- *日付範囲の設定、181 ページ*

[Presentation Reports] > [Scheduler] ページの **[Select Report（レポートの選択）]** タブを使用して、ジョブのためのレポートを選択します。

1. Report Catalog ツリーでジョブのためのレポートを強調表示にします。
2. 右向き矢印（>）ボタンをクリックし、そのレポートを **[Selected]** リストに追加します。
3. ジョブのためのすべてのレポートが **[Selected]** リストに表示されるまで、ステップ 1 および 2 を繰り返します。
4. **[Next]** をクリックして、Date Range（日付の範囲）タブを開きます。*日付範囲の設定、181 ページ*を参照してください。

日付範囲の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プレゼンテーション レポートのスケジュール設定、177 ページ*
- *スケジュールの設定、179 ページ*
- *スケジュールするレポートの選択、180 ページ*
- *出力オプションの選択、182 ページ*

[Presentation Reports] > [Scheduler] ページの **[Date Range（日付範囲）]** タブを使用して、ジョブの日付範囲を設定します。利用できるオプションは、**[Date range]** の選択によって異なります。

日付範囲	説明
すべての日付	レポートは、ログ データベースに含まれるすべての日付を含みます。追加のエントリは必要ありません。 繰り返しジョブにこのオプションを使用すると、別の日に実行されたレポートとの間で情報が重複する場合があります。
特定の日付	このジョブのレポートの開始日（**[開始日]**）および終了日（**[終了日]**）を選択します。 このオプションは 1 回だけ実行するジョブに適しています。繰り返しジョブにこのオプションを使用すると、レポートが重複する場合があります。

日付範囲	説明
日付範囲を指定	ドロップダウン リストを使用して、レポートする期間の数（This（今）、Last（前）、Last 2（過去 2）、等々）と期間の種類（Days（日）、Weeks（週）、または Months（月））を選択します。たとえば、[Last 2 Weeks（最近 2 週間）] あるいは [This Month（今月）] を対象とするレポートを作成できます。 週は、日曜日から土曜日までの 1 週間を表します。月は暦上の月を表します。たとえば、[This Week（今週）] は、日曜から今日までのレポートを作成します。[This Month（今月）] は、月の初めから今日までのレポートを作成します。[Last Week（先週）] は、前の日曜から土曜までのレポートを作成します。 このオプションは、繰り返し実行するジョブに適しています。これによって各レポートに表示されるデータの量を管理し、異なるスケジュールで実行するレポートの間のデータの重複を最小限に抑えることができます。

ジョブの日付範囲の設定を終えたら、**[Next]** をクリックして、Output（出力）タブを表示します。*出力オプションの選択*、182 ページを参照してください。

出力オプションの選択

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：
- *プレゼンテーション レポートのスケジュール設定*、177 ページ
- *スケジュールの設定*、179 ページ
- *スケジュールするレポートの選択*、180 ページ
- *日付範囲の設定*、181 ページ

ジョブのためのレポートを選択したら、**[Output]** タブにより出力フォーマットと配布オプションを選択します。

1. 生成したレポートのファイル フォーマットを選択します。

フォーマット	説明
PDF	ポータブル ドキュメント フォーマット。受信者は、PDF レポートを表示するために、Adobe Reader v7.0 以降をインストールしている必要があります。
XLS	Excel スプレッドシート。受信者は、XLS レポートを表示するために、Microsoft Excel v2003 以降をインストールしている必要があります。

2. レポートの配信先の電子メール アドレスを入力します。

   1 行に 1 つのアドレスを入力します。

3. 必要に応じて、**[Customize subject and body of email（電子メールの件名と本文のカスタマイズ）]** チェックボックスをオンにします。次に、ジョブの配布電子メールのカスタム **Subject（件名）**および **Body（本文）**テキストを入力します。

4. **[Save Job（ジョブの保存）]** をクリックして、ジョブ定義を保存および適用し、[Job Queue] ページを表示します。

5. このジョブおよび他のスケジュールされているジョブを確認します。*スケジュールされたジョブのリストの表示、183 ページ*を参照してください。

スケジュールされたジョブのリストの表示

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プレゼンテーション レポート、161 ページ*
- *プレゼンテーション レポートのスケジュール設定、177 ページ*
- *出力オプションの選択、182 ページ*
- *調査レポートのスケジュール設定、208 ページ*

[Presentation Reports] > [Job Queue] ページで、プレゼンテーション レポートのために作成された スケジュール設定ジョブのリストが表示されます。リストは、各ジョブのステータスやジョブに関する基本情報（ジョブが実行する頻度など）を示します。このページから、スケジュールされたジョブの追加および削除、ジョブの一時的中断などの操作を実行できます

（調査レポートのためのスケジュールされたジョブについては、*スケジュール設定調査レポート ジョブの管理、212 ページ*を参照してください。）

リストは、各ジョブに関する以下の情報を含みます。

列	説明
ジョブ名	ジョブが作成されたとき割り当てられた名前。
Status（ステータス）	ジョブが以下のいずれであるかを示します • 実行中 • スケジュール設定されている（次のスケジュール実行時を待っている） • 正常終了 • 失敗 • ミスファイヤー（直近のスケジュール実行時にメモリ不足やサーバー シャットダウンのために実行されなかった）

列	説明
状態	次のどちらかを示します。 • ENABLED（有効）は、設定されている繰り返しパターンに従って実行されるジョブであることを示します。 • DISABLED（無効）は、アクティブでなく、実行されないジョブであることを示します。
Recurrence（実行頻度）	ジョブで設定されている繰り返しパターン（Once（1 回だけ）、Daily（毎日）、Weekly（毎週）、Monthly（毎月））。
履歴	**[Details（詳細）]** リンクをクリックして、選択されているジョブの [Job History（ジョブ履歴）] ページを開きます。*ジョブ履歴の表示、185 ページ*を参照してください。
次回スケジュール	次回実行する日付と時刻。
所有者	ジョブのスケジュールを設定した管理者の名前。

ページ上のオプションを使用してジョブを管理します。いくつかのボタンでは、ボタンを選択する前に、リストに含める各ジョブの名前の隣のチェックボックスをオンにしておく必要があります。

オプション	説明
ジョブ名リンク	[Scheduler] ページが開きます。ここでジョブ定義を編集することができます。*プレゼンテーション レポートのスケジュール設定、177 ページ*を参照してください。
ジョブの追加	[Scheduler] ページが開きます。ここで新しいジョブを定義することができます。*プレゼンテーション レポートのスケジュール設定、177 ページ*を参照してください。
削除	Job Queue からリスト内で選択されているすべてのジョブを削除します。削除されたジョブを復元することはできません。 特定のジョブの実行を一時的に停止するには、**[Disable（無効にする）]** ボタンを使用します。
Run Now（すぐに実行）	リスト内で選択されているジョブの実行を即座に開始します。これは定期的にスケジュールされた実行とは別に実行されます。
有効化する	リスト内で選択されている無効になっているジョブを再度アクティブにします。ジョブは設定されたスケジュールに従って実行を開始します。
無効化する	リスト内で選択されている有効になっているジョブの実行を停止します。このオプションを使用して、将来復元したいジョブを一時的に中断します。

ジョブ履歴の表示

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プレゼンテーション レポートのスケジュール設定、177 ページ*
- *スケジュールされたジョブのリストの表示、183 ページ*

[Presentation Reports] > [Job Queue] > [Job History（ジョブ履歴）] ページを使用して、選択されているジョブの近時の実行履歴に関する情報を表示します。このページは、各レポートを別々に表示し、以下の情報を示します。

列	説明
Report Name（レポート名）	レポートで表示されるタイトル。
Start Date（開始日）	レポートの実行開始の日付と時刻。
End Date（終了日）	レポートが完了した日付と時刻。
Status（ステータス）	レポートが成功したか失敗したかを示します。
Message（メッセージ）	ジョブに関連する情報（たとえば、レポートの電子メールでの送信が正常に完了したか否か）を示します。

スケジュール設定プレゼンテーション レポートのレビュー

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プレゼンテーション レポート、161 ページ*
- *プレゼンテーション レポートの実行、175 ページ*
- *プレゼンテーション レポートのスケジュール設定、177 ページ*

[Presentation Reports] > [Review Reports（レポートのレビュー）] ページを使用して、スケジュール設定レポートの検出、アクセス、および削除を行うことができます。デフォルトで、レポートは最も古いものからリストアップされます。

リスト中のレポートを表示するには、そのレポート名をクリックします。

- そのレポートが単一の PDF または XLS ファイルであると、そのレポートを開くか、または保存するオプションがあります。これは、ユーザーのコンピュータ上のブラウザ セキュリティ設定とインストールされているプラグインに依存しています。

- レポートが非常に大きい場合は、複数の PDF または XLS ファイルになっていて、ZIP ファイルとして保存されているかもしれません。レポートが Windows コンピュータまたは Linux コンピュータのどちらで作成されたものであっても、そのファイル圧縮は ZIP フォーマットで行われます。ZIP ファイルを保存し、それに含まれている PDF または XLS ファイルを展開して、レポートの内容を表示します。
- レポート名の隣にあるレポート アイコンに マウス を進めることにより、レポートが単一のファイルであるか複数のファイルであるか確認することができます。

リストの表示をまもなく削除するレポートだけに限定するには、**Show only reports due to be purged（消去されうレポートだけを表示）**チェックボックスをオンにします。レポートが保存される期間は、[Settings] > [Reporting] > [Preferences] ページで設定されます（*レポートの優先設定、503 ページ*を参照してください）。

レポート リストで検索するには、**Filter by（フィルタ）**ドロップダウン リストでエントリを選択し、次に名前または日付のすべてまたは一部を入力します。以下の事項によって検索できます：

- レポート名またはジョブ名
- レポートのスケジュール設定を行った管理者の名前（Requestor（要求者））
- レポートが作成された日付（Creation Date（作成日））
- レポートが消去される日付（Purge Date（消去日））

検索条件を入力し、**[Go]** をクリックします。検索は大文字と小文字を区別します。

[Clear] をクリックして現在の検索条件を消去し、別の検索を行うか、または **[Refresh（リフレッシュ）]** をクリックしてレポートの完全なリストを表示します。

直近に完了したレポートが [Review Reports] ページで表示されない場合は、**[Refresh]** をクリックして最新のデータでページを更新します。

レポートを削除するには、レポート ファイル サイズの右側にある X をクリックします。

スケジュール設定レポート ジョブのステータスを調べるには、ページ最上部の **[Job Queue]** をクリックします。ジョブ キューの使用法の詳細については、*スケジュールされたジョブのリストの表示、183 ページ*を参照してください。

新しいレポート ジョブのスケジュールを設定するには、**[Scheduler]** をクリックします（*プレゼンテーション レポートのスケジュール設定、177 ページ*を参照してください）。

調査レポート

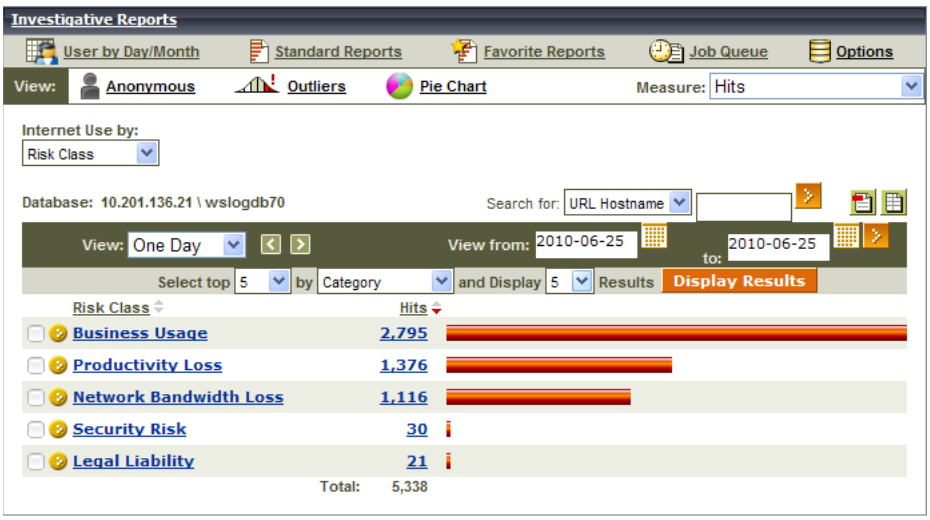
Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *要約レポート*、190 ページ
- *マルチレベル要約レポート*、196 ページ
- *柔軟な詳細レポート*、197 ページ
- *User Activity Detail（ユーザー アクティビティ詳細）レポート*、203 ページ
- *標準レポート*、206 ページ
- *使用頻度の高い調査レポート*、207 ページ
- *調査レポートのスケジュール設定*、208 ページ
- *外れ値レポート*、213 ページ
- *調査レポートの出力のオプション*、214 ページ
- *データベース接続とレポートのデフォルト*、535 ページ

[Reporting] > [Investigative Reports（調査レポート）] ページを使用して、インターネット フィルタリング アクティビティを対話的に分析することができます。

最初に、メインの [Investigative Reports] ページでリスク クラス別のアクティビティ要約レポートが示されます（*リスク クラス*、64 ページを参照してください）。



要約レポート ビューで利用できるリンクや要素をクリックすることで、関心領域を調べたり、組織のインターネット使用状況の概要を把握したりすることができます（*要約レポート、190 ページ*を参照してください）。

マルチレベル要約レポート（*マルチレベル要約レポート、196 ページ*参照）と 柔軟な詳細レポート（*柔軟な詳細レポート、197 ページ*参照）によって、さまざまな角度から情報を分析することができます。

他のレポート ビューおよび調査レポートの機能には、ページの上部のリンクからアクセスできます。それぞれのリンクと、そこからアクセスできる機能のリストを下の表に示しています（ページによっては、一部のリンクは使用できません）。

オプション	アクション
User by Day/Month（日 / 月別ユーザ）	特定のユーザーのアクティビティに関する日別または月別レポートを定義するためのダイアログ ボックスが表示されます。詳細については、*User Activity Detail（ユーザー アクティビティ詳細）レポート、203 ページ*を参照してください。
Standard Reports（標準レポート）	事前定義レポートのリストが表示され、これによりデータの特定の組み合わせを速やかに調べることができます。*標準レポート、206 ページ*を参照してください。
Favorite Reports（使用頻度の高いレポート）	これにより現在のレポートを使用頻度の高いレポートとして保存することができるし、また生成またはスケジュール設定ができる既存の Favorites（使用頻度の高いレポート）のリストが表示されます。*使用頻度の高い調査レポート、207 ページ*を参照してください。
Job Queue（ジョブ キュー）	スケジュール設定されている調査レポート ジョブのリストが表示されます。*調査レポートのスケジュール設定、208 ページ*を参照してください。
Outliers（外れ値）	平均と著しく異なるインターネット使用状況を示すレポートが表示されます。*外れ値レポート、213 ページ*を参照してください。
Options（オプション）	レポート作成用に種々のログ データベースを選択するためのページを表示します。[Options] ページによって、要約レポートで最初に示される時間間隔や詳細レポートのデフォルト列などのような一部のレポーティング機能をカスタマイズすることができます。*データベース接続とレポートのデフォルト、535 ページ*を参照してください。

オプション	アクション
	[Search] フィールドの右側にあるこのボタンをクリックすると、現在のレポートが Microsoft Excel 2003 以降と互換のスプレッドシート ファイルにエクスポートされます。 ファイルを開くかまたは保存するかを尋ねられます。*調査レポートの出力のオプション、214 ページ*を参照してください。
	[Search] フィールドの右側にあるこのボタンをクリックすると、現在のレポートが Adobe Reader v7.0 以降と互換の PDF ファイルにエクスポートされます。 ファイルを開くかまたは保存するかを尋ねられます。*調査レポートの出力のオプション、214 ページ*を参照してください。

レポートは Log Database で記録されている情報に限定されます。

- ユーザー名、IP アドレス、または選択カテゴリについてログ記録を無効すると（*要求がログ記録される方法の設定、505 ページ*参照）、その情報は含められません。
- 同様に、特定のプロトコルについてログ記録を無効にすると（*プロトコル フィルタの編集、77 ページ*参照）、それらのプロトコルへの要求は取得できません。
- レポートがドメイン名（www.domain.com）とそのドメインの特定のページへのパス（/products/productA）の両方を示すようにしたい場合は、完全な URL をログ記録させなければなりません（*URL がログ記録される方法の設定、524 ページ*参照）。
- ディレクトリ サービスがユーザーの姓名を含んでいないと、レポートはユーザー名情報を表示できません。

調査レポートは、TRITON 管理サーバーのプロセッサ、使用可能なメモリ、およびいくつかのネットワーク リソースによって制限されます。一部の大きなレポートでは、その生成に長時間かかるでしょう。進捗メッセージにはレポートを [使用頻度の高いレポート] として保存するオプションがあり、そのレポートを後に実行するようにスケジュール設定することができます。*調査レポートのスケジュール設定、208 ページ*を参照してください。

要約レポート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *マルチレベル要約レポート、196 ページ*
- *柔軟な詳細レポート、197 ページ*
- *User Activity Detail（ユーザー アクティビティ詳細）レポート、203 ページ*
- *標準レポート、206 ページ*
- *使用頻度の高い調査レポート、207 ページ*
- *調査レポートのスケジュール設定、208 ページ*
- *外れ値レポート、213 ページ*
- *調査レポートの出力のオプション、214 ページ*

最初に調査レポート ページはすべてのユーザーのリスク クラス別使用状況の要約レポートを表示し、Log Database から本日のアクティビティを示します。この最初の棒グラフの測定基準はヒット件数（サイトが要求された回数）です。この要約レポートの時間間隔の設定については、*データベース接続とレポートのデフォルト、535 ページ*を参照してください。

ページのリンクとオプションを使用して、レポートされる情報を速やかに変更したり、レポートの詳細について絞り込んだりすることができます。

1. **Measure（測定基準）**リストの以下のようなオプションの 1 つを選択することによって、結果を数量化する方式をカスタマイズすることができます。

オプション	説明
Hits（ヒット件数）	URL に対する要求の回数。 Log Server の構成の方法に従って、これはヒット件数またはアクセス件数のいずれかを表します。ヒット件数では、要求されたサイトの個別の要素の個別のレコードをログします。アクセス件数では、サイトの種々の要素を 1 つのログ レコードにまとめます。
Bandwidth（帯域幅）[KB]	ユーザーからの最初の要求と Web サイトからの応答の両方に含まれるデータの量（キロバイト単位）。これは、[Sent（送信済み）] 値と [Received（受信済み）] 値の合計です。 一部の統合製品は、帯域幅データを Filtering Service に送信しません。お客様の統合製品でこの情報が送信されないが、Network Agent がインストールされている場合、**Log HTTP 要求**を有効にして、帯域幅ベースのレポートを可能にします。*NIC の設定、547 ページ*を参照してください。

オプション	説明
Sent（送信済み）[KB]	インターネット要求として送信されたバイト数（キロバイト単位）。これは送信されたデータの量を表します。これは単なる URL 要求であるかもしれず、またはそれ以上のことであるかもしれません（例えば、ユーザーがウェブサイトへ登録するような場合など）。
Received（受信済み）[KB]	要求に対する応答として受信されたデータのバイト数（キロバイト単位）であり、これはページ上のすべてのテキスト、グラフィックス、およびスクリプトを含んでいます。 ブロックされているサイトについては、このバイト数は、ログ記録を作成するソフトウェアによって異なります。Websense Network Agent がレコードをログ記録する場合は、ブロックされているサイトについての受信バイト数は Websense ブロック ページのサイズを表します。 スキャンの結果として Websense Security Gateway によってログ レコードが作成された場合、受信バイト数はスキャンされたページのサイズを表します。詳細については、*Content Gateway 分析、229 ページ*を参照してください。 他の統合製品によりログ レコードが作成される場合、ブロックされたサイトの受信バイト数は 0 となるか、ブロック ページのサイズを表すか、または要求されたサイトから取得した値となります。
Browse Time（ブラウズ時間）	サイトを表示するために要した時間の概算。*インターネット閲覧時間とは何か？、160 ページ*を参照してください。

2. レポートの上にある **Internet Use by（インターネット使用状況）**リストでオプションを選択して、レポートのプライマリ グルーピングを変更します。

   オプションは、Log Database の内容およびいくつかのネットワークの条件によって異なります。たとえば、Log Database 内に 1 つのグループまたはドメインしかない場合、Groups および Domains はこのリストに示されません。同様に、ユーザが多すぎる（5,000 を超える）またはグループが多すぎる（3,000 を超える）場合、これらのオプションは表示されません（これらの制限の一部は設定可能です。*表示および出力のオプション、537 ページ*を参照してください。）

3. 左列の名前（または名前の横の矢印）をクリックして、[by user（ユーザ別）]、[by domain（ドメイン別）]、[by action（アクション別）] などオプションのリストを表示します。

表示されるオプションは [Internet Use by（インターネット使用状況）] の下にリストされたオプションと似ており、現在表示されている内容に対応するサブセットにカスタマイズされています。

> **注意**
>
> [User] や [Group] のようなオプションが 赤い文字表示になっていることがあります。この場合、そのようなオプションを選択すると、非常に大きなレポートが生成され、作成に時間がかかる可能性があります。そのようなオプションを選択する前に、もっと詳細なレベルに絞り込むことを検討してください。

4. これらのオプションのいずれかを選択して、関連するエントリに関する選択した情報を示す新しい要約レポートを作成します。

   例えば、[Risk Class（リスク クラス）] 要約レポート上で [Legal Liability（法的責任）] リスク クラスのもとで [by User（ユーザー別）] をクリックすると、[Legal Liability（法的責任）] リスク クラスの各ユーザーのアクティビティのレポートが生成されます。
5. 左の列の新しいエントリをクリックし、その項目に関する詳細を確認するためのオプションを選択します。
6. 列見出しの横にある矢印を使用して、レポートのソート順序を変更します。
7. グラフの上の以下のオプションを使って要約レポートをコントロールします。次に、新しいレポートの要素をクリックすることによって関連する詳細を表示します。

オプション	アクション
Report path（レポート パス） （[User（ユーザー）] > [Day（日）]）	**[Internet use by（インターネット使用状況）]** リストの横には、現在のレポートの作成に用いた選択を示すパスが表示されます。パス内の任意のリンクをクリックすると、データのそのビューに戻ります。
View（表示）	レポートの期間として次のうちのいずれかを選択します：One Day（1 日）、One Week（1 週間）、One Month（1 カ月）、または All（すべて）。レポートが更新され、選択された期間のデータが示されます。 隣の矢印ボタンを使って、利用できるデータを一度に 1 期間（1 日、1 週間、1 カ月）ずつ移動できます。 この選択を変更すると、**[View from（対象期間）]** フィールドが更新されて、表示される期間が反映されます。 [View from] フィールドまたは [Favorites] ダイアログボックスで特定の日付が選択されていると、**[View]** フィールドには時間の代わりに [カスタム] という語が表示されます。

オプション	アクション
View from... to...（対象期間）	これらのフィールドの日付は、**[表示]** フィールドで変更を行ったとき、表示される時間を反映するように自動的に更新されます。 代わりに、レポートの開始日と終了日を入力するか、またはカレンダ アイコンをクリックして希望する日付を選択することもできます。 日付を選択した後レポートを更新するには、隣の右矢印をクリックします。
Pie Chart（円グラフ）/Bar Chart（棒グラフ）	棒グラフが表示されているとき、**[Pie Chart（円グラフ）]** をクリックすると、現在の要約レポートが円グラフで表示されます。スライス ラベルをクリックすると、棒グラフの左列のエントリをクリックしたとき使用できるのと同じオプションが表示されます。 円グラフが表示されているとき、**[Bar Chart（棒グラフ）]** をクリックすると、現在の要約レポートが棒グラフで表示されます。
Full Screen（全画面）	このオプションを選択すると、現在の調査レポートが、左右のナビゲーションペインのない独立した画面に表示されます。
Anonymous / Names（匿名 / 名前）	• **[Anonymous（匿名）]** をクリックすると、レポートの中のユーザー名を表示する箇所に、内部的に割り当てられたユーザー ID 番号が表示されます。 • 名前が非表示であるとき、**[Names（名前）]** をクリックすると、ユーザー名の表示に戻ります。 ユーザー名を表示できない場合もあります。詳細については、*要求がログ記録される方法の設定、505 ページ*を参照してください。 ユーザー識別情報の非表示に関する詳細については、*調査レポートの匿名化、194 ページ*を参照してください。
Search for（検索対象）	リストからレポート要素を選択し、その横にあるテキストボックスで検索対象の値のすべてまたは一部を入力します。隣の矢印ボタンをクリックして検索を開始し、結果を表示します。 [10.5.] のように部分的 IP アドレスを入力すると、この例では 10.5.0.0 ～ 10.5.255.255 のすべてのサブネットが検索されます。 詳細は、*検索による要約レポートの生成、194 ページ*を参照してください。

8. マルチレベル要約レポートを作成することによって、左列のすべてまたは選択したエントリの情報のサブセットを追加します。*マルチレベル要約レポート、196 ページ*を参照してください。
9. 隣の番号または測定バーをクリックすることによって、左列の特定の項目の表形式のレポートを作成します。この詳細レポートを特定のニーズに対応するように変更できます。*柔軟な詳細レポート、197 ページ*を参照してください。

検索による要約レポートの生成

Investigative Reports のメイン ページの **[Search for（検索対象）]** ボックスは、調べたいインターネット トラフィックまたはクライアント アクティビティに関する情報をすばやく見つけるために使用します。

最初にリストからレポート要素を選択し、次に、レポート対象の文字列のすべてまたは一部を入力します。

検索には下記の要素を利用できます。

- 要求されたウェブサイトの **URL ホスト名**
- ディレクトリ サービスで定義済みの**グループ**
- ディレクトリ サービスで定義済みの**ユーザー**

  ユーザーを選択し、IP アドレスも入力した場合は、選択した IP アドレス（ユーザーが指定されていない）からの要求だけが検索されます。
- 要求の発信元のコンピュータの**ソース IP** アドレス
- 要求されたウェブサイトの **宛先 IP**
- 要求に使用した **ポート**
- 要求の発信元の **ソース IP 範囲**
- 要求の発信元の**複数のソース IP 範囲**（カンマ区切りリスト）

  複数の IP アドレス範囲を入力するとき、その範囲の中の個別の IP アドレスまたはサブ範囲を検索から除外することができます。そのためには感嘆符（!）のあとに除外する IP アドレスまたは範囲を指定します。例：

  ```
  10.21.1.1-10.21.1.10,10.22.55.1-10.22.55.50,!10.22.55.5
  ```

調査レポートの匿名化

Web Security Help | Web Security ソリューション | バージョン 7.8.x

調査レポートで識別情報が表示されるのを避けたい場合、いくつかのオプションがあります。

- 最も確実な方法は、ユーザー名、ソース IP アドレス、およびホスト名のログ記録を行わないことです。この場合、いかなるユーザー識別情報も Log Database に記録されず、この情報を調査またはプレゼンテーション レポートに含めることは不可能になります。手順については、*要求がログ記録される方法の設定、505 ページ*を参照してください。
- 一部の管理者はユーザー情報を含むレポートへのアクセスを必要とし、その他の管理者はユーザー情報を必要としない場合は、指定済み管理ロールによりレポーティング アクセスをコントロールすることができます。調査レポートへのアクセスを付与するロールを作成し、レポート中のユーザー名を非表示にすることができます。詳細については、*代理管理およびレポート作成、405 ページ*を参照してください。
- ユーザー情報を含むレポートを生成しなければならない場合と匿名のレポートを生成しなければならない場合があるならば、[Investigative Reports（調査レポート）] ページの最上部にある **Anonymous（匿名）**オプションを使用して、ユーザー名を非表示にし、オプションとしてソース IP アドレスを一時的に非表示にすることができます。詳細については、*Anonymous（匿名）オプション、195 ページ*を参照してください。

Anonymous（匿名）オプション

Web Security Help | Web Security ソリューション | バージョン 7.8.x

デフォルトでは、**[Anonymous（匿名）]** をクリックすると、レポートでユーザー名だけが非表示になり、ソース IP アドレスの表示は継続します。調査レポートを以下のように設定することによって、Anonymous を選択すると、ユーザー名とソース IP アドレスの両方とも非表示にすることができます：

1. TRITON 管理サーバーで **wse.ini** ファイルをテキスト エディタで開きます。（デフォルトでは、このファイルは C:\Program Files（x86）\Websense\Web Security\webroot\Explorer にあります）。
2. **[explorer]** 見出しの下に次の行を追加します：

   ```
   encryptIP=1
   ```

3. ファイルを保存して、閉じます。

これにより、[Anonymous] をクリックすると、すべてのユーザー情報が表示されなくなります。

[Anonymous] をクリックし、次に詳細ビューや外れ値などの別のデータ 表示に移っても、新しいレポートにおいてユーザー名はやはり表示されません。しかしながら、名前を表示しない要約ビューに戻るには、バナーのブレッドクラムではなく、レポート最上部のリンクを使用しなければなりません。

マルチレベル要約レポート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *調査レポート*、187 ページ
- *要約レポート*、190 ページ
- *柔軟な詳細レポート*、197 ページ
- *User Activity Detail（ユーザー アクティビティ詳細）レポート*、203 ページ
- *標準レポート*、206 ページ
- *使用頻度の高い調査レポート*、207 ページ
- *調査レポートのスケジュール設定*、208 ページ
- *外れ値レポート*、213 ページ
- *調査レポートの出力のオプション*、214 ページ

マルチレベル要約レポートは、表示されるプライマリ情報を補足する二次レベルの情報を提供します。たとえば、プライマリ情報がリスク クラスを表示している場合、各リスク クラスの中の最も要求数が多いカテゴリを調べるために第 2 レベルを定義できます。もう 1 つの例として、プライマリ レポートが各カテゴリへの要求数を示している場合、上位 5 つのカテゴリと、各カテゴリへの要求の上位 10 人のユーザを表示することができます。

これらの設定を要約レポートのすぐ上に置くことによってマルチレベル要約レポートを作成します。

1. **[Select top（上位 ... 件を選択）]** リストで、レポートすべきプライマリ エントリ（左列）の数を選択します。生成されるレポートには、値が最も大きいプライマリ エントリが表示されます（Day（日）がプライマリ エントリである場合、これは最も古い日付を示します。）

   代わりに、左列の個別のエントリの隣のチェックボックスにマークを付けると、それらのエントリのみがレポートされます。**[Select top]** フィールドは **[Custom（カスタム）]** を表示します。
2. **[by（ソート キー）]** リストで、レポートする 2 番目の情報を選択します。
3. **[Display（表示）]** フィールドで、各プライマリ エントリについてレポートするセカンダリ結果の数を選択します。

4. **[Display Results（結果を表示）]** をクリックして、マルチレベル要約レポートを生成します。

   要約レポートは、選択した数のプライマリ エントリだけを表示するように更新されます。各プライマリ エントリのバーの下に、セカンダリ エントリのリストが表示されます。

5. 列見出しの横にある矢印を使用して、レポートのソート順序を変更します。

シングル レベルの要約レポートに戻るには、**[Internet Use by（インターネット使用状況）]** のもとで別のオプションを選択します。代わりに、いずれかのプライマリ エントリまたはセカンダリ エントリをクリックし、その情報に関する新しい調査レポートを生成するためオプションを選択することもできます。

柔軟な詳細レポート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *調査レポート*、187 ページ
- *要約レポート*、190 ページ
- *マルチレベル要約レポート*、196 ページ
- *使用頻度の高い調査レポート*、207 ページ
- *調査レポートのスケジュール設定*、208 ページ
- *外れ値レポート*、213 ページ
- *調査レポートの出力のオプション*、214 ページ
- *データベース接続とレポートのデフォルト*、535 ページ
- *柔軟な詳細レポートの列*、200 ページ

詳細レポートは、Log Database 内の情報を表形式で示します。要約レポートを表示した後、より詳細な情報を得るために、メインページから詳細レポート ビューにアクセスします。

どの行からでも詳細ビューを要求できます。しかし、ヒット件数に基づき詳細レポートを要求する場合、ヒット件数が 100,000 未満の行から開始することを推奨します。行のヒット件数が 100,000 件を超えている場合、ヒット件数が赤で表示され、詳細レポートの生成に時間がかかることを警告します。

詳細レポート ビューは、自分の固有のレポートを設計できるため、柔軟なレポートであると考えられます。情報の列を追加または削除したり、列の表示順序を変更することができます。情報は列の順序に従ってソートされます。さらに、どの列でもソート順序を昇順から降順へ、またはその逆に変更することができます。

Websense 調査レポートは、TRITON 管理サーバーのプロセッサ、使用可能なメモリ、およびいくつかのネットワーク リソースによって制限されます。大きなレポートを要求するとタイムアウトになることがあります。大きなレポートを要求するとき、タイムアウトなしにレポートを生成するオプションが示されます。

重要
どのドロップダウンリストまたは数値リストでも、一部のオプションが赤で表示されることがあります。赤の文字は、このオプションを選択した場合にレポートのサイズが非常に大きくなる可能性があることを警告します。一般的に、そのようなオプションを選択する前に、もっと詳細なレベルに絞り込むことを検討してください。

1. 調査レポートのメインページで、要約レポートまたはマルチレベル レポートを生成します（*要約レポート、190 ページ*または *マルチレベル要約レポート、196 ページ*を参照してください。）
2. 直ちに関係のある情報に絞り込むために結果を絞り込みます。

   ヒット件数に基づきレポートを生成するとき、詳細レポート ビューを開く前に、100,000 未満のヒット件数を示すエントリに絞り込むことを推奨します。
3. より詳細に探索したい行の番号またはバーをクリックします。1 つのレポートに複数の行を含めるには、各行のチェックボックスをオンにしてから行の番号またはバーをクリックします。

   詳細レポートのロード中、ポップアップ メッセージにより進捗状況が示されます。

注意
レポートを作成するのに時間がかかる場合、[ロードしています] というメッセージの中のリンクをクリックすることによって、そのレポートを使用頻度の高いレポートとして保存し、後で実行するようにスケジュールを設定することもできます。*使用頻度の高い調査レポート、207 ページ*を参照してください。

4. 最初のレポートの情報を検討します。

   デフォルト列は、レポートの基準としてヒット件数、帯域幅、ブラウズ時間のどれを選択したか、また、[オプション] ページで何を選択したかによって異なります。（*データベース接続とレポートのデフォルト、535 ページ*を参照してください。）

5. ページ最上部の **[Modify Report（レポートの変更）]** をクリックします。

   Modify Report ダイアログ ボックスの **[Current Report（現在のレポート）]** リストで、現在の詳細レポートで表示される列が示されます。

6. **[Available Columns（使用可能な列）]** または **[Current Report]** リストで列名を選択し、右向き矢印（>）ボタンまたは左向き矢印（<）ボタンをクリックして、その列を他方のリストに移します。

   レポートに対して最大 7 つの列を選択できます。最初の要約レポートで指定されている測定基準（ヒット件数、帯域幅、ブラウズ時間）を示す列は、常に右端の列として表示されます。レポートを変更するとき、この列は選択対象としては表示されません。

   利用できる列のリストと各列の説明を*柔軟な詳細レポートの列、200 ページ*に示しています。

7. **[Current Report（現在のレポート）]** リストで列名を選択し、上および下矢印ボタンを使用して、列の順序を変更します。

   [Current Report] リストで上に表示される列が、レポートでは左に表示されます。

8. レポートの上にある **[Summary（要約）]** または **[Detail（詳細）]** リンクをクリックすると、表示が切り替わります。

オプション	説明
要約	要約レポートを表示するには [Time（時間）] 列を削除する必要があります。要約レポートは、特定の要素を共有するすべてのレコードを 1 つのエントリにまとめます。この要素は、レポートされる情報によって異なります。一般に、測定基準の前の右端の列は要約された要素を示します。
Detail（詳細）	[Detail] オプションはすべてのレコードを独立した行として表示します。[Time] 列を表示できます。

9. **[Submit（送信）]** をクリックして、定義したレポートを生成します。
10. 表示されたレポートを変更するには、以下のオプションを使用します。
    - レポートの対象となる期間を変更するには、レポートの上の **[View]** オプションを使用します。
    - 列および関連付けられたデータのソート順序を逆にするには、列見出しの横の上または下矢印をクリックします。
    - レポートの追加のページ（もしあれば）を表示するには、レポートの上および下にある **[Next]** および **[Prev]** リンクを使用します。デフォルトでは、1 つのページに 100 行が表示されますが、これは必要に応じて調整できます。*表示および出力のオプション、537 ページ*を参照してください。
    - 要求したウェブサイトを新しいウィンドウで開くには、URL をクリックします。

11. レポートを保存して、それをすぐに、または定期的に再生成できるようにするには、**[Favorite Reports]** をクリックします。（*使用頻度の高いレポートの使用、175 ページ*を参照してください）。

柔軟な詳細レポートの列

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *柔軟な詳細レポート、197 ページ*
- *使用頻度の高い調査レポート、207 ページ*
- *調査レポートのスケジュール設定、208 ページ*

詳細レポートで利用できる列について、以下の表で説明しています（*柔軟な詳細レポート、197 ページ*を参照してください）。

常にすべての列が使用できるわけではありません。たとえば、[User] 列が表示される場合、[Group] 列は使用できません。[Category] 列が表示される場合、[Risk Class] 列は使用できません。

列名	説明
User（ユーザー）	要求を行ったユーザーの名前。ユーザー情報をレポートに含めるためには、それがログ データーベースに登録されている必要があります。ユーザー ベースのレポートではグループ情報は利用できません。
Day（日）	インターネット要求が行われた日付。
URL Hostname（URL ホスト名）	要求されたサイトのドメイン名（[ホスト名] とも言います）。
Domain（ドメイン）	要求を行ったディレクトリ ベースのクライアント（ユーザー、グループ、ドメイン、または組織単位）のディレクトリ サービス ドメイン。
Group（グループ）	要求者が属しているグループの名前。個々のユーザー名はグループ ベースのレポートには示されません。サイトを要求したユーザーがディレクトリ サービス内の 2 つ以上のグループに属している場合、レポートはこの列に複数のグループをリストします。
Risk Class（リスク クラス）	要求されたサイトが属しているカテゴリに関連付けられているリスク クラス。カテゴリが複数のリスク クラスに含まれている場合、すべての関連するリスク クラスがリストされます。*カテゴリのリスク クラスへの割り当て、502 ページ*を参照してください。

列名	説明
Directory Object（ディレクトリ オブジェクト）	要求を行ったユーザーのディレクトリ パス（ユーザー名を除く）。一般的に、同じトラフィックについて複数の行が作成されます。なぜなら各ユーザーは複数のパスに属しているからです。 LDAP 以外のディレクトリ サービスを使用する場合は、この列は利用できません。
Disposition（処置）	要求に対応して実行するアクション（例、[カテゴリーを許可]、[カテゴリをブロック]）。
Source Server（送信元サーバー）	Filtering Service に要求を送信しているコンピュータの IP アドレス。スタンドアロン型の配備では、これは Network Agent IP アドレスです。統合されたネットワークでは、これは、ゲートウェイ、ファイアウォール、またはキャッシュの IP アドレスです。 Websense Web Security Gateway Anywhere では、このオプションを使用して、オンサイト（フィルタリングされた場所）とオフサイトの両方のユーザーからの、ハイブリット サービスによってフィルタリングされた要求を特定します。
Protocol（プロトコル）	要求のプロトコル（例、HTTP、FTP）。
Protocol Group（プロトコル グループ）	要求されたプロトコルが含まれているマスタ データベース グループ（例、リモート アクセス、ストリーミング メディア）。
Source IP（送信元 IP）	要求を行ったコンピュータの IP アドレス Websense Web Security Gateway Anywhere では、このオプションを使用して、特定のハイブリッド フィルタリングされた場所からの要求を確認できます。*フィルタ対象の場所を定義、263 ページ*を参照してください。
Destination IP（宛先 IP）	要求されたサイトの IP アドレス。
Full URL（完全 URL）	要求されたサイトのドメイン名とパス（例、http://www.mydomain.com/products/itemone/）。完全な URL をログ記録していない場合、この列は空白になります。*URL がログ記録される方法の設定、524 ページ*を参照してください。
Month（月）	要求が行われた暦月。
Port（ポート）	ユーザーがサイトとの通信で使用した TCP/IP ポート。

列名	説明
Bandwidth（帯域幅）	ユーザーからの最初の要求と Web サイトからの応答の両方に含まれるデータの量（キロバイト単位）。これは、[Sent（送信済み）] 値と [Received（受信済み）] 値の合計です。 一部の統合製品は、帯域幅データを Filtering Service に送信しません。統合製品がこの情報を送信しない場合、Websense Network Agent がインストールされていれば、対応する NIC の **[Log HTTP requests（HTTP 要求をログ）]** オプションをオンにして、帯域幅情報に関するレポートを有効化してください。*NIC の設定*、547 ページを参照してください。
Bytes Sent（送信バイト数）	インターネット要求として送信したバイトの数。これは、送信したデータの量を表します。これは単なる URL の要求である場合があり、また、たとえばユーザーが Web サイトへの登録を行っている場合のように、もっと多くのデータが送信される場合もあります。
Bytes Received（受信バイト数）	要求に対する応答としてインターネットから受信したバイトの数。これは、サイトを構成するすべてのテキスト、グラフィック、およびスクリプトを含みます。 ブロックされているサイトについては、このバイト数は、ログ レコードを作成するソフトウェアによって異なります。Websense Network Agent がレコードをログ記録するとき、ブロックされているサイトの受信バイト数は、ブロック ページのサイズを表します。 スキャンの結果として Websense Security Gateway によってログ レコードが作成された場合、受信バイト数はスキャンされたページのサイズを表します。詳細については、*Content Gateway 分析*、229 ページを参照してください。 他の統合製品がログ レコードを作成した場合、ブロックされたサイトの受信バイト数は 0 とされるか、ブロック ページのサイズを表すか、または要求されたサイトから取得した値となります。
Time（時刻）	サイトが要求された時刻。24 時間クロックを使用し、HH:MM:SS（時間：分：秒）の形式で表示されます。
Category（カテゴリ）	要求が割り当てられたカテゴリ。これは、マスタ データベースのカテゴリ、またはカスタム カテゴリです。

User Activity Detail（ユーザー アクティビティ詳細）レポート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *調査レポート、187 ページ*

[User by Day/Month（日 / 月別ユーザー）] リンクをクリックして、1 人のユーザーの [User Activity Detail（ユーザー アクティビティ詳細）] レポートを生成します。このレポートは、そのユーザーの 1 日または 1 カ月間のインターネット アクティビティのグラフィカルな分析を示します。

最初に、特定のユーザーの選択した日のレポートを生成します。このレポートから、同じユーザーによる 1 カ月間のインターネット アクティビティについてのレポートを生成することができます。手順の詳細については、以下を参照してください：

- *日付別ユーザー アクティビティ詳細、203 ページ*
- *月別ユーザー アクティビティ詳細、205 ページ*

日付別ユーザー アクティビティ詳細

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *調査レポート、187 ページ*
- *User Activity Detail（ユーザー アクティビティ詳細）レポート、203 ページ*
- *月別ユーザー アクティビティ詳細、205 ページ*

User Activity Detail by Day（日付別ユーザー アクティビティ詳細）レポートは、特定のユーザーによる特定日のアクティビティの詳細なビューを提供します。

1. メイン ページの上部の **[User by Day/Month（日 / 月別ユーザー）]** を選択します。[User Detail by Day（日付別ユーザー詳細）] ダイアログボックスが表示されます。
2. **[Search for user（ユーザの検索）]** フィールドでユーザの名前またはその一部を入力し、つづいて **[Search]** をクリックします。

   検索の結果、ログ データベースから条件に一致する最大 100 件のユーザ名が抽出され、スクロール可能なリストに表示されます。
3. **[Select user（ユーザーの選択）]** リストからユーザーを選択します。

4. **[Select day（日付の選択）]** フィールドで、最後の活動の日付（デフォルトで表示される）を受け入れるか、または別の日付を選択します。

   新しい日付を入力するか、またはカレンダ アイコンをクリックして日付を選択します。カレンダ選択ボックスは、アクティブなログ データベースに含まれる日付の範囲を示します。

5. **[Go to User by Day（日別ユーザに移動）]** をクリックして、要求した日付のそのユーザの活動の詳細なレポートを表示します。

   最初のレポートは、ユーザーの活動を 5 分刻みの時系列で表示します。各要求は Websense マスタ データベースのカテゴリに対応するアイコンとして表示されます。すべてのカスタム カテゴリは 1 つのアイコンで表されます（アイコンの色は、[User Activity by Month] レポートに表示されるリスク グループに対応します）。

   アイコン上にマウスを置くと、関連付けられている要求の正確な時刻、カテゴリ、およびアクションが表示されます。

   下にリストしているコントロールを使って、レポートの表示を変更したり、凡例を表示できます。

オプション	説明
Previous Day / Next Day（前日 / 翌日）	このユーザーの前または次の暦日のインターネット アクティビティを表示します。
Table View（一覧表示）	要求された各 URL のリストを、要求の日付および時刻、カテゴリ、実行された処置（ブロック、許可、その他）と共に表示します。
Detail View（詳細ビュー）	レポートの最初のグラフィカル ビューを表示します。
Group Similar Hits / View All Hits（類似ヒットのグループ化 / すべてのヒットの表示）	10 秒以内の間隔で行われ、ドメイン、カテゴリ、および処置も同じであるすべての要求を 1 つの行にまとめます。それによって、情報がより簡潔な要約ビューとして表示されます。 標準の時間しきい値は 10 秒です。この値の変更が必要である場合は、*表示および出力のオプション、537 ページ*を参照してください。 このリンクをクリックすると、View All Hits（すべてのヒットの表示）に戻り、各要求の元のリストが復元されます。
Category View Control（カテゴリ表示の制御）	現在のレポート内の各カテゴリのカテゴリ名とそのカテゴリを表すアイコンのリストを表示します。 カテゴリのチェックボックスをオン / オフにすることによって、レポートにどのカテゴリを表示するかを制御します。次に、**[Accept]** をクリックすることによって、この選択に従ってレポートを更新します。

6. レポートの上にある **[User Activity Detail by Month（月別ユーザー アクティビティ詳細）]** をクリックして、同じユーザーによる 1 カ月間のアクティビティを表示します。詳細は、*月別ユーザー アクティビティ詳細*、205 ページを参照してください。

月別ユーザー アクティビティ詳細

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *調査レポート*、187 ページ
- *User Activity Detail（ユーザー アクティビティ詳細）レポート*、203 ページ
- *日付別ユーザー アクティビティ詳細*、203 ページ

User Activity Detail by Day（日付別ユーザー アクティビティ詳細）レポートが開いているとき、そのユーザーの月間アクティビティに切り替えることができます。

1. [User Activity Detail by Day（日別ユーザー アクティビティ詳細）] レポートを開きます。*日付別ユーザー アクティビティ詳細*、203 ページを参照してください。
2. 上部の **[User Activity Detail by Month（月別ユーザー アクティビティ詳細）]** をクリックします。

   新しいレポートによってカレンダーの画像が表示されますが、その各々の日付で色付きのブロックが示されていて、これはユーザーによる当日のインターネット アクティビティを表しています。カスタム カテゴリに含まれるサイトへの要求はグレイのブロックで示されます。
3. 左上の **[Database Category Legend（データベース カテゴリ凡例）]** をクリックして、それぞれの色が要求されたサイトの潜在的リスクの大きさとどのように対応しているかを確認してください。

   カテゴリ割り当ては固定されており、変更できません。
4. **[Prev（前）]** または **[Next（次）]** をクリックすると、当該ユーザーによる前月または翌月のインターネット アクティビティが表示されます。

標準レポート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *調査レポート、187 ページ*
- *使用頻度の高い調査レポート、207 ページ*
- *調査レポートのスケジュール設定、208 ページ*

標準レポートによって、絞り込みを利用せずに、特定のグループの情報をすみやかに表示することができます。

1. メイン [Investigative Reports（調査レポート）] ページで **Standard Reports（標準レポート）** リンクをクリックします。
2. 必要とされる情報を含んでいるレポートを選択します。以下のようなレポートが利用できます。

Highest Activity Levels（最高アクティビティ レベル）

- ヒット件数が最も多かったのはどのユーザーか？
- アクセス件数上位 10 URL の上位 10 ユーザ
- ショッピング、エンターテイメント、およびスポーツでアクティビティが活発だった上位 5 ユーザ
- アクセス件数上位 5 カテゴリの上位 5 URL

Highest Bandwidth Consumption（最高の帯域幅消費）

- 帯域幅を最も消費しているのはどのグループか
- ストリーミング メディアで帯域幅を最も多く消費しているグループ
- ユーザーについてのネットワーク帯域幅損失別詳細 URL レポート
- 各帯域幅カテゴリの上位 10 グループ

Most Time Online（最長時間のオンライン）

- どのユーザーのオンライン時間が最も長かったか
- どのユーザーが生産性カテゴリのサイトで最も長時間費やしたか

Most Blocked（最多のブロック回数）

- どのユーザーが最も多くブロックされたか？
- どのサイトが最も多くブロックされたか？
- ブロックされたユーザーについての詳細 URL レポート
- ブロックされた上位 10 カテゴリ

Highest Security Risk（最高のセキュリティ リスク）

- セキュリティ リスクがある上位カテゴリ
- P2P プロトコル使用の上位ユーザ
- セキュリティ カテゴリに属するサイトの上位ユーザー
- スパイウェア アクティビティが認められた上位 10 コンピュータの URL

Legal Liability（法的責任）

- カテゴリ別法的責任リスク
- アダルト カテゴリの上位ユーザー

3. 表示されるレポートを調べます。
4. このレポートを使用頻度の高いレポートとして保存し、繰り返し実行するようにスケジュール設定することができます。*使用頻度の高い調査レポート、207 ページ*を参照してください。

使用頻度の高い調査レポート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *調査レポート、187 ページ*
- *調査レポートのスケジュール設定、208 ページ*

ほとんどの調査レポートを **Favorites（使用頻度の高いレポート）**として保存することができます。これには、特定の情報に絞り込んで生成されたレポート、標準レポート、および特定の必要に基づいて変更された詳細レポートが含まれます。こうして、使用頻度の高いレポートをいつでも実行できるし、またそれが特定の日時に実行されるようにスケジュール設定することができます。

指定済み管理を利用する組織では、使用頻度の高いレポートの保存およびスケジュール設定をおこなう許可は Super Administrator（優先管理者）によって付与されます。この許可を付与された管理者が実行およびスケジュール設定できるのはその管理者が保存した使用頻度の高いレポートだけであり、他の管理者によって保存された使用頻度の高いレポートにはアクセスできません。

レポートを Favorite（使用頻度の高いレポート）として保存するには、下記の手順を実行します。

1. 必要とされるフォーマットと情報に基づいてレポートを生成します。
2. **[Favorite Reports（使用頻度の高いレポート）]** をクリックします。

3. デフォルト名を受け入れるかまたは変更します。

   この名前では、英字、数字、およびアンダースコア（_）使用できます。空白やその他の特殊文字は使用できません。

4. **[Add（追加）]** をクリックします。

   レポート名が使用頻度の高いレポートのリストに追加されます。

使用頻度の高いレポートのリストから、いつでも使用頻度の高いレポートを生成でき、また不用となったのを削除することができます。

1. **[Favorite Reports]** をクリックして、[使用頻度の高いレポート] として保存されているレポートのリストを表示します。
2. リストからレポートを選択します。
3. 以下のいずれかを行います：
   - **[Run Now（すぐに実行）]** をクリックして、選択したレポートを直ちに生成し、表示します。
   - **[Schedule（スケジュール設定）]** をクリックして、レポートを後で実行させるか、または繰り返しベースで実行させるようにスケジュール設定します。詳細については、*調査レポートのスケジュール設定、208 ページ*を参照してください。
   - **[Delete（削除）]** をクリックして、使用頻度の高いレポートのリストからレポートを削除します。

[Favorite Reports] ページから既存の使用頻度の高いレポートと類似する新しい使用頻度の高いレポートを作成できます。

1. **[Favorite Reports]** をクリックして、[使用頻度の高いレポート] として保存されているレポートのリストを表示します。
2. 作成しようとする新しいレポートに最も似ている既存の [使用頻度の高いレポート] を選択して、実行します。
3. 表示されたレポートに必要な変更を加えます。
4. **[Favorite Reports]** をクリックして、変更されたレポートを新しい名前で [使用頻度の高いレポート] として保存します。

調査レポートのスケジュール設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *使用頻度の高い調査レポート、207 ページ*
- *使用頻度の高い調査レポート、207 ページ*
- *スケジュール設定調査レポート ジョブの管理、212 ページ*

調査レポートを後に実行させるか、または繰り返しベースで実行させるようにスケジュール設定するためには、あらかじめそのレポートを [使用頻度の高いレポート] として保存しておかねばなりません。スケジュール設定レポート ジョブが実行されると、生成されたレポートは電子メールによって指定の受信者に送られます。スケジュール設定ジョブを作成するとき、お客様の電子メール サーバーが添付のレポート ファイルのサイズと量を処理できるかどうか確認してください。

スケジュール設定レポートのファイルは次のディレクトリに保存されます：

```
<install_path> \webroot\Explorer\<name> \
```

デフォルトのインストールパスは、C:\Program Files（x86）\Websense\Web Security です。スケジュール設定ジョブの受信者が 1 人である場合、*<name>* が電子メール アドレスの最初の部分（[@] の前）になります。受信者が複数の場合は、レポートは "Other" というディレクトリに保存されます。

注意

繰り返しのジョブから保存されたレポートでは、毎回、同じファイル名が使用されます。ファイルを 1 サイクル終了後も保存したい場合は、ファイル名を変更するか、ファイルを別の場所へ移動してください。

スケジュール設定されているレポートのサイズと数によっては、そのディレクトリは非常に大きくなるかもしれません。定期的にディレクトリをクリアし、不要なレポート ファイルを除去してください。

1. 1 つ以上のレポートを[使用頻度の高いレポート]として保存します。（*使用頻度の高い調査レポート、207 ページ*を参照してください。）
2. **[Favorite Reports]** をクリックして、[使用頻度の高いレポート] として保存されているレポートのリストを表示します。

注意

組織で指定済み管理ロールを利用していると、このリストには他の管理者によって保存された [使用頻度の高いレポート] は含まれません。

3. ジョブの中で実行するレポート（5 つまで）をハイライトします。
4. **[Schedule]** をクリックして、スケジュール設定レポートジョブを作成し、つづいて [Schedule Report（レポートのスケジュール設定）] ページで必要な情報を与えます。

Log Database の過負荷を防止し、ログ記録および対話的レポーティングのパフォーマンス低下を避けるために、レポート ジョブの実行スケジュールを異なる日時に設定すべきです。

フィールド	説明
Recurrence（実行頻度）	レポート ジョブを実行する頻度（Once（1 回だけ）、Daily（毎日）、Weekly（毎週）、Monthly（毎月））を選択します。
Start Date（開始日）	ジョブを最初に（または 1 回だけ）実行させる曜日または暦日を選択します。
Run Time（実行時刻）	ジョブを実行させる時刻を設定します。
Email to（電子メール送信先）	**[Additional Email Addresses（追加の電子メール アドレス）]** フィールドをクリックし、必要なアドレスをこのリストに追加します。 ジョブによるレポートを受け取る 1 つ以上の電子メール アドレスを強調表示にします。（レポートを受け取るべきでないアドレスが選択されていれば、取り消してください。）
Additional Email Addresses（追加の電子メール アドレス）	電子メール アドレスを入力し、**[Add（追加）]** をクリックして、そのアドレスを **Email to（電子メール送信先）** リストに入れます。 新しい電子メール アドレスは、選択されている他の電子メール アドレスと共に自動的に強調表示になります。
Customize email subject and body text（電子メール件名および本文のカスタマイズ）	このチェックボックスをオンにして、電子メール通知の件名と本文をカスタマイズします。 このチェックボックスがオンになっていないと、デフォルトの件名と本文が使用されます。
Email Subject（電子メール件名）	スケジュール設定レポートの配布時に電子メール件名行で表示されるテキストを入力します。 デフォルトの電子メール件名は次のとおりです： Investigative Reports scheduled job （調査レポートのスケジュール設定ジョブ）

フィールド	説明
Email Text（電子メール テキスト）	スケジュール設定ジョブを配布する電子メール メッセージに追加されるテキストを入力します。 電子メールの内容は以下のようになり、このフィールドで設定されたテキストが <CUSTOM TEXT> 部分に入ります。 添付のファイルは Report Scheduler により [日時] に作成されました。 <CUSTOM TEXT> 作成されたレポートを表示するには、以下のリンクをクリックしてください。 注意：ジョブ送信元の Web サーバへのアクセス許可が受信者にない場合、このリンクは機能しません。
Schedule Job Name（スケジュール設定ジョブ名）	スケジュール設定ジョブに一意の名前を与えます。この名前によって、ジョブが Job Queue（ジョブ キュー）中で特定されます。*スケジュール設定調査レポート ジョブの管理、212 ページ*を参照してください。
Output Format（出力フォーマット）	スケジュール設定レポートのためのファイル フォーマットを選択します： **PDF**:Portable Document Format ファイルは Adobe Reader で表示されます。 **Excel**:Excel スプレッドシート ファイルは Microsoft Excel で表示されます。
Date Range（日付範囲）	ジョブによるレポートによってカバーされる日付範囲を設定します。 **All Dates（すべての日付）**：Log Database 中のすべての日付。 **Relative（相対）**：期間（Days（日）、Weeks（週）、または Months（月））と含めるべき期間の特定（This（今）、Last（前）、Last 2（過去 2）、等々）を選択します。 **Specific（特定）**：ジョブによるレポートについて特定の日付または日付の範囲を設定します。

5. **[Next（次へ）]** をクリックして、[Schedule Confirmation（スケジュールの確認）] ページを表示します。
6. **[Save（保存）]** をクリックして、選択項目を保存し、[Job Queue（ジョブ キュー）] ページへ進みます（*スケジュール設定調査レポート ジョブの管理、212 ページ*を参照してください）。

スケジュール設定調査レポート ジョブの管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *調査レポート、187 ページ*
- *プレゼンテーション レポートのスケジュール設定、177 ページ*

調査レポートのスケジュール設定ジョブを作成するとき、**[Job Queue]** ページが表示され、新しいジョブと既存のスケジュール設定ジョブのリストが示されます。メイン調査レポート ページ上の **[Job Queue]** リンクをクリックすることでも、このページにアクセスすることができます。

注意
組織で指定済み管理を利用していると、このページでは他の管理者によってスケジュール設定されたジョブは表示されません。

Schedule Report Detail（スケジュール設定レポート詳細）セッションでは、スケジュール設定ジョブがその作成順にリストアップされ、各ジョブの設定スケジュールとステータスの概要が示されます。さらに、以下のオプションが利用できます。

オプション	説明
Edit（編集）	ジョブで設定されているスケジュールが表示され、必要に応じて、それを変更することができます。
Delete（削除）	ジョブを削除し、Status Log（ステータス ログ）セッションにエントリを追加して、当該ジョブを [Deleted（すでに削除）] として示されるようにします。

Status Log セッションでは、なんらかの変更があったジョブがリストアップされ、各ジョブのスケジュール設定開始時刻、実際の終了時刻、およびステータスが示されます。

[Clear Status Log（ステータス ログのクリア）] をクリックして、Status Log セッションのすべてのエントリを消去します。

外れ値レポート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *調査レポート、187 ページ*
- *要約レポート、190 ページ*

Outliers（外れ値）レポートは、データベースで最も異常なインターネット アクティビティが認められるユーザーを示します。レポート クエリーは、すべてのユーザのアクティビティについてカテゴリ別、日付別、処置（ディスポジション）別、プロトコル別に計算して、アクティビティの平均を求めます。つづいて、このソフトウェアは、その平均から統計的に最も顕著に偏差しているユーザー アクティビティを示します。偏差は平均値からの標準偏差として計算されます。

1. メイン [Investigative Reports] ページで、外れ値を調べようとする情報を含む要約レポートを生成します。Internet Use by（インターネット使用状況）フィールドの横で下線入りのブルー表示になっているレポートの選択は、外れ値レポートで反映されます。

   例えば、特定のカテゴリについてヒット件数の外れ値を表示するには、**Internet Use by** リストで **Category（カテゴリ）**を選択し、つづいて **Hits（ヒット件数）**を **Measure（測定基準）**として選択します。

   注意
   外れ値レポートは、ブラウズ時間については作成できません。ブラウズ時間を示す要約レポートから始めても、外れ値レポートのベースになるのはヒット件数です。

2. **[Outliers（外れ値）]** をクリックします。

   行は降順にソートされ、偏差が最も大きいものが最初に表示されます。各行で以下の事項が示されます：

   - 特定ユーザー、カテゴリ、プロトコル、日付、および処置についてのトータル（ヒット件数または帯域幅）。
   - 当該のカテゴリ、プロトコル、日付、および処置に関する、すべてのユーザーについての平均（ヒット件数または帯域幅）。
   - 特定ユーザーの平均からの偏差。

3. 当該カテゴリにおける個別のユーザによる一定期間内のアクティビティを調べるには、ユーザ名をクリックします。

   例えば、あるユーザーによる特定の日付のアクティビティが著しく活発である場合に、そのユーザーの名前をクリックして、そのユーザーの全体的アクティビティのより詳細な理解を可能にするレポートを調べることができます。

調査レポートの出力のオプション

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *調査レポート*、187 ページ

調査レポートを生成したら、レポートの上のボタンによってレポートをファイルとして保存することができます。クリックするボタンによって、そのファイルのフォーマットが決まります。

オプション	説明
	レポートを XLS フォーマットで保存します。 TRITON コンソールにアクセスしているコンピュータで Microsoft Excel 2003 以降がインストールされていると、レポートの表示または保存を促されます。インストールされていないと、ディレクトリを選択し、保存されるレポートのファイル名を選択するように促されます。 Microsoft Excel のオプションを使用して、レポートの印刷、保存、または電子メール送信を行います。
	レポートを PDF フォーマットで生成します。 TRITON コンソールにアクセスしているコンピュータで Adobe Reader v7.0 以降がインストールされていると、レポートの表示または保存を促されます。インストールされていないと、ディレクトリを選択し、保存されるレポートのファイル名を選択するように促されます。 Adobe Reader のオプションを使用して、レポートの印刷、保存、または電子メール送信を行います。

また下記のように調査レポートを印刷することもできます。

- レポートを表示しているときに、ブラウザの印刷機能を使用します。
- 上記の説明に従って、PDF または XLS ファイルを作成し、次に Adobe Reader または Microsoft Excel の印刷機能を使用します。

レポートはブラウザにより正常に印刷されるようになっていますが、結果を確認するためにテスト印刷を行うこともできます。

User Activity Detail by Month（月別ユーザー アクティビティ詳細レポート）レポートは横方向モードで印刷されるようになっています。その他のレポートはすべて縦方向モードになっています。

ユーザー独自のデザインによるレポートでは（*柔軟な詳細レポート、197 ページ*参照）、レポートに含まれる情報によって列の幅が異なります。レポートの幅が 8 1/2 インチ以上であると、そのページは横方向になります。

ページのコンテンツの幅は 7 1/2 インチまたは 10 インチです。A4 版の場合、余白が少し狭くなりますが、印刷範囲に収まります。（ページ サイズのデフォルトは レター サイズまたは 8.5 x 11 インチです。A4 用紙を使用する場合、wse.ini ファイルでこの設定を変更してください。*表示および出力のオプション、537 ページ*を参照してください。）

セルフレポートへのアクセス

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *調査レポート、187 ページ*
- *レポートの優先設定、503 ページ*
- *セルフレポーティング、540 ページ*

Websense セルフレポートによって、ユーザー自身のインターネット ブラウズ アクティビティを評価し、適宜、そのアクティビティを組織のガイドラインに合致するように調整することができます。これによって、ユーザーが自分について収集された情報の種類を確認できるようにすることを組織に要求する政府規制にも対応することもできます。

セルフレポートが有効になっていると、各自のブラウザからそれにアクセスすることができます。

1. Web Security 管理者によって提供された URL を入力するか、TRITON コンソールのログオン ページの [Self-Reporting（セルフレポート）] リンクをクリックし、セルフレポート ログオン ページにアクセスします。
2. **Policy Server（ポリシー サーバー）**がドロップダウン リストを表示すれば、ユーザー自身のインターネット アクティビティに関する情報をログ記録している Policy Server の IP アドレスを選択します。

   問題があれば、Web Security 管理者に連絡してください。
3. ネットワークへのログオンで使用する **User name（ユーザー名）**と **Password（パスワード）**を入力します。
4. **[Log On（ログオン）]** をクリックします。

Web Security manager が、ユーザー自身のリスク クラス別インターネット アクティビティを示す調査レポートを表示します。ページ上で種々のリンクや要素をクリックして、ユーザー自身のアクティビティについて保存されている情報を異なる角度から示す他のオプションを利用することができます。レポートでの作業で問題があれば、**Help**（ヘルプ）システムを利用してください。

アプリケーション レポートの作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ユーザー エージェント データを収集する方法*、219 ページ
- *ブラウザ使用状況の詳細*、221 ページ
- *プラットフォーム使用状況の詳細*、222 ページ

Web Security Gateway および Gateway Anywhere 環境、ならびにスタンドアロン Web Security および Web Filter 環境では、**[Reporting] > [Applications]** ページを使用してネットワーク内でのウェブ要求の作成に使用しているブラウザおよびオペレーティング システムを検討します。また [Search] タブを使用してユーザー エージェント文字列に基づいてアクティビティを調査します（ユーザー エージェント文字列は、要求の発信元のクライアント ソフトウェアを識別する HTTP ヘッダーです）。

- セキュリティの脆弱性をもたらす可能性のある古いブラウザのインスタンスを見つける。
- ゼロデイ エクスプロイトが発見されたときに脆弱性をもたらす可能性があるネットワーク内のコンピュータを特定する。
- 新しいブラウザまたはオペレーティング システムの導入を追跡する。
- アプリケーションに関連するユーザー エージェント文字列を使用して、ネットワーク内でそのアプリケーションが実行しているコンピュータを特定する。
- マルウェアまたは疑わしいアクティビティと関連するユーザー エージェント文字列を検索して、リスクにさらされている可能性があるコンピュータを特定する。

Web Security および Web Filter がサードパーティのプロキシ、キャッシュ、ファイアウォールまたは他のデバイスと統合されている環境では、統合製品は Websense Filtering Service にアプリケーション データを送信しません。そのため、[Applications（アプリケーション）] ページにはデータは表示されません。

重要
新規インストールまたはアップグレードの後、夜間のデータベース ジョブが実行されるまで、[Applications] ページの [Browser] または [Source Platform] タブにデータは表示されません。ユーザーがインターネットに接続すると、新しいユーザー エージェント文字列が [Search] タブに表示されますが、この文字列は、このジョブが実行されるまでは、認識されているブラウザおよびプラットフォームに置換されません。

ユーザー エージェント データが、ログ記録され、処理され、レポートに表示される方法については、*ユーザー エージェント データを収集する方法*、219 ページを参照してください。

[Applications] ページは下の 3 つのタブで構成されています。

- **[Browser]** タブのレポートは、サポートされていて、ネットワークからインターネットにアクセスするために使用されているブラウザ ファミリー（Microsoft Internet Explorer、Mozilla Firefox、Google Chrome、Safari、Opera のデスクトップおよびモバイル バージョン含む）とそのバージョンを示します。

  [Browser] タブは、[Applications] ページに移動したときにデフォルトで選択されます。
- **[Source Platform（ソース プラットフォーム）]** タブ上のレポートは、サポートされていて、インターネットにアクセスしているブラウザが実行しているオペレーティング システム（Windows、Linux、UNIX、OS X、iOS、Android、BlackBerry、Symbian、Java ME など）を示します。
- **[Search（検索）]** タブを使用して、ネットワーク内で検出されたユーザー エージェント ヘッダーに含まれる特定の文字列を検索できます。検索結果は、条件に適合するユーザー エージェントを、要求数または帯域幅の大きい順で示します。

どのタブでも、タブの上部のドロップダウン リストから代替の**期間**を選択できます。デフォルトでは、グラフおよびテーブルに 30 日分の情報（もしあれば）が表示されます。

使用している SQL サーバーが Microsoft SQL Server の標準バージョンまたはエンタープライズ バージョンか、Microsoft SQL Server Express かによって、異なる期間が選択可能です。

[Browser] および [Source Platform] タブでは、ページに表示される情報を制限するために **[Device type（デバイス タイプ）]**（デスクトップまたはモバイル）を選択できます。デフォルトでは、デスクトップとモバイルの両方のブラウザまたはプラットフォームの情報が表示されます。

[Browser] タブと [Source Platform] タブの両方に、ブラウザまたはプラットフォーム、およびバージョンをリストするテーブルが含まれます。

- **[Type]** 列のアイコンは、ブラウザまたはプラットフォームがデスクトップ コンピュータ用かモバイル デバイス用かを示します。
- 隣の列は、ブラウザ ファミリーまたはオペレーティング システム プラットフォームの名前を示します。
- **[Lowest Version（最下位バージョン）]** の値と **[Highest Version（最上位バージョン）]** の値は、選択した期間中にネットワークで使用されたバージョンの範囲を示します。
- 指定したタイプのブラウザのうち要求を作成するために実際に使用されたブラウザ、または、要求の発信元となったソース プラットフォームの**数**。このカウントは、ブラウザまたはオペレーティング システムに関連づけられている一意なクライアント IP アドレスの数に基づいて行われます。

選択したブラウザ ファミリー、プラットフォーム、またはバージョン番号に関する詳細な情報を示す詳細レポートを表示するには、テーブルのリンクをクリックします。詳細は、*ブラウザ使用状況の詳細、221 ページ*または*プラットフォーム使用状況の詳細、222 ページ*を参照してください。

ネットワークで頻繁に使用されているブラウザ ファミリーまたはオペレーティングシステムを表示するには **[Browser Family（ブラウザ ファミリー）]** または **[Platform Comparison（プラットフォームの比較）]** を使用し、各ブラウザまたはオペレーティング システムの経時的な使用状況を追跡するには **[Browser]** または **[Platform Use Trend（プラットフォーム使用傾向）]** グラフを使用します。

どのグラフでも、情報の表示方法を変更するには、別の **[Chart type（グラフのタイプ）]** を選択します。

[Search] タブは最初に、要求の数に基づき上位 10 のユーザー エージェントを表示します。特定のユーザー エージェントのデータベースを検索するには、**[User agent（ユーザー エージェント）]** フィールドに文字列を入力し、**[Searc h]** をクリックします。文字列は、ユーザーエージェント ヘッダーのすべてまたは一部とし、最大 128 文字です。

検索文字列に一致する上位（200 位まで）の検索結果が **[User Agent Search Results（ユーザー エージェントの検索結果）]** テーブルに表示されます。このテーブルには下記の情報が含まれます。

- 検索基準に一致する実際の**ユーザー エージェント**。文字列が切り捨てられている場合、マウスをエントリの上に置き、完全な文字列を確認します。
- 最後の列ヘッダーは、結果を**要求**によってソートするか、**帯域幅**によってソートするかを示します（**[Sort by（ソート基準）]** リストを使用して、ソート基準を選択します）。

検索を実行した後、デフォルトの [Top 10 User Agents] テーブルの表示に戻るには **[Clear]** をクリックします。

[Top 10 or Results（上位 10 または検索結果）] テーブル内のユーザー エージェントをクリックすると、ページの下部に **[User Agent Detail（ユーザー エージェントの詳細）]** テーブルが表示されます。詳細なテーブルは下記の情報を示します。

- ユーザー エージェントを閲覧している**ユーザー**。
- 要求の発信元の**クライアント IP アドレス**。
- 要求を処理している統合コンポーネント（Content GatewayまたはNetwork Agent）の**ソース サーバー IP アドレス**。
- 選択したユーザー エージェントに含まれている**要求**の数。
- 指定したユーザーおよびクライアント コンピュータからのユーザー エージェントを含むすべての要求の**帯域幅**の大きさ。

レポートの詳細情報を Microsoft Excel などのスプレッドシート ソフトウェアを使って処理できる CSV ファイルにエクスポートするには、**[Export to CSV（CSV へのエクスポート）]** をクリックします。

> **注意**
> レコードの数がシステムで処理できる数より多い場合、出力ファイルには実際の CSV フォーマットのデータは含まれません。そのような場合、より短い時間帯を選択し、データ セットを小さくしてから、再びデータをエクスポートします。

ユーザー エージェント データを収集する方法

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *アプリケーション レポートの作成、216 ページ*
- *ブラウザ使用状況の詳細、221 ページ*
- *プラットフォーム使用状況の詳細、222 ページ*

ユーザー エージェントは、ウェブ ブラウザおよび他のウェブ アプリケーションが自分と自分の機能を識別するために使用する HTTP ヘッダーです。ユーザーがインターネットを閲覧したとき、ウェブ セキュリティ ソフトウェアはユーザー エージェント データを捕捉し、ログ記録します。ユーザー エージェント データはブラウザおよびプラットフォーム情報を含み、その情報は構文解析されてアプリケーション レポートに表示されます。

- ブラウザまたはプラットフォームがネットワークにインストールされているが、インターネット アクセスのために**使用されていない**場合、それはアプリケーション レポートには表示されません。
- ユーザー エージェント ヘッダーについては広く採用されている標準がないため、ウェブ セキュリティ ソフトウェアはインターネットにアクセスするすべてのアプリケーションを特定することはできません。

  実際、一部のアプリケーションは、検出されるのを避けるために、ユーザー エージェント ヘッダーで自分の ID を意図的に偽ります。

Websense Log Server が受け取るアプリケーション閲覧データは、ユーザー エージェント ヘッダー、ユーザー名、およびソース IP アドレスを含みます。60 秒の間に同じユーザー エージェント、ユーザー、ソース IP アドレスを共有するすべての要求は、要求の合計数およびそれらの要求と関連する帯域幅の使用量を提供する 1 つのレコードに結合されます。そのレコードはその後、ログ データベースに転送されます。ブラウザおよびプラットフォーム レポートが現在のインターネット アクティビティに関するデータによって更新されるまでの時間は、ユーザー エージェントが以前に検出され、分析されたかどうかによって異なります。

- そのユーザー エージェントに対応するブラウザ、ブラウザ バージョン、またはプラットフォームが以前に解析および識別されていない場合、そのブラウザおよびプラットフォームからの要求に関する情報は、夜間のトレンド ジョブが終わるまでアプリケーション レポートには表示されません（*データベース ジョブ*、516 ページを参照）。

  つまり、新しいブラウザ、ブラウザ バージョン、およびプラットフォームに関する情報がブラウザおよびプラットフォーム レーポートに表示されるまでに、最大 24 時間の遅延があります。

  そのため、新規インストールまたは v 7.8 へのアップグレードの後、[Browser] および [Source Platform] タブは当初は何のレポートも表示しません。
- そのユーザー エージェントに対応するブラウザ、ブラウザ バージョン、およびプラットフォームが以前に解析および識別されていた場合、そのブラウザおよびプラットフォームからの要求に関する情報は、Log Database に記録された時にすぐにブラウザおよびプラットフォーム レポートに表示されます。

[Search] タブ上のデータにはブラウザおよびプラットフォーム レポートと同様の遅延は生じません。ユーザー エージェント文字列は、ログ データベースに記録された時すぐに、検索に利用できるようになります。これは、ブラウザおよびプラットフォームに関連する文字列と、他のタイプのウェブ アプリケーションによって使用される文字列の両方を含みます。

ブラウザ使用状況の詳細

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *アプリケーション レポートの作成*、216 ページ
- *ユーザー エージェント データを収集する方法*、219 ページ
- *プラットフォーム使用状況の詳細*、222 ページ

[Applications] ページの [Browser] タブでブラウザ ファミリーまたはバージョンをクリックしたとき、**ブラウザ詳細レポート** が表示されます。

この**ブラウザ インベントリ** は次の情報の視覚的な概要を提供します。

- 選択したブラウザ ファミリについて、使用頻度が最も高いバージョンと、各バージョンの使用状況の傾向。
- 選択したブラウザ バージョンについて、そのバージョンの使用頻度の高いユーザーと、そのバージョンの使用状況の傾向。

グラフの種々の要素の上にカーソルを置くことによって追加的な詳細情報を表示することができ、また、各グラフ下の **[Chart type（グラフのタイプ）]** オプションを使用してデータの表示方法を変更することができます。

グラフの下の **[Users Sending Requests（要求を送信しているユーザー）]** テーブルは、選択したブラウザ ファミリーまたはバージョンの使用頻度が高い 200 のアクティブ ユーザーをリストします。このテーブルは以下の項目を含みます。

- インターネット要求を行っている**ユーザー**の名前。
- **クライアント ホスト名**（もしあれば）、およびインターネットを閲覧するために使用されているコンピュータの**クライアント IP アドレス**。
- HTTP 要求を処理する統合コンポーネント（Content Gateway または Network Agent）に対応する**ソース サーバー IP アドレス**。
- **ブラウザ**の名前およびバージョン。
- 使用されているブラウザの**タイプ**（モバイルまたはデスクトップ）。
- ブラウザを通じて行われた要求の量（**件数**および**帯域幅**）。
- このブラウザおよびバージョンに関連する**ユーザー エージェント**。完全なユーザー エージェントを表示するには、そのアイコンをクリックします。

使用可能なデータを Microsoft Excel などのスプレッドシート プログラムでの処理のために CSV ファイルにエクスポートするには、**[Export to CSV（CSV へのエクスポート）]** をクリックします。

> **注意**
> レコードの数がシステムで処理できる数より多い場合、出力ファイルには実際の CSV フォーマットのデータは含まれません。そのような場合、より短い時間帯を選択し、データ セットを小さくしてから、再びデータをエクスポートします。

テーブルの下部のページング オプションを使用して、データ間を移動します。各ページには最大 20 行の情報を表示できます。

[Close] をクリックすると [Application] ページの [Browser] タブの要約データに戻ります。

プラットフォーム使用状況の詳細

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *アプリケーション レポートの作成*、216 ページ
- *ユーザー エージェント データを収集する方法*、219 ページ
- *ブラウザ使用状況の詳細*、221 ページ

[Applications] ページの [Source Platform（ソース プラットフォーム）] タブでプラットフォーム ファミリーまたはバージョンをクリックしたとき、**[Platform Detail Report（プラットフォームの詳細レポート）]** が表示されます。

このプラットフォーム インベントリ は次の情報の視覚的な概要を提供します。

- 選択したオペレーティング システムについて、使用頻度が最も高いバージョンと、各バージョンの使用状況の傾向。
- 選択したオペレーティング システムのバージョンについて、そのバージョンの使用頻度の高いユーザーと、そのバージョンの使用状況の傾向。

グラフの種々の要素の上にカーソルを置くことによって追加的な詳細情報を表示することができ、また、各グラフ下の **[Chart type（グラフのタイプ）]** オプションを使用してデータの表示方法を変更することができます。

グラフの下の **[Users Sending Requests（要求を送信しているユーザー）]** テーブルは、選択したオペレーティング システムまたはバージョンの使用頻度が高い 200 のアクティブ ユーザーをリストします。このテーブルは以下の項目を含みます。

- インターネット要求を行っている**ユーザー**の名前。
- **クライアント ホスト名**（もしあれば）、およびインターネットを閲覧するために使用されているコンピュータの**クライアント IP アドレス**。
- HTTP 要求を処理する統合コンポーネント（Content Gateway または Network Agent）に対応する**ソース サーバー IP アドレス**。
- オペレーティング システムの**プラットフォーム**名およびバージョン。
- 使用されているオペレーティング システムの**タイプ**（モバイルまたはデスクトップ）。
- ブラウザを通じて行われた要求の量（**件数**および**帯域幅**）。
- このオペレーティング システムおよびバージョンに関連する**ユーザー エージェント**。完全なユーザー エージェントを表示するには、そのアイコンをクリックします。

使用可能なデータを Microsoft Excel などのスプレッドシート プログラムでの処理のために CSV ファイルにエクスポートするには、**[Export to CSV（CSV へのエクスポート）]** をクリックします。

> **注意**
> レコードの数がシステムで処理できる数より多い場合、出力ファイルには実際の CSV フォーマットのデータは含まれません。そのような場合、より短い時間帯を選択し、データ セットを小さくしてから、再びデータをエクスポートします。

テーブルの下部のページング オプションを使用して、データ間を移動します。各ページには最大 20 行の情報を表示できます。

[Close] をクリックすると [Application] ページの [Source Platform] タブの要約データに戻ります。

Real-Time Monitor

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *レポートによるインターネット アクティビティの評価*、159 ページ
- *複数の Policy Server 配備環境での Real-Time Monitor*、227 ページ

[Reporting] > [Real-Time Monitor（リアルタイム モニタ）] ページを使用して、ネットワーク中の現在のインターネット アクティビティを調べることができます。

重要

Real-Time Monitor による表示が Internet Explorer で正常でない場合、（ブラウザのアドレス バーの URL と Refresh ボタンの間にある）Compatibility View（互換性表示）ボタンの選択を解除してください。

[Start（スタート）] をクリックして、ページにデータを取り込みます。このページでは直近のインターネット要求が示され、それには以下の情報が含まれています。

- 要求を出した**ユーザー**の IP アドレスまたは名前。
  - ネットワーク上でユーザー ベースのポリシーを使用していて、ユーザー名が示される場合、エントリ上にマウスを進めて IP アドレスを確認します。
  - ユーザー名が 31 文字以上であると、ハイフン（ “-” ）と名前の最後の 30 文字が表示されます。右クリックにより長いユーザー名を検索フィルタに追加する場合、ハイフン文字をフィルタ フィールドから削除し、**[Show Result（結果の表示）]** をクリックして一致するエントリを表示させます。
- 要求された **URL**。

  デフォルトにより、用意されているフィールドで完全に表示できないほど URL が長い場合、フィールドで示されるのはその URL の最初の 30 文字、スペース、ハイフン（ “-” ）、スペース、および同 URL の最後の 20 文字になります。切り詰められた URL を右クリックすると、全体の文字列が示されます。

  ページ最上部のツールバーで **[Customize（カスタマイズ）]** をクリックし、次に **[Show the full URL（完全な URL の表示）]** を選択すると、この方式が変更されます。

- Content Gateway スキャンの結果として要求されたサイトの分類が変更されたかどうか。
  - アイコンの存在によって、サイトがスキャンの結果に基づいて動的に再分類されたことが示されます。マウスをアイコンの上に置いて、元のカテゴリを確認します。
  - アイコンがないことは、Master Database カテゴリまたはカスタム URL カテゴリが使用されたことを示します。（これには、Content Gateway によってスキャンされたが、再分類されなかったサイトが含まれます。）
- サイトに割り当てられている **Category（カテゴリ）**。

  要求をフィルタリングするために実際に使用されたカテゴリ - Master Database カテゴリ、カスタム URL カテゴリ、またはスキャンの結果として動的に割り当てられたカテゴリ - が示されます。
- 要求に適用された **Action（処置）**（許可またはブロック）。

  マウスをエントリ上に進め、処置を決めるために使用された 1 つまたは複数のポリシーを調べます。例えば、以下のような場合、複数のポリシーがリストされます：
  - 複数のグループ ポリシーがを同じユーザーに適用できる。
  - 1 つのポリシーが IP アドレスとユーザーまたはグループの両方に割り当てられている。

  複数のポリシーがリストされている場合、Web Security manager Toolbox 中の Test Filtering（フィルタリングのテスト）を使用して、Real-Time Monitor で示されるユーザーまたは IP アドレスからの要求で優先されるポリシーを調べることができます。
- 要求が Real-Time Monitor に渡された **時刻**。

  Real-Time Monitor は、ログ データベースから要求を読み込むのではなく、Usage Monitor からリアル タイムで要求を受信するので、ここに示される要求時刻は、調査レポートおよびプレゼンテーション レポートに表示される要求時刻とは一致しないことがあります。

現在のデータを確認するために、**[Pause（一時停止）]** をクリックして、ページを更新させないようにします。新しい情報のモニターを開始する準備ができたら、再び **[Start（開始）]** をクリックします。

- デフォルトでは、データは 15 秒 毎に更新されます。更新のペースを変更するには、ページ最上部のツールバーで **[Customize（カスタマイズ）]** をクリックして、新しい **Data refresh rate（データ更新頻度）**値を選択します。

Real-Time Monitor は現在の設定値に従って一定数のレコード（250、500、または 1000 個）を保持していて、利用可能な最新のレコードのセットが常に表示されます。現在のデータを確認するために新しいレコードの表示を一時停止した場合、表示が一時停止されている間に行われた多くの要求がモニタで表示されないことになるかもしれません。（しかし、要求は Log Database に保存されており、調査レポートとプレゼンテーション レポートでも表示されます）。

表示されるレコードの数を変更するには、ページ最上部のツールバーで **[Customize]** をクリックして、新しい **Number of records shown**（**表示レコード数**）値を選択します。

フィルタを使用して特定の Real-Time Monitor データを表示する

Web Security Help | Web Security ソリューション | バージョン 7.8.x

画面で表示されるデータをフィルタするには、以下の手順を実行します：

1. **[Filter results by**（**フィルタリング結果のための基準**）フィールドで、ユーザー名または IP アドレスの全部または一部、URL、カテゴリ、あるいは処置を入力します。また、時間フィルタを選択して、過去 5 分、10 分、または 15 分の有効な結果を示すこともできます。
2. **[Show Results**（**結果の表示**）**]** をクリックします。
3. すべての結果の表示に戻るには、**[Clear Search Filters**（**検索フィルタのクリア**）**]** をクリックします。

また、[User]、[URL]、[Category]、または [Action] フィールドのエントリを右クリックし、次に **[Filter by**（**フィルタ基準**）**]** または **[Add...to search filter**（**検索フィルタに追加**）**]** オプションを選択して、選択されている文字列に基づいて結果をフィルタすることができます。

タイムアウト動作について

Web Security Help | Web Security ソリューション | バージョン 7.8.x

デフォルトでは、TRITON Unified Security Center のセッションは 30 分でタイムアウトになります。Real-Time Monitor をタイムアウトなしで動作させるには、**[Full Screen**（**全画面**）**]** をクリックして、モニタを新しいウィンドウで開きます。モニタされている Policy Server の IP アドレスが Real-Time Monitor のタイトル バーに表示されます。複数の Policy Server インスタンスをモニタしたい場合は、考慮事項と手順について *複数の Policy Server 配備環境での Real-Time Monitor*、227 ページ を参照してください。

複数の Policy Server 配備環境での Real-Time Monitor

[Reporting] > [Real-Time Monitor] ページに入ると、管理コンソールが現在接続している Policy Server インスタンスについての情報が Real-Time Monitor によって示されます。つまり、複数の Policy Server を利用している場合、管理コンソールを新しい Policy Server インスタンスに接続すると、Real-Time Monitor は異なるセットのクライアントに関する情報を表示しはじめるのです。

Web Security manager が接続している Policy Server インスタンスとは無関係に、Real-Time Monitor に特定の Policy Server のトラフィックをモニタさせつづけるには、**[Full Screen]** をクリックして新しいウィンドウでモニタを開きます。モニタされる Policy Server の IP アドレスが画面の最上部に表示されます。

- Real-Time Monitor は、インターネット アクティビティ情報を Usage Monitor から受け取ります。Real-Time Monitor が Policy Server のインターネット アクティビティを示すためには、各 Policy Server はいずれかの Usage Monitor インスタンスと関連付けられていなければなりません。
- 複数の Real-Time Monitor インスタンスをフルスクリーン モードで動作せさることができるし、この場合、各インスタンスはそれぞれ異なる Policy Server のデータを示します：
  1. TRITON コンソールにログ オンし、Web Security manager を選択します。それによって中央（デフォルト）Policy Server と接続します。
  2. [Reporting] > [Real-Time Monitor] ページに入り、[Full Screen] をクリックします。

     中央 Policy Server の IP アドレスがタイトル バーに表示されます。
  3. Web Security manager に戻り、ツールバーの [Policy Server Connection（Policy Server 接続）] ボタンを使用して、別の Policy Server インスタンスに接続します。
  4. ステップ 2 を繰り返します。
  5. ネットワーク上の個別の Policy Server インスタンスについて同じ手順を繰り返します。
- フルスクリーン モードでは、Real-Time Monitor はタイムアウトしません。

9 Content Gateway 分析

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *スキャン オプション*、232 ページ
- *コンテンツの分類*、233 ページ
- *トンネリング プロトコルの検出*、235 ページ
- *セキュリティの脅威：Content security*、236 ページ
- *セキュリティの脅威：ファイル分析*、237 ページ
- *Outbound security（アウトバウンド セキュリティ）*、244 ページ
- *拡張オプション*、245 ページ
- *例外のスキャン*、249 ページ
- *スキャンで使用するデータ ファイル*、251 ページ
- *高度な分析アクティビティに関するレポート*、252 ページ
- *SSL 復号化バイパス*、256 ページ

高度な分析と SSL 復号化バイパスの機能は、Websense Web Security Gateway および Websense Web Security Gateway Anywhere で利用できます。

Websense Content Gateway は、ウェブ トラフィックが Websense オンプレマイズ プロキシを通過するとき、ウェブ トラフィックの高度な分析をサポートします。まだブロックされていないサイトだけが、アクティブなポリシーに基づき分析されます。

- *コンテンツの分類*、233 ページでは、Websense Master Database に登録されていない URL や、Websense Security Labs によって指定されているダイナミック コンテンツを含むサイトからのコンテンツを分類します。分析の結果として、ポリシーの実施で使用するカテゴリが戻されます。
- *トンネリング プロトコルの検出*、235ページでは、トラフィックを分析して、**HTTP** および **HTTPS** 上でトンネリングされたプロトコルを検出します。そのようなトラフィックは、プロトコル ポリシーの実施のために Filtering Service に報告されます。インバウンドとアウトバウンドの両方のトラフィックの分析が行われます。

- *セキュリティの脅威：Content security、236 ページ*では、インバウンド コンテンツを分析して、マルウェア、ウィルス、フィッシング、URL リダイレクト、Web エクスプロイト、プロキシ回避などのセキュリティ脅威を検出します。
- *セキュリティの脅威：ファイル分析、237 ページ*では、セキュリティ脅威を検出するために下記の 2 つの検査方法を適用します。
  - **Websense Advanced Detection（Websense 高度な検出）**は、ウィルス、トロイの木馬、ワームなどの不正なコンテンツを検出し、ポリシーの実施のために使用する脅威カテゴリを戻します。
  - **従来のアンチウィルス（AV）検出ファイル**は、ファイルに感染したウィルスを検出します。
  - **Websense ThreatScope Analysis** は、疑わしいファイルを分析のためにクラウドによってホストされているサンドボックスにアップロードし、ファイルに不正なコンテンツがあるとわかったとき、管理者宛てにアラートを電子メールで送信します。

  [Advanced Detection（高度な検出）] または **[Antivirus Scanning（アンチウィルス スキャン）]** のどちらかを有効化した場合、オプションで下記のファイルも分析できます。
  - **リッチ インターネット アプリケーション**（Flash ファイルなど）を分析し、不正なコンテンツを検出してブロックします。
  - **FTP ファイル**を分析し、不正なコンテンツを検出してブロックします。

  [File Type Options（ファイル タイプ オプション）] の設定によって、不正なコンテンツに関する分析の対象とするファイルのタイプ（実行ファイルおよび認識されないファイルを含む）を指定します。個別のファイル拡張子を指定することもできます。この設定は、ThreatScope の分析には適用しません。
- *Outbound security（アウトバウンド セキュリティ）、244 ページ*は、下記の 2 種類のアウトバンドの分析方法を提供します。一つ目の方法は、インバウンド セキュリティ脅威コンテンツ分析およびファイル分析の設定をミラーリングするアウトバンド コンテンツの分析を実行します。もう一つの分析方法は、データ脅威分析を実行し、アウトバウンド カスタム暗号化ファイル、パスワード ファイル、および他の機密データを検出してブロックします。
- **[Content Categorization and Scanning Sensitivity（コンテンツの分類とスキャンの感度）]** コントロールによって、コンテンツの分類およびコンテンツの分析の感度のしきい値を微調整できます（*拡張オプション、245 ページ*）。
- 大容量、ストリーミング、または低速トランザクションでは、**[Content Delay Handling（コンテンツ遅延処理）]** オプションによって、バッファに格納されているコンテンツの 1 つの部分のクライアントへの配信を遅らせる時間を制御できます（*拡張オプション、245 ページ*）。

- **[Scanning Timeout（スキャン タイムアウト）]**、**[File Size Limit（ファイル サイズ制限）]**、および **[Content Stripping（コンテンツのストリッピング）]** 拡張オプションは、プロキシが通過するすべてのトラフィックに適用します（*拡張オプション、245 ページ*）。

いくつかのプレゼンテーション レポートは、高度な分析機能が脅威を含んでいるサイトへのアクセスの試みからネットワークを保護する方法に関する詳細を提供します。*高度な分析アクティビティに関するレポート、252 ページ*を参照してください。

SSL 復号化バイパス オプションを使用すると、プロキシを通過するときに復号化および分析の対象に**ならない** クライアント、ウェブサイト、およびウェブサイト カテゴリを指定できます。これらのオプションは、SSL サポートが Content Gateway で有効化されている場合のみ適用します。*SSL 復号化バイパス、256 ページ*を参照してください。

スキャンの例外は、常に分析するまたは分析しないホストまたは URL のリストです。常に実行するまたは常に実行しない分析のタイプは、ホスト名 / URL またはホスト名 /URL のグループごとに指定します。コンテンツを常に分析しないクライアント IP アドレスのリストも指定できます。*例外のスキャン、249 ページ*を参照してください。

スキャンおよび SSL 復号化の機能の有効化

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Web Security Gateway および Gateway Anywhere で利用できる高度な分析および SSL 復号化バイパスの機能を有効化するには、Web Security manager で適切なサブスクリプション キーを入力する必要があります。下記の場合にキーを入力できます。

- ログ オンの後要求されたとき
- **[Settings] > [General] > [Account]** ページで
- 編集する Policy Server インスタンスを選択した後、**[Settings（設定）] > [General（一般）] > [Policy Servers]** ページで。

[Account] または [Policy Servers] ページで現在のキー情報を確認します。

キーは、現在の Policy Server に関連するすべての Content Gateway のインスタンスに自動的に渡されます。詳細については、*Policy Server 接続の確認、459 ページ*と *Content Gateway 接続の管理、474 ページ*を参照してください。

高度な分析のオプションの設定の詳細については、*スキャン オプション、232 ページ*を参照してください。SSL 復号化バイパスのオプションの詳細については、*SSL 復号化バイパス、256 ページ*を参照してください。

スキャン オプション

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *コンテンツの分類*、233 ページ
- *トンネリング プロトコルの検出*、235 ページ
- *セキュリティの脅威：Content security*、236 ページ
- *セキュリティの脅威：ファイル分析*、237 ページ
- *Outbound security（アウトバウンド セキュリティ）*、244 ページ
- *拡張オプション*、245 ページ
- *例外のスキャン*、249 ページ
- *高度な分析アクティビティに関するレポート*、252 ページ

Websense Web Security Gateway および Websense Web Security Gateway Anywhere で利用できる分析オプションは、Web トラフィックが Content Gateway モジュール（Websense オンプレマイズ プロキシ）を通過するとき Web トラフィックに対して実行される高度な分析のタイプをコントロールします。

高度な分析のオプションまたは Content Gateway に関連する他のオプションの概要については、*Content Gateway 分析*、229 ページを参照してください。

下記のオプションを設定するには、**[Settings] > [Scanning（スキャン）] > [Scanning Options（スキャンのオプション）]** ページを順に選択します。

- *コンテンツの分類*、233 ページ
- *トンネリング プロトコルの検出*、235 ページ
- *セキュリティの脅威：Content security*、236 ページ
- *セキュリティの脅威：ファイル分析*、237 ページ
- *Outbound security（アウトバウンド セキュリティ）*、244 ページ
- スキャンの感度、スキャン タイムjアウト、ファイル サイズ制限、コンテンツ遅延処理、およびコンテンツのストリッピング（*拡張オプション*、245 ページを参照）

基本の設定は下記の通りです。

- **Off** - 分析なし。
- **On**（デフォルト）- Websense Security Lab で [高リスク] と指定されているコンテンツまたはファイルを分析します。

- **Aggressive analysis（積極的な分析）** - [高リスク] と指定されているコンテンツおよびファイル、および [低リスク] と指定されているコンテンツおよびリスクを分析します。Aggressive analysis は、より多くのリソースを使用します。最適の分析結果を得るために、システム パフォーマンスをモニタし、必要に対応するようにシステム リソースを拡大 / 縮小します。

On/Off/Aggressive 分析の設定のほかに、Always Scan（常にスキャン）、Never Scan（常にスキャンしない）、およびクライアント IP 例外のリストに基づき、分析を実行するかどうかを決定します。これらのリストは、**[Settings] > [Scanning] > [Scanning Exceptions（スキャンの例外）]** ページに保存されます。*例外のスキャン、249 ページ*を参照してください。

警告

[Never Scan] リストに含まれるサイトは、いかなる状況においても分析されません。[Never Scan] リストのサイトが危険なものであっても、スキャン オプションは不正なコードの分析や検出を行いません。

現在のページで設定を完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

コンテンツの分類

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *スキャン オプション、232 ページ*
- *トンネリング プロトコルの検出、235 ページ*
- *セキュリティの脅威：Content security、236 ページ*
- *セキュリティの脅威：ファイル分析、237 ページ*
- *Outbound security（アウトバウンド セキュリティ）、244 ページ*
- *拡張オプション、245 ページ*
- *例外のスキャン、249 ページ*
- *高度な分析アクティビティに関するレポート、252 ページ*

ウェブ ページが要求されたとき、下記の場合にコンテンツの分類が実行されます。

- URL がアクティブなポリシーによってまだブロックされていない場合
- URL が Websense Master Database にない場合
- URL が Websense Security Lab で [高リスク] と指定されている場合

コンテンツの分類によって決定されるカテゴリは、ポリシーの実施のために Filtering Service に転送されます。

コンテンツの分類には、オプションで**コンテンツに埋め込まれた URL リンクの分析**を含めることができます。そのような分析によって、一部のタイプのコンテンツをより的確に分類できます。たとえば、それ自体としては望ましくないコンテンツをほとんど含んでいないか、まったく含んでいないが、リンクしているサイトに望ましくないコンテンツが含まれるようなページを、より正確に分類することができます。リンク分析は、ページの隠れている部分に埋め込まれている不正なリンクを検出することができ、また望ましくないサイトへサムネイルをリンクさせるイメージ サーバーから戻されるページを検出することができます。リンク先の分析による適用範囲の改善についての詳細は Websense Security Labs のブログ ポスト [In Bad Company] を参照してください。

コンテンツの分類とリンクの分析の効果は、複数のプレゼンテーション レポートで数量化されています。詳細は、*プレゼンテーション レポート、161 ページ*を参照してください。

> **重要**
> 高度な分析アクティビティのレポートを生成する場合は、完全な URL のログ記録を有効化します（*URL がログ記録される方法の設定、524 ページ*を参照）。そうしない場合は、ログ記録には、分類されたサイトのドメイン（www.domain.com）しか記録されず、サイトの個々のページが別のカテゴリに適合している可能性があります。

サイトが WebCatcher を使用して未分類 URL を Websense, Inc. に報告している場合には（*WebCatcher とは、36 ページ*を参照）、コンテンツの分類によって分類された URL は、マスタ データベースへの登録のために転送されます。

コンテンツの分類機能を設定するには、下記の手順を実行します。

1. **[Settings] > [Scanning] > [Scanning Options]** ページを順に選択します。
2. コンテンツの分類を無効化するには、**[Off（オフ）]** を選択します。
3. コンテンツの分類を有効化するには、**[On（オン）]**（デフォルト）を選択します。
4. コンテンツの分析に埋め込みリンクの分析を含めるには、**[Analyze links embedded in Web content（Web コンテンツ内に埋め込まれたリンクを分析）]** を選択します。リンクの分析の結果ブロックされる要求は、Scanning Activity（スキャン アクティビティ）プレゼンテーション レポートにログ記録され、確認することができます。
5. 完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

コンテンツの分類を実行するために使用するアルゴリズムは、Websense Security Lab で調整され、ほとんどの組織に最適の結果をもたらします。しかし、最適化された設定が期待した結果をもたらさなかった場合、より限定的な結果またはより許容性のある結果にするように、感度レベルを調整できます。この画面の*拡張オプション*セクションを参照してください。

トンネリング プロトコルの検出

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *スキャン オプション*、232 ページ
- *コンテンツの分類*、233 ページ
- *セキュリティの脅威：Content security*、236 ページ
- *セキュリティの脅威：ファイル分析*、237 ページ
- *Outbound security（アウトバウンド セキュリティ）*、244 ページ
- *拡張オプション*、245 ページ
- *例外のスキャン*、249 ページ
- *高度な分析アクティビティに関するレポート*、252 ページ

トンネリングプロトコル検出オプションは、トラフィックを分析し、HTTP と HTTPS をトンネリングするプロトコルを検出します。特定のポートをトンネリングすることを許可されているトラフィックも分析されます。そのようなトラフィックは、プロトコルベースのポリシーの実施のために Filtering Service に報告されます。トンネリング プロトコル検出のオプションを有効にしたとき、他のスキャンの設定に関係なく、インバウンド トラフィックとアウトバウンド トラフィックの両方で分析が実行されます。

HTTP トンネリングは、通信のためにカスタム プロトコルを使用するアプリケーションが、HTTP にラップされている場合（つまり、標準 HTTP 要求 / 応答形式が存在する場合）に、HTTP/HTTPS トラフィック用に指定されたポートを使用するために行われます。これらのポートは、Web との間のトラフィックを許可するために開かれます。HTTP トンネリングは、これらのアプリケーションにファイアウォールおよびプロキシをバイオアスすることを許可しますから、システムを脆弱にします。

トンネリング プロトコル検出機能は、HTTP および HTTPS トラフィックを分析し、プロトコルを検出したとき、ポリシー実施のためにそのプロトコルを Filtering Service に転送します。この時点で、プロトコルはポリシーの定義に基づきブロックされるか、または許可されます。この機能により、インスタント メッセージング、ピアツーピア アプリケーションおよびプロキシ回避で利用されるプロトコルをブロックすることができます。HTTP を使って実行する一部のアプリケーション（例、Google Video）では、プロトコル ブロック ページが表示されないことがあります。プロトコルベースのポリシー

の実施の詳細については、*カテゴリおよびプロトコルへのアクセスの管理、59 ページ*を参照してください。

> **注意**
> トンネリング プロトコル検出は、コンテンツの分類の前に行われます。そのため、トンネリング プロトコルが特定された場合、プロトコル ポリシーが実施され、コンテンツの分類は行われません。

トンネリング プロトコル検出機能を設定するには、**[Settings] > [Scanning] > [Scanning Options]** ページを順に選択します。

1. トンネリング プロトコル検出機能を無効化するには、**[Off]** を選択します。
2. HTTP または HTTPS をトンネリングするポートを検出するためにすべてのトラフィックを分析するには、**[On]**（デフォルト）を選択します。そのようなトラフィックは、ポリシーの実施のために Filtering Service に報告されます。
3. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

常に分析しない信用のあるサイトを指定するには、**[Settings] > [Scanning] > [Scanning Exceptions（スキャンの例外）]** ページを順に選択します（*例外のスキャン、249 ページ*）。

セキュリティの脅威：Content security

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *スキャン オプション、232 ページ*
- *コンテンツの分類、233 ページ*
- *トンネリング プロトコルの検出、235 ページ*
- *セキュリティの脅威：ファイル分析、237 ページ*
- *Outbound security（アウトバウンド セキュリティ）、244 ページ*
- *拡張オプション、245 ページ*
- *例外のスキャン、249 ページ*
- *高度な分析アクティビティに関するレポート、252 ページ*

[Content Security（コンテンツ セキュリティ）] は、ウェブページのコンテンツの分析を実行し、HTTP および HTTPS コンテンツ（Content Gateway SSL サポートを有効化している場合は HTTPS）に含まれているセキュリティの脅威および不正なコードを検出します。

コンテンツ セキュリティのオプションを設定し有効化するには、**[Settings] > [Scanning] > [Scanning Options]** ページを順に選択します。

1. コンテンツの分析を無効化するには、**[Off]** を選択します。
2. 未分類のサイトおよび Websense Security Lab で[高リスク]と指定されているサイトに対するコンテンツの分析を有効化にするには、**[On]**（デフォルト）を選択します。
3. [高リスク]と指定されているサイトおよび[低リスク]と指定されているサイトからのコンテンツを分析するには、**[Aggressive analysis（積極的な分析）]** を選択します。このオプションは余分なシステムリソースを使用します。
4. 完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

常に分析する信用のないサイトまたは分析しない信用のあるサイトを指定するには、**[Settings] > [Scanning] > [Scanning Exceptions]** ページを順に選択します（*例外のスキャン、249 ページ*）。

コンテンツの分析の感度は、Websense Security Lab で調整され、ほとんどの組織に最適の結果をもたらします。しかし、最適化された設定が期待した結果をもたらさなかった場合、*拡張オプション*セクションで感度を調整できます。

セキュリティの脅威：ファイル分析

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *スキャン オプション、232 ページ*
- *コンテンツの分類、233 ページ*
- *セキュリティの脅威：Content security、236 ページ*
- *Outbound security（アウトバウンド セキュリティ）、244 ページ*
- *拡張オプション、245 ページ*
- *例外のスキャン、249 ページ*
- *高度な分析アクティビティに関するレポート、252 ページ*

ファイル分析のオプションは、ユーザーがリモートでダウンロードまたは開こうとしたファイルにウィルスや他の不正なコンテンツがないか調べます。ファイル分析は、ポリシー実施のためにカテゴリを Filtering Service フィルタリングに戻します。

次の 5 つのタイプのファイル分析のオプションがあります。それらのオプションは共に使用できます。

- *Advanced Detection（高度な検出）*は、Websense が開発した手法を適用し、ウィルス、トロイの木馬、ワーム、および他の不正なコンテンツなど、既知または新種の脅威を検出します。
- *Antivirus Scanning（アンチウィルス スキャン）*は、アンチウィルス検出ファイルを使って、ウィルスに感染したファイルを特定します。
- *ThreatScope™ 分析*は、Websense Security Labs によって定義されているプロファイルに適合するファイルを、アクティブ化および監視のために、クラウドによってホストされているサンドボックスに送信します。ファイルが不正なファイルであると判明した場合、脅威の説明、詳細な ThreatScope レポートへのリンク、およびログ データベースから作成された調査レポートへのリンクを含む電子メール警告が、Web Security アラート受信者に送信されます。

  ThreatScope は、Web Security Gateway Anywhere の加入者が使用できるプレミア機能です。詳細については、下の設定手順の中で説明しています。
- *リッチ インターネット アプリケーション スキャン*は、Flash ファイルに不正なコンテンツがないか調べます。
- *FTP ファイル スキャン*は、インバウンド Flash ファイルに不正なコンテンツがないか調べます。

分析対象のファイルの特定の種類を設定するには、**[File Type Options（ファイル タイプのオプション）]** をクリックします。（これらの設定は、ThreatScope には適用しません）。

注意

ファイル分析機能がマルチメディア ファイルを含むように設定されている場合、ストリーミング メディアがバッファに格納され分析されたとき、サーバーへの接続がタイムアウトになることがあります。そのような場合、最善の改善策は、そのサイトに対する例外を作成することです。*例外のスキャン*を参照してください。

常に分析する信用のないサイトまたは分析しない信用のあるサイトを指定するには、**[Settings] > [Scanning] > [Scanning Exceptions]** ページを順に選択します（*例外のスキャン、249 ページ*）。

ファイル分析のオプションを有効化し、設定するには、**[Settings] > [Scanning] > [Scanning Options]** ページを順に選択します。

Advanced Detection（高度な検出）

1. ファイル分析のオプションを無効化するには、**[Off]** を選択します。
2. 未分類のサイトからのファイルおよび Websense Security Lab で [高リスク] と指定されているサイトからのファイルに対するファイル分析のオプションを有効化にするには、**[On]**（デフォルト）を選択します。
3. [高リスク]と指定されているサイトおよび[低リスク]と指定されているサイトからのインバウンド ファイルを分析するには、**[Aggressive analysis]** を選択します。このオプションは余分なシステムリソースを使用します。

Antivirus Scanning（アンチウィルス スキャン）

1. アンチウィルス分析オプションを無効化するには、**[Off]** を選択します。
2. 未分類のサイトからのファイルおよび Websense Security Lab で [高リスク] と指定されているサイトからのファイルに対するアンチウィルス分析オプションを有効化するには、**[On]**（デフォルト）を選択します。
3. [高リスク]と指定されているサイトおよび[低リスク]と指定されているサイトからのインバウンド ファイルにアンチウィルス分析を適用するには、**[Aggressive analysis]** を選択します。このオプションは余分なシステムリソースを使用します。

ThreatScope™ 分析

このオプションは、ThreatScope クラウド サービスの加入者のみ使用できます。

1. ThreatScope 分析オプションを無効化するには、**[Off]** を選択します。
2. 分析対象となる実行ファイルを、分析のためにクラウドによってホストされているサンドボックスに送信するには、**[On]** を選択します。
3. 追加のサポートされているファイル タイプを分析のために ThreatScope 送信するには、**[Submit additional documents（追加のドキュメントの送信）]** を選択します。

ThreatScope サンドボックスで処理できるファイルの必要条件：

- Websense Master Database で [不正] として分類**されていない**
- すべての **[Security Threats（セキュリティの脅威）：File Analysis（ファイル分析）]** をパスする。
- 疑わしいファイルに対する Websense Security Labs のプロファイルに適合している
- サポートされているファイル タイプである。実行可能ファイルは常にサポートされています。知識ベースについての次の記事を参照してください：ThreatScope Supported File Types。

注意

ファイルは不正なファイルとして検出**されなかった**ので、**ブロックされず**、要求元に配信されました。

重要

そのトラフィックがクラウドに直接に送信され、そこでセキュリティの分析とポリシーの実施が行われるオフプレマイズのユーザーには ThreatScope は適用**されません**。

重要

ThreatScope が不正なファイルを報告するために使用する唯一のメカニズムである ThreatScope 電子メール メッセージを受け取るためには、**電子メール アラートを有効化し、設定する必要があります**。

[Settings] > [Alerts（アラート）] > [Enable Alerts（アラートを有効化）] を順に選択し、次に **[Enable email alerts（電子メール アラートを有効化する）]** を選択し、**[Administrator email address（管理者の電子メール アドレス）]** を指定します。また SMTP の設定値が正しいことも確認してください。

重要

Content Gateway ウェブ プロキシは、ThreatScope トラフィックを管理します。

トラフィックは下記へ送信されます。

- *.websense.net
- *.blackspider.com

ユーザー エージェントは **ssbc** です。

ThreatScope トラフィックに対して、手動での復号化を行ってはいけません。

ThreatScope トラフィックに対してネットワーク内のどのデバイスからも認証を要求することはできません。

Content Gateway では、デフォルトで **Filter.config** ルールが設定されます。Content Gateway がプロキシ チェーンの中またはファイアウォールの後にある場合、これらのデバイスを上記の要件に一致するように設定しなければなりません。

http://testdatabasewebsense.com/ の **[Real-time Analysis Test Pages（リアルタイム分析テスト ページ）]** セクションにあるリンク、**ThreatScope: Malicious App** を使って設定をテストし、ThreatScope Analysis がユーザーの環境の中で正しく設定されていることを確認することができます。

ThreatScope トランザクションの概要

1. エンド ユーザーがウェブサイトを閲覧し、明示的または暗示的にファイルをダウンロードします。
2. URL は、[不正な] URL に分類**されず**、**[Security Threats: File Analysis]** はファイルが不正なファイルとは**みなしません**。
3. ファイルが要求元に配信されます。
4. しかし、ファイルは Websense Security Labs プロファイルの [疑わしいファイル] に適合するため、分析のためにクラウド内の ThreatScope に送信されます。
5. ThreatScope はファイルを分析します。この分析には 5 ～ 10 分かかることもがありますが、通常はもっと迅速に行われます。
6. ファイルが不正なファイルであることが判明した場合、Content Gateway は ThreatScope 不正ファイル検出メッセージを、設定されたアラート受信者に送信します。アラート電子メールには、ThreatScope レポートと、ログ レコードから作成された調査レポートへのリンクが含まれます（下に例を示しています）。
7. メッセージを受信した時、管理者は次のことを行う必要があります。
   a. ファイルの ThreatScope レポートにアクセスし、評価する
   b. 調査レポートでインシデントについて調べる
   c. ネットワークへの侵入の影響を評価する
   d. 修復を計画し開始する
8. そのほかに、ThreatScope® は、ファイル、ソース URL、コマンドおよびコントロール ターゲットに関する情報によって ThreetSeeker® Intelligence Cloud を更新します。
9. ThreatSeeker は Websense Master Database、ACE 分析データベース、および他のセキュリティー コンポーネントを更新し、更新された情報がその後、Websense 配備で使用されるようになります。
10. 次に誰かがそのサイトの閲覧を試みたとき、そのユーザーと組織は、その Websense Web Security 配備によって保護されます。

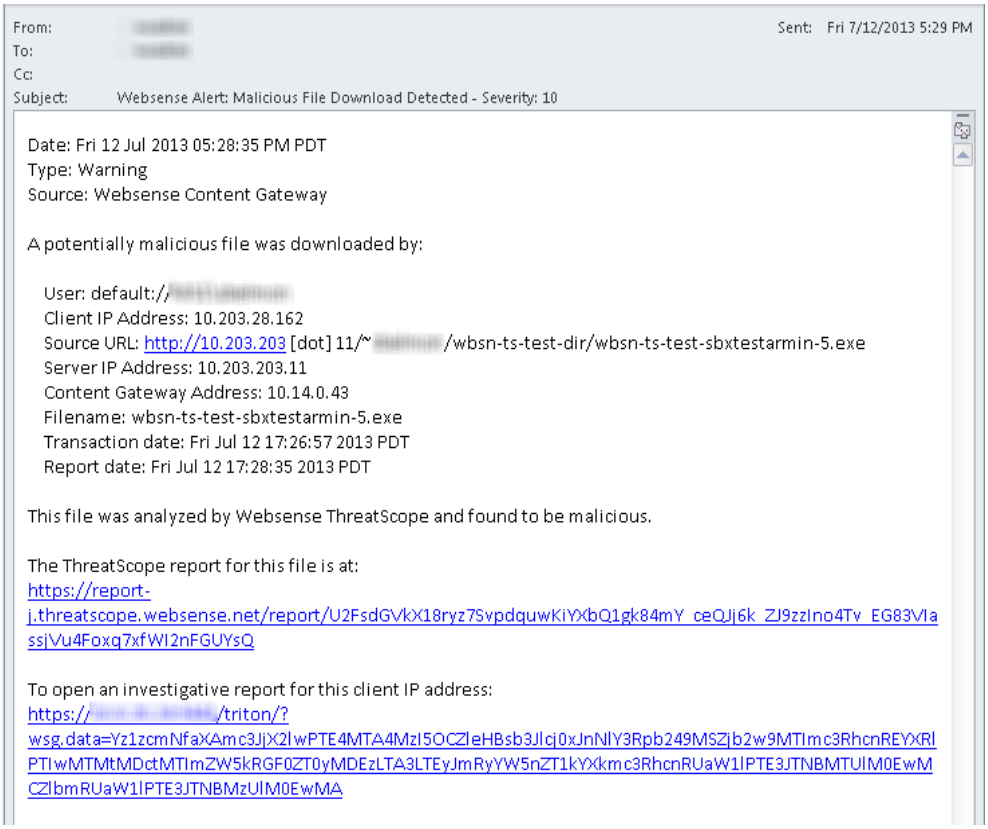
ThreatScope のアラート メッセージおよびレポート

Content Gateway は、ThreatScope が不正なファイルを検出したことを知ったとき、ThreatScope アラート電子メールを、設定されている管理者に送信します。メッセージはプレーン テキストです。下に例を示しています。

本文で、**[User（ユーザー）]** フィールドにユーザー名が表示されるのは Content Gateway ユーザー認証を使ってクライアントを識別した場合だけです。それ以外の場合は、このフィールドにはクライアントの IP アドレスが表示されます。

2 つのリンクが含まれています。最初のリンクは、ファイルおよびその不正なコンテンツに関する詳細な ThreatScope レポートにリンクします。2 番目のリンクは、ユーザーのログ レコードを使用して、ファイルのダウンロードが行われた時間の調査レポートを起動します。ブラウザによっては、レポートを表示できるようにするために、ポップアップを許可しなければならない場合があります。また、Web Security Gateway Anywhere がすべてのトランザクション レコードをログ データベースに書き込む前に、ThreatScope アラート メッセージを受け取ることがあります。保留されているレポートを含めるように、定期的にレポートを更新してください。

一般的なアラート メッセージの概要：


From:
To:
Cc:
Subject: Websense Alert: Malicious File Download Detected - Severity: 10
Sent: Fri 7/12/2013 5:29 PM

Date: Fri 12 Jul 2013 05:28:35 PM PDT
Type: Warning
Source: Websense Content Gateway

A potentially malicious file was downloaded by:

User: default:/
Client IP Address: 10.203.28.162
Source URL: http://10.203.203 [dot] 11/~ /wbsn-ts-test-dir/wbsn-ts-test-sbxtestarmin-5.exe
Server IP Address: 10.203.203.11
Content Gateway Address: 10.14.0.43
Filename: wbsn-ts-test-sbxtestarmin-5.exe
Transaction date: Fri Jul 12 17:26:57 2013 PDT
Report date: Fri Jul 12 17:28:35 2013 PDT

This file was analyzed by Websense ThreatScope and found to be malicious.

The ThreatScope report for this file is at:
https://report-j.threatscope.websense.net/report/U2FsdGVkX18ryz7SvpdquwKiYXbQ1gk84mY_ceQJj6k_ZJ9zzIno4Tv_EG83VIassjVu4Foxq7xfWI2nFGUYsQ

To open an investigative report for this client IP address:
https:// /triton/?wsg.data=Yz1zcmNfaXAmc3JjX2lwPTE4MTA4MzI5OCZleHBsb3Jlcj0xJnNlY3Rpb249MSZjb2w9MTImc3RhcnREYXRlPTIwMTMtMDctMTImZW5kRGF0ZT0yMDEzLTA3LTEyJmRyYW5nZT1kYXkmc3RhcnRUaW1lPTE3JTNBMTUlM0EwMCZlbmRUaW1lPTE3JTNBMzUlM0EwMA

これは ThreatScope レポートの一部の例です。

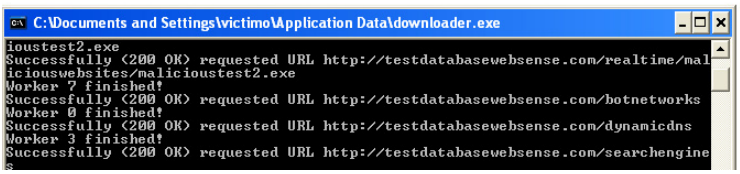
ThreatScope Analysis Report

For file with ID **23f9baa1f9873090d49b073d1e1309a1f2aa955e**

Assessment details:

Threat	Rating	Freq	Description
PROC_DROPPER_APPDATA	10		Drops and runs executable file(s) in a directory of the user profile often used by malware
CAT_BOTNET	10	1	Traffic to known botnet C&C server
CAT_MWS	10	1	Traffic to server hosting malicious content
REG_AUTORUN	8	1	Adds a registry key to automatically start an executable when the system starts
FS_DROPPER	8		Drops executable file(s)
PROC_POSSIBLE_INJECTED	6		Possibly injects code into remote process(es)
CAT_PDC	6	2	Traffic to server hosting potentially malicious content
FS_APPDATA	4	2	Writes to the filesystem in a directory of the user profile often used by malware

Screenshots



リッチ インターネット アプリケーション スキャン

Flash ファイルに不正なコンテンツがないか分析するには、**[Scan rich Internet applications（リッチ インターネット アプリケーションをスキャン）]** を選択します。

FTP ファイル スキャン

FTP プロトコルを使ってダウンロードされるファイルを分析するには、**[Scan FTP files（FTP ファイルをスキャン）]** を選択します（FTP over HTTP ファイルのダウンロードおよびアップロードは、HTTP/HTTPS ファイル スキャン機能の設定を必要とします）。重要な点としては、このオプションは、Content Gateway をプロキシ FTP トラフィックに構成する必要があることです。Content Gateway Manager ヘルプを参照してください。

注意

[Scan rich Internet applications] および **[Scan FTP files]** のオプションは、Advanced Detection が有効化されているときのみ使用できます。Advanced Detection ファイル分析機能をオフにした場合、リッチ インターネット アプリケーション スキャン機能が無効化され、チェックボックスがクリアされます。

FileType Options（ファイル タイプのオプション）

1. 分析するファイルのタイプを指定するには、**[File Type Options（ファイル タイプのオプション）]** をクリックします。最善の方法として、Websense Security Lab によって指定されているすべての [疑わしいファイル]、すべての実行ファイル、および認識されていないファイルを分析します。
2. 特定の識別子をもつファイルを常に分析するには、**[Files with the following extensions（拡張子付きファイル）]** を選択し、入力フィールドに拡張子を入力して **[Add]** をクリックします。

   リストから拡張子を削除するには、拡張子をクリックして選択し、**[Delate]** をクリックします。

ファイル分析のオプションの設定を完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

複数のプレゼンテーション レポートが、セキュリティ リスクを含んでいるファイルをダウンロードする試みに関する詳細を提供します。これらのレポートが Report Catalog（レポート カタログ）にリストされるのは、分析アクティビティの結果、マスタ データベースのカテゴリに割り当てられた後でアクティビティが変更されたサイトがみつかった後でだけです。詳細は、*プレゼンテーション レポート*、161 ページを参照してください。

ファイル タイプおよび URL カテゴリに基づくファイルのブロックの詳細については、*ファイル タイプに基づくトラフィックの管理*、345 ページを参照してください。

Outbound security（アウトバウンド セキュリティ）

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *スキャン オプション*、232 ページ
- *コンテンツの分類*、233 ページ
- *セキュリティの脅威：Content security*、236 ページ
- *セキュリティの脅威：ファイル分析*、237 ページ
- *例外のスキャン*、249 ページ
- *高度な分析アクティビティに関するレポート*、252 ページ
- *拡張オプション*、245 ページ

Outbound security の機能：

- インバウンド セキュリティ脅威の設定をミラーするアウトバンド分析を提供します。このオプションは、Web Security ソーシャル ウェブ コントロールもサポートします。
- 特別のデータ脅威保護を実行し、アウトバウンド カスタム暗号化ファイル、パスワード ファイル、および他の形式の機密データがないか分析して、ブロックします（下記の手順 2 を参照）。

1. ボットおよびスパイウェアのフォーン ホーム トラフィックなどの脅威についてアウトバウンド コンテンツを分析するには、**[Analyze for and block outbound security threats（アウトバンド セキュリティ脅威について分析してブロック）]**（デフォルト）を有効化します。このオプションは、インバウンド セキュリティ脅威の設定をミラーするアウトバンド分析を実行します。

   重要
   このオプションは、ソーシャル ウェブ コントロールをサポートするために有効化する必要があります。

2. 以下のファイルを分析およびブロックするには **[Data theft protection（データ脅威保護）]** を有効化します（デフォルト）。
   a. Websense Security Labs の定義によると**[未分類]**のサイトおよび[疑わしい宛先] に送信されるアウトバウンド カスタム暗号化ファイル
   b. 宛先に関係なく、パスワード ファイル、および機密データや疑わしいデータを含んでいるファイル。

   分析の結果は、Threats（脅威）ダッシュボードに報告され、またトランザクション ログおよびレポートに含まれます。

拡張オプション

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *スキャン オプション*、232 ページ
- *コンテンツの分類*、233 ページ
- *セキュリティの脅威：Content security*、236 ページ
- *セキュリティの脅威：ファイル分析*、237 ページ
- *Outbound security（アウトバウンド セキュリティ）*、244 ページ
- *例外のスキャン*、249 ページ
- *高度な分析アクティビティに関するレポート*、252 ページ

これらのオプションは、下記の場合に設定します。

- コンテンツの分類およびコンテンツ セキュリティ分析の感度レベルを設定するとき
- 分析時間制限 * を設定するとき
- 分析サイズ制限 * を設定するとき
- HTML コンテンツ * からコードの特定のタイプのストリッピングを有効化するとき

* これらの設定は、すべての着信トラフィックに適用します。

コンテンツの分類およびスキャン感度レベル

コンテンツの分類およびコンテンツの分析を実行するために使用するアルゴリズムは、Websense Security Lab で調整され、ほとんどの組織に最適の結果をもたらします。しかし、最適化された設定が期待した結果をもたらさなかった場合、より限定的な結果またはより許容性のある結果にするように、感度レベルを調整できます。

下記の 5 つの感度レベルがあります。

- **[Optimized（最適化）]** は、Websense Security Lab が調整した感度レベルです。
- **[More Stringent（より厳しい）]** および **[Most Stringent（最も厳しい）]** は、分析の感度を上げます。
- **[Less Stringent（それほど厳しくない）]** および **[Least Stringent（最も厳しくない）]** は、分析の感度を下げます。

完了したとき、**[OK]** をクリックして、変更をキャッシュします。

[Save and Deploy] をクリックするまで変更は適用されません。

スキャンのタイムアウト

各コンテンツまたはファイルの分析に要する時間は状況によって異なり、分析が開始するまでわかりません。デフォルトでは、ユーザーに適するようにするために、分析は、1.5 秒（1500 ミリ秒）に限定されています。タイムアウトを調整するには、**[Custom（カスタム）]** を選択し、500 ～ 10000 の範囲内で値を入力します（単位 ミリ秒）。

スキャン サイズの制限

スキャン サイズの制限は、分析が実行されるしきい値です。しきい値になると分析は停止します。デフォルトは 10 MB です。値を変更するには、**[Custom]** を選択し、サイズを単位メガバイトで入力します。

コンテンツ遅延処理 [こんてんつちえんしょり]

Content Gateway の構成およびロード条件によっては、非常に大きなファイル、ストリーミング トランザクション、および低速のオリジン サーバーが、コンテンツの待機中にクライアントから転送されることがあります。

このセクションのオプションを使用して、**分析を実行する前に**、バッファに入れられたコンテンツの一部をクライアントに配信することができます。分析は、すべてのデータが受信された時、またはスキャン サイズ制限を超えた時に開始されます。

[Begin returning data to the client after（クライアントへのデータの返送を開始するまでの時間）] で時間を指定します。この時間を過ぎると、バッファに入れられたデータの一定の割合（%）がクライアントに転送されます。デフォルトは 30 秒です。他の値を指定するには、**[Custom]** を選択します。

[Specify how much data to return to the client（クライアントに戻すデータの量を指定）] で、バッファに入れられたデータのうちクライアントに転送する割合（%）を指定します。デフォルト設定は 80 パーセントです。別の値（最大 90 パーセント）を指定するには、**[Custom]** を選択します。

コンテンツのストリッピング

システムへの脅威が、ウェブ ページによって送られる**アクティブなコンテンツ**の中に隠されている可能性があります。アクティブ コンテンツとは、HTML ページに埋め込まれていて、アクションを実行する（例、アニメーション、プログラムを実行する）コンテンツです。

コンテンツのストリッピング オプションによって、特定のスクリプト言語（ActiveX、JavaScript、または VB Script）によるコンテンツを着信するウェブ ページからストリップすることが可能になります。コンテンツのストリッピングが有効化されている場合、指定したスクリプト言語を使用するすべてのコンテンツが、[ダイナミック コンテンツを含む]、または [『Always Scan』 リストに含まれる] というフラグが付けられているサイトから削除されます（*スキャン オプション*、232 ページを参照）。

コンテンツの削除は、高度な分析オプションによってサイトが分類され、Filtering Service がどのポリシーを適用するかを決定した後にのみ行われます。

警告
ストリップされたアクティブ コンテンツに基づいている Web ページは、期待通りには機能しません。アクティブ コンテンツを必要とするサイトへの全面的なアクセスを許可するには、コンテンツのストリッピングを無効化するか、サイトを [Never Scan] リストに追加します。

アクティブ コンテンツを含むページを要求するユーザは、コンテンツが削除されていることについて何も通知を受け取りません。

コンテンツのストリッピングのオプションを設定するには、**[Settings] > [Scanning] > [Scanning Options] > [Advanced Options（拡張オプション）]** エリアを順に選択します。

1. **[Advanced Options] > [Content Stripping（コンテンツのストリッピング）]** エリアを順に選択して、着信ウェブ ページから削除するスクリプト言語のタイプを選択します。

   選択した言語のコンテンツのストリッピングを無効化するには、関連するチェックボックスをオフにします。
2. 完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

警告
コンテンツ ストリッピングによって、一部のコンテンツが文字化けしたり、判読不能になることがあります。Content Gateway の構成に少し変更を行うことによって、そのようなことが発生する回数を減らすことができます。

1 Content Gateway manager を開き、**[Configure] > [Protocols] > [HTTP] > [Privacy（プライバシー）]** タブを順に選択します。

2 **[Remove Headers（ヘッダーを削除）] > [Remove Others（その他を削除）]** フィールドで、Accept-Encoding を追加します。

3 **[Apply]** をクリックし、Content Gateway を再起動します。

例外のスキャン

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *スキャン オプション*、232 ページ
- *コンテンツの分類*、233 ページ
- *セキュリティの脅威：Content security*、236 ページ
- *セキュリティの脅威：ファイル分析*、237 ページ
- *Outbound security（アウトバウンド セキュリティ）*、244 ページ
- *拡張オプション*、245 ページ

例外のスキャンは、**常に分析しない**信用あるまたは**常に分析する**信用のないサイト（ホスト名および URL）のリストです。実行しないまたは常に実行する分析のタイプは、ホスト名、URL、またはホスト名および URL のグループごとに指定します。

コンテンツを常に分析しない信用あるクライアント IP アドレスのリストも作成できます。

スキャンのオプションの概要については、*Content Gateway 分析*、229 ページを参照してください。

コンテンツの分類、トンネリング プロトコルの検出、セキュリティ脅威（コンテンツ分析およびファイル分析）、およびコンテンツのストリッピングの動作を精緻化するには、**[Always Scan]** リストと **[Never Scan]** リストを使用します。

- [Content Categorization]、[Content Security]、[File Analysis] のオプションが **[On]** である場合は、**[Always Scan]** リストにあるサイトが常に分析され、**[Never Scan]** リストにあるサイトは分析されません（*スキャン オプション*、232 ページを参照）。
- [Tunneled Protocol Detection] オプションが **[On]** であるか、または **[Aggressive analysis]** が選択されている場合は、**[Never Scan]** リストにあるサイトは分析されません。

[Never Scan] リストの使用には、注意が必要です。リストに含まれるサイトが危険なものであっても、Websense Security Gateway はそのサイトを分析して問題を検出することができません。

ホスト名 /URL の例外

[Always Scan] リストまたは [Never Scan] リストにサイトを追加するには、下記の手順を実行します。

1. **[Add Hostname/URL（ホスト名 /URL を追加）]** ボタンをクリックします。

   サイトをいくつかの方法で指定でき、また一度に複数のホスト名または URL を指定できます。

   - 1 つのホスト名、たとえば、**thissite.com** を入力できます。ドメインと拡張子の両方を入力してください（**thissite.com** と **thissite.net** は、別個のホストです）。
   - 複数のラベルが付いたサイトを使用できます。例：**www.bbc.co.uk**
   - ワイルド カード [*] を使用して先頭のサブドメインのみを照合できます。

     例：***.yahoo.com**.
   - 完全なまたは一部のホスト名または URL を入力できます。先頭のスキーム [HTTPS://] は必要ありません。正確な照合は、指定した文字列で実行されます。

     例：**www.example.com/media/**

     または、**www.youtube.com/watch?v=**
2. 1 つホスト名/URL またはホスト名/URL のグループを入力した後、入力したすべてのサイトに適用するスキャンのオプションを選択します。1 つまたは複数のオプションを選択できます。

   異なるサイトに異なるオプションを適用するには、名前を別個に入力します。

   サイトは、2 つのリストの一方にのみ表示されます。たとえば、同じサイトに対してトンネリング プロトコルを分析せず、コンテンツの分類を常に分析するように指定することはできません。

   [OK] をクリックして、エントリを追加します。
3. リストからサイトを削除するには、サイトを選択し、**[Delete]** をクリックします。
4. 完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

サイトに関連付けられたスキャンのオプションを変更するには、下記の手順を実行します。

1. リストからサイトを選択し、オプションを変更します。
2. 完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

クライアントの例外

コンテンツを常に分析しない信用のあるユーザー（クライアント IP アドレス）を特定するには、[Client Exceptions（クライアントの例外）] リストを使用します。

リストに IP アドレスを追加するには、下記の手順を実行します。

[Enter clients（クライアントを入力）] ボックスをクリックし、IP アドレスまたは IP アドレスの範囲を入力します。例、10.201.67.245、または 10.201.67.245 - 10.201.67.250。

右矢印（>）をクリックして、アドレスをリストに追加します。

エントリを編集するには、下記の手順を実行します。

リストからエントリを選択し、**[Edit（編集）]** をクリックします。

変更を行い、**[OK]** をクリックします。

エントリを削除するには、下記の手順を実行します。

リストからエントリを選択し、**[Delete]** をクリックします。

完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

スキャンで使用するデータ ファイル

分析はその作業をサポートする一組のデータ ファイルを使用します。これらのファイルは、Websense Security Lab によって定期的に更新され、Websense ダウンロード サーバーで使用できるようにされます。Websense Content Gateway は、定期的に分析データ ファイルの更新をチェックします。各ファイルの名前およびバージョンは、Content Gateway manager の **[Monitor] > [MyProxy] > [Summary]** ページに表示されます。

ファイルの更新は、Websense マスタ データベースの更新（リアルタイム データベース更新および Real-Time Security Updates を含む）とは無関係に行われます。

./WCGAdmin start コマンドが実行するたびに、データ ファイルのチェックおよびダウンロードが実行されます。ダウンロードが失敗した場合、ダウンロードが正常に完了するまで 15 分ごとに新たなダウンロードが試行されます。

データベース更新チェックのデフォルトの間隔は 15 分です。この設定を使用することを推奨します。間隔を長くすると新種の *zero day* エクスプロイトに対する脆弱性の隙間が増えます。

Websense Content Gateway コンピュータ上の **/opt/bin/downloadservice.ini** ファイルの **[PollInterval]** 値を編集することにより、ポーリングの間隔を変更することができます。**downloadservice.ini** ファイルを編集した後、下記のコマンド ラインから Websense Content Gateway を停止し、再起動しなければなりません。

```
/opt/WCG/WCGAdmin restart
```

高度な分析アクティビティに関するレポート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *スキャン オプション*、232 ページ
- *コンテンツの分類*、233 ページ
- *セキュリティの脅威：ファイル分析*、237 ページ
- *コンテンツのストリッピング*、247 ページ

Websense Content Gateway をインストールし、高度な分析機能を有効化するキーを入力した後、ダッシュボード、プレゼンテーション レポート、および調査レポートでこれらの機能の効果を確認し、分析することができます。

[Usage（使用状況）] ダッシュボードには、デフォルトでは、2 文字が過去 30 日間の Web 2.0 サイトへの要求を集計します。

- Web 2.0 Categories（Web 2.0 カテゴリ）
- Web 2.0 URL Bandwidth（Web 2.0 URL 帯域幅）

グラフのカスタム化の方法またはグラフを別のダッシュボード タブに移動する方法については、*Web Security Dashboard*、39 ページを参照してください。

[Presentation Reports（プレゼンテーション レポート）]ページでは、**[Scanning Activity（スキャン アクティビティ）]** グループは、Web 2.0 参照および分析アクティビティ（コンテンツ分類の結果生じる再分類を含む）に重点を置いたレポートを含みます。また、リンク分析の結果生じるページのブロックを追跡するレポートもあります。

重要
分析アクティビティのレポートを有効に活用できるように、[full URL logging（完全な URL によるログ記録）] を有効化します（*URL がログ記録される方法の設定、524 ページ*を参照）。そうしないと、サイト内の各ページが異なったカテゴリに含まれるか、または異なった理由で再分類される場合でも、レポートは分類されたサイトのドメイン（www.domain.com）だけを表示します。

カスタム レポートを作成するために、セキュリティまたは分析レポート テンプレートをコピーできます。次にレポート フィルタを編集して、カスタム レポートを作成する際に含める情報を絞り込むことができます。

一部のセキュリティの脅威レポートには、**[Threat ID（脅威 ID）]** 列が含まれています。個々の脅威 ID をクリックすると、指定された脅威のタイプを記載する [Websense Secirity Labs] のウェブ ページが開きます。

他のプレゼンテーション レポートには、分析アクティビティおよび一般的なポリシーの実施に関する情報が含まれる場合があります。たとえば、[Report Catalog（レポート カタログ）] の [Internet Activity（インターネット アクティビティ）] グループの中の [Detail of Full URLs by Category（カテゴリ別完全な URL の詳細）] レポートには、各カテゴリのアクセスされた各 URL の詳細なリストが示されます。高度な分析に固有のレポートを作成するには、[Detail of Full URLs by Category（カテゴリ別完全な URL の詳細）] レポートをコピーし、そのレポート フィルタを新しいカスタム レポート用に編集します。[Actions（アクション）] タブで、分析に関連する許可およびブロックのアクションのみを選択します。[Options（オプション）] タブで、レポート カタログ名およびレポートのタイトルを変更し、これが高度な分析レポートであることを識別できるようにします。たとえば、名前およびタイトルを Advanced Analysis:Detail of Full URLs by Category に変更したとします。

また、調査レポートを使用して、高度な分析アクティビティの状況を把握することもできます。

1. **[Internet use by（インターネット使用状況）]** ドロップダウンリストで **[Action]** を選択します。
2. 編集したレポートで、アクション（例、**[Category blocked real time（リアルタイムのブロックされたカテゴリ）]**）をクリックし、ドリルダウン オプションのリストを表示します。
3. 使用するドリルダウン オプション（例、**[Category（カテゴリ）]** または **[User（ユーザー）]**）をクリックします。

4. **[Hits value（ヒット件数）]** または任意の行のバーをクリックすると、関連する詳細情報が表示されます。
5. ページの上部の **[Modify Report（レポートを変更）]** をクリックして、**[Full URL（完全 URL）]** 列をレポートに追加します。

すべての調査レポートの機能の使用方法については、*調査レポート*、187 ページを参照してください。

分析アクティビティがログ記録される方法

Web Security Help | Web Security ソリューション | バージョン 7.8.x

一般的なインターネット アクティビティがログ記録される方法と高度な分析アクティビティがログ記録される方法とでは重要な違いがあります。

一般的なインターネット アクティビティの場合は、Log Database のサイズを小さくする複数のオプションがあります。

- 要求されたウェブサイトごとに 1 つのレコードだけをログ記録するには、**[visits（アクセス件数）]** を有効化します。*Log Server の設定*、507 ページを参照してください。
- 特定の共通要素を持つ複数の要求を 1 つのログ記録に統合するには、**[consolidation（統合）]** を有効化します。*Log Server の設定*、507 ページを参照してください。
- 各要求についてドメイン名（www.domain.com）のみをログ記録し、ドメインの特定ページへのパス（/products/productA）をログ記録しないようにするには、**[full URL logging（完全な URL によるログ記録）]** を無効化します。*URL がログ記録される方法の設定*、524 ページを参照してください。

注意

組織がアクセスされた各サイトの完全な URL を含むレポートを必要とする場合は、[full UR logging] を有効化したままにしておく必要があります。そうしないと、サイト内の各ページが異なったカテゴリに含まれるか、または異なった理由で再分類される場合でも、レポートは分類されたサイトのドメイン（www.domain.com）だけを表示します。

- ログ記録を組織にとって必要なカテゴリに限定するには、**[selective category logging（選択可能なカテゴリのログ記録）]** を有効化します。*要求がログ記録される方法の設定、505 ページ*を参照してください。

> **注意**
> **[visits]** を有効化した場合、**[consolidation]**、または **[selective category logging]** がインターネット ブラウズ 時間の精度に影響を与えます。

しかし、高度な分析機能は、これらの設定によって部分的にのみ制約されます。サイトを分析すると、2 つの別個のログ記録が作成されます。

- **標準ログ記録**は、実施されているすべてのサイズ削減設定を活用します。これはすべての Web フィルタ レポートに利用できます。
- **高度な分析の記録**は、ほとんどのサイズ削減設定を無視します。すべての個別のヒットがログ記録され、すべてのカテゴリへの要求がログ記録され、レコードは統合されません。これらのレコードは、分析の結果としてサイトがブロックされたか許可されたかに関係なく生成されます。高度な分析のレコード記録では、[full URL logging] に関する設定のみが尊重されます。

いずれかのログ データベース サイズ削減オプションを有効化した場合、レポートが同じユーザ、期間、およびカテゴリに構成されていても、分析レポートで報告される数が標準レポートで報告される数と一致**しない**場合があります。たとえば、アクセス件数をログ記録することを選択した場合、スキャン機能の分析対象となっているサイトをユーザが要求すると、そのユーザ要求は標準レポートでは 1 件のアクセスとして表示されますが、高度な分析レポートでは複数のヒット件数として表示される可能性があります。

標準 アクティビティと高度な分析で同じようなデータを表示させるには、ログ データベース サイズ削減の設定を**無効化**します。これはデータベースを非常に大きくし、急速に成長させる可能性があるので、Log Database コンピュータが適切なサイズのハードディスク、処理能力、およびメモリー容量を持っていることを確認してください。

サイズ削減設定の構成の詳細については、*レポート管理、501 ページ*を参照してください。レポートの生成については、*プレゼンテーション レポート、161 ページ*および*調査レポート、187 ページ*を参照してください。

SSL 復号化バイパス

Web Security Help | Web Security ソリューション | バージョン 7.8.x

暗号化トラフィックを管理するために Content Gateway で SSL サポートを有効化したとき、下記の事柄を実行できます。

- カテゴリの設定を使用して、復号化および検査をバイパスするウェブサイトのカテゴリを指定できます。
- 復号化と検査をバイパスする信用あるクライアントを使用するためにクライアント IP アドレス、および IP アドレスの範囲のリストを作成できます。
- 復号化と検査をバイパスする信用ある宛先サーバーを使用するために宛先ホスト名、IP アドレス、および IP アドレスの範囲のリストを作成できます。

注意

Internet Explorer バージョン 8（IE8）には既知の制約があり、そのために一部のサイトが設定どおりにバイパスされません。IE8 は Server Name Indicator（SNI）を送信せず、オリジン サーバー証明書の中のホスト名がワイルドカード（*）を含む場合、共通名とホスト名は一致しません。その結果、カテゴリ検索は宛先 IP アドレスに対して実行されます。

カテゴリの設定

[Category（カテゴリ）] の設定では、事前定義済みの **[Privacy Category（プライバシー カテゴリ）]** グループは、規制的必要が認められるようなカテゴリを含んでいます。

デフォルトのプライバシー カテゴリは下記のカテゴリを含みます。

- 教育
- 金融情報＆サービス
- 政府
- 健康
- オンライン証券＆トレーディング
- 処方薬

これらのカテゴリに含まれるウェブサイトに関係するトラフィックに含まれる個人の ID 情報は復号化してはなりません。このタイプの情報を検査する責任を回避するために、これらのカテゴリの一部またはすべてを復号化バイパスの対象として指定できます。エンド ユーザーは、閲覧する ウェブサイトの証明書がオリジナルであることを確認することによって、そのサイトを復号化しないことを決定することができます。

SSL 復号化バイパスのデフォルトのプライバシー カテゴリを選択するには **[Settings] > [Scanning] > [SSL Decryption Bypass]** ページを順に選択し、下記の手順を実行します。

1. **[Select Privacy Categories（プライバシー カテゴリを選択）]** ボタンをクリックします。[Category Bypass（カテゴリ バイパス）] ボックスで選択されているデフォルトのグループを構成するウェブサイトのカテゴリのボックスをオンにします。
2. カテゴリ ツリーの右側の矢印をクリックして、プライバシー カテゴリを **[Categories selected for SSL decryption bypass（SSL 復号化バイパスに選択したカテゴリ）]** ボックスに追加します。

SSL 復号化バイパス用の独自のカテゴリ セットを作成できます。**[SSL Decryption Bypass]** ページで、復号化が許可されない個別のウェブサイト カテゴリを指定します。

1. バイパスするカテゴリまたはサブカテゴリを選択するために、チェックボックスをクリックします。
2. カテゴリ ツリーの右側の矢印をクリックして、選択したカテゴリを **[Categories selected for SSL decryption bypass]** ボックスに追加します。

カテゴリ ツリーからすべての選択をクリアするには、**[Clear All（すべてクリア）]** ボタンをクリックします。

リストから 1 つのカテゴリまたはサブカテゴリを削除するには、削除するカテゴリを選択し、**[Remove（削除）]** ボタンをクリックします。

クライアント リスト

SSL 復号化バイパスのためのクライアント IP アドレスまたは IP アドレス範囲を特定するには、下記の手順を実行します。

1. **[Add]** をクリックし、**[Add Client Entry（クライアント エントリを追加）]** ボックスにクライアント IP アドレスまたは IP アドレス 範囲を入力します（1 行に 1 つのエントリ）。

   IP アドレス範囲を指定する場合、最初のアドレスを最後のアドレスと分けるために [-]（ハイフン）を使用します。

   IPv6 アドレスは、明示的プロキシ トラフィックの場合のみ有効です。

2. リストのメンテナンスを容易にするために、エントリを特定する説明を追加します。
3. **[OK]** をクリックして、エントリをリストに追加します。

エントリを変更するには、その IP アドレスをクリックし、**[Edit Client Entry（クライアント エントリを編集）]** ボックスでエントリを変更します。変更を保存するには **[OK]** をクリックし、また変更を保存せずにダイアログ ボックスを閉じるには **[Cancel]** をクリックします。

リストからエントリを削除するには、エントリの隣のチェックボックスを選択し、**[Delete]** をクリックします。削除することを確認します。

完了したとき、**[OK]** をクリックして、変更をキャッシュします。

[Save and Deploy] をクリックするまで変更は適用されません。

宛先リスト

SSL 復号化バイパスのための宛先ホスト名、IP アドレスまたは IP アドレス範囲を特定するには、下記の手順を実行します。

1. **[Add]** をクリックし、**[Add Destination Entry（宛先エントリを追加）]** ボックスに宛先ホスト名、IP アドレスまたは IP アドレス 範囲を入力します（1 行に 1 つのエントリ）。
   - 簡単なホスト名を入力できます。

     例：**thissite.com**.

     ドメインと拡張子の両方を入力してください（**thissite.com** と **thissite.net** は、別個のホストです）。
   - 複数のラベルが付いたサイトを使用できます。

     例、**www.bbc.co.uk**
   - ワイルド カード [*] を使用して先頭のサブドメインのみを照合できます。

     例：***.yahoo.com**.
   - 完全なまたは一部のホスト名または URL を入力できます。先頭のスキーム [HTTPS://] は必要ありません。正確な照合は、指定した文字列で実行されます。

     例：**www.example.com/media/**

     または、**www.youtube.com/watch?v=**
   - アドレス範囲の最初のアドレスと最後のアドレスと分けるために [-]（ハイフン）を使用します。
   - IPv6 アドレスは、明示的プロキシ トラフィックの場合のみ有効です。

2. リストのメンテナンスを容易にするために、エントリを明確に特定する説明を追加します。
3. **[OK]** をクリックして、エントリをリストに追加します。

エントリを変更するには、ホスト名または IP アドレスをクリックし、**[Edit Destination Entry（宛先エントリを編集）]** ボックスでエントリを変更します。変更を保存するには **[OK]** をクリックし、また変更を保存せずにダイアログ ボックスを閉じるには **[Cancel]** をクリックします。

エントリを削除するには、エントリの隣のチェックボックスを選択し、**[Delete]** をクリックします。削除することを確認します。

完了したとき、**[OK]** をクリックして、変更をキャッシュします。

[Save and Deploy] をクリックするまで変更は適用されません。

10 ハイブリッド サービスの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websens 組織は、メイン オフィスやキャンパスではウェブセキュリティを提供するために堅牢なオンプレマイズ ソフトウェアを使用し、小規模な地域事業所やサテライトではハイブリッド サービス通じてインターネット要求を送信することができます。ハイブリッド サービスは、在宅勤務者などオフネットワークのユーザーや出張するユーザーなどにとっても役立ちます（*オフサイト ユーザーのハイブリッド管理、308 ページ*を参照）。

Web Security Gateway Anywhere を使用して、クライアントを定義し、同じユーザー インターフェース ― TRITON コンソール ― でオンプレマイズおよびハイブリッド インターネット アクセス管理のためのポリシーを作成します。また、これによっては設定およびレポート機能を中央管理できます。

ハイブリッド サービスを使用するには、下記の手順を実行します。

1. *ハイブリッド サービス アカウントをアクティブにする、262 ページ*
2. *フィルタ対象の場所を定義、263 ページ*
3. *ハイブリッド サービスによって管理されないサイトの指定、270 ページ*（もしあれば）
4. *ハイブリッド サービスへのユーザーのアクセスの設定、272 ページ*
5. *ハイブリッド ユーザーの識別、391 ページ*
6. *ユーザーおよびグループ データをハイブリッド サービスに送信、280 ページ*

ハイブリッド サービスがポリシー、ユーザー、およびグループの現在の情報を保持すること、およびオンプレマイズ レポーティング ソフトウェアがハイブリッド サービスにより管理されているユーザーからのデータをレポーティングしていたことを確認するために、*ハイブリッド サービスとの通信のスケジュール設定、290 ページ*を参照してください。

ハイブリッド サービス アカウントをアクティブにする

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *フィルタ対象の場所を定義*、263 ページ
- *ハイブリッド サービスによって管理されないサイトの指定*、270 ページ
- *ハイブリッド サービスへのユーザーのアクセスの設定*、272 ページ
- *ユーザーおよびグループ データをハイブリッド サービスに送信*、280 ページ
- *ハイブリッド サービスとの通信のスケジュール設定*、290 ページ

ハイブリッド サービスを設定して組織のインターネット要求の管理を開始する前に、コンタクト電子メール アドレスを送信してハイブリッド アカウントをアクティブ化する必要があります。それによって、Websense Web Security Gateway Anywhere のオンプレマイズとハイブリッド部分の間の接続が作成されます。

[Settings（設定）] > [General（一般）] > [Account（アカウント）] ページの [Hybrid Filtering（ハイブリッド フィルタリング）] セクションを使用して、Web Security 管理者のコンタクト電子メール アドレスおよび国を入力します（*アカウント情報の設定*、29 ページを参照）。

電子メール アドレスは、一般的には、組織のウェブ セキュリティの管理を担当するグループによってモニタされる別名です。このアカウントに送信された電子メールが速やかに受信され、処理されることが非常に重要です。

- Websense テクニカル サポートは、このアドレスを使用して、ハイブリッド サービスに影響を与える緊急の問題に関する通知を送付します。
- アカウントに設定上の問題がある場合、テクニカル サポートからの電子メール メッセージに迅速に対応できなかったためにサービスの中断が起こる可能性があります。
- 一定の稀な問題が発生した場合、電子メール アドレスは、Sync Service がハイブリッド サービスとの通信を再開できるようにするために必要な情報を送信するために使用されます。
- この電子メール アドレスは、マーケティング、セールス、または他の一般的な情報を送信するためには使用**されません**。

入力する国は、システムにタイム ゾーン情報を提供します。

アカウントのハイブリッド サービスをアクティブ化した後、ハイブリッド サービスによって管理される場所（IP アドレス、IP アドレス範囲、またはサブネットにより特定）、情報が Web セキュリティ ソフトウェアのオンプレマイズの部分とハイブリッドの部分の間で交換される方法、ハイブリッド サービスによって管理されるユーザーが認証される方法などを指定できます。

フィルタ対象の場所を定義

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ハイブリッド サービスによって管理されないサイトの指定*、270 ページ
- *ハイブリッド サービスへのユーザーのアクセスの設定*、272 ページ
- *ハイブリッド サービスとの通信のスケジュール設定*、290 ページ

ユーザーがハイブリッド サービスに要求を送信する場所に関する情報を表示、追加、編集するには、**[Settings] > [Hybrid Configuration（ハイブリッド設定）] > [Filtered Locations（フィルタ対象の場所）]** ページを順に選択します。

フィルタ対象の場所は、ハイブリッド サービスから見た時に、インターネット要求の発信元であるかのように見える外部 IP アドレス、IP アドレス範囲、またはサブネットです。Web Security Gateway Anywhere 環境では、オフサイトのユーザーに対して、そのユーザーがネットワーク内にいるときにそのユーザーからの要求がどのように管理されるかに関係なく、ハイブリッド ポリシーを適用できます。

- ネットワークの内外の両方でハイブリッド サービスによって管理されるユーザーの場合、そのネットワーク内の場所の詳細情報を入力し、ハイブリッド サービスによって管理される場所を指定します。オフサイト ユーザーがインターネット要求を行ったとき、適切なユーザーまたはグループベースのポリシーを適用できるようにするために、ハイブリット サービスにログオンするように要求されます。

  ハイブリッド サービスはネットワークの外側にホストされていますから、ハイブリッド サービスによって管理されるされるすべての場所は、インターネットから見ることのできる、**外部**アドレスでなければなりません。ハイブリッド サービスによる管理対象の場所は、下記の通りです。

  - Web Security Gateway Anywhere を使用ているオフィスの公開 IP アドレス
  - Network Address Translation（NAT）ファイアウォールの外部アドレス
  - 支店、リモート サーと、またはサテライト キャンパスなど

これらの場所の IP アドレスには該当しません。

- 個々のクライアント コンピュータの IP アドレス
- Websense Web Security Gateway Anywhere のオンプレマイズ コンポーネントによって使用されている Content Gateway コンピュータの IP アドレス

- ユーザーがネットワークに含まれていて、オンプレマイズ コンポーネント（Filtering Service）によって管理される場合、インターネット要求を送信する前に、ネットワーク内のユーザーかオフサイトのユーザーかを指定するためにブラウザ PAC ファイルを設定できます。

  ハイブリッド サービスによって生成された PAC ファイルを使用しているとき、この構成は、[Filtered Locations] ページで入力した設定に基づき自動的に行われます。ローカル Websense ソフトウェアによって管理されるユーザーを指定し、それらのオンプレマイズ ポリシーの実施がファイアウォール統合プロキシ、透過的プロキシ（例、透過的モードの Content Gateway）、または明示的プロキシのいずれを通じて行われるかを指定します。ネットワーク内のコンピュータから指定された場所でインターネット要求が明示的プロキシを通過する場合は、要求がその場所のユーザーに適切にルーティングされていることを確認するために、プロキシの場所（ホスト名または IP アドレス）およびポートを指定する必要があります。

指定した各場所は、名前および説明と、技術的詳細情報を組み合せたテーブルに表示されます。技術的詳細情報には、選択したプロキシ モード、場所のタイプ（単一の IP アドレス、IP アドレス範囲、またはサブネット）、および要求の発信元の実際の外部 IP アドレス（1 つまたは複数）が含まれます。

- 既存のエントリを編集するには、場所の **[Name]** をクリックし、次に*フィルタ対象の場所の追加または編集、265 ページ*を参照してください。
- 新しい場所を指定するには、**[Add（追加）]** をクリックし、次に*フィルタ対象の場所の追加または編集、265 ページ*を参照してください。
- 場所を削除するには、場所の名前の横のチェックボックスをオンにし、**[Delete（削除）]** をクリックします。
- フィルタ対象の場所で使用するためにオンプレマイズの明示的プロキシを追加および編集するには、**[Manage Explicit Proxies（明示的プロキシを管理）]** をクリックし、次に*明示的プロキシの管理、267 ページ*を参照します。

場所のエントリを追加または編集した場合、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

フィルタ対象の場所の追加または編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Filtered Locations] > [Add Filtered Location] または **[Edit Filtered Locations]** ページで以下の処理を行います。

- ハイブリッド サービスによって管理される場所（支店、リモート サイト、サテライト キャンパスなど）か、またはオフ サイトである場合にハイブリッド サービスによって管理されるユーザーを含む場所を指定する。
- ハイブリッド サービスによって管理される場所を指定する方法を変更する。

フィルタ対象の場所指定するか、または既存のエントリを更新するには、下記の手順を実行します。

1. 場所の **[Name（名前）]** を入力、検討、または更新します。名前は、一意な名前で、1 ～ 50 文字で指定します。名前には下記の文字を含めることはできません。

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   名前にはスペース、ダッシュ、アポストロフィーを含めることができます。

2. **[Description（説明）]** に場所の簡潔な説明を入力、検討、または更新します（最大 255 文字）。この説明は、[Filtered Locations] ページの場所の名前の横に表示されます。これはすべての管理者にその場所を明確に指定するものである必要があります。

   名前に適用される使用文字の制限は、説明にも適用されますが、2 つの例外があります。説明では、ピリオド（.）とカンマ（,）が使用できます。

3. フィルタ対象の場所の **[Time zone（タイム ゾーン）]** を選択または確認します。タイム ゾーン情報は、ポリシーの適用で使用され、適切なフィルターが適切な時刻に適用されるようにします。

   要求がハイブリッド サービスを経由する各場所は、異なるタイム ソーン設定にされることがあります。透過的プロキシまたは明示的プロキシが配置されている場所では、ポリシー実施のためのタイム ソーンとして、Filtering Service が実行しているコンピュータのタイム ゾーンを使用します。

4. **[Type（タイプ）]** フィールドに、下記のいずれかからこの場所を指定するために使用する方法を指定するか、または確認します。**[IP address]**、IP アドレスの **[Range]**、または **[Subnet]**。

   サブネットを指定する場合は、それを **[By bit range（CIDR）（ビット範囲を基準）]** または **[By subnet mask（サブネットを基準）]** のどちらを基準にして特定するかを指定し、次にビット範囲またはマスクを選択します。

5. この場所でフィルタリングされているクライアントがインターネットにアクセスする際に通過するファイアウォール（1 つまたは複数）の外部 IP アドレス、範囲、またはサブネットを入力、確認、または更新します。
   - ハイブリッド サービスによって管理される場所の場合、これらのアドレスはネットワークの外側から見ることができる外部 IP アドレスであり、内部（LAN）アドレスではありません。

     重要

     ハイブリッド サービスによって管理される場所を指定するとき、プライベート IP アドレス（範囲 10.0.0.0 ～ 10.255.255.255、172.16.0.0 ～ 172.31.255.255、および 192.168.0.0 ～ 192.168.255.255）を入力してはいけません。なぜなら、これらのアドレスはネットワークの外側から見ることができず、複数のローカル エリア ネットワーク内で使用されるので、ハイブリッド サービスはプライベート IP アドレスを有効なエントリとして受け入れないからです。

     この場所のプロキシモードが [Transparent（透過的）] または [Explicit（明示的）] である場合は、プライベート IP アドレスを入力できます。

   - Websense Web Security Gateway Anywhere のオンプレマイズ コンポーネントによって使用されている Content Gateway コンピュータの IP アドレスを含めてはいけません。
   - ハイブリッド サービスがそれらの場所から発信される要求を組織に固有のポリシーと関連付けられるようにするために、外部 IP アドレスは組織に対して一意なアドレスでなければならず、他のエンティティと共有するアドレスは使用できません。
6. 下記のどちらかを使って場所からの要求を管理する方法を指定、確認、または更新します。ハイブリッド サービスを使用する、またはローカル Websense ソフトウェアを使用する
7. サイトをローカル Websense ソフトウェアによって管理する場合は、下記のどちらかのプロキシを使ってこの場所のプロキシモードを選択、確認、または更新します。**[Transparent]** プロキシ、または **[Explicit]** オンプレマイズ プロキシを使用。

   [Explicit] を選択した場合、[Explicit Proxy Configuration（明示的プロキシ設定）] テーブルで少なくとも 1 つのプロキシを指定する必要があります。テーブルに新しいプロキシを追加するには、**[Add]** をクリックし、ポップ ウィンドウからプロキシの場所と優先順位を選択し、**[OK]** をクリックします。使用可能な明示的プロキシの詳細については、*明示的プロキシの管理、267 ページ*を参照してください。

フィルタ対象の場所は、リストの最初にあるプロキシを使用します。そのプロキシが利用できない場合は、フィルタ対象の場所からのウェブの要求はリストの次のプロキシにリダイレクトされます。順位を変更するには、リストにある任意のプロキシを選択し、次に **[Move Up（上に移動）]** または **[Move Down（下に移動）]** を選択し、リストでそのプロキシの位置を変更します。

テーブルからプロキシを削除するには、プロキシの名前の横のチェックボックスをオンにし、**[Delete]** をクリックします。削除されたプロキシはこのフィルタ対象の場所では利用できませんが、他のフィルタ対象の場所ではまだ選択できます。

8. **[OK]** をクリックして [Filtered Locations] ページに戻り、再び **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

明示的プロキシの管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

フィルタリング対象の場所で使用するために利用可能なオンプレマイズの明示的プロキシを表示、追加、編集するには、**[Filtered Locations] > [Manage Explicit Proxies（明示的プロキシを管理）]** ページを順に選択します。

指定した明示的プロキシは、プロキシ名、その IP アドレスまたはホスト名、HTTP、SSL、FTP アクセスに使用されるポート番号、現在プロキシを参照しているフィルタ対象の場所（もしあれば）を示すテーブルに表示されます。

- 既存のエントリを編集するには、プロキシの **[Name]** をクリックし、次に*明示的プロキシの追加または編集、268 ページ*を参照してください。
- 新しい明示的プロキシを指定するには、**[Add]** をクリックし、次に*明示的プロキシの追加または編集、268 ページ*を参照してください。
- プロキシを削除するには、プロキシの名前の横のチェックボックスをオンにし、**[Delete]** をクリックします。

注意

1 つ以上のフィルタ対象の場所によって使用されるプロキシは、削除できません。プロキシを削除する場合は、最初にフィルタ対象の場所を編集し、削除対象のプロキシを [Explicit Proxy Configuration] から削除します。

明示的プロキシの追加または編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

明示的プロキシを管理するとき、フィルタ対象の場所に使用するようにオンプレマイズの明示的プロキシに関する情報を指定するには、**[Add Explicit Proxy（明示的プロキシを追加）]** ページを使用し、また更新するには **[Edit Explicit Proxy（明示的プロキシを編集）]** ページを選択します。

1. プロキシの **[Name（名前）]** を入力、確認、または更新します。名前は、一意な名前で、1 ～ 50 文字で指定します。名前には下記の文字を含めることはできません。

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   名前にはスペース、ダッシュ、アポストロフィーを含めることができます。
2. 明示的プロキシの **[IP address or name]** を入力、確認、または更新します。これは下記のどちらかの形式にする必要があります。
   - IP アドレス（例、123.45.67.89）
   - ホスト名（例、my.example.com）

   IP アドレスまたはホスト名には、ポート番号（例、123.45.67.89:443）を含めることができます。
3. プロキシ ポートまたはポートを入力または更新します。少なくとも 1 つのプロキシのポート番号にする必要があります。このポートは、**HTTP ポート**、**SSL ポート**、**FTP ポート** のどれでもかまいません。
4. **[OK]** をクリックして、[Manage Explicit Proxies] ページに戻ります。

ハイブリッド サービスのフェイルオーバの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

明示的プロキシを使用するフィルタリング対象の場所に対して、ハイブリッド サービスのフェイルオーバを設定できます。これにより、他のプロキシが利用できなくなった場合にも、ユーザーがインターネットにアクセスでき、プロキシの実施が常に行われるようにすることができます。

Websense サービスがお客様所在地の最寄のデータ センターで正しい数のユーザーに対応できるようになるために、フィルタ対象の場所へのハイブリッド サービスに対するフェイルオーバは承認が必要です。フィルタ対象の場所のためのフェイルオーバがひとたび承認されると、フェイルオーバの詳細の変更やフェイルオーバの中断と再開の際に再度の承認は不要です。

ハイブリッド サービスのフェイルオーバを設定するには、下記の手順を実行します。

1. **[Hybrid Configuration] > [Filtered Locations]** ページを順に選択して、編集するフィルタ対象の場所を選択します。この場所は、プロキシ モードが [Explicit] に設定されているローカル Websense ソフトウェアによって管理される場所でなければなりません。
2. **[Advanced（詳細）]** をクリックします。
3. **[Enable failover to hybrid service（ハイブリッド サービスのフェイルオーバを有効化）]** をオンにします。
4. **[Number of users filtered by this filtered location（このフィルタ対象の場所によってフィルタリングされるユーザーの数）]** を入力します。
5. フィルタ対象の場所に **[Nearest data center（最も近いデータ センター）]** を選択します。
6. **[OK]** をクリックして [Filtered Locations] ページに戻り、再び **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

フィルタ対象の場所のフェイルオーバーが承認されたとき、[System] ダッシュボードと [Status（ステータス）] > [Alerts（アラート）] ページにアラートが表示されます。[Status] > [Hybrid Service（ハイブリッド サービス）] ページを順に選択してすべてのフェイルオーバ要求の承認ステータスを表示できます。

注意

Internet Explorer で自動プロキシ キャッシングが無効化されている場合、エンド ユーザーがページを閲覧するたびにブラウザがプロキシのリストをチェックすため、アクセスに時間がかかることがあります。自動プロキシ キャッシングが有効化されている場合は、ブラウザは、起動時のみプロキシ リストをチェックします。詳細については、http://support.microsoft.com/kb/271361 の Microsoft による関連する説明を参照してください。

ハイブリッド サービスによって管理されないサイトの指定

関連項目：

- *フィルタ対象の場所を定義、263 ページ*
- *ユーザーおよびグループ データをハイブリッド サービスに送信、280 ページ*
- *ハイブリッド サービスとの通信のスケジュール設定、290 ページ*

クライアントに無制限のアクセスを許可するターゲット サイトに関する情報を検討、追加、または編集するには、**[Settings] > [Hybrid Configuration] > [Unfiltered Destinations（フィルタなし宛先）]** ページを順に選択します。クライアントは、フィルタ対象の場所でハイブリッド サービスまたはオンプレマイズの明示的プロキシを使用していた場合そのどちらかへ要求を送信しないで、直接にこれらのサイトにアクセスできます。通常、フィルタなし宛先には、組織の Web メールサイト、内部 IP アドレス、Microsoft の更新のサイトを含みます。

ヒント

最善の方法として、組織の ウェブメール アドレスをフィルタなし宛先として追加します。それによって、下記の事柄を確実にします。

- プロキシまたはハイブリッド サービスによってすべての要求がブロックされている状況で、テクニカル サポートからのメッセージにアクセスできる。
- ハイブリッド サービスのパスワードを忘れた（または作成していなかった）オフサイトのユーザーが電子メールを通じてそれを取得できる。

ここにリストされる宛先は、ユーザーのブラウザがハイブリッド サービスに接続する方法を指定する Proxy Auto-Configuration（PAC）ファイルに追加されます（*ハイブリッド サービスへのユーザーのアクセスの設定、272 ページ* を参照）。デフォルトでは、PAC ファイルは、ルーティングできない IP アドレス範囲とマルチキャストの IP アドレス範囲をプロキシの実施から除外します。そのため、RFC 1918 または RFC 3330 で指定されているプライベート IP アドレス範囲を使用している場合は、ここにそれらの IP アドレス範囲を入力する必要はありません。

指定した各フィルタなし宛先は、名前および説明と技術的設定の詳細情報を組み合せたテーブルに表示されます。技術的詳細情報には、宛先を指定する方法（IP アドレス、ドメイン、またはサブネット）、およびユーザーが直接にアクセスできる実際の IP アドレス、ドメイン、またはサブネットが含まれます。

- 既存のエントリを編集するには、場所の **[Name]** をクリックし、次に *フィルタなし宛先の追加または編集、271 ページ*を参照してください。
- 新しい場所を指定するには、**[Add（追加）]** をクリックし、次に *フィルタなし宛先の追加または編集、271 ページ*を参照してください。
- フィルタなし宛先を削除するには、宛先名の横のチェックボックスをオンにし、**[Delete]** をクリックします。

フィルタなし宛先のエントリを追加または編集した場合、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

フィルタなし宛先の追加または編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ユーザーがハイブリッド サービスまたはオンプレマイズの明示的プロキシに要求を送信せずに、直接にアクセスできる URL（1 つまたは複数）を指定、または変更するには、**[Unfiltered Destinations] > [Add Unfiltered Destination（フィルタなし宛先を追加）]** または **[Edit Unfiltered Destination（フィルタなし宛先を編集）]** ページを順に選択します。

1. プロキシの **[Name（名前）]** を入力、確認、または更新します。名前は、一意な名前で、1 ～ 50 文字で指定します。名前には下記の文字を含めることはできません。

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   名前にはスペース、ダッシュ、アポストロフィーを含めることができます。

2. **[Description]** に宛先の短い説明を入力または更新します。この説明は [Unfiltered Destinations] ページのフィルタされていない宛先名の隣に表示されます。これはすべての管理者がターゲットサイト（1 つまたは複数）を明確に指定するものである必要があります。

   名前に適用される使用文字の制限は、説明にも適用されますが、2 つの例外があります。説明では、ピリオド（.）とカンマ（,）が使用できます。

3. **[Type]** フィールドでは、この宛先をどのタイプとして指定、確認、または変更するかを指定します：**[IP address]**、**[Domain]**、または **[Subnet]**。

   サブネットを指定する場合は、それを **[By bit range（CIDR）（ビット範囲を基準）]** または **[By subnet mask（サブネットを基準）]** のどちらを基準にして特定するかを指定し、次にビット範囲またはマスクを選択します。

4. ユーザーがハイブリッド サービスまたはオンプレマイズの明示的プロキシに要求を送信せずにアクセスできる IP アドレス、ドメイン、またはサブネットを入力、確認、または更新します。
5. 下記の場合にこのフィルタなし宛先が適用する **[Proxy（プロキシ）]** のタイプを選択または確認します。
   - すべてのハイブリッド ユーザーがハイブリッド サービスに要求を送信せずに、直接にアクセスできるようにするとき、**[Hybrid（ハイブリッド）]** を選択します。
   - オンプレマイズの明示的プロキシを使用しているフィルタ対象の場所にいるすべてのユーザーが宛先に直接にアクセスできるようにするとき、**[Explicit（明示的）]** を選択します。
   - フィルタ対象の場所からのハイブリッド サービスおよびオンプレマイズのプロキシによって管理されるすべてのユーザーが宛先に直接にアクセスできるようにするとき、**[Hybrid and Explicit（ハイブリッドおよび明示的）]** を選択します。
6. **[OK]** をクリックして [Unfiltered Destinations] ページに戻り、再度 **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

ハイブリッド サービスへのユーザーのアクセスの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ポリシーの実施にハイブリッド サービスを使用するためには、ユーザーがハイブリッド サービスに接続する方法とハイブリッド サービスによって管理される方法を設定する必要があります。そうするには、**[Settings] > [Hybrid Configuration] > [User Access（ユーザーのアクセス）]** を順に選択します。

[Proxy Auto-Configuration（PAC）File] セクションは、ユーザーのブラウザが PAC ファイルを取得する URL を表示します（*PAC ファイルとは、278 ページ*を参照）。

PAC ファイルは、ブラウザがハイブリッドに送信する要求、およびターゲットサイトに直接に送信される要求を指定します（*ハイブリッド サービスによって管理されないサイトの指定、270 ページ*を参照）。また、すべての場所でトラフィックを正しくルーティングできるようにするために、PAC ファイルは、フィルタ対象の場所、およびオンプレマイズ時にユーザーのインターネット アクセスを明示的プロキシまたは透過的プロキシを通じて管理する場所のプロキシ設定に関する情報も含みます。

> **注意**
> PAC ファイルを使用するためにユーザーのブラウザを設定する方法の詳細は、ブラウザおよびネットワーク環境によって異なります。たとえば、Microsoft Active Directory と Internet Explorer または Mozilla Firefox を使用している場合、グループ ポリシーを使用して処理を自動化できます。

デフォルト PAC ファイルはポート 8082 を通じて取得されます。ユーザーが、ポート 8082 がロック ダウンされている場所から PAC ファイルを要求した場合、ユーザーはその PAC ファイルにアクセスできません。この場合、このセクションで 2 番目の PAC ファイル アドレスを使用することによって、ユーザーはポート 80 を通じて PAC フィアルおよびハイブリッド サービスにアクセスできるようになります。リモート ユーザーも、ポート 8081 がロック ダウンしているネットワークからアクセスを要求する場合は、ポート 80 の PAC ファイル アドレスを使用する必要があります。ユーザーがポート 8082 上の PAC ファイルにアクセスできる場合でも、ポート 8081 は、ハイブリッド サービスを使用できるようにするために必要な標準ポートです。

> **注意**
> Web Security Gateway Anywhere の旧バージョンでの PAC ファイルは、[User Access] ページに表示される URL とは別の URL を使用します。旧バージョンで PAC ファイルを配備している場合は、希望しない限り URL を変更する必要はありません。Web Security Gateway Anywhere の以前のバージョンで提供されている PAC ファイルの URL は引き続き有効です。

ハイブリッド サービスが組織のポリシー情報にアクセスできない場合に、**[Availability（可用性）]** セクションを使用して、すべてのインターネット要求を許可するまたはブロックするかどうかを指定します。

[Time Zone] の下に表示されるドロップダウン リストを使用して、下記の状況でポリシーを適用するときに使用するデフォルトのタイム ゾーンを選択します。

- ユーザーが既存のフィルタ対象の場所に含まれない IP アドレスからハイブリッド サービスに接続している（*フィルタ対象の場所を定義、263 ページ*を参照）。

  デフォルトのタイム ゾーンが使用されている（たとえば、オフサイトのユーザーによって）、または他のユーザーがハイブリッド サービスに自己登録を行っている。
- フィルタ対象の場所のタイム ゾーン情報が利用できない。

ハイブリッド サービスによって表示されるブロック ページのカスタマイズされたロゴまたはテキストを指定するには、**[Custom End User Block Page（カスタム エンド ユーザー ブロック ページ）]** セクションを使用します（*ハイブリッド ブロック ページのカスタマイズ、276 ページ*を参照）。

ユーザーが該当する Websense 通知ページを表示するために HTTPS 要求を発行できるようにするには、**[HTTP Notification Pages（HTTP 通知ページ）]** セクションを使用します（*HTTP 通知ページの有効化、277 ページ*を参照）。

ハイブリッド サービスが Websense Directory Agent によって収集されたディレクトリ データを使用してユーザーを特定する場合は、**[Hybrid Configuration] > [Shared User Data（共有ユーザー データ）]** ページでユーザーのアカウントのハイブリッド パスワードを設定できます（*ユーザーおよびグループ データをハイブリッド サービスに送信、280 ページ*を参照）。組織が Directory Agent によって収集されたディレクトリ データを使って、フィルタ対象の場所以外からハイブリッド サービスに接続するユーザーを識別していない場合、ユーザーがそのサービスに**自己登録**できるようにすることができます。それによって **[Registered Domains（登録済みドメイン）]** で指定したドメインに関連付けられている電子メール アカウントをもつユーザーが、ハイブリッド サービスによって識別されるようになります。

認識されていない IP アドレスからインターネット アクセスを要求するユーザーは、自己登録するように要求されます。ユーザーの電子メール アドレスのドメイン部分は、ユーザーを組織と関連づけるために使用し、それによって適切なデフォルト ポリシーが適用されます。

組織に関連付けることができないユーザーは、ハイブリッド サービスのデフォルト ポリシーを受け取ります。

- ドメインを追加するには、**[Add]** をクリックします（*ドメインの追加、275 ページ*を参照）。
- ドメインまたはその属性を編集するには、ドメイン エントリをクリックします（*ドメインの編集、275 ページ*を参照）。

また、ユーザーがネットワーク内にいるとき、またはフィルタ対象の場所から接続するときにどのようにフィルタリングされるかに関わりなく、そのユーザーがオフサイトの未知の IP アドレスから接続しているときに、ハイブリッド ポリシーの実施を適用できます。[Off-site Users（オフサイト ユーザー）] で **[Enable hybrid filtering of off-site users（オフサイト ユーザーのハイブリッド フィルタリングを有効化）]** をオンにします。

このボックスをオフにした場合は、未知の IP アドレスから接続するすべてのユーザーをフィルタリングできなくなります。

詳細は、*オフサイト ユーザーのハイブリッド管理、308 ページ*を参照してください。

ドメインの追加

Web Security Help | Web Security ソリューション | バージョン 7.8.x

組織に属するドメインおよびサブドメイン（もしあれば）を特定するには、**[User Access] > [Add Domain（ドメインを追加）]** ページを順に選択します。それによって、指定したドメイン内の電子メール アドレスをもつユーザーがハイブリッド サービスに自己登録する（自己を認証する）ことができるようになります。これは、一般的には Directory Agent を使ってユーザー情報をハイブリッド サービスに送信しない組織でのみ有効化されます。

ハイブリッド サービスは、自己登録したユーザーに関するユーザー名情報をレポーティングに使用するオンプレマイズのコンポーネントに提供できません。要求が発信された IP アドレスのみがログ記録されるだけです。

1. 組織に属する **ドメイン** 名を、**sampledomain.org** の形式で入力します。
2. ハイブリッド サービス管理を簡素化するために基準点としてドメインの明確な**説明**を入力します。
3. ドメインとそのサブドメインの両方に含まれている電子メール アドレス（例、**university.edu** と **humanities.university.edu**）をもつユーザーが自己登録できるようにする場合は、**[Include subdomains（サブドメインを含む）]** をオンにします。
4. **[OK]** をクリックして、[User Access] ページに戻ります。
5. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

ドメインの編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ユーザーがハイブリッド サービスの自己登録をできるようにドメイン エントリを変更するには、**[User Access] > [Edit Domain（ドメインを変更）]** ページを順に選択します。

1. ドメインの **[Name]** を確認し、必要な場合は変更を行います。
2. 必要に応じて **[Description]** を更新します。
3. サブドメインに含まれる電子メール アドレスを有効と見なすかどうかを変更するには、**[Include subdomains（サブドメインを含める）]** のオン / オフを切り替えます。
4. **[OK]** をクリックして、[User Access] ページに戻ります。
5. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

ハイブリッド ブロック ページのカスタマイズ

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ハイブリッド サービスがリソースへのアクセスを拒否するとき、デフォルト ブロック ページを提供します。デフォルト ページを使用するか、またはニーズに適合するようにページ テキストを変更できます。たとえば、下記のようにカスタマイズできます。

- 組織のインターネット利用ポリシーについての情報を追加します。
- インターネット使用ポリシーについて人事部または Websense 管理者に連絡する方法を提供します。
- 組織のロゴを追加します。

組織のロゴのカスタマイズ

ハイブリッド ブロック ページに表示されるロゴをカスタマイズする場合は、Websense **ssdata** ディレクトリ（デフォルトでは、Windows の場合は C:\Program Files *または* Program Files（x86）\Websense\Web Security\bin\ssdata\、Linux の場合は /opt/websense/bin/ssdata/）で **[logo]** と言う名前のディレクトリを作成します。次にロゴ ファイルをそのディレクトリに入れます。

ロゴは、JPEG、GIF、または PNG ファイルでなければなりません。これらの拡張子のいずれかをもつファイルが **logo** ディレクトリにある場合、Sync Service はそのファイルを検出し、データをハイブリッド サービスに送信します。Sync Service で送信するファイルは 0 KB より大きく、かつ 50 KB 未満でなければなりません。Sync Service は、ファイルの新しいバージョンがあるときそれを検出し、ファイルのバージョンをハイブリッドサービスで更新します。このディレクトリに複数の有効なファイルがある場合、Sync Service は、最新のファイルを使用します。

[Hybrid Service] ページは、Sync Service がカスタマイズしたブロック ページ ロゴをハイブリッド サービスに送信する日付と時刻を表示します（*モニタのハイブリッド サービスとの通信、298 ページ*を参照）。

カスタマイズしたロゴ ファイルの使用を停止するには、**logo** ディレクトリからそのファイルを削除します。

注意

[Hybrid Configuration] > [User Access] ページで **[Use a custom block page title and message（カスタム ブロック ページ タイトルおよびメッセージを使用）]** をオフにしても、ブロック ページからカスタマイズした ロゴを自動的には削除されません。Sync Service がハイブリッド サービスへファイルをプッシュするのを停止するには、logo ファイルを logo ディレクトリから削除する必要があります。

テキストのカスタマイズ

1. **[Hybrid Configuration] > [User Access]** ページで、**[Use a custom block page title and message（カスタム ブロック ページ タイトルおよびメッセージを使用）]** をオンにします。
2. **[Title（タイトル）]** および **[Message（メッセージ）]** にページのタイトルとメッセージを入力します。これはプレーン テキストでなければなりません。HTML タグを付けてはいけません。
3. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

HTTP 通知ページの有効化

Web Security Help | Web Security ソリューション | バージョン 7.8.x

SSL（Secure Sockets Layer）は、インターネット上のセキュアなデータ転送のための業界標準です。これは、認証機関により発行されサーバーにより承認されている信頼される証明書のシステムをベースとしています。

ハイブリッド サービス用に Websense SSL 証明書をインストールした場合、ハイブリッド プロキシはユーザーに通知ページ（例、SSL サイトが通知を必要とするカテゴリに含まれている場合はブロックページ、認証を必要とする場合はそれに対応するページ）を提供するために、新しいブラウザ（Internet Explorer 8 以上、および Firefox 3.5 以上）との SSL チャネルを確立できます。

パフォーマンスを維持するために、HTTPS トラフィックのみがこの方法で転送されます。HTTP トラフィックはプロキシを経由して要求されたサイトに転送されます。

ハイブリッド ユーザーが HTTPS を使ってサイトを参照しているときに通知ページを表示できるように、各クライアント コンピュータ上にハイブリッド プロキシへの SSL 要求のための認証機関として機能するルート証明書が必要です。

ハイブリッド ルート証明書をハイブリッド サービスを使用するすべてのクライアントにインストールするには、下記の手順を実行します。

1. **[Hybrid Configuration] > [User Access]**ページを順に選択し、**[View Hybrid SSL Certificate（ハイブリッド SSL 証明書を表示）]** をクリックします。
2. 証明書ファイルを任意の場所に保存します。
3. SSL 証明書を優先する管理または配備方法（例、Microsoft Group Policy Object（GPO）またはサードパーティの配備ツール）を使ってハイブリッド ユーザーに配備します。

証明書を配布した後、**[Use the hybrid SSL certificate to display a notification page for HTTPS requests when required（要求された時に HTTPS 要求の通知ページを表示するためにハイブリッド SSL 通知を使用）]** をオンにして、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

PAC ファイルとは

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Proxy Auto-Configuration ファイルは、ブラウザが要求を処理する方法を決定するために呼び出す JavaScript 関数定義です。ハイブリッド ポリシーの実施を可能にするために使用する PAC ファイルは、いくつかのグローバル設定を含んでおり、このファイルによってユーザーがハイブリッド サービスに要求を送信せずに直接にアクセスできるサイト（例、イントラネット サイト、組織のウェブメール）を設定することができます（*ハイブリッド サービスによって管理されないサイトの指定、270 ページ*を参照）。

クライアント コンピュータ上でハイブリッド サービスを使用する場合は、各クライアント上でブラウザが PAC ファイルをホストしている URL を参照するように設定しなければなりません。この URL は、**[Hybrid Configuration] > [User Access]** ページに表示されます（*ハイブリッド サービスへのユーザーのアクセスの設定、272 ページ*を参照）。

PAC ファイルを使用するためにブラウザを設定する方法の詳細は、ブラウザおよびネットワーク環境によって異なります。たとえば、Microsoft Active Directory と Internet Explorer、または Mozilla Firefox を使用している場合、グループ ポリシーを使用して処理を自動化したい場合があります。また、ユーザーにブラウザを手動で設定するように指示できます。

- Microsoft Internet Explore の場合は、**[Tools（ツール）] > [Internet Options（インターネット オプション）]** を順に選択し、**[Connections（接続）]** タブをクリックします。**[LAN Settings（LAN の設定）]** をクリックし、**[Use automatic configuration script（自動構成スクリプトを使用）]** をオンにします。**[Address（アドレス）]** フィールドに PAC ファイルの URL を入力します。
- Mozilla Firefox の場合は、**[Tools] > [Options（オプション）]** を順に選択し、**[Advanced（拡張）]** アイコンをクリックし、**[Network（ネットワーク）]** タブを選択します。[Connection] で、**[Settings]** をクリックし、次に **[Automatic proxy configuration URL（自動プロキシ構成 URL）]** を選択します。空白のフィールドに PAC ファイルの URL を入力します。

デフォルトの PAC ファイルは、Websense によって供給され、またハイブリッド サービスからのデフォルトの設定と [Hybrid Configuration] のページで行う変更を含みます。PAC ファイルをカスタマイズする場合は、Websense **ssdata** ディレクトリに **[pac]** という名前のディレクトリを作成します（デフォルトでは、Windows の場合は \Program Files または Program Files（x86）\Websense\Web Security\bin\ssdata\pac、Linux の場合は /opt/websense/bin/ssdata/pac）。次に下記のどちらかのオプションがあります。

- 自らの PAC ファイルを使用するには、**websense.pac** と言う名前のフィルを作成し、そのファイルを Websense **pac** ディレクトリに格納します。
- デフォルトの PAC ファイルにカスタマイズしたフラグメントを追加するには、JavaScript フラグメントを **customfinal.pac** という名前のファイルに入れ、そのファイルを Websense **pac** ディレクトリに入れます。このフラグメントはデフォルトの PAC ファイルに付加され、トークン _CUSTOMFINALPAC_ を置換します。

注意

カスタマイズした **websense.pac** ファイルには、下記の関数を含める必要があります。

```
function FindProxyForURL(url, host){}
```

この関数がファイルに含まれていない場合、ファイルはハイブリッド サービスによって拒否されます。

これらのいずれのファイルが **pac** ディレクトリにある場合、Sync Service はそのファイルを検出し、データをハイブリッド サービスに送信します。Sync Service で送信するファイルは 0KB より大きく、かつ 50KB 未満でなければなりません。Sync Service は、PAC ファイルの新しいバージョンがあるときそれを検出し、ファイルのバージョンをハイブリッドサービスで更新します。

カスタム PAC ファイルについては、カスタム ファイルまたはカスタム フラグメントのいずれか（両方ではなく）をセットアップすることを推奨します。両方のファイルが **pac** ディレクトリにある場合は、完全にカスタマイズした PAC ファイルとカスタマイズしたフラグメント スーツのどちらがニーズに適合するか判断し、ニーズに適合しないファイルをディレクトリから削除することを推奨します。

カスタマイズした PAC ファイルまたはフラグメントの使用を停止するには、**pac** ディレクトリからそのファイルまたはフラグメントを削除します。

[Hybrid Service] ページは、使用している PAC ファイルの種類を表示し、Sync Service がハイブリッド サービスにカスタマイズ ファイルまたはフラグメントを最後に送信した日付および時刻をリストします（*モニタのハイブリッド サービスとの通信、298 ページ*を参照）。

PAC ファイルに習熟していない場合は、インターネットで基本情報について検索しておくと役に立ちます。Wikipedia には、優れた紹介の記事があります。また、優れた詳細情報のウェブサイトおよびいくつかの PAC ファイルの例が http://www.findproxyforurl.com/ にあります。

ユーザーおよびグループ データをハイブリッド サービスに送信

組織がサポートされている、LDAP ベースのディレクトリ サービス（Windows Active Directory（Native Mode）、Oracle（Sun Java）Directory Server、または Novell eDirectory）を使用している場合、ユーザーおよびグループ データを収集して、それをハイブリッド サービスに送信できます。これは、下記の 2 つの Websense コンポーネントを使用することによって実現されます。

- **Websense Directory Agent** は、Directory Server からユーザーおよびグループ情報を収集し、ハイブリッドサービスのためにそれを照合します。
- **Websense Sync Service** は、ポリシー、レポーティング、カスタム PAC ファイル情報、およびユーザー/ グループ データをオンプレマイズのシステムとハイブリッド システムの間で転送します。

ハイブリッド サービスが適切に設定された場合、Directory Agent からの情報を使用して、ユーザーベースおよびグループベースのポリシーを適用できます。

組織が Windows Active Directory をミックス モードで使用している場合、ユーザーおよびグループ データを収集してハイブリッド サービスに送信することはできません。

ハイブリッド サービスが Directory Agent によって収集したディレクトリ データを使用してユーザーを特定する場合は、下記の 2 つのオプションがあります。

- Directory Agent によって送信されるすべてのユーザー アカウントのハイブリッド ログオン パスワードを自動的に作成するようにハイブリッド サービスを設定する。電子メール メッセージの突然の殺到を避けるために、パスワードは時差的な間隔で各ユーザーの電子メール アドレスに送信されます。
- ユーザーがフィルタ対象の場所の外側からハイブリッド サービスに最初に接続するとき、ユーザーに独自のパスワードを要求させる。処理を正常に完了させるために、ユーザーは、Directory Agent によって送信されたアカウントに対応する電子メール アドレスを提供しなければなりません。次にパスワードがその電子メール アドレスに送信されます。

  そのため、組織の Web 電子メール アドレスがフィルタなし宛先として追加されていることを確認してください。*ハイブリッド サービスによって管理されないサイトの指定、270 ページ*を参照してください。

Directory Agent の設定をハイブリッド サービス用に設定する

Web Security Help | Web Security ソリューション | バージョン 7.8.x

現在の Directory Agent の設定を表示および編集し、Directory Agent を Sync Service と通信するように設定するには、**[Settings] > [Hybrid Configuration] > [Shared User Data（共有ユーザー データ）]** を順に選択します。

ページの上部の近くのテーブルは、**[Settings] > [General] > [Directory Services（ディレクトリ サービス）]** ページで識別された Active Directory グローバル カタログをリストします。そのページで、グローバル カタログ サーバーを追加または削除するか、または Websense ソフトウェアによって使用されているディレクトリ サービスを変更します。

注意

[Directory Services] ページから Active Directory サーバーを削除した場合は、下記の手順を実行し、そのサーバーが完全に Directory Agent の設定から削除されていることを確認します。

- ソフトウェアの配備：**Websense/Web Security/bin/snapshots** ディレクトリにあるすべてのファイルを削除します。次に **[Settings] > [Hybrid Configuration] > [Scheduling（スケジュール設定）]** を順に選択し、[Send Update Now（すぐに更新を送信）] の下の **[Send（送信）]** をクリックします。
- アプライアンスの配備：サポートが必要な場合、Websense テクニカル・サポートにご連絡ください。

Directory Agent がハイブリッド サービス用のディレクトリおよびパッケージを検索する方法を絞り込むには、テーブルにある IP アドレスまたはホスト名をクリックします。*ハイブリッド サービス用にデータを収集する方法を設定する、282 ページ*を参照してください。

ハイブリッド ユーザーを特定するために定義されているグローバル カタログ ディレクトリのコンテクストを表示するには、テーブルの [Contexts（コンテクスト）] の下の **[View Context（コンテクストを表示）]** をクリックします。*ディレクトリ コンテクストの追加および編集、286 ページ*を参照してください。

ハイブリッド サービスが確認するすべてのユーザーのアカウントに対してパスワードを生成するように指定するために、**[Generate User Passwords（ユーザー パスワードを作成）]** セクションにスクロールして、**[Automatically generate and email passwords（パスワードを自動的に生成し電子メール送信）]** をオンにします。

Directory Agent データがハイブリッド サービスに送信されるようにするために、下記の手順を実行します。

1. **[Synchronize User Data（ユーザー データを同期化）]** セクションにスクロールします。
2. Sync Service コンピュータの **[Name or IP address（名前または IP アドレス）]** および Sync Service 通信に使用する **[Port（ポート）]**（デフォルトでは 55832）を確認します。

   ほとんどの設定では、これらのフィールドは自動的に入力されますが、必要に応じて手動で更新することができます。
3. **[Test Connection（テスト接続）]** をクリックして、Directory Agent がデータを Sync Service に送信できることを確認します。テストは 1 分以上かかることがあります。
   - 接続が確立すると、成功したことを知らせるメッセージが表示されます。
   - 接続ができなかった場合は、Sync Service コンピュータの IP アドレスまたはホスト名および通信ポートを確認してください。また、Sync Service コンピュータがオンにされていること、Sync Service が実行中であること、ネットワーク ファイアウォールが Sync Service ポートでの接続を許可していることも確認してください。
4. 完了したら、**[OK]** をクリックして変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

ハイブリッド サービス用にデータを収集する方法を設定する

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Directory Agent が選択されたディレクトリ サーバーを検索し、ユーザーおよびグループ情報をハイブリッド サービスとしてパッケージする方法を絞り込むには、**[Shared User Data] > [Active Directory（Native Mode）（Active Directory（ネイティブ モード））]** ページを順に選択します。

ディレクトリからユーザーおよびグループ データを収集する時使用する **[Root Context（root コンテクスト）]** を入力するには、[Root Context for Hybrid Filtering Users（ハイブリッド フィルタリング ユーザーの root コンテクスト）] の下の **[Add]** をクリックします。コンテクストを絞り込むと、速度と効率が高まります。*ディレクトリ コンテクストの追加および編集、286 ページ*を参照してください。

警告

ハイブリッド サービスがサポートできるグループの数に制限があります。制限は多くの要因の影響を受けますが、制限を超えた場合、ユーザー要求は適切にフィルタリングされません（サービス を開始できません）。

組織のディレクトリ フォレストが大きく、多数のグループが含まれる場合、Directory Agent がハイブリッド サービスに要求が送信されたユーザーを管理するために必要な情報だけをアップロードするように設定してください。アップロードするグループだけを選択するか、または絞り込んだ root コンテクストを設定することができます。

ハイブリッド サービスによって管理されるユーザーだけを含むコンテクストを指定することを推奨します。

Active Directory を使用し、複数の Directory Agent インスタンスがある場合は、各インスタンスが一意な、重複しない root コンテクストをもっていることを確認してください。特に下記の場合に、そのことについて注意してください。

- 複数の Directory Agent インスタンスが 同じ Active Directory サーバーを管理する複数のドメイン コントローラに接続するように接続されている。
- 1 つの Directory Agent インスタンスが Active Directory 親ドメインと通信するように設定され、他の Directory Agent インスタンスが Active Directory 子ドメイン（別のグローバル カタログ サーバー）と通信するように設定されている。

ディレクトリ検索結果から重複や他の不必要なエントリを除去するためにパターンまたは検索フィルタを指定することによって、ハイブリッド サービスに送信するデータをさらに絞り込むことができます。詳細は、*検索結果の最適化*、289 ページを参照してください。

Oracle (Sun Java) Directory Server とハイブリッド サービス

組織が Oracle（Sun Java）Directory Server を使用している場合は、Directory Agent がディレクトリを検索し、ハイブリッド サービス用にユーザーおよびグループ情報をパッケージする方法を絞りこむには、**[Settings] > [Hybrid Configuration] > [Shared User Data]** を順に選択します。

重要

ユーザーおよびグループ情報をハイブリッド サービスに送信するために Sun Java System Directory または Oracle Directory Server のいずれかのバージョンを使用するには、Directory Agent の設定変更が必要です。

das.ini ファイル（Directory Agent コンピュータの Websense **bin** ディレクトリに格納されています）を開き、下記のセクションを見つけます。

```
# Enable next two parameters if your DS
is Sun Java
# GroupMembershipAttribute=uniqueMember
# MemberOfAttribute=memberOf
```

これらの行の先頭から記号 # を削除して GroupMembershipAttribute および MemberOfAttribute パラメータを有効化し、次にそのファイルを保存し、Directory Agent を再起動します。

1. ディレクトリからユーザーおよびグループ データを収集する時使用する **[Root Context（root コンテクスト）]** を入力するには、[Root Context for Hybrid Filtering Users（ハイブリッド フィルタリング ユーザーの root コンテクスト）] の下の **[Add]** をクリックします。コンテクストを絞り込むと、速度と効率が高まります。*ディレクトリ コンテクストの追加および編集、286 ページ*を参照してください。

   ハイブリッド サービスによって管理されるユーザーだけを含むコンテクストを入力します。

2. [Synchronize User Data] の下の Sync Service コンピュータの **[Name or IP address（名前または IP アドレス）]** および Sync Service 通信に使用する **[Port（ポート）]**（デフォルトでは 55832）を確認します。

   これらのフィールドは自動的に入力されますが、必要に応じて手動で更新することができます。

3. **[Test Connection（テスト接続）]** をクリックして、Directory Agent がデータを Sync Service に送信できることを確認します。テストは 1 分以上かかることがあります。
   - 接続が確立すると、成功したことを知らせるメッセージが表示されます。
   - 接続ができなかった場合は、Sync Service コンピュータの IPv4 アドレスまたはホスト名および通信ポートを確認してください。また、Sync Service コンピュータがオンにされていること、Sync Service が実行中であること、ネットワーク ファイアウォールが Sync Service ポートでの接続を許可していることも確認してください。

ディレクトリ検索結果から重複や他の不必要なエントリを除去するためにパターンまたは検索フィルタを指定することによって、ハイブリッド サービスに送信するデータをさらに絞り込むことができます。詳細は、*検索結果の最適化、289 ページ*を参照してください。

Novell eDirectory とハイブリッド サービス

Web Security Help | Web Security ソリューション | バージョン 7.8.x

組織が Novell eDirectory を使用している場合は、Directory Agent がディレクトリを検索し、ハイブリッド サービス用にユーザーおよびグループ情報をパッケージする方法を絞りこむには、**[Settings] > [Hybrid Configuration] > [Shared User Data]** を順に選択します。

1. ディレクトリからユーザーおよびグループ データを収集する時使用する **[Root Context（root コンテクスト）]** を入力するには、[Root Context for Hybrid Filtering Users（ハイブリッド フィルタリング ユーザーの root コンテクスト）] の下の **[Add]** をクリックします。コンテクストを絞り込むと、速度と効率が高まります。*ディレクトリ コンテクストの追加および編集、286 ページ*を参照してください。

   ハイブリッド サービスによって管理されるユーザーだけを含むコンテクストを入力します。

2. [Synchronize User Data] の下の Sync Service コンピュータの **[Name or IP address（名前または IP アドレス）]** および Sync Service 通信に使用する **[Port（ポート）]**（デフォルトでは 55832）を確認します。

   これらのフィールドは自動的に入力されますが、必要に応じて手動で更新することができます。

3. **[Test Connection（テスト接続）]** をクリックして、Directory Agent がデータを Sync Service に送信できることを確認します。テストは 1 分以上かかることがあります。
   - 接続が確立すると、成功したことを知らせるメッセージが表示されます。

- 接続ができなかった場合は、Sync Service コンピュータの IPv4 アドレスまたはホスト名および通信ポートを確認してください。また、Sync Service コンピュータがオンにされていること、Sync Service が実行中であること、ネットワーク ファイアウォールが Sync Service ポートでの接続を許可していることも確認してください。

ディレクトリ検索結果から重複や他の不必要なエントリを除去するためにパターンまたは検索フィルタを指定することによって、ハイブリッド サービスに送信するデータをさらに絞り込むことができます。詳細は、*検索結果の最適化*、289 ページを参照してください。

ディレクトリ コンテクストの追加および編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Directory Agent がディレクトリを検索し、ハイブリッド サービス用にユーザーおよびグループ情報をパッケージする方法を絞りこむには、**[Settings] > [Hybrid Configuration] > [Shared User Data] > [Add Context（コンテクストを追加）]** ページを順に選択します。

警告

ハイブリッド サービスがサポートできるグループの数に制限があります。制限は多くの要因の影響を受けますが、制限を超えた場合、ユーザー要求は適切にフィルタリングされません（サービス を開始できません）。

組織のディレクトリ フォレストが大きく、多数のグループが含まれる場合、Directory Agent がハイブリッド サービスに要求が送信されたユーザーをフィルタリングするために必要な情報だけをアップロードするように設定してください。アップロードするグループだけを選択するか、または絞り込んだ root コンテクストを設定することができます。

ディレクトリ内の複数のコンテクストを選択できます。ハイブリッド サービスによって管理されるユーザーだけを含むコンテクストを含めることを推奨します。たとえば、複数のハイブリッド ユーザーが複数の OU 内にある場合があります。代わりに、いくつかのグループ内のすべてのユーザーを同期化させる場合、各グループについて 1 つのコンテクスト、つまり完全修飾グループ名を選択できます。

デフォルトでは、Directory Agent は、**[Settings] > [General] > [Directory Services]** ページで*拡張ディレクトリ設定*に基づき指定されているユーザーおよびグループ フィルタを使用します。必要な場合は、各ハイブリッド サービス コンテクストについてこれらのフィルターをカスタマイズできます（例、ハイブリッドサービスによって管理されるグループのメンバーであるユーザーだけを含むようにする）。

また、Directory Agent の検索から特定のコンテクストを除外するように選択することもできます。これは、不必要なコンテクストやハイブリッド サービスに問題を発生させる可能性があるコンテクスト（たとえば、1 つのレコードの中に複数の電子メール アドレスがある管理者グループ）がある場合に利用できます。コンテクストが内包されたディレクトリ コンテクストの中にある場合、除外コンテクストとして 1 つのコンテクストだけを設定できます。

1. ディレクトリ エントリツリーを展開して、ディレクトリからユーザーおよびグループデータを収集するときに使用するコンテクストを見つけます。コンテクストを絞り込むと、速度と効率が高まります。

   必要な場合、検索フィールドを使用して、コンテクスト名を見つけます。複数の OU、グループ、ユーザー、またはすべてのディレクトリ エントリを検索できます。検索結果に複数のコンテクストが表示された場合は、1 つのコンテクストを選択し、**[Show in Tree（ツリーに表示）]** をクリックして、ディレクトリ エントリ ツリー内でそのコンテクストの場所を確認します。
2. そのコンテクストにマークを付け、次に **[Specify Include Context（インクルード コンテキストを指定）]** をクリックします。
3. 表示されるポップアップ ウィンドウに、Directory Agent がユーザーおよびグループを検索するのが roo t コンテストよりどれぐらい下位にあるかを指定します。
   - 検索を root コンテクストのみに限定するには、**[Context Only（コンテクストのみ）]** を選択します。
   - 検索を root コンテクストと 1 レベル下のコンテクストのみに限定するには、**[One Level（1 レベル）]** を選択します。
   - 検索を root コンテクストと下位のすべての レベルのコンテクストに拡大するには、**[All Levels（すべてのレベル）]** を選択します。
4. **[Specify Include Context（インクルード コンテキストを指定）]** の対象にするグループまたは OU を選択し、次にグループ検索のために [One Level] または [All Levels] を選択した場合、**[Include all users in selected groups, regardless of context（選択したグループのすべてのユーザーをコンテクストに関わりなく含める）]** オプションが有効になります。グループの中の一部のユーザーが異なるコンテクストに属している場合でも、グループ内のすべてのユーザーがディレクトリ検索で検出されるようにする場合、このボックスにチェックを付けます。

5. Directory Agent がこのコンテクストに対して使用する検索フィルタを微調整するには、**[Customize Search Filters（検索フィルタをカスタマイズ）]** をクリックします。
6. **[Customize search filters（検索フィルタをカスタマイズ）]** をオンにし、必要に応じてユーザーおよびグループ検索フィルターを編集します。
7. **[OK]** をクリックしてディレクトリ コンテクストを保存します。
8. コンテクストをインクルードするように指定した場合、デフォルトではツリー内のそのコンテクストより下位のすべてのコンテクストもインクルードされます。内包されたコンテクスト内部のコンテクストを除外するには、ハイブリッド サービスに送信してはならないコンテキストをマーク付けし、次に **[Specify Exclude Context（除外コンテキストを指定）]** をクリックします。必要な場合、複数のコンテクストを選択できます。
9. 表示されるポップアップ ウィンドウで、**[Set as exclude context（除外コンテクストとして設定）]** が選択されていることを確認してください。既存の除外されたコンテクストを選択し、それを編集するために **[Specify Exclude Context（除外コンテクストを指定）]** をクリックした場合だけ、**[Remove exclude context（除外コンテクストを削除）]** オプションを利用できます。
10. Directory Agent がユーザーおよびグループを検索するのが除外されたコンテクストよりどれぐらい下位にあるかを指定します。
    - 検索を指定したコンテクストのみに限定するには、**[Context Only]** を選択します。
    - 検索を指定したコンテクストと 1 レベル下のコンテクストのみに限定するには、**[One Level]** を選択します。
    - 検索を指定したコンテクストと下位のすべての レベルのコンテクストに拡大するには、**[All Levels]** を選択します。

    除外されたコンテクストのユーザーおよびグループのレベルを、その root コンテクストに対して指定されているレベル以上に設定することはできません。たとえば、ユーザーまたはグループの root コンテクストのディレクトリ 検索レベルが [Context Only] に設定されている場合、除外されたコンテクストの対応するユーザーまたはグループの検索レベルも [Context Only] に設定され、それを変更することはできません。

    ユーザーとグループの両方に対して [All Levels] を選択した場合、選択したコンテクストより下位のすべてのコンテクストが除外され、ディレクトリ エントリ ツリーのさらに下位のレベルを参照することはできません。
11. バージョン7.8.2以降、グループだけが**除外**として指定され、**1つ**または**すべての**レベルが除外対象として選択されている場合、下記のいずれかを決定するコンテクスト**オプションに関わりなく**、[Exclude all users in selected groups（選択したグループのすべてのユーザーを除外する）] を使用します。

- （チェック ボックスがマークされている場合）除外コンテクストに含まれるユーザーは、他の（含める）コンテクストでも定義されているか否かに関わりなく、常に除外される。
- （チェック ボックスがクリアされている場合）除外コンテクストに含まれるユーザーは、他の（含める）コンテクストでも定義されている場合には除外されない。

12. **[OK]** をクリックして排除したコンテクストを保存します。

手順を完了したとき、**[OK]** をクリックして [Add Context] ページを閉じ、[Root Context for Hybrid Filtering Users（ハイブリッド フィルタリング ユーザーの root コンテクスト）] テーブルを更新します。変更をキャッシュするために、[Shared User Data] ページでも **[OK]** をクリックする必要があります。

検索結果の最適化

Web Security Help | Web Security ソリューション | バージョン 7.8.x

検索結果の最適化では、ディレクトリ検索結果から重複や他の不必要なエントリを除去するためにパターンまたは検索フィルタを指定することによって、ハイブリッド サービスに送信するデータをさらに絞り込みます。また、それによって、Directory Agent によって収集されたディレクトリ エントリがハイブリッド サービスに送信される前に、その **mail** 属性を変更することもできます。

たとえば、ディレクトリ サービスに含まれる**メール**属性に部分的または内部メール アドレス参照がある場合は、検索フィルタを使用して、その部分的情報または内部情報をハイブリッド サービスによって使用できる外部情報に置き換えることができます。これは、オフ サイトからハイブリッド サービスに接続できるように、ハイブリッド サービスがユーザーのパスワードを自動的に作成するように設定しているユーザーには便利です（*オフサイト ユーザーに対するハイブリッド フィルタリングの設定、309 ページ*を参照）。

Web Security manager で作成するすべての検索フィルターが Directory Agent によって収集されたディレクトリ データに適用してから、それらのデータがハイブリッド サービスに送信されます。

現在の検索フィルターを確認するか、またはワイルド カードや正規表現を使って新しい検索フィルタを作成するには、**[Optimize Search Results（検索結果を最適化）]** をクリックします。2 種類の検索フィルタ（ユーザー エントリーのフィルタとグループ エントリのフィルタ）があります。

- 新しい検索フィルタを作成するには、適当なテーブルの下の **[Add]** をクリックします。
- 既存の検索フィルタを編集するには、関連する **[Find String（検索文字列）]** をクリックします。

ポップアップ ダイアログが編集または入力するように要求します。

- **Find string**：Directory Agent によって収集された元のディレクトリ データに含まれている検索対象のテキスト。
- **Replace string（置換文字列）**：ハイブリッド サービスに送信するデータ内の元のテキストと置き換える新しいテキスト。

完了したとき、**[OK]** をクリックしてダイアログボックスを閉じ、[Filter User Results（ユーザーの結果のフィルタリング）] または [Filter Group Results（グループの結果のフィルタリング）] テーブルを更新します。変更をキャッシュするために、[Shared User Data] ページでも **[OK]** をクリックする必要があります。

この時点で、Directory Agent は、作成した検索フィルタを**メール**属性にのみ適用します。

ハイブリッド サービスとの通信のスケジュール設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Directory Agent によって収集されたディレクトリ データがハイブリッド サービスに送信される頻度、およびレポーティング データが取得される頻度を指定するには、**[Settings] > [Hybrid Configuration] > [Scheduling（スケジュール設定）]** を順に選択します。

> **注意**
> ポリシー データは、Web Security manager で **[Save and Deploy]** をクリックすると常に収集され、デフォルトでは 15 分ごとにハイブリッド サービスに送信されます。ポリシー データに重要な更新を行い、すぐにユーザーおよびグループ情報を送信する場合は、[Send Policy Data Now（今すぐポリシー データを送信）] の下の **[Send]** をクリックします。

ディレクトリ情報をハイブリッド サービスに送信する頻度を設定するには、下記の手順を実行します。

1. **[Send User Data（ユーザー データを送信）]** の下で、ユーザーおよびグループ情報をハイブリッド サービスに送信する 1 つ以上の曜日を選択します。ディレクトリ情報を使用してユーザーを特定する場合は、Directory Agent データの送信を少なくとも週 1 回行う必要があります。

2. Sync Service がハイブリッド サービスにディレクトリ データを送信する時間を指定するには、開始時刻と終了時刻を入力します。通常、ディレクトリ データは、ネットワークでトラフィック量の少ない時間に送信されます。
3. ポリシー データに重要な更新を行い、すぐにユーザーおよびグループ情報を送信する場合は、[Send Update Now（今すぐ更新を送信）] の下の **[Send]** をクリックします。

   Web Security manager が Sync Service から確認を受け取った場合は、正常完了メッセージが表示されます。このメッセージは、Sync Service がデータを送信したことを表し、データがハイブリッド サービスによって受信されたことを表しているのではありません。

ハイブリッド サービスがレポーティング データを収集するかどうか、また Sync Service がデータを取得する頻度を設定するには、下記の手順を実行します。

> **重要**
>
> Sync Service がハイブリッド レポーティング データを Log Server に渡すために、[Settings] > [General] > [Logging（ログ記録）] ページを順に選択し、ハイブリッド通信ポートを設定する必要があります。詳細については、*要求がログ記録される方法の設定、505 ページ*を参照してください。
>
> 分散ログ記録を使用している場合は、Sync Service を中央 Log Server と通信するように設定しなければなりません。ハイブリッド ログ記録データは、リモート Log Server インスタンスから中央 Log Server に渡すことはできません。

1. [Collect and Retrieve Reporting Data（レポーティング データを収集および取得）] の下の **[Have the hybrid service collect reporting data for the clients it filters（ハイブリッド サービスがフィルタリング対象のクライアントのレポーティング データを収集するように設定する）]** をオンにします。

   このチェック ボックスをオフにした場合は、ハイブリッド ユーザーのログ データは保存されません。これらのユーザのインターネット アクティビティに関する一切の情報がレポートに表示されません。
2. Sync Service がハイブリッド サービスからレポーティング データを要求する 1 つ以上の曜日を選択します。データの取得を、少なくとも週 1 回行う必要があります。
3. Sync Service がハイブリッド サービスからデータを取得する時間を指定するには、開始時刻と終了時刻を入力します。データの取得は、ネットワーク内のトラフィック量が少ない時間に行うことができます。

4. 指定した開始時刻から終了時刻の範囲内で Sync Service がハイブリッド サービスからレポーティングデータを要求する頻度を選択します。

   Sync Service は、15 分ごとを超える頻度ではレポーティング データをダウンロードできません。つまり、ハイブリッド サービスがインターネット要求を行う時間とそれらの要求がレポートに表示される時間との間に時間遅延があるのです。

Sync Service のトラフィックをプロキシ サーバーまたはファイアウォールを経由してハイブリッド サービスとの間でルーティングする必要がある場合は、下記の手順を実行します。

1. [Route Sync Service Traffic（Sync Service のトラフィックをルーティング）] の下の **[Route Sync Service traffic through a proxy server or firewall（プロキシ サーバまたはファイアウォールを経由して Sync Service のトラフィックをルーティング）]** をオンにします。
2. プロキシ サーバーの IP アドレスまたはホスト名を入力し、使用されるポートを指定します。
3. 指定したサーバーが認証を必要とする場合、Sync Service のユーザー名およびパスワードを入力してそのサーバーにアクセスします。

完了したら、**[OK]** をクリックして変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

カスタム認証の設定を指定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

カスタム ルールを追加および編集して、特定のアプリケーションまたはサイトのデフォルトの認証動作を変更するには、**[Settings] > [Hybrid Configuration] > [Custom Authentication（カスタム認証）]** ページを順に選択します。

場合によっては、一部のインターネット アプリケーションおよびウェブサイトは、ハイブリッド サービスでは認証できません。これは、たとえば、インスタント メッセージング プログラム、アンチウィルスの更新、またはソフトウェア更新サービスで起こることがあります。

認証チャレンジを適切に処理しないアプリケーションが認証をバイパスできるようにするために、ユーザー エージェント、ドメイン、または URL、もしくはこれらの組み合わせを指定することができます。

ユーザー エージェントは、ブラウザまたはインターネット アプリケーションから閲覧しているサイトをホストしているサーバーに送信する文字列です。この文字列は、使用するブラウザまたはアプリケーション、そのバージョン番号、およびシステムに関する詳細情報（例、オペレーティング システムおよびバージョン）を指定します。宛先サーバーは、この情報を使用して、特定のブラウザまたはアプリケーションに適したコンテンツを提供します。

たとえば、これが Firefox のユーザー エージェントである場合、下記の文字列です。

```
Mozilla/5.0(Windows; U; Windows NT 5.1; en-US; rv:1.9.2.6)
```

この例では、Windows NT 5.1 は、オペレーティング システムが Windows XP であり、使用する言語が米国英語であることを示しています。

ブラウザのユーザー エージェント文字列を取得するには、ブラウザのアドレスバーに下記のように入力します。

```
javascript:alert(navigator.userAgent)
```

ハイブリッド サービスを通じて認証要求を行ったユーザー エージェントを User Agents by Volume（ボリューム別ユーザ エージェント）レポートで見ることができます。このレポートは、[Custom Authentication] ページ、および **[Main（メイン）] > [Status] > [Hybrid Service]** ページから入手できます。このレポート中のユーザー エージェントの認証要求数が多い場合は、認証上の問題が発生している可能性があります。エージェントの新しいカスタム認証ルールを追加するには、レポートでそのユーザー エージェントを選択し、**[Create Rule（ルールを作成）]** をクリックします。*ユーザー エージェント ボリューム レポートを表示、301 ページ*を参照してください。

カスタム認証ルールを指定するには、**[Add]** をクリックし、次に*カスタム認証ルールの追加、293 ページ*を参照してください。

既存のカスタム ルールを編集するには、ルールの **[Name]** をクリックし、次に *カスタム認証ルールの編集、296 ページ*を参照してください。

カスタム認証ルールを削除するには、ルールの名前の横のチェックボックスをオンにし、**[Delete]** をクリックします。

カスタム認証ルールを追加または編集した場合、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

カスタム認証ルールの追加

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ハイブリッド サービスでは認証できない 1 つ以上のユーザー エージェント、ドメイン、または URL を指定するには、**[Custom Authentication] > [Add Custom Authentication Rule（カスタム認証ルールを追加）]** ページを順に選択します。

1. ルールの **[Name]** を入力します。名前は長さが 1 ～ 50 字で、下記の文字を含めることはできません：

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   名前にはスペース、ダッシュ、アポストロフィーを含めることができます。

2. ルールの **[User agents]**（もしあれば）を指定します。
   - すべてのユーザー エージェント文字列を照合するには、**[All user agents（すべてのユーザー エージェント）]** を選択します。これは組織内のすべてのオペレーティング システム上のすべてのブラウザに適合するカスタム ルールを設定するために使用します。
   - アプリケーションがユーザー エージェント文字列をインターネットに送信しない場合は、**[No user agent header sent（ユーザー エージェント ヘッダーを送信しない）]** を選択します。

     このオプションは、ユーザー エージェントを送信しないすべてのアプリケーションを照合します。この場合、**[Destinations（宛先）]** フィールドで 1 つ以上の URL またはドメインを入力することによってルールを絞り込みます。
   - カスタム認証を 1 つ以上のユーザー エージェントに適用するには、**[Custom user agents]** を選択します。各ユーザー エージェントを 1 行に 1 つずつ入力します。1 つの行を複数のユーザー エージェント文字列と照合するには、アスタリスク ワイルドカードを使用します（例、Mozilla/5.0*）。

   > **注意**
   > User Agents by Volume レポートから直接に新しいレポートを作成している場合は、レポートで選択したユーザー エージェントはすでにこのフィールドに入れられています。

3. **[Destinations]** フィールドでルールとして URL またはドメイン（もしあれば）を下記のいずれかの選択で指定します。
   - すべての RUL およびドメインを照合するには、**[All destinations]** を選択します。複数のサイトをアクセスする特定のユーザー エージェントに適用するカスタム ルールを設定する場合にこれを行います。
   - カスタム認証を 1 つ以上の特定のドメインまたは URL に用するには、**[Custom destinations]** を選択します。URL またはドメインを 1 行に 1 件ずつ入力します。

     URL は、先頭にプロトコル部分（http://）、および末尾にスラッシュ（/）を含む必要があります（例、http://www.google.com/）。これらの要素がない場合は、文字列はドメインとして処理されます。ドメインは、末尾にスラッシュを含めることができません（例、mydomain.com）。

     1 つの行を複数の宛先と照合するには、アスタリスク ワールドカードを使用します。例えば、*.mydomain.com と入力すると、[mydomain.com.] で終わるすべてのドメインを照合します。

4. カスタム ルールとして **[Authentication method（認証方法）]** で下記のいずれかを選択します。
   - **[Default]**：デフォルト認証方法を使用します。
   - **[NTLM]**：指定したユーザー エージェントおよび宛先に対して NTLM 識別を使用します。アプリケーションに NTLM 認証機能がない場合、基本認証が使用されます。

     注意
     このオプションを使用するためには、アカウントの NTLM 識別が有効化されている必要があります。

   - **[Secure form authentication（高セキュリティの認証方式）]**：エンド ユーザーにセキュアなログオン フォームを表示するために、セキュリティ フォーム認証を使用します。詳細については、*ハイブリッド ユーザーの識別、391 ページ*を参照してください。
   - **[Basic authentication（基本認証）]**：多数の Web ブラウザによってサポートされている基本認証メカニズムを使用します。ようこそページは表示されません。基本認証の詳細については、*ハイブリッド ユーザーの識別、391 ページ*を参照してください。
   - **[Welcome page（ようこそページ）]**：ユーザーが基本認証を使用する前に、ユーザーにようこそページが表示されます。
   - **[None（なし）]**：ハイブリッド サービスでのすべての認証および識別方法をバイパスします。認証機能がないインターネット アプリケーションに対してこのオプションを選択します。
5. オプションで、指定したユーザー エージェントおよび宛先に対するすべてのフィルタリグをバイパスするには、**[Bypass content scanning]** を選択します。

   重要
   何らか理由でハイブリッド サービスでは機能せず、暗示的に信頼するアプリケーションおよびサイトに対して**のみ**このオプションを選択します。このオプションを選択すると、ウィルスや他のマルウェアがネットワーク内に侵入することがあります。

6. **[OK]** をクリックして [Custom Authentication] に戻り、再度 **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

カスタム認証ルールの編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ハイブリッド サービスでは認証できない 1 つ以上のユーザー エージェント、ドメイン、または URL を編集するには、**[Custom Authentication] > [Edit Custom Authentication Rule（カスタム認証ルールを編集）]** ページを順に選択します。

1. ルールの **[Name]** に編集を行う場合は、名前は長さが 1 ～ 50 字で、下記の文字を含めないようにします。

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   名前にはスペース、ダッシュ、アポストロフィーを含めることができます。

2. ルールの **[User agents]**（もしあれば）を定義または更新します。
   - すべてのユーザー エージェント文字列を照合するには、**[All user agents（すべてのユーザー エージェント）]** を選択します。これは組織内のすべてのオペレーティング システム上のすべてのブラウザに適合するカスタム ルールを設定するために使用します。
   - アプリケーションがユーザー エージェント文字列をインターネットに送信しない場合は、**[No user agent header sent（ユーザー エージェント ヘッダーを送信しない）]** を選択します。

     このオプションは、ユーザー エージェントを送信しないすべてのアプリケーションを照合します。この場合、**[Destinations）]** フィールドで 1 つ以上の URL またはドメインを入力することによってルールを絞り込むことを推奨します。
   - カスタム認証を 1 つ以上のユーザー エージェントに適用するには、**[Custom user agents]** を選択します。各ユーザー エージェントを 1 行に 1 つずつ入力します。1 つの行を複数のユーザー エージェント文字列と照合するには、アスタリスク ワイルドカードを使用します（例、Mozilla/5.0*）。
3. **[Destinations]** フィールドでルールとして URL またはドメイン（もしあれば）を下記のいずれかの選択で指定または更新します。
   - すべての RUL およびドメインを照合するには、**[All destinations]** を選択します。複数のサイトをアクセスする特定のユーザー エージェントに適用するカスタム ルールを設定する場合にこれを行います。
   - カスタム認証を 1 つ以上の特定のドメインまたは URL に用するには、**[Custom destinations]** を選択します。URL またはドメインを 1 行に 1 件ずつ入力します。

     URL は、先頭にプロトコル部分（http://）、および末尾にスラッシュ（/）を含む必要があります（例、http://www.google.com/）。これらの要素がない場合は、文字列はドメインとして処理されます。ドメインは、末尾にスラッシュを含めることができません（例、mydomain.com）。

1 つの行を複数の宛先と照合するには、アスタリスク ワールドカードを使用します。例えば、*.mydomain.com と入力すると、[mydomain.com.] で終わるすべてのドメインを照合します。

4. カスタム ルールとして **[Authentication method]** で下記のいずれかを確認または更新します。
   - **[Default]**：デフォルト認証方法を使用します。
   - **[NTLM]**：指定したユーザー エージェントおよび宛先に対して NTLM 識別を使用します。アプリケーションに NTLM 認証機能がない場合、基本認証が使用されます。

     注意
     このオプションを使用するためには、アカウントの NTLM 識別が有効化されている必要があります。

   - **[Form Authentication]**：エンド ユーザーにセキュアなログオン フォームを表示するために、セキュリティ フォーム認証を使用します。詳細については、*ハイブリッド ユーザーの識別*、391 ページを参照してください。
   - **[Basic Authentication]**：多数の Web ブラウザによってサポートされている基本認証メカニズムを使用します。ようこそページは表示されません。基本認証の詳細については、*ハイブリッド ユーザーの識別*、391 ページを参照してください。
   - **[Welcome page]**：ユーザーが基本認証を使用する前に、ユーザーにようこそページが表示されます。
   - **[None]**：ハイブリッド サービスでのすべての認証および識別方法をバイパスします。認証機能がないインターネット アプリケーションに対してこのオプションを選択します。
5. オプションで、指定したユーザー エージェントおよび宛先に対するすべてのフィルタリグをバイパスするには、**[Bypass content scanning]** を選択します。

   重要
   何らか理由でハイブリッド サービスでは機能せず、暗示的に信頼するアプリケーションおよびサイトに対して**のみ**このオプションを選択します。このオプションを選択すると、ウィルスや他のマルウェアがネットワーク内に侵入することがあります。

6. **[OK]** をクリックして [Custom Authentication] に戻り、再度 **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

モニタのハイブリッド サービスとの通信

Web Security manager で **[Status] > [Dashboard] > [Hybrid Service]** ページを順に選択することによって、ハイブリッドサービスのステータスを確認できます。このページは、ハイブリッド サービスとの間でデータが最近送 / 受信された時に表示されます。データの送 / 受信を失敗した場合は、エラーが発生した時刻、および関わっていたコンポーネントを見つけます。

このページは、Sync Service が下記のことを行った日付および時刻をリストします。

- 何らかの理由でハイブリッド サービスに接続したか、または接続を試みた
- ハイブリッド サービスにディレクトリ情報を送信したか、または送信を試みた
- ハイブリッド サービスからログ（レポーティング）データを取得したか、または取得を試みた
- Log Server にログ データを送信したか、または送信を試みた
- ハイブリッド サービスにアカウント情報を送信したか、または送信を試みた
- ハイブリッド サービスにアカウント情報を送信したか、または送信を試みた

Websense Web Security Gateway Anywhere のオンプレマイズの部分とハイブリッドの部分との間の接続をまだ設定していない場合、[No communication has occurred（通信が行われませんでした）] というメッセージが表示されます。

[Last Directory Agent Sync Results（最後の Directory Agent Sync の結果）] の下にページは下記の事柄をリストします。

- Directory Agent がハイブリッド サービスに最後にデータを送信した日付と時刻
- Directory Agent によって処理されたユーザーとグループの合計数
- ハイブリッド サービスで更新されたユーザーとグループの合計数
- 無効な値を含んでいたために除外されたグループの数
- 無効な電子メール アドレスを含んでいるために除外されたユーザーの数
- ハイブリッド サービスと同期化した新しいユーザーおよびグループの数
- ハイブリッド サービスから削除された陳腐化したユーザーおよびグループの数

このページでは、ハイブリッド サービスからの認証方式およびユーザー エージェント レポートにアクセスでき（*ハイブリッド サービス認証レポートを表示、299 ページ*および*ユーザー エージェント ボリューム レポートを表示、301 ページ*を参照）、また、使用している PAC ファイルのタイプが表示されます。

- ハイブリッド サービス からのデフォルトの PAC ファイル
- Websense **pac** ディレクトリからアップロードしカスタマイズした PAC ファイル（*PAC ファイルとは、278 ページ*を参照）
- デフォルトの PAC ファイルとアップロードされ、カスタマイズされたフラグメント

カスタム ファイルまたはフラグメントを使用している場合は、ページはファイルまたはフラグメントが使用中であった時間を示します。

PAC ファイルの **[Secondary date stamp（2 番目の日付スタンプ）]** が表示された場合、Sync Service は、**pac** ディレクトリからカスタム PAC ファイルとカスタム フラグメントの両方をアップロードしていたことを示します。カスタム PAC ファイルについては、カスタム ファイルまたはカスタム フラグメントのいずれか（両方ではなく）をセットアップすることを推奨します。これを修正するには、**pac** ディレクトリ（デフォルトでは、Windows の場合は \Program Files *または* Program Files（x86）\Websense\Web Security\bin\data\pac、Linux の場合は /opt/websense/bin/data/pac）に移動し、websense.pac または customfinal.pac のどちらかを削除します。

カスタマイズしたブロック ページ ロゴを使用している場合は、このページは、ロゴ ファイルがハイブリッド サービスにアップロードされた日付と時刻を表示します。

ハイブリッド サービス認証レポートを表示

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ハイブリッド サービスからレポーティング データをダウンロードし、ハイブリッド ユーザーがサービスで識別または認証される方法の詳細を確認するには、**[Main] > [Status] > [Hybrid Service]** ページを順に選択し、[Authentication Report（認証レポート）] の下の **[View Report（レポートを表示）]** を選択します。

レポート出力は、円グラフとテーブルで構成されており、最後の 7 日間に当る利用可能なそれぞれの認証方式を使用するクライアントの数を示します。[Settings] > [Hybrid Configuration] > [Hybrid User Identification] ページで、クライアントのための **[Web Endpoint]**, **[NTLM identification]**, **[Form authentication]** および **[Manual authentication]** がすべて設定されます（*ハイブリッド ユーザーの識別、391 ページ*を参照）。

下記のいすれかをダウンストリーム チェーン型オンプロキシ サーバーとして配備している場合は、**[X-Authenticated-User（X- 認証された - ユーザー）]** 認証が利用できます。

- Microsoft® Internet Security and Acceleration（ISA）ServerまたはForefront™ Threat Management Gateway（TMG）server
- BlueCoat Proxy SG

ダウンストリーム プロキシ サーバーは、ユーザー認証を実行し、X-Authenticated-User ヘッダーを使用して要求をハイブリッド プロキシに転送します。

その方式で最近認証されたユーザーのリストを確認するには、テーブル内の認証方式をクリックします。配備していない、または現在使用中でない認証方式をクリックできません。

各認証方式レポートには最大 1000 件のユーザーを含めることができます。ユーザーは、ユーザー名、電子メールアドレス、および最後のログオン時刻別にリストされます。以前のまたは以後のページを表示するには、レポートの下部の矢印ボタンをクリックします。

コンテンツ ペインで表示されるレポートは印刷できず、またファイルとして保存することもできません。レポートを印刷するか、またはファイルに保存するには、**[Export to PDF]** をクリックし、また適当な出力形式でレポートを表示するには **[Export to XLS]** をクリックします。

重要

認証レポートを PDF フォーマットで表示するには、TRITON コンソールをアクセスしているコンピュータに Adobe Reader v7.0 以上がインストールされていなければなりません。

認証レポートを XLS フォーマットで表示するには、TRITON コンソール をアクセスしているコンピュータに Microsoft Excel 2003 以上がインストールされていなければなりません。

各レポートは、レポートが最後に更新された日付と時刻を含みます。更新は自動的にはおこなわれません。ハイブリッド サービスから最新のレポートデータをダウンロードするとき、**[Update]** をクリックします。

ユーザー エージェント ボリューム レポートを表示

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ハイブリッド サービスを通じて認証要求を行ったユーザー エージェントを表示するには、**[Main] > [Status] > [Hybrid Service]** ページを順に選択し、[User Agent Volume Report（ユーザー エージェント ボリューム レポート）] の下の **[View Report（レポートを表示）]** を選択します。

レポート出力は、各ユーザー エージェントが行った認証要求の数と要求の総数を示すテーブルで構成されいます。ユーザー エージェントがそれに関連すうるカスタム認証ルールをすでにもっている場合、マウスを **[Rule（ルール）]** 列の上で動かし、カスタム ルールの詳細を確認できます。

下記のようにレポート結果をフィルタリングできます。

- 検索条件を入力し、**[Search（検索）]** をクリックします。
- ドロップダウンリストから **[Time range（時間の範囲）]** を選択します。[Custom（カスタム）] 日付範囲を選択した場合は、1 日から 14 日の間の期間を選択します。
- それらの関連するカスタム認証ルールだけをもつユーザー エージェントのみを表示するには、**[View only user agents with rules（ルールをもつユーザー エージェントのみ表示）]** をオンにします。

1 ページを超える結果がある場合は、レポートの下部の矢印ボタンをクリックして、前のページまたは次のページを表示します。

このレポート中のユーザー エージェントの認証要求数が多い場合は、認証上の問題が発生している可能性があります。レポート内の 1 つ以上のユーザー エージェントに対して新しいカスタム認証ルールを追加するには、各エージェントのチェック ボックスをオンにし、**[Create Rule（ルールを作成）]** をクリックします。選択したユーザー エージェントは、[Add Custom Authentication Rule（カスタム認証ルールを追加）] ページの **[Custom user agents（カスタム ユーザー エージェント）]** フィールドに自動的に入れられます。*カスタム認証ルールの追加、293 ページ*を参照してください。

コンテンツ ペインで表示されるレポートは印刷できず、またファイルとして保存することもできません。レポートを印刷するか、またはファイルに保存するには、**[Export to PDF]** をクリックし、また適当な出力形式でレポートを表示するには **[Export to XLS]** をクリックします。

重要

認証レポートを PDF フォーマットで表示するには、TRITON コンソールをアクセスしているコンピュータに Adobe Reader v7.0 以上がインストールされていなければなりません。

認証レポートを XLS フォーマットで表示するには、TRITON コンソール をアクセスしているコンピュータに Microsoft Excel 2003 以上がインストールされていなければなりません。

各レポートは、レポートが最後に更新された日付と時刻を含みます。更新は自動的にはおこなわれません。ハイブリッド サービスから最新のレポートデータをダウンロードするとき、**[Update]** をクリックします。

11 オフサイト ユーザーの管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連トピック：

- *リモート フィルタリング ソフトウェアの使用*、304 ページ
- *オフサイト ユーザーのハイブリッド管理*、308 ページ

組織内のネットワークに含まれているユーザーのポリシーの実施に加えて、Websense Web Security ソリューションは、ユーザーがネットワークの外側にいる場合にインターネットの要求に応答するオプションを提供します。

- ネットワークの外側のユーザーのインターネット アクティビティをモニタするには、リモート フィルタリング ソフトウェアをインストールしてください。*リモート フィルタリング ソフトウェアの使用*、304 ページを参照してください。

  リモート フィルタリング ソフトウェアは、Websense Web Security Gateway Anywhere のサブスクリプションと共に含まれており、Websense Web Filter、Websense Web Security、Websense Web Security Gateway のオプションとして利用できます。
- ネットワークの外側のユーザーのインターネット アクティビティをモニタするには、それらのユーザーがネットワーク内にいるときにそれらの要求が処理される方法に関係なく、ハイブリッド サービスを使用します。*オフサイト ユーザーのハイブリッド管理*、308 ページを参照してください。

  ハイブリッド サービスは、Websense Web Security Gateway Anywhere でのみ利用できます。

これらの方法は、例えば、在宅勤務するユーザー、会社のラップトップを使って出張するユーザー、またはキャンパスの内外で機関のラップトップを使用する学生に対してポリシーの実施を提供するために使用します。

重要

Websense Web Security Gateway Anywhere では、一部のオフサイト ユーザーに対してリモート フィルタリング ソフトウェアを使用し、他のオフサイト ユーザーに対してハイブリッド サービスを使用できます。しかし、ハイブリッド サービスは、Remote Filtering Client もインストールされているコンピュータのインターネット アクティビティをモニタするために使用できません。

リモート フィルタリング ソフトウェアの使用

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Remote Filtering の設定の構成、306 ページ*

デフォルトでは リモート フィルタリング ソフトウェア コンポーネントは、HTTP、SSL、および FTP トラフィックをモニタし、ユーザーベースのポリシーまたはデフォルト ポリシーを適用します。リモート フィルタリング ソフトウェアは、ポリシーを IP アドレス（コンピュータ またはネットワーク範囲）に適用しません。

- 帯域幅制限は、リモート フィルタリング クライアントには適用されず、リモート フィルタリング トラフィックによって生成された帯域幅は、帯域幅の測定およびレポートには含まれません。
- リモート フィルタリング ソフトウェアは、FTP および SSL（HTTPS）要求をブロックまたは許可するだけです。割り当て時間アクションまたは確認アクションが割り当てられたカテゴリの FTP サイトまたは HTTPS サイトは、ユーザーがネットワークの外側にいる場合はブロックされます。
- リモート フィルタリング ソフトウェアは、HTTP トラフィックを常にモニタしますが、FTP トラフィック、HTTPS トラフィック、またはその両方を無視するように設定できます。*FTP または HTTPS トラフィックを無視するようにリモート フィルタリングを設定、307 ページ*を参照してください。

リモート フィルタリング ソフトウェアは、下記のコンポーネントを含みます。

- **Remote Filtering Server** は、ネットワークの一番外側のファイアウォールの内側にインストールされます。それによってネットワークの外側のフィルタリング対象のコンピュータがそれと通信できます。
- **Remote Filtering Client** は、ネットワークの外側で使用される Microsoft Windows コンピュータにインストールされます。

> **注意**
> Deployment and Installation Center の推奨事項に従って、これらのコンポーネントを慎重に配備してください。これらのコンポーネントのインストールの手順については、テクニカル ペーパー Remote Filtering Software を参照してください。

Remote Filtering Client と Remote Filtering Server の間のすべての通信は、認証され、暗号化されます。

デフォルトでは、HTTP、SSL または FTP 要求が Remote Filtering Client をインストールしているコンピュータから行われた場合、下記の手順を実行します。

1. クライアントは、最初に DMZ 内の Remote Filtering Server に**ハートビート**を送信することによって Remote Filtering Server がネットワークの内側にあるかどうかを判断します。
2. コンピュータがネットワークの**内側**にある場合は、Remote Filtering Client は何も処置しません。要求は、Network Agent または統合製品に渡され、他のネットワーク内のインターネット アクティビティのようにフィルタリングされます。
3. コンピュータがネットワークの**外側**にある場合、Remote Filtering Client は、設定されたポート（デフォルトでは 80）上で Remote Filtering Server と通信します。
4. 続いて、Remote Filtering Server は、（ネットワークの内側にインストールされている）Filtering Service に連絡をとり、要求に対してどんなアクションを適用するかを問い合わせます。
5. Filtering Service は、要求を評価し、応答を Remote Filtering Server に送信します。
6. 最後に、Remote Filtering Server は、Remote Filtering Client に応答し、サイトを許可するか、または該当するブロック メッセージを送信します。

リモート フィルタリング ソフトウェアのプランニング、配備、設定の詳細については、support.websense.com から入手できるテクニカル ペーパー Remote Filtering Software を参照してください。

Remote Filtering の設定の構成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *FTP または HTTPS トラフィックを無視するようにリモート フィルタリングを設定、307 ページ*
- *Remote Filtering Client のハートビート間隔の設定、307 ページ*

いずれかの Remote Filtering Client インスタンスが Remote Filtering Server と通信できない場合の処置を設定するには、**[Settings] > [General] > [Remote Filtering]** ページを使用します。

- デフォルトでは、Remote Filtering Client は、すべての HTTP、SSL、および FTP 要求を許可しますが、引き続き Remote Filtering Server に通信しようと試みます（フェイル オープン）。通信に成功した場合には、該当するフィルタリング ポリシーが実施されます。
- Remote Filtering Client が Remote Filtering と通信できない場合、ユーザーがインターネットにアクセスできないようにする（フェイル クローズ）には、**[Block all requests...（すべての要求をブロック ...）]** を選択します。

  Remote Filtering Client がフェイル クローズに設定されている場合には、タイムアウト値が適用されます（デフォルトは 15 分）。リモート コンピュータが起動すると、クロックが動作を開始します。Remote Filtering Client はただちに Remote Filtering Server への接続を試み、成功するまで使用可能な Remote Filtering Server に対して順番に試行を続けます。

  ユーザが起動時に Web アクセスを行った場合は、タイムアウト中、Remote Filtering Client が Remote Filtering Server に接続するまでは、すべての要求が許可されます。

  Remote Filtering Client が設定されたタイムアウト時間内に接続できなかった場合は、Remote Filtering Server への接続が確立できるまで、すべてのインターネット アクセスはブロックされます（フェイル クローズ）。

  注意
  何らかの理由で Remote Filtering Server が Filtering Service に接続できなかった場合には、Remote Filtering Client にエラーが返され、すべての要求が許可されます（フェイル オープン）。

  このタイムアウト時間は、インターネット アクセスの料金を支払っているユーザが、移動中にコンピュータを起動し、ロックアウトされることなく接続を設定することを可能にします。15 分のタイムアウト時間が切れる前にユーザが Web アクセスを確立しなかった場合、ユーザはコンピュータを再起動して、タイムアウト間隔を再開する必要があります。

リモート フィルタリングの機能、関連するコンポーネント、およびコンポーネントを配備する方法の詳細については、テクニカル ペーパー Remote Filtering Software を参照してください。

FTP または HTTPS トラフィックを無視するようにリモート フィルタリングを設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

FTP トラフィック、HTTPS トラフィックまたはその両方のトラフィックを無視するようにリモート フィルタリング ソフトウェアを設定できます。HTTP トラフィックは常にモニタされます。

複数の Remote Filtering Server がある場合は、各インスタンスについてこれらの手順を繰り返します。

1. Remote Filtering Server コンピュータ上で Websense **bin** ディレクトリ（デフォルトでは、C:\Program Files\Websense\Web Security\bin or /opt/Websense/bin/）に移動します。
2. テキスト エディタで、**securewispproxy.ini** ファイルを開きます。
3. この Remote Filtering Server インスタンスが FTP トラフィックを無視するように設定するには、ファイルに下記の行を追加します。

   ```
   FilterFTP=0
   ```

   後で FTP 管理を有効化する場合は、パラメータ値を [0] から [1] に変えます。
4. この Remote Filtering Server インスタンスが HTTPS トラフィックを無視するように設定するには、ファイルに下記の行を追加します。

   ```
   FilterHTTPS=0
   ```

   後で HTTPS 管理を有効化する場合は、パラメータ値を [0] から [1] に変えます。
5. ファイルを保存して、閉じます。
6. Remote Filtering Server サービスまたはデーモンを再起動します。

Remote Filtering Client のハートビート間隔の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Remote Filtering Server がネットワークの内側にあるのか、外側にあるのかを判断するために、Remote Filtering Client は、ハートビートを Remote Filtering Server に送信します。ハートビート接続が成功した場合は、Remote Filtering Client は Remote Filtering Server がネットワークの内側にあるこがわかります。デフォルトでは Remote Filtering Client は、15 分ごとにハートビートを送り続け、Remote Filtering Server のステータスが変更されていないことを確認します。

Remote Filtering Server がネットワークの内側にあることを Remote Filtering Client が判断した後のハートビート間隔の送信の頻度を少なくする場合は、ハートビート間隔を大きくすることができます。この場合、Remote Filtering Client は、ネットワーク内で変更を登録した場合だけより頻繁にハートビートを送信します。

ハートビート間隔を変更するには、下記の手順を実行します。

1. Remote Filtering Server コンピュータ上で Websense **bin** ディレクトリ（デフォルトでは、C:\Program Files\Websense\Web Security\bin or /opt/Websense/bin/）に移動します。
2. テキスト エディタで、**securewispproxy.ini** ファイルを開きます。
3. **HeartbeatRetryInterval** パラメータを見つけ、その値を変更します。例：

   ```
   HeartbeatRetryInterval=360
   ```

   この例では、ハートビートは 360 分（6 時間）ごとに送信されます。
   - 値を 0 ～ 1440（24 時間）の任意の数値にできます。
   - デフォルトは 15 分です。
4. ファイルを保存して、閉じます。
5. Remote Filtering Server サービスまたはデーモンを再起動します。

オフサイト ユーザーのハイブリッド管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *オフサイト ユーザーに対するハイブリッド フィルタリングの設定、309 ページ*
- *オフサイトユーザーの自己登録、310 ページ*

Web Security Gateway Anywhere 環境では、ハイブリッド サービスを、ユーザーがネットワーク内のユーザーであるときこれらのユーザーの要求が処理される方法に関係なく、オフサイトのユーザーを管理するように設定できます。

- ユーザーがネットワークに含まれていて、オンプレマイズ コンポーネント（Filtering Service）によって処理される場合、インターネット要求を送信する前に、ネットワーク内のユーザーかオフサイトのユーザーかを指定するためにブラウザ PAC ファイルを設定できます。

  ハイブリッド サービスによって生成された PAC ファイルを使用しているとき、この構成は、Web Security manager で入力した設定に基づき自動的に行われます。

- ネットワークの内側と外側の両方でハイブリッド サービスによって管理されるユーザーの場合、PAC ファイルの変更は必要ありません。オフサイト ユーザーがインターネット要求を行ったとき、適切なユーザーまたはグループベースのポリシーを適用できるようにするために、ハイブリット サービスにログオンするように要求されます。

重要
一部のオフサイト ユーザーに対してリモート フィルタリング ソフトウェアを使用し、他のオフサイト ユーザーに対してハイブリッド サービスを使用できますが、ハイブリッド サービスは、Remote Filtering Client もインストールしているコンピュータのインターネット アクティビティをモニタするために使用できません。

オフサイト ユーザーに対するハイブリッド フィルタリングの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

フィルタ対象の外側のユーザーを管理するようにハイブリッド サービスを設定するには、下記のいずれかの条件に適合する手順を実行します。

- ハイブリッド サービスがユーザーを特定するために、Websense Directory Agent によって収集されたデータを使用する場合は、Directory Agent によって送信されたすべてのユーザー アカウントに対してハイブリッド ログオン パスワードを自動的に作成するように設定する（*ユーザーおよびグループ データをハイブリッド サービスに送信、280 ページ*を参照）か、またはユーザーがフィルタ対象の場所の外側からハイブリッド サービスに最初に接続するときユーザーが自らのパスワードを要求するように設定できます（*オフサイトユーザーの自己登録、310 ページ*を参照）。
- 組織が Directory Agent によって収集されたディレクトリ データを使って、ハイブリッド サービスに接続するユーザーを識別していない場合、ユーザーがそのサービスに**自己登録**できるようにすることができます。*ハイブリッド サービスへのユーザーのアクセスの設定、272 ページ*を参照してください。
- オフサイト ユーザーの識別ポリシーを確定した後、Web Security manager で **[Settings] > [Hybrid Configuration（ハイブリッド設定）] > [User Access（ユーザー アクセス）]** ページを順に選択し、**[Enable off-site users（オフサイト ユーザーを有効化）]** をオンにします。*ハイブリッド サービスへのユーザーのアクセスの設定、272 ページ*を参照してください。

オフサイトユーザーの自己登録

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ディレクトリ サービス データをハイブリッド サービスに送信している場合は（つまり、Directory Agent を有効化していない場合）、ユーザーはオフサイト（フィルタ対象の場所の外側）にいる場合に適切にフィルタリングされるために、自己登録しなければなりません。

ユーザーに対して自己登録を許可するために、Web Security manager の **[Settings] > [Hybrid Configuration] > [User Access]** ページを順に選択して、最初に組織に関連するドメインを特定する必要があります（*ハイブリッド サービスへのユーザーのアクセスの設定、272 ページ*を参照）。

フィルタ対象の外側からハイブリッド サービスに接続しているユーザーは、ユーザー名およびパスワードを入力するか、登録するように要求されます。ハイブリッド サービスに登録するには、下記の手順を実行します。

1. ユーザーは、名前および電子メール アドレスを入力します。
2. 次にハイブリッド サービスは、電子メールを通じてユーザーにパスワードとパスワードの変更に使用できるリンクを送信します。
3. ユーザーはそのリンクをクリックし、パスワードを入力するように要求されます。
4. 登録が完了します。

登録したユーザーがフィルタ対象の場所の外側からハイブリッド サービスに接続した場合、それらのユーザーは、電子メール アドレスとパスワードを入力します。次にハイブリッド サービスは組織のデフォルト ポリシーをそれらのユーザーのインターネット要求に適用します。

12 重要な情報を保護

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Web Security は、企業をウェブベースの脅威、責任問題、および生産性の損失から保護します。しかし、社会保障番号やクレジット カード番号など機密データが Web 上で漏洩するのを防ぐことを希望する場合またはそうすることが必要な場合どうしますか。またはそのようなデータについてリムーバブル メディア デバイス、プリンタ、インスタント メッセージ、コピー/ 張付け動作、または電子メールをモニタしたいと場合どうしますか。

そのようなデータの損失を防ぐために、Websense Web Security Gateway Anywhere を配備します。Web に加えて、他のチャネル上のデータ損失を防ぐために、ご使用のウェブ セキュリティ ソフトウェアへのアドオンとして Websense Data Protect、Data Monitor、Data Discover、Data Endpoint、または完全な Data Security Suite を購入することができます。

Websense Web およびデータ セキュリティ ソリューションは、基本的方法で連係動作し、データ セキュリティ ソフトウェアに、User Service によって収集されたユーザー情報およびマスタ データベースからの URL 分類情報へのアクセス提供します。

ウェブとデータ セキュリティを組み合せることによって、URL の分類に関するルールに基づくデータ損失防止（DLP）ポリシーを作成できます。たとえば、クレジット カード番号を既知の詐欺サイトに送信できないルールを定義できます。また、IP アドレスではなく、ユーザーおよびコンピュータに基づくルールを定義できます。たとえば、Jane Doe は金融情報を FTP サイトに送信できません。

Web 上でのデータ損失保護の設定方法のエンドツーエンドの説明については、Deployment and Installation Center を参照してください。この説明は、Websense Content Gateway を含む種々のコンポーネントのインストール、配備、および設定を含みます。

データ セキュリティ ポリシーの作成方法については、Data Security Help を参照してください。

13 Web Security ポリシーの調整

Web Security Help | Web Security ソリューション | バージョン 7.8.x

もっとも単純なインターネット アクセス ポリシーの実施では、1 つのポリシーを使って 1 つのカテゴリ フィルタと 1 つのプロトコル フィルタを週 7 日、1 日 24 時間適用します。しかし、Web Security ソリューションは、この基本的なセーフティ ネットをはるかに超えて、インターネット使用状況を必要とされる詳細レベルで管理できるツールを提供します。以下のことが可能です。

- **制限付きアクセス フィルタ**を作成し、特定のユーザーに対して、指定されたサイトのリスト以外のすべてのサイトへのアクセスをブロックする（*ユーザーのアクセスを、指定した URL のリストに制限する*、314 ページを参照）。
- **カスタム カテゴリ**を作成し、選択したサイトのフィルタリング方法を再定義する（*カテゴリの使用*、322 ページを参照）。
- **URL をカテゴリ変更**し、特定のサイトをデフォルトのマスタ データベースのカテゴリから他の Websense 定義のカテゴリまたはカスタム カテゴリに移動する（*特定の URL の再分類*、330 ページを参照）。
- **帯域幅**制限を適用し、帯域幅使用状況が指定したしきい値に到達したとき、そうでなければ許可されていたカテゴリおよびプロトコルへのユーザーのアクセスをブロックする（*Bandwidth Optimizer による帯域幅の管理*、342 ページを参照）。

  Websense Web Security Gateway Anywhere 環境の場合、帯域幅ベースの制限は、ハイブリッド サービスによって管理されている要求には適用されません。
- **キーワード**を定義し、キーワード ブロック機能が有効で、アクティブ化されているとき、そのキーワードを使って、そうでなければ許可されていたカテゴリ内のサイトをブロックする（*キーワードベースのポリシーの実施*、327 ページを参照）。
- **ファイル タイプ**を定義し、ファイル タイプ ブロック機能がアクティブ化されているとき、そのファイル タイプを使って、そうでなければ許可されていたカテゴリからの選択したファイル タイプのダウンロードをブロックする（*ファイル タイプに基づくトラフィックの管理*、345 ページを参照）。

ユーザーのアクセスを、指定した URL のリストに制限する

関連トピック：
- *制限付きアクセス フィルターと実施の順序*、314 ページ
- *制限付きアクセス フィルタの作成*、316 ページ
- *制限付きアクセス フィルタの編集*、317 ページ

制限付きアクセス フィルタは、インターネット アクセスを許可するための非常に正確な方法を提供します。それぞれの制限付きアクセス フィルタは、個別の URL または IP アドレス、または正規表現のリストです。制限付きアクセス フィルタは、カテゴリ フィルタと同様に、指定した時間の間、ポリシーに追加され、適用されます。ポリシー内で制限付きアクセス フィルタがアクティブにされているとき、そのポリシーを割り当てられているユーザは、そのリストのウェブサイトにのみアクセスできます。他のすべてのサイトはブロックされます。

たとえば、[一年生] ポリシーが特定の教育および参照サイトのみを含む制限付きアクセス フィルタを適用する場合、[一年生] ポリシーによって管理される生徒はこれらのサイトにのみアクセスでき、他のサイトにはアクセスできません。

制限付きアクセス フィルタがアクティブであるとき、そのフィルタに含まれていない URL が要求されたときブロック ページが返されます。

Websense ソフトウェアは、最大 2,500 個の制限付きアクセス フィルタで合計 25,000 個の URL をサポートできます。

制限付きアクセス フィルターと実施の順序

1 人のユーザーに複数のポリシーが適用される場合があります。これが行われるのは、ユーザーが複数のグループに属し、それらのグループが異なるポリシーによって管理されているときです。

1 人のユーザーに複数のグループ ポリシーが適用されるとき、**[Use more restrictive blocking（より厳格な制限でブロックをする）]** の設定（*適用順序*、119 ページを参照）によって、ユーザーの要求に対して適用されるグループ ポリシーが決まります。デフォルトでは、この設定はオフにされています。

Filtering Service は、どのフィルタリング設定がフィルタ レベルで、より緩やかな制限であるかを判断します。ユーザが複数のポリシーに割り当てられ、そのいずれかが制限付きアクセス フィルタを適用する場合、[より緩やかな制限] であるかどうかが直感では判断できない場合があります。

[Use more restrictive blocking] が**オフ**のとき、次のように判断します。

- **[すべてブロック]** のカテゴリ フィルタと制限付きアクセス フィルタが適用可能である場合、常に制限付きアクセス フィルタが [より緩やか] であるとみなされます。
- 他のカテゴリ フィルタと制限付きアクセス フィルタが適用可能である場合、カテゴリ フィルタが [より緩やか] であるとみなされます。

  つまり、制限付きアクセス フィルタがサイトを許可していても、カテゴリ フィルタがそのサイトをブロックした場合は、そのサイトはブロックされます。

[Use more restrictive blocking] が**オン**のとき、制限付きアクセス フィルタは、[すべてブロック] を除くすべてのカテゴリ フィルタよりも厳密な制限であると見なされます。

下の表は、複数のポリシーが適用可能であるとき、**[Use more restrictive blocking]** の設定のポリシー実施への影響を要約しています。

	[Use more restrictive blocking] がオフ	***[Use more restrictive blocking] がオン***
制限付きアクセス フィルタ ＋ **[すべてブロック]** カテゴリのフィルタ	制限付きアクセス フィルタ（要求が許可される）	**すべてブロック**（要求がブロックされる）
制限付きアクセス フィルタ ＋許可されたカテゴリ	カテゴリ フィルタ（要求が許可される）	制限付きアクセス フィルタ（要求が許可される）
制限付きアクセス フィルタ ＋ブロックされたカテゴリ	カテゴリ フィルタ（要求がブロックされる）	制限付きアクセス フィルタ（要求が許可される）
制限付きアクセス フィルタ ＋割り当て時間 / 確認カテゴリ	カテゴリ フィルタ（要求が割り当て時間 / 確認によって制限される）	制限付きアクセス フィルタ（要求が許可される）

制限付きアクセス フィルタの作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *フィルタの使用、71 ページ*
- *ユーザーのアクセスを、指定した URL のリストに制限する、314 ページ*
- *制限付きアクセス フィルタの編集、317 ページ*

[Add Limited Access Filter（制限付きアクセス フィルタの追加）] ページ（**[Filters]** または **[Edit Policy]** ページからアクセス）で、新しいフィルタの一意な名前と説明を入力します。フィルタを作成した後、許可する URL のリストを入力し、フィルタをポリシーに割り当て、そのポリシーをクライアントに割り当てます。

1. 一意な**フィルタ名**を入力します。名前は 1 ～ 50 文字でなければならず、また、以下の文字を含むことはできません。

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   フィルタ名にはスペース、ダッシュ、アポストロフィーを含めることができます。

2. フィルタの短い**説明**を入力します。この説明は、[Filters]ページの [Limited Access Filters] セクションのフィルタ名の隣に表示されます。管理者が継続的にポリシーを管理するのを支援するために、フィルタの目的を説明する必要があります。

   フィルタ名に適用される使用文字の制限は、説明にも適用されますが、2 つの例外があります。説明にはピリオド（.）およびカンマ（,）を使用できます。

3. 新しいフィルタを確認および編集するには、**[OK]** をクリックします。変更を取り消し、[Filters] ページに戻るには、**[Cancel]** をクリックします。

新しい制限付きアクセス フィルタを作成すると、そのフィルタは **[Policy Management] > [Filters] > [Limited Access Filters]** リストに追加されます。フィルタ名をクリックして、フィルタを編集します。

新しいフィルタのカスタマイズを完了するには、*制限付きアクセス フィルタの編集*の手順に進みます。

制限付きアクセス フィルタの編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ユーザーのアクセスを、指定した URL のリストに制限する*、314 ページ
- *制限付きアクセス フィルターと実施の順序*、314 ページ
- *制限付きアクセス フィルタの作成*、316 ページ
- *ポリシーの編集*、116 ページ

制限付きアクセス フィルタは URL、IP アドレス、正規表現から成るリストで、ユーザーがアクセスできるウェブサイトを指定するために使用します。クライアントにフィルタが適用されると、そのクライアントはリストにないサイトにアクセスできません。

重要

制限付きアクセスフィルタによって許可されている URL が悪意のあるコードに感染した場合、[セキュリティ] カテゴリがブロックされている限り、そのサイトへのユーザー要求はブロックされます。

この動作を変更する手順は、*[セキュリティ リスク] カテゴリを優先*、331 ページを参照してください。

[Policy Management（ポリシーの管理）] > [Filters（フィルタ）] > [Edit Limited Access Filter（制限付きアクセス フィルタの編集）] ページを使用して、既存の制限付きアクセス フィルタを変更します。フィルタ名および説明を変更し、フィルタを適用するポリシーのリストを表示し、どの URL、IP アドレス、正規表現がそのフィルタに含まれるかを管理できます。

制限付きアクセス フィルタを編集すると、変更はそのフィルタを適用するすべてのポリシーに影響を与えます。

1. フィルタ名と説明を確認します。フィルタ名を変更するには、**[Rename（名前の変更）]** をクリックし、新しい名前を入力します。選択した制限付きアクセス フィルタを適用するすべてのポリシーで名前が更新されます。
2. **[Policies using this filter（このフィルタを使用しているポリシー）]** フィールドを使用して、現在このフィルタを適用しているポリシーの数を確認します。1 つ以上のポリシーがフィルタを適用する場合、**[View policies（ポリシーの表示）]** をクリックしてそれらのポリシーをリストします。

3. [Add or Remove Sites（サイトを追加または削除）] で、制限付きアクセス フィルタに追加する URL および IP アドレスを入力します。IP アドレスは IPv4 または IPv6 フォーマットを使用できます。

   1 行に 1 件の URL または IP アドレスを入力します。

   - HTTP サイトの接頭語 **http://** を含める必要はありません。
   - HTTP サイトがそのマスタ データベースのカテゴリに従って管理されるとき、Websense ソフトウェアは URL をその同等の IP アドレスと照合します。制限付きアクセス フィルタの場合はそうではありません。ウェブサイトの URL および IP アドレスを許可するには、その両方をフィルタに追加します。
   - FTP および HTTPS サイトについては、接頭語を付けて、サイトのホスト（ドメイン）名ではなく IP アドレスを指定します。

4. 右矢印（>）をクリックして、URL および IP アドレスを許可されたサイトのリストに追加します。
5. 個別のサイトを制限付きアクセス フィルタに追加するだけでなく、複数のサイトに一致する正規表現を追加することもできます。正規表現を作成するには、**[Advanced（詳細）]** をクリックします。
   - 正規表現を 1 行に 1 つずつ入力し、右矢印をクリックして、その表現を許可されたサイトのリストに追加します。
   - 正規表現が想定しているサイトと一致することを確認するには、**[Test（テスト）]** をクリックします。
   - ポリシー実施での正規表現の使用の詳細については、*正規表現の使用*、355 ページを参照してください。
6. **[Permitted sites（許可されたサイト）]** リストで URL、IP アドレス、および正規表現を確認します。
   - サイトまたは正規表現を変更するには、それを選択し、**[Edit]** をクリックします。
   - リストからサイトまたは正規表現を削除するには、それを選択し、**[Delete]** をクリックします。
7. フィルタを編集した後、**[OK]** をクリックして変更をキャッシュし、[Filters] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

[Edit Policy（ポリシーを編集）] ページからのサイトの追加

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ユーザーのアクセスを、指定した URL のリストに制限する、314 ページ*
- *制限付きアクセス フィルターと実施の順序、314 ページ*
- *制限付きアクセス フィルタの作成、316 ページ*
- *ポリシーの編集、116 ページ*

制限付きアクセス フィルタに URL および IP アドレスを追加するには、**[Policies] > [Edit Policy] > [Add Sites（サイトの追加）]** ページを使用します。

1 行に 1 件の URL または IP アドレスを入力します。プロトコルを指定しない場合、Websense ソフトウェアは自動的に接頭語 **HTTP://** を追加します。

変更を完了したら、**[OK]** をクリックし、[Edit Policy] ページに戻ります。変更をキャッシュするために、[Edit Policy] ページでも **[OK]** をクリックする必要があります。**[Save and Deploy]** をクリックするまで変更は適用されません。

制限付きアクセス フィルタに行った変更は、フィルタを適用するすべてのポリシーに影響を及ぼします。

ロールへのフィルタおよびポリシーのコピー

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリ フィルタの作成、72 ページ*
- *プロトコル フィルタの作成、76 ページ*
- *制限付きアクセス フィルタの作成、316 ページ*
- *ポリシーの作成、115 ページ*

優先管理者は、**[Filters] > [Copy Filters To Role（ロールにフィルタをコピー）]** および **[Policies] > [Copy Policies To Role（ロールにポリシーをコピー）]** ページを使用して、1 つ以上のフィルタまたはポリシーを指定済み管理ロールにコピーできます。フィルタまたはポリシーがコピーされた後、指定済み管理者は、そのフィルタまたはポリシーを管理対象のクライアントに適用することができます。

- ターゲット ロールには、[Copied（コピー済み）] タグ がフィルタまたはポリシー名の末尾に追加されます。同じフィルタまたはポリシーを複数回コピーした場合、番号が付けられます。例、[（Copied 2）]
- 指定済み管理者は、自分のロールにコピーされたフィルタまたはポリシーを名前変更したり、編集したりできます。
- 指定済み管理ロールにコピーされたカテゴリ フィルタは、そのロールで作成されたカスタム カテゴリのアクションを [Permit（許可）] に設定します。指定済み管理者は、自分のロールに固有のカスタム カテゴリに希望するアクションを設定するために、コピーされたカテゴリ フィルタを更新する必要があります。
- 指定済み管理者が優先管理者によってそのロールにコピーされたフィルタまたはポリシーに対して行った変更は、優先管理者の元のフィルタまたはポリシーにも、そのフィルタまたはポリシーのコピーを受け取った他のロールにも影響を及ぼしません。
- フィルタ ロックの制限は、優先管理者の元のフィルタまたはポリシーに影響を及ぼしませんが、指定済み管理者のフィルタまたはポリシーのコピーには影響を及ぼします。
- 指定済み管理者はフィルタ ロックの制限の影響を受けますから、[すべて許可] のカテゴリおよびプロトコル フィルタを指定済み管理ロールにコピーすることはできません。

フィルタまたはポリシーをコピーするには、以下の手順を実行します。

1. [Copy Filters to Role] または [Copy Policies to Role] ページで、ページ上部のリストに正しいポリシーまたはフィルタが示されていることを確認します。
2. **[Select a role（ロールの選択）]** ドロップダウンリストを使用して、宛先ロールを選択します。
3. **[OK]** をクリックします。

   ポップアップ ダイアログボックスに、選択したフィルタまたはポリシーがコピーされたことが示されます。コピー プロセスには少し時間がかかります。

   [Save and Deploy] をクリックするまで変更は適用されません。

コピー プロセスが完了した後、選択したロール内の指定済み管理者が次回 TRITON コンソール にログオンするとき、コピーされたフィルタまたはポリシーを使用できるようになります。フィルタまたはポリシーをコピーするときに指定済み管理者がそのポリシーへのアクセス権をもつロールにログオンしている場合、指定済み管理者は、ログオフして再びログオンするまで、新しいフィルタまたはポリシーを表示することはできません。

フィルタ コンポーネントの作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Policy Management] > [Filter Components（フィルタ コンポーネント）] ページを使用して、Websense ソフトウェアが組織内のインターネット アクセス ポリシーを適用する方法を精緻化およびカスタマイズするためのツールにアクセスします。画面上の 3 つのボタンは、下記のタスクに関連付けられています。

Edit Categories	• URL をカテゴリ変更します（*特定の URL の再分類、330 ページ*を参照）。たとえば、[ショッピング] カテゴリがポリシーによってブロックされている場合に、特定のサプライヤーのサイトまたはパートナーのサイトへのアクセスを許可するために、これらのサイトを [ビジネス] や [経済] のような、許可されたカテゴリに移動することができます。 • カスタム カテゴリを定義または編集します（*カスタム カテゴリの作成、326 ページ*を参照）。Websense によって定義されている親カテゴリ、またはユーザ定義の親カテゴリの中に追加のサブカテゴリを作成し、次にその新しいカテゴリに URL を割り当てます。 • カテゴリにキーワードを割り当てます（*キーワード ベースのポリシーの実施、327 ページ*を参照）。URL が特定の文字列を含むサイトをカテゴリ変更し、そのサイトへのアクセスをブロックするには、最初にキーワードを定義し、次にカテゴリ フィルタ内でキーワード ブロックを有効にします。 • 複数のURLに一致する正規表現（*正規表現の使用、355 ページ*を参照）、パターン、またはテンプレートを作成し、それらをカテゴリに割り当てます。
Edit Protocols	カスタム プロトコル定義を定義または編集します（*カスタム プロトコルの作成、340 ページ*および*カスタム プロトコルの編集、337 ページ*を参照）。たとえば、組織のメンバーがカスタム メッセージング ツールを使用する場合、そのツールの使用を許可しながら、他のインスタント メッセージ / チャット プロトコルをブロックするようにカスタム プロトコル定義を作成することができます。
File Types	通常は許可されるカテゴリ内の特定のファイル タイプをブロックするために使用するファイル タイプを作成または編集します（*ファイル タイプに基づくトラフィックの管理、345 ページ*を参照）。

カテゴリの使用

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリとその属性の編集、322 ページ*
- *カスタム カテゴリの作成、326 ページ*
- *キーワードベースのポリシーの実施、327 ページ*
- *特定の URL の再分類、330 ページ*

Websense ソフトウェアでは、マスタ データベースに登録されていないサイトを管理したり、マスタ データベース内の個別の URL の処理方法を変更するための種々の方法を利用できます。

- より精緻なポリシーの実施およびレポート作成のために**カスタム カテゴリ**を作成する。
- カテゴリ変更された **URL** を使用して、未分類のサイトのカテゴリを定義したり、マスタ データベースに登録されているサイトのカテゴリを変更する。
- URL が特定の文字列を含むすべてのサイトをカテゴリ変更するために**キーワード**を定義する。

カテゴリへのアクセスの試みをログ データベースに記録するかどうかを設定する場合は、*要求がログ記録される方法の設定、505 ページ*を参照してください。カテゴリをログに記録しない場合、クライアントからのそのカテゴリへの要求はレポートに表れません。

カテゴリとその属性の編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カスタム カテゴリの作成、326 ページ*
- *カスタマイズされたすべてのカテゴリ属性の確認、324 ページ*
- *グローバル カテゴリの変更 [グローバル カテゴリのへんこう]、324 ページ*
- *キーワードベースのポリシーの実施、327 ページ*
- *特定の URL の再分類、330 ページ*

[Policy Management] > [Filter Components] > [Edit Categories] ページを使用して、カスタム カテゴリ、カテゴリ変更された URL、キーワードを作成および変更します。

Websense 定義およびカスタムの既存のカテゴリの両方がコンテンツ ペインの左側にリストアップされています。カテゴリと関連付けられている現在のカスタム設定を表示するか、または新しいカスタム定義を作成するには、最初にリストからカテゴリを選択します。

すべてのカテゴリに関連付けられているすべてのカスタム URL、キーワード、および正規表現をリストアップするには、ページ最上部のツールバーの **[View All Custom URLs / Keywords（すべてのカスタム URL/ キーワードの表示）]** をクリックします。詳細は、*カスタマイズされたすべてのカテゴリ属性の確認、324 ページ*を参照してください。

- 新しいカテゴリを作成するには、**[Add]**をクリックし、次に、*カスタム カテゴリの作成、326 ページ*で説明する手順を実行します。

  既存のカスタム カテゴリを削除するには、そのカテゴリを選択し、次に、**[Delete]** をクリックします。Websense 定義カテゴリは削除できません。
- カスタム カテゴリの名前または説明を変更するには、そのカテゴリを選択し、**[Rename（名前の変更）]** をクリックします（*カスタム カテゴリの名前変更、325 ページ*を参照）。
- すべてのカテゴリ フィルタでカテゴリに関連付けられたフィルタリング アクションを変更するには、**[Override Action（アクションの優先設定）]** をクリックします（*グローバル カテゴリの変更 [グローバル カテゴリのへんこう]、324 ページ*を参照）。
- **[Recategorized URLs（カテゴリ変更された URL）]** リストは、カテゴリ変更され、このカテゴリに割り当てられたサイト（URL および IP アドレス）を示します。
  - リストにサイトを追加するには、**[Add URLs]** をクリックします。その後の手順については、*特定の URL の再分類、330 ページ*を参照してください。
  - 既存のカテゴリ変更されたサイトを変更するには、URL または IP アドレスを選択し、**[Edit]** をクリックします。
- **[Keywords]** リストにこのカテゴリに関連付けられたキーワードが示されます。
  - 選択したカテゴリに関連付けられたキーワードを定義するには、**[Add Keywords（キーワードの追加）]** をクリックします。その後の手順については、*キーワードベースのポリシーの実施、327 ページ*を参照してください。
  - 既存のキーワードの定義を変更するには、キーワードを選択し、**[Edit]** をクリックします。

- URL とキーワードの他に、カテゴリの**正規表現**を定義できます。各正規表現は、複数のサイトをカテゴリに関連付けるために使用するパターンまたはテンプレートです。

  カテゴリの正規表現を表示または作成するには、**[Advanced]** をクリックします。

  - 正規表現を定義するには、[Add Expressions（式の追加）] をクリックします（*正規表現の使用、355 ページ*を参照）。
  - 既存の正規表現を変更するには、正規表現を選択し、**[Edit]** をクリックします。
- カテゴリ変更された URL、キーワード、または正規表現を削除するには、削除対象の項目を選択し、**[Delete]** をクリックします。

[Edit Categories（カテゴリの編集）] ページでの変更を完了した後、**[OK]** をクリックして変更をキャッシュし、[Filter Components] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

カスタマイズされたすべてのカテゴリ属性の確認

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Filter Components] > [Edit Categories] > [View All Custom URLs and Keywords（すべてのカスタム URL/ キーワードを表示）] ページを使用して、カスタム URL、キーワード、および正規表現の定義を確認します。また、必要がなくなった定義を削除することもできます。

このページには 3 つのよく似たテーブルが含まれます。それぞれのテーブルはカスタム URL、キーワード、正規表現の各カテゴリ属性に対応しています。各テーブルでは、属性は関連付けられているカテゴリの隣にリストされます。

カテゴリ属性を削除するには、対応するチェックボックスをオンにし、**[Delete]** をクリックします。

[Edit Categories] ページに戻るには、**[Close]** をクリックします。[View All Custom URLs and Keywords] ページのいずれかの項目を削除した場合、[Edit Categories] ページで **[OK]** をクリックして変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

グローバル カテゴリの変更 [グローバル カテゴリのへんこう]

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Filter Components] > [Edit Categories] > [Override Action（アクションの優先設定）] ページを使用して、既存のすべてのカテゴリ フィルタでカテゴリに適用されるアクションを変更します。また、これによって新しいフィルタでカテゴリに適用されるデフォルト アクションが決まります。

この変更は既存のすべてのフィルタでそのカテゴリに適用されるアクションを無効にしますが、管理者は後でこれらのフィルタが別のアクションを適用するように編集できます。

カテゴリに適用される設定を変更する前に、**[Selected Category（選択したカテゴリ）]** の隣に正しいカテゴリ名が表示されていることを確認します。次に、以下の手順を実行します。

1. 新しい**アクション**（[許可]、[ブロック]、[確認]、または[割り当て時間]）を選択します。詳細は、*処置、68 ページ*を参照してください。

   デフォルトでは、ページ上のすべてのオプションについて **[Do not change current settings（現在の設定を変更しない）]** が選択されます。
2. **キーワードをブロックする**かどうかを指定します。詳細は、*キーワードベースのポリシーの実施、327 ページ*を参照してください。
3. **ファイル タイプをブロックする**かどうかを指定し、ブロック設定をカスタマイズします。詳細は、*ファイル タイプに基づくトラフィックの管理、345 ページ*を参照してください。
4. **[Block with Bandwidth Optimizer（Bandwidth Optimizer を使用してブロックする）]** によって HTTP サイトへのアクセスを管理するかどうかを指定し、ブロック設定をカスタマイズします。詳細は、*Bandwidth Optimizer による帯域幅の管理、342 ページ*を参照してください。

   重要
   ここで行った変更は、**[すべてブロック]** および **[すべて許可]** を除いて、既存のすべてのカテゴリ フィルタに影響を及ぼします。

5. **[OK]** をクリックして、[Edit Categories] ページに戻ります（*カテゴリとその属性の編集、322 ページ*を参照）。[Edit Categories] ページで **[OK]** をクリックするまで、変更はキャッシュされません。

カスタム カテゴリの名前変更

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Filter] [Components] > [Edit Categories] > [Rename Category（カテゴリの名前を変更）] ページを使用して、カスタム カテゴリに関連付けられた名前または説明を変更します。

- カテゴリ名を編集するには、**[Filter name（フィルタ名）]** フィールドを使用します。新しい名前は一意でなければならず、50 文字以内で指定します。

  名前には下記の文字を含めることはできません。

  ```
  * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
  ```

- カテゴリの説明を編集するには、**[Description（説明）]** フィールドを使用します。説明は 255 文字以内で入力します。

  フィルタ名に適用される使用文字の制限は、説明にも適用されますが、2 つの例外があります。説明にはピリオド（.）およびカンマ（,）を使用できます。

変更を完了したら、**[OK]** をクリックし、[Edit Categories] ページに戻ります。[Edit Categories] ページで **[OK]** をクリックするまで、変更はキャッシュされません。

カスタム カテゴリの作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリとその属性の編集、322 ページ*
- *キーワードベースのポリシーの実施、327 ページ*
- *特定の URL の再分類、330 ページ*

マスタ データベースに登録されている 90 個以上の Websense 定義のカテゴリのほかに、より詳細なポリシーの実施およびレポート作成のためにユーザー固有の**カスタム カテゴリ**を定義できます。たとえば、以下のようなカスタム カテゴリを作成します。

- **[出張]**。従業員が航空券の購入、自動車のレンタル、ホテルの予約のために使用できる承認されたベンダーからのサイトをグループ化します。
- **[参考資料]**。小学生に適しているとみなされるオンライン辞書サイトまたは百科事典サイトをグループ化します。
- **[専門開発]**。従業員がスキルを向上させるために使用することを奨励されるトレーニング サイトまたは他のリソースをグループ化します。

[Policy Management] > [Filter Components] > [Edit Categories] > [Add Category（カテゴリの追加）] ページを使用して、カスタム カテゴリを任意の親カテゴリに追加します。最大 100 個のカスタム カテゴリを作成できます。

1. 一意で、わかりやすい**カテゴリ名**を入力します。名前には下記の文字を含めることはできません。

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

2. 新しいカテゴリの**説明**を入力します。

   フィルタ名に適用される使用文字の制限は、説明にも適用されますが、2 つの例外があります。説明にはピリオド（.）およびカンマ（,）を使用できます。

3. **[Add to（追加先）]** リストから親カテゴリを選択します。デフォルトでは、**[All Categories（すべてのカテゴリ）]** が選択されます。

4. このカテゴリに追加するサイト（URL または IP アドレス）を入力します。詳細は、*特定の URL の再分類、330 ページ*を参照してください。

   カテゴリを作成した後でこのリストを編集することもできます。

5. このカテゴリに関連付けるキーワードを入力します。詳細は、*キーワードベースのポリシーの実施、327 ページ*を参照してください。

   カテゴリを作成した後でこのリストを編集することもできます。

6. 既存のすべてのカテゴリ フィルタでこのカテゴリに適用するデフォルトの**アクション**を選択します。後で個別のフィルタでこのアクションを編集できます。

> **注意**
> 指定済み管理ロールにコピーされたカテゴリ フィルタは、そのロールで作成されたカスタム カテゴリのアクションを [Permit（許可）] に設定します。指定済み管理者は、自分のロールに固有のカスタム カテゴリに希望するアクションを設定するために、コピーされたカテゴリ フィルタを更新する必要があります。

7. 既存のすべてのカテゴリ フィルタでこのカテゴリを適用する必要がある**高度なフィルタリング** アクション（[キーワード ブロック]、[ファイル タイプ ブロック]、または [帯域幅ブロック]）を有効にします。
8. 新しいカテゴリの定義を完了したとき、**[OK]** をクリックして変更をキャッシュし、[Edit Categories] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

新しいカテゴリが [Categories] リストに追加され、そのカテゴリのカスタム URL およびキーワード情報が表示されます。

キーワードベースのポリシーの実施

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *特定の URL の再分類、330 ページ*
- *フィルタリング設定値の設定、81 ページ*
- *カテゴリ フィルタの作成、72 ページ*
- *カテゴリ フィルタの編集、73 ページ*
- *カテゴリの使用、322 ページ*

カテゴリにキーワードを関連付けることによって、明示的にマスタ データベースに追加されていない、またはカスタム URL として定義されていない

URL に対する保護を提供することができます。キーワード ブロックを有効にするには次の 3 つの手順が必要です。

1. グローバル レベルでキーワード ブロックを有効にします（*フィルタリング設定値の設定、81 ページ*を参照）。
2. カテゴリに関連付けられたキーワードを定義します（*キーワードの定義、329 ページ*を参照）。
3. アクティブ カテゴリ フィルタでそのカテゴリに対してキーワード ブロックを有効にします（*カテゴリ フィルタの編集、73 ページ*を参照）。

キーワードが定義され、特定のカテゴリに対してキーワード ブロックが有効にされたとき、Websense ソフトウェアは次のように、キーワードをそれぞれの要求された URL と照合します。

- キーワードが ASCII 文字のみを含んでいる場合、キーワードは URL のドメイン、パス、クエリ部分と照合されます。

  たとえば、キーワード [nba] を許可されている [スポーツ] カテゴリに関連付けている場合、下記の URL はブロックされます。

  - sports.espn.go.com/**nba**/
  - moder**nba**kery.com
  - fashio**nba**r.com

- キーワードが ASCII 文字セット以外の文字を含んでいる場合、キーワードは文字列のパスおよびクエリ部分とだけ照合されます。

  たとえば、キーワード [futbol] を許可されている [スポーツ] カテゴリに関連付けている場合、下記のようになります。

  - [www.**futbol**.com] は、**許可されます**（URL のドメインの部分は照合されません）
  - [es.wikipedia.org/wiki/**Futbol**] は、**ブロックされます**（URL のパス部分は許可されます）

サイトがキーワードによってブロックされている場合、サイトはキーワードの一致に従ってカテゴリ変更されます。レポートはサイトのマスタ データベース カテゴリではなく、キーワード カテゴリを示します。

キーワードを定義するとき、ブロックする必要がないサイトがブロックされないように注意してください。

重要

[Extended Protection] サブカテゴリにキーワードを関連付けることは避けてください。これらのカテゴリに対してはキーワード ブロックは適用されません。

要求がキーワードに基づいてブロックされたとき、ユーザが受け取る Websense ブロック ページにそのことが示されます。

キーワードの定義

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリ フィルタの編集、73 ページ*
- *カテゴリの使用、322 ページ*
- *キーワードベースのポリシーの実施、327 ページ*
- *正規表現の使用、355 ページ*

キーワードは、URL に含まれる文字（語、句、頭字語など）から成る文字列です。キーワードをカテゴリに割り当て、カテゴリ フィルタでキーワード ブロックを有効にします。

[Policy Management] > [Filter Components] > [Edit Categories] > [Add Keywords] ページを使用して、キーワードをカテゴリに関連付けます。キーワード定義を変更する必要がある場合は、**[Edit Keywords]** ページを使用します。

キーワードを定義するとき、ブロックする必要がないサイトがブロックされないように注意してください。たとえば、キーワード [sex] を使用してアダルト サイトをブロックしようとすると、sextuplets や City of Essex のような語や、m**sex**change.org（IT）、vega**sex**perience.com（旅行）、sci.esa.int/mar**sex**press（教育機関）などのサイトに対する検索エンジン要求がブロックされます。

キーワードを 1 行に 1 つずつ入力します。

- キーワードにスペースを含めてはいけません。URL および CGI 文字列は、語と語の間にスペースを含みません。
- 以下のような特殊文字の前にはバックスラッシュ（\）を入力します。

  ```
  . , # ? * +
  ```

  バックスラッシュを入力しないと、Websense ソフトウェアは特殊文字を無視します。
- [Extended Protection] サブカテゴリにキーワードを関連付けることは避けてください。これらのカテゴリに対してはキーワード ブロックは適用されません。

キーワードの追加または編集が完了したとき、**[OK]** をクリックして変更をキャッシュし、[カテゴリの編集] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

キーワード ブロックを適用するためには、さらに以下の手順を実行する必要があります。

1. **[Settings] > [General] > [Filtering]** ページを順に選択して、キーワード ブロックを有効化します（*フィルタリング設定値の設定、81 ページ*を参照）。
2. 1 つ以上のアクティブ カテゴリ フィルタでキーワード ブロックを有効にします（*カテゴリ フィルタの編集、73 ページ*を参照）。

特定の URL の再分類

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ポリシーの例外、129 ページ*
- *カスタム カテゴリの作成、326 ページ*
- *キーワードベースのポリシーの実施、327 ページ*

Web Security manager を使用して、URL に割り当てられているカテゴリを変更することができます。新しいカテゴリに追加された URL を カスタム URL またはカテゴリ変更された URL と言います。

- **[Policy] [Management] > [Filter Components] > [Edit Categories] > [Recategorize URLs（URL のカテゴリ変更）]** ページを使用して、個別のサイトをいずれかのカテゴリに追加します。
- 既存のカテゴリ変更されたサイトの変更は、**[Edit URLs（URL の編集）]** ページで行います。

URL のカテゴリを変更するためには、その URL を下記のカテゴリに追加します。

- 異なる Websense 定義のカテゴリ
- 任意のカスタム カテゴリ（*カスタム カテゴリの作成、326 ページ*を参照）

デフォルトではカテゴリ変更された URL はブロックされません。それらの URL は、各アクティブ カテゴリ フィルタで新しいカテゴリに適用されるアクションに従ってフィルタリングされます。

重要

許可されているカテゴリにカテゴリ変更された URL が悪意のあるコードに感染した場合、[セキュリティ] カテゴリがブロックされている限り、そのサイトへのユーザー要求はブロックされます。

この動作を変更する手順は、*[セキュリティ リスク] カテゴリを優先、331 ページ*を参照してください。

サイトをカテゴリ変更するとき、以下の手順を実行します。

- URL または IP アドレスを 1 行に 1 件ずつ入力します。
  - サイトが複数の URL によってアクセスできる場合、そのサイトにアクセスするために使用できる各 URL をカスタム URL として定義し、サイトが意図している通りに許可またはブロックされるようにします。
  - カテゴリ変更された URL の場合、URL は自動的には同等の IP アドレスと照合されません。サイト要求が適切に処理されるようにするために、サイトの URL と IP アドレスの両方を指定します。
- 非 HTTP サイトのプロトコルを含めます。このプロトコルを省略した場合、Websense ソフトウェアはサイトを HTTP サイトとしてフィルタリングします。

  HTTPS サイトでは、ポート番号（https://63.212.171.196:443/、https://www.onlinebanking.com:443/）も含めます。
- Websense ソフトウェアは、カスタム URL を入力された通りに認識します。[検索エンジン & ポータル] カテゴリがブロックされていて、**www.yahoo.com** を許可されたカテゴリにカテゴリ変更した場合、このサイトはユーザーが完全なアドレスを入力した場合のみ許可されます。ユーザーが images.search.yahoo.com、または単に yahoo.com と入力した場合、サイトはブロックされます。しかし、**yahoo.com** をカテゴリ変更した場合、アドレスに yahoo.com という語を含むすべてのサイトは許可されます。

カテゴリ変更されたサイトの追加または編集が終ったら、**[OK]** をクリックして [Edit Categories] ページに戻ります。変更をキャッシュするために、[Edit Categories] ページでも **[OK]** をクリックする必要があります。**[Save and Deploy]** をクリックするまで変更は適用されません。

Websense ソフトウェアは、マスタ データベースを参照する前にサイトのカスタム URL 定義を検索しますから、カテゴリ変更された URL に割り当てられているカテゴリに従ってサイトをフィルタリングします。

カテゴリ変更した URL を保存した後、右側のショートカット ペインの**[URL Category（URL カテゴリ）]** ツールを使用して、サイトが正しいカテゴリに割り当てられていることを確認します。*ツールボックスによるポリシーの実施動作の確認、356 ページ*を参照してください。

[セキュリティ リスク] カテゴリを優先

Web Security Help | Web Security ソリューション | バージョン 7.8.x

デフォルトでは、サイトが [セキュリティ リスク] カテゴリに分類されている時、サイトは下記のような場合でも、そのセキュリティ リスクの分類を基にフィルタリングされます。

- サイトがカテゴリ変更された URL として [許可されている] カテゴリに追加されている
- サイトが制限付きアクセス フィルタの中にある

> **注意**
> [Extended Protection] カテゴリは [セキュリティ リスク] クラスのデフォルトのメンバーですが、このカテゴリはまだ解析されていないサイトを集めているため、他のカテゴリよりも低い優先順位が与えられます。そのため、カスタム カテゴリは常に [Extended Protection] カテゴリに優先されます。

Filtering Service またはハイブリッド サービスがサイトを [セキュリティ リスク] クラス カテゴリに割り当てた場合（マスタ データベースのカテゴリまたは Content Gateway の分析に基づいて）、次のようになります。

- カテゴリ フィルタが有効で、セキュリティ関連のサイトがブロックされる場合、サイトはブロックされます。
- 制限つきアクセス フィルタが有効である場合、サイトはブロックされます。

Web Security manager の **[Settings] > [General] > [Risk Classes（リスク クラス）]** ページで、どのカテゴリが [セキュリティ リスク] クラスに含まれるかを設定します。

サイトが [セキュリティ リスク] カテゴリ（[悪意のある Web サイト]、[スパイウェア] など）に含まれているかどうかに関わりなく、常にカスタム カテゴリに基づいてフィルタリングする場合は、以下の手順を実行します。

1. Filtering Service を実行しているコンピュータ上で Websense **bin** ディレクトリ（C:\Program Files または Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）に移動し、テキスト エディタで **eimserver.ini** ファイルを開きます。
2. **[FilteringManager]** セクションへ移動し、下記の行を追加します。

   ```
   SecurityCategoryOverride=OFF
   ```

3. ファイルを保存して、閉じます。
4. Filtering Service を再起動します。
   - *Windows*: [Services（サービス] ツールを使用して Websense Filtering Service を再起動します。
   - *Linux*: /opt/Websense/WebsenseDaemonControl コマンドを使って Filtering Service を停止してから起動します。

Websense Web Security Gateway Anywhere 環境の場合、ハイブリッド サービスによってこの機能を無効化できます。

1. Filtering Service を実行しているコンピュータ上で Websense **bin** ディレクトリ（C:\Program Files または Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）に移動し、テキスト エディタで **eimserver.ini** ファイルを開きます。
2. このパラメータがまだ存在しない場合は、**[hybrid]** というセクションを追加し、次に、下記のように **SecurityCategoryOverride** パラメータを追加します。

   ```
   [hybrid]
   SecurityCategoryOverride=false
   ```

3. ファイルを保存して、閉じます。
4. Sync Service を再起動します。
   - *Windows* の場合：[Services（サービス] ツールを使用して Websense Sync Service を再起動します。
   - *Linux* の場合：/opt/Websense/WebsenseDaemonControl コマンドを使って Sync Service を停止してから起動します。

一部のカテゴリに属するサイトへの送信のブロック

デフォルトでは、ユーザーがあるカテゴリ（例、[メッセージ ボード]、[フォーラム]）へのアクセスを許可されている場合、ユーザーはそのカテゴリのサイトを閲覧し、そのサイトに送信することができます。

BlockMessageBoardPosts 設定パラメータを使用して、Websense ソフトウェアが特定のカテゴリのサイトへの転送をブロックするように設定できます。

- このパラメータが**オン**に設定されている場合、ユーザーは [メッセージ ボード] および [フォーラム] カテゴリのサイトへの送信のみをブロックされます。
- このパラメータにカテゴリ識別子のカンマ区切りリスト（**112,122,151** のような形式）を付加することができます。この場合、ユーザーはリストされているいずれかのカテゴリに含まれるサイトへの送信をブロックされます。

オン プレマイズ コンポーネントでこの機能を有効化するには、以下の手順を実行します。

1. Filtering Service を実行しているコンピュータ上で Websense **bin** ディレクトリ（C:\Program Files または Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）に移動し、テキスト エディタで **eimserver.ini** ファイルを開きます。
2. **[WebsenseServer]** セクションへ移動し、下記の行を追加します。

   ```
   BlockMessageBoardPosts=<value>
   ```

   ここで、*<value>* には、**[ON]** またはカテゴリ識別子のカンマ区切りリストを入力します。
3. ファイルを保存して、閉じます。
4. Filtering Service を再起動します。
   - *Windows* の場合：[Services（サービス] ツールを使用して Websense Filtering Service を再起動します。
   - *Linux* の場合：/opt/Websense/WebsenseDaemonControl コマンドを使って Filtering Service を停止してから起動します。

Websense Web Security Gateway Anywhere 環境の場合、ハイブリッド サービスとしてこの機能を有効化するには、下記の手順を実行します。

1. Filtering Service を実行しているコンピュータ上で Websense **bin** ディレクトリ（C:\Program Files または Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）に移動し、テキスト エディタで **eimserver.ini** ファイルを開きます。
2. このパラメータがまだ存在しない場合は、**[hybrid]** というセクションを追加し、次に、下記のように **BlockMessageBoardPosts** パラメータを追加します。

   ```
   [hybrid]
   BlockMessageBoardPosts=<value>
   ```

   ここで、*<value>* はカテゴリ識別子のカンマ区切りリストです。
3. ファイルを保存して、閉じます。
4. Sync Service を再起動します。
   - *Windows* の場合：[Services（サービス] ツールを使用して Websense Sync Service を再起動します。
   - *Linux* の場合：/opt/Websense/WebsenseDaemonControl コマンドを使って Sync Service を停止してから起動します。

プロトコルの使用

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense マスタ データベースは、HTTP、HTTPS、および FTP 以外のインターネット プロトコルをフィルタリングするために使用するプロトコル定義を含んでいます。これらの定義は、インスタント メッセージ、ストリーミング メディア、ファイル共有、ファイル転送、インターネット メール、その他のネットワークおよびデータベース操作に使用するインターネット アプリケーションやデータ転送方法を含みます。

これらのプロトコル定義を使用して、通常は HTTP トラフィックが使用するポートをトンネルすることによってファイアウォールを迂回するプロトコルまたはアプリケーションをフィルタリングすることもできます。たとえば、インスタント メッセージ データは、HTTP ポートをトンネルすることによって、ファイアウォールでインスタント メッセージング プロトコルをブロックしているネットワークに侵入することができます。Websense ソフトウェアはこれらのプロトコルを正確に識別し、それらをユーザが設定したポリシーに従ってフィルタリングします。

注意

Websense Web Filter および Websense Web Security 環境では、プロトコルベースのポリシー適用を有効化するために Network Agent をインストールする必要があります。

Websense Web Security Gateway の場合は、Network Agent を使用せずに HTTP ポートをトンネリングする非 HTTP プロトコルをフィルタリングできます。詳細は、*トンネリング プロトコルの検出*、235 ページを参照してください。

Websense 定義のプロトコル定義を使用するだけでなく、カスタム プロトコルを定義できます。カスタム プロトコル定義は、IP アドレスまたはポート番号を基に作成でき、編集可能です。

特定のポート上のトラフィックをブロックするには、そのポート番号をカスタム プロトコルに関連付け、そのプロトコルのデフォルト アクションを **[Block（ブロック）]** に設定します。

カスタム プロトコル定義を使用するには、**[Policy Management] > [Filter Components）]** を選択し、**[Protocols]** をクリックします。詳細については、*カスタム プロトコルの編集*、337 ページおよび*カスタム プロトコルの作成*、340 ページを参照してください。

プロトコルベースのポリシーの実施

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プロトコルの使用*、335 ページ
- *カスタム プロトコルの編集*、337 ページ
- *カスタム プロトコルの作成*、340 ページ
- *プロトコル ID の追加または編集*、338 ページ
- *Websense によって定義されたプロトコルへの追加*、342 ページ

Network Agent がインストールされているとき、または Websense Web Security Gateway 環境で、Websense ソフトウェアは、データの性質に関係なく、特定のポート上で送信された、または特定の IP アドレスを使用する、もしくは特定の署名が付いているインターネット コンテンツをブロックできます。デフォルトでは、ポートをブロックすると、ソースに関係なく、そのポートを通ってネットワークに入るすべてのインターネット コンテンツがブロックされます。

注意

場合によっては、特定のポート上で送信される内部ネットワーク トラヒックが、そのポートを使用するプロトコルがブロックされている場合でも、ブロックされないことがあります。プロトコルが内部サーバー上でデータを送信する速度が、Network Agent でデータをキャプチャおよび処理できる速度を上回ることがあります。これはネットワークの外側から発信されたデータでは起こりません。

プロトコル要求が行われたとき、Web Security ソリューションは、以下の手順によって、その要求をブロックするか許可するかを決定します。

1. プロトコル（またはインターネット アプリケーション）の名前を調べます。
2. 要求の宛先アドレスを基にプロトコルを識別します。
3. カスタム プロトコル定義の中の関連するポート番号または IP アドレスを検索します。
4. Websense によって定義されたプロトコル定義の中の関連するポート番号、IP アドレスまたは署名を検索します。

この情報のいずれかがわからない場合、このプロトコルに関連するすべてのコンテンツが許可されます。

プロトコルが FTP、HTTPS、または gopher である場合、最初にプロトコルがブロックされているかどうか確認するためのチェックが行われます。プロトコルが許可されている場合は、Filtering Service は、要求されたサイトが許可されているか、ブロックされているかを確認するために、URL のルックアップを実行します。

カスタム プロトコルの編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プロトコルの使用、335 ページ*
- *カスタム プロトコルの作成、340 ページ*
- *プロトコル フィルタの作成*
- *プロトコル フィルタの編集*
- *カテゴリの使用*

[Policy Management] > [Filter Components] > [Edit Protocols] ページを使用して、カスタム プロトコル定義を作成および編集したり、Websense によって定義されたプロトコル定義を検討することができます。Websense によって定義されたプロトコルを編集することはできません。

プロトコル リストは、すべてのカスタム プロトコルおよび Websense によって定義されたプロトコルを含みます。プロトコルまたはプロトコル グループをクリックすると、選択した項目に関する情報がコンテンツ ペインの右側の部分に表示されます。

新しいカスタム プロトコルを追加するには、**[Add Protocol]** をクリックして、*カスタム プロトコルの作成、340 ページ*の手順を実行します。

プロトコル定義を編集するには、以下の手順を実行します。

1. プロトコル リストでプロトコルを選択します。リストの右側にプロトコル定義が表示されます。
2. すべてのプロトコル フィルタでこのプロトコルに適用されるフアクションを変更するために、**[Override Action]** をクリックします（*グローバル カテゴリの変更 [グローバル カテゴリのへんこう]、339 ページ*を参照）。
3. このプロトコルのための追加のプロトコル ID を定義するために、**[Add Identifier（ID の追加）]** をクリックします（*プロトコル ID の追加または編集、338 ページ*を参照）。
4. リストの中の ID を選択し、次に **[Edit]** をクリックして、その ID によって定義されている**ポート**、**IP アドレス範囲**、または**トランスポート方法**を変更します。

5. 完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

プロトコル定義を削除するには、プロトコル リストから項目を選択し、**[Delete]** をクリックします。

プロトコル ID の追加または編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Filter Components] > [Edit Protocols] > [Add Protocol Identifie] ページを使用して、既存のカスタム プロトコルのための追加のプロトコル ID を定義します。**[Edit Protocol Identifier]** ページを使用して、前に定義されている ID を変更します。

ID を作成または変更する前に、**選択したプロトコル**の横に正しいプロトコル名が表示されていることを確認します。

プロトコル ID を処理するときに、各プロトコルの 1 つ以上の基準（ポート、IP アドレス、またはトランスポート タイプ）が一意でなければならないことに留意してください。

1. この ID に含まれる**ポート**を指定します。
   - **[All Ports（すべてのポート）]** を選択すると、その基準は他のプロトコル定義で入力した他のポートまたは IP アドレスと重複します。
   - ポート範囲に重複があれば、それは一意とはみなされません。たとえば、ポート範囲 80-6000 は、範囲 4000-9000 と重複します。
   - ポート 80 またはポート 8080 でプロトコルを指定するとき注意が必要です。Network Agent はこれらのポートを通じてインターネット要求をリッスンします。

     Network Agent が Websense Web Security Gateway 環境においてはこれらのポートを無視するように設定することができます。

     カスタム プロトコルは Websense プロトコルに優先しますから、ポート 80 を使用するカスタム プロトコルを定義すると、ポート 80 を使用する他のすべてのプロトコルはフィルタされ、カスタム プロトコルと同じようにログ記録されます。
2. この ID に含まれる **IP アドレス**を指定します。
   - **[All external IP addresses（すべての外部 IP アドレスポート）]** を指定すると、その基準は他のプロトコル定義で入力した他の IP アドレスと重複します。
   - IP アドレス範囲に重複があれば、それは一意とはみなされません。
3. この ID に含まれる**プロトコル トランスポート**方法を指定します。
4. **[OK]** をクリックして変更をキャッシュし、[Edit Protocols] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

カスタム プロトコルの名前の変更

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Filter Components] > [Edit Protocols] > [Rename Protocol（プロトコル名の変更）] ページを使用して、カスタム プロトコルの名前を変更するか、またはそれを別のプロトコル グループに移動します。

- **[名前]** フィールドを使ってプロトコル名を編集します。新しい名前は 50 文字以内でなければなりません。

  名前には下記の文字を含めることはできません。

  ```
  * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
  ```

- プロトコルを別のプロトコル グループへ移動するには、**[In group（グループ）]** フィールドから新しいグループを選択します。

変更を完了したら、**[OK]** をクリックし、[Edit Protocols] ページに戻ります。変更をキャッシュするために、[Edit Protocols] ページでも **[OK]** をクリックしなければなりません。

グローバル カテゴリの変更 [グローバル カテゴリのへんこう]

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Filter Components] > [Edit Protocols] > [Override Action] ページを使用して、既存のすべてのプロトコル フィルタでのプロトコルのフィルタリング方法を変更できます。この操作はまた、新しいフィルタでプロトコルに適用されるデフォルトのアクションを決定します。

この変更は既存のすべてのプロトコル フィルタで適用されるアクションを無効化しますが、管理者は後でそれらのフィルタが異なるアクションを適用するように編集することができます。

1. **選択したプロトコル**の横に正しい名前が表示されていることを確認します。
2. このプロトコルに適用する新しい **[Action（アクション）]**（[許可]または [ブロック]）を選択します。デフォルトでは、**[No change（変更なし）]** が選択されています。詳細は、*処置、68 ページ*を参照してください。
3. 新しい **ログ記録**オプションを指定します。プロトコル トラフィックをレポートに表示したり、プロトコル使用状況アラートを有効にするためには、プロトコル トラフィックをログ記録しなければなりません。
4. **Bandwidth Optimizer** を使用してこのプロトコルへのアクセスを管理するかどうかを指定します。詳細は、*Bandwidth Optimizer による帯域幅の管理、342 ページ*を参照してください。

重要
ここで行った変更は、**[すべてブロック]** および **[すべて許可]** を除いて、既存のすべてのプロトコル フィルタに影響を及ぼします。

5. 変更を完了したら、**[OK]** をクリックして、[プロトコルの編集] ページに戻ります（*カスタム プロトコルの編集、337 ページ*を参照）。変更をキャッシュするために、[Edit Protocols] ページでも **[OK]** をクリックする必要があります。

カスタム プロトコルの作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *プロトコルの使用、335 ページ*
- *プロトコルベースのポリシーの実施、336 ページ*
- *カスタム プロトコルの編集、337 ページ*
- *Websense によって定義されたプロトコルへの追加、342 ページ*

[Filter Components] > [Protocols] > [Add Protocol] ページで、新しいカスタム プロトコルを定義します。

1. プロトコルの**名前**を入力します。

   名前には下記の文字を含めることはできません。

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   元のプロトコルに割り当てられている IP アドレスまたはポートの数を拡張するために、カスタム プロトコルに Websense 定義プロトコルと同じ名前を割り当てることができます。詳細は、*Websense によって定義されたプロトコルへの追加、342 ページ*を参照してください。

2. **[Add protocol to this group（このグループにプロトコルを追加）]** ドロップダウンリストを展開して、プロトコル グループを選択します。新しいプロトコルが、すべてのプロトコル リストおよびフィルタで、このグループの中に表示されます。

3. このグループに一意な**プロトコル ID**（**ポート**、**IP アドレス**および**トランスポート方法**のセット）を定義します。あとで [Edit Protocols] ページから追加の ID を追加できます。

   プロトコル ID を作成するには、以下の手順を実行します。

   - 各プロトコル定義の 1 つ以上の基準（ポート、IP アドレス、またはトランスポート タイプ）が一意でなければなりません。

- **[All Ports（すべてのポート）]** または **[All external IP addresses（すべての外部 IP アドレス）]** を選択すると、この基準は他のプロトコル定義に入力する他のポートまたは IP アドレスと重複することになります。
- ポート範囲または IP アドレス範囲に重複があれば、それは一意とはみなされません。たとえば、ポート範囲 80-6000 は、範囲 4000-9000 と重複します。

> **注意**
>
> ポート 80 またはポート 8080 でプロトコルを指定するとき注意が必要です。Network Agent はこれらのポートを通じてインターネット要求をリッスンします。（Websense Web Security Gateway 環境においては、Network Agent がこれらのポートを無視するように設定することができます。）
>
> カスタム プロトコルは Websense プロトコルに優先しますから、ポート 80 を使用するカスタム プロトコルを定義すると、ポート 80 を使用する他のすべてのプロトコルはフィルタされ、カスタム プロトコルと同じようにログ記録されます。

下の表は、有効なプロトコル定義と無効なプロトコル定義の例を示しています。

ポート	IP アドレス	トランスポート方法	有効 / 無効
70	任意	TCP	有効 - ポート番号が一意なので、各プロトコル ID は一意です。
90	任意	TCP	

ポート	IP アドレス	トランスポート方法	有効 / 無効
70	任意	TCP	無効 - IP アドレスが一意ではありません。[10.2.1.201] は [ANY（任意）] セットに含まれます。
70	10.2.1.201	TCP	

ポート	IP アドレス	トランスポート方法	有効 / 無効
70	10.2.3.212	TCP	有効 - IP アドレスが一意です。
70	10.2.1.201	TCP	

4. [Default Filtering Action（デフォルトのフィルタリング アクション）] で、すべてのアクティブ プロトコル フィルタでこのプロトコルに適用するデフォルト アクション（**[許可]** または **[ブロック]**）を指定します。
   - このプロトコルを使用しているトラフィックを**ログ記録するかどうか**を指定します。プロトコル トラフィックをレポートに表示したり、プロトコル使用状況アラートを有効にするためには、プロトコル トラフィックをログ記録しなければなりません。
   - **Bandwidth Optimizer** によってこのプロトコルへのアクセスを制限するかどうかを指定します（*Bandwidth Optimizer による帯域幅の管理*、342 ページを参照）。
5. 完了したら、**[OK]** をクリックして、[Edit Protocols] ページに戻ります。プロトコル リストに新しいプロトコル定義が表示されます。
6. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

Websense によって定義されたプロトコルへの追加

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense によって定義されたプロトコルにポート番号または IP アドレスを直接に追加することはできません。しかし、Websense によって定義されたプロトコルと同じ名前のカスタム プロトコルを作成し、その定義にポート番号または IP アドレスを直接に追加することは可能です。

カスタム プロトコルと Websense によって定義されたプロトコルが同じ名前である場合、Websense ソフトウェアは両方の定義の中で指定されているポートと IP アドレスでのポート トラフィックを見つけます。

レポートではカスタム プロトコルの名前には接頭語 [C_] が付けられます。たとえば、SQL_NET のカスタム プロトコルを作成し、追加のポート番号を指定した場合、プロトコルでカスタム プロトコルの中のポート番号が使用されたときレポートには C_SQL_NET と表示されます。

Bandwidth Optimizer による帯域幅の管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリの使用*、322 ページ
- *プロトコルの使用*、335 ページ
- *デフォルトの Bandwidth Optimizer 制限の設定*、344 ページ

カテゴリまたはプロトコル フィルタを作成するとき、次のように、帯域幅の使用量を基にカテゴリまたはプロトコルへのアクセスを制限することを指定できます。

- 合計のネットワーク帯域幅使用量を基にカテゴリまたはプロトコルへのアクセスをブロックする。
- HTTP トラフィックによる合計の帯域幅使用量を基にカテゴリへのアクセスをブロックする。
- 特定のプロトコルによる帯域幅使用量を基にそのプロトコルへのアクセスをブロックする。

注意

Websense Web Security Gateway Anywhere では、ハイブリッド サービスは帯域幅ベースの制限を適用しません。

例：

- 合計のネットワーク帯域幅使用量が利用可能な帯域幅の 50% を超えるか、または現在の AOL Instant Messenger（AIM）による帯域幅使用量が合計のネットワーク帯域幅の 10% を超える場合に、AIM プロトコルをブロックします。
- 合計のネットワーク帯域幅使用量が 75% に達したか、またはすべての HTTP トラフィックによる帯域幅使用量が利用可能なネットワーク帯域幅の 60% を超える場合に、[スポーツ] カテゴリをブロックします。

プロトコル帯域幅使用量には、そのプロトコルのために定義されているすべてのポート、IP アドレス、または署名を通じたトラフィックが含まれます。つまり、プロトコルまたはインターネット アプリケーションがデータ転送に複数のポートを使用する場合、プロトコル定義に含まれているすべてのポートを通るトラフィックが、そのプロトコルの合計の帯域幅使用量にカウントされます。しかし、インターネット アプリケーションが使用するポートがプロトコル定義に含まれていない場合、そのポートを通るトラフィックは帯域幅使用量の計算には含まれません。

Websense ソフトウェアは、フィルタリングされた TCP および UDP ベースのプロトコルを記録します。

Websense, Inc., は、帯域幅の計算の正確さを保証するために、Websense プロトコルの定義を定期的に更新します。

Network Agent は、事前定義された間隔で、ネットワーク帯域幅データを Filtering Service に送信します。これによって Websense ソフトウェアが帯域幅使用量を正確にモニタし、平均に最も近い測定値を受け取ることが保証されます。

Websense Web Security Gateway *トンネリング プロトコルの検出、235 ページ*）環境では、Content Gateway は、FTP、HTTP、および（有効化されている場合）HTTP 上をトンネリングするプロトコルの帯域幅に関する情報を収集します。測定とレポートは Network Agent で使用する方法と同じです。Bandwidth Optimizer の設定で、プロトコルに対する帯域幅ベースのポリシーの実施を決定するためにこのデータを使用することを指定できます。

1. Web Security manager で、**[Settings] > [General] > [Filtering]** を順に選択します。
2. **[Bandwidth Monitoring（帯域幅モニタリング）]** チェック ボックスを選択します。
3. 完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

帯域幅オプションがアクティブのとき、実施は初期設定の 10 分後、および各 Websense Policy Server 再起動の 10 分後に開始します。この遅延によって、帯域幅データの正確な計算が確保されます。

要求が帯域幅制限に基づきブロックされると、Websense ブロック・ページの **[Reason]** フィールドにこの情報が表示されます。詳細については、*ブロック ページ、143 ページ*を参照してください。

デフォルトの Bandwidth Optimizer 制限の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリ フィルタの編集、73 ページ*
- *プロトコル フィルタの編集、77 ページ*
- *Bandwidth Optimizer による帯域幅の管理、342 ページ*

ポリシーの中で帯域幅設定を指定する前に、帯域幅ベースの実施をトリガするデフォルトの帯域幅しきい値を確認します。

- ネットワークのデフォルト帯域幅：**50%**
- プロトコル別のデフォルト帯域幅：**20%**

デフォルト帯域幅は Policy Server に よって保存され、Network Agent のすべての関連するインスタンスに適用されます。複数の Policy Server がある場合、1 つの Policy Server 上でのデフォルト帯域幅の変更は他の Policy Server には影響を及ぼしません。

デフォルト帯域幅の値を変更するには、以下の手順を実行します。

1. Web Security manager で、**[Settings] > [General] > [Filtering]** を順に選択します。
2. 帯域幅ベースの実施を有効にしている場合、それをトリガする帯域幅使用量しきい値を入力します。
   - ネットワーク全体のトラフィックを基にカテゴリまたはプロトコルをブロックするとき、**[Default bandwidth for network（ネットワークのデフォルト帯域幅）]** でデフォルトのしきい値を定義します。
   - プロトコルのトラフィックを基にカテゴリまたはプロトコルをブロックするとき、**[Default bandwidth per protocol（プロトコル別のデフォルト帯域幅）]** でデフォルトのしきい値を定義します。

   どのカテゴリまたはプロトコル フィルタでも、各カテゴリまたはプロトコルのデフォルトのしきい値を無効にすることができます。
3. 完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

デフォルトの変更は、Bandwidth Optimizer 制限を適用するすべてのカテゴリおよびプロトコル フィルタに影響を及ぼす可能性があります。

- 特定のプロトコルに関連する帯域幅使用量を管理するには、アクティブ プロトコル フィルタ（1 つまたは複数）を編集します。
- 特定の URL カテゴリに関連する帯域幅使用量を管理するには、該当するカテゴリ フィルタ（1 つまたは複数）を編集します。

  HTTP 帯域幅使用量を基にカテゴリをフィルタリングするとき、Websense ソフトウェアは Websense ソフトウェア用に HTTP ポートとして指定されているすべてのポートでの合計の HTTP 帯域幅使用量を測定します。

ファイル タイプに基づくトラフィックの管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ファイル拡張子に基づく実施、347 ページ*
- *ファイルの解析に基づく実施、350 ページ*
- *ファイル タイプ定義の使用、352 ページ*
- *カスタム ファイル タイプの追加、353 ページ*
- *ファイル タイプへのファイル拡張子の追加、354 ページ*

カテゴリ フィルタを作成または編集する時、許可されているカテゴリに対してファイル タイプ ブロックを設定することができます。これによって組織は、一部またはすべての許可されているカテゴリのウェブサイト上の特定のファイル タイプへのアクセスを制限できます。たとえば、[スポーツ] カテゴリを許可するが、[スポーツ] カテゴリに含まれるサイトからのマルチメディア（オーディオおよびビデオ）をブロックするという設定が可能です。

ファイル タイプ ブロックの実施方法は、使用する Websense Web セキュリティ ソリューションによって異なります。

- Websense Web Filter および Websense Web Security（Content Gateway またはハイブリッド サービス プロキシがない）では、ファイル拡張子のみを基準にしてファイル タイプ ブロックを実施できます（*ファイル拡張子に基づく実施*、347 ページを参照）。

  例：

  1. [General Email] カテゴリがアクティブ カテゴリ フィルタで許可されていますが、このカテゴリの [圧縮ファイル] に対してファイル タイプ ブロックが有効化されています。
  2. エンド ユーザーが拡張子 .zip 拡張子が付いているファイル（例、[myfile.zip]）のダウンロードを試みます。
  3. このユーザーは、ファイル タイプによってダウンロードがブロックされたことを知らせるブロック ページを受け取ります。なぜなら、拡張子 [.zip] は [圧縮ファイル] ファイル タイプに関連付けられているからです。

- Websense Web Security Gateway および Gateway Anywhere（Content Gateway およびハイブリッド サービスを含んでいる）では、ファイル拡張子（*ファイル拡張子に基づく実施*、347 ページを参照）と 要求されているファイルの分析（*ファイルの解析に基づく実施*、350 ページを参照）の組み合わせを基にした 2 パートのファイル タイプ ブロックを導入できます。

  例：

  1. [General Email] カテゴリがアクティブ カテゴリ フィルタで許可されていますが、このカテゴリの [圧縮ファイル] に対してファイル タイプ ブロックが有効化されています。
  2. エンド ユーザーが拡張子 .zip 拡張子が付いているファイル（例、[myfile.zip]）のダウンロードを試みます。
  3. このユーザーは、ファイル タイプによってダウンロードがブロックされたことを知らせるブロック ページを受け取ります。なぜなら、拡張子 [.zip] は [圧縮ファイル] ファイル タイプに関連付けられているからです。
  4. ユーザーは電子メールから別のファイルのダウンロードを試みます。このファイルのファイル拡張子は未知です（例、[myfile.111]）。

5. ファイルをスキャンして、ファイル タイプを検出します。
   - 解析の結果、ファイルが圧縮ファイルであることが判明した場合、このユーザーは、ファイル タイプによってダウンロードがブロックされたことを知らせるブロック ページを受け取ります。
   - 解析の結果、ファイルが圧縮ファイルでないことが判明した場合、ダウンロード要求は許可されます。

インターネット オーディオおよびビデオ メディアをより適切に管理するには、プロトコルベースのポリシーの実施とファイル タイプの実施を組み合せます。プロトコル フィルタはストリーミング メディアを処理し、ファイル タイプの実施はダウンロードして再生できるファイルを処理します。

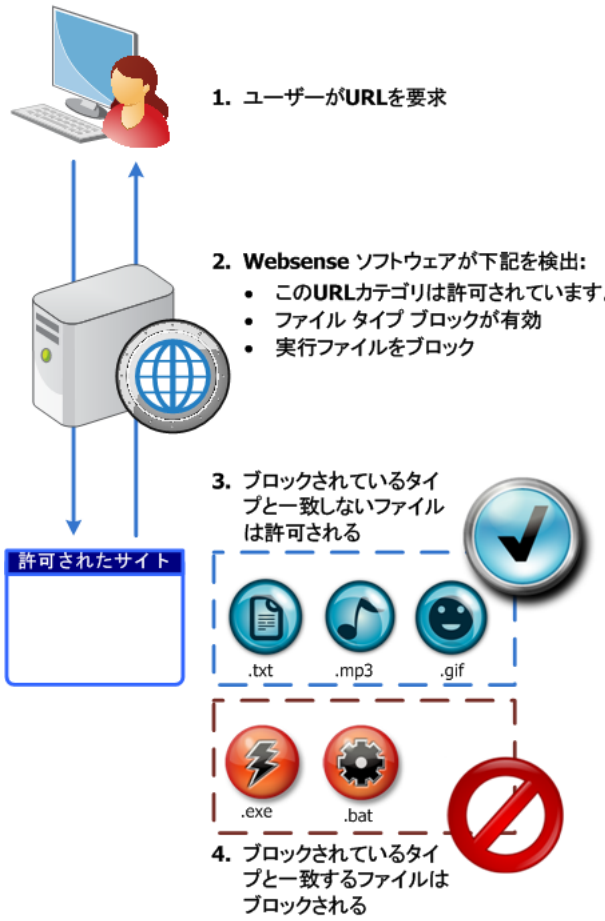
ファイル拡張子に基づく実施

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリ フィルタでのファイル タイプ ブロッキングの有効化、352 ページ*
- *ファイル タイプ定義の使用、352 ページ*
- *カスタム ファイル タイプの追加、353 ページ*
- *ファイル タイプへのファイル拡張子の追加、354 ページ*

ユーザーが要求した URL が許可されているカテゴリーにあり、そのカテゴリに対してファイル タイプによるブロックが有効化されている場合、Filtering Service はその URL に関連付けられているファイルをチェックし、ブロックされるファイル タイプに関連付けられているファイル拡張子が付いているファイルがあるかどうかをチェックします。そのようなファイルがある場合、要求はブロックされ、このユーザーは、ファイル タイプによって要求がブロックされたことを知らせるブロック ページを受け取ります。



どのファイルのファイル拡張子もブロックされるファイル タイプに関連付けられていない場合の処置は、使用している Web セキュリティ ソリューションによって異なります。

- *Websense Web Security* および *Web Filter*：ファイルは許可されます。
- *Websense Web Security Gateway* および *Gateway Anywhere*：ファイルの実際のファイル タイプを調べるために解析が行われ、解析結果に基づいて許可またはブロックされます（*ファイルの解析に基づく実施*、350 ページを参照）。

製品にはいくつかの事前定義されたファイル タイプ（ファイル拡張子のグループ）が含まれています。これらのファイル タイプ定義はマスタ データベースに保存され、マスタ データベースの更新プロセスの中で変更できます。

事前定義されたファイル タイプを使用してフィルタリングするか、既存のファイル タイプ定義を編集するか、新規のファイル タイプを作成することができます。ただし、Websense によって定義されたファイル タイプを削除したり、それに関連付けられているファイル拡張子を削除することはできません。

Websense によって定義されたファイル タイプに関連付けられているすべてのファイル拡張子は、カスタム ファイル タイプに追加できます。ファイル拡張子は次に、カスタム ファイル タイプに関連付けられている設定に従ってフィルタリングおよびログ記録されます。

ファイル タイプの定義には、実施のために利用できるファイル拡張子をいくつでも含めることができます。たとえば、事前定義済みのファイル タイプには、以下のファイル拡張子が含まれます。

ファイル タイプ	関連付けられている拡張子
圧縮ファイル：	.ace、.arc、.arj、.b64、.bhx、.cab、.gz、.gzip、.hqx、.iso、.jar、.lzh、.mim、.rar、tar、taz、.tgz、.tz、.uu、.uue、.xxe、.z、.zip
ドキュメント	.ade、.adp、.asd、.cwk、.doc、.docx、.dot、.dotm、.dotx、.grv、.iaf、.lit、.lwp、.maf、.mam、.maq、.mar、.mat、.mda、.mdb、.mde、.mdt、.mdw、.mpd、.mpp、.mpt、.msg、.oab、.obi、.oft、.olm、.one、.ops、.ost、.pa、.pdf、.pip、.pot、.potm、.potx、.ppa、.ppam、.pps、.ppsm、.ppsx、.ppt、.pptm、.pptx、.prf、.pst、.pub、.puz、.sldm、.sldx、.snp、.svd、.thmx、.vdx、.vsd、.vss、.vst、.vsx、.vtx、.wbk、.wks、.wll、.wri、.xar、.xl、.xla、.xlb、.xlc、.xll、.xlm、.xls、.xlsb、.xlsm、.xlsx、.xlt、.xltm、.xltx、.xlw、.xsf、.xsn
実行ファイル	.bat、.exe
画像	.bmp、.cmu、.djvu、.emf、.fbm、.fits、.gif、.icb、.ico、.jpeg、.jpg、.mgr、.miff、.pbf、.pbm、.pcx、.pdd、.pds、.pix、.png、.psb、.psd、.psp、.rle、.sgi、.sir、.targa、.tga、.tif、.tiff、.tpic、.vda、.vst、.zif
マルチメディア	.aif、.aifc、.aiff、.asf、.asx、.avi、.ivf、.m1v、.m3u、.mid、.midi、.mov、.mp2、.mp2v、.mp3、.mpa、.mpe、.mpg、.mpv2、.ogg、.qt、.ra、.ram、.rmi、.snd、.wav、.wax、.wm、.wma、.wmp、.wmv、.wmx、.wxv
Rich Internet Applications（リッチ インターネット アプリケーション）	.swf
テキスト	.htm、.html、.txt、.xht、.xhtml、.xml
Threats	.vbs、.wmf

ユーザーがサイトを要求した時、Websense ソフトウェアで以下のことが実行されます：

1. その URL カテゴリを特定します。
2. ファイル拡張子を調べます。
3. （*Websense Web Security Gateway* および *Gateway Anywhere*）拡張子によってブロックされない場合は、ファイルの実際のファイル タイプを調べるために解析を行います。

注意

1 つのユーザー要求に対して複数のグループ ポリシーが適用可能であれば、ファイル タイプ ブロックは実行できません。

ユーザーがブロックされているファイル タイプにアクセスしようとしたとき、Websense ブロック ページの **[Reason]** フィールドにそのファイル タイプがブロックされていることが示されます（*ブロック ページ、143 ページ*を参照）。

ブロックされたイメージが許可されているページの一部である場合、標準のブロック ページは表示されません。代わりに、イメージ領域が空白になります。それによって、イメージを除いて許可されているページの複数の場所にブロック ページの小さな部分が表示されるのを防止しています。

既存のファイル タイプ定義を表示したり、ファイル タイプを編集したり、拡張子による適用のためのカスタム ファイル タイプを作成するには、**[Policy Management] > [Filter Components（フィルタ コンポーネント）]** を選択し、**[File Types]** をクリックします。詳細は、*ファイル タイプ定義の使用、352 ページ*を参照してください。

ファイル タイプ ブロッキングを有効化する方法については、*カテゴリ フィルタでのファイル タイプ ブロッキングの有効化、352 ページ*を参照してください。

ファイルの解析に基づく実施

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリ フィルタでのファイル タイプ ブロッキングの有効化、352 ページ*
- *セキュリティの脅威：ファイル分析、237 ページ*

ユーザー トラフィックが Websense Content Gateway またはハイブリッド サービスを通過する時、下記のすべての条件が真である場合、要求されたファイルの実際のファイル タイプを調べるために解析が行われます。

1. ユーザーが要求している URL が [許可されている] カテゴリに含まれる。
2. アクティブ カテゴリ フィルタの中のカテゴリにファイル タイプ ブロックが有効化されている。
3. ブロックされているファイル タイプの中に一致するファイル拡張子がない（*ファイル拡張子に基づく実施、347 ページ*を参照）。

この場合、ポリシーの実施のために戻されるファイル タイプは、拡張子に関わりなく、同種のファイルの目的または動作を記述します。したがって、実行ファイルに [.txt] や他の無意味なファイル拡張子を付けることによってその性質を隠す試みはファイル タイプの解析によって防止されます。

ファイル タイプ定義は解析データベースに保存され、Content Gateway データベースまたはハイブリッド サービスの更新プロセスの中で変更できます。

ファイル解析によって、下記のファイル タイプが識別されます。

ファイル タイプ	説明
圧縮ファイル：	使用するスペースを節約するためにパッケージ化されたファイル。例、ZIP、RAR、JAR アーカイブ。
ドキュメント	バイナリ形式のドキュメント。例、DOCX、PDF。
実行ファイル	コンピュータ上で実行できるプログラム。例、EXE、BAT ファイル。
画像	画像形式。例、JPG、BMP、GIF。
マルチメディア	オーディオ ビジュアル形式。例、MP3、WMV、MOV。
リッチ インターネット アプリケーション	ブラウザ内で実行する Web アプリケーション。例、Flash。
テキスト	形式のないテキスト データ。例 HTML、TXT ファイル。
脅威	コンピュータやネットワークに危害を及ぶす可能性がある悪意のあるアプリケーション。例、スパイウェア、ワーム、ウィルス。

ユーザーがサイトを要求したとき、Websense Web Security Gateway ソリューションは最初にサイト カテゴリを判断し、次に、フィルタリングされるファイル タイプをチェックします（最初に拡張子によって、次に解析によって）。

注意

1 つのユーザー要求に対して複数のグループ ポリシーが適用可能であれば、ファイル タイプ ブロックは実行できません。

ユーザーがブロックされているファイル タイプにアクセスしようとしたとき、Websense ブロック ページの **[Reason]** フィールドにそのファイル タイプがブロックされていることが示されます（ブロック ページ、143 ページを参照）。

ブロックされたイメージが許可されているページの一部である場合、標準のブロック ページは表示されません。代わりに、イメージ領域が空白になります。それによって、イメージを除いて許可されているページの複数の場所にブロック ページの小さな部分が表示されるのを防止しています。

ファイル タイプの既存の拡張子を表示したり、ファイル タイプを編集したり、拡張子による実施のためのカスタム ファイル タイプを作成するには、**[Policy Management] > [Filter Components]** を選択し、**[File Types]** をクリックします。詳細は、*ファイル タイプ定義の使用、352 ページ*を参照してください。

ファイル タイプ ブロッキングを有効化する方法については、*カテゴリ フィルタでのファイル タイプ ブロッキングの有効化、352 ページ*を参照してください。

カテゴリ フィルタでのファイル タイプ ブロッキングの有効化

Web Security Help | Web Security ソリューション | バージョン 7.8.x

通常は許可されているカテゴリの中の一部のファイル タイプへのアクセスを禁止するには、以下の手順を実行します。

1. **[Policy Management] > [Filters]** ページに移動し、カテゴリ フィルタ名をクリックします。

   カテゴリ フィルタをポリシー内からも編集できます。
2. **[Categories]** リストでカテゴリを選択します。
3. ページ右側の [Advanced Filtering] の下の **[Block file types（ファイル タイプをブロック）]** チェック ボックスをオンにします。

   ファイル タイプのリストが表示されます。
4. チェック ボックスを使ってブロックするファイル タイプ（1 つまたは複数）を選択します。
5. このカテゴリ フィルタによって許可されているすべてのカテゴリの中で選択したファイル タイプをブロックする場合、**[Apply to All Categories（すべてのカテゴリに適用）]** をクリックします。
6. **[OK]**、**[Save and Deploy]** をクリックして、変更を適用します。

ファイル タイプ定義の使用

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ファイル タイプに基づくトラフィックの管理、345 ページ*
- *カテゴリ フィルタの編集、73 ページ*
- *URL 要求への応答、122 ページ*

[Policy Management] > [Filter Components] > [Edit] [File Types] ページを使用して、カテゴリ フィルタ内で明示的にブロックできる最大 32 のファイル タイプ（ファイル拡張子のグループ）を作成および管理できます（ *ファイル タイプに基づくトラフィックの管理、345 ページ*を参照）。

> **重要**
> カスタム ファイル タイプおよび事前定義されているタイプへのカスタム追加は、拡張子ベースの実施では使用しますが、Websense Web Security Gateway や Gateway Anywhere での実際のファイル タイプの分析では使用しません。詳細については、*ファイル拡張子に基づく実施、347 ページ*と *ファイルの解析に基づく実施、350 ページ*を参照してください。

- ファイル タイプをクリックすると、そのファイル タイプに関連付けられたファイル拡張子が表示されます。
- 選択したファイル タイプに拡張子を追加するには、**[Add Extension]** をクリックし、次に *ファイル タイプへのファイル拡張子の追加、354 ページ* の指示に従います。
- 新規ファイル タイプを作成するには、**[Add File Type]** をクリックし、次に *カスタム ファイル タイプの追加、353 ページ*の指示に従います。
- カスタム ファイル タイプまたは拡張子を削除するには、項目を選択し、**[Delete]** をクリックします。

  Websense によって定義されたファイル タイプを削除したり、それに関連付けられているファイル拡張子を削除することはできません。

  しかし、Websense によって定義されたファイル タイプに関連付けられているファイル拡張子をカスタム ファイル タイプに追加することは可能です。ファイル拡張子は次に、カスタム ファイル タイプに関連付けられている設定に従ってフィルタリングおよびログ記録されます。同じ拡張子を複数のカスタム ファイル タイプに追加することはできません。

ファイル タイプの定義の変更を完了したら。**[OK]** をクリックします。**[Save and Deploy]** をクリックするまで変更は適用されません。

カスタム ファイル タイプの追加

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Filter Components] > [Edit File Types（ファイル タイプの編集）] > [Add File Type（ファイル タイプの追加）] ページを使用して、カスタム ファイル タイプを定義します。

重要
カスタム ファイル タイプおよび事前定義されているタイプへのカスタム追加は、拡張子ベースの実施では使用しますが、Websense Web Security Gateway や Gateway Anywhere での実際のファイル タイプの分析では使用しません。詳細については、*ファイル拡張子に基づく実施、347 ページ*と*ファイルの解析に基づく実施、350 ページ*を参照してください。

1. 一意な**ファイル タイプ名**を入力します。

   Websense によって定義されたファイル タイプと同じ名前のカスタム ファイル タイプを作成することによって、既存のファイル タイプに追加のファイル拡張子を追加できます。
2. **ファイル拡張子**のリストにファイル拡張子を、1 行に 1 つ入力します。各拡張子の前にドット（[.]）を入力する必要はありません。
3. **[OK]** をクリックして、[Edit File Types] 画面に戻ります。新しいファイル タイプがファイル タイプのリストに表示されます。
4. ファイル タイプの定義の処理が完了したら、[Edit File Types] ページで **[OK]** をクリックします。**[Save and Deploy]** をクリックするまで変更は適用されません。

ファイル タイプへのファイル拡張子の追加

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Filter Components] > [Edit File Types] > [Add File Extensions（ファイル拡張子の追加）] ページを使用して、選択したファイル タイプにファイル拡張子を追加します。

重要
カスタム ファイル タイプおよび事前定義されているタイプへのカスタム追加は、拡張子ベースの実施では使用しますが、Websense Web Security Gateway や Gateway Anywhere での実際のファイル タイプの分析では使用しません。詳細については、*ファイル拡張子に基づく実施、347 ページ*と*ファイルの解析に基づく実施、350 ページ*を参照してください。

1. **[Selected file type（選択したファイル タイプ）]** の横に希望するファイル タイプ名が表示されていることを確認します。

2. **ファイル拡張子**のリストにファイル拡張子を、1 行に 1 つ入力します。各拡張子の前にドット（[.]）を入力する必要はありません。
3. **[OK]** をクリックして、[Edit File Types] 画面に戻ります。新しいファイル拡張子がカスタム ファイル拡張子のリストに表示されます。
4. ファイル タイプの定義の処理が完了したら、[Edit File Types] ページで **[OK]** をクリックします。**[Save and Deploy]** をクリックするまで変更は適用されません。

正規表現の使用

Web Security Help | Web Security ソリューション | バージョン 7.8.x

正規表現とは複数の文字列、または文字のグループとの一致を検出するために使用するテンプレートまたはパターンです。制限付きアクセス フィルタで正規表現を使用することができ、また、正規表現を使用してカスタム URL またはキーワードを定義することができます。次に Filtering Service は、特定の単一の URL またはキーワードではなく、一般的なパターンとの一致を検出しようとします。

次の単純な正規表現を見てみましょう。

```
domain.(com|org|net)
```

この式のパターンは次の URL と一致します。

- domain.com
- domain.org
- domain.net

正規表現を使用するときは注意が必要です。正規表現は強力なツールですが、想定していないサイトをブロックまたは許可してしまうことがあります。また、煩雑な正規表現は、オーバーヘッドを過度に大きくします。

重要

正規表現をポリシーの実施基準として使用すると、CPU 使用量が増える可能性があります。テストの結果として、100 の正規表現を使用した場合に Filtering Service がインストールされているコンピュータの CPU 使用量が 20% 増えることが示されています。

キーワードの場合と同様に、正規表現に ASCII 以外の文字が含まれる場合、正規表現は URL のパスおよびクエリ文字列とだけ照合され、ドメイン部分（[www.domain.com/**path?query**]）とは照合されません。

Websense ソフトウェアは、2 つの例外を除いて、大部分の Perl 正規表現構文をサポートします。サポートされていない構文は、URL の中で検出される可能性がある文字列との一致を見つけるために役に立ちません。

次のような正規表現構文はサポートされません。

```
(?{code})
??{code})
```

正規表現の詳細については、下記を参照してください。

en.wikipedia.org/wiki/Regular_expression

www.regular-expressions.info/

ツールボックスによるポリシーの実施動作の確認

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Web Security manager の右側のショートカット ペインの**ツールボックス**を使用して、ポリシーのセットアップをすばやくチェックできます。

ツールにアクセスするには、ツール名をクリックします。名前をもう一度クリックすると、ツールのリストが表示されます。ツールの使用の詳細については、下記を参照してください。

- *URL カテゴリ*、356 ページ
- *ポリシーの確認*、357 ページ
- *フィルタリングのテスト*、357 ページ
- *URL アクセス*、358 ページ
- *ユーザーの調査*、358 ページ

また、**[Support Portal（サポート ポータル）]** をクリックすると、新しいブラウザ タブまたはウィンドウに Websense Technical Support のウェブサイトが表示されます。サポート ポータルから、Knowledge Base を検索して関連記事、ヒント、チュートリアル、ビデオ、製品マニュアルにアクセスすることができます。

URL カテゴリ

Web Security Help | Web Security ソリューション | バージョン 7.8.x

サイトが現在どのカテゴリに分類されているかを調べるには、以下の手順を実行します。

1. ツールボックスで **[URL Category（URL カテゴリ）]** をクリックします。
2. URL または IP アドレスを入力します。
3. **[Go]** をクリックします。

ポップアップ ウィンドウにサイトの現在のカテゴリが表示されます。URL が分類変更された場合は、新しいカテゴリが表示されます。

サイトの分類は、使用しているマスタ データベースのバージョン（リアルタイム更新を含む）によって異なることがあります。

ポリシーの確認

Web Security Help | Web Security ソリューション | バージョン 7.8.x

このツールを使用して特定のクライアントにどのポリシーが適用されるかを判断できます。結果は現在の日付および時刻にのみ対応します。

1. ツールボックスの **[Check Policy]** をクリックします。
2. ディレクトリまたはコンピュータ クライアントを識別するために、以下のいずれかを入力します。
   - 完全修飾ユーザ名

     ディレクトリを参照または検索してユーザを識別するには、**[Find User（ユーザーの検索）]** をクリックします（*ポリシーの確認またはフィルタリング テストの対象のユーザーの指定、359 ページ*を参照）。
   - IP アドレス
3. **[Go]** をクリックします。

1 つ以上のポリシーの名前がポップアップ ウィンドウに表示されます。複数のポリシーが表示されるのは、ユーザーに割り当てられているポリシーがなく、ユーザーが属している複数のグループ、ドメイン、組織単位にポリシーが割り当てられている場合だけです。

複数のポリシーが表示される場合でも、特定の時点でユーザに適用されるポリシーは 1 つだけです（*適用順序、119 ページ*を参照）。

フィルタリングのテスト

Web Security Help | Web Security ソリューション | バージョン 7.8.x

特定のクライアントが特定のサイトを要求したときにどうなるかを調べるには、以下の手順を実行します。

1. ツールボックスで **[Test Filtering（フィルタリングのテスト）]** をクリックします。
2. ディレクトリまたはコンピュータ クライアントを識別するために、以下のいずれかを入力します。
   - 完全修飾ユーザ名

     ディレクトリを参照または検索してユーザを識別するには、**[Find User（ユーザーの検索）]** をクリックします（*ポリシーの確認またはフィルタリング テストの対象のユーザーの指定、359 ページ*を参照）。
   - IP アドレス

3. 調べたいサイトの URL または IP アドレスを入力します。
4. **[Go]** をクリックします。

サイト カテゴリ、カテゴリに適用されるアクション、アクションの理由がポップアップ ウィンドウに表示されます。

URL アクセス

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ユーザーが過去 2 週間の間（今日を含む）にサイトをアクセスしたかどうかを調べるには、以下の手順を実行します。

1. ツールボックスで **[URL Access（URL アクセス）]** をクリックします。
2. 調べたいサイトの URL または IP アドレスまたはその一部を入力します。
3. **[Go]** をクリックします。

調査レポートに、サイトがアクセスされたかどうか、アクセスされた場合はいつかアクセスされたかが示されます。

セキュリティ アラートを受け取ってから、このツールを使用して、お客様の組織がフィッシングまたはウィルス感染サイトに曝されたかどうかについて調べることができます。

ユーザーの調査

Web Security Help | Web Security ソリューション | バージョン 7.8.x

過去 2 週間（今日を除く）のクライアントのインターネット使用状況の履歴を調べるには、以下の手順を実行します。

1. ツールボックスで **[Investigate User（ユーザーの調査）]** をクリックします。
2. ユーザー識別が設定されている場合はユーザー名のすべてまたは一部を入力し、ユーザーが識別されないコンピュータの場合は IP アドレスを入力します。

   IP アドレス検索では、ユーザー名がログにない IP アドレスだけが検索結果として表示されます。
3. **[Go]** をクリックします。

当該クライアントの使用履歴を示す調査レポートが表示されます。

ポリシーの確認またはフィルタリング テストの対象のユーザーの指定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Find User（ユーザーの検索）] ページを使用して、Check Policy または Test Filtering ツールの対象となるユーザー（ディレクトリ）クライアントを指定します。

ページが開かれ、**[User]** オプションが選択された状態になっています。**Directory Entries** フォルダを展開してディレクトリを参照するか、または **[検索]** をクリックします。検索機能は、LDAP ベースのディレクトリ サービスを使用している場合のみ利用できます。

ディレクトリを検索してユーザーを見つけるには、以下の手順を実行します。

1. **ユーザー名**またはその一部を入力します。
2. **Directory Entries** ツリーを展開して、検索コンテクストを参照します。

   コンテクストを指定するには、ツリーの中のフォルダ（DC、OU または CN）をクリックしなければなりません。このとき、フィールドがツリーの下に表示されます。
3. **[Search]** をクリックします。検索条件に一致するエントリが **[Search Results（検索結果）]** の下にリストされます。
4. ユーザー名をクリックしてユーザーを選択するか、または **[Search Again（再検索）]** をクリックして新しい検索条件またはコンテクストを入力します。

   [Cancel Search（検索のキャンセル）] をクリックすると、ディレクトリの参照に戻ります。
5. 正しい完全修飾ユーザー名が **[User]** フィールドに表示されたとき、**[Go]** をクリックします。

Test Filtering ツールを使用している場合、**[Go]** をクリックする前に、**[URL]** フィールドに URL または IP アドレスが表示されていることを確認してください。

ユーザーではなくコンピュータ クライアントを指定する場合は、**[IP address]** をクリックします。

14 ユーザーの識別

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ポリシーをユーザーおよびグループに適用するために、Websense ソフトウェアは、要求元の IP アドレスから、要求を発行したユーザーを識別できる必要があります。種々の識別方法が利用できます：

- 統合デバイスまたはアプリケーションがユーザーを識別および認証し、Websense ソフトウェアにユーザー情報を渡します。詳細については、[Deployment and Installation Center] を参照してください。
- Websense 透過的識別エージェントはバックグラウンドで動作して、ディレクトリ サービスと通信し、ユーザーを識別します（*透過的識別*を参照）。
- Websense ソフトウェアは、ユーザーが Web ブラウザを開くときに、ネットワーク資格情報の入力を促し、ログオンを要求します（*手動認証、363 ページ*を参照）。

Websense Web Security Gateway Anywhere 環境では、ハイブリッド サービスも同様に、ユーザーまたはグループ ベースのポリシーを適用するために、ユーザーを識別できなければなりません。これは User Service または透過的識別エージェントによって提供される情報を使用しません。代わりに、下記の方法を利用できます。

- Websense Directory Agent という名前のコンポーネントは、ユーザーを識別するために使用する情報を収集します（*ハイブリッド ユーザーの識別、391 ページ*を参照）。
- Websense Web Endpoint はクライアント コンピュータ上にインストールされ、透過的認証を提供し、ハイブリッド サービスの使用を強制し、認証の詳細をハイブリッド サービスに渡します。

透過的識別

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *手動認証*、363 ページ
- *ユーザー識別方法の設定*、364 ページ

一般に、**透過的識別**とは、Websense ソフトウェアがログオン情報の入力を促すことなくディレクトリ サービスでユーザーを識別するために使用する方法を言います。これには、Web Security ソリューションにユーザー情報を提供するデバイスまたはアプリケーションを統合する方法や、オプションの Websense 透過的識別エージェントを使用する方法が含まれます。

- Websense *DC Agent*、373 ページは Windows ベースのディレクトリ サービスで使用されます。エージェントは定期的にユーザー ログオン セッションをドメイン コントローラにクエリし、ログオン ステータスを確認するためにクライアント コンピュータを調査します。それは、Windows サーバー上で動作し、ネットワークのどのドメインにでもインストールすることができます。
- Websense *Logon Agent*、380 ページは、Windows ドメインにログインするユーザーを透過的に識別します。エージェントは、Linux または Windows サーバー上で動作し、その連携するログオン アプリケーションは、Windows または Mac クライアント上で動作します。
- Websense *RADIUS Agent*、383 ページは、Windows または LDAP ベースのディレクトリ サービスと共に使用することができます。リモートの場所からユーザがログオンすることを識別するために、エージェントは RADIUS サーバーとクライアントと共に動作します。
- Websense *eDirectory Agent*、385 ページは Novell eDirectory で使用されます。エージェントは、Novell eDirectory 認証をユーザを IP アドレスにマップするために使用します。

各エージェントのインストール方法については、Deployment and Installation Center を参照してください。エージェントは、単独または特定の組み合わせで使用することができます。

Web Security manager では、一般のユーザー識別の設定と特定の透過的識別エージェントの両方が設定されます。**[Settings（設定）] > [General（一般）] > [User Identification（ユーザー識別）]** ページに移動します。

詳細な設定方法は、*ユーザー識別方法の設定*、364 ページを参照してください。

場合によっては、透過的識別エージェントは、他のコンポーネントに正しいユーザー情報を提供できないことがあります。これは、1 人以上のユーザーが同じコンピュータに割り当てられている、ユーザーが匿名ユーザーまたは

ゲストである、もしくは他の理由で起こります。そのような場合、ユーザーにブラウザを通じてログオンするよう促すことができます（*手動認証*、363 ページを参照）。

リモート ユーザーの透過的識別

Web Security Help | Web Security ソリューション | バージョン 7.8.x

特定の設定では、Websense ソフトウェアは、リモートの場所からネットワーク上にログオンするユーザーを透過的に識別することができます：

- Websense Remote Filtering Server と Remote Filtering Client を配備している場合、Websense ソフトウェアはドメイン アカウントを使用してキャッシュされたドメインにログオンするすべてのオフサイト ユーザーを識別することができます。詳細については、*オフサイト ユーザーの管理*、303 ページを参照してください。
- DC Agent を配備していて、リモート ユーザーがネットワーク上の指定された Windows ドメインに直接ログオンするとき、DC Agent は これらのユーザを識別することができます（*DC Agent*、373 ページを参照）。
- リモートの場所からログオンするユーザーを認証するために RADIUS サーバーを使用している場合、RADIUS Agent が透過的にそれらのユーザーを識別できますから、ユーザーまたはグループに基づくポリシーを適用することができます（*RADIUS Agent*、383 ページを参照）。

手動認証

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *透過的識別*、362 ページ
- *特定のコンピュータの認証ルールの設定*、366 ページ
- *セキュア手動認証*、369 ページ
- *ユーザー識別方法の設定*、364 ページ

環境によっては透過的識別が利用できない、または利用することが望ましくない場合もあります。透過的識別を使用しない組織や、透過的識別が利用可能でない場合でも、**手動認証**を使用してユーザーおよびグループ ベースのポリシーに基づくフィルタリングを行うことができます。

手動認証では、ユーザーが初めてブラウザを介してインターネットにアクセスするときに、ユーザー名とパスワードを入力するよう促します。Websense ソフトウェアは、サポートされるディレクトリ サービスでパスワードを確認し、そのユーザーのポリシー情報を検索します。

透過的識別が使用できない時に常に手動認証を有効化するように Websense ソフトウェアを設定できます（*ユーザー識別方法の設定、364 ページ*および*ハイブリッド サービスへのユーザーのアクセスの設定、272 ページ*を参照）。

また、カスタム認証設定によって、ユーザーがブラウザを開いた時にログオンを促される特定のコンピューターのリストを作成することもできます（*特定のコンピュータの認証ルールの設定、366 ページ*を参照）。

手動認証が有効化されている時、下記の場合にユーザーは HTTP エラーを受信し インターネットにアクセスできないことがあります。

- パスワードの入力に 3 回失敗した。これはユーザー名またはパスワードが無効であるときに起こります。
- 認証要求を回避するために **[Cancel]** をクリックした。

手動認証が有効な場合、識別できないユーザは インターネットをブラウズできません。

ユーザー識別方法の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *透過的識別、362 ページ*
- *手動認証、363 ページ*
- *ユーザーおよびグループの処理、92 ページ*

[Settings] > [General] > [User Identification] ページで、Websense ソフトウェアがユーザーおよびグループ ベースのポリシーを適用するために、いつ、どのようにネットワークのユーザーを識別するかを管理します。

- Policy Server が透過的識別エージェントと通信するよう設定します。
- 透過的識別エージェントの設定を確認し、更新します。
- 透過的識別エージェントまたは統合デバイスによってユーザーを識別することができないときに、Websense ソフトウェアが、どのように応答するか決定するために、グローバル ルールを設定します。
- グローバル ユーザー識別ルールが適用されないネットワーク上のコンピュータを指定し、それらのコンピュータのユーザーが認証されるべきか、どのように認証されるべきかを指定します。

Websense 透過的識別エージェントを使用している場合、エージェントは **[Transparent Identification Agents（透過的識別エージェント）]** にリストされます：

- **[Server（サーバー）]** に、透過的識別エージェントをホストするコンピュータの IP アドレスまたは名前が表示されます。
- **[Port（ポート）]** に、Websense ソフトウェアがエージェントと通信するために使用するポートがリストされます。
- **[Type（タイプ）]** に、指定されたインスタンスが DC Agent、Logon Agent、RADIUS Agent、または eDirectory Agent であるかどうかが表示されます。（エージェントの各タイプの説明は、*透過的識別*、362 ページを参照してください。）

リストにエージェントを追加するためには、**[Add Agent（エージェントの追加）]** ドロップダウン リストからエージェント タイプを選択します。設定するために 次のリンクの 1 つをクリックします：

- *DC Agent の設定*、374 ページ
- *Logon Agent の設定*、381 ページ
- *RADIUS Agent の設定*、383 ページ
- *eDirectory Agent の設定*、386 ページ

リストからエージェントのインスタンスを削除するためには、リストでエージェント情報の隣のチェックボックスにマークを付け、**[Delete（削除）]** をクリックします。

1 つ以上の DC Agent インスタンスがある場合、[DC Agent Domains and Controllers（DC Agent ドメインおよびコントローラ）] の下で **[View Domain List（ドメイン リストの表示）]** をクリックし、エージェントが現在どのドメイン コントローラをポーリングしているかを調べます。詳細は、*DC Agent によってポーリングされたドメインおよびドメイン コントローラの検討*、378 ページを参照してください。

[User Identification Exceptions（ユーザー識別例外）] リストの下に、ネットワーク内の他のコンピュータと異なる方法でユーザー識別を設定するコンピュータの IP アドレスをリストします。

例えば、透過的識別エージェントまたは統合製品を使用してユーザーを識別し、手動認証を有効にして、透過的に識別できないときにユーザーに資格情報の入力を促す場合、特定のコンピュータを以下のように設定することができます。

- 識別できないユーザーに資格情報の入力を要求しない。言い換えれば、透過的識別が失敗した場合、手動認証は試みられず、コンピュータまたはネットワーク ポリシー、またはデフォルト ポリシーが適用されます。
- ユーザー情報が利用可能な場合でも、常にそれを無視し、ユーザーに常に資格情報の入力を促す。
- ユーザー情報が利用可能な場合でも、常にそれを無視し、ユーザーに資格情報の入力を促さない（常にコンピュータまたはネットワーク ポリシー、またはデフォルト ポリシーが適用されます）。

例外を作成するためには、**[Add（例外）]** をクリックし、次に、*特定のコンピュータの認証ルールの設定、366 ページ*の手順を実行します。例外を削除するには、IP アドレスまたは IP アドレス範囲の横のチェックボックスをオンにし、**[Delete（削除）]** をクリックします。

[Additional Authentication Options（追加の認証オプション）] で、ユーザーが（エージェントまたは統合製品によって）透過的に識別されないときの Websense ソフトウェアのデフォルトの応答を指定します。

- ユーザーおよびグループ ベースのポリシーを無視し、コンピュータまたはネットワーク ベースのポリシー、デフォルト ポリシーを適用する場合、**[Apply computer or network policy（コンピュータまたはネットワークのポリシーを適用する）]** をクリックします。
- ブラウザを開くとき、ログオン資格情報を提供するようにユーザーに要求するためには、**[Prompt user for logon information（ログオン情報についてユーザーにプロンプトを表示する）]** をクリックします。ユーザーおよびグループ ベースのポリシーが適用されます（*手動認証、363 ページ*を参照）。
- ユーザーがログオン資格情報を要求される場合に Websense ソフトウェアが使用するデフォルト ドメイン コンテクストを指定します。これは、ユーザ資格情報が有効であるドメインです。

  ログオン情報の入力を要求されるコンピュータを指定するために [Exceptions] リストを使用している場合は、グローバル ルールがコンピュータまたはネットワーク ベースのポリシーを適用する場合でも、デフォルト ドメイン コンテクストを指定する必要があります。

このページの変更が完了したら、**[OK]** をクリックして、変更を保存します。**[Save and Deploy]** をクリックするまで変更は適用されません。

特定のコンピュータの認証ルールの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ユーザー識別方法の設定、364 ページ*
- *手動認証、363 ページ*
- *セキュア手動認証、369 ページ*

選択的認証によって、ユーザーが特定のクライアント コンピュータ（IP アドレスによって識別）からインターネット アクセスを要求する時に、ブラウザでログオン資格情報を提供するよう促されるかどうかを決定できます。これにより以下のようなことが可能になります：

- 公開キオスクを提供する組織の従業員向けの認証ルールとは異なる認証ルールを公開キオスクのために設定する。
- インターネットにアクセスする前に、医療オフィス内の診察室コンピュータのユーザーが、常に識別されることを保証する。

特別のユーザー識別設定が提供されるコンピュータは、**[Settings] > [General] > [User Identification]** ページにリストされます。ネットワークの特定のコンピュータに特別のユーザー識別設定を行う、または特定のコンピュータに特別の設定が行われているかどうかを表示するためには、**[Exceptions]** をクリックします。

リストにコンピュータを追加するためには、**[Add]** をクリックし、次に*ユーザー識別設定例外の定義、367 ページ*に示す手順を実行します。

リストへのコンピュータまたはネットワーク範囲の追加が完了したら、**[OK]** をクリックします。**[Save and Deploy]** をクリックするまで変更は適用されません。

ユーザー識別設定例外の定義

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *透過的識別、362 ページ*
- *手動認証、363 ページ*
- *ユーザー識別方法の設定、364 ページ*

特定のユーザー識別ルールが適用されるコンピュータを指定するためには、**[User Identification] > [Add IP Addresses]** ページを使用します。

1. 特定の認証方法を適用するコンピュータを指定するために **IP アドレス**またはネットワーク**範囲**を IPv4 または IPv6 形式で入力し、次に、右矢印ボタンをクリックしてそれらを **[Selected（選択済み）]** リストに追加します。

   同じルールを複数のコンピュータに適用する場合、リストにそれらすべてを追加します。
2. Websense ソフトウェアがこれらのコンピュータのユーザーを透過的に識別するかどうかを指定するために、**[User identification]** ドロップダウンリストでエントリを選択します。
   - 透過的識別エージェントまたは統合デバイスからのユーザー情報を要求する場合は、**[Try to identify user transparently（ユーザーの透過的識別を試行）]** を選択します。
   - 透過的方法によるユーザー識別を行わない場合は、**[Ignore user information（ユーザー情報を無視する）]** を選択します。

3. ユーザーがブラウザによってログオン資格情報を提供するよう促されるかどうかを指定します。ユーザー情報が有効でない、他の識別が失敗した、またはユーザー情報が無視された場合に、この設定が適用されます。
   - ユーザーがログオン資格情報の提供を要求されないようにするには、**[Apply computer or network policy（コンピュータまたはネットワークのポリシーを適用する）]** を選択します。

     また、[ユーザの透過的識別を試行] が選択されている場合、その資格情報が透過的に確認されたユーザは 適切なユーザ ベースのポリシーによってフィルタされます。
   - ログオン資格情報を提供するようにユーザーに要求するためには、**[Prompt user for logon information（ログオン情報についてユーザーにプロンプトを表示する）]** をクリックし、次に、使用する**デフォルト ドメイン コンテクスト**（もしあれば）を指定します。

     また、[ユーザの透過的識別を試行] が選択されている場合、透過的に識別されない場合に限り、ユーザにブラウザ プロンプトが表示されます。
4. [User Identification] ページに戻るためには、**[OK]** をクリックします。
5. [Exceptions] リストの更新が完了したら、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

ユーザー識別設定例外の修正

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *透過的識別*、362 ページ
- *手動認証*、363 ページ
- *ユーザー識別方法の設定*、364 ページ

[Exceptions] リストの項目を変更するためには、**[Settings] > [User Identification] > [Edit IP Addresses（IP アドレスの編集）]** ページを使用します。このページで行われた変更は、[Selected] リストに表示される（IP アドレスまたは範囲によって識別される）すべてのコンピュータに影響を与えます。

1. Websense ソフトウェアがこれらのコンピュータのユーザーを透過的に識別するかどうかを指定するために、**[User identification]** ドロップダウン リストでエントリを選択します。
   - 透過的識別エージェントまたは統合デバイスからのユーザー情報を要求する場合は、**[Try to identify user transparently（ユーザーの透過的識別を試行）]** を選択します。
   - 透過的方法によるユーザー識別を行わない場合は、**[Ignore user information（ユーザー情報を無視する）]** を選択します。

2. ユーザーがブラウザによってログオン資格情報を提供するよう促されるかどうかを指定します。ユーザー情報が有効でない、透過的識別が失敗した、または透過的識別が無視された場合に、この設定は適用されます。
   - ユーザーがログオン資格情報の入力を要求されないようにするためには、**[Apply computer or network policy（コンピュータまたはネットワークのポリシーを適用する）]** を選択します。
   - また、[ユーザの透過的識別を試行] が選択されている場合、その資格情報が透過的に確認されたユーザは 適切なユーザ ベースのポリシーによってフィルタされます。
   - ログオン資格情報を提供するようにユーザーに要求するためには、**[Prompt user for logon information（ログオン情報についてユーザーにプロンプトを表示する）]** をクリックし、次に、使用する**デフォルト ドメイン コンテクスト**（もしあれば）を指定します。

     また、[ユーザの透過的識別を試行] が選択されている場合、透過的に識別されない場合に限り、ユーザにブラウザ プロンプトが表示されます。
3. [User Identification] ページに戻るためには、**[OK]** をクリックします。
4. [Exceptions] リストの更新が完了したら、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

セキュア手動認証

関連項目：
- *ユーザー識別方法の設定、364 ページ*
- *手動認証、363 ページ*
- *特定のコンピュータの認証ルールの設定、366 ページ*
- *セキュア手動認証の有効化、371 ページ*

Websense セキュア手動認証は、クライアント コンピュータと Websense ソフトウェア間で送信される認証データを保護するために、Secure Sockets Layer（SSL）暗号化を使用します。Filtering Service に組み込まれた SSL サーバーは、クライアント コンピュータと Filtering Service の間で送信されるユーザー名とパスワードの暗号化を提供します。デフォルトで、セキュア手動認証は無効になっています。

注意
セキュア手動認証はリモート フィルタリング ソフトウェアでは使用できません。Remote Filtering Server が、セキュア手動認証を有効にした Filtering Service インスタンスに関連付けられる場合、Remote Filtering Server は、クライアントにブロック ページを配信することができません。

この機能を有効にするためには、次のステップを実行してください：

1. SSL 証明書 および キーを作成し、それらを Websense ソフトウェアがアクセス可能で、Filtering Service が読み取り可能な場所に配置します（*キーと証明書の作成、370 ページ*を参照）。
2. セキュア手動認証を有効にし（*セキュア手動認証の有効化、371ページ*を参照）、ディレクトリ サービスとの通信を確認します。
3. ブラウザに証明書をインポートします（*クライアント ブラウザ内での証明書の適用、372 ページ*を参照）。

キーと証明書の作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：
- *手動認証、363 ページ*
- *特定のコンピュータの認証ルールの設定、366 ページ*
- *セキュア手動認証、369 ページ*
- *セキュア手動認証の有効化、371 ページ*
- *クライアント ブラウザ内での証明書の適用、372 ページ*

証明書は、データを暗号化するために使用される公開キーとデータを解読するために使用される秘密キーで構成されます。証明書は Certificate Authority（CA）から公布されます。内部証明書サーバーから証明書を作成するか、または VeriSign のような第三者 CA からクライアント証明書を入手することができます。

クライアント証明書を発行する CA は、Websense ソフトウェアによって正当性が確認される必要があります。一般に、これは ブラウザ設定によって決定されます。

- プライベート キー、CSR、証明書についての FAQ は、httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts を参照してください。
- 自身のプライベート キー、CSR、証明書の作成の詳細は、www.akadia.com/services/ssh_test_certificate.html を参照してください。

OpenSSL ツールキットを含む、自己署名証明書を作成するために使用できる多くのツールがあります（openssl.org から利用可能）。

証明書を作成する方法の選択にかかわらず、次の一般的なステップを使用してください。

1. プライベート キー（**server.key**）を作成する。
2. プライベートキーで 証明書署名要求（CSR）を作成する。

> **重要**
> CommonName の入力を要求されたとき、Filtering Service コンピュータの IP アドレスを入力する。このステップを省略すると、クライアント ブラウザがセキュリティー証明書エラーを表示します。

3. 自己署名証明書（**server.crt**）を作成するために、CSR を使用する。
4. Websense ソフトウェアがアクセスできる場所、および Filtering Service が読み込むことができる場所に、**server.crt** および **server.key** ファイルを保存する。

セキュア手動認証の有効化

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：
- *手動認証*、363 ページ
- *特定のコンピュータの認証ルールの設定*、366 ページ
- *セキュア手動認証*、369 ページ
- *キーと証明書の作成*、370 ページ
- *クライアント ブラウザ内での証明書の適用*、372 ページ

1. Websense Filtering Service を停止します（*Websense サービスの停止と起動*、477 ページを参照）。
2. Filtering Service コンピュータ上で Websense のインストール ディレクトリ（デフォルトでは、**C:\Program Files** *または* **Program Files（x86）\Websense\bin** もしくは **/opt/Websense/bin/**）に移動します。
3. **eimserver.ini** を見つけ、他のディレクトリにファイルのバックアップ コピーを作成します。
4. テキストエディタで original INI ファイルを開きます。
5. **[WebsenseServer]** セクションを見つけ、次のラインを追加します：

```
SSLManualAuth=on
```

6. 前のラインの下に、次を追加します：

   ```
   SSLCertFileLoc=[path]
   ```

   [path] を証明書ファイル名を含めた SSL 証明書の完全なパスに置き換えます（例えば、C:\secmanauth\server.crt）。

7. 同じく次を追加します：

   ```
   SSLKeyFileLoc=[path]
   ```

   [path] をキーファイル名を含めた SSL キーの完全なパスに置き換えます（例えば、C:\secmanauth\server.key）。

8. **eimserver.ini** を保存し、閉じます。
9. Websense Filtering Service を起動します。

起動後、Filtering Service は、デフォルト セキュア HTTP ポート（**15872**）上で要求をリッスンします。

前のステップは、クライアント コンピュータと Websense ソフトウェア間のセキュア通信を確認します。また、Websense ソフトウェアとディレクトリ サービス間のセキュア通信を確認するためには、**[Settings] > [Directory Services（ディレクトリ サービス）]** ページで **[Use SSL（SSL を使用する）]** が選択されていることを確認します。詳細については、*拡張ディレクトリ設定、98 ページ*を参照してください。

クライアント ブラウザ内での証明書の適用

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *手動認証、363 ページ*
- *特定のコンピュータの認証ルールの設定、366 ページ*
- *セキュア手動認証、369 ページ*
- *キーと証明書の作成、370 ページ*
- *セキュア手動認証の有効化、371 ページ*

ウェブサイトを閲覧する最初のとき、ブラウザはセキュリティ証明書について警告を表示します。今後このメッセージが表示されることを避けるためには、証明書を証明書ストアにインストールします。

Microsoft Internet Explorer

1. ブラウザを開き、ウェブサイトに移動します。

   サイトのセキュリティ証明書に問題があるという警告が表示されます。

2. **[Continue to this website（not recommended）（このサイトの閲覧を続行する（（推奨されません））]** をクリックします。

   認証プロンプトを受け取ったら、**[Cancel]** をクリックします。

3. アドレス バー（ブラウザ ウインドウの上部）の右側の **[Certificate Error（認証エラー）]** ボックスをクリックし、次に **[View certificates（証明書の表示）]** をクリックします。
4. [Certificate] ダイアログ ボックスの一般タブ上で、**[Install Certificate（証明書のインストール）]** をクリックします。
5. **[Automatically select the certificate store based on the type of certificate（自動的に証明書の種類に基づいて証明書ストアを選択）]** を選択して、**[Next]** をクリックします。
6. **[Finish]** をクリックします。
7. 証明書をインストールするか尋ねられるとき、**[Yes]** をクリックします。

ユーザーは、このコンピュータで Filtering Service に関連する証明書セキュリティ警告を受け取らないようになります。

Mozilla Firefox

1. ブラウザを開き、ウェブサイトに移動します。

   警告メッセージが表示されます。
2. **[Or you can add an exception（例外を追加することができます）]** をクリックします。
3. **[Add Exception（例外の追加）]** をクリックします。
4. **[Permanently store this exception is selected（この例外を永久にストアする）]** が選択されていることを確認し、**[Confirm Security Exception（セキュリティ例外の確認）]** をクリックします。

ユーザーは、このコンピュータで Filtering Service に関連する証明書セキュリティ警告を受け取らないようになります。

DC Agent

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *透過的識別*、362 ページ
- *DC Agent の設定*、374 ページ

Websense DC Agent は Windows 上で動作し、NetBIOS、WINS、または DNS ネットワーク サービスで機能する Windows ネットワークでユーザーを検出します。

DC Agent と User Service がネットワーク ユーザー データを収集し、Websense Filtering Service にそれを送信します。いくつかの変数により、ネットワーク サイズと既存のネットワーク トラフィック量を含めて、データ伝送速度を決定します。

DC Agent による透過的識別を有効にする方法は、次の通りです：

1. DC Agent をインストールします。詳細については、[Deployment and Installation Center] を参照してください。

   ドメインの検出（ドメインおよびドメイン コントローラの自動検出）およびコンピュータのポーリングを実行するには、DC Agent は **domain admin** または **enterprise admin** 権限で実行しなければなりません。これらの機能を使用しない場合、DC Agent はドメイン コントローラへのリードアクセス権限がある任意のネットワーク ユーザーとして実行できます。ドメイン検出が無効化されている時、各 DC Agent インスタンスのドメインおよびドメイン コントローラ リストを手動で維持しなければなりません（*dc_config.txt ファイル、379 ページ*を参照）。
2. DC Agent をネットワーク内の他の Web Security コンポーネント および ドメイン コントローラと通信するように設定します（*DC Agent の設定*を参照）。
3. ポリシーをユーザー、グループ、および OU に割り当てるには、Web Security manager を使用します（*クライアントの追加、102 ページ*を参照）。

DC Agent が透過的にユーザーを識別できない場合、Web Security ソリューションがユーザーに識別を要求することができます。詳細については、*手動認証、363 ページ*を参照してください。

DC Agent の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *透過的識別*
- *手動認証*
- *ユーザー識別方法の設定*
- *DC Agent*

DC Agent の新しいインスタンスを設定するため、および DC Agent のすべてのインスタンスに適用されるグローバル設定を設定するためには、**[User Identification] > [DC Agent]** ページを使用します。

DC Agent の新しいインスタンスを追加するために、最初にエージェントがどこにインストールされているか、Filtering Service とどのように通信するかについての基本情報を提供します。これらの設定は、各エージェント インスタンスに対して固有なものであるかもしれません。

1. [Basic Agent Configuration（基本エージェントの構成）] に、エージェントがインストールされているコンピュータの **IPv4 アドレスまたはホスト名**を入力します。

   > **注意**
   > コンピュータ名はアルファベット（a-z）で始めます。数字や特殊文字で始めることはできません。
   >
   > 一部の拡張アスキー文字を含んでいるコンピュータ名は、適切に認識されない場合があります。Websense ソフトウェアの非英語バージョンを使用している場合、コンピュータ名の代わりに IP アドレスを入力してください。

2. DC Agent が 他の Websense コンポーネントと通信するために使用する**ポート**を入力します。デフォルトは 30600 です。
3. Filtering Service と DC Agent の間で認証接続を確立するためには、**[Enable authentication（認証を有効にする）]** を選択し、接続のための**パスワード**を入力します。

次に、グローバル DC Agent 通信とトラブルシューティング通信、ドメイン コントローラ ポーリング、コンピュータ ポーリング設定をカスタマイズします。デフォルトでは、ここでの変更はすべての DC Agent インスタンスに影響を与えます。

しかし、これらの設定の一部は、設定ファイルの中で無効にできます（テクニカル ペーパー[Using DC Agent for Transparent User Identification] を参照）。

1. [Domain Discovery] の下の **[Enable automatic domain discovery（自動ドメイン検索を有効化）]** をオンまたはオフにすることによって、DC Agent がネットワーク内のドメインおよびドメイン コントローラを自動的に検出するかどうかが決まります。
2. ドメインの検出が有効化されている場合、下記も指定します。
   - **ドメインを検出する**頻度。デフォルトでは、ドメインの検出は 24 時間間隔で行われます。
   - **DC Agent** または **User Service** のどちらでドメイン検出を行うか。

     多くの環境では、ドメインの検出に User Service を使用することを推奨します。

     ドメインの検出に DC Agent を使用する場合、このサービスは **domain** または **enterprise admin** 権限で実行しなければなりません。

3. User Service が Websense アプライアンスまたは Linux サーバー上にインストールされている場合、このページには **[Linux WINS Server Information（Linux WINS サーバー情報）]** セクションが含まれます。ドメイン名をドメイン コントローラの IP アドレスに解決するために WINS サーバーが必要とされます。

   まだ [Settings] > [Directory Services] ページで WINS 情報を提供していない場合、下記を入力します。

   a. ディレクトリ サービスにアクセスできる**管理ユーザー**のアカウント名。
   b. アカウントの**パスワード**。
   c. アカウントの**ドメイン**情報。
   d. ネットワーク内の WINS サーバーの IP アドレスまたはホスト名

4. DC Agent がドメイン コントローラにユーザー ログオン セッションをクエリーできるようにするために、[DC Agent Communication（DC Agent 通信）] の [Domain Controller Polling（ドメイン コントローラのポーリング）] セクションで、**[Enable domain controller polling（ドメイン コントローラのポーリングを有効にする）]** をオンにします。

   ドメイン コントローラのポーリングを実行するには、DC Agent サービスはドメイン コントローラに対するリード アクセス権限のみを必要とします。自動ドメイン検出（ステップ 1 および 2）およびコンピュータ ポーリング（ステップ 7）を実行するには、サービスがより高レベルの権限で実行している必要があります。

   設定ファイルで、DC Agent の各インスタンスがどのドメイン コントローラをポーリングするかを指定することができます（*dc_config.txt ファイル、379 ページ*を参照）。

5. **[Query interval（クエリー間隔）]** フィールドは、DC Agent がドメイン コントローラに対してクエリーする頻度（秒単位）を指定するために使用します。

   クエリー間隔を小さくすると、ログオン セッションを取得する正確性が高くなりますが、ネットワーク全体のトラフィックが増加します。クエリー間隔を大きくすると、ネットワーク トラフィックは減少しますが、若干のログオン セッションの取得が遅れるか、取得できない場合があります。デフォルトは 10 秒です。

6. **[User entry timeout（ユーザー エントリのタイムアウト）]** フィールドは、DC Agent がマップでユーザ エントリを更新する頻度（時間単位）を指定するために使用します。デフォルトは 24 時間です。

7. ユーザー ログオン セッション取得のためのコンピュータのクエリーを有効にするために、[Computer Polling（コンピュータ ポーリング）] で **[Enable computer polling（コンピュータのポーリングを有効にする）]** をチェックします。これは、エージェントがすでにクエリーしているドメイン外にあるコンピュータを含む場合があります。

   DC Agent は、コンピュータ ポーリングに、WMI（Windows Management Instruction）を使用します。コンピュータ ポーリングを有効にした場合、クライアント コンピュータで Windows ファイアウォールがポート **135** 上の通信を許可するように設定してください。

   コンピュータのポーリングに DC Agent を使用する場合、このサービスは **domain** または **enterprise admin** 権限で実行しなければなりません。

8. ユーザーがログオンしているかを確認するために DC Agent がクライアント コンピュータと通信する頻度を指定するために、**[User map verification interval（ユーザ マップの確認間隔）]** を入力します。デフォルトは 15 分です。

   DC Agent は、Filtering Service に送信するクエリー結果とユーザマップのユーザー名 /IP アドレスの対比とを比較します。この間隔を小さくすると、ユーザマップの正確性が高くなりますが、ネットワーク トラフィックも増加します。間隔を小さくすると、ネットワーク トラフィックは減少しますが、正確性も低くなります。

9. DC Agent が コンピュータ ポーリングで取得したユーザー マップのエントリをリフレッシュする頻度を指定するために、**[User entry timeout（ユーザ エントリのタイムアウト）]** を入力します。デフォルトは 1 時間です。

   DC Agent は、このタイムアウト期間より古く、DC Agent が現在ログオンしていることを確認できないユーザー名 /IP アドレスのエントリを削除します。この間隔を大きくすると、マップはより長い時間潜在的に古いユーザー名を保持しますので、ユーザー マップの正確性を低くすることがあります。

> **注意**
> ユーザー エントリのタイムアウト間隔を ユーザー マップの確認間隔より短くしないでください。これは、ユーザー名が確認される前に、ユーザー マップから削除される原因になります。

10. [User Identification] ページに戻るために **[OK]** をクリックし、次に **[OK]** をもう一度クリックして変更をキャッシュに入れます。**[Save and Deploy]** をクリックするまで変更は適用されません。

DC Agent によってポーリングされたドメインおよびドメイン コントローラの検討

[User Identification] > [DC Agent Domains and Controllers] ページを使用して、ネットワーク内の各 DC Agent インスタンスが現在、どのドメイン コントローラをポーリングしているかを検討します。

> **重要**
> [DC Agent Domains and Controllers] ページに [現在 DC Agent がポーリングしているドメイン コントローラはありません] というテキストが表示された場合は、*[DC Agent Domains and Controllers（DC Agent ドメインおよびコントローラ）] ページが空白*、580 ページを参照してください。

通常は、このページはネットワーク内の各 **DC Agent インスタンス**が検出した**ドメイン**および**ドメイン コントローラ**を表示します。

デフォルトでは、DC Agent は**ドメイン検出**プロセス（ドメインおよびドメイン コントローラの識別）をスタートアップ時、およびその後は 24 時間間隔で実行します。ドメインおよびコントローラの情報は、**dc_config.txt** という名前のファイルに保存されます（*dc_config.txt ファイル*、379 ページを参照）。

[DC Agent Domains and Controllers] ページに表示される情報は、ユーザーの環境の中の各 dc_config.txt ファイルから収集されます。

- このリストは実際に照会されているドメインおよびコントローラのみを含みます。
  - dc_config.txt ファイルで照会を無効化した場合、そのドメイン コントローラは表示されません。
  - 同様に、ドメイン内のすべてのドメイン コントローラへの照会を無効化した場合、ドメインもそのドメイン コントローラもリストされません。
- ネットワーク内のすべての DC Agent インスタンスの情報が表示されます。
  - 複数の DC Agent インスタンスによって同じドメイン コントローラがポーリングされた場合、それぞれがリストされます。
  - 異なる DC Agent インスタンスが異なるドメインをポーリングするように設定するには、各インスタンスについて dc_config.txt ファイルを更新します。*dc_config.txt ファイル*、379 ページを参照してください。

- [DC Agent Domains and Controllers] ページを開くごとに TWeb Security manager は最新のドメインおよびコントローラ情報をチェックします。そのため、このページを表示中にドメイン検出が実行されている場合は、一度このページを離れてからこのページに戻り、更新を確認しなければなりません。

dc_config.txt ファイル

Web Security Help | Web Security ソリューション | バージョン 7.8.x

DC Agent はネットワーク内のドメイン コントローラを識別し、次にドメイン コントローラに対してユーザー ログオン セッションについての照会を行います。デフォルトでは、エージェントは自動的に既存のドメイン コントローラを確認し、ネットワークに追加された新しいドメインまたはドメイン コントローラを検出します。

- デフォルトでは、DC Agent はドメイン検出プロセス（ドメインおよびドメイン コントローラの識別）をスタートアップ時、およびその後は 24 時間間隔で実行します。
- ドメイン検出には DC Agent または User Service を使用できます。

ドメイン検出の有効化、および検出間隔の設定については、*DC Agent の設定*、374 ページを参照してください。

DC Agent はドメインおよびドメイン コントローラ情報を **dc_config.txt** ファイル（デフォルトでは、各 DC Agent コンピュータの C:\Program Files または Program Files（x86）\Websense\Web Security\bin\ ディレクトリにあります）に保存します。

DC Agent がポーリングするドメイン コントローラを変更するには、dc_config.txt ファイルを編集します。

1. 各 DC Agent コンピュータの Websense **bin** ディレクトリ（デフォルトでは C:\Program Files または Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）に移動します。
2. 別のディレクトリに **dc_config.txt** ファイルのバックアップ コピーを作成します。
3. テキスト エディタ（Notepad など）で元の **dc_config.txt** ファイルを開きます。
4. すべてのドメインおよびドメイン コントローラがリストされていることを確認します。例：

```
[WEST_DOMAIN]
dcWEST1=on
dcWEST2=on
[EAST_DOMAIN]
dcEAST1=on
dcEAST2=on
```

5. リストの中のいずれかのドメイン コントローラを DC Agent がポーリングしないように設定するには、そのエントリの値を **on** から **off** に変更します。例：

   ```
   dcEAST2=off
   ```

   - DC Agent がアクティブ ドメイン コントローラをポーリングしないように設定した場合、エージェントはそのドメイン コントローラにログオンするユーザーを透過的に識別できません。
   - DC Agent の自動ドメイン検出によってユーザーの識別のために使用するべきでないドメイン コントローラが検出された場合、そのエントリを削除するのではなく、**off** に設定します。そうしないと、次の検出プロセスによってコントローラが再度追加されてしまいます。
6. リストから欠落しているドメインまたはドメイン コントローラ エントリがある場合、手動でそれを追加できます。エントリを追加する前に、DC Agent コンピュータ上で **net view /domain** コマンドを実行して、エージェントが新しいドメインを認識できることを確認してください。
7. 変更を保存してファイルを閉じます。
8. **Websense DC Agent** サービスを再起動します。

Logon Agent

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *透過的識別*、362 ページ
- *Logon Agent の設定*、381 ページ

Websense Logon Agent は、ユーザーがドメインにログオンしたときにリアルタイムでユーザーを識別します。これによってクエリー タイミングの問題でユーザー ログオンが見落とされる可能性が除去されます。

Logon Agent（または Authentication Server と呼ばれる）は、Windows または Linux コンピュータに配置することができます。Windows ドメインにログオンするユーザを識別するために、Windows クライアント コンピュータ上の Websense ログオン アプリケーション（LogonApp）と共に動作します。

ほとんどの場合、DC Agent または Logon Agent を使用すれば十分です。しかし、両方のエージェントを一緒に使用することもできます。この場合、Logon Agent が DC Agent より優先されます。DC Agent は、Logon Agent が ログオン セッションを見落す稀なイベントの場合にのみ、ログオン セッションを Filtering Service に送信します。

Logon Agent をインストールし、中央からクライアント コンピュータへログオン アプリケーションを配備します。詳細についてはテクニカル・ホワイト・ペーパー『Using Logon Agent for Transparent User Identifcation』を参照してください。

インストール後、エージェントが、クライアント コンピュータおよび Websense Filtering Service と通信するように設定します（*Logon Agent の設定*を参照）。

注意

Windows Active Directory（ネイティブ モード）を使用している場合に、User Service が Linux コンピュータにインストールされている場合、追加の設定ステップについて、*Websense アプライアンスまたは Linux サーバーに配備された User Service*、585 ページを参照してください。

Logon Agent の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *透過的識別*、362 ページ
- *手動認証*、363 ページ
- *ユーザー識別方法の設定*、364 ページ
- *Logon Agent*、380 ページ

Logon Agent のすべてのインスタンスに適用されるグローバル設定を設定するために、および Logon Agent の新しいインスタンスを設定するために、**[User Identification] > [Logon Agent]** ページを使用します。

Logon Agent の新しいインスタンスを追加する方法は、次の通りです：

1. [Basic Agent Configuration）] に、Logon Agent がインストールされているコンピュータの **IPv4 アドレスまたはホスト名**を入力します。

注意

コンピュータ名は、数字、特殊文字ではなく、アルファベット文字（a-z）で始まる必要があります。

特定の拡張アスキー文字を含んでいるコンピュータ名は、適切に認識されない場合があります。Websense ソフトウェアの非英語バージョンを使用している場合、コンピュータ名の代わりに IP アドレスを入力してください。

2. Logon Agent が他の Websense コンポーネントと通信するために使用する**ポート**を入力します（デフォルトでは 30602）。
3. Filtering Service と Logon Agent の間で認証接続を確立するためには、**[Enable authentication]** をオンにし、接続のための**パスワード**を入力します。

次に、グローバル Logon Agent 通信設定をカスタマイズします。デフォルトでは、ここでの変更は すべての Logon Agent インスタンスに影響を与えます。

1. [Logon Application Communication（ログオン アプリケーションの通信）] で、ログオン アプリケーションが Logon Agent と通信するために使用する **[Connection port（接続ポート）]** を指定します（デフォルトでは 15880）。
2. 各 Logon Agent インスタンスが許容する **[Maximum number of connections（最大接続数）]** を入力します。

   ネットワークが大規模である場合、この数を増やす必要があります。この数を増やすと、ネットワーク トラフィックが増加します。

ユーザー エントリの正当性を決定する方法をデフォルト設定で設定するために、最初に Logon Agent とクライアント ログオン アプリケーションが**永続モード**または**非永続モード**（デフォルト）のどちらで動作するかを決定する必要があります。（詳細については、テクニカル ペーパー『Using Logon Agent for Transparent User Identification』を参照してください）。

- 永続モードでは、ログオン アプリケーションは ユーザー ログオン情報を送信するために、定期的に Logon Agent と通信します。

  永続モードを使用している場合、ログオン アプリケーションがログオン情報を通信する頻度を決定するためには、**[Query interval（クエリー間隔）]** を指定します。

  注意
  この値を変更した場合、前に指定した間隔の期間が終了するまで、変更は有効になりません。例えば、15 分から 5 分に間隔を変更した場合、現在の 15 分の間隔が終了したあとで、クエリーが 5 分ごとに発生するようになります。

- 非永続モードでは、ログオン アプリケーションは 各ログオンのユーザー ログオン情報を 1 度だけ Logon Agent に送信します。

  非永続モードを使用している場合、**[User entry expiration（ユーザー エントリの失効）]** 時間間隔を指定してください。このタイムアウト期間に達したとき、ユーザー エントリはユーザー マップから削除されます。

設定変更が終わったら、[Settings] > [User Identification] ページに戻るために **[OK]** をクリックし、次に **[OK]** をもう一度クリックして変更をキャッシュに入れます。**[Save and Deploy]** をクリックするまで変更は保存されません。

RADIUS Agent

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *透過的識別*、362 ページ
- *RADIUS Agent の設定*、383 ページ

Websense RADIUS Agent では、RADIU サーバーによって提供された認証を使用してユーザーおよびグループ ベースのポリシーを適用することができます。ダイアルアップ、Virtual Private Network（VPN）、Digital Subscriber Line（DSL）、または 他のリモート接続（設定に依存）を使用してネットワークにアクセスするユーザーを、RADIUS Agent によって透過的に識別することができます。

RADIUS Agent は、ネットワーク内の RADIUS サーバーと RADIUS クライアントと共に動作し、Remote Access Dial-In User Service（RADIUS）プロトコルのトラフィックを追跡します。これにより、リモート操作でネットワークにアクセスするユーザーまたはグループ、およびローカル ユーザーに対して、特定のポリシーを割り当てることができます。

RADIUS Agent をインストールするとき、エージェントは既存の Websense コンポーネントと統合されます。ただし、RADIUS Agent、RADIUS サーバーおよび RADIUS クライアントを適切に設定する必要があります（*RADIUS Agent の設定*、383 ページを参照）。

RADIUS Agent の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *透過的識別*、362 ページ
- *手動認証*、363 ページ
- *ユーザー識別方法の設定*、364 ページ
- *RADIUS Agent*、383 ページ

RADIUS Agent のすべてのインスタンスに適用されるグローバル設定を設定するために、および RADIUS Agent の新しいインスタンスを設定するために、**[User Identification] > [RADIUS Agent]** ページを使用します。

RADIUS Agent の新しいインスタンスを追加する方法は、次の通りです：

1. [Basic Agent Configuration）] に、Logon Agent がインストールされているコンピュータの **IPv4 アドレスまたはホスト名**を入力します。

   > **注意**
   > コンピュータ名は、数字、特殊文字ではなく、アルファベット文字（a-z）で始まる必要があります。
   >
   > 特定の拡張アスキー文字を含んでいるコンピュータ名は、適切に認識されない場合があります。非英語環境では、名前の代わりに IP アドレスを入力します。

2. RADIUS Agent が他の Websense コンポーネントと通信するために使用する**ポート**を入力します（デフォルトでは 30800）。
3. Filtering Service と RADIUS Agent の間で認証接続を確立するためには、**[Enable authentication]** をオンにし、接続のための**パスワード**を入力します。

次に、グローバル RADIUS Agent 設定をカスタマイズします。デフォルトでは、ここでの変更は すべての RADIUS Agent インスタンスに影響を与えます。しかし、アスタリスク（*）が付いた設定 は、そのエージェントのインスタンスの動作をカスタマイズするために、エージェント設定ファイルで上書きできます（テクニカル ペーパー『Using RADIUS Agent for Transparent User Identification』を参照）。

1. RADIUS Server で、**[RADIUS server address or name（RADIUS サーバーの IP または名前）]** を入力します。IP アドレスを提供する場合、IPv4 アドレス形式を使用します。

   RADIUS Agent は、認証要求を RADIUS サーバーに転送します。このコンピュータの識別子を知っている必要があります。
2. ネットワークに RADIUS クライアントが含まれる場合、**[RADIUS client address or name（RADIUS クライアントの IP または名前）]** を入力します。IP アドレスを提供する場合、IPv4 アドレス形式を使用します。

   Websense ソフトウェアはこのコンピュータにユーザー ログオン セッションをクエリーします。
3. RADIUS Agent がユーザ マップを更新する頻度を決定するために、**[User entry timeout]** 間隔を入力します。一般には、デフォルト クエリー値（24 時間）が最良です。
4. RADIUS Agent が、認証およびアカウンティングの要求を送受信するためにどのポートを使用するか指定するために、**[Authentication Ports（認証ポート）]** および **[Accounting Ports（アカウンティング ポート）]** の設定を使用します。各タイプの通信で、次の通信のためにどのポートを使用するるかを指定します：

- RADIUS Agent と RADIUS サーバーの通信（認証ポートのデフォルトは 1645、アカウンティング ポートのデフォルトは 1646）
- RADIUS Agent と RADIUS クライアントの通信（認証ポートのデフォルトは 12345、アカウンティング ポートのデフォルトは 12346）

5. 設定変更が終わったら、[Settings] > [User Identification] ページに戻るために **[OK]** をクリックし、次に **[OK]** をもう一度クリックして変更をキャッシュに入れます。**[Save and Deploy]** をクリックするまで変更は保存されません。

RADIUS クライアントおよび RADIUS サーバーと Websense RADIUS Agent との通信の設定の詳細については、テクニカル ペーパー『Using RADIUS Agent for Transparent User Identification』を参照してください。

eDirectory Agent

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *透過的識別*、362 ページ
- *eDirectory Agent の設定*、386 ページ

Websense eDirectory Agent は Novell eDirectory と共に動作して透過的にユーザーを識別し、Websense ソフトウェアがユーザー、グループ、ドメイン、組織単位に割り当てられたポリシーに従ってフィルタリングを行うことができるようにします。

eDirectory Agent は、ネットワークにログオンするユーザーを認証する Novell eDirectory から、ユーザー ログオン セッション情報を収集します。エージェントは、認証された各ユーザーを IP アドレスと関連づけ、ローカルなユーザー マップにユーザーと IP アドレスの組合せを記録します。その後、eDirectory Agent はこの情報を Filtering Service に送信します。

注意

Windows が稼働している Novell クライアントから、複数のユーザーが 1 つの Novell eDirectory サーバーにログオンすることができます。これによって 1 つの IP アドレスが複数のユーザーと関連づけられます。この場合、その IP アドレスから最後にログオンしたユーザーのユーザー名 /IP アドレスのペアだけが eDirectory Agent のユーザー マップに保存されます。

Websense eDirectory Agent の 1 つのインスタンスは、1 つの Novell eDirectory マスタと、任意の数の Novell eDirectory レプリカをサポートすることができます。

eDirectory Agent の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *透過的識別*、362 ページ
- *手動認証*、363 ページ
- *ユーザー識別方法の設定*、364 ページ
- *eDirectory Agent*、385 ページ
- *eDirectory Agent が LDAP を使用するための設定*、388 ページ

eDirectory Agent のすべてのインスタンスに適用されるグローバル設定を設定するために、および eDirectory Agent の新しいインスタンスを設定するために、**[User Identification] > [eDirectory Agent]** ページを使用します。

eDirectory Agent の新しいインスタンスを追加する方法は、次の通りです：

1. [Basic Agent Configuration）] に、eDirectory Agent がインストールされているコンピュータの **IPv4 アドレスまたはホスト名**を入力します。

   注意
   コンピュータ名は、数字、特殊文字ではなく、アルファベット文字（a-z）で始まる必要があります。

   特定の拡張アスキー文字を含んでいるコンピュータ名は、適切に認識されない場合があります。非英語環境では、名前の代わりに IP アドレスを入力します。

2. eDirectory Agent が他の Websense コンポーネントと通信するために使用する**ポート**を入力します（デフォルトでは 30700）。
3. Filtering Service と eDirectory Agent の間で認証接続を確立するためには、**[Enable authentication（認証を有効にする）]** を選択し、接続のための**パスワード**を入力します。

次に、グローバル eDirectory Agent 通信設定をカスタマイズします。

1. [eDirectory Server] で、ディレクトリでユーザー情報をサーチするとき、eDirectory Agent が開始点として使用する **検索基準**（ルート コンテクスト）を指定します。
2. eDirectory Agent がディレクトリと通信するために使用する管理ユーザー アカウント情報を指定します：
   a. Novell eDirectory の管理ユーザー アカウントの**管理者識別名** を入力します。
   b. そのアカウントで使用する**パスワード**を入力します。

c. エージェントのユーザー マップでエントリが保存される期間を指定するために、**ユーザー エントリのタイムアウト**間隔を指定します。

この値は一般的なユーザー ログオン セッションの場合よりも約 30% 長く設定する必要があります。これは、ユーザーがブラウズを完了する前に、ユーザー エントリが マップから削除されることを防止するのに役立ちます。

一般に、デフォルト値（24 時間）が推奨されます。

> **注意**
> 環境によっては、[ユーザー エントリのタイムアウト] 間隔を使用して eDirectory Agent がユーザー マップを更新する頻度を決定するよりも、一定間隔で eDirectory Server にクエリーしてユーザー ログオンの更新をチェックするほうが適切な場合があります。*eDirectory Server の完全クエリーの有効化*、389 ページを参照してください。

3. **[eDirectory Replicas]** リストに、すべてのレプリカと、eDirectory Server マスタを追加します。リストに eDirectory Server のマスタ またはレプリカを追加するためには、**[Add]** をクリックし、*eDirectory サーバー レプリカの追加*、387 ページの手順に従ってください。

設定変更が終わったら、[Settings] > [User Identification] ページに戻るために **[OK]** をクリックし、次に **[OK]** をもう一度クリックして変更をキャッシュに入れます。**[Save and Deploy]** をクリックするまで変更は保存されません。

eDirectory サーバー レプリカの追加

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense eDirectory Agent の 1 つのインスタンスは、1 つの Novell eDirectory マスタと、個別のコンピュータで動作している任意の数の Novell eDirectory レプリカをサポートすることができます。

eDirectory Agent は、ディレクトリ サービスのレプリカが稼働する各コンピュータと通信できる必要があります。これにより、エージェントは、可能な限り速く最新のログオン情報を入手でき、eDirectory のレプリケーションの発生を待つ必要がなくなります。

Novell eDirectory は、5 分ごとにユーザー ログオンを識別する属性を複製します。この複製のタイムラグにもかかわらず、eDirectory Agent はすべての eDirectory レプリカにユーザーがログオンするとすぐに、新しいログオン セッションをピックアップします。

インストールされた eDirectory Agent を eDirectory と通信するように設定するためには、次を実行します：

1. eDirectory マスタまたはレプリカ **サーバー IP アドレス**を入力します。
2. eDirectory Agent が eDirectory コンピュータと通信するために使用する**ポート**を入力します。有効な値は **389**（デフォルト）と **636**（SSL ポート）です。
3. **[OK]** をクリックして、[eDirectory Agent] ページに戻ります。新しいエントリが [eDirectory レプリカ] リストに表示されます。
4. すべての追加する eDirectory サーバー コンピュータに対して、この処理を繰り返します。
5. [Settings] > [User Identification] ページに戻るために **[OK]** をクリックし、次に **[OK]** をもう一度クリックして変更をキャッシュに入れます。
6. **[Save and Deploy]** をクリックし、変更を適用します。
7. エージェントが新しいレプリカとの通信を開始するために、eDirectory Agent を停止し、起動します。手順については、*Websense サービスの停止と起動、477 ページ*を参照してください。

eDirectory Agent が LDAP を使用するための設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense eDirectory Agent は、Novell eDirectory からユーザ ログオン情報を入手するために、Netware Core Protocol（NCP）または Lightweight Directory Access Protocol（LDAP）を使用することができます。デフォルトでは、Windows 上の eDirectory Agent は NCP を使用します。Linux 上では、eDirectory Agent は LDAP を使用する必要があります。

eDirectory Agent を Windows 上で実行している場合に、エージェントが Novell eDirectory にクエリーするために LDAP を使用することを希望する場合、エージェントが NCP の代わりに LDAP を使用するように設定します。一般に、NCP は より効率的なクエリー メカニズムを提供します。

Windows 上の eDirectory Agent が LDAP を使用するためには、次を実行します：

1. 少なくとも 1 つの Novell eDirectory レプリカが、ネットワークをモニタし、フィルタするすべてのディレクトリ オブジェクトを含んでいることを確認します。
2. Websense eDirectory Agent サービスを停止します（*Websense サービスの停止と起動、477 ページ*を参照）。
3. eDirectory Agent のインストール ディレクトリ（デフォルトでは、**\Program Files または Program Files（x86）\Websense\bin**）に移動し、テキストエディタで **wsedir.ini** ファイルを開きます。

4. **QueryMethod** のエントリを次のように修正します：

   ```
   QueryMethod=0
   ```

   これは、エージェントが Novell eDirectory にクエリーするために、LDAP を使用するように設定します。（デフォルト値は、NCP を指定する 1 です。）
5. ファイルを保存して、閉じます。
6. Websense eDirectory Agent サービスを再起動します。

eDirectory Server の完全クエリーの有効化

Web Security Help | Web Security ソリューション | バージョン 7.8.x

小さなネットワークでは、すべてのログオンするユーザーを一定間隔で eDirectory サーバーにクエリーするように、Websense eDirectory Agent を設定することができます。これにより、新しくログオンしたユーザーと最後のクエリーからログオフしたユーザーの両方を検出することができ、ローカル ユーザー マップを更新することができます。

重要
クエリー結果が返ってくるのに必要な時間はユーザー ログオン数に依存するため、大きなネットワークで完全クエリーを使用するように eDirectory Agent を設定することは推奨されません。ログオンしているユーザーが多いほど、よりパフォーマンスに影響を与えます。

eDirectory Agent の 完全クエリーを使用する場合、ログオフしたユーザーはクエリーによって識別されるため、**[User entry timeout]** 間隔は使用されません。デフォルトで、クエリーは 30 秒ごとに実行されます。

この機能を有効にすると、eDirectory Agent の 2 つの処理時間が増加します：

- クエリーが行なわれるたびに、ログオンしたユーザーの名前を検索するために必要な時間。
- ユーザー名情報を処理する時間、ローカル ユーザー マップから不要なエントリを削除し、最新のクエリーに基づいて新しいエントリを追加するために必要とされます。

eDirectory Agent は、新しいログオンだけを確認するのではなく、各クエリー後にすべてのローカル ユーザー マップを調査します。この処理に必要な時間は、各クエリーによって返されたユーザー数に依存します。従って、クエリー処理は、eDirectory Agent と Novell eDirectory Server の両方の応答時間に影響を与えます。

完全クエリーを有効にするためには、次を行います：

1. eDirectory Agent を実行しているコンピュータ上で Websense **bin** ディレクトリ（デフォルトでは C:\Program Files または Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）に移動します。
2. **wsedir.ini** ファイルを見つけ、他のディレクトリにバックアップ コピーを作成します。
3. （メモ帳または vi などの）テキスト エディタで **wsedir.ini** を開きます。
4. ファイルの **[eDirAgent]** のセクションに移動し、次のエントリを見つけます：

   ```
   QueryMethod=<N>
   ```

   後でデフォルト設定に戻す場合のために QueryMethod 値をメモしてください。
5. **QueryMethod** 値を次のように更新します：
   - 現在の値が 0（LDAP でディレクトリと通信している）の場合、値を **2** に変更します。
   - 現在の値が 1（NCP でディレクトリと通信している）の場合、値を **3** に変更します。

   注意
   クエリー値を変更したことでシステム パフォーマンスが遅くなった場合、前の値に QueryMethod エントリを戻します。
6. デフォルト クエリー間隔（30 秒）が、お客様の環境で適切でない場合、**PollInterval** を適当な値に編集します。

   間隔は**ミリ秒**単位で設定します。
7. ファイルを保存して、閉じます。
8. Websense eDirectory Agent サービスを再起動します（*Websense サービスの停止と起動*、477 ページを参照）。

特定のユーザー名を無視するエージェントの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

透過的識別エージェントを、実際のユーザーに関連していないログオン名を無視するように設定することができます。この機能は、特定の Windows 200x および XP のサービスが ネットワークでドメイン コントローラに接続する方法に対処するために使用されます。

例えば、**user1** がネットワークにログオンし、ドメイン コントローラによって **computerA/user1** であると識別されます。そのユーザーは、**user1** に割り当てられた Websense ポリシーによってフィルタされます。**computerA/ServiceName** と識別されるユーザーのコンピュータ上で、ドメイン コントローラと接続するためのサービスが起動した場合、ポリシー実施の問題を引き起こすことがあります。Websense ソフトウェアは、**computerA/ServiceName** を割り当てられたポリシーがない新しいユーザーとして扱い、コンピュータ ポリシーまたは**デフォルト**ポリシー を適用します。

この問題は 次のように対処します：

1. エージェント サービスを停止します（*Websense サービスの停止と起動*、477 ページを参照）。
2. **\Websense\bin** ディレクトリに移動し、テキスト エディタで **ignore.txt** ファイルを開きます。
3. 別個のラインに、各ユーザー名を入力します。[*] のようなワイルドカード文字を含めないでください：

   ```
   maran01
   WindowsServiceName
   ```

   それらがどのコンピュータに関連しているかにかかわらず、Websense ソフトウェアはこれらのユーザー名を無視します。

   Websense ソフトウェアが特定のドメインのユーザー名を無視するようにするためには、**username, domain** の形式を使用してください。

   ```
   aperez, engineering1
   ```
4. 完了したら、ファイルを保存し、閉じます。
5. エージェント サービスを再起動します。

エージェントは指定されたユーザー名を無視します。Filtering Service は、これらの名前をポリシーの実施の対象とみなしません。

ハイブリッド ユーザーの識別

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Websense Directory Agent*、400 ページ
- *ユーザーが識別されない時*、403 ページ
- *認証の優先順と無効化*、394 ページ
- *ハイブリッド サービス クライアントの処理*、109 ページ

ハイブリッド サービスでユーザーを識別する方法を設定するため、およびユーザーのサービスへの接続をテストおよび設定するためには、**[Settings] > [Hybrid] [Configuration] > [Hybrid] [User Identification]** を選択します。必要ならハイブリッド ユーザーのために複数の認証および識別オプションを設定できます。

ハイブリッド ユーザーに対して、フィルタ対象の場所からのアクセスかオフサイトからのアクセスかに関わりなく、適当なユーザーごと、またはグループごとのポリシーが適用されるようにするために、Websense Web Security Gateway Anywhere はハイブリッド ユーザーを透過的に識別するオプションを提供します。

- **Websense Web Endpoint** はクライアント コンピュータ上にインストールされ、透過的認証を提供し、ハイブリッド サービスの使用を強制し、認証の詳細をハイブリッド サービスに渡します。*Web Endpoint の配備の概要、395 ページ*を参照してください。

Web Endpoint を配備しない場合、ハイブリッド サービスはユーザーがハイブリッド サービスに接続する時に透過的に、または手動でユーザーを識別できます。

- ユーザーが **[フィルタされている場所]**（see *フィルタ対象の場所を定義、263 ページ*を参照）として定義されている既知の IP アドレスからログオンしている場合、ユーザーは NTLM を通じて透過的にのみ識別できます。NTLM 識別はオフサイトのユーザーには利用できません。
- ハイブリッド サービスは、Directory Agent によって情報が収集されているすべてのユーザーに対してパスワードを自動的に生成するように設定できます（*ハイブリッド サービスへのユーザーのアクセスの設定、272 ページ*を参照）。
- どの形式の透過的認証も有効化しない場合、次のようになります。
  - Web Endpoint を利用できないオフサイト ユーザーは、ブラウザを開いてインターネットに接続しようとした時に電子メール アドレスとパスワードの入力を要求されます。
  - 他のハイブリッド ユーザーは、Web EndpointまたはNTLM 識別を利用できない場合、IP アドレスを基にポリシーを割り当てられます。

ハイブリッド サービスがインターネット アクセスを要求するユーザーを識別する方法を指定します。これらのオプションは、endpoint が停止した場合のフォールバックとしても使用されます。

- **[Always authenticate users on first access（常にユーザーを最初のアクセス時に認証する）]** をオンにすると、ユーザーが最初にハイブリッド サービスに接続した時に透過的 NTLM 認証、高セキュリティ認証または手動認証が有効化されます。

  このオプションを選択せず、フィルタリングされている場所で他のユーザー認証方法を有効にしていない場合、ユーザーは IP アドレス ベースのポリシーを適用され、その識別情報はレポートには示されません。

Internet Explorer および Firefox は透過的ユーザー認証で使用できます。他のブラウザはユーザーにログオン情報の入力を要求します。

Directory Agent がハイブリッド サービスのデータを送信している場合、NTLM を使用してユーザーを識別することを推奨します。

- **[Use NTLM to identify users when possible（可能な時は NTLM を使用してユーザーを識別する）]** をオンにすると、可能な場合に Directory Agent によって収集された情報によってユーザーが透過的に識別されます。

  このオプションを選択している時、ハイブリッド サービスは、クライアントが NTLM をサポートする場合は NTLM を使用してユーザーを識別し、それ以外の場合はログオンを要求するプロンプトを返します。

> **注意**
> NTLM を使用してユーザーを識別する時、自動登録（[Registered Domains（登録されているドメイン）] の下の [User Access（ユーザー アクセス）] ページで設定）を**使用してはいけません**。

- [Use secured form authentication **to identify users（セキュアな形式の認証を使ってユーザーを認証する）]** をオンにすると、エンド ユーザーに対してセキュアなログオン フォーマットが表示されます。ユーザーが電子メール アドレスとハイブリッド サービス パスワードを入力した時、認証のために資格情報がセキュアな接続を通じて送信されます。

  このオプションを選択する場合、[Session Timeout（セッション タイムアウト）] で、セキュリティ上の理由でユーザーの資格情報を再確認する頻度を指定します。デフォルトのオプションは 1、7、14 または 30 日です。

> **注意**
> [Session Timeout] オプションを 3 カ月、6 カ月、12 カ月に延長することもできます。この拡張機能を有効化するには、サポートに連絡してください。

ユーザーがこのサービスを使用するように登録されていない場合、ログオン フォームで **[Register（登録する）]** をクリックすることによって登録できます。このオプションを使用するには、自動登録（[Registered Domains] の下の [User Access] ページで設定）を有効化します。エンド ユーザーに対して、ハイブリッド サービス アクセスではネットワークにログオンする時に使用するものと同じパスワードを**使用しない**よう助言してください。

NTLM またはセキュアな形式の認証オプションを選択せず、**[Always authenticate users on first access（常に最初のアクセス時にユーザーを認証する）]** が選択されている場合、他の手段によって識別できないユーザーには、インターネットにアクセスするたびにログオン プロンプトが表示されます。ログオン プロンプトを受け取ったユーザーの識別には基本認証が使用されます。

- NTLM を通じて認証されていない、またはセキュアな形式の認証を使用していないユーザーがインターネットに接続するためにブラウザを開いた時に Welcome ページが表示されるようにするかどうかを指定します。Welcome ページは、
  - ユーザーが使用開始する際に使用する一般的な検索エンジンの選択肢を提供します
  - 主に、フィルタリングされている場所の外からハイブリッド サービスに接続するユーザーが使用します（たとえば、自宅または出張先で勤務している時）

完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

ハイブリッド サービスを設定し、ユーザーのブラウザが PAC ファイルにアクセスするように設定した後は、**[Verify End User Configuration（エンド ユーザーの設定の確認）]** の下のリンクを使って、エンド ユーザーのコンピュータがインターネットにアクセスでき、ハイブリッド サービスに接続するように正しく設定されていることを確認することができます。

まだハイブリッド サービス アカウントが確認されていない場合（[Settings] > [General > Account] ページで電子メール アドレスを入力していない可能性があります）、URL は表示されません。

認証の優先順と無効化

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Settings] > [Hybrid Configuration] > [Hybrid User Identification] ページで、エンド ユーザーのために複数の認証オプションを選択することができます。これらのオプションの優先順は次の通りです。

- Web Endpoint がクライアント コンピュータにインストールされている場合は、常に使用されます。
- Web Endpoint が利用できない場合、下記の両方の条件が満たされていればエンド ユーザーは高セキュリティ方式の認証によって認証されます。
  a. [Hybrid User Identification] ページ上で選択されている。
  b. 認証を要求しているユーザー エージェントまたはアプリケーションが HTML ページを通じたフォーム ベースの認証をサポートしている。
- フォーム ベースの認証をサポートしないアプリケーションは、NTLM 識別または基本識別を使用します。**[Always authenticate users on first access]** が選択されていて、他に選択できるまたは利用できるオプションがない場合は、常に基本認証が使用されます。

また、PAC ファイルの URL を以下の形式で配備することによって、特定のエンド ユーザー - たとえば、支店のすべてのユーザー - に対して特定の認証オプションを強制することができます。

```
http://hybrid-web.global.blackspider.com:8082/proxy.pac?a=X
```

a= パラメータは認証オプションを制御し、X は下記のいずれかの値に設定することができます。

パラメータ	説明
a=n	ポリシー設定およびブラウザまたはアプリケーションの機能に応じて、NTLM 通知または基本認証を使用します。
a=f	認証はセキュアなフォーム ベースの認証を使用して実行されます。

Web Endpoint の配備の概要

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Web Endpoint for Windows の手動でのインストール*、398 ページ
- *Web Endpoint for Mac OS X の手動でのインストール*、400 ページ

Websense Web Endpoint は、クライアント コンピュータにインストールされるソフトウェアです。これは Web Security にハイブリッド サービスを使用することを強制し、認証情報をハイブリッド プロキシに渡し、セキュアで透過的な認証を可能にします。

サポートされている OS のリストは、Web Endpoints のドキュメントの [システム要件] の項目に示しています。

Web Endpoint を Windows クライアントに配備するには、下記の方法を利用できます。

- インストール ファイルをダウンロードし、次に Microsoft Group Policy Object または同様の配布ツールを使用してファイルを、選択したクライアント コンピュータに配備する。
- インストール ファイルをクライアント コンピュータにダウンロードし、次に Web Endpoint ソフトウェアを手動でインストールする。
- エンドポイントをハイブリッド サービスから一部またはすべてのハイブリッド ユーザーに直接に配備する。各ユーザーは、自分のコンピュータにエンドポイント ソフトウェアをインストールするように促されます。
  - この配備方法は Google Chrome ブラウザではサポートされていません。
  - Internet Explorer 10 では、この配備方法はブラウザがデスクトップ モードである時にのみサポートされます。

ユーザーがエンドポイントをインストールしていない場合、そのユーザーは [User Identification] ページで選択されているオプションに従って認証されます。ユーザーは、次にブラウズ セッションを開始した時に、再びエンドポイントをインストールするように要求されます。

*Web Endpoint for Windows の手動でのインストール、398 ページ*を参照してください。

Web Endpoint を Mac OS X クライアントに配備するには、下記の方法を利用できます。

- ファイルを個別のクライアント コンピュータにダウンロードまたはコピーし、次にパッケージをダブルクリックしてインストーラを起動する。
- ファイルを Mac コンピュータにダウンロードまたはコピーし、次に Apple Remote Desktop ソフトウェアを使ってインストール パッケージを配布する。

*Web Endpoint for Mac OS X の手動でのインストール、400 ページ*を参照してください。

Data Security ソリューションもあり、Web Endpoint と Data Endpoint の両方をクライアント コンピュータに配備したい場合、Websense Endpoint Package Builder を使用して両方のエンドポイントの配備パッケージを作成しなければなりません。各エージェントのインストール方法については、Deployment and Installation Center を参照してください。

エンドポイントには改ざん防止のためのいくつかのキー プロテクションがあり、それによって大多数のエンド ユーザーが、ローカル管理者権限がある場合でも、エンドポイントをアンインストールまたは削除するのを禁止されます。

- エンドポイント ファイル およびフォルダは削除や名前変更から保護されています。
- エンドポイントが停止したり削除された場合、エンドポイント プロセスが自動的に再開されます。
- エンドポイントをアンインストールしたり、エンドポイント サービスを停止するためにはパスワードが必要とされます。
- エンドポイントのレジストリ設定を変更または削除することはできません。
- エンドポイント サービスを削除する Service Control コマンドはブロックされます。

インストール ファイルをダウンロードする、またはハイブリッド サービスからの配備を可能にする前に、エンドポイント サービスを停止したりエンドポイントをアンインストールするために使用する改ざん防止用パスワードを定義しなければなりません。パスワードは配備されるすべてのエンドポイントに自動的にリンクされます。

> **重要**
> セキュリティ上の理由により、Websense は改ざん防止用パスワードのコピーを保持しません。パスワードを忘れた場合、[Hybrid User Identification] ページで新しいパスワードを入力し、確認することによってパスワードを再設定できます。インストールされているすべてのエンドポイントは、次にインターネットに接続する時、新しいパスワードを使用するように更新されます。

Web Endpoint 環境を有効にするには、以下の手順を実行します。

1. [Settings] > [Hybrid Configuration] > [Hybrid User Identification] ページで、**[Enable installation and update of Web Endpoint on client machines（クライアント コンピュータ上での Web Endpoint のインストールおよび更新を有効化する）]** にマークを付けます。

   このオプションを選択すると、Web Endpoint 環境と自動更新の設定が可能になります。あとでこのオプションの選択を解除した場合、インストールされているエンドポイント クライアントは、アンインストールされるまで引き続き機能しますが、自動更新は受け取らなくなります。
2. 改ざん防止用パスワードを入力し、確認します。パスワードは 4 ～ 25 文字で指定してください。
3. 配備方法を選択します。
   - Web Endpoint を個別のコンピュータに手動でインストールする場合、または希望する分配方法でインストールする場合 **[Deploy Web Endpoint Manually（Web Endpoint を手動で配備する]** をクリックします。（Web Endpoint の Mac バージョンではこのオプションだけが利用可能です）。

     画面に表示される WSCONTEXT 値を書き留めておきます。GPO を使用してエンドポイントを分散する場合、配備スクリプトでこの値を使用し、Web Endpoint ユーザーが組織に正しく関連付けられるようにします。*Web Endpoint for Windows の手動でのインストール、398 ページ* を参照してください。

     使用しているクライアント コンピュータに適したエンドポイントのバージョンを表示するには、**[View Web Endpoint Files（Web Endpoint ファイルを）]** をクリックします。クライアントのオペレーティング システムを選択し、次に、ダウンロードするエンドポイントのバージョンをクリックします。また、リリース ノートのリンクをクリックすることによって各バージョンのリリース ノートの PDF を表示することもできます。完了した時、**[Close]** をクリックします。

- エンドポイントをハイブリッド サービスから直接に Windows クライアントに配備するには、**[Deploy Web Endpoint from hybrid service proxies（Web Endpoint をハイブリッド サービス プロキシから配備する）]** にマークを付けます。

  エンドポイントを、ハイブリッド サービスによってフィルタリングする**すべてのユーザー**に配備するか、**オフサイトのユーザー**のみに配備するかを選択します。

  エンドポイントのダウンロードおよびインストール プロセスの始めにエンド ユーザーに対して表示されるカスタマイズされたメッセージを指定することができます。このメッセージは、ユーザーに対して、ダウンロードが会社によって承認されていることを保証するため、また、ユーザーが必要とする情報を提供するために使用できます。メッセージをカスタマイズするには、**[Advanced Settings（拡張設定）]** をクリックし、次に、組織名および表示するメッセージを入力します。エンドユーザーに何が表示されるかを確認するには、**[View Sample Page（サンプル ページを表示する）]** をクリックします。

  サンプル ページにはまた、ダウンロードの開始時にエンドユーザーの画面に常に表示されるデフォルトのテキストが含まれます。

4. ハイブリッド サービスから最新バージョンが入手可能になった時にクライアント コンピュータ上のすべてのエンドポイントに最新バージョンが配備されるようにするには、**[Automatically update endpoint installations when a new version is released（新しいバージョンがリリースされた時に自動的にエンドポイントを更新する）]** にマークを付けます。
5. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

Web Endpoint for Windows の手動でのインストール

Web Security Help | Web Security ソリューション | バージョン 7.8.x

GPO を通じた配備

Web Endpoint をグループ ポリシー オブジェクト（GPO）を通じて配備するには、以下の手順を実行します。

1. ドメイン コントローラで共有フォルダを作成し、その権限をリード オンリーに設定します。
2. テキスト エディタを使って共有フォルダの中にバッチ ファイル（例、**installwebep.bat**）を作成します。
3. バッチ ファイルに下記の **msiexec** コマンドを入力します。

   ```
   msiexec /package "\\<path> \Websense Endpoint.msi" /quiet
   /norestart WSCONTEXT=<value>
   ```

使用しているファイルでは下記の項目に代入します。

- <path> に Websense Endpoint.msi ファイルへの実際のパスを代入
- <value> に [Settings] > [Hybrid Configuration] > [Hybrid User Identification] ページに表示される WSCONTEXT 文字列を代入

4. ファイルを保存して、閉じます。
5. Group Policy Management Console（GPMC）を開き、ユーザーのコンピューター アカウントが常駐している OU のために新しい GPO を作成するか、既存の GPO を開きます。新しい GPO を作成するには、以下の手順を実行します。
   a. コンソール ツリーで、グループ ポリシー オブジェクト（GPO）を作成するフォレストおよびドメインで [Group Policy Objects（グループ ポリシー オブジェクト）] を右クリックします。
   b. **[New]** をクリックします。
   c. [New GPO] ダイアログ ボックスで、新しい GPO の名前を指定してから **[OK]** をクリックします。
6. **[Computer Configuration] > [Windows Settings] > [Scripts（スクリプト）]** に移動し、右側のパネルで **[Startup（スタートアップ）]** をクリックします。
7. **[Add]** をクリックします。
8. [Script Name（スクリプト名）] フィールドにステップ 2 で作成したバッチファイルの完全なネットワーク パスとファイル名を入力し、次に **[OK]** をクリックして GPMC を閉じます。
9. コマンド プロンプトから **gpupdate /force** コマンドを実行し、グループ ポリシーを更新します。

アプリケーションはスタートアップ時にインストールされます。リブートが行われるまで、クライアントは完全には機能しないことがあります。

1 台のコンピュータへの配備

1. エンドポイント クライアントのインストール ファイルをクライアント コンピュータ上の一時フォルダにコピーし、ファイルを解凍します。
2. コマンド プロンプトを開き、次に、解凍したエンドポイント クライアント ファイルの保存場所に移動します。
3. 次のコマンドを入力します：

   ```
   msiexec /package "Websense Endpoint.msi" /norestart
   WSCONTEXT=xxxx
   ```

   [xxxx] には Web Security manager の [Settings] > [Hybrid Configuration] > [Hybrid User Identification] ページに示している一意な設定コードを代入します。このコードは **GPO コマンド**文字列の一部として示されます。

Web Endpoint for Mac OS X の手動でのインストール

Web Security Help | Web Security ソリューション | バージョン 7.8.x

1. Web Security manager を通じてインストール パッケージをダウンロードし（*Web Endpoint の配備の概要、395 ページ*を参照）、ファイルを以下のコンピュータにコピーします。
   - Web Endpoint をインストールするコンピュータ
   - Web Endpoint を他の Mac クライアントに配備するために使用するコンピュータ
2. クライアント ソフトウェアをインストールするには、下記の手順のどれかを使用します。
   - Apple Remote Desktop を使ってファイルを他の Mac クライアントに配備する。
   - ダウンロードした endpoint パッケージをダブルクリックしてインストーラを起動する。

endpoint クライアント ソフトウェアをインストールするには管理者権限が必要です。

Websense Directory Agent

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Web Security Gateway Anywhere 環境では、ハイブリッド サービスを通じてユーザー、グループ、およびドメイン（OU）ベースのポリシーの実施を有効化するためには、**Websense Directory Agent** という相互運用性コンポーネントが必要です。

下記との通信に使用できるコンピュータ上に Directory Agent がインストールされていなければなりません。

- サポートされている LDAP ベースのディレクトリ サービス（Windows Active Directory [ネイティブ モード]、Oracle Directory Server、または Novell eDirectory）

  組織が Windows Active Directory を混合モードで使用している場合、ユーザーおよびグループ データを収集してハイブリッド サービスへ送信することはできません。
- Websense Sync Service

Directory Agent は、他の Websense コンポーネント（Sync Service、User Service など）と同じコンピュータ上にインストールできます。

配備後に、Web Security manager を使用して Directory Agent がご使用のディレクトリ サービスからデータを収集するように設定します（*ユーザーおよびグループ データをハイブリッド サービスに送信、280 ページ*を参照）。設定後、Directory Agent はご使用のディレクトリ サービスからユーザーおよびグループ データを収集し、それを LDIF フォーマットで Sync Service に送信します。

Sync Service は、スケジュール設定された間隔で（*ハイブリッド サービスとの通信のスケジュール設定、290 ページ*を参照）、Directory Agent によって収集されたユーザーおよびグループ情報をハイブリッド サービスに送信します。Sync Service は大きなファイルを圧縮してから送信します。

Directory Agent と User Service

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ハイブリッド ユーザーの識別、391 ページ*
- *ユーザーおよびグループの処理、92 ページ*
- *ディレクトリ サービス、93 ページ*
- *ユーザーおよびグループ データをハイブリッド サービスに送信、280 ページ*

Directory Agent はディレクトリ情報を独自で収集しますが、User Service に対して 1 つの重要な依存関係があります。インストール時に Directory Agent は User Service に関連付けられている Policy Server インスタンスに接続しなければなりません。Directory Agent はこの User Service インスタンスが使用するように設定されているディレクトリとのみ通信するように設定できます。

つまり、分散環境で、複数のポリシー サーバーが存在し、それぞれが User Service に関連付けられていて、User Service のインスタンスが異なるディレクトリ サーバーに接続する場合、Directory Agent を、その User Service がハイブリッド ユーザー識別に使用するディレクトリに接続しているポリシー サーバーと関連付けなければなりません。

- Directory Agent の複数のインスタンスを実行することができます。
- 各 Directory Agent インスタンスを異なる Policy Server に関連付ける必要があります。
- すべての Directory Agent インスタンスは 1 つの Sync Service に接続する必要があります（1 つの配備には 1 つの Sync Service インスタンスのみを含めることができます）。

  すべての追加的な Directory Agent インスタンスのために Sync Service 接続を手動で設定しなければなりません。（Directory Agent インスタンスに対して Sync Service と同じ Policy Server に接続する通信が自動的に設定されます。）そのために以下の手順を実行します。

  1. TRITON コンソールにログオンする時に、設定する Directory Agent に適当な Policy Server インスタンスを選択します。
  2. [Settings] > [Hybrid Configuration] > [Shared User Data（共有ユーザー データ）] ページへ移動します。

3. [Synchronize User Data（ユーザー データの同期化）] の下で、Sync Service コンピュータの**名前または IP アドレス**、および Sync Service 通信に使用する **ポート**（デフォルトは 55832）を確認します。
4. **[Test Connection（テスト接続）]** をクリックして、Directory Agent が Sync Service にデータを送信できることを確認します。テストには 1 分以上かかることがあります。
   - 接続が確立すると、成功したことを知らせるメッセージが表示されます。
   - 接続ができなかった場合は、Sync Service コンピュータの IP アドレスまたはホスト名および通信ポートを確認してください。また、Sync Service コンピュータが稼働中で、ネットワークのファイアウォールが Sync Service ポート上の接続を許可していることを確認します。
5. **[OK]** をクリックして変更をキャッシュし、**[Save and Deploy]** をクリックしてそれらの変更を適用します。

サポートされている User Service 設定がない間は、Directory Agent の設定は実行できません。また、User Service 設定を変更するために Directory Agent 設定も更新する必要があるかも知れません。

- User Service の設定は、[Settings] > [General] > [Directory Services] ページで行います（*ユーザーおよびグループの処理*、92 ページを参照）。
- Directory Agent の設定は、[Settings] > [Hybrid Configuration] > [Shared User Data] ページで行います（*ユーザーおよびグループ データをハイブリッド サービスに送信*、280 ページを参照）。

Directory Agent が User Service とは異なる root コンテクストを使用し、そのディレクトリ データを User Service とは異なる方法で処理するように設定できます。また、Windows Active Directory では User Service が複数のグローバル カタログ サーバーと通信するように設定されている場合、Directory Agent はそれらのすべてと通信できます。

複数の Directory Agent インスタンスがある場合、各インスタンスは一意な、重複しない root コンテクストを使用する必要があります。

ユーザーが識別されない時

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ハイブリッド ユーザーの識別*、391 ページ
- *ハイブリッド サービス クライアントの処理*、109 ページ

Directory Agent、Web Endpoint を配備しない場合、もしくはユーザー識別を無効化している場合、ユーザーに対して 3 つのタイプのポリシーだけが適用可能です。

- ユーザーが接続に使用している外部 IP アドレスに対して適用されるポリシー。

  この IP アドレスはフィルタリングされている場所として定義されていなければなりません。
- 要求がフィルタリングされている場所の外から発信されている、またはフィルタリングされている場所にコンピュータまたはネットワーク ポリシーが適用されていない場合、組織のデフォルト ポリシー。
- ユーザーの接続を組織と関連付けられない場合、ハイブリッド サービスのデフォルト ポリシー。

  これは稀なケースであり、ハイブリッド サービス アカウントに設定の問題がある場合にのみ起こります。

ユーザーおよびグループ ポリシーは、自己登録されたユーザーには適用できません。自己登録されたユーザーは常にデフォルト ポリシーによってフィルタリングされます（*オフサイト ユーザーの自己登録*、310 ページを参照）。

15 代理管理およびレポート作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

代理管理は、Web Securit 構成設定、インターネット アクセス管理、ポリシー管理、レポート作成、およびコンプライアンス監査の責務を複数の個人に配分する効果的方法です。例：

- 各チーム内のユーザーについて個々のマネージャによるポリシーの設定とレポートの実行を可能にします。
- 地域事業所またはキャンパスのローカル管理者に対してポリシー管理許可とローカル構成設定オプションへの部分的アクセスを付与しますが、エンドユーザーのプライバシー保護のためにレポート作成アクセスを制限します。
- ユーザー名または IP アドレスにより識別されるクライアントの一部またはすべてについて、人事部がインターネット アクティビティ レポートを実行できるようにします。
- 変更を保存する権限なしに、Web Security manager のすべての構成設定およびポリシー管理画面を表示するアクセス許可を監査者に付与します。

以下のセクションで代理管理の主要な概念について詳しく説明し、つづいて個別の設定および実装上の手順について説明します。

代理管理の基本

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連トピック：
- *代理管理ロール*、406 ページ
- *代理管理者*、407 ページ
- *代理管理およびレポート作成の許可*、409 ページ
- *複数のロールの管理者*、413 ページ
- *複数の管理者による TRITON コンソールへのアクセス*、414 ページ

お客様の組織で代理管理をセットアップする前に、下記の 3 つの主要概念を理解する必要があります：

- **ロール**は、**管理者**とクライアントをグループとしてまとめるコンテナーです。3 種類のロールがあります。*代理管理ロール*、406 ページを参照してください。
- **管理者**は、Web Security manager 設定の構成、クライアントに対するポリシーの管理、インターネット アクティビティ レポートの実行、システムの監査などの責務を与えられた個人またはグループです。管理者の設定の責務は、管理者に割り当てられる**ロール**と**許可**によって定められます。*代理管理者*、407 ページを参照してください。
- **許可**は、**管理者**が特定の**ロール**内で付与される責務（ポリシーの作成やレポートの実行など）を決定します。利用できる許可は、管理者に割り当てられるロールの種類によって異なります。*代理管理およびレポート作成の許可*、409 ページを参照してください。

代理管理ロール

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ロールは、クライアント（ユーザー、グループ、ドメイン（OU）、コンピュータ、およびネットワーク）を 1 人以上の管理者のもとでグループにまとめます。

- 代理管理ロール中のクライアントのことを**処理対象クライアント**と言います。
- 管理者は、保持している**許可**に基づいて、そのロール中の処理対象クライアントについて様々なタスク（ポリシーの管理やレポートの実行など）を遂行することができます。

Web Security manager には、事前定義のロールとして Super Administrator（優先管理者）があります。明示されていませんが、**admin**（Global Security Administrator（グローバル セキュリティ管理者）アカウント）はこのロールのメンバーです。admin アカウントは削除できないし、またその許可を変更することもできません。

> **重要**
> Super Administrator ロールまたは admin アカウントの削除はできません。

Super Administrator ロールに割り当てられている管理者は、ロールを作成し、管理者と処理対象クライアントをロールに割り当て、ロール中の管理者の許可を決めることができます。Global Security Administrator（グローバル セキュリティ管理者）は Super Administrator ロールに管理者を追加することができます。

Super Administrator は、下記のような 2 つの代理管理およびレポート作成ロールを作成することができます：

- **Policy management and reporting（ポリシー管理およびレポート作成）**：ユーザー ポリシーは、このロールの管理者によって管理されます。このロールの管理者は、オプションとしてレポートを実行することもできます。
- **Investigative reporting（調査レポート作成）**：管理者は、ロール中の処理対象クライアントについてだけ、インターネット アクティビティを示す調査レポートを実行することができます。クライアント ポリシーは 1 つ以上の他のロールで管理されます。

お客様の組織で必要とされる数のロールを作成してください。例：

- 部門のマネージャーを管理者とし、部門のメンバーを処理対象クライアントとするロールを各部門ごとに作成することができます。
- 地理的に分散している組織では、所在地ごとにロールを作成し、その所在地のすべてのユーザーをそのロールの処理対象クライアントにすることができます。そして、その所在地の 1 人以上の個人を管理者に割り当てます。

代理管理者

Web Security Help | Web Security ソリューション | バージョン 7.8.x

管理者は TRITON コンソールににアクセスできる個々人です。それぞれの許可によって異なりますが、Web Security manager では管理者は下記のようなことができます：

- ログオンして、Web Security Dashboard の一部の要素を表示できますが、その他のアクションはできません。

- Web Security manager のすべての構成設定および管理の機能にアクセスできますが、変更の保存はできません。
- 特定のグループまたはすべてのクライアントについてレポートを実行することができます。
- クライアントの特定のグループについてポリシーを管理することができます。
- Web Security manager のすべての機能に対する完全な構成設定アクセス権を保持しています。

利用できる個々の許可は、管理者ロールのタイプ（Super Administrator、ポリシー管理およびレポート作成、または調査レポート作成）によって異なります。*代理管理ロール、406 ページ*を参照してください。

Global Security Administrator（グローバル セキュリティ管理者）は、**admin** 同様に、TRITON Settings（TRITON 設定）で管理者アカウントを作成します。これらのアカウントは、ネットワーク ログオン アカウント（サポートされているディレクトリ サービスで定義されます）か、または TRITON へのアクセス専用のローカル アカウントのどちらかです。アカウントが作成されると、Global Security Administrator は 1 つ以上の TRITON モジュールへのログオン アクセスのレベルをアカウントに割り当てます。

管理者に付与できる Web Security アクセスのレベルは下記のとおりです：

- **Access and account management（アクセスおよびアカウント管理）**- これは無制限 Super Administrator 許可を付与します（*代理管理およびレポート作成の許可、409 ページ*を参照してください）。
- **Access（アクセス）**- これは、管理者がログオンして、[Status（ステータス）] > [Dashboard（ダッシュボード）] および [Alerts（アラート）] ページの限られた部分だけを表示することを可能にします。Super Administrator は、これらの管理者に対して、若干のレベルのポリシー管理アクセスまたはレポート作成アクセス、もしくはその両方を可能にするロールを追加的に付与することができます。

Web Security モジュールへのアクセス権を付与されている管理者アカウントは、[Delegated Administration（代理管理）] > [View Administrator Accounts（管理者アカウントの表示）] ページで示されます。これらのアカウントは、[Delegated Administration] > [Edit Role（編集ロール）] > [Add Administrators（管理者の追加）] ページでもリストされます。

ロールに追加できるのは、[TRITON Settings] で Web Security アクセス権をすでに付与されている管理者だけです。

代理管理およびレポート作成の許可

Web Security Help | Web Security ソリューション | バージョン 7.8.x

管理者が利用できる許可は、その管理者が Super Administrator ロール、ポリシー管理およびレポート作成ロール、または調査レポート作成ロールのどれに割り当てられているかによって異なります。

Super Administrator 許可

Super Administrator ロールには 2 つのタイプの管理者 - 無制限 Super Administrator と条件付き Super Administrator - が含まれます。

[TRITON Settings] > [Administrators（管理者）] ページで Global Security Administrator アカウントを作成するか、または **[Web Security] > [Grant access and the ability to modify access permissions for other accounts（アクセス許可と他のアカウントのアクセス許可を変更する権限を付与する）]** オプションを選択すると、そのアカウントは無制限の許可を保持するものとして Web Security manager の Super Administrator ロールに自動的に追加されます。

無制限 Super Administrator は下記のことができます：

- （[Settings（設定）] タブで管理される）Websense Web セキュリティ ソリューションのすべてのシステム構成設定へのアクセス。
- Super Administrator ロールへの管理者の追加とそこからの管理者の除去。
- 代理管理ロールによって管理されるすべてのユーザーについて特定のカテゴリとプロトコルをブロックする Filter Lock（フィルタ ロック）の作成と編集。*Filter Lock（フィルタ ロック）の作成*、416 ページを参照してください。
- Super Administrator ロール中のクライアントについてのポリシーの管理 - これには、いかなるロールでも別のポリシーを割り当てられていないすべてのクライアントに適用される Default（デフォルト）ポリシーも含まれます。
- どのロールに割り当てられているかということは無関係に、すべてのクライアントについてのレポートの作成と実行。
- Real-Time Monitor（リアルタイム モニタ）へのアクセス。
- [Web Security manager] > [Deployment] ページからコンポーネントのステータスを検討し、コンポーネントを停止または起動する
- 管理者による Web Security manager へのアクセスとその内部でのアクションを記録する監査ログのレビュー。
- （*Web Security Gateway および Gateway Anywhere*）[Settings（設定）] > [General（一般）] > [Content Gateway Access] ページ上のボタンにより Content Gateway manager を開き、資格情報を提供せずに自動的にログオンすること。

無制限優先管理者が Web Security manager の [Policy Management（ポリシー管理）] > [Delegated Administration（代理管理）] ページで新しい管理者を優先管理者 ロールに追加すると、その管理者には条件付き許可が付与されます。

無制限 Super Administrator の許可は変更できませんが、条件付き Super Administrator には、ポリシー管理許可、レポート作成許可、およびアクセス許可の組み合わせを付与することができます。

- **Full policy（[Full] ポリシー）**許可により、条件付き Super Administrator は下記のことができます：
  - 代理管理ロール、フィルタ コンポーネント、フィルタ、ポリシー、および例外の作成と編集、そして他のいかなるロールによっても管理されていないクライアントに対するポリシーの適用。
  - データベース ダウンロード、ディレクトリ サービス、ユーザー識別、および Network Agent 構成設定へのアクセス。レポート作成許可を持っている条件付き Super Administrator はレポート作成ツールの構成設定にアクセスすることもできます。
  - 代理管理ロールの作成と編集 - しかしロールの削除、または管理者の除去もしくは管理者に割り当てられている処理対象クライアントの除去はできません。
- **Exceptions only（例外のみ）**許可により、Super Administrator は例外を作成し、編集することができます。（個々のユーザーのインターネット アクセスで、通常、適用されるポリシーとは無関係に、例外は特定のユーザーについて URL を許可またはブロックします。）

  ポリシー、フィルタ、フィルタ コンポーネント、Filter Lock, およびすべての [Settings（設定）] ページは、例外のみ許可の Super Administrator には表示されません。
- **Reporting（レポート作成）**許可により、条件付き Super Administrator は下記のことができます：
  - Web Security Dashboard（Web Security ダッシュボード）グラフへのアクセス。
  - すべてのユーザーについて調査レポートとプレゼンテーション レポートの実行。

  管理者がレポート作成許可のみ付与されている場合、Check Policy（ポリシーの確認）ツールは、[Toolbox（t ツールボックス）] に表示されません。
- **Real-Time Monitor（リアルタイム モニタ）**許可により、優先管理者 は Web Security manager と関連付けられている各 Policy Server のすべてインターネット アクティビティをモニタすることができます。
- **Content Gateway direct access（Content Gateway 直接アクセス）**許可により、優先管理者 は Web Security manager の [Settings] > [General] > [Content Gateway Access（Content Gateway アクセス）] ページのボタンで Content Gateway Manager に自動的にログオンできます。

[Full] ポリシー許可または**例外のみ**許可を持つ管理者がロールにログオンできるのは、一度に 1 人だけです。したがって、ある管理者が Super Administrator ロールにログオンしてポリシーまたは構成設定タスクを行っていると、他の Super Administrator はロール中のレポート作成許可、監査者許可、またはモニタ許可だけをもってしかログオンできません。Super Administrator には、管理タスクのために別のロールを選択するオプションもあります。

ログオン後に別のロールに切り替える ためには、Web Security ツールバーの **[Role（ロール）]** ドロップダウン リストに移り、ロールを選択します。

ポリシー管理およびレポート作成の許可

ポリシー管理およびレポート作成ロールの代理管理者には、下記の許可の任意の組み合わせを付与することができます：

- **Full policy（[Full] ポリシー）**許可により、代理管理者はその管理対象クライアントについてフィルタ コンポーネント（カスタム カテゴリと再分類 URL を含みます）、フィルタ（カテゴリ、プロトコル、および制限付きアクセス）、ポリシー、例外（ブラックリストとホワイトリスト）を作成し、管理することができます。

  代理管理者によって作成されたフィルタは、一部のカテゴリとプロトコルを**ブロックおよびロック**に指定することができる Filter Lock により制限されます。代理管理者は、このようなカテゴリとプロトコルを許可することはできません。（フィルタ ロックの適用の一環として、代理管理者は、その管理対象のクライアントに対してパスワード無効化許可を与えることができません）。

  ポリシー許可を持つ管理者がロールにログオンできるのは、一度に 1 人だけです。したがって、管理者がロールにログオンしてポリシー タスクを行っていると、そのロールの他の管理者は監査者許可（読み取り専用）、レポート作成許可、または Real-Time Monitor 許可だけをもってしかログオンできません。複数のロールに割り当てられている管理者には、管理タスクのために別のロールを選択するオプションもあります。

  ログオン後に別のロールに変更するには、バナーの **[Role]** ドロップダウン リストに移り、ロールを選択します。

- **Exceptions only（例外のみ）**許可により、管理者はそのロールの管理対象クライアントについて例外を作成し、管理することができます。（個々のユーザーのインターネット アクセスで、通常、適用されるポリシーとは無関係に、例外は特定のユーザーについて URL を許可またはブロックします。）

  ポリシー、フィルタ、およびフィルタ コンポーネントは、例外のみ許可の代理管理者には表示されません。

- **配備ステータス**許可により、代理管理者は、[Status] > [Deployment] ページでコンポーネントのステータスを検討できます。配備ステータス許可を持つ代理管理者は、コンポーネントの起動、停止、またはその両方を行う許可を与えられることもあります。
- レポート作成許可は、2 つの一般的カテゴリ - **すべてのユーザー**についてのレポート、または当該ロール中の**処理対象クライアントだけ**についてのレポート - のどちらかで付与することができます。
  - レポート作成許可を持つ代理管理者に対して、Web Security Dashboard および調査レポートへのアクセス権と Log Server および Log Database 管理のために使用する [Settings] ページへのアクセス権を付与することができます。
  - すべてのクライアントについてレポート作成オプションを持つ代理管理者に対して、プレゼンテーション レポートへのアクセス権を付与することができます。
- **Real-Time Monitor** 許可により、管理者は Web Security manager と関連付けられている各 Policy Server のすべてインターネット アクティビティをモニタすることができます。

調査レポート作成許可

調査レポート作成ロール中の管理者は、自身のロールの処理対象クライアントについて調査レポートを作成することができます。（クライアントのポリシーは他のロールで管理されます）。このロールの管理者は、[URL Category（URL カテゴリ）]、[URL Access（URL アクセス）]、および [Investigate User（ユーザーの調査）] ツールを使用することもできます。

これらの管理者はプレゼンテーション レポートまたは Real-Time Monitor にアクセスできませんが、オプションとして Web Security Dashboard でグラフを表示することができます。

監査者

条件付き Super Administrator または代理管理者アカウントに **Auditor（監査者）**許可を付与することができます。監査者は、ほとんどの Web Security manager の特徴および機能を見ることができますが、変更を保存することはできません。

他の管理者が変更をキャッシュまたは破棄するために使用する [OK] および [Cancel（キャンセル）] ボタンは利用できず、監査者に提供されるのは [Back（戻る）] ボタンだけです。[Save and Deploy（保存と配備）] ボタンは無効です。

複数のロールの管理者

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *代理管理ロール、406 ページ*
- *代理管理者、407 ページ*
- *代理管理およびレポート作成の許可、409 ページ*

お客様の組織のニーズによっては、同じ管理者を複数のロールに割り当てることができます。複数のロールに割り当てられた管理者は、ログオン時に管理する 1 つのロールを選択しなければなりません。

ログオン後、許可は下記のようになっています：

- **ポリシー管理**：
  - **Full policy（[Full] ポリシー）**：ログオン時に選択したロールのフィルタとポリシーを追加および編集し、そのロールの処理対象クライアントにポリシーを適用することができます。
  - **Exceptions only（例外のみ）**：ログオン時に選択したロールの例外を追加および編集し、そのロールの処理対象クライアントに例外を適用することができます。
- **レポート作成**：すべてのロールの組み合わされたレポート作成許可を保持します。例えば、下記のようなレポート作成許可を持つ 3 つのロールに割り当てられているとします：
  - ロール 1：レポート作成なし
  - ロール 2：調査レポートのみ
  - ロール 3：すべてのクライアントについてのレポート、すべてのレポート作成機能への完全なアクセス

  この場合、ログオン時に選択したロールとは無関係に、Web Security Dashboard 上でグラフを表示することができ、また、すべてのレポート作成機能を使用して、すべてのクライアントについてレポートを作成することができます。

  レポート作成のみでログオンしている場合、[Full Reporting（完全レポート作成）]（すべてのクライアントに関するレポート）許可を持つか、または [Limited Reporting（制限付きレポート作成）]（処理対象クライアントのみに関するレポート）許可を持つかについて、バナー バーの [Role] フィールドで示されます。

複数の管理者による TRITON コンソールへのアクセス

Web Security Help | Web Security ソリューション | バージョン 7.8.x

異なるロールの管理者は、それぞれのロール許可が許容するどのような作業を行なうためにでも同時に Web Security manager にアクセスすることができます。各管理者はそれぞれ異なるクライアントを管理するので、競合なしにポリシーを作成し、適用することができます。

同じロールのポリシー許可を持つ複数の管理者が同時に接続しようとすると、状況は異なります。共有ロールで [Full] ポリシー許可または例外のみ許可を持つ管理者がログオンできるのは、**一度に 1 人だけ**です。共有ロールの別の管理者がログオンしているとき、第二の管理者が [Full] ポリシー許可または例外のみ許可をもってログオンしようとすると、その管理者に下記のような選択肢が与えられます：

- 読み取り専用アクセスによるログオン（一時的監査者許可に類似しています）。

  このオプションを選択すると、[Role] ドロップダウン ボックスで [Role Name（ロール名）- [Read-Only（読み取り専用）]] が現在のロールとして示され、[Role Name]（モディファイアなし）に切り替えるオプションが提供されます。これにより、共有ロールがもはやロックされていないとき、ポリシー許可をもってそのロールにアクセスすることが可能になります。
- レポート作成のみのログオン　-　管理者がレポート作成許可を持っている場合。
- 別のロールへのログオン - 管理者が他のロールに割り当てられている場合。
- [Status（ステータス）- ページのみを表示するためのログオン - 共有ロールが利用できるようになるまで（Limited Status（制限付きステータス）アクセス）。
- 再試行 - 最初の管理者がログオフした後で。

自分のポリシー許可を使用していない管理者は、下記のいずれかによって、共有ロールのロックを解除し、別の管理者がポリシー管理のためにログオンできるようにすることができます：

- レポートを生成する場合、**Role** ドロップダウン リストで **[Release Policy Permissions（ポリシー許可のリリース）]** を選択します。

  このオプションを選択すると、ポリシー管理機能はログオンしている管理者から隠されますが、レポート作成機能は有効なままです。
- システム パフォーマンスをモニタする場合、**[Role]** ドロップダウン リストで **[Status Monitor（ステータス モニタ）**を選択します。

  Status Monitor モードの管理者は [Status] > [Dashboard] および [Alerts] ページと [Real-Time Monitor] ページ（可能であれば）にアクセスすることができます。このセッションはタイムアウトしません。

Status Monitor モードの管理者が [Dashboard]、[Alerts]、または [Real-Time Monitor] 以外のページにアクセスしようとすると、再度のログオンが求められます。

代理管理の準備

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *代理管理の基本*、406 ページ
- *Filter Lock（フィルタ ロック）の作成*、416 ページ
- *代理管理者の準備*、419 ページ
- *代理管理者ロールの管理*、420 ページ

代理管理ロールを作成する前に、優先管理者が行うべき計画およびセットアップ上の 2 つの重要なタスクがあります：

- すべての代理管理ロールの処理対象クライアントで特定のカテゴリとプロトコルをブロックする Filter Lock を確認し、編集します。デフォルトでは Filter Lock はいくつかのカテゴリをブロックおよびロックするので、お客様の組織の必要に基づいてデフォルトの設定をチェックすることが重要です。（*Filter Lock（フィルタ ロック）の作成*、416 ページを参照してください。）
  - Filter Lock の制限は、代理管理ロールで作成されたか、またはそこにコピーされたすべてのフィルタに自動的に適用され、代理管理者はこの制限を変更できません。
  - 代理管理者が処置を適用できるのは、Filter Lock でブロックおよびロックされて**いない**カテゴリとプロトコルに対してです。
  - Filter Lock に対する変更が保存されると、その変更がすべての処理対象クライアントでただちに適用されます。この変更が有効になったとき Web Security manager で作業していた代理管理者は、次にログオンするまで自分のフィルタの変更を知ることができません。
  - Filter Lock の制限は、Super Administrator ロールによって管理されているクライアントには適用されません。
- これから作成される個々の新しいロールにコピーすべき Super Administrator ポリシーおよびフィルタを決定し、必要に応じて既存のポリシーとの関係で調整します。
  - デフォルトでは、各ロールは単一の Default（デフォルト）ポリシーをもって作成されますが、このポリシーは Super Administrator ロールのために現在設定されている Default のカテゴリおよびプロトコル フィルタ（Default ポリシーでは**ありません**）から作成されています。

- オプションとして、Super Administrator ロールからすべてのポリシー オブジェクト（ポリシー、フィルタ、カスタム カテゴリ、およびカスタム URL）を新しいロールにコピーすることもできます。次に、代理管理者はポリシーおよびポリシー コンポーネントの完全なセットをもって始めます。
  - 代理管理者ロール中のポリシーおよびフィルタのコピーは Filter Lock によって制約されるので、これらは Super Administrator ロール中の同じポリシーおよびフィルタと同一ではありません。
  - Unrestricted（制約なし）ポリシーがコピーされると、ポリシー**および**フィルタの名前は、それらが Filter Lock に制約され、すべての要求を許可しなくなっているという事実を反映するように変更されます。

  Super Administrator ポリシー オブジェクトの新しいロールへのコピーは、コピーされる情報の量によっては、非常に長時間かかることがあります。

これらのプランニング手順が完了したら、下記の代理管理コンポーネントの作業を行います：

1. Global Security Administrator が [TRITON Settings（TRITON 設定）] > [Administrators（管理者）] ページで管理者アカウントを作成し、そのアカウントに適切なレベルの Web Security アクセス権を付与します。
2. Super Administrator が [Policy Management（ポリシー管理）] > [Delegated Administration（代理管理）] ページで代理管理ロールを作成し、そのロールに管理者と処理対象クライアントを追加します。*代理管理者ロールの管理*、420 ページを参照してください。
3. 優先管理者は代理管理者に対して、Web Security manager への管理アクセス権が付与されたことを通知し、その許可のレベルについて説明します。*代理管理者の準備*、419 ページを参照してください。

Filter Lock（フィルタ ロック）の作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *カテゴリのロック*、417 ページ
- *プロトコルのロック*、418 ページ

[Policy Management] > [Filter Lock] ページで、代理管理者ロール中のすべての処理対象クライアントでブロックされるカテゴリとプロトコルを指定することができます。Filter Lock でブロックされるカテゴリまたはプロトコルは、**ブロックおよびロック**されていると見なされます。

- **[Categories（カテゴリ）]** ボタンをクリックして、特定のカテゴリまたはカテゴリ要素（キーワードおよびファイル タイプ）をブロックおよびロックします。*カテゴリのロック、417 ページ*を参照してください。
- **[Protocols（プロトコル）]** ボタンをクリックして、プロトコルをブロックおよびロックするか、または常にログ記録されるプロトコルを指定します。*プロトコルのロック、418 ページ*を参照してください。

カテゴリのロック

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Filter Lock（フィルタ ロック）の作成、416 ページ*
- *プロトコルのロック、418 ページ*

[Policy Management] > [Filter Lock] > [Categories] ページを使用して、代理管理ロールのすべてのメンバーでブロックおよびロックするカテゴリを選択します。また、カテゴリのキーワードとファイル タイプをブロックおよびロックすることもできます。

1. ツリーでカテゴリを選択します。

   代理管理ロールでは、Super Administrator によって作成されたカスタム カテゴリへのアクセスはできません。したがって、カスタム カテゴリは このツリーで表示されません。
2. カテゴリ ツリーの横に表示されるボックスで、このカテゴリの制限を設定します。

オプション	説明
Lock category（カテゴリのロック）	このカテゴリのサイトへのアクセスをブロックおよびロックします。
Lock keywords（キーワードのロック）	各ロール中のこのカテゴリについて定義されたキーワードに基づくアクセスをブロックおよびロックします。
Lock file types（ファイル タイプのロック）	このカテゴリ中のサイトについて選択されたファイル タイプをブロックおよびロックします。 ブロックおよびロックされるべき各ファイル タイプのチェックボックスをオンにします。 Super Administrator によって作成されたカスタム ファイル タイプは代理管理ロールで利用できるため、それらのカスタム ファイル タイプはこのリストに含まれます。
Apply to Subcategories（サブカテゴリに適用）	このカテゴリのすべてのサブ カテゴリに同じ設定を適用します。

適切であるなら、すべてのカテゴリで選択された要素を同時にブロックおよびロックすることができます。ツリーで **[All Categories（すべてのカテゴリ）]** を選択し、すべてのカテゴリでブロックされる要素を選択します。つづいて **[Apply to Subcategories（サブカテゴリに適用）]** をクリックします。

3. 変更を終了したら、**[OK]** をクリックして、変更をキャッシュし、[Filter Lock] ページに戻ります。**[Save and Deploy（保存と配備）]** をクリックするまで変更は適用されません。

プロトコルのロック

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Filter Lock（フィルタ ロック）の作成、416 ページ*
- *カテゴリのロック、417 ページ*

[Policy Management] > [Filter Lock] > [Protocols] ページを使用して、代理管理ロールで管理されるすべての管理クライアントについて選択されたプロトコルへのアクセスをブロックおよび ロックするか、それらのプロトコルのログ記録をロックします。

注意

プロトコルのログ記録は、プロトコル使用状況アラートと関連付けられています。プロトコルが少なくとも 1 つのプロトコル フィルタでログ記録に設定されていないと、そのプロトコルについて使用状況アラートを生成することはできません。Filter Lock により **[Lock protocol logging（プロトコル ログ記録のロック）]** オプションを有効にすると、プロトコルの使用状況アラートが生成されます。*プロトコル使用状況アラートの設定、487 ページ*を参照してください。

1. ツリーでプロトコルを選択します。

   代理管理ロールから、Super Administrator によって作成されたカスタム プロトコルへアクセスすることができます。したがって、カスタム プロトコルは このツリーで表示されます。

2. プロトコル ツリーの横に表示されるボックスで、このプロトコルの制限を設定します。

オプション	説明
Lock protocol（プロトコルのロック）	このプロトコルを使用するアプリケーションおよびウェブサイトへのアクセスをブロックおよびロックします。
Lock protocol logging（プロトコル ログ記録のロック）	このプロトコルへのアクセス情報をログ記録し、代理管理者がログ記録を無効にすることを防止します。
Apply to Group（グループに適用）	同じ設定をグループのすべてのプロトコルに適用します。

変更を終了したら、**[OK]** をクリックして、変更をキャッシュし、[Filter Lock] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

代理管理者の準備

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：
- *代理管理の基本*、406 ページ
- *代理管理の準備*、415 ページ
- *代理管理者タスクの実行*、435 ページ

個人をいずれかの管理ロールの管理者として割り当てたたら、彼らに下記の情報を通知してください：

- TRITON コンソールにログオンするための URL。デフォルトでは：

  ```
  https://<TRITON_location> :9443/triton/
  ```

  TRITON 管理サーバーの IP アドレスまたはホスト名を入力します。
- ログオン後に選択すべき Policy Server（該当する場合）。複数の Policy Server インスタンスがインストールされている環境では、管理者は使用する Policy Server を Web Security ツールバーで選択することができます。管理者は、その処理対象クライアントを認証するディレクトリ サービスと通信するように設定されている Policy Server を選択しなければなりません。
- TRITON コンソール にログオンするとき使用するのは、ネットワーク ログオン アカウント またはローカル Websense アカウントのどちらかです。管理者がローカル アカウントでログオンする場合、ユーザー名とパスワードを提供します。

- 管理者の許可：ロール中のクライアントに対するポリシーの作成と適用、レポートの生成、ポリシーの作成とレポートの生成、または変更を適用せずに管理者タスクを監査するための許可。

  ポリシーとレポート作成の両方の許可を持つ管理者に対して、セッション中にどのような活動を行なうつもりか考えるようにアドバイスします。レポートを作成することのみを計画している場合は、バナーの **[Role（ロール）]** フィールドに移り、**[Release Policy Permissions（ポリシー許可のリリース）]** を選択するよう推奨します。これによってロールのポリシー許可が解放され、他の管理者が Web Security manager にアクセスし、当該のロールのポリシーを管理できるようになります。
- ロールによる処理対象のクライアントのリストを見つける方法。管理者は [Policy Management] > [Delegated Administration] に移り、つぎにそのロール名をクリックして、処理対象クライアントのリストを含んでいる [Edit Role（ロールの編集）] ページを表示することができます。
- カテゴリまたはプロトコルがブロックおよびロックされている場合、Filter Lock によって適用されている制限。
- 管理者によって遂行される一般的なタスク*代理管理者タスクの実行*、435 ページを参照してください。

カスタム ファイル タイプおよびプロトコルを追加または変更したときは、代理管理者に必ず通知します。これらのコンポーネントはすべてのロールのフィルタおよびポリシーで自動的に表われます。したがって、管理者にとって、変更がいつ行われたかを知ることは重要です。

代理管理者ロールの管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *代理管理の基本*、406 ページ
- *代理管理の準備*、415 ページ
- *ロール競合の管理*、431 ページ

優先管理者または代理管理者のどちらが表示しているかによって、**[Policy Management] > [Delegated Administration]** ページは異なるオプションを提供します。

Super Administrator は、現在定義されているすべてのロールのリストを参照することができるし、また下記のオプションを利用することができます。

オプション	説明
Add（追加）	これをクリックして、新しいロールを追加します。*ロールの追加*、422 ページを参照してください。
Role（ロール）	ロール名をクリックして、ロールを表示するか、またはその設定を行います。*ロールの編集*、423 ページを参照してください。
Delete（削除)	ロール名の横のチェックボックスをオンにし、つづいてボタンをクリックして、選択されているロールを削除します。利用できるのは無制限 Super Administrator だけです。 ロールの削除後、そのロールのクライアントを管理する方法については、*ロールの削除*、433 ページを参照してください。
Advanced（詳細）	これをクリックして、[Manage Role Priority（ロールの優先順位の管理）] 機能にアクセスします。
Manage Role Priority（ロールの優先順位の管理）	これをクリックすることで、異なるロールによって管理される複数のグループに同じクライアントが属している場合に使用すべきロールのポリシー設定を指定します。*ロール競合の管理*、431 ページを参照してください。
View Administrator Accounts（管理者アカウントの表示）	これをクリックして、Web Security manager へのアクセス権を持つローカルおよびネットワーク管理者アカウントを表示し、その許可レベルとロール割り当てを確認します。*管理者アカウントのレビュー[かんりしゃあかうんとのれびゅー]*、440 ページを参照してください。

代理管理者は自身が管理者であるロールだけを表示でき、アクセスできるオプションも限定されています。

オプション	説明
Role（ロール）	これをクリックして、ロールに割り当てられているクライアントと付与されているレポート作成許可を表示します。*ロールの編集*、423 ページを参照してください。

ロールの追加

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *代理管理の準備*、415 ページ
- *代理管理者ロールの管理*、420 ページ
- *ロールの編集*、423 ページ

[Delegated Administration] > [Add Role（ロールの追加）] ページを使用して、新しいロールの名前と説明を指定します。

1. 新しいロールの **[Name（名前）]** を入力します。

   名前は 1 ～ 50 文字でなければならず、また下記の文字を含むことはできません：

   ```
   * < > ' { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   ロール名にスペースとダッシュを含めることができます。
2. 新しいロールの **[Description（説明）]** を入力します。

   説明は 255 文字までです。ポリシー名に適用される使用文字の制限は説明にも適用されますが、2 つの例外があります：説明では、ピリオド（.）とカンマ（,）が使用できます。
3. **[Role Type（ロールのタイプ）]** を指定します：
   - **[Policy management and reporting（ポリシー管理およびレポート作成）]** ロールによって、管理者はフィルタとポリシーを作成し、それらを適用してクライアントを管理することができます。これらのロールの管理者には、処理対象クライアントまたはすべてのクライアントについてレポートする許可を付与することもできます。

     このロール タイプを選択すると、**[Copy all Super Administrator policies, filters, and filter components to the new role（すべての Super Administrator ポリシー、フィルタ、およびフィルタ コンポーネントを新しいロールにコピーする）]** を選択するかどうか指示しなければなりません。このオプションを選択すると、ロールを作成するプロセスは数分かかるでしょう。

     すべての Super Administrator ポリシーを新しいロールにコピーしない場合、Super Administrator の Default（デフォルト）カテゴリおよびプロトコル フィルタを適用する Default ポリシーがロールのために作成されます。

- **[Investigative reporting（調査レポート作成）]** ロールによって、管理者は、調査レポート ツールを使用して、その処理対象クライアントについてのみレポートすることができます。調査レポート作成ロールの処理対象クライアントをポリシー管理およびレポート作成ロールに追加することもできます。

4. **[OK]** をクリックして、**[Edit Role（ロールの編集）]** ページを表示し、このロールの特性を定義します。*ロールの編集、423 ページ*を参照してください。
   - ポリシー管理およびレポート作成ロールを作成したら、次のログオン時に、新しいロールが Web Security ツールバーの [Role（ロール）] ドロップダウン リストに追加されます。
   - 調査レポート作成ロールに作成した場合、その名前はロール ドロップダウン リストで表示されません。このことは、レポート作成許可が累積的であることを反映しています（*複数のロールの管理者、413 ページ*を参照してください）。

ロールの編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *代理管理者ロールの管理、420 ページ*
- *ロールの追加、422 ページ*
- *ロール競合の管理、431 ページ*

代理管理者は、**[Delegated Administration] > [Edit Role（ロールの編集）]** ページを使用して、そのロールの処理対象クライアントのリストと付与されているレポート作成許可を表示することができます。

Super Administrator は、このページを使用して、ロールの管理者とクライアントを選択し、管理者許可を設定することができます。無制限 Super Administrator だけがロールから管理者とクライアントを削除することができます。

1. 必要に応じて、ロールの **[Name（名前）]** と **[Description（説明）]** を変更します。

   Super Administrator ロールの名前は変更できません。

2. このロールの管理者を追加または除去します（優先管理者のみ）。

項目	説明
User Name（ユーザー名）	管理者のユーザー名。
Account Type（アカウント タイプ）	ユーザーがネットワーク ディレクトリ サービスで定義されているか（Directory（ディレクトリ））、または TRITON コンソールに固有のものであるか（Local（ローカル））のどちらであるかについて指示します。
Reporting（レポート作成）	レポート作成ツールを使用する管理者許可を付与します。
Real-Time Monitor	任意の Policy Server についてすべてのインターネット アクティビティをモニタする管理者許可を付与します。
Policy（ポリシー）	フィルタとポリシーを作成し、ロールの処理対象クライアントに対してポリシーを適用する管理者許可を付与します。 また Super Administrator ロールでは、ポリシー許可を持つ管理者は一部の Websense 構成設定を管理することができます。*Super Administrator 許可*、409 ページを参照してください。
Auditor（監査者）	ロール中の他の管理者が利用できるすべての機能を表示する管理者許可を付与します（この許可では変更を保存することはできません）。 Auditor 許可が選択されると、他の許可のチェックボックスは無効になります。
Add（追加）	**[Add Administrators（管理者の追加）]** ページを開きます。*管理者の追加*、428 ページを参照してください。
Delete（削除）	選択されている管理者をロールから除去します。 • 利用できるのは無制限 Super Administrator だけです。 • 無制限 Super Administrator アカウントを除去できるのは [TRITON Settings] > [Administrators] ページからだけです。

3. ロールの **[Managed Clients（処理対象クライアント）]** を追加および削除します。

   変更できるのは Super Administrator だけです。代理管理者は、自分のロールに割り当てられているクライアントを表示することができます。

項目	説明
<Name>（名前）	明示的にロールに割り当てられている各クライアントの名前を表示します。ロールの管理者は、ポリシーを適用する前に、[Clients（クライアント）] ページでクライアントを追加する必要があります。*代理管理者タスクの実行、435 ページ*を参照してください。
Add（追加）	**[Add Managed Clients（処理対象クライアントの追加）]** ページを開きます。*処理対象クライアントの追加、429 ページ*を参照してください。
Delete（削除）	無制限優先管理者だけが利用可能です。このボタンは、処理対象クライアント リストでマークされているクライアントをロールから除去します。 一部のクライアントは、処理対象クライアント リストから直接に削除することができません。詳細は、*処理対象クライアントの削除、434 ページ*を参照してください。

4. **[Deployment Status Permissions（配備ステータス許可）]** エリアを使って、このロールの管理者が **[Access the Status（ステ - タスにアクセス）] > [配備] ページ** でユーザーの配備の中の Web Security コンポーネントに関する情報を見ることができるかどうかを指定します。

   代理管理者にこのページへのアクセスを付与する場合、それらの管理者が**コンポーネントを起動**または**停止**できるかをどうかも選択します。

5. **[Reporting Permissions（レポート作成の許可）]** エリアを使用して、このロール中でレポート作成アクセス権を持つ管理者が利用できる機能を選択します。

a. レポート作成許可の一般的レベルを選択します：

オプション	説明
Report on all clients（すべてのクライアントについてのレポート）	このオプションを選択して、すべてのネットワーク ユーザーについてレポートを生成する許可を管理者に付与します。 [Reporting Permissions（レポート作成許可）] エリアの他のオプションを使用して、このロールの管理者に特定の許可を設定します。
処理対象クライアントのみについてのレポート	このオプションを選択して、このロールに割り当てられている処理対象クライアントについてレポートすることに管理者を制限します。次に、これらの管理者がアクセスできる調査レポートの機能を選択します。 処理対象クライアントのみについてのレポート作成に限定された管理者は、Web Security Dashboard 上のプレゼンテーション レポートまたはユーザーベースのレポートにアクセスすることはできません。

b. ロールの適切な管理者による使用が許可される各レポート作成機能のチェックボックスにマークを付けます。

オプション	説明
Access presentation reports（プレゼンテーション レポートへのアクセス）	プレゼンテーションレ ポート機能へのアクセスを有効にします。管理者がすべてのクライアントについてレポートできる場合にのみ、このオプションは利用可能です。*プレゼンテーション レポート、161 ページ*を参照してください。
Access the Web Security Dashboard（Web Security Dashboard へのアクセス）	[Risks（リスク）]、[Usage（使用状況）]、および [System（システム）] ダッシュボード上でインターネット アクティビティを示すグラフの表示を有効にします。*Web Security Dashboard、39 ページ*を参照してください。 このオプションが選択されていない場合、管理者が見ることができるのは System ダッシュボードの [Health Alert（ヘルス アラート）] および [Value Estimates（推定値）]（表示される場合）セクションだけになります。
Access the Threats dashboard（Threats（脅威）ダッシュボードへのアクセス）	管理者は、ネットワーク中の高度のマルウェア脅威アクティビティと関連するグラフ、要約テーブル、およびイベント詳細へアクセスできるようになります。*Threats ダッシュボード、41 ページ*を参照してください。

オプション	説明
Access forensics data in the Threats dashboard（Threats（脅威）ダッシュボードのフォレンシック データへのアクセス）	Websense Web Security Gateway または Gateway Anywhere で、管理者は脅威アクティビティと関連するファイルを表示し、そのようなファイルを送ろうとする試みに関する情報を検討できるようになります。*フォレンシック データの格納の設定、532 ページ*を参照してください。
Access investigative reports（調査レポートへのアクセス）	基本的な調査レポート機能へのアクセスを有効にします。このオプションが選択されると、追加の調査レポート機能を選択することもできます。*調査レポート、187 ページ*を参照してください。
View user names in investigative reports（調査レポートのユーザー名の参照）	このロールの管理者はユーザー名を表示できるようになります（ユーザー名がログ記録されている場合）。*要求がログ記録される方法の設定、505 ページ*を参照してください。 このオプションが選択されないと、名前ではなく、システムによって生成され識別コードだけが表示されます。 このオプションは、管理者が調査レポートへのアクセス権を付与されている場合にだけ利用可能です。
Save investigative reports as favorites（調査レポートを使用頻度の高いレポートとして保存）	このロールの管理者は使用頻度の高い調査レポートを作成できるようになります。*使用頻度の高い調査レポート、207 ページ*を参照してください。 このオプションは、管理者が調査レポートへのアクセス権を付与されている場合にだけ利用可能です。
Schedule investigative reports（調査レポートのスケジュール設定）	このロールの管理者は後刻または繰り返しベースで調査レポートを実行するようにスケジュール設定できるようにします。 *調査レポートのスケジュール設定、208 ページ*を参照してください。 管理者が調査レポートを使用頻度の高いレポートとして保存する許可を付与されているときだけ、このオプションは利用可能です。
ログ データベースの管理	管理者が [Settings] > [Reporting] > [Log Database] のページにアクセスできるようにします。 *Log Database 管理の設定、517 ページ*を参照してください。
アプリケーション レポートへのアクセス	管理者が [Reporting] > [Applications] ページでブラウザ、プラットフォーム、およびユーザー エージェント データを表示できるようにします。 *アプリケーション レポートの作成、216 ページ*を参照してください。

6. 変更を終了したら、**[OK]** をクリックして、変更をキャッシュし、[Delegated Administration（代理管理）] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

管理者の追加

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *代理管理者、407 ページ*
- *ロールの編集、423 ページ*

Super Administrator は、**[Delegated Administration（代理管理）] > [Edit Role（ロールの編集）] > [Add Administrators（管理者の追加）]** を使用して、ロールの管理者を指定することができます。

注意
管理者を複数のロールに追加することができます。これらの管理者は、ログオン時にロールを選択する必要があります。この場合、管理者はすべてのロールについて組み合わされたレポート作成許可を付与されます。

代理管理者は、その処理対象クライアントのインターネット アクティビティに対して重要な管理ができます。お客様の組織の許容使用ポリシーのとおりにこの管理が責任を持って処理されていることを保証するために、Super Administrator は管理者によって行われた変更をモニタするために [Audit Log（監査ログ）] ページを使用すべきです。*監査ログの表示とエクスポート、475 ページ*を参照してください。

1. ネットワーク アカウントに代理管理者を割り当てる場合、[TRITON Settings（TRITON 設定）] > [User Directory（ユーザー ディレクトリ）] 設定と一致している [Settings] > [General] > [Directory Service（ディレクト リサービス）] 設定（*ディレクトリ サービス、93 ページ* 参照）の Policy Server にログオンしていなければなりません。

   ローカル アカウントだけを管理者として追加する場合は、任意の Policy Server にログオンできます。

2. **[Local Accounts（ローカル アカウント）]** で 1 人以上のユーザーのチェックボックスにオンにし、次に右矢印 ボタンをクリックして、ハイライトされているユーザーを **[Selected（選択済み）]** リストに移します。

3. **[Network Accounts（ネットワーク アカウント）]** で 1 人以上のユーザーのチェックボックスにオンにし、次に右矢印（>）ボタンをクリックして、そのユーザーを **[Selected（選択済み）]** リストに移します。

> **注意**
> カスタム LDAP グループを管理者として追加することはできません。

4. このロールの管理者の **[Permissions（許可）]** を設定します。

オプション	説明
Administrator（管理者）：Policy Management（ポリシー管理）	このロールの管理者がその処理対象クライアントに対してポリシーを適用できるようにします。これは、一部の Websense 構成設定へのアクセス権も付与します。
Administrator（管理者）：Reporting（レポート作成）	管理者にレポート作成ツールへのアクセス権を付与します。[Edit Role（ロールの編集）] ページを使用して、許可するレポート作成機能を設定します。
Administrator（管理者）：Real-Time Monitor	管理者がインターネット トラフィックをリアルタイムでモニタできるようにします。*Real-Time Monitor*、224 ページを参照してください。
Auditor（監査者）	ロール中の他の管理者が利用できるすべての機能を表示するアクセス権を管理者に付与します - この場合、変更を保存することはできません。

5. 変更が完了したら、**[OK]** をクリックして [Edit Role（ロールの編集）] ページに戻ります。
6. [Edit Role] ページで **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy（保存と配備）]** をクリックするまで変更は適用されません。

処理対象クライアントの追加

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *代理管理者ロールの管理*、420 ページ
- *ロールの編集*、423 ページ

処理対象クライアントはロールに割り当てられたユーザーおよびコンピュータであり、そのポリシーはロールの管理者によって設定されます。ディレクトリ クライアント（ユーザー、グループ、およびドメイン [OU]）、コンピュータ（個々の IPv4 または IPv6 アドレス）、およびネットワーク（IPv4 または IPv6 アドレス範囲）をすべて処理対象クライアントとして定義することができます。

Super Administrator は、**[Delegated Administration] > [Edit Role] > [Add Managed Clients（[処理対象クライアントの追加）]** ページを使用して、必要とされる数のクライアントをロールに追加することができます。各クライアントに割り当てることができるのは、ただ 1 つのポリシー管理およびレポート作成ロールです。

ネットワーク範囲を 1 つのロールの処理対象クライアントに割り当てる場合、その範囲内の個々の IP アドレスを他のロールに割り当てることはできません。また、ユーザー、グループ、またはドメイン（OU）を 2 つの異なるロールに割り当てることはできません。しかし、ユーザーを 1 つのロールに割り当て、そのユーザーが所属しているグループまたはドメイン（OU）を異なるロールを割り当てることはできます。

注意
グループが 1 つのロールの処理対象クライアントであり、そのロールの管理者がポリシーをグループの個々のメンバーに適用する場合、その後、そのグループの個々のユーザーを別のロールに割り当てることはできません。

処理対象クライアントに追加するとき、含めるべきクライアント タイプについて検討してください。

- ロールに IP アドレスを追加すると、コンピュータに誰がログオンしているかということは無関係に、そのロールの管理者は当該コンピュータの**すべての**アクティビティに関するレポートを作成することができます。
- ロールにユーザーを追加する場合、どのコンピュータが利用されていても、管理者は そのユーザーのすべてのアクティビティをレポートすることができます。

管理者は、彼らが管理するロールの処理対象クライアントに自動的には含められません。なぜなら、そうなると、管理者が自身のポリシーを設定できるようになるからです。管理者が自身のインターネット利用状況を表示するためには、セルフ レポート作成を有効にしてください（*セルフレポーティング、540 ページ*を参照）。

お客様の組織が複数の Policy Server を配備し、Policy Server が種々のディレクトリと通信している場合、追加しようとするクライアントを含んでいるディレクトリに接続している Policy Server を選択してください。

> **注意**
> 同じロールのすべてのディレクトリ クライアントは同じディレクトリ サービスで定義されているべきでしょう。

1. ロールのクライアントを選択します：
   - **[Directory（ディレクトリ）]** で、1 人または複数のユーザーのチェックボックスをオンにします。

     お客様の環境が、Active Directory（Native Mode）または他の LDAP ベースのディレクトリ サービスを使用している場合、特定のユーザー、グループ、またはドメイン（OU）の名前を見つけるために、ディレクトリを検索することができます。*ディレクトリ サービスの検索、103 ページ*を参照してください。
   - **[Computer（コンピュータ）]** で、このロールに追加される IP アドレスを IPv4 または IPv6 フォーマットで入力します。
   - **[Network（ネットワーク）]** で、範囲として最初と最後の IP アドレスを IPv4 または IPv6 フォーマットで入力します。
2. クライアントを **[Selected（選択済み）]** リストに移動するためには、クライアント タイプの隣の右矢印（>）ボタンをクリックします。
3. 変更が完了したら、**[OK]** をクリックして [Edit Role（ロールの編集）] ページに戻ります。
4. [Edit Role] ページで **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy（保存と配備）]** をクリックするまで変更は適用されません。

ロール競合の管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：
- *代理管理者ロールの管理、420 ページ*
- *処理対象クライアントの追加、429 ページ*

ディレクトリ サービスでは、同じユーザーが複数のグループに属することができます。その結果、複数の代理管理ロールによって管理される異なるグループ内に 1 人のユーザーが存在する可能性があります。同じ状況はドメイン（OU）でも存在します。

さらに、ユーザーが 1 つのロールによって管理され、別のロールによって管理されるグループまたはドメイン（OU）に属する可能性があります。両方のロールの管理者が同時にログオンした場合、グループの管理者がポリシーをグループの個々のメンバーに適用すると同時に、ユーザーの管理者がポリシーをそのユーザーに適用することがあります。

重複があるために異るポリシーが同じユーザーに適用される場合の Websense ソフトウェアの処理を指定するためには、**[Delegated Administration] > [Manage（管理）] [Role（ロール）] [Priority（優先順位）]** ページを使用します。競合が発生すると、Websense ソフトウェアはこのリストの最上位に表示されるロールからポリシーを適用します。

1. Super Administrator 以外のロールをリスト上で選択します。

> **注意**
> Super Administrator ロールは常にこのリストの最初にあります。これは移動できません。

2. 位置を変更するためには、**[Move Up（上に移動）]** または **[Move Down（下に移動）]** をクリックします。
3. すべてのロールが希望する優先順位になるまで、ステップ 1 とステップ 2 を繰り返します。
4. 変更を終了したら、**[OK]** をクリックして、変更をキャッシュし、[Delegated Administration（代理管理）] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

代理管理者ロールの更新

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ロールの削除、433 ページ*
- *処理対象クライアントの削除、434 ページ*

ポリシーと処理対象クライアントは、通常、ロールの作成時にロールに追加されます。

- ポリシー許可を持つ代理管理者は自身が管理するロール内において既存のポリシーを編集し、新しいロールを作成することができます。
- 新しいメンバーが組織に参加するとき、優先管理者はそのメンバーを既存のロールに追加することができます（*ロールの編集、423 ページ*を参照してください）。

優先管理者は、いつでもクライアント（*クライアントをロールに移動、108 ページ*参照）とポリシー（*ロールへのフィルタおよびポリシーのコピー、319 ページ*）を 優先管理者ロールから既存の代理管理ロールに移すことができます。

- クライアントを代理管理ロールに移すと、優先管理者ロールで適用されていたポリシーもコピーされます。Filter Lock の制限があれば、このコピー処理中にフィルタが更新され、その制限が適用されます。

  ターゲット ロールには、[Copied（コピー済み）] タグ がフィルタまたはポリシー名の末尾に追加されます。そのロールの管理者は、容易に新しい項目を識別し、適切にそれを更新することができます。

  ロールの管理者に対して、フィルタおよびポリシーをリネームし、必要な場合にそれらを編集し、それらの設定を明確にし、重複をできるだけなくすよう推奨してください。これらの変更は、将来のメンテナンス作業を簡単にすることができます。

  クライアントが新しいロールに移されると、そのロールの管理者だけが当該クライアントのポリシーまたはフィルタを変更することができます。Super Administrator ロール中の元のポリシーまたはフィルタの変更は、代理管理ロールのポリシーまたはフィルタのコピーに影響を与えません。
- 直接にフィルタとポリシーを代理管理ロールにコピーすると、クライアントの移動時にフィルタとポリシーがコピーされるときに適用されるのと同じ制限が適用されます。
  - Filter Lock の制限がコピー中に適用されます。
  - [Permit All（すべての許可）]カテゴリおよびプロトコル フィルタはリネームされ、Filter Lock の制限内で編集可能なフィルタになります。
  - コピーされたフィルタおよびポリシーにはロール内で名前に [Copied（コピー済み）] タグが付けられ、識別されます。

  ターゲットのロールで管理者にとってわかり易いように、コピーを開始する前にポリシーの説明を編集することを考えてください。

ロールの削除

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Delegated Administration（代理管理）] ページで、無制限優先管理者は使用されなくなったロールを削除することができます。

ロールを削除すると、そのロールの管理者が [Clients（クライアント）] ページに追加したすべてのクライアントが除去されます。ロールが削除された後は、そのクライアントが他のロールによって管理さるネットワーク、グループ、またはドメインに属する場合、それらのロールで適用される適切なポリシーによって管理されます（*適用順序、119 ページ*を参照）。そうでない場合は、優先管理者の Default（デフォルト）ポリシーがクライアントに適用されます。

1. **[Delegated Administration]**のページで、削除すべき各ロールの横のチェックボックスをオンにします。

   > **注意**
   > 優先管理者ロールは削除できません。

2. **[Delete]** をクリックします。
3. [Delegated Administration] ページから選択されているロールを除去する削除要求を確認します。**[Save and Deploy（保存と配備）]** をクリックするまで変更は確定しません。

   次に TRITON コンソールにログオンしたときに、削除したロールはバナーのロール ドロップダウンリストからクリアされます。

処理対象クライアントの削除

Web Security Help | Web Security ソリューション | バージョン 7.8.x

下記の場合、処理対象クライアント リスト（[Delegated Administration] > [Edit Role]）からクライアントを直接に削除することはできません：

- 管理者がポリシーをクライアントに適用している。
- 管理者がネットワーク、グループ、またはドメイン（OU）の 1 つ以上のメンバーにポリシーを適用している。

Super Administrator が接続している Policy Server が、削除されるはずのクライアントを含むディレクトリ サービスと通信している Policy Server ではない場合、問題が発生するかもしれません。この場合、現在の Policy Server およびディレクトリ サービスはクライアントを認識しません。

次のようにすれば、無制限優先管理者は適切なクライアントが削除されるようにすることができます。

1. Web Security のツールバーで **Policy Server** リストを開き、適切なディレクトリと交信している Policy Server と接続していることを確認します。無制限 Super Administrator 許可でログオンする必要があります。
2. Web Security ツールバーで **[Role（ロール）]** リストを開き、削除すべき管理対象クライアントを含んでいるロールを選択します。
3. **[Policy Management] > [Clients]** へ進み、当該代理管理者が明白にポリシーを割り当てているすべてのクライアントのリストを表示します。

   これには、ロールの処理対象クライアント リストで特定されているクライアントと処理対象クライアント リストのネットワーク、グループ、ドメイン、または組織単位のメンバーであるクライアントの両方が含まれます。
4. 適切なクライアントを削除します。
5. **[OK]** をクリックして、変更をキャッシュします。

6. バナーの **[Role]** リストを開き、**[Super Administrator]** ロール を選択します。
7. **[Policy Management] > [Delegated Administration] > [Edit Role]** に移動します。
8. 処理対象クライアント リストから適切なクライアントを削除し、削除を確認するために **[OK]** をクリックします。
9. 変更をキャッシュするために、[Edit Role] ページで **[OK]** をクリックします。**[Save and Deploy（保存と配備）]** をクリックするまで変更は適用されません。

Super Administrator クライアントの管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

代理管理ロールに割り当てられていないクライアントは優先管理者によって管理されます。Super Administrator ロールには Managed Clients（処理対象クライアント）リストはありません。

ポリシーをこのようなクライアントに適用するためには、[Policy Management] > [Clients] ページにそれらを追加します。*クライアントの追加、102 ページ*を参照してください。特定のポリシーを割り当てられていないクライアントは Super Administrator の Default ポリシーで管理されます。

[Clients（クライアント）] ページでクライアントを追加できない場合があるかもしれません。クライアントが他のロールに割り当てられているネットワーク、グループ、またはドメイン（OU）のメンバーであるとき、これは起ります。他のロールの管理者がネットワークまたはグループの個々のメンバーにポリシーを適用している場合、それらのクライアントを Super Administrator ロールに追加することはできません。

代理管理者タスクの実行

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense アカウント（自分のネットワーク資格情報ではなく）を使用して TRITON コンソールにログオンする代理管理者は、自分のアカウント情報を検討して、パスワードを変更することができます。*ユーザー アカウントの表示、436 ページ*を参照してください。

ポリシー許可を持つ代理管理者は下記のタスクを行なうことができます。

- ロール定義の表示

  [Policy Management] > [Delegated Administration] ページを順に選択し、ロール名をクリックします。[Edit Role（ロールの編集）] ページが表示されます。このページには、ロールの処理対象クライアントがリストされ、ロールのレポート作成許可をもつ管理者が利用できるレポート作成機能が示されます。

- *[Clients（クライアント）] ページへのクライアントの追加*、437 ページ
- *ポリシーとフィルタの作成*、438 ページ
- [Clients] ページでクライアントにポリシーを適用します（*1 つのポリシーを複数のクライアントに割り当てる*、119 ページを参照）。

詳細なレベルで**レポート作成**の許可を与えることができます。ロールに与えられた特定のレポート作成許可によって、レポート作成許可をもつ管理者にとって次のどのタスクが利用可能であるかが決定されます。

使用できる機能を知るには、[Delegated Administration] ページに移動し、ロール名をクリックします。[Edit Role] ページで、許可を与えられているレポート作成機能が表示されます。これらの機能の使用方法については、下記を参照してください。

- *Web Security Dashboard*、39 ページ
- *プレゼンテーション レポート*、161 ページ
- *調査レポート*、187 ページ
- *アプリケーション レポートの作成*、216 ページ
- *Real-Time Monitor*、224 ページ

ユーザー アカウントの表示

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *代理管理者タスクの実行*、435 ページ
- *[Clients（クライアント）] ページへのクライアントの追加*、437 ページ
- *ポリシーとフィルタの作成*、438 ページ

ネットワーク資格情報を入力して TRITON コンソールにログオンした場合、パスワード変更はネットワーク ディレクトリ サービスを通じて処理されます。問題があれば、システム管理者に連絡してください。

ローカル ユーザー名とパスワードが割り当てられている場合、TRITON コンソール内でアカウントの情報を表示し、パスワードを変更します。

1. バナーのすぐ下にある TRITON ツールバーで **[TRITON Settings（TRITON 設定）]** をクリックします。

   [My Account（マイ アカウント）] ページが開きます。
2. パスワードを変更するには、最初に現在のパスワードを入力し、次に新しいパスワードを入力し、確認します。

- パスワードは 4 ～ 255 文字で指定してください。
- 強いパスワード、つまり 8 文字以上で、大文字、小文字、数字および特殊文字（ハイフン、下線、空白など）をそれぞれ 1 文字以上含むパスワードの使用を推奨します。

[OK] をクリックし、変更を保存し、適用します。

3. 管理することができるロールのリストを表示するには、[Web Security manager Policy Management] > [Delegated Administration] > [View Administrator Accounts（管理者アカウントの表示）] ページに進みます。
   - ただ 1 つのロールの管理が割り当てられていると、その名前がリストで表示されます。
   - 複数のロールの管理が割り当てられているときは、ユーザー名の隣の **[View（表示）]** をクリックして、リストされているロールを表示します。
4. 完了したら **[Close（閉じる）]** をクリックして、[Delegated Administration] ページに戻ります。

[Clients（クライアント）] ページへのクライアントの追加

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *代理管理者タスクの実行、435 ページ*
- *ユーザー アカウントの表示、436 ページ*
- *ポリシーとフィルタの作成、438 ページ*

優先管理者は、ロールに処理対象クライアントを割り当てます。しかし代理管理者は、ポリシーを適用する前に、[Clients] ページでそれらのクライアントを追加する必要があります。手順については、*クライアントの追加、102 ページ*を参照してください。

クライアントを処理対象クライアント リストに追加すると、それらのインターネット要求は直ちにロールの中のポリシーの対象となります。

- Super Administrator ロール中でポリシーを割り当てられていたクライアントには、新しいロール中にコピーされているそのポリシーが適用されます。[Move to Role（ロールに移動）] プロセスは適用されるべきポリシーを自動的にコピーします。
- 何らかのポリシーを割り当てられていなかったクライアントは、新しいロールの Default ポリシーを受け取ります。最初に、この Default ポリシーは Super Administrator ロールからコピーされた Default カテゴリおよびプロトコルを適用します。

[Delegated Administration] > [Edit Role] ページの [Managed Clients（処理対象クライアント）] リストに示されるすべてのクライアントを [Clients] ページに追加し、ポリシーを割り当てることができます。ロールに割り当てられているグループ、ドメイン（OU）、およびネットワークでも、下記のものを追加することができます：

- グループまたは OU のメンバーである個々のユーザー
- ネットワーク上の個々のコンピュータ

ユーザーが複数のグループ、または OU に含まれていることがあるため、異なるロールが共通のメンバーを持つグループ、または OU を管理する場合、より大きなクライアント グループから個人を追加すると競合が発生する可能性があります。いくつかの異なるロールの管理者が同時に Web Security manager にアクセスすると、[Clients] ページで同じクライアント（例えばグループの個々のメンバー）を追加することがあります。この状況では、そのクライアントのポリシーの実施は、それぞれのロールで指定されている優先権によって管理されます。*ロール競合の管理*、431 ページを参照してください。

ポリシーとフィルタの作成

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *代理管理者タスクの実行*、435 ページ
- *ユーザー アカウントの表示*、436 ページ
- *[Clients（クライアント）] ページへのクライアントの追加*、437 ページ

ロールが作成されたとき、それは Super Administrator ロールから現在の Default カテゴリ フィルタおよびプロトコル フィルタを自動的に継承しています。ロール固有の Default ポリシーが作成され、これは継承した Default カテゴリおよびプロトコル フィルタを適用します。（このロール固有 Default ポリシーは、別のポリシーが割り当てられないかぎり、あらゆるクライアントに自動的に適用されます。）

また、Super Administrator が当該のロールに他のポリシーとフィルタをコピーしているかもしれません。

さらに、ポリシーとフィルタの他に、Super Administrator によって作成されたカスタム ファイル タイプおよびプロトコルも継承されます。

継承された ポリシーとフィルタを編集することができます。行われた変更は、自身のロールのみに影響を与えます。以前に継承したフィルタとポリシーに対して Super Administrator が行う変更は自身のロールには影響を与えません。

> **注意**
>
> Super Administrator がファイル タイプとプロトコルに対して行う変更は、自動的にロールのフィルタとポリシーに影響を与えます。
>
> Super Administrator があなたにこれらのコンポーネントの変更を通知したとき、ポリシーとフィルタが適切に処理されているかどうか確認してください。

また、必要なだけの新しいフィルタとポリシーを作成することができます。代理管理者によって作成されたフィルタとポリシーは、そのロールにログオンした管理者にのみ有効です。ポリシーを作成する手順については、*ポリシーの使用、113 ページ*を参照してください。フィルタを作成する手順については、*フィルタの使用、71 ページ*を参照してください。

いくつかの制限付きで、ロールのフィルタ コンポーネントを編集することができます。

- **Categories（カテゴリ）**：カスタム カテゴリの追加または編集、カスタムまたはマスタ データベース カテゴリへのカスタム URL およびキーワードの割り当て、カテゴリ フィルタでデフォルトで割り当てられるアクションの変更（カテゴリが Filter Lock によってロックされていない場合だけ、カテゴリのデフォルト アクションに対する変更が実行されます。）
- **Protocols（プロトコル）**：ロールのプロトコルフィルタでデフォルト時に適用されるアクションの変更（プロトコルが Filter Lock によってロックされていない場合だけ、プロトコルのデフォルト アクションに対する変更が実行されます。）代理管理者はプロトコル定義を追加 / 削除することはできません。
- **File Types（ファイル タイプ）**：各ファイル タイプに割り当てられているファイル拡張子の表示。代理管理者はファイル タイプの追加またはファイルタイプに割り当てられている拡張子の変更はできません。

詳細については、*フィルタ コンポーネントの作成、321 ページ*を参照してください。

優先管理者が Filter Lock 制限を実行している場合、カテゴリまたは プロトコルが自動的にブロックされ、作成および編集したフィルタを変更できない場合があります。

管理者アカウントのレビュー[かんりしゃあかうんとのれびゅー]

[Delegated Administration] > [View Administrator Accounts（管理者アカウントの表示）] ページを使用して、下記のことを行います：

- Global Security administrator（グローバル セキュリティ管理者）によって Web Security アクセス権を与えられているローカルおよびネットワークアカウントのリストを表示する。
- 各アカウントに割り当てられている許可のレベルを確認する。
- 各アカウントと関連付けられているロールのリストを表示する。

  あるアカウントが 1 つのロールに管理者として追加されると、そのロールがアカウント名の右側にリストされます。アカウントが複数のロールを管理できるものであるとき、**[View]** をクリックし、リストされるロールを表示します。

代理管理者は自分自身のアカウント情報を見ることができますが、すべてのアカウントについてはできません。

管理者アカウントの確認が終わったら、**[Close]** をクリックして、[Delegated Administration] ページに戻ります。

ネットワーク アカウントの有効化

グローバル セキュリティ管理者は、**[TRITON Settings] > [User Directory（ユーザー ディレクトリ）]** ページを使用して、管理者が自分のネットワーク資格情報を使って TRITON コンソールにログオンするのに必要なディレクトリ サービス情報を入力することができます。

このタスクは、ユーザーおよびグループ クライアントを識別するために使用されるディレクトリ サービスを定義する Web Security Super Administrator による構成設定とは**別個に**行われます。

> **注意**
> クライアント ディレクトリ サービス情報は [Settings（設定）] > [Directory Services（ディレクトリ サービス）] ページで設定されます（*ディレクトリ サービス、93 ページ*を参照してください）。

TRITON 管理者のネットワーク資格情報は、1 つのディレクトリ サービスに対して認証される必要があります。ネットワークが複数のディレクトリを含む場合、TRITON Settings（TRITON 設定）で指定されているディレクトリとその他のディレクトリの間に信頼関係がなければなりません。

TRITON Unified Security Center で使用する 1 つのディレクトリ サービスを定義できない場合、管理者のローカル アカウントを作成することを考えてください。

管理者のログオンの認証のために使用されるディレクトリを定義する手順についての説明は TRITON Settings Help にあります。

16 Web Security Server Administration

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連トピック：

- *Websense Web Security コンポーネント*、444 ページ
- *Policy Broker について*、456 ページ
- *Policy Server の動作*、458 ページ
- *Filtering Service の動作*、465 ページ
- *サードパーティ SIEM ソリューションとの統合*、472 ページ
- *Content Gateway の動作*、473 ページ
- *監査ログの表示とエクスポート*、475 ページ
- *Websense サービスの停止と起動*、477 ページ
- *警告*、481 ページ
- *Websense データのバックアップと復元*、492 ページ

インターネットポリシーの実施は、複数の Websense Web Security コンポーネント間のやりとりを必要とします。

- インターネット アクセスのユーザ要求は、Network Agent、Content Gateway、または サードパーティ統合製品 / デバイスによって受信されます。
- 要求は Filtering Service（フィルタリング サービス）に送信され、そこで処理されます。
- Filtering Service は、Policy Server および Policy Broker と通信し、要求に適切に応答します。

中央 Policy Broker は、他のコンポーネントにクライアント、フィルタ、ポリシー、および一般設定情報へのアクセスを提供します（Policy Broker の追加的な、レプリカ インスタンスを配備し、この情報の読み取り専用コピーを配置しておくことができますが、ポリシーまたは設定データへの更新に使用されるのは中央（プライマリ）インスタンスだけです）。

TRITON コンソールは中央 Policy Broker に関連付けられ、配備されているどの Policy Server の設定にも使用できます。

Websense Web Security コンポーネント

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Policy Broker について*、456 ページ
- *Policy Server の動作*、458 ページ
- *Filtering Service の動作*、465 ページ
- *Policy Server、Filtering Service、および State Server*、469 ページ
- *Websense サービスの停止と起動*、477 ページ
- *現在のシステム ステータスの確認*、490 ページ

Websense Web Security ソリューションは、インターネット セキュリティ、ユーザ識別、レポート機能を提供するために共に動作する複数のコンポーネントで構成されています。このセクションでは、お客様の環境を理解し、管理するための手助けのために、各コンポーネントの概要を提供します。

ここで説明するコンポーネントのリストについては、下記を参照してください：

- *ポリシーの実施および管理コンポーネント*、445 ページ
- *レポーティング コンポーネント*、448 ページ
- *ユーザ識別コンポーネント*、449 ページ
- *相互運用性コンポーネント*、450 ページ

Websense ソフトウェアが Citrix、Microsoft Forefront TMG、または ICAP を使用するプロキシもしくはプロキシ - キャッシュと統合されると、別の統合コンポーネント（統合サービス、プラグイン、または ICAP サーバー）もインストールされます。

ポリシーの実施および管理コンポーネント

Web Security Help | Web Security ソリューション | バージョン 7.8.x

コンポーネント	説明
Policy Database（ポリシー データベース）	Websense ソフトウェア設定とポリシー情報を保存します。Policy Broker（ポリシー ブローカ）と併せて自動的にインストールされます。
Policy Broker（ポリシー ブローカ）	ポリシーおよび一般設定情報についての Websense コンポーネントからの要求を管理します。
Policy Server（ポリシー サーバー）	• 他の Websense コンポーネントの位置およびステータスを識別し、追跡します。 • 1 つの Policy Server インスタンス専用の設定情報を保存します。 Web Security manager で Policy Server 設定を構成します（*Policy Server の動作*、458 ページを参照してください）。 ポリシーとほとんどの設定は、Policy Database を共有する複数の Policy Server で共有されます（*複数 Policy Server 環境での動作*、462 ページを参照）。
Filtering Service（フィルタリング サービス）	Network Agent、Content Gateway、またはサードパーティ統合製品と連携して、インターネットポリシーを実施します。ユーザがあるサイトを要求すると、Filtering Service が要求を受信し、どのポリシーを適用するか決定します。 • インターネット要求の管理とログ記録のために、Filtering Service が実行している必要があります。 • 各 Filtering Service インスタンスは、Websense Master Database の自身用のコピーをダウンロードします。 Web Security manager で Filtering Service の動作を設定します（*インターネット使用状況のフィルタ*、57 ページおよび *フィルタリング設定値の設定*、81 ページを参照）。
Network Agent（ネットワーク エージェント）	• ポリシーの実施およびログ記録機能の拡張 • プロトコル管理を有効にします。 • スタンドアロン環境でポリシーの実施を有効化します。 詳細については、*ネットワークの構成*、541 ページを参照してください。

コンポーネント	説明
Master Database（マスタ データベース）	• 数百万のウェブサイトを含み、それらを 90 以上のカテゴリおよびサブカテゴリに分類しています。 • 非 HTTP プロトコルの管理で使用される 100 以上のプロトコル定義を含みます。 インターネット ポリシーの実施を有効にするために Websense Master Database をダウンロードし、そのデータベースを常に最新の状態で維持します。マスタ データベースが 2 週間以上古くなると、ポリシーの実施は行われません。詳細は、*Websense マスタ データベース*、32 ページを参照してください。
TRITON Infrastructure（TRITON インフラストラクチャ）	TRITON コンソールの Web Security、Data Security、および Email Security のモジュールをサポートし、統合するプラットフォームです。 すべての TRITON モジュールに適用されるグローバル設定の内部データベースを維持します。
Web Security manager（TRITON コンソールの一部）	ウェブ セキュリティ ソフトウェアの設定、管理、およびレポート作成とのインターフェースを提供します。 Web Security manager を使用して、インターネット アクセス ポリシーの定義とカスタマイズ、コンポーネントの設定、インターネット アクティビティについてのレポート、その他のタスクを行います。 Web Security manager は下記のサービスによって構成されています： • Websense - TRITON Web Security • Websense Web Reporting Tools • Websense Explorer Report Scheduler • Websense Information Service for Explorer • Websense Reporter Scheduler 詳細は、*TRITON コンソールの使用方法*、21 ページを参照してください。
Usage Monitor（使用状況モニタ）	• インターネット使用状況に基づくアラートを有効にします。 • インターネット使用状況情報を Real-Time Monitor に提供します。 Usage Monitor は、URL カテゴリ アクセス（Real-Time Monitor で示されます）とプロトコル アクセスを追跡し、設定されているアラート動作に従ってアラート メッセージを生成します。詳細については、*警告*、481 ページ と *Real-Time Monitor*、224 ページを参照してください。

コンポーネント	説明
Content Gateway（コンテンツ ゲートウェイ）	• 堅固なプロキシおよびキャッシュ プラットホームを提供します。 • まだ分類されていないサイトを分類するために、リアルタイムでウェブサイトとファイルの内容を分析することができます。 • プロトコル管理を有効にします。 • セキュリティ脅威を発見するために HTML コードを解析します（例えば、フィッシング、URL リダイレクション、Web エクスプロイト、およびプロキシ回避）。 • 脅威カテゴリ（例えば、ウイルス、トロイの木馬、またはワーム）を割り当てるために、ファイル コンテンツを検査します。 • 特定の Web ページからアクティブなコンテンツを取り除きます。 *Content Gateway 分析、229 ページ*を参照してください。
Remote Filtering Client（リモート フィルタリング クライアント）	• ネットワーク ファイアウォールの外側のクライアント コンピュータに存在します。 • フィルタリングされるクライアントとしてコンピュータを識別し、Remote Filtering Server と通信します。 詳細は、*オフサイト ユーザーの管理、303 ページ*を参照してください。
Remote Filtering Server（リモート フィルタリング サーバー）	• ネットワーク ファイアウォールの外側のクライアントのポリシーの実施をできるようにします。 • リモート コンピュータのインターネット アクセスを管理するために、Filtering Service と通信します。 詳細は、*オフサイト ユーザーの管理、303 ページ*を参照してください。
State Server（状態サーバー）	複数の Filtering Service 環境で、クライアント割り当て、確認、パスワード アクセス、およびアカウント無効化のセッションをトラックし、アクセス時間が適切に割り当てられるようにします。 この機能を有効にするには、各 Policy Server について 1 つの State Server を配備します。

他のコンポーネントについては、下記を参照してください。

- *レポーティング コンポーネント、448 ページ*
- *ユーザ識別コンポーネント、449 ページ*
- *相互運用性コンポーネント、450 ページ*

レポーティング コンポーネント

Web Security Help | Web Security ソリューション | バージョン 7.8.x

コンポーネント	説明
Log Server（ログ サーバー）	下記のようなインターネット要求データを記録します： • 要求ソース • 要求と関連するカテゴリまたはプロトコル • 要求が許可されたか、ブロックされたか • キーワード ブロック、ファイル タイプ ブロック、割り当て時間、帯域幅レベル、またはパスワード保護が適用されたかどうか。 また、Network Agent と特定の統合製品では、Log Server は使用された帯域幅量の情報も保存します。 Log Server は、ほとんどの Web Security レポーティング機能を有効化するためにインストールしなければならない Windows 専用コンポーネントです。 Log Server をインストールした後で、正しい場所にログ記録データを伝達するように Filtering Service を設定します（*要求がログ記録される方法の設定、505 ページ*を参照）。
Log Database（ログ データベース）	Websense レポーティング ツールで使用するために、Log Server によって収集されたインターネット要求データを保存します。
Real-Time Monitor（リアルタイム モニタ）	下記の情報を含む現在のインターネット アクティビティを表示します。 • 要求ソース（ユーザ名または IP アドレス） • URL（完全またはドメインのみ） • カテゴリ（Master Database、カスタム URL、または動的（Content Gateway スキャンに基づく）） • 要求が許可されたか、ブロックされたか • 要求の時刻 Real-Time Monitor は下記の 3 種類のサービスによって構成されています： • Websense RTM Client • Websense RTM Server • Websense RTM Database *Real-Time Monitor、224 ページ*を参照してください。

コンポーネント	説明
Multiplexer（マルチプレクサ）	これを有効にすると、ログ記録データが Filtering Service から下記へ渡されます： • 特定の SIEM ソリューション • Log Server これが使用されるのは、Websense ソフトウェアがサポートされている SIEM 製品と統合されている場合だけです。SIEM 統合を有効にするには、Policy Server ごとに 1 つの Multiplexer インスタンスをインストールします。

他のコンポーネントについては、下記を参照してください。

- *ポリシーの実施および管理コンポーネント、445 ページ*
- *ユーザ識別コンポーネント、449 ページ*
- *相互運用性コンポーネント、450 ページ*

ユーザ識別コンポーネント

Web Security Help | Web Security ソリューション | バージョン 7.8.x

コンポーネント	説明
User Service（ユーザー サービス）	• ディレクトリ サービスと通信します。 • 適切なポリシーを使用するために、[ユーザー対グループ] おおび [ユーザー対ドメイン] の関係を Filtering Service に伝達します。 • Web Security manager でのディレクトリ クライアント情報の表示を有効化します。 ディレクトリ サービス アクセスを設定するための情報については、*ディレクトリ サービス、93 ページ*を参照してください。
DC Agent（DC エージェント）	• Windows ベースのディレクトリ サービスで定義されたユーザの透過的識別を行います。 • ポリシーの実施で使用するための最新のユーザ ログオン セッション情報を提供するために、User Service と通信します。 詳細については、*DC Agent、373 ページ*を参照してください。

コンポーネント	説明
Logon Agent（ログオン エージェント）	• Linux および Windows ネットワークにおいて透過的ユーザ識別で卓越した正確性を提供します。 • ユーザ ログオン セッションを取得するとき、ディレクトリ サービスまたはその他の手段に依存しません。 • ユーザ ログオン セッションをその発生時に検出します。 Logon Agent は クライアント コンピュータ上のログオン アプリケーションと通信して、個々のユーザ ログオン セッションが確実に取得および処理されるようにします。 詳細については、*Logon Agent*、380 ページを参照してください。
eDirectory Agent（eDirectory エージェント）	• 透過的にユーザを識別するために、Novell eDirectory と共に動作します。 • ネットワークにログオンするユーザを認証する Novell eDirectory からユーザ ログオン セッション情報を収集します。 • 認証された各ユーザと IP アドレスを関連付け、Filtering Service に情報を提供するために User Service と共に動作します。 詳細については、*eDirectory Agent*、385 ページを参照してください。
RADIUS Agent（RADIUS エージェント）	ダイアルアップ、Virtual Private Network（VPN）、Digital Subscriber Line（DSL）、または その他のリモート接続を使用してネットワークにアクセスするユーザの透過的識別を有効にします。 詳細については、*RADIUS Agent*、383 ページを参照してください。

他のコンポーネントについては、下記を参照してください。

- *ポリシーの実施および管理コンポーネント*、445 ページ
- *レポーティング コンポーネント*、448 ページ
- *相互運用性コンポーネント*、450 ページ

相互運用性コンポーネント

Web Security Help | Web Security ソリューション | バージョン 7.8.x

コンポーネント	説明
Directory Agent	Websense Web Security Gateway Anywhere 配備のもとで、ハイブリッド サービスで使用されるユーザーおよびグループ情報をサポートされているディレクトリサービスから収集します。

コンポーネント	説明
Filtering Plug-In	Websense ソフトウェアが一部のファイアウォール、プロキシ、キャッシュ、または他の同様な製品と統合されると、Filtering Service と統合製品との通信を可能にするためにプラグインがインストールされることがあります。
Linking Service	Websense Web Security Gateway Anywhere 配備、または Websense ウェブおよびデータ セキュリティ コンポーネント結合した環境のもとで、データ セキュリティ ソフトウェアに User Service によって収集される Master Database 分類情報およびユーザー/グループ情報へのアクセスを提供します。
Sync Service	Websense Web Security Gateway Anywhere 配備のもとで： • ポリシー更新とユーザーおよびグループ情報をハイブリッド サービスに送ります。 • ハイブリッド サービスからレポート データを受け取ります。

他のコンポーネントについては、下記を参照してください：

- *ポリシーの実施および管理コンポーネント、445 ページ*
- *レポーティング コンポーネント、448 ページ*
- *ユーザ識別コンポーネント、449 ページ*

Web Security 配備の検討

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Status] > [Deployment] ページを使用して、配備に含まれている各 Policy Server、または各 Policy Server に接続するコンポーネントのステータス情報を検討します。また User Service ディレクトリの接続および検索速度も調べます。

[Deployment] ページには最大 3 つのタブがあります。

- **[Policy Server Map（Policy Server マップ）]** はネットワーク内の Policy Server インスタンスの概要をビジュアルな表形式で示します。選択した Policy Server に関連付けられているコンポーネントのステータスを確認するには、[Policy Server] アイコンまたは IP アドレスをクリックします。*Policy Server マップの使用、452 ページ*を参照してください。

  ユーザーの環境に Policy Server が 1 つしか存在しない場合は、このタブは表示されません。

- **[Component List（コンポーネント リスト）]** は、ネットワーク内の Web Security コンポーネントをリストしているテーブルを表示し、適切な許可をもつ管理者がコンポーネントを停止または起動することを可能にします。*コンポーネント リストの使用、453 ページ*を参照してください。

- **[Directory Performance（ディレクトリ パフォーマンス）]** は、User Service がユーザーおよびグループ情報を問い合わせる各 LDAP ベースのディレクトリ サーバーの接続および検索速度に関する情報を提供します。*ディレクトリ パフォーマンスの評価*、454 ページを参照してください。

  User Service がインストールされていない場合、または組織が Windows Active Directory を混在モードで使用している場合、このタブは表示されません。

Policy Server マップの使用

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Websense Web Security コンポーネント*、444 ページ
- *Policy Broker について*、456 ページ
- *Policy Server の動作*、458 ページ
- *Websense のヘルス アラート*、590 ページ

複数 Policy Server 環境で、[Status] > [Deployment] ページの **[Policy Server Map]** タブはすべての Policy Server インスタンスをグラフィカルに表示します。

- すべての追加的な Policy Server インスタンスは、ユーザー環境内の中央（ベース）Policy Server に接続されている状態で表示されます。
- 各 Policy Server は、Policy Broker 接続を示すマーカーが付いたサーバー タワーまたはアプライアンス アイコンによって表されます。

  マップの下の凡例は、アイコンを説明します。
- いずれかの Policy Server インスタンスの上にマウスを置くと、そのインスタンスの完全な IP アドレスと説明、そのインスタンスが現在接続されている Policy Broker の IP アドレス、および Policy Broker のモード（スタンドアロン、プライマリ、レプリカ）が表示されます。

  スタンドアロンまたはプライマリ Policy Broker には設定変更を書き込むことができますが、レプリカ Policy Broker インスタンスは読み取り専用です。

マップの下のテーブルは、IP アドレス、説明、Policy Broker IP アドレス、キー タイプ、および各 Policy Server インスタンスの現在のステータスをリストします。

選択した Policy Server に関連づけられているコンポーネント（Filtering Service、Log Server、User Service など）のリストを表示するには、マップの中の Policy Server のアイコン、またはテーブルの中の IP アドレスをクリックします。1 つのコンポーネント名（例、Real-Time Monitor）が、相互に依存する複数のサービス（例、RTM Client、RTM Server、RTM Database）を表している場合もありますので注意してください。

各コンポーネントについて、リストには、その名前、IP アドレスまたはホスト名、バージョン、およびステータスが表示されます。

ステータス列には下記のいずれかのアイコンが表示されます。

- チェック マークが付いた緑色のアイコンは、Policy Server とそれに関連づけられたコンポーネントがすべて実行中であることを示します。
- [x]が付いた赤のアイコンは、Policy Server またはそれに関連づけられた 1 つ以上のコンポーネントが停止していることを示します。
- 感嘆符が付いた黄色のアイコンは、Policy Server コンピュータ上の Websense Control Service インスタンスが見つからないため、そのポリシー サーバーおよびそれに関連づけられたコンポーネントのステータス情報がないことを示します。

コンポーネント サービスまたはデーモンを起動および停止する許可をもつ管理者の場合、このテーブルには起動または停止リンクも含まれます。

リスト内の 1 つのエントリが複数のサービスを表している場合もあります。そのような場合、リンクをクリックしたとき、そのコンポーネントを構成するすべてのサービスが起動または停止します。

そのほかに、選択した Policy Server に関連するすべてのヘルス アラートを [Components] ポップアップ ウィンドウに表示するオプションを提供するリンクもあります。

コンポーネント リストの使用

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Websense Web Security コンポーネント、444 ページ*
- *トラブルシューティングのヒントとツール、650 ページ*

[Status] > [Deployment] ページの **[Component List（コンポーネント リスト）]** タブは、ネットワーク内に配備されている Web Security コンポーネントを示すテーブルを表示します。各コンポーネントにつて、テーブルに下記の項目が表示されます。

- Name（名前）
- IP address or hostname（IP アドレスまたはホスト名）
- Policy Broker IP address or hostname（Policy Broker IP アドレスまたはホスト名）
- Version（バージョン）
- Status:

- チェック マークが付いた緑色のアイコンは、コンポーネントが実行中であることを示します。
- [x] が付いた赤のアイコンは、コンポーネントが停止していることを示します。
- 感嘆符が付いた黄色のアイコンは、Websense Control Service が実行していないため、ステータス情報がないことを示します。

コンポーネント サービスまたはデーモンを起動および停止する許可をもつ管理者の場合、このテーブルには起動または停止リンクも含まれます。

コンポーネント データをサードパーティのスプレッドシートまたはレポート作成ツールでの処理用にエクスポートするには、テーブルの上の **[Export to CSV（CSV へのエクスポート）]** リンクを使用します。

ディレクトリ パフォーマンスの評価

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ユーザー設定およびユーザー識別の問題、574 ページ*
- *ユーザーおよびグループの処理、92 ページ*
- *ユーザーの識別、361 ページ*

User Service がインストールされており、LDAP ベースのディレクトリ サービスに接続するように設定されている場合、[Status] > [Deployment] ページの **[Directory Performance]** タブには、選択した時間（デフォルトでは直近の 1 時間）のディレクトリ サーバーのパフォーマンス統計を示すテーブルが表示されます。

時間の幅を長くするか短くするには、異なる**時間範囲**を選択します（設定可能な時間範囲は、[直近 24 時間]、[直近 1 時間]、[直近 5 分間] です）。

テーブルには、選択した時間中に User Service が接続を試みた各ディレクトリ サーバーについて 1 つの行が含まれます。各行は以下の情報を示します。

- **Directory Host** を実行しているコンピュータの IP アドレス
- **処理**のタイプ（バインドまたは検索）
- 選択した時間中の各タイプの処理の **[Average（平均）]**、**[Most Recent（直近）]**、および **[Maximum（最大）]** の時間。時間はミリ秒単位で示されます。
- 指定したディレクトリについて User Service が各処理の実行を試みた回数
- 処理が失敗した回数

[Directory Host（ディレクトリ ホスト）] のエントリをクリックすると、そのディレクトリの [午前 0 時以降]、[直近の 1 時間]、および [直近の 5 分間] のパフォーマンスに関する詳細が表示されます（*ディレクトリ サーバーの詳細の検討、455 ページ*を参照）。

組織内のユーザーにブラウズの遅延や、誤ったポリシーの適用（特に、その日の最初のウェブ要求や、長時間にわたってブラウズを行っていなかった後に）が起こっている場合、ディレクトリ パフォーマンス統計を使用してパフォーマンスが低いディレクトリを特定します。特定のディレクトリ ホストで継続的に問題が起こる場合、下記の条件を改善するための措置を取る必要があります。

- User Service とディレクトリの間のネットワーク 接続
- ディレクトリ サーバーが実行しているコンピュータのメモリ、ディスク、または CPU

複数のディレクトリで問題が発生している場合は、ネットワーク、DNS、または他の設定の問題が起こっている可能性があります。

ディレクトリ サーバーの詳細の検討

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ディレクトリ パフォーマンスの評価、454 ページ*
- *ユーザー設定およびユーザー識別の問題、574 ページ*

指定したディレクトリの [午前 0 時以降]、[直近の 1 時間]、および [直近の 5 分間] のパフォーマンス データを表示するには、**[Status] > [Deployment] > [Directory Server Details（ディレクトリ サーバーの詳細）]** ページを選択します。

表示されるテーブルは、それぞれの時間のバインド（接続）および検索処理について下記の情報を表示します。

- **[Average]**、**[Most Recent]**、および **[Maximum]** 時間（ミリ秒単位）
- 処理の実行を試みた回数
- 失敗した回数

[Directory Performance] タブに戻るには、**[Close]** をクリックします。

Policy Broker について

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Policy Server の動作*、458 ページ
- *Filtering Service の動作*、465 ページ
- *Policy Server、Filtering Service、および State Server*、469 ページ

Websense Policy Broker は、ポリシー データ（クライアント、フィルタ、フィルタ コンポーネント、代理管理の設定を含む）と、配備全体に適用する特定のグローバル設定の両方へのアクセスを管理します。1 つの Policy Server インスタンス固有の設定（Filtering Service や Network Agent の接続など）は個別に保存されます。

Policy Broker の働きによって、複数 Policy Server 環境でも、ユーザー環境全体で共通のポリシーおよび一般的設定データのセットが共有されます。

1. 起動時に、各 Websense コンポーネントは、Policy Broker から適用可能な設定情報を要求します。
2. 稼働中のコンポーネントは、設定情報の変更について頻繁にチェックします。
3. プライマリまたはスタンドアロン Policy Broker は、管理者が Web Security manager で変更を行い [Save and Deploy] をクリックするたびに、そのデータベースを更新します。
4. 設定の変更の後、各コンポーネントは、Policy Broker を通じてその機能に影響する変更を要求し、受信します。

プライマリ Policy Broker のほかに、1 つ以上の Policy Broker の**レプリカ**をインストールできます。複製が作成されている環境では、Web Security manager で行われた変更は、プライマリ Policy Broker に保存されます。変更の後、各レプリカは、最新の更新を受け取るためにレプリカ上のデータのコピーを同期化します。

- Policy Broker モード（スタンドアロン、プライマリ、またはレプリカ）は、インストール時に設定されますが、後でコマンドライン ユーティリティを使用して後で変更することができます（例、スタンドアロン環境から複製環境への変更）。詳細については、ホワイト ペーパー 『Websense Policy Broker』 を参照してください。
- 複製環境では、ユーザー環境内の各 Policy Server インスタンスについて、Policy Broker の接続順序を設定できます。それによって、Policy Server に接続されたコンポーネント（Filtering Service など）が設定情報の更新のために最初にどこを検索するかが決まります。*Policy Broker の接続の検討*、457 ページを参照してください。

1 つの（スタンドアローン）Policy Broker または、プライマリ Policy Broker とレプリカをインストールしている場合、必ずポリシーおよび設定データのバックアップを定期的に行ってください。詳細は、*Websense データのバックアップと復元、492 ページ*を参照してください。

Policy Broker の接続の検討

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Policy Broker について、456 ページ*
- *Policy Server の動作、458 ページ*

複数 Policy Broker 環境（プライマリ Policy Broker と 1 つ以上のレプリカ）では、**[Settings] > [General] > [Policy Brokers]** ページにユーザーの環境の中の Policy Broker インスタンスのリストが表示されます。また、ネットワーク内の各 Policy Server が最初にどのインスタンスとの接続を試みるかも設定できます。

[Installed Policy Broker Instances（インストールされている Policy Broker インスタンス）] テーブルには以下の情報が含まれます。

- **[Host（ホスト）]** 列は、Policy Broker が実行しているコンピュータの IP アドレスまたはホスト名を示します。
- **[Type（タイプ）]** 列は、そのインスタンスがプライマリか、レプリカかを示します。プライマリ インスタンスは常にリストの先頭に示されます。
- インスタンスの **説明**。説明を更新するには、既存の説明の隣のペンシルアイコンをクリックします。
- 各 Policy Broker レプリカに対して**最後のポリシー同期化** が行われた時刻これは、レプリカが最後にプライマリ Policy Broker から更新されたポリシーおよび設定情報を受け取った時刻です。

ユーザーの環境内の Policy Server インスタンスが Policy Broker に接続する方法をカスタマイズするには、**[Policy Server Connections（Policy Server の接続）]** テーブルを使用します。テーブルには下記の項目があります。

- 各 Policy Server **[Host（ホスト）]** の IP アドレスまたはホスト名
- Policy Server インスタンスの **[Description（説明）]**。
- Policy Server インスタンスが Policy Broker に接続するとき使用する **[Connection Order（接続の順序）]**（IP アドレスのリスト）

接続の順序を変更するには、Policy Server の IP アドレスまたはホスト名をクリックします。それによって、[Policy Broker Connection Order] ウィンドウが開き、現在の接続の順序がリストされます。リスト内でインスタンスを上下に移動するには、下記の手順を実行します。

1. テーブルの行をクリックして、Policy Broker エントリを選択します。
2. **[Up（上）]** または **[Down（下）]** ボタンをクリックしてリストでエントリを移動します。
3. 移動する各エントリについて上記の手順を繰り返します。
4. 変更を完了したら、**[OK]** をクリックし、[Policy Brokers] ページに戻ります。
5. 変更をキャッシュするには、[Policy Brokers] ページで **[OK]** を再度クリックします。**[Save and Deploy]** をクリックするまで変更は適用されません。

Policy Server の動作

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Policy Server 接続の確認*、459 ページ
- *Policy Server インスタンスの追加と編集*、460 ページ
- *複数 Policy Server 環境での動作*、462 ページ
- *Policy Server IP アドレスの変更*、463 ページ
- *Filtering Service の動作*、465 ページ
- *Policy Server、Filtering Service、および State Server*、469 ページ

Policy Server は、他の Websense software コンポーネントを識別し、それらのステータスを追跡します。

the Web Security manager にログオンするとき、Policy Server のグラフィカルインターフェースにログオンします。

- Web Security manager が Policy Server と通信するように設定されるまで、それにログオンすることはできません。
- Websense ソフトウェア インストールが複数の Policy Server を含んでいる場合、Web Security manager へのログオン後に Policy Servers のインスタンスを切り替えることができます。
- Web Security manager で Policy Server のインスタンスを追加 / 削除することができます。

Web Security manager と 1 つの Policy Server インスタンスとの通信は、インストール時に確立されます。

多くのの環境では、1 つの Policy Server のみを必要とします。負荷分散のために、1 つの Policy Server は複数の Filtering Service および Network Agent インスタンスと通信することができます。しかし、非常に大きい組織（10,000 以上のユーザ）では、Policy Server の複数のインスタンスをインストールする

ことが有用である場合があります。追加の Policy Server をインストールする場合、Web Security manager に各インスタンスを追加します（*Policy Server 接続の確認、459 ページ*を参照）。

Policy Server 接続の確認

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Settings] > [General] > [Policy Servers] ページを使用して、Web Security manager と関連付けられているすべての Policy Server インスタンスの Policy Server 情報を確認します。

サブスクリプション キーを共有する複数の Policy Server インスタンスがある場合、1 つのインスタンスをプライマリ Policy Server にすることができます。他のインスタンスをセカンダリ インスタンスとして追加したとき、それらのインスタンスは、それらのキー情報をプライマリ インスタンスから受け取ります。それによって、設定プロセスを迅速化し、キー メンテナンスを簡略化できます（将来に新しいサブスクリプション キーを受け取る場合）。

- Web Security manager は、インストール時に 1 つのプライマリ Policy Server インスタンスと関連付けられます。これが Web Security manager のベース Policy Server になり、その IP アドレスと説明を変更することはできません。
- プライマリ Policy Server と関連付けられているセカンダリ Policy Server インスタンスについてリスト中で確認するには、その Policy Server 名または IP アドレスの隣の [+] 記号をクリックします。
- ページに表示される情報を更新するには（例、最新のサブスクリプション キー情報または Policy Broker 接続を表示するため、および最近 Web Security manager に自動的に追加された可能性がある Policy Server のインスタンスを表示するため）、コンテンツ ペインの上部のツールバーの **[Refresh（リフレッシュ）]** ボタンをクリックします。
- ベース Policy Server 以外の Policy Broker に接続している Policy Server インスタンスには、現在設定可能でないことを示すアイコン（  ）が付けられます。

各 Policy Server エントリには短い説明が含まれます。プライマリ Policy Server エントリはまた下記の項目も含みます。

- インスタンスおよびそのセカンダリに関連付けられているキー、サブスクリプション レベル（例、Web Security、Web Security Gateway）を含むサブスクリプション情報
- Policy Server が使用している Policy Broker の IP アドレス

  複数 Policy Broker 配備の場合、**[Settings] > [General] > [Policy Brokers]** ページを順に選択して、Policy Server が Policy Broker に接続する方法を設定します。

追加の Policy Server を Web Security manager と関連付けるには、**[Add]** をクリックします。また、選択したインスタンスの設定情報を編集するには、Policy Server の IP アドレスまたは名前をクリックします（*Policy Server インスタンスの追加と編集*、460 ページを参照）。

Web Security manager に Policy Server インスタンスが自動的に追加される場合もあります。たとえば、Policy Server シンスタンスが Policy Broker レプリカと同じコンピュータ上にインストールされている場合、その Policy Server インスタンスは自動的に [Policy Servers] ページに表示されます。この場合でも、必要に応じてこれらのインスタンスを編集できます（例、インスタンスの説明を変更する）。

1 つ以上の Policy Server エントリをマークし、**[Delete（削除）]** をクリックすると、Web Security manager と選択した Policy Server との接続が削除されます。

- それによって、Web Security manager から Policy Server インスタンスが削除されますが、Websense Policy Server サービスがアンインストールまたは停止されることはありません。ベース Policy Server インスタンスを削除することはできません。
- 配備から Policy Server インスタンスを削除するときは必ず、Web Security manager の [Policy Servers] ページでもそのインスタンスを削除してください。

  Policy Server を実行している 1 台のコンピュータを停止し、その後新しいコンピュータを起動し、それに古い IP アドレスを割り当てた場合でも、新しいコンピュータにインストールされている Policy Server インスタンスは古いインスタンスからサブスクリプション キー情報を自動的には継承しません。Web Security manager から古いインスタンスを削除したあとで、新しいインスタンスを追加する必要があります。

Policy Server 接続を追加または編集したら、[Policy Servers] ページで **[OK]** をクリックして、その変更をキャッシュします。**[Save and Deploy（保存と配備）]** をクリックするまで、変更は適用されません。

Policy Server インスタンスの追加と編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Settings] > [General] > **[Add Policy Server（Policy Server の追加）]** または **[Edit Policy Server（Policy Server の編集）]** ページを使用して、新しい Policy Server インスタンスを Web Security manager と関連付けるか、または既存の Policy Server の設定情報を更新します。

1. Policy Server インスタンスの **IP アドレスまたは名前**と通信 **Port（ポート）**を入力または編集します。デフォルト ポートは **55806** です。
2. 選択されている Policy Server インスタンスの **[Description（説明）]** を入力または更新します。

   ベース Policy Server の説明を変更することはできません。

3. これが **Primary**（プライマリ）または **Secondary**（セカンダリ）Policy Server のどちらであるか指示します。
   - プライマリ Policy Server は、Web Security manager に関連付けられている他の Policy Server インスタンスとは異なるサブスクリプション キーを持っています。
   - セカンダリ Policy Server は、すでに Web Security manager と関連付けられている別の Policy Server と同じサブスクリプション キーを使用します。
4. これが**セカンダリ** Policy Server である場合、下記の手順を実行します。
   a. セカンダリ Policy Server にそのキーを提供するプライマリ Policy Server の IP アドレスを選択します。
   b. このセカンダリ Policy Server がプライマリ Policy Server から Directory Service 設定を継承するかどうかを指定します。

      この設定は User Service がディレクトリに接続し、ユーザーおよびグループ情報を取得するために使用します（[Settings] > [General] > [Directory Services] ページで設定されます）。
   c. **[OK]** をクリックして [Policy Servers] ページに戻り、次に [Policy Servers] ページでもう一度 **[OK]** をクリックして変更をキャッシュに保存します。**[Save and Deploy]** をクリックするまで変更は適用されません。

   セカンダリ Policy Server を追加した後、Policy Server の **[Switch]** ボタン使用して新しい Policy Server インスタンスに接続できるようになるには、その前に、TRITON コンソールをログオフしてから、もう一度ログオフしなければならない場合があります。
5. **プライマリ** Policy Server の場合、新しいインスタンスのために登録されている **[Use the current subscription key（現在のサブスクリプション キーを使用）]** または **[Enter a subscription key（サブスクリプション キーの入力）]** のどちらかを選択します。
   - 既存のエントリを編集しているときは、現在のサブスクリプション キーとサブスクリプション タイプがラジオ ボタンの下に表示されます。
   - **[Verify Policy Server（Policy Server の確認）]** をクリックして、Web Security manager が新しい Policy Server と通信できることを確認します。[Use the current subscription key（現在のサブスクリプション キーを使用）] を選択していて、接続が正常である場合、サブスクリプション キーが表示されます。
   - 新しい Policy Server インスタンスにすでにキーが登録されているかどうか明白でないときは、手動でキーを入力するオプションを選択するか、または **[Verify Policy Server]** をクリックして、Web Security manager がそのインスタンスの既存のキーを検出するかどうか確かめます。
6. [Policy Server s]ページに戻るために、**[OK]** をクリックします。**[OK]**をクリックして、変更をキャッシュしなければなりません。**[Save and Deploy]** をクリックするまで変更は適用されません。

複数 Policy Server 環境での動作

Web Security Help | Web Security ソリューション | バージョン 7.8.x

分散環境、または多数のユーザを抱える配備では、複数の Policy Server インスタンスをインストールすることが適切である場合があります。これには、いくつかの特別な配慮を必要とします。

- ポリシー情報は Policy Broker によって管理されますから、**[Save and Deploy]** をクリックしたとき、ポリシーの変更がすべての Policy Server インスタンスで利用可能になります。
- 多くのグローバル設定（リスク クラス定義とアラート オプションなど）も Policy Server インスタンス間で共有されます。
- 1 つの Policy Server に固有の設定（Filtering Service および Network Agent 接続など）はローカルに各 Policy Server に保存され、配信されません。
- 時間ベースのアクション（Confirm（確認）、Quota（割り当て）、Password Override（パスワード無効化）、または Account Override（アカウント無効化））を正しく適用するためには、 1 つ以上の Websense State Server が必要です。State Server はこれらのフィルタリング アクションと関連する時間情報の共有を可能にし、狙いどおりの正確なインターネット アクセスをクライアントに提供できるようになります（*Policy Server、Filtering Service、および State Server、469 ページ*を参照）。

Web Security manager で複数の Policy Server インスタンスを切り替えるには下記のようにします。

1. Web Security ツールバーで、現在の Policy Server の IP アドレスの横にある **[Switch（切り替え）]** をクリックします。

   現在の Policy Server インスタンスに対する保存されていない変更がある場合、警告プロンプトが表示されます。変更の保存のために現在の Policy Server との接続を維持するには、**[Cancel（キャンセル）]** をクリックします。
2. **[Connect to（接続の設定）]** リストから Policy Server IP アドレスまたはホストネームを選択します。
3. **[OK]** をクリックします。

選択されている Policy Server に自動的にログオンし、Web Security manager インターフェースが更新されます。

Policy Server IP アドレスの変更

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Policy Server コンピュータの IP アドレスを変更する前に、**コンピュータ上のすべての Websense サービスを停止してください。**

IP アドレスを変更した後、ポリシーの適用を再開する前に、Web Security manager、Policy Server、およびその他の Websense サービスによって使用される Websense 設定ファイルを手動で更新する必要があります。

ステップ 1：Web Security manager の設定の更新

Policy Server と接続する新しい IP アドレスを使用するように Web Security manager を更新します。

1. TRITON 管理サーバー上で **Websense Web Reporting Tools** と **Websense TRITON - Web Security** のサービスを停止します（必要であれば）。

   TRITON コンソール と Policy Server がこの同じコンピュータにインストールされている場合、前記のサービスはすでに停止しているはずです。
2. 下記のディレクトリに移動します：

   ```
   Websense\Web Security\tomcat\conf\Catalina\localhost\
   ```
3. **mng.xml** ファイルを見つけ、別のディレクトリにファイルのバックアップ コピーを作成します。
4. テキスト エディタ（Notepad または vi など）で **mng.xml** を開き、古い Policy Server IP アドレスの各インスタンスを新しいものに置き換えます。

   Policy Server IP アドレスは 2 回あらわれます：**ps/default/host** 値としておよび **psHosts** 値として。
5. 完了したら、ファイルを保存し、閉じます。

このセクションの残りの設定の更新を完了するまで、すべてのサービスを再起動しないでください。

ステップ 2：Policy Server の更新

Policy Server 設定ファイルと Websense コンポーネント間の通信を設定するために使用される初期化ファイルを更新します。

1. Policy Server コンピュータ上のすべての Websense サービスをまだ停止していなければ、それらのサービスを停止します（*Websense サービスの停止と起動、477 ページ*を参照）。
2. Websense **bin** ディレクトリ（デフォルトでは C:\Program Files、*または* Program Files（x86）\Websense\Web Security\bin、もしくは /opt/Websense/bin/）に移動します。

3. **config.xml** ファイルを見つけ、他のディレクトリにファイルのバックアップ コピーを作成します。
4. テキスト エディタで **config.xml** を開き、古い Policy Server IP アドレスの各インスタンスを新しいものに置き換えます。
5. 完了したら、ファイルを保存し、閉じます。
6. **bin** ディレクトリで **websense.ini** ファイルを見つけ、別のディレクトリにバックアップ コピーを作成します。
7. テキスト エディタで **websense.ini** を開き、古い Policy Server IP アドレスの各インスタンスを新しいものに置き換えます。
8. 完了したら、ファイルを保存し、閉じます。

ステップ 3：Log Database 接続の確認

Log Database に対する ODBC 接続を確認するために、Policy Server コンピュータ上の Windows ODBC Data Source Administrator を使用します。

1. 下記のどちらかの Data Sources ツールを開きます。
   - Windows Server 2012：**[Server Manager] > [Tools] > [ODBC Data Sources 64-bit（ODBC データソース 64 ビット）]** を順に選択します。
   - Windows Server 2008：**[Start] > [Administrative Tools（管理ツール）] > [Data Sources（ODBC）]** を順に選択します。
2. **[System DSN（システム DSN）]** タブで適切なデータソース名（デフォルトは、**wslogdb70**）を選択し、**[Configure（設定）]** をクリックします。
3. 正しいデータベース サーバー コンピュータが選択されていることを確認し、**[Next（次へ）]** をクリックします。
4. データベースとの接続のために使用される資格情報を入力し、**[Next]** をクリックします。
5. 次の 2 つの画面でデフォルトを受け入れ、次に **[Test Data Source（データソースのテスト）]** をクリックします。

> **注意**
> テストが失敗した場合、データベース サーバー コンピュータ名を確認し、再度試みます。
>
> コンピュータ名は正しいが、テストが失敗し続ける場合、正しい接続ポートが使用されているか、ファイアウォールが選択されているポート上の通信を許可しているかを確認してください。

ステップ 4：Websense サービスの再起動

1. Policy Server コンピュータを再起動します。コンピュータ上のすべての Websense サービスが正常に再起動することを確認します。
2. この Policy Server の設定のために使用される Web Security manager が別のコンピュータ上にインストールされている場合は、そのコンピュータ上の **Websense Web Reporting Tools** と **Websense TRITON - Web Security** のサービスを再起動します。

> **注意**
> TRITON コンソールが Policy Server と同じコンピュータ上にインストールされている場合、管理者はログオンするために新しい IP アドレスを使用する必要があります。

Filtering Service の動作

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Filtering Service 詳細の確認*、466 ページ
- *Master Database ダウンロードの再開*、468 ページ
- *Policy Server、Filtering Service、および State Server*、469 ページ
- *Content Gateway の動作*、473 ページ

Filtering Service は、インターネット活動を管理するために Network Agent、Content Gateway、またはサードパーティ統合製品と共に動作する Websense ソフトウェア コンポーネントです。ユーザがあるサイトを要求すると、Filtering Service が要求を受信し、どのポリシーを適用するかを決定し、サイトが許可されるかブロックされるかについて決定するために適用可能なポリシーを使用します。

各 Filtering Service インスタンスは、Websense Master Database から自身のコピーをダウンロードして、インターネット要求の処理方法を決定するために使用します。

複数の Filtering Service インスタンスがある場合は、時間ベースの アクション（Confirm（確認）、Quota（割り当て）、Password Override（パスワード無効化）、または Account Override（アカウント無効化））の正しい適用を有効化するために、追加のコンポーネントとして Websense State Server が必要とされます。State Server はこれらのフィルタリング アクションと関連する時間情報の共有を可能にし、狙いどおりの正確なインターネット アクセスをクライアントに提供できるようになります（*Policy Server、Filtering Service、および State Server、469 ページ*を参照）。

また Filtering Service は Log Server にインターネット アクティビティについての情報を送信し、この情報は記録され、レポーティングで使用できるようになります。

Web Security manager の System ダッシュボード上の **[Filtering Service Summary（フィルタリング サービス要約）]** で、現在の Policy Server と関連付けられている各 Filtering Service インスタンスの IP アドレスと現在のステータスがリストされます。選択された Filtering Service の詳細情報を見るためには、Filtering Service の IP アドレスをクリックします。

Filtering Service 詳細の確認

Web Security Help | Web Security ソリューション | バージョン 7.8.x

各 Filtering Service インスタンスのステータスを確認するためには、**[Satus] > [Dashboard] > [Filtering Service Details（Filtering Service 詳細）]** ページを順に選択して使用します。このページでは下記の情報がリストされます：

- Filtering Service の IP アドレス
- 選択されたインスタンスが動作しているかどうか
- Filtering Service のバージョン

  これは、適用されたすべてのホットフィックスも含めて、Websense ソフトウェア バージョンと一致するはずです。
- Filtering Service コンピュータのオペレーティング システム
- Websense ソフトウェア プラットホーム

  これは、Web Security ソリューションがスタンド アローン モードで実行しているか、あるいは Content Gateway またはサードパーティ製品と統合されているかを示します。
- 選択された Filtering Service が通信しているあらゆる Network Agent インスタンスの IP アドレスとステータス。
- 選択された Filtering Service が通信しているあらゆる Content Gateway インスタンスの IP アドレスとステータス

[Close] をクリックして Web Security Dashboard に戻ります。

Master Database ダウンロード ステータスの確認

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ネットワークの各 Filtering Service インスタンスは Master Database のコピーを自分用としてダウンロードします。Web Security manager を使用しているとき、[Status] > [Alerts] ページに、Master Database のダウンロードが進行中である場合はステータス メッセージ表示され、またダウンロードに失敗した場合はアラートメッセージが表示されます。

最近または進行中のデータベース ダウンロードの詳細情報を見るためには、Web Security Dashboard ツールバー上で **[Database Download（データベース ダウンロード）]** をクリックします。[Database Download] ページは、現在の Policy Server に関連付けられている各 Filtering Service インスタンスのエントリを含んでいます。

最初に [Database Download] ページで表示されるのは簡単なダウンロード要約であり、データベースがどこにダウンロードされたか、どのデータベース バージョンがダウンロードされたか、そしてダウンロードが成功したかどうかが示されます。この要約表示から、下記のことを行うことができます：

- 1 つの Filtering Service のためにデータベースのダウンロードを開始する（**[Update（更新）]** をクリックします）。
- リストされているすべての Filtering Service インスタンスのためにデータベース ダウンロードを開始する（**[Update All（すべて更新）]** をクリックします）。
- 1 つまたはすべての進行中の更新をキャンセルする。

選択されている Filtering Service についてデータベース ダウンロードの詳細なステータスを確認するためには、右側のリストで IP アドレスをクリックします。

- 選択されている Filtering Service のダウンロードに問題が発生した場合、問題に対処するための推奨事項が表示されます。
- 選択されている Filtering Service のデータベース ダウンロードを手動で開始するには、**[Update]** をクリックします。

データベース ダウンロード中に、ダウンロード処理の各段階の詳細な進捗情報がステータス画面に表示されます。進捗情報を非表示にし、Web Security manager で作業を続けるには、**[Close]** をクリックします。

Master Database ダウンロードの再開

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Master Database ダウンロードが中断された場合、Websense ソフトウェアは自動的にダウンロードの再開を試みます。Filtering Service がダウンロード サーバーと再接続できる場合、ダウンロードは中断されたところから再開します。

失敗または中断した ダウンロードを手動で再起動することができます。これは、中断したポイントからのダウンロードを再開するのではなく、最初からのプロセスを再起動します。

1. Web Security manager で **[Status] > [Dashboard]** を順に選択し、**[Database Download]** をクリックします。
2. 中断している処理を中止するには、**[Stop All Updates（すべての更新の中止）]** をクリックします。
3. 最初からのダウンロード プロセスを再起動するには、Filtering Service インスタンスを選択し、**[Update]** または **[Update All]** をクリックします。

学校 YouTube に対する Filtering Service サポート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Web Security または Web Filter ソフトウェアを配備する教育機関は、YouTube for Schools（学校向け YouTube）を有効にする Filtering Service 設定パラメータを利用することができます。この YouTube サービスは、他の YouTube コンテンツがブロックされている場合でも、学校ネットワーク内部からの教育ビデオへのアクセスを提供します。

> **注意**
> Web Security Gateway および Gateway Anywhere ソフトウェアまたはアプライアンス配備では、Filtering Service を介してではなく、Content Gateway を介して YouTube for Schools を有効にすることができます。

プログラムに加入し、教育機関アカウント コードまたは ID を入手したら、下記のことを行います：

- Web Security manager で [Settings] > [General] > [Filtering（フィルタリング）] ページを順に選択し、ページ最下部の **[Enable search filtering（検索フィルタリングを有効化する）]** が選択されていることを確認します。

  [YouTube in Schools（学校 YouTube）]] 機能を利用するには、検索フィルタリングが有効でなければなりません。

  検索フィルタリングが有効になっていなければ、**[OK]** と **[Save and Deploy（保存と配備）]** をクリックし、変更をキャッシュして適用します。

- [YouTube in Schools]アクセスが認められるクライアントに対して YouTube が許可されていなければなりません。

上記の設定が完了したら、組織の環境中の各 Filtering Service インスタンスについて下記の手順を実行します：

1. Filtering Service コンピュータ上で Websense **bin** ディレクトリ（デフォルトでは、C:\Program Files または Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）に移動します。
2. **eimserver.ini** ファイルのバックアップ コピーを別の場所に作成します。
3. 元の **eimserver.ini** ファイルを開き、下記の行を追加します：

   ```
   [SafeSearchCustomValues]
   YouTubeEDUFilter=<school_account_code>
   ```

   <school_account_code> を YouTube から受け取る実際のコードまたは ID に置き換えます。
4. ファイルを保存し、閉じます。
5. Filtering Service を再起動します。
   - Windows: [Windows Services（Windows サービス）] ツールで **Websense Filtering Service** を再起動します。
   - Linux: /opt/Websense/WebsenseDaemonControl コマンドを使って **Filtering Service** を再起動します。

Policy Server、Filtering Service、および State Server

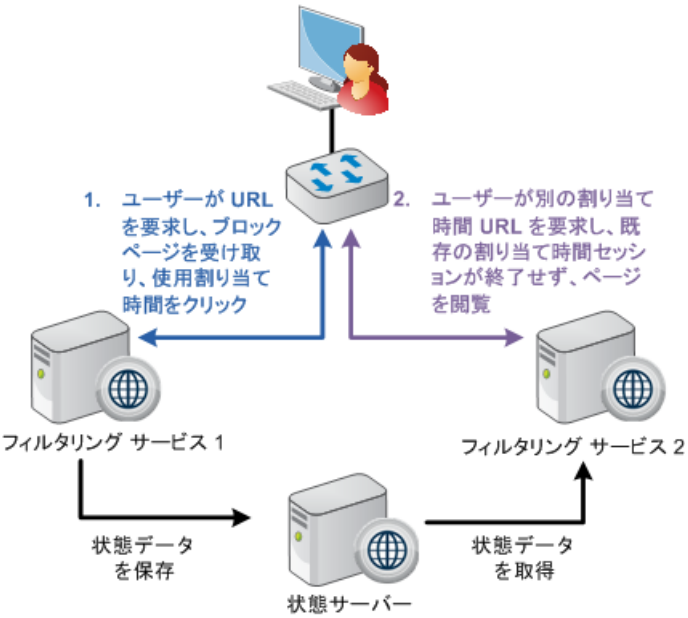
Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Policy Server の動作*、458 ページ
- *Filtering Service の動作*、465 ページ
- *処置*、68 ページ
- *パスワード無効化*、105 ページ
- *アカウントの無効化*、106 ページ

お客様の配備で同じユーザーの要求を処理する複数のインスタンスの Filtering Service がある場合、オプションのコンポーネントである **Websense State Server**（**Websense ステート サーバー**）をインストールし、適切な時間ベースのアクション（Quota（割り当て）、Confirm（確認））または無効化（Password Override（パスワード無効化）、Account Override（アカウント無効化））を有効化することができます。

State Server をインストールすると、それと関連付けられている複数の Filtering Service インスタンスは時間情報を共有するようになり、その結果、ユーザーは割り当て、確認、または無効化セッション時間の適切な配分を受けるようになります。

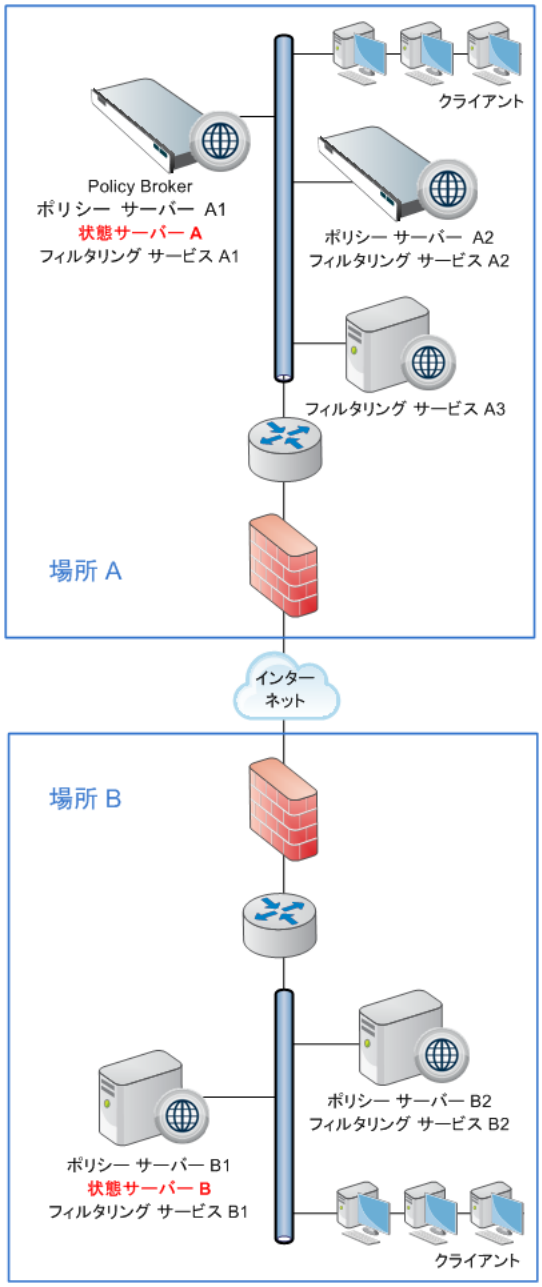


State Server は、通常、1 台の Policy Server コンピュータにインストールされ、**論理的配備** ごとにただ 1 つの State Server インスタンスが必要とされます。論理的配備とは、同じセットのユーザーからの要求を処理する Policy Server および Filtering Service インスタンスの任意のグループを意味します。

- 同じ State Server インスタンスと通信するすべての Filtering Service インスタンスは同じタイム ゾーンを共有しなければならず、すべてのコンピュータ上の時間は同期していなければなりません。
- 各 Filtering Service インスタンスが通信できるのは、ただ 1 つの State Server だけです。
- 同じ Policy Server と関連付けられているすべての Filtering Service インスタンスは同じ State Server と通信しなければなりません。
- 複数の Policy Server インスタンスはただ 1 つの State Server を共有することができます。

Web Security manager の **[Settings] > [General] > [Filtering]** ページで、Policy Server が通信する State Server インスタンスを設定します（*フィルタリング設定値の設定、81 ページ*を参照）。

地理的に分散した組織において個別の場所でそれぞれ独自の Policy Server および Filtering Service インスタンスがある場合、個別の場所ごとに（Policy Server コンピュータまたは V-Series アプライアンスに）1 つの State Server インスタンスを配備してください。例：



すべての要求が集中的場所を通じて管理される組織では、ただ 1 つの State Server インスタンスが必要とされるだけです。

サードパーティ SIEM ソリューションとの統合

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Settings] > [General] > [SIEM Integration（SIEM 統合）] ページを順に選択して、ログ データを Filtering Service からサポートされている Security Information and Event Management（セキュリティ情報およびイベント管理、SIEM）ソリューションに送信するように Websense ソフトウェアを設定します。

このページを使用して SIEM 統合を有効にする前に、お客様の環境の各 Policy Server について 1 つのインスタンスの Websense Multiplexer をそれぞれインストールしなければなりません。

組織の環境の各 Policy Server インスタンスについて下記の手順を実行します。

1. **[Enable SIEM integration for this Policy Server（この Policy Server のために SIEM 統合を有効にする）]** を選択し、SIEM 統合機能をアクティブにします。
2. SIEM 製品のホスト コンピュータの **[IP address or hostname（IP アドレスまたはホストネーム）]** と SIEM データの送信で使用する通信 **[Port（ポート）]** を提供します。
3. SIEM 製品へのデータ送信で使用する **[Transport protocol（トランスポート プロトコル）]**（UDP または TCP）を指定します。
4. 使用する **[SIEM format（SIEM フォーマット）]** を指定します。これによって、統合機能へのログ データ送信で使用される文字列の構文が決まります。
   - 利用可能なフォーマットは、syslog/CEF（ArcSight）、syslog/ キー値ペア（Splunk およびその他）、syslog/LEEF（QRadar）、およびカスタムです。
   - [Custom（カスタム）] を選択すると、テキスト ボックスが表示されます。使用しようとする文字列を入力または貼り付けます。**[View SIEM format strings（SIEM フォーマット文字列の表示）]** をクリックし、レファレンスまたはテンプレートとして使用する文字列サンプルのセットを表示します。
   - 非カスタム オプションを選択すると、フィールドと値のキーを示すサンプルの **[Format string（フォーマット文字列）]** が表示されます。
5. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy（保存と配備）]** をクリックするまで、変更は適用されません。

変更を保存すると、Websense Multiplexer は Filtering Service と接続し、Log Server と選択されている SIEM 統合機能へログ データを配信するジョブを引き受けます。

同じデータが Filtering Service から Log Server と SIEM 製品の両方に送られますが、Log Server はデータ処理タスク（ヒットでなくアクセスの記録やログ記録の集約など）を行うように設定されているかもしれません。SIEM 製品はこのようなデータ処理タスクを行わないので、SIEM のエントリが Log Database のレコードよりも多くなるかもしれません。

SIEM 統合に渡されるデータの詳細については、[サードーパーティ SIEM 製品との Web Security の統合] を参照してください。リンクされたドキュメントのサブセクションは、カテゴリ番号、説明コード、理由文字列、および SIEM 出力に含まれている他の情報に関するマッピング情報を提供します。

Content Gateway の動作

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Filtering Service の動作*、465 ページ
- *Policy Server の動作*、458 ページ
- *Content Gateway 接続の管理*、474 ページ

Content Gateway は、Websense Web Security Gateway および Gateway Anywhere 配備で高性能の Web プロキシ サービスを提供する Linux 専用 Websense ソフトウェア コンポーネントです。Content Gateway は、Websense Data Security および Email Security Gateway ソリューションによってプロキシとしても利用されます。

Websense Web Security Gateway および Gateway Anywhere 配備で Content Gateway は下記の機能を提供します：

- 悪質な Web コンテンツからネットワークを保護するためのリアルタイム コンテンツ スキャンとウェブサイトの分類。これはとりわけ Web 2.0 サイトに対して有益です。というのも、Web 2.0 サイトの複数ソースと動的性格は静的分類の有効性を制約するからです。
- 感染したファイルや悪意あるファイルを検出し、この種のファイルのアップロードとダウンロードをブロックする高度なファイル スキャン
- HTTP および HTTPS をトンネルするインバウンドおよびアウトバウンド プロトコルの検出とプロトコルベースのポリシーの実施の適用

Content Gateway は Filtering Service と連携し、下記の両方の分類に基づいて要求を管理します。

- Master Database またはカスタム URL 定義による静的分類
- コンテンツ スキャンおよび分析に基づく動的分類

インストール時に Content Gateway は 1 つの Policy Server インスタンスとの接続を確立します。この接続により下記のことが実現されます：

- Policy Server がサブスクリプション キー情報を Content Gateway に渡せるようにし、2 つの管理コンソールでキーを維持する必要性を緩和します。
- Filtering Service による Content Gateway との接続に関する情報を Web Security manager に提供します。
- Web Security manager の [Settings] > [General] > [Content Gateway Access（Content Gateway アクセス）] ページに取り込むために使用され、Content Gateway Manager を TRITON コンソール内部から起動できるようにします。

Content Gateway 接続の管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Settings] > [General] > [Content Gateway Access（Content Gateway アクセス）] ページを使用して、現在の Policy Server と関連付けられている複数の Content Gateway インスタンスの設定およびステータス情報を確認したり、選択されているインスタンスのために Content Gateway manager を起動したりします。

Content Gateway のインスタンスが Policy Server に登録されると、[Content Gateway Access] ページはその Content Gateway の IP アドレス、ホスト名およびステータス情報によって自動的の更新されます。この情報は下記の 3 つのテーブルの 1 つで表示されます：

- Content Gateway がクラスタの一部であると、そのクラスタ名をタイトルとするテーブルが表示されます。クラスタ中のすべての Content Gateway インスタンスがリストされます。複数のクラスタがあると、複数のテーブルが表示されます。
- Content Gateway がクラスタになっていないと、それは[Unclustered Content Gateway instances（非クラスタ Content Gateway インスタンス）] テーブルで示されます。
- Policy Server が Content Gateway インスタンスと通信できないと、それは [Not Responding（非応答）] テーブルで表示されます。このテーブルが表示されるのは、Policy Server が登録されている Content Gateway インスタンスと通信できない場合だけです。

リストされている任意のインスタンスのために Content Gateway manager を起動するには、テーブルの **[IP Address（IP アドレス）]** 列の対応するリンクをクリックします。

インスタンスの説明を更新して Content Gateway 接続の管理を容易にするには、インスタンスの IP アドレスの横のラジオ ボタンをオンにし、**[Edit Description（説明の更新）]** をクリックします。

Content Gateway インスタンスがアンインストールされたか、または移動されたために、そのインスタンスが **[Not Responding]** テーブルで表示される場合は、そのインスタンス名の横のラジオ ボタンをオンにし、**[Delete（削除）]** をクリックします。

Content Gateway 説明の編集または古くなったエントリの削除を終えたら、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

監査ログの表示とエクスポート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense ソフトウェアは、管理者による Web Security manager へのアクセスとポリシーおよび設定に対する変更とを示す監査履歴を提供します。この情報はポリシー許可を与えられている優先管理者にだけ有効です（*Super Administrator 許可*、409 ページを参照）。

指定済み管理者は、その処理対象クライアントのインターネット アクティビティに対して高度な管理ができます。監査ログを通して変更をモニタすることで、お客様の組織の使用許容ポリシーに従って、責任を持って、この管理が処理されることを保証することができます。

監査ログを表示し、必要に応じて、その選択されている部分を Excel スプレッド シート（XLS）ファイルにエクスポートするためには、**[Status（ステータス）] > [Audit Log（監査ログ）]** ページを順に選択し使用します。

監査レコードは 60 日間保存されます。60 日間より長く監査レコードを保持するためには、定期的にログをエクスポートするエクスポート オプションを使用します。エクスポートは、監査ログからレコードを除去しません。

[Audit Log（監査ログ）] ページが開くと、最新のレコードが表示されます。古いレコードを見るためには、スクロールバーとログの上のページング ボタンを使用します。

ログは下記の情報を表示します。項目が省略されている場合、ポップアップ ウィンドウで完全なレコードを表示するためにエントリの一部をクリックします。

列	説明
Date（日付）	タイムゾーンで調整された変更の日付と時刻。 監査ログでデータの一貫性を保証するために、Websense コンポーネントが稼働しているすべてのコンピュータで日付と時刻の設定が同期していることを確認してください。
User（ユーザー）	変更を行った管理者のユーザ名。

列	説明
Server（サーバー）	変更で影響を受ける Policy Server を実行しているコンピュータの IP アドレスまたは名前。 これは、[Settings（設定）] タブ上で行われた変更等の Policy Server に影響を与える変更の場合にだけ表示されます。
Role（ロール）	変更の影響を受ける指定済み管理ロール。 変更が指定済み管理者ロールで管理される処理対象クライアントとして明示的に割り当てられているクライアントに影響を与える場合、その変更は Super Administrator ロールに影響を与えると表示します。変更がロールに割り当てられているネットワーク範囲、グループ、ドメイン、または組織単位のメンバーであるクライアントに影響を与える場合、その変更は指定済み管理者ロールに影響を与えると表示します。
Type（タイプ）	ポリシー、カテゴリ フィルタ、またはログオン / ログオフのような変更された設定要素。
Element（エレメント）	カテゴリ フィルタ名またはロール名のような変更された特定のオブジェクトの識別子。
Action（アクション）	追加、削除、変更、ログオン、等々のような実行された変更の種類。
Previous（前回）	変更前の値。
Current（現在）	変更後の新しい値。

すべてのレコードですべての項目が表示されるわけではありません。例えば、ロールはログオン / ログオフ レコードでは表示されません。

監査ログ レコードをエクスポートするためには、下記のようにします：

1. **[Export range（エクスポート範囲）]** リストから期間を選択します。
   全部の監査ログ ファイルをエクスポートするには、**[Last 60 days（最新 60 日間）]** を選択します。
2. **[Go（実行）]** をクリックします。
   コンピュータに Microsoft Excel が インストールされている場合、エクスポートされたファイルが開きます。ファイルを保存または印刷するためには、Excel のオプションを使用します。
   コンピュータに Microsoft Excel がインストールされていない場合、ソフトウェアを指定するか、ファイルを保存するために、画面上の指示に従ってください。

Websense サービスの停止と起動

Web Security Help | Web Security ソリューション | バージョン 7.8.x

コンピュータが再起動するたびに Websense サービスが起動するように設定されています。しかし、ある場合には、コンピュータの再起動とは別に、1 つ以上の製品コンポーネントを停止または起動する必要があります。

> **注意**
> Filtering Service がマスタ データベースをダウンロードしている途中であると、ダウンロードが完了するまで、それは停止しません。

すべての **Websense サービス**を停止する場合、常に下記の順序でポリシー サービスを終了してください：

1. Websense Policy Server
2. Websense Policy Broker
3. Websense Policy Database

問題が特に Policy Broker または Policy Database と関連しない場合、これらのサービスを再起動することはほとんど必要ありません。可能なかぎり、これらのサービスを再起動することを避けてください。

すべての Websense サービスを起動する場合、常にシャットダウンとは逆の順序でポリシー サービスを起動してください（Policy Database が最初で、Policy Server が最後です）。

Real-Time Monitor と関連付けられているサービスを停止する場合は下記のようにしま。

- TRITON - Web Security サービスと Websense Web Reporting Tools サービスも停止します。
- Real-Time Monitor サービスを下記の順序で終了します：
  1. Websense RTM Client
  2. Websense RTM Server
  3. Websense RTM Database

Start the Real-Time Monitor サービスをシャットダウンとは逆の順序で起動します（RTM Database が最初で、RTM Client が最後です）。

管理コンソールから

条件無し優先管理者（admin を含む）および適切な許可をもつ指定済み管理者は、Web Security manager の **[Status] > [Deployment]** ページからサービスを停止および起動できます。

サービスの起動および停止は、[Policy Server Map] または [Component List] のどちらのタブからでも実行できます。

- [Policy Server Map] タブの場合、[Policy Server] アイコンまたは IP アドレスをクリックし、その後関連するコンポーネントの **[Start]** または **[Stop]** リンクをクリックします。
- [Component List] タブの場合、リストで適切なコンポーネントを見つけ、その後 **[Start]** または **[Stop]** リンクをクリックします。

Windows

Windows を実行しているコンピュータの場合、下記の手順を使って**個々の**サービスを停止または起動します。

1. 下記のどちらかの Windows のサービス ツールを開きます。
   - Windows Server 2012：**[Server Manager] > [Tools] > [Services]**
   - Windows Server 2008：**[Start] > [Administrative Tools] > [Services]**
2. Websense サービス名を右クリックし、次に **[Stop]** または **[Start]** を選択します。

コンピュータ上ですべてのサービスを起動、停止、または再起動するには、下記の手順を実行します。

1. Websense **bin** フォルダ（C:\Program Files、*または* Program Files（x86）\Websense\Web Security\bin）に移動します。
2. 下記のいずれかのコマンドを使用してサービスを停止、起動、または再起動します。

```
WebsenseAdmin start
WebsenseAdmin stop
WebsenseAdmin restart
```

Linux

Linux コンピュータには、デーモンの停止と起動で使用できる 下記の 2 つのツールがあります。

- **WebsenseAdmin** スクリプトは、コンピュータ上の**すべて**のデーモンを起動、停止、および再起動します。
- **WebsenseDaemonControl** スクリプトは**個々の**デーモンを起動および停止します。

警告

kill コマンドはサービスを壊す可能性があるので、このコマンドを使って Websense サービスを停止しないでください。

WebsenseAdmin スクリプトを使用して、すべてのデーモンを起動または停止するには、下記の手順に従います：

1. **/opt/Websense** ディレクトリへ移動します。
2. 次のコマンドで、Websense サービスのステータスをチェックします：

   ```
   ./WebsenseAdmin status
   ```

3. 下記のコマンドで、すべての Websense サービスを停止、起動、または再起動します：

   ```
   ./WebsenseAdmin stop
   ./WebsenseAdmin start
   ./WebsenseAdmin restart
   ```

WebsenseDaemonControl スクリプトを使用して、1 つのデーモンを起動または停止するには下記の手順に従います：

1. **/opt/Websense** ディレクトリへ移動します。
2. 下記のコマンドを入力します：

   ```
   WebsenseDaemonControl
   ```

   インストールされているコンポーネントのリストが表示され、各プロセスが動作中であるか、または停止しているかが示されます。
3. コンポーネントと関連付けられている文字を入力し、関連付けられているプロセスを起動または停止します。リストを更新するには、**R** を入力します。
4. 完了したら、**Q** または **X** を入力してツールを終了します。

Websense アプライアンス

Websense アプライアンス上では、Appliance Manager を使用して Websense サービスを停止、起動および再起動します。

サービスを再起動するには下記の手順に従います：

1. [Status] > [General] ページに移動します。このページは、Appliance Manager にログオンするとデフォルトで表示されます。
2. [Network Agent] セクションへスクロールし、**[Restart Module（モジュールの再起動）]** をクリックします。
3. Network Agent モジュールが再起動したら、Web Security セクションに移り、**[Restart Module（モジュールの再起動）]** をクリックします。

（おそらくメンテナンス タスク中に）サービスを停止するには下記の手順に従います：

1. [Status] > [General] ページの [Network Agent] セクションへスクロールし、**[Stop Services（サービスの停止）]** をクリックします。
2. [Websense Web Security] セクションで、やはり **[Stop Services（サービスの停止）]** をクリックします。
3. 再びサービスを起動できるようになったら、下記のようにします：
   a. [Websense Web Security] セクションへ移り、**[Start Services（サービスの起動）]** をクリックします。
   b. [Network Agent] セクションへ移り、**[Start Services（サービスの起動）]** をクリックします。

Websense Web Security インストール ディレクトリ

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Web Security インストール ディレクトリは、コンピュータのオペレーティング システムによって異なります。

Windows コンピュータでは、デフォルトのインストール ディレクトリは下記のようになっています。

```
C:\Program Files または Program Files（x86）\Websense\Web Security\
```

Linux コンピュータでは、デフォルトインストール ディレクトリは下記のようになっています：

```
/opt/Websense/
```

警告

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *警告数コントロール*、481 ページ
- *一般的アラート オプションの設定*、482 ページ
- *システム アラートの設定*、484 ページ
- *カテゴリ使用状況アラートの設定*、485 ページ
- *プロトコル使用状況アラートの設定*、487 ページ

Websense ソフトウェアおよびクライアントのインターネット アクティビティの両方の追跡および管理を容易にするために、優先管理者は、選択されているイベントが発生したときにアラートを送信するように設定することができます。

- **System alerts（システム アラート）**は、サブスクリプション ステータスおよび Master Database アクティビティと関連する Web Security イベントならびに Content Gateway イベントについて、ドメイン コントローラとの通信の消失、ログ スペース問題、等々を含めて、管理者に知らせます。
- **Usage alerts（使用状況アラート）**は、選択されているカテゴリまたはプロトコルについてのインターネット アクティビティが設定されているしきい値に達したときに管理者に知らせます。

  使用状況アラートは、Websense 定義およびカスタム両方のカテゴリまたはプロトコルについて生成可能です。
- **Suspiciousactivity alerts（疑わしいアクティビティ アラート）**は、選択されている重大度の脅威関連イベントが設定されているしきい値に達したときに管理者に知らせます。

すべてのアラートを選択されている受信者に電子メールまたは SNMP で送信することができます。

警告数コントロール

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *警告*、481 ページ
- *一般的アラート オプションの設定*、482 ページ

使用状況アラートがアラート メッセージを過度に生成することを避けるための組み込みコントロールがあります。特定のカテゴリおよびプロトコルに対するユーザ要求に対応して送信されるアラート数の制限を指定するためには、**[Maximum daily alerts per usage type（使用状況タイプごとの日次アラートの最大数）]** 設定を使用します。詳細は、*一般的アラート オプションの設定、482 ページ*を参照してください。

しきい値限界をカテゴリおよびプロトコル使用状況アラートごと、ならびに疑わしいアクティビティ アラートごとに設定することもできます。例えば、10 のしきい値限界をあるカテゴリに設定した場合、そのカテゴリへの要求が（すべてのクライアントの合計として）10 になった後にアラートが生成されます。詳細については、*カテゴリ使用状況アラートの設定、485 ページ*と*プロトコル使用状況アラートの設定、487 ページ*を参照してください。

日次の最大アラート数が 20 であり、カテゴリのしきい値が 10 であるとします。管理者がアラート通知を受けるのは、しきい値を超えるカテゴリ要求の最初の 20 回のについてだけです。このことは、最初の 200 件の発生だけがアラート メッセージを生成することを意味します（アラートの最大数 20 × しきい値 10）。

一般的アラート オプションの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *警告、481 ページ*
- *システム アラートの設定、484 ページ*
- *カテゴリ使用状況アラートの設定、485 ページ*
- *プロトコル使用状況アラートの設定、487 ページ*
- *疑わしいアクティビティ アラートの設定、489 ページ*

Websense ソフトウェアは、各種のシステム イベントと定義されているしきい値を超えるインターネット使用状況や疑わしいアクティビティについて管理者に通知することができます。

[Settings] > [Alerts（アラート）] > [Enable Alerts（アラートの有効化）] ページを使用して、警告数コントロールを指定し、1 つ以上のアラート通知方法を有効にして設定します。このページでアラートを有効にしたら、[Settings] > [Alerts] セクションの他のページを使用して、受け取ろうとするアラートを指定します。

1. [Alert Limits per 24 Hours（24 時間ごとのアラート最大数）] のもとで、カテゴリ使用状況、プロトコル使用状況、および疑わしいアクティビティの各アラートについて生成される **[Maximum daily alerts per type（使用状況タイプごとの日次アラートの最大数）]** を指定します。

例えば、誰かがスポーツ カテゴリのサイトに 5 回（しきい値）要求する毎に送信されるようにカテゴリ使用状況アラートを設定します。ユーザ数とインターネット使用状況のパターンによっては、毎日、数百のアラートが生成されることがあります。

[使用状況タイプごとの日次アラートの最大数] を 10 にすると、管理者が特定の日付に [Sports（スポーツ）] サイトに対する最初の 50 件の要求についてアラートを受け取ることになりますが（アラート当り 5 件の要求 × 10 回のアラート）、同日中の当該カテゴリに対する引き続く要求についてはアラートは生成されません。

2. アラートと通知を電子メールでる配信するには、**[Enable email alerts（電子メール アラートを有効化する）]** をオンにします。次に、電子メールの設定を行います。

SMTP server IPv4 address or name（SMTP サーバー IPv4 アドレスまたは名前）	電子メール アラートをルーティングする SMTP サーバーの IPv4 アドレスまたはホストネーム。
From email address（送信者の電子メール アドレス）	電子メール アラートの送信元として使用される電子メール アドレス。
Administrator email address（管理者の電子メール アドレス）（To）	電子メール アラートのプライマリ受信者の電子メール アドレス。
Recipient email addresses（受信者の電子メール アドレス）（Cc）	最高 50 人までの追加の受信者の電子メール アドレス。各アドレスは個別の行にある必要があります。

3. ネットワークにインストールされている SNMP Trap システムを使用してアラート メッセージを配信するためには、**[Enable SNMP alerts（SNMP アラートの有効化）]** にマークを付けます。次に、SNMP Trap システムの情報を提供します。

Community name（コミュニティ名）	SNMP Trap サーバー上のトラップ コミュニティの名前。
IPv4 address or hostname（IPv4 アドレスまたはホストネーム）	SNMP Trap サーバーの IPv4 アドレスまたはホストネーム。
Port（ポート）	SNMP メッセージが使用するポート番号。デフォルトは 162 です。

4. 完了したら、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

システム アラートの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *警告*、481 ページ
- *一般的アラート オプションの設定*、482 ページ
- *現在のシステム ステータスの確認*、490 ページ

Web Security manager は、詳細なシステム ヘルスおよびステータス情報を **[Status（ステータス）] > [Alerts（アラート）]** ページで表示します（*現在のシステム ステータスの確認*、490 ページを参照してください）。

管理者が重要なシステム イベントについて確実に通知されるようにするために、Websense システム アラートが SNMP Trap による電子メールで配信されるように設定します。

Websense Web Security Gateway および Gateway Anywhere 管理者は、サブスクリプションおよびデータベース ダウンロード問題に関する Web Security イベントと各種の問題に関する Content Gateway イベントの両方についてのアラートを有効にすることができます。

[Settings] > [Alerts] > [System] ページを使用して、送信するアラートを指定し、各通知を送信する方法を選択します。

アラートを有効にするには、管理者にどのように通知するかを指示するメッセージ要約の右側のチェックボックスの 1 つ以上をオンにします。[Enable Alerts（アラートの有効化）] ページで有効にされている方法によって、**Email（電子メール）**、**SNMP**、または組み合わせを選択することができます。

アラートを無効にするには、メッセージ要約の右側のチェックボックスをすべてクリアします。

デフォルトでは、すべてのアラートが有効になっています。電子メール通知に SMTP 情報を提供していると、下記の 4 つの Web Security イベントを無効にすることはできません：

- Websense Master Database のダウンロードが失敗しました。
- 現在のユーザの数はサブスクリプション レベルを超えています。
- 1 ヶ月以内にサブスクリプションが失効します。
- 1 週間以内にサブスクリプションが失効します。

さらにオプションとして、下記の 3 つのアラートがあります：

- 現在のユーザの数がサブスクリプション レベルの 90% に達しています。
- Search Filtering（検索フィルタリング）でサポートされている検索エンジンが変更されました。
- Websense Master Database が更新されました。

Websense Web Security Gateway および Gateway Anywhere 環境では、オプションとして下記のようなシステム アラートを有効にすることができます：

- ドメイン コントローラがダウンしました。
- セキュア コンテンツの復号化と検査が無効になっています。
- ログ スペースが極度に少なくなっています。
- サブスクリプション情報を取得できません。
- クリティカルでないアラートを受け取りました。（このアラートをもたらす条件については、*Content Gateway のクリティカルでないアラート*、632 ページを参照してください。）

完了したら、**[OK]** をクリックして変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

カテゴリ使用状況アラートの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *警告*、481 ページ
- *警告数コントロール*、481 ページ
- *一般的アラート オプションの設定*、482 ページ
- *カテゴリ使用状況アラートの追加または編集*、486 ページ

特定の URL カテゴリのインターネット アクティビティが定義されているしきい値に達すると、Websense ソフトウェアは通知をだすことができます。そのカテゴリに対する許可要求またはブロック要求についてのアラートを定義することができます。

例えば、カテゴリに対して制限を加えるかどうかを決めるために、ショッピング カテゴリのサイトに対して 50 回の要求が許可される毎にアラートを発生させることが求められるかもしれません。または、ユーザが新しいインターネット使用ポリシーに適合しているか調べるために、エンターテインメント カテゴリのサイトに対する 100 回の要求がブロックされる毎にアラートを受信することが望まれるかもしれません。

すでに設定されているアラートを表示して、使用状況アラート カテゴリを追加または削除するには、**[Settings] > [Alerts] > [Category Usage（カテゴリ使用状況）]** ページを使用します。

1. アラートに設定されているカテゴリ、それぞれのしきい値、および選択されているアラート方法を知るには、**[Permitted Category Usage Alerts（許可カテゴリ使用状況アラート）]** および **[Blocked Category Usage Alerts（ブロック カテゴリ使用状況アラート）]** リストを表示します。
2. [Add Category Usage Alerts（カテゴリ使用状況アラートの追加）] ページ（*カテゴリ使用状況アラートの追加または編集、486 ページ*を参照）を開いて、アラートに URL カテゴリを追加するには、適切なリストの下の **[Add（追加）]** をクリックします。
3. 希望するカテゴリをそのリストから削除するには、そのチェックボックスにマークを付け、適切なリストの下の **[Delete（削除）]** をクリックします。
4. 完了したら、変更をキャッシュするために **[OK]** をクリックし、[Category Usage（カテゴリ使用状況）] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

カテゴリ使用状況アラートの追加または編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *警告、481 ページ*
- *一般的アラート オプションの設定、482 ページ*
- *カテゴリ使用状況アラートの設定、485 ページ*

[Category Usage] > [AddCategory Usage Alerts（カテゴリ使用状況アラートの追加）] または **[[Edit Category Usage Alerts（カテゴリ使用状況アラートの編集）]** ページを使用して、以下の処理を実行します。

- （[add] ページのみ）使用状況アラートの新しいカテゴリを選択する
- 使用状況アラートのしきい値を設定または変更する
- アラートの方法（電子メール、SNMP）を選択または更新する

1 つ以上の新しいアラートを作成する場合、最初に、同じしきい値およびアラート方法を設定して追加する各カテゴリの隣のチェック ボックスにマークを付けます。

注意

ログ記録から除外されているカテゴリでは使用状況アラートの追加はできません。*要求がログ記録される方法の設定、505 ページ*を参照してください。

以降の手順は使用状況アラートの追加および編集の両方に使用できます。

1. アラートが生成される時の要求の数を選択することによって **[Threshold（しきい値）]** を設定または更新します。
2. これらのカテゴリの希望するアラート方法（**Email（電子メール）**、**SNMP**）のチェックボックスにマークを付けます。

   [Alerts] ページで有効になっているアラート方法（*一般的アラート オプションの設定、482 ページ*を参照）だけが選択可能です。
3. 変更をキャッシュし、[Category Usage] ページに戻るには、**[OK]** をクリックします（*カテゴリ使用状況アラートの設定、485 ページ*を参照してください）。**[Save and Deploy]** をクリックするまで変更は適用されません。

プロトコル使用状況アラートの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *警告、481 ページ*
- *警告数コントロール、481 ページ*
- *一般的アラート オプションの設定、482 ページ*
- *プロトコル使用状況アラートの追加または編集、488 ページ*

特定のプロトコルのインターネット アクティビティが定義されているしきい値に達すると、Websense ソフトウェアは通知をだすことができます。選択されているプロトコルに対する許可またはブロック要求のアラートを定義することができます。

例えば、プロトコルに対して制限を加えるかどうかを決めるために、特定のインスタント メッセージ送信プロトコルに対する 50 回の要求が許可される毎にアラートをだすことを希望されるかもしれません。または、ユーザが新しいインターネット使用ポリシーに適合しているか調べるために、特定の P2P ファイル共有プロトコルに対する 100 回 の要求がブロックされる毎にアラートを受信することを希望されるかもしれません。

すでに設定されているアラートを表示し、使用状況アラートのプロトコルを追加または削除するには、[Settings（設定）] タブの **[Alerts] > [Protocol Usage]** ページを使用します。

1. アラートが設定されているプロトコル、それぞれのしきい値、および選択されているアラート方法を知るためには、**[Permitted Category Protocol Alerts（許可プロトコル使用状況アラート）]** および **[Blocked Protocol Usage Alerts（ブロック プロトコル使用状況アラート）]** リストを表示します。

2. [Add Protocol Usage Alerts（プロトコル使用状況アラートの追加）] ページを開いて（*プロトコル使用状況アラートの追加または編集、488 ページ* を参照）、アラートにプロトコルを追加するには、適切なリストの下の **[Add]** をクリックします。
3. 希望するプロトコルを削除するためには、そのチェックボックスを選択し、適切なリストの下の **[Delete]** をクリックします。
4. 完了したら、変更をキャッシュするために **[OK]** をクリックし、[Protocol Usage（プロトコル使用状況）] ページに戻ります。**[Save and Deploy]** をクリックするまで変更は適用されません。

プロトコル使用状況アラートの追加または編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *警告、481 ページ*
- *一般的アラート オプションの設定、482 ページ*
- *プロトコル使用状況アラートの設定、487 ページ*

[Protocol Usage] > **[Add Protocol Usage Alerts（プロトコル使用状況アラートの追加）]** または **[[Edit Protocol Usage Alerts（プロトコル使用状況アラートの編集）]** ページを使用して、下記の事柄を実行します。

- （[add] ページのみ）使用状況アラートの新しいプロトコルを選択する
- 使用状況アラートのしきい値を設定または更新する
- 当該のアラートのアラートの方法（電子メール、SNMP）を選択または更新する

1 つ以上の新しいプロトコル使用状況アラートを作成する場合、最初に、同じしきい値およびアラート方法を設定して追加する各プロトコルの隣のチェック ボックスにマークを付けます。

注意

プロトコルが 1 つ以上のプロトコル フィルタでログ記録されるように設定されていない場合、アラートで使用するようにそのプロトコルを選択することはできません。

プロトコル アラートは、プロトコルをログ記録するプロトコル フィルタによって管理されているクライアントのよる使用状況だけを反映します。

以降の手順は使用状況アラートの追加および編集の両方に使用できます。

1. アラートが生成される時の要求の数を選択することによって **[Threshold（しきい値）]** を設定または変更します。
2. これらのプロトコルで希望するアラート方法（**Email**、**SNMP**）を選択します。

   [Alerts] ページで有効になっているアラート方法（*一般的アラート オプションの設定、482 ページ*を参照）だけが選択可能です。
3. 変更をキャッシュし、[Protocol Usage] ページに戻るには、**[OK]** をクリックします（*プロトコル使用状況アラートの設定、487 ページ*を参照してください）。**[Save and Deploy]** をクリックするまで変更は適用されません。

疑わしいアクティビティ アラートの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *警告、481 ページ*
- *警告数コントロール、481 ページ*
- *一般的アラート オプションの設定、482 ページ*

Websense Web Security ソリューションは、指定した重要度レベルの疑わしいアクティビティが定義されているしきい値に達したときに通知を発行することができます。それぞれの重大度レベルで許可される要求とブロックされる要求のアラートを定義します。

Content Gateway はクリティカルな強度の重要度アラートを検出しなければならないので、そのような重要度のアラートの設定は Websense Web Security および Websense Web Filter 配備では不可能です。

[Settings] > [Alerts] > [Suspicious Activity（疑わしいアクティビティ）] ページを使用して、ネットワーク中の疑わしいイベントと関連付けられているアラートのアラート設定を有効または無効にしたり、あるいは変更することができます。これらのイベントに関する詳細な情報は [Threats（脅威）] ダッシュボードで表示されます。

このページで 2 つのテーブル - **[Permitted Suspicious Activity Alerts（許可される疑わしいアクティビティのアラート）]** と **[Blocked Suspicious Activity Alerts（ブロックされる疑わしいアクティビティのアラート）]** - が表示されます。それぞれのテーブルには下記の項目があります：

- 設定される **[Severity（重要度）]** レベル。4 段階の重要度レベルは、クリティカル、高度、中度および低度です。重要度レベルは、アラートと関連付けられている脅威カテゴリによって決まります。詳細は、*疑わしいアクティビティに重大度を関連付ける方法、47 ページ*を参照してください。

- アラート **[Threshold（しきい値）]**。デフォルトでは、クリティカルと高度の重要度アラートのしきい値は、許可およびブロックのいずれの場合も、**1** です。
- 1 つ以上の通知方法。疑わしいアクティビティ アラートは **[Email]**、**[SNMP]**、またはその両方によって送信されます。
- アラートが **[Enabled（有効）]** であるか、そうでないか。グリーンのチェック マークは、選択されている重要度の疑わしいアクティビティについてアラートが生成されることを示しています。赤い [X] は、選択されている重要度についてアラートが無効化されていることを示します。

疑わしいアクティビティ アラートを更新するには、下記の手順を実行します：

1. 重要度レベルの左側のチェックボックスをオンにして **[Enable]** または **[Disable（無効）]** をクリックし、選択されているタイプのアラートを有効または無効にします。
2. 有効なアラートについて、**[Threshold]** フィールドに数値を入力し、アラートを生成させる疑わしいイベントの数を指定します。
3. 疑わしいアクティビティ アラートの配信で使用する通知方法（**[Email]**、**[SNMP]**）を選択します。

   [Enable Alerts] ページで有効になっているアラート方法（*一般的アラート オプションの設定*、482 ページを参照）だけが選択できます。
4. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

現在のシステム ステータスの確認

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense ソフトウェアの健全性に影響する問題に関する情報を検出するために **[Status]> [Alerts]** ページを使用し、トラブルシューティング ヘルプを参照し、Websense Master Database の最近のリアルタイム更新の詳細を確認します。

[Active Alerts（アクティブなアラート）] リストは、モニタされている Websense ソフトウェア コンポーネントのステータスを示します。

- どのコンポーネントがモニタされているかについての詳細な情報を見るには、アラート メッセージ リストの上で **[What is monitored?（現在モニタ中の内容）]** をクリックします。
- 問題解決のためには、エラーあるいは警告メッセージの隣りの **[Solutions（ソリューション）]** ボタンをクリックします。

- アラート メッセージを非表示にするには、**[Hide Persistent Alerts（持続的アラートを表示しない）]** をクリックします。お客様の組織で Log Server、Network Agent、または User Service を使用しない場合、または WebCatcher を有効にする計画がない場合は、テーブルの **[Hide Alert（アラートを表示しない）]** 列の適切なチェックボックスにマークを付けます。選択されているサービスと関連付けられているアラートは表示されなくなります。

[Real-Time Database Updates（リアルタイム データベース更新）] リストは、Websense Master Database の緊急更新についての情報を提供し、下記を示します：

- いつ更新が発生したか
- 更新のタイプ
- 新しいデータベース バージョン番号
- 更新の理由
- 更新を受信した Filtering Service インスタンスの IP アドレス

これらの補足の更新は、通常のスケジュールされた Master Database 更新とは別に発生し、例えば、一時的に間違えて分類されたサイトを再分類するために使用されます。Websense ソフトウェアがデータベース更新を 1 時間ごとにチェックします。

Websense Web Security ユーザーのために、[Alerts] ページには第 3 のリストとして **Real-Time Security Updates（リアルタイム セキュリティ更新）** - があります。このリストは Real-Time Database Updates リストと同じフォーマットですが、特にセキュリティ関連のデータベースの更新が表示されます。

セキュリティ アップデートをインストールすると、新たなフィッシング（身元詐称）詐欺、犯罪的なアプリケーション、あるいはウェブサイトまたはアプリケーションに感染する悪意のあるコードの脅威に対する脆弱性が除去されます。

Real-Time Security Updates の詳細については、*Real-Time Security Updates™*、33 ページを参照してください。

[Alerts] エリアの印刷可能なバージョンを第 2 のウィンドウで開くには、ページ上部の **[Print（印刷）]** ボタンを使用します。ブラウザのオプションを使用してこのページを印刷します。

Websense データのバックアップと復元

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *バックアップのスケジュール設定*、494 ページ
- *即時バックアップの実行*、496 ページ
- *バックアップ ファイルの管理*、497 ページ
- *Websense データの復元*、498 ページ
- *スケジュール設定バックアップの中止*、499 ページ
- *コマンド リファレンス*、500 ページ

Websense Backup Utility は、お客様の Websense ソフトウェア設定とポリシー データのバックアップと以前の設定への復元を容易にします。また、このユーティリティによって保存されたデータは、アップグレード後に Websense 設定情報をインポートするために使用することもできます。

重要
設定をバックアップまたは復元する前に、すべての管理者が TRITON コンソールからログオフしていることを確認してください。

Backup Utility は下記のものを保存します：

- Policy Database に保存されているグローバル設定情報（これにはクライアントおよびポリシー データが含まれます）。
- 各 Policy Server によって保存されている Filtering Service と Log Server の設定などのローカルな設定情報。
- Websense コンポーネントの初期設定ファイルと設定ファイル。

バックアップ プロセスは下記のようになっています：

1. 即時バックアップを開始するか（*即時バックアップの実行*、496 ページを参照）、またはバックアップ スケジュールを定義します（*バックアップのスケジュール設定*、494 ページを参照）。
   - バックアップはいつでも手動で開始できます。
   - バックアップ ファイルは、バックアップを実行またはスケジュールするときに指定されるディレクトリに保存されます。

2. Backup Utility は、コンピュータ上のすべての Websense コンポーネントをチェックし、バックアップに適格なデータを収集し、アーカイブ ファイルを作成します。ファイル名は下記のフォーマットになります：

   ```
   wsbackup_<yyyy-mm-dd_hhmmss> .tar.gz
   ```

   この場合、<yyyy-mm-dd_hhmmss> はバックアップの日付と時刻です。**tar.gz** はポータブル圧縮ファイル フォーマットです。

   root（Linux）と Administrator グループのメンバー（Windows）だけがバックアップ ファイルにアクセスすることができます。

Websense コンポーネントを含んでいる各コンピュータ上で Websense Backup Utility を実行します。このツールは、現在のコンピュータ上で発見される下記のすべてのファイルを識別し、保存します：

パス	ファイル名
\Program Files または **Program Files（x86）\Websense\Web Security\bin** もしくは **/opt/Websense/bin**	authserver.ini BrokerService.cfg config.xml eimserver.ini icap.conf ignore.txt LogServer.ini securewispproxy.ini transid.ini upf.conf websense.ini WebUI.ini wsauthserver.ini wscitrix.ini WSE.ini wsedir.ini wsradius.ini wsufpserver.ini
bin/i18n	i18n.ini
bin/postgres/data	postgresql.conf pg_hba.conf
BlockPages/*/Custom	（すべてのファイル）
tomcat/conf/Catalina/Localhost	mng.xml

Websense バックアップ ファイルを安全で確実な場所に保存してください。これらのファイルを組織の定期的バックアップ手順に組み込む必要があります。

以前の設定に復元するには 下記の手順を実行します：

1. バックアップ ファイルを保存場所から取り出します。
2. それが作成された Websense コンピュータにそれぞれのバックアップ ファイルをコピーします。

> **重要**
> 1 つのオペレーティングシステム プラットフォーム上で作成されたバックアップ ファイルを別のプラットフォーム上のインストールに対して設定を復元しようとしないでください。
>
> 例えば、Linux 上で作成されたバックアップ ファイルを Windows コンピュータに対して復元しようとしないでください。

3. Backup Utility を復元モードで実行します。

> **重要**
> Websense ソフトウェア設定を復元するには、必ず Backup Utility を使用してください。他の展開ユーティリティを使用して、アーカイブからファイルを抽出しないでください。
>
> バックアップ ファイルが破損した場合、設定を復元することはできません。

復元処理中に、復元を実行しているコンピュータ上でエラー メッセージまたは警告が表示されます。

バックアップのスケジュール設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *即時バックアップの実行*、496 ページ
- *バックアップ ファイルの管理*、497 ページ
- *Websense データの復元*、498 ページ
- *スケジュール設定バックアップの中止*、499 ページ
- *コマンド リファレンス*、500 ページ

Websense 管理者にバックアップ スケジュールを通知することによって、管理者にバックアップ プロセス中 TRITON コンソールからログオフするように指示します。

バックアップをスケジュール設定するには、下記の手順を実行します。

- Windows:
  1. コマンド プロンプトを開き、Websense **bin** ディレクトリ（デフォルトでは C:\Program Files または C:\Program Files（X86）\Websense\Web Security\bin）に移動します。
  2. 下記のコマンドを入力します。

     ```
     wsbackup -s -t "<m> <h> <day_of_month> <month>
     <day_of_week> " -d <directory>
     ```

     時間情報は **crontab** フォーマットを使用しており、コーテーション マークとスペースが必要であることに注意してください。
- Linux:
  1. コマンド シェルを開き、**Websense** directory（デフォルトでは /opt/Websense/） に移動します。
  2. 下記のコマンドを入力します：

     ```
     ./WebsenseTools -b -s -t \"<m> <h> <day_of_month>
     <month> <day_of_week> \" -d <directory>
     ```

     時刻と日付の文字列全体の最初と最後の \" 文字とは別に、この文字列にアスタリスク文字（*）が含まれるとき、アスタリスク文字も \" ペアによって囲われねばなりません。例：

     ```
     ./WebsenseTools -b -s -t \"45 1 \"*\" \"*\" 5\"
     ```

     この場合、バックアップは、月や日と関係なく、金曜日の 1:45 a.m. に実行されるようにスケジュール設定されています。

コマンドで示されている変数の代わりに、次の情報を与えてください：

変数	情報
<m>	0 - 59 バックアップを開始する時刻の分を指定します。
<h>	0 - 23 バックアップを開始するその日の一般時間 を指定します。
<day_of_month>	1 - 31 バックアップを実行する日付を指定します。バックアップを 29 － 31 日にスケジュール設定すると、その日付を含まない月では、ユーティリティはオペレーティング システムの標準代替手順を使用します。
<month>	1 - 12 バックアップを実行する月を指定します。
<day_of_week>	0 - 6 曜日を指定します。0 は日曜日を表します。

各フィールドでは、数値、アスタリスク、またはパラメータ リストを使用できます。詳細については、**crontab** のリファレンスを参照してください。

即時バックアップの実行

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *バックアップのスケジュール設定*、494 ページ
- *バックアップ ファイルの管理*、497 ページ
- *Websense データの復元*、498 ページ
- *スケジュール設定バックアップの中止*、499 ページ
- *コマンド リファレンス*、500 ページ

Backup Utility を実行する前に、すべての管理者が TRITON コンソールをログオフしていることを確認します。

即時バックアップを起動するには、下記の手順を実行します：

- Windows:
  1. コマンド プロンプトを開き、Websense **bin** ディレクトリ（デフォルトでは C:\Program Files または C:\Program Files（X86）\Websense\Web Security\bin）に移動します。
  2. 下記のコマンドを入力します。

     ```
     wsbackup -b -d <directory>
     ```
- Linux:
  1. コマンド シェルを開き、**Websense** directory（デフォルトでは /opt/Websense/） に移動します。
  2. 下記のコマンドを入力します。

     ```
     ./WebsenseTools -b -b -d <directory>
     ```

ここで、<directory> はバックアップ アーカイブの保存先ディレクトリを指します。

警告

バックアップ ファイルを Websense **bin** ディレクトリに保存しないでください。Websense ソフトウェアをアンインストールすると、このディレクトリは削除されます。

即時バックアップを開始すると、エラー メッセージと通知がバックアップを実行しているコンピュータのコンソール上に表示されます。

バックアップ ファイルの管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *バックアップのスケジュール設定*、494 ページ
- *即時バックアップの実行*、496 ページ
- *Websense データの復元*、498 ページ
- *スケジュール設定バックアップの中止*、499 ページ
- *コマンド リファレンス*、500 ページ

バックアップを実行するとき、設定ファイル（**WebsenseBackup.cfg**）が作成され、バックアップ アーカイブとともに保存されます。この設定ファイルでは下記のことが指定されています：

- どのくらいの期間、バックアップ アーカイブをバックアップ ディレクトリに保存するか
- ディレクトリ内のすべてのバックアップ ファイルによって消費できる最大ディスク スペース

下記のパラメータを変更するには、テキスト エディタで **WebsenseBackup.cfg** ファイルを編集します：

パラメータ	値
KeepDays	アーカイブ ファイルがバックアップ ディレクトリで保存される日数。デフォルトは 365 です。 **KeepDays** 値より古いすべてのファイルはバックアップ ディレクトリから削除されます。割り当てられているディスク スペース量を超える場合、最も古いファイルは新しいファイルのスペースをつくるためにバックアップ ディレクトリから削除されます。
KeepSize	バックアップ ファイルに割り当てられるバイト数。デフォルトは 10857600 です。 **KeepSize** パラメータは、ディレクトリ内に複数のバックアップ ファイルが存在しない限り、適用されません。最後（最新）のバックアップ ファイルのサイズはこの設定によって影響されません。（つまり最新のバックアップ ファイルが KeepSize 制限より大きい場合、そのファイルがディレクトリ内の唯一のファイルとなりますが、ファイルの切り捨ては行われません）。

デフォルト設定ファイルが作成されたとき、デフォルトではこれらのパラメータのどちらかまたは両方がコメント扱いにされる場合があります。どちらかのパラメータの値をカスタマイズするとき、行の先頭に [#] 文字がある場合、変更を有効化するために [#] を削除します。

Websense データの復元

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *バックアップのスケジュール設定、494 ページ*
- *即時バックアップの実行、496 ページ*
- *バックアップ ファイルの管理、497 ページ*
- *スケジュール設定バックアップの中止、499 ページ*
- *コマンド リファレンス、500 ページ*

Websense 設定データを復元するとき、現在のコンピュータに存在するコンポーネントのデータが復元されることを確認してください。またすべての管理者が TRITON コンソールからログオフしていることを確認します。

Policy Broker コンピュータ上で復元プロセスを実行する場合は、復元が完了したら配備されているすべての Websense サービスを再起動します。これは、Policy Broker 上のサービスとそれ以外のサービスを含みます。

復元プロセスを開始するには下記の手順を実行します：

- Windows:
  1. コマンド プロンプトを開き、Websense **bin** ディレクトリ（デフォルトでは C:\Program Files または C:\Program Files（X86）\Websense\Web Security\bin）に移動します。
  2. 下記のコマンドを入力します。

     ```
     wsbackup -r -f archive_file.tar.gz
     ```

- Linux:
  1. コマンド シェルを開き、**Websense** directory（デフォルトでは /opt/Websense/） に移動します。
  2. 下記のコマンドを入力します。

     ```
     ./WebsenseTools -b -r -f archive_file.tar.gz
     ```

重要
復元プロセスは数分かかる場合があります。復元が進行している間は、プロセスを停止しないでください。

復元プロセス中は、Backup Utility はすべての Websense サービスを停止します。ユーティリティがサービスを停止することができない場合、ユーザに手動で停止するように求めるメッセージが送信されます。*Websense サービスの停止と起動、477 ページ* で説明されている順序でサービスを停止する必要があります。

Backup Utility は、サードパーティ統合製品との通信で使用されるいくつかのファイルを保存します。これらのファイルは Websense ディレクトリ構造の外部に配置されるため、正しいディレクトリに各ファイルをコピーして、それらを手動で復元する必要があります。

手動で復元する必要があるファイルは下記のとおりです：

ファイル名	復元先
isa_ignore.txt	**Windows\system32**
ignore.txt	**Windows\system32\bin**

スケジュール設定バックアップの中止

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *バックアップのスケジュール設定、494 ページ*
- *即時バックアップの実行、496 ページ*
- *バックアップ ファイルの管理、497 ページ*
- *Websense データの復元、498 ページ*
- *コマンド リファレンス、500 ページ*

バックアップ スケジュールをクリアし、現在スケジュール設定されているバックアップの実行を中止するためには、コマンド シェルを開き、Websense **bin** ディレクトリ（デフォルトでは C:\Program Files または Program Files（x86）\Websense\Web Security\bin）に移動します。下記のコマンドを入力します。

```
wsbackup -u
```

コマンド リファレンス

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *バックアップのスケジュール設定*、494 ページ
- *即時バックアップの実行*、496 ページ
- *バックアップ ファイルの管理*、497 ページ
- *Websense データの復元*、498 ページ
- *スケジュール設定バックアップの中止*、499 ページ

root（Linux）または Administrator グループのメンバー（Windows）だけが Backup Utility を実行できます。

wsbackup および **WebsenseTools -b** コマンドには下記のようなオプションがあります：

- -b（または --backup）
- -d directory_path（または --dir directory_path）
- -f full_file_name（または --file full_file_name）
- -h（または --help、もしくは -?）
- -r（または --restore）
- -s（または --schedule）
- -t（または --time）
- -u（または --unschedule）
- -v（または --verbose [0 - 3]）

17 レポート管理

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *要求がログ記録される方法の設定、505 ページ*
- *カテゴリのリスク クラスへの割り当て、502 ページ*
- *レポートの優先設定、503 ページ*
- *Log Server の設定、507 ページ*
- *Log Database 管理の設定、517 ページ*
- *調査レポートの設定、534 ページ*
- *セルフレポーティング、540 ページ*

デフォルトの管理者アカウント（admin）のみを使用する組織では、Web Security manager を使用する全てのユーザーがすべてのレポート設定およびツールにアクセスできます。指定済み管理を使用する組織では、レポート設定およびツールに対するアクセスは、優先管理者ロールのメンバーによって管理されます（*ロールの編集、423 ページ*を参照）。

レポート設定へのアクセス権限を持つ管理者は、環境に合わせてレポートをカスタマイズする多くのオプションを利用できます。

- Websense マスタ データベースはカテゴリを**リスク クラス**に編成します。リスク クラスは、各カテゴリのサイトに含まれる可能性がある脆弱性のタイプまたはレベルを示します。組織の必要に応じてリスク クラスをカスタマイズするためには、[Settings（設定）] > [General（一般）] > [Risk Classes（リスク クラス）] ページを使用します。*カテゴリのリスク クラスへの割り当て、502 ページ*を参照してください。
- [Settings] > [Reporting（レポート）] > [Preferences（優先設定）] ページを使用して、レポートの配布に使用する電子メール サーバーを設定し、セルフレポート作成をアクティブ化し、スケジュール設定されたレポートが TRITON 管理サーバーに保存される期間を設定します。また、Real-Time Monitor が常時データを収集するのか、Real-Time Monitor が開いている時だけかを設定します。*レポートの優先設定、503 ページ*を参照してください。

ログ記録は、レポートを作成できるようにするために、インターネット アクティビティに関する情報を ログ データベースに保存するプロセスです。

- ログ記録を有効にし、ログ記録するカテゴリを選択し、どのユーザー情報をログ記録するかを決定するためには、[Settings] > [General] > [Logging（ログ記録）] ページを使用します。詳細は、*要求がログ記録される方法の設定、505 ページ*を参照してください。
- ログ レコードを処理する方法、および Log Database への接続を管理するためには、[Settings] > [Reporting] > [Log Server] ページを使用します。*Log Server の設定、507 ページ*を参照してください。
- Log Database の管理 - データベースの分割、URL のロギング、ブラウズ時間、トレンド データ オプションを含む - を行うためには、[Settings] > [Reporting] > [Log Database] ページを使用します。*Log Database 管理の設定、517 ページ*を参照してください。

カテゴリのリスク クラスへの割り当て

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *リスク クラス、64 ページ*
- *ブロック ページ、143 ページ*
- *レポートによるインターネット アクティビティの評価、159 ページ*

Websense マスタ データベースはカテゴリを**リスク クラス**に編成します。リスク クラスは、各カテゴリのサイトに含まれる可能性がある脆弱性のタイプまたはレベルを示します。

リスク クラスは主にレポーティングで使用されます。Web Security Dashboard は、インターネット アクティビティがリスク クラス別に表示されるグラフを含んでおり、また、リスク クラス別に編成されたプレゼンテーション レポートまたは調査レポートを作成できます。

各リスク クラスを構成するカテゴリを変更するには、**[Settings] > [General] > [Risk Classes（リスク クラス）]** ページを使用します。

1. **リスク クラス** リストのエントリを選択します。
2. どのカテゴリが現在そのリスク クラスに含まれているかを見るためには、**[Categories]** リストを表示します。

   チェックマークは、そのカテゴリが現在選択されているリスク クラスに割り当てられていることを示しています。青色の [W] アイコンは、デフォルトでそのリスク クラスに含まれているカテゴリを示しています。

3. 選択されているリスク クラスのカテゴリを含める、または除外するためには、カテゴリ ツリーでエントリにマークを付けるか、またはクリアします。カテゴリは、1 つ以上のリスク クラスに属することができます。

   他に次の選択が含まれます：

オプション	説明
Select All（すべて選択）	ツリーのすべてのカテゴリを選択します。
Clear All（すべてクリア）	ツリーのすべてのカテゴリを選択解除します。
Restore Defaults（デフォルトの復元）	選択されたリスク クラスを、Websense ソフトウェアによって提供されていたカテゴリ選択にリセットします。青色の W アイコンはデフォルト カテゴリを示します。

4. 各リスク クラスでこの手順を繰り返します。
5. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy（保存と配備）]** をクリックするまで、変更は適用されません。

レポートの優先設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *セルフレポーティング*、540 ページ
- *プレゼンテーション レポートのスケジュール設定*、177 ページ
- *調査レポートのスケジュール設定*、208 ページ

作成したスケジュールされたレポートを選択した受信者に電子メールで送信したり、セルフレポート作成をアクティブ化したり、スケジュールされたプレゼンテーション レポートを保存する期間を決定したり、Real-Time Monitor がいつデータを収集するかを設定するために使用する情報を提供するには、**[Settings] > [Reporting] > [Preferences]** ページを使用します。

1. [Email Reports] の下に、スケジュールされたレポートを電子メールによって配信するときに [From（送信元）] フィールド に表示する**電子メール アドレス**を入力します。
2. 電子メール サーバーがスケジュールされたレポートを配信するために使用する **SMTP サーバーの IPv4 アドレスまたは名前**を入力します。

3. 組織内のエンド ユーザーが Web Security manager にアクセスし、自分の個人インターネット利用状況の調査レポートを実行することを許可するためには、**[Allow self-reporting（セルフ レポートを許可する）]** チェックボックスをオンにします。

   このオプションが選択されている時、セルフレポート作成機能にアクセスするために使用する URL が表示されます。*セルフレポーティング*、540 ページを参照してください。

4. [Scheduled Presentation Reports（スケジュールされているプレゼンテーション レポート）] の下で、**[Store reports for（レポート保存期間）]** ドロップダウン リストを使って、レポートを TRITON 管理サーバーに保存する期間を指定します（デフォルトでは 5 日間）。

   レポートを保存する期間を長くすると、TRITON 管理サーバーで必要とされるディスク スペースの量に影響が及びます。管理サーバーは長期的なレポート アーカイブの保存には適していません。

5. **[Warn administrators...（管理者への警告期間）]** ドロップダウン リストは、スケジュールされているプレゼンテーション レポートが削除される前に [Review Reports（レポートの検討）] ページに警告が表示される期間を指定するために使用します（デフォルトは 3 日間）。

   この警告は、管理者に、重要なレポートが管理サーバーから削除される前に適当な場所へアーカイブ保管するための時間を提供することを目的としています。

6. [Real-Time Monitor] の下のいずれかのラジオ ボタンを選択して、Real-Time Monitor がいつユーザー データのキャプチャを開始するかを決定します。

   - システム パフォーマンスを改善するには、**[Capture data only when Real-Time Monitor is active（Real-Time Monitor がアクティブである時にだけデータをキャプチャする）]**（デフォルト）を選択します。このオプションが選択されている時、データの収集は Real-Time Monitor を起動した時に開始します。レコードが画面に表示されるまでにわずかな遅延（数秒）が起こることがあります。
   - 誰もデータを見ていない時でも Real-Time Monitor クライアントが継続的にデータを RTM データベースへ供給するようにするには **[Always capture data（常にデータをキャプチャする）]** を選択します。これはシステムのパフォーマンスに大きな影響を及ぼすことがあります。

7. **[Save Now（すぐに保存）]** をクリックし、変更を適用します。

要求がログ記録される方法の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Log Database の概要*、515 ページ
- *Log Server の設定*、507 ページ

[Settings] > [General] > [Logging] ページを使用して、以下のことを行います。

- Filtering Service がログ レコードを Log Server へ送信するために使用する IP アドレスおよびポートを指定する。
- （*Websense Web Security Gateway Anywhere*）Sync Service がハイブリッド ログ レコードを Log Server へ送信するために使用するポートを指定する。
- Filtering Service がレポート作成に使用するために Log Server に送信するクライアント識別情報（もしあれば）を指定する。
- レポート作成およびカテゴリ使用状況アラートに使用するためにログ記録する URL カテゴリを指定します（*カテゴリ使用状況アラートの設定*、485 ページを参照）。

複数の Policy Server を使用している環境では、Policy Server のそれぞれのインスタンスに対して別々に [Logging（ログ記録）] ページを設定します。アクティブな Policy Server に関連付けられたすべての Filtering Service インスタンスは、そのログ レコードをこのページで指定された Log Server に送信します。

複数の Policy Server を使用している時は、以下のことに注意してください。

- 各 Policy Server は 1 つの Log Server インスタンスと通信できます。
- レポート データが Web Security manager に正しく表示されるためには、ベース Policy Server（インストール時に指定した Policy Server のインスタンス。[Settings] > [General] > [Policy Server] ページに表示されます）に関連付けられている Log Server がなければなりません。

  これは通常は、Policy Broker と合わせてインストールされている Policy Server（例、Full ポリシー ソース アプライアンス上の Policy Server）です。
- いずれかの Policy Server との接続に使用する Log Server の IP アドレスとポートが空白である場合、その Policy Server と関連付けられている Filtering Service インスタンスは、レポートまたはアラートのためにトラフィックを記録することができません。
- ユーザー名および IP アドレスをログ記録するかどうかの情報はセンターで保存されますから、同じ設定がユーザーの環境全体で使用されます。

  同様に、カテゴリをログ記録する方法に対する変更は、Filtering Service および Log Server のすべてのインスタンスで共有されます。

複数の Policy Server と複数の Log Server を含む環境の場合、それぞれの Policy Server にログオンし、それらが正しい Log Server と通信していることを確認してください。

1. **Log Server IPv4 のアドレスとホスト名**を入力します。
2. Filtering Service がログ レコードを Log Server へ送信するために使用する**ポート**を指定します（デフォルトは 55805 です）。
3. （*Websense Web Security Gateway Anywhere*）Sync Service がハイブリッド サービスからのログ レコードを Log Server へ送信するために使用するポートを指定します。
4. Web Security manager が指定された場所とポートを使って Log Server と通信できるかどうかを判断するためには、**[Check Status（ステータスの確認）]** をクリックします。

   接続テストを成功したかどうかを知らせるメッセージが表示されます。必要なら、テストが成功するまで、IP アドレスまたはホスト名とポートを更新します。
5. ログ レコードに保存され、レポートに表示されるログ レコードの量を指定します。
   - インターネットにアクセスしているコンピュータの識別情報を記録するためには、**[Log IP addresses（IP アドレスのログ記録）]** にマークを付けます。
   - インターネットにアクセスしているユーザーの識別情報を記録するためには、**[Log user names（ユーザー名のログ記録）]** にマークを付けます。

     注意
     IP アドレスまたはユーザー名を記録しない場合、レポートにユーザー データは表示されません。これは**匿名ログ**と呼ばれることもあります。

   - Web Security Gateway または Gateway Anywhere を使用していて、ダッシュボードの [Threats] テーブルにソース デバイス名情報（入手できる場合）を含める場合は、**[Log hostnames（ホスト名をログ記録する）]** をクリックします。

     名前情報は脅威関連のログでのみ利用できます。この情報は、重大度レベルを割り当てられていないインターネット アクティビティに対しては利用できません。
6. ログ記録しない URL カテゴリを指定するには、**[Selective Category Logging（選択的カテゴリ ログ記録）]** リストを使用します。ここで行う選択は、すべてのアクティブ ポリシーのすべてのカテゴリ フィルタに適用されます。

> **注意**
> 使用状況アラートが設定されているカテゴリのログ記録を無効にした場合（*カテゴリ使用状況アラートの設定、485 ページ*を参照）、使用状況アラートは送信されません。
>
> レポートにログ記録されていないカテゴリの情報を含めることはできません。

- 特定のカテゴリにすばやく移動するには、**[Find category（カテゴリの検索）]** 検索ボックスを使用します。
- サブカテゴリのログ記録の設定を変更するには、必要に応じて親カテゴリを拡張します。
- カテゴリのログ記録を中止するには、そのカテゴリ名の横のチェックボックスをオフにします。

  カテゴリの選択または選択解除は個別に行う必要があります。親カテゴリを選択しても、そのサブカテゴリは自動的には選択されません。選択の補助に **[Select All（すべて選択）]** および **[Clear All（すべて選択解除）]** を使用できます。

7. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy（保存と配備）]** をクリックするまで、変更は適用されません。

Log Server の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

インストール中に、Log Server がどのようにポリシーの実施コンポーネントと相互通信するかを含む Log Server 動作の特定の設定を行います。**[Settings] > [Reporting] > [Log Server]** ページを使用してこれらの設定を更新するか、または Log Server の動作に関して他の詳細を設定します。

設定の更新を完了したとき、**[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は保存されません。

データベース接続を変更した場合、変更を保存して配備した後、すべてのレポーティング ツールのデータベース接続を更新するために、管理サーバー コンピュータ上で **Websense TRITON - Web Security** サービスを再起動します。

複数の Log Server を含む環境では、このページで行った設定は、Web Security ツールバーに IP アドレスが表示されている Policy Server に割り当てられている Log Server インスタンスに適用されます。

注意

[Settings] > [Reporting] > [Log Server] ページは、以前のバージョンでこれらのタスクを実行するために使用していた Log Server Configuration Utility に代わるものです。

基本 Log Server の詳細の確認

[Location（場所）] の下で、Log Server の IP アドレスを確認します。必要な場合、**[Port]** フィールドを使って Log Server が Filtering Service との通信に使用するポートを更新します（デフォルトは 55805 です）。

このポートは **[Settings] > [General] > [Logging]** ページに表示されるロギングポートと一致していなければなりません。

Log Database 接続の設定

[Log Database Connection（ログ データベースの接続）] の下で、Log Server が Log Database への接続に使用する ODBC 接続を設定します。

1. ODBC **データ ソース名（DSN）**を指定し、データベース接続のための一意な**説明**を入力します。
2. ログ データベース をホストする Microsoft SQL Server の **SQL Server の場所**（IP アドレスまたはホスト名およびインスタンス名（もしあれば））と、ログ データベースにデータを送信するための**接続ポート**（デフォルトでは 1433）を指定します。
3. お客様の環境で SQL Server クラスタ化を使用している場合、クラスタの仮想 IP アドレスを入力します。
4. **デフォルト データベース**の名前を入力します（デフォルトでは wslogdb70）。
5. **SSL を使用して Log Database に接続する**かどうかを指定します。SSL 暗号化が有効化されている時、
   - BCP を使用して Log Database にレコードを追加することはできません。
   - Log Database 接続に時間がかかり、レポーティングのパフォーマンスに影響を及ぼします。

重要

Microsoft SQL Server コンポーネントで [Trust Server Certificate（サーバー認証を信頼する）] が **[No]**（デフォルト）に設定されている時、自己署名 SSL 証明書はデータベース接続の暗号化のためには受け入れられません。

この場合、Web Security manager で [Use SSL（SSL を使用）] オプションを有効化する前に、Certificate Authority が署名する SSL 証明書を SQL Server、TRITON 管理サーバー、および Log Server を実行するコンピュータに適切に配備しておかなければなりません。

データベース暗号化の詳細については、SQL Server のマニュアルを参照してください。

6. Log Server の接続方法を指定します。
   - デフォルトでは **[SQL Server authentication（SQL サーバー認証）]** が選択されています。SQL Server 認証を使用するには、使用する SQL Server **アカウント**および**パスワード**を提供します。
   - 代わりに **Windows 信頼される接続（ネットワーク ログオン アカウント）**を使用することもできます。Websense Log Server サービスがこのアカウントで実行するように設定されていなければなりません。
7. **[Test Connection（テスト接続）]** をクリックして、それが提供された資格情報を使って Log Database に接続できることを確認します。

   このボタンをクリックした時に実行されるテストについては、*Log Database 接続のテスト、513 ページ*を参照してください。

データベース接続を変更した場合、変更を保存して配備した後、すべてのレポーティング ツールのデータベース接続を更新するために、管理サーバー コンピュータ上で **Websense TRITON - Web Security** サービスを再起動します。

ログ レコードがデータベースに追加される方法の指定

Log Server がログ データベースにレコードを追加する方法を指定するには、**[Log Record Creation（ログ レコードの作成）]** をクリックします。

- **[ODBC（データベース接続を開く）]** を指定すると、データベース ドライバを使用して Log Server と Log Database の間のデータを管理して、レコードを個別にデータベースに挿入します。

  このオプションを設定する場合、Log Server とデータベース エンジンの間で確立できる内部接続の数を指定するために **[Maximum number of connections（最大接続数）]** も設定します。

SQL Server ライセンスに応じて 4 から 50 までの値を選択します。

> **注意**
> 接続数を増やすとログ記録の処理スピードが増加します。しかし、同じ SQL Server を使用するネットワークの他のプロセスに影響を与えることがあります。ほとんどの場合、接続数を 20 未満に設定するべきです。データベース管理者に相談してください。

- **[BCP（Bulk Copy Program）]**（*推奨*）を指定すると、レコードを一括で Log Database に挿入します。このオプションは ODBC による挿入よりも効率的であり、コンピュータ上に **bcp.exe** ファイルがある場合は、デフォルトで選択されます。

  BCP オプションは、SQL Server Native Client Utility と Command Line Utility を Log Server コンピュータ上にインストールしている場合にのみ利用可能です。

  BCP は、SQL Server SSL 暗号化が使用されている時は使用できません。

  BCP オプションを選択する場合、下記のオプションも指定してください。

オプション	説明
BCP file location（BCP ファイルの場所）	BCP ファイルを保存するディレクトリ パスです。Log Server はこの場所へのリードおよびライト アクセス権限を持っていなければなりません。（デフォルト フォルダは C:\Program Files または Program Files（x86）\Websense\Web Security\bin\Cache\BCP\ です） パスを入力した後、**[Test Location（場所をテスト）]** をクリックして、その場所がアクセス可能であることを確認します。
File creation rate（ファイル作成レート）	Log Server が 1 つのバッチ ファイルにレコードを挿入するために費やす最大時間（分）です。この時間を超えるとバッチ ファイルが閉じ、新しいバッチ ファイルが作成されます。 この設定はバッチ サイズの設定との組み合わせで作用します。Log Server は、いずれかの制限に達した時に新しいバッチ ファイルを作成します。
Maximum batch size（最大バッチ サイズ）	バッチ ファイルに挿入できるログ レコードの最大数です。この数に達すと新しいバッチ ファイルが作成されます。 この設定は作成レートの設定との組み合わせで作用します。Log Server は、いずれかの制限に達した時に新しいバッチ ファイルを作成します。

ログ レコード挿入方法を選択した後、**[Log Cache Files（ログ キャッシュ ファイル）]** をクリックして、ログ キャッシュ ファイルをどこに、どのように作成するかを指定します。ログ キャッシュ ファイルは、まだ Log Database に挿入されていない、または BCP ファイルに移動されていないログ レコードのための一時的な保管場所となります。

1. **[Cache location（キャッシュの場所）]** には、ログ キャッシュ ファイルを保存する Log Server コンピュータ上の場所を指定します（デフォルトでは C:\Program Files または Program Files （x86）\Websense\Web Security\bin\Cache\）。
2. **[Test Location]** をクリックして、そのパスがアクセス可能であることを確認します。
3. **[Cache file creation rate（キャッシュファイルの作成レート）]** に、Log Server がログ キャッシュ ファイルにインターネット アクセス情報を送信する時間の最大値（分）を指定します（デフォルトは 1）。この時間を過ぎるとログ キャッシュ ファイルが閉じ、新しいファイルが作成されます。
4. **[Maximum cache file size（キャッシュ ファイルの最大サイズ）]** にログ キャッシュ ファイルの最大サイズを指定します。このサイズに達したとき、Log Server はログ キャッシュ ファイルを閉じ、新しいファイルを作成します。

ファイル作成レートと最大ファイル サイズの設定は組み合わせで作用します。Log Server は、いずれかの制限に達した時に新しいログ キャッシュ ファイルを作成します。

データベース サイズ設定の調整

お客様の組織のニーズに合わせて **[Database Size Management（データベース サイズ管理）]** の設定を行います。記録する詳細のレベルが高いほど、Log Database が大きくなります。

1. Log Database のサイズを最小化するためには、**[Enable log record consolidation（ログ レコードの集約を有効化する）]** にマークを付けます。これは、複数の同様のインターネット要求を 1 つのログ レコードに集約することによってレポーティング データの詳細度を下げます。

   SIEM 集約を有効化した場合、Log Server は Log Database に挿入したログ レコードに対して集約を適用します。集約は SIEM 製品に送られたレコードには適用されません。

   集約が有効化されている時、以下のすべての要素を共有している要求は 1 つのログ レコードに集約されます。

   - ドメイン名（例、www.websense.com）
   - カテゴリ
   - キーワード
   - アクション（例：ブロックされたカテゴリ）
   - ユーザー / IP アドレス

ログ レコードは、集約されたレコードに含まれる要求の数、およびすべての集約された要求の合計の帯域幅を含みます。

Log Database が小さい場合、レポートがより高速に動作します。しかし、ログデータを集約すると、同じドメイン名の別個のレコードが失われる可能性があり、いくつかの詳細レポートの正確性を損ないます。

重要

レポートの一貫性を保証するためには、集約を有効 / 無効にする場合はいつでも、新しいデータベース パーティションを作成してください。また、必ず同じ集約設定で、パーティションからレポートを作成してください。

Websense Web Security Gateway（Anywhere）では、集約が有効化されている時、スキャンによってブロックされたトラヒックについてレポートに示される数が、スキャン固有のレポートに示される数よりも**小さく**なります。これはスキャンのアクティビティを記録する方法の副次的影響です。

2. 集約を有効化する場合、**[Consolidation time interval（集約間隔）]** も指定します。これは、1 つの集約レコードに結合される最初と最後のレコードの間で許容される最大時間間隔を表します。

   レポートの精度を上げるためには、間隔を小さくします。集約を大きくするためには、間隔を大きくします。また、間隔を大きくすると、メモリ、CPU、ディスク スペースなどのシステム リソースの使用量が増加します。

   [Settings] > [Reporting] > [Log Database] ページで [full URL（完全 URL）] ロギングを有効化した場合、集約されるログ レコードには、Log Server が最初にマッチするサイトの完全なパス（最大 255 文字）が含められます。

   例えば、ユーザーが次の場所にアクセスし、それらの場所がすべて [ショッピング] カテゴリ に分類されているとします。

   - www.domain.com/shoeshopping
   - www.domain.com/purseshopping
   - www.domain.com/jewelryshopping

   [full URL logging（完全な URL によるログ記録）] が有効な場合、集約により、URL www.domain.com/shoeshopping に対する 3 つの要求を示す 1 つのログ エントリが作成されます。

3. [Hits and Visits（ヒット件数とアクセス件数）] の下の **[Enable visits（アクセス件数を有効化する）]** チェックボックスを使って、各ユーザーのインターネット要求を記録する際の詳細度のレベルを指定します。

> **注意**
> ロギング方法をアクセス件数とヒット件数の間で切り換える前に、新しいデータベース パーティションを作成することを推奨します。新しいデータベース・パーティションを作成するには、**[Settings] > [Reporting] > [Log Database]** ページを使用します。

このオプションを**選択していない**場合、画像、広告、埋め込まれたビデオなど種々のページ要素を表示するために生成された各 HTTP 要求に対して別々のログ レコードが作成されます。この方法は、[ヒット件数によるロギング] と呼ばれ、Log Database が非常に大きくなり、しかも急速に拡大します。

このオプションを**選択している**時、Log Server はウェブ ページを作成する個々の要素（画像、広告など）を 1 つのログ レコードに結合します。

Websense Web Security Gateway（Anywhere）では、アクセス件数が有効化されている時、レポートに示される数（スキャンによってブロックされたトラヒックを含む）が、スキャン固有のレポートに示される数よりも**小さく**なります。これはスキャンのアクティビティを記録する方法の副次的影響です。

User Service の通信の設定

[User Service Connection（User Service の接続）] ボタンをクリックし、次に **[User and group update interval（ユーザーおよびグループの更新間隔）]** フィールドを使って、Log Server が User Service に接続して完全ユーザー名およびグループ割り当ての情報を取得する頻度を指定します（デフォルトでは 12 時間ごと）。

ユーザー名またはグループが変更されたユーザーのアクティビティは、次の更新が行われるまで、元のユーザー名またはグループ割り当てで報告されます。ディレクトリ サービスを頻繁に更新するか、多数のユーザーを持つ組織では、ユーザー/ グループ情報の更新の頻度を上げる必要があります。

Log Database 接続のテスト

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Web Security manager の [Settings] > [Reporting] > [Log Server] ページで、Log Server および他のレポーティング ツールで使用するデータベース接続情報を更新できます。

ページの [Log Database Connection] のセクションに **[Test Connection（テスト接続）]** ボタンがあります。このボタンをクリックすると、Log Server は以下のテストを実行します。

1. Log Server は、Web Security manager から更新されたデータベース接続情報を取得します。

   Log Server が停止した場合、または TRITON 管理サーバーと Log Server コンピュータの間のネットワークが停止した場合、このテストは失敗です。Log Server への接続が失敗し、IO 例外エラーが表示されます。
2. Log Server は ODBC を使用してテスト用のデータ ソース名（DSN）を作成します。
3. Log Server は DSN を使用して Log Database への接続を確立します。Log Server は、下記のことを確認します。
   - Websense データベースが存在する。
   - データベースのバージョンが正しい。
4. Log Server はそのデータベース許可を確認します。

   必要とされるデータベースのロールおよび許可については *Microsoft SQL Server のユーザ許可の設定、613 ページ*を参照してください。
5. Log Server はテストのために使用した DSN を削除します。
6. Log Server は Web Security manager に、テストが成功したことを知らせます。

   このリターン通知が失敗した場合、IO 例外エラーが表示されます。

さらに、Web Security manager は、データベースへの JDBC 接続を確立できることを確認します。Log Server テストが失敗した後でも Web Security manager テストに合格する可能性があります。

新しいデータベース接続情報は、変更をキャッシュし、保存するまでは使用されません。変更をキャッシュし、保存した時、

- 新しいデータベース接続情報が Policy Server 設定ファイルに保存されます。
- Log Server は永久的 DSN を作成します（接続テストで使用した一時的 DSN を再生成します）。

レポーティング ツール（プレゼンテーション レポートなど）を更新し、新しいデータベース接続を使用するために、Websense TRITON - Web Security サービスを再起動します。

Log Database の概要

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *データベース ジョブ、516 ページ*
- *Log Database 管理の設定、517 ページ*

ログ データベースは、Websense Web Security ソリューションによって処理されたインターネット アクティビティのレコードを保存します。インストール時に、ログ データベースとカタログ データベース、および 1 つのデータベース パーティションが作成されます。

カタログ データベース（デフォルトは wslogdb70）は、ログ データベースにアクセスする必要がある種々の Websense コンポーネント（ダッシュボード、Log Server、プレゼンテーション レポート、調査レポート ）のための単一の接続ポイントを提供します。これはデータベース パーティションに関する補助的な情報 - カテゴリ名のリスト、リスク クラス定義、トレンド データ、ユーザーのグループへのマップ、データベース ジョブなど - を含みます。また、カタログ データベースは、すべての利用可能なデータベース パーティションのリストを管理します。

データベース パーティションは、インターネット アクティビティについての個々のログ レコードを保存します。パーティションには次の 2 つのタイプがあります。

- 標準ロギング パーティション（wslogdb70_1、wslogdb70_2 など）は、ログ記録されたすべてのインターネット要求に関する情報を格納します。標準ロギング パーティションからの情報は、調査およびプレゼンテーション レポートならびにダッシュボード チャートへのデータの入力のために使用されます。
- [脅威] パーティション（wslogdb70_amt_1）は、重大度レベルが割り当てられている要求に関する情報を格納します（*疑わしいアクティビティに重大度を関連付ける方法、47 ページ*を参照）。[脅威] パーティションからの情報は、[脅威] ダッシュボードへのデータの入力のために使用されます。

サイズおよび日付を基にして、新しい標準ロギング パーティションが作成されます。詳細は、*データベース パーティション オプションの設定*、518 ページを参照してください。

- パーティションがサイズに基づいている場合、すべての着信ログ レコードは、サイズ ルールを満たす最も新しいアクティブなパーティションに挿入されます。パーティションが指定された最大のサイズに達したとき、新しいログ レコードを挿入するために、新しいパーティションが作成されます。
- パーティションが日付に基づいている場合設定されたサイクルに従って、新しいパーティションが作成されます。例えば、ロールオーバー オプションが毎月である場合、新しい月にレコードが受信されるとすぐに、新しいパーティションが作成されます。着信ログ レコードは 日付に基づいて適切なパーティションに挿入されます。

データベース標準ロギング パーティションは柔軟性とパフォーマンスの向上に役立ちます。例えば、必要な情報を見つけるために解析する必要のあるデータ範囲を制限するために、1 つのパーティションからレポートを作成することができます。

データベース ジョブ

Web Security Help | Web Security ソリューション | バージョン 7.8.x

次のデータベース ジョブが Log Database とともにインストールされます。

> **重要**
> Microsoft SQL Server の完全バージョン（Express ではなく）を使用している場合、SQL Server Agent サービスがデータベース エンジン コンピュータ上で実行していなければなりません。SQL Server またはコンピュータが再起動された時にこのサービスが自動的に開始するように設定されていることを確認してください。

- **Extract、Transform、Load（ETL）ジョブ**は連続して実行され、Log Server からデータを受信し、それを処理し、標準ロギング パーティション データベースに挿入します。トレンド データの保持が有効化されている場合、ETL ジョブはカタログ データベースへのトレンド データの挿入も行います。

  ログ レコードを Log Database 内へ挿入するためには、ETL ジョブが実行していなければなりません。
- **データベース メンテナンス ジョブ**は、データベース メンテナンス タスクを実行し、最適なパフォーマンスを維持します。デフォルトで、このジョブは毎晩実行されます。

- **インターネット ブラウズ時間（IBT）ジョブ**は、受信データを分析し、各クライアントのブラウズ時間を計算します。IBT データベース ジョブは、リソースを集中的に消費し、ほとんどのデータベース リソースに影響を与えます。デフォルトで、このジョブは毎晩実行されます。
- トレンド データの保持が有効化されている時、**トレンド ジョブ** は ETL ジョブによって作成される毎日のトレンド データを使って、プレゼンテーション レポートのために使用する週間、月間、年間のトレンド レコードを更新します。

  トレンド データの保持が無効化されている時でも、トレンド ジョブは [脅威]（AMT）パーティションからのデータを処理して、[脅威] ダッシュボードにトレンド データを供給します。

  トレンド ジョブはまた、ユーザー エージェント文字列を解析して、[Reporting] > [Applications] ページの [Browser] および [Source Platform] タブにデータを入力します（*アプリケーション レポートの作成*、216 ページを参照）

  このジョブは毎晩実行されます。
- **Advanced Malware Threat（AMT）ETL ジョブ**は、データを受信し、処理し、[脅威] パーティション データベースへ挿入します。重大度ランキングを含むログ レコードだけが [脅威] パーティションに記録されます（*疑わしいアクティビティに重大度を関連付ける方法*、47 ページを参照）。このパーティションからのデータは、[脅威] ダッシュボードへのデータの入力のために使用されます（*Threats ダッシュボード*、41 ページを参照）。

[Settings] > [Reporting] > [Log Database] ページでこれらのデータベース ジョブのいくつかの条件を設定できます。詳細は、*Log Database 管理の設定*、517 ページを参照してください。

メンテナンス ジョブとインターネットブラウズ時間ジョブの開始時間を設定するときに、システム リソースとネットワーク トラフィックを考慮してください。これらのジョブは集中的にリソースを消費します。ログ記録とレポートのパフォーマンスを遅くすることがあります。トレンド データの保持が有効化されている時、デフォルトでトレンド ジョブは午前 4 時 30 分に実行されます。トレンド ジョブと重なる可能性がある時間に他のジョブを開始するのは避けてください。

Log Database 管理の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

下記の条件を管理するには、**[Settings] > [Reporting] > [Log Database]** ページを使用します。

- Log Database が新しい標準ロギング パーティションをいつ、どこで、どのように作成し、レポートの作成のためにどのパーティションが使用されるか（*データベース パーティション オプションの設定、518 ページ*を参照）
- メンテナンス ジョブをいつ、どのように実行するか（*Log Database メンテナンス オプションの設定、522 ページ*を参照）
- ログ レコードがドメインと、ページまたは項目への完全なパスを含む完全 URL を含むかどうか（*URL がログ記録される方法の設定、524 ページ*を参照）
- インターネット ブラウズ時間を計算する方法（*インターネット ブラウズ時間の設定、525 ページ*を参照）
- トレンド およびアプリケーション データを保存するかどうか、および保存期間（*トレンドおよびアプリケーション データの保持の設定、527 ページ*を参照）

アクティブな Log Database インスタンスの名前がページの上部に表示されます。

データベース パーティション オプションの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Log Database 管理の設定、517 ページ*
- *ログ データベースのサイズ設定のガイドライン、529 ページ*
- *インターネット ブラウズ時間の設定、525 ページ*
- *URL がログ記録される方法の設定、524 ページ*
- *Log Database メンテナンス オプションの設定、522 ページ*
- *トレンドおよびアプリケーション データの保持の設定、527 ページ*

[Settings] > [Reporting] > [Log Database] ページの **[Database Rollover Configuration（データベース ロールオーバー設定）]** セクションを使用して、Log Database がいつ新しいデータベース パーティションを作成する（ロールオーバーする）か、どこにデータベース パーティションを格納するか、およびパーティションのサイズを指定します。また、計画されているロールオーバーを待つのでなく、手動で新しいパーティションを作成し、レポーティングできるすべてのデータベース パーティションを検討します。

毎日のデータベース パーティション サイズの平均の経時的な変化を調べるには、[Database Rollover Configuration] セクションの下部の **[Growth Rates and Sizing（増加率とサイズ設定）]** チャートを参照してください。これは将

来の増加に備えたり、新しいパーティションを作成する頻度を決定したり、パーティション サイズおよび増加オプションを設定するために役立ちます。

- チャートの下のドロップダウン リストを使用して、表示する **[Time period（期間）]** を設定します。（期間はパーティション作成日付を基にします。パーティションがスパンした日付ではありません。）直前の 1 週間、1 カ月、3 カ月、6 カ月に作成したパーティション、または利用可能なすべてのパーティションを表示できます。

  長い期間を選択すると、各パーティションがチャート上の小さなドットのように表示されることがあります。
- **チャートの判例を表示**するかどうかを指定します。凡例は、表示されている時、どのパーティション（パーティション名）がチャートにマッピングされているかを示します。

  判例は、選択した期間のチャートに含まれるパーティションの数が 20 以内である場合にのみ利用可能です。
- チャートの中の、もっと詳しく検討したいセクションを選択します。表示の詳細レベルを下げるには、**[Zoom Out（ズーム アウト）]** または **[Reset Chart（チャートのリセット）]** をクリックします。

データベースのサイズ設定の詳細は、*ログ データベースのサイズ設定のガイドライン、529 ページ*を参照してください。

データベースのロールオーバーと増加を管理するには、以下の手順を実行します。

1. **[Roll over every（ロールオーバーの間隔）]** の横のフィールドに、新しいパーティションを作成する頻度を指定します。
   - サポートされているすべてのデータベース エンジンについて、各パーティションのサイズ制限を入力できます。サイズ制限に達した時、新しいパーティションが作成されます。

     サイズ制限は、下記のように設定できます。
     - *SQL Server Standard または Enterprise*:100-1,000,000 MB、デフォルトは 5000
     - *Microsoft SQL Server Express*:100-8,000 MB、デフォルトは 5000
   - Microsoft SQL Server StandardまたはEnterprise を使用している場合、代わりにパーティション ロールオーバー間隔（1-52 週間ごと、または 1-12 カ月ごと）を指定することもできます。

> **注意**
> ロールオーバーが繁忙な時間帯に開始される場合、ロールオーバー プロセス中に処理速度が遅くなる可能性があります。
>
> この可能性を避けるために、組織によっては自動ロールオーバーの間隔またはサイズ制限設定を大きい値に設定しています。そして、自動ロールオーバーが行われないように、手動でロールオーバーを実行します。手動ロールオーバーについては、*Log Database メンテナンス オプションの設定*、522 ページを参照してください。
>
> 極端に大きい個別のパーティションは推奨されません。データが複数のより小さいパーティションに分割されている場合、レポートの処理速度が遅くなることがあります。

新しいパーティション データベースが作成されると、そのパーティションは自動的にレポートで使用可能になります。

2. [Partition Management（パーティション管理）] の下で、次の情報を提供してください。
   a. 新しいデータベース パーティションのための**データ** ファイルと**ログ** ファイルの両方を作成するための**ファイル パス**を入力します。
   b. **[Init Size（初期サイズ）]** で、新しいデータベース パーティションを構成する**データ** ファイルと**ログ** ファイルの両方の初期ファイル サイズを設定します。
      - *SQL Server Standard または Enterprise*：データ ファイルの初期サイズは 50-500,000 MB、デフォルトは 2000。ログ ファイルの初期サイズは 50-250,000 MB、デフォルトは 100
      - *SQL Server Express*：データ ファイルの初期サイズは 50-5000 MB、デフォルトは 100。ログ ファイルの初期サイズは 50-4000 MB、デフォルトは 100

> **注意**
> 最善の方法として、一定期間の平均のパーティション サイズを計算し、次に初期サイズをそれに近い値に更新します。たとえば、初期サイズを平均サイズの 80% に設定します。この方法によって、パーティションが拡張される回数を最小にし、パーティションにデータを挿入するためのリソースを解放します。
>
> [Growth Rates and Sizing（増加率とサイズ設定）] リスト（使用可能なパーティションのリストの下）の情報は、この計算に役に立ちます。

c. **[Growth（増加）]** で、追加スペースが要求されるときのパーティションの**データ**ファイルと**ログ** ファイルのサイズの増加の単位を設定します。

- *SQL Server Standard または Enterprise*：データ ファイルの増加は 100-500,000 MB、デフォルトは 500。ログ ファイルのサイズは 1-250,000 MB、デフォルトは 100
- *SQL Server Express*：データ ファイルの増加は 1-1,000 MB、デフォルトは 100。ログ ファイルのサイズは 1-1,000 MB、デフォルトは 100

3. 次の自動ロールオーバーを待たずに、次に ETL ジョブ（*データベース ジョブ、516 ページ*を参照）を実行するときにパーティションを作成するには、**[Manually Create Partition（手動でのパーティションの作成）]** をクリックします。この処理は通常、数分かかります。

   - 新しいパーティションに [Log Database] ページ上の変更を反映させるには、**[Manually Create Partition]** をクリックする前に **[OK]** と **[Save and Deploy]** をクリックします。
   - 定期的に [Available Partitions（使用できるパーティション）] の下の [Refresh（リフレッシュ）] リンクをクリックします。作成プロセスが完了した時に、新しいパーティションがリストに追加されます。

4. レポーティングのために使用可能パーティションを検討するには、**[Available Partitions（使用可能パーティション）]** リストを使用します。リストには、各パーティションのカバーされる日付、サイズ、と名前が表示されます。

   パーティション名の隣のチェック ボックスにマークを付け、リストの下のボタンを使ってパーティション データがレポートで使用されるか、除外されるか、またはパーティションを削除するかを指定します。

- 選択したパーティション データをレポートに含めるには、**[Enable]** をクリックします。レポートのために少なくとも 1 つのパーティションを有効にする必要があります。
- 選択したパーティション データをレポートから除外するには、**[Disable]** をクリックします。

  [Enable] と [Disable] のオプションを組み合わせることによって、レポート生成時に解析するデータの量を管理でき、レポートの処理を迅速化できます。
- パーティションが必要でなくなった場合、**[削除]** をクリックして削除します。パーティションが実際に削除されるのは、次に毎晩のデータベース メンテナンス ジョブが実行される時です。

  有効化されているパーティションだけが削除可能です。無効化されているパーティションを削除するには、はじめにそれを有効化し、その後に削除します。

警告
このオプションの使用には注意が必要です。削除されたパーティションを復元することはできません。

古いパーティションを削除すると、Log Database のパーティション数が最小になり、データベースとレポート パフォーマンスが改善されます。必要に応じて、個々のパーティションを削除するために、この [削除] オプションを使用してください。スケジュールに従って古いパーティションを削除する場合、*Log Database メンテナンス オプションの設定、522 ページ* を参照してください。

5. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy（保存と配備）]** をクリックするまで、変更は適用されません。

Log Database メンテナンス オプションの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Log Database 管理の設定、517 ページ*
- *データベース パーティション オプションの設定、518 ページ*
- *インターネット ブラウズ時間の設定、525 ページ*
- *URL がログ記録される方法の設定、524 ページ*
- *トレンドおよびアプリケーション データの保持の設定、527 ページ*

[Settings] > [Reporting] > [Log Database] ページの **[Database Maintenance（データベースのメンテナンス）]** セクションを使って、データベース メンテナンス ジョブをいつ実行するか、データベース パーティションの自動削除を行うかどうか、およびその頻度、パーティションの索引の再作成やエラー ログ メッセージの削除などのタスクが行われる頻度を制御します。

1. **[Maintenance start time（メンテナンスの開始時刻）]** で、データベース メンテナンス ジョブを実行する時刻を選択します（デフォルトは 01:00）。

   時間およびこのジョブによって必要とされるシステム リソースは、エリアで選択したタスクによって変化します。他の動作やシステムに対する影響を最小にするためには、ネットワークが混雑していない時間、IBT ジョブが指定されていない時間に、このジョブを実行することが最良です（*インターネット ブラウズ時間の設定、525 ページ*を参照）。

2. 経過時間に基づいてパーティションを永久的に削除するには、**[Automatically delete partitions when data is older than（一定期間後にパーティションを自動的に削除する）]** を選択し、日数（1 ～ 1825）を指定します。この日数を過ぎるとパーティションは削除されます。

   警告

   パーティションが削除された後、データを復元することはできません。パーティションを削除する代わりの方法は、*データベース パーティション オプションの設定、518 ページ*を参照してください。

3. **[Enable automatic reindexing of partitions（索引自動再作成を有効にする）]** をチェックし、次に、自動的にこの処理を実行する曜日を選択します（デフォルトは [Saturday]）。

   データベース索引再作成は、データベースの完全性を維持し、レポート速度を最適化するために重要です。

   重要

   ネットワークが混雑していない時間に、この処理を行うことが最良です。データベース パーティションの索引再作成は、リソースを集中的に消費し、時間がかかります。レポートを処理中に実行するべきではありません。

4. 毎晩のデータベース メンテナンス ジョブがすべての失敗したバッチを再処理するようにするためには、**[Process failed batches during the database maintenance job（未処理のバッチを処理する）]** をチェックします。

   バッチの失敗は、ディスク スペースが足りないか、ログ レコードをデータベースに挿入するためのデータベース許可がない場合に起こります。一般に、これらのバッチは再処理され、毎晩のデータベース メンテナン

ス ジョブ中にデータベースに挿入されます。しかし、ディスク スペースまたは許可の問題が解決されていない場合、この再処理は成功しません。

この選択のチェックが外されている場合、失敗したバッチは決して再処理されません。代わりに、下で指定された時間（もしあれば）後に削除されます。

5. **[Delete failed batches after（失敗したバッチを削除するまでの日数）]** を選択し、次に指定したバッチを削除するまでの日数（0 ～ 90、デフォルトでは 20）を入力します。

   このオプションが選択されていない場合は、失敗したバッチは将来の処理のために無期限に維持されます。

6. **[Delete the error log after（エラー ログを削除するまでの日数）]** を選択し、次にカタログ データベースからデータベース エラー レコードを削除するまでの日数（0 ～ 90、デフォルトでは 60）を入力します。

   このオプションがチェックされていない場合、エラー ログは無期限に維持されます。

7. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで、変更は適用されません。

URL がログ記録される方法の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Log Database 管理の設定、517 ページ*
- *データベース パーティション オプションの設定、518 ページ*
- *インターネット ブラウズ時間の設定、525 ページ*
- *Log Database メンテナンス オプションの設定、522 ページ*
- *トレンドおよびアプリケーション データの保持の設定、527 ページ*

[Settings] > [Reporting] > [Log Database] ページの **[Full URL Logging（完全な URL によるログ記録）]** セクションを使って、要求された URL をどの程度ログ記録されるか決定します。

注意

ログ データベースのサイズを管理することは、ボリュームの大きなネットワークで重要です。完全 URL によるログ記録 オプションを無効にすることは、データベースのサイズと増加量を制御する 1 つの方法です。

1. 各サイトのドメイン（www.domain.com）と特定のページへのパス（/products/productA.html）を含めて、URL 全体をログ記録するためには、**[Record domain and full URL of each site requested（要求された各サイトのドメインと完全な URL を記録]** を選択します。

   重要
   リアルタイム スキャンのレポートを作成する計画がある場合、[full URL logging（完全な URL によるログ記録）] を有効化にします（*高度な分析アクティビティに関するレポート、252 ページ*を参照）。そうしないと、サイト内の各ページに異なったカテゴリか、異なった脅威が含まれていても、レポートはサイトのドメイン（www.domain.com）だけを表示します。

   このオプションがチェックされていない場合、ドメイン名だけが記録されます。この選択により、データベースはより小さくなりますが、詳細もより少なくなります。

   集約が有効であるときに、[full URL logging] を有効にした場合、集約レコードは、集約グループの最初のレコードから完全な URL を含みます。詳細は、*Log Server の設定、507 ページ*を参照してください。

2. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで、変更は適用されません。

インターネット ブラウズ時間の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Log Database 管理の設定、517 ページ*
- *データベース パーティション オプションの設定、518 ページ*
- *URL がログ記録される方法の設定、524 ページ*
- *Log Database メンテナンス オプションの設定、522 ページ*
- *トレンドおよびアプリケーション データの保持の設定、527 ページ*

インターネットブラウズ時間（IBT）のレポートは、ユーザーがインターネットで費やす時間量を表示します。毎晩、データベース ジョブが、その日に受信した新しいログに基づいて、各クライアントのブラウズ時間を計算します。[Settings] > [Reporting] > [Log Database] のページの **[Internet Browse Time（インターネット ブラウズ時間）]** セクションで、ブラウズ時間のオプションを設定します。

1. IBT データベース ジョブの **[IBT job start time（ジョブ開始時刻）]** を選択します。

   時間およびこのジョブによって必要とされるシステム リソースは、毎日の記録されたデータ容量によって変化します。毎晩のメンテナンス ジョブと異なった時間にこのジョブを実行するようにし（*Log Database メンテナンス オプションの設定、522 ページ*を参照）、ネットワーク上が混雑していない時間を選択するようにして、レポート作成に対する影響を最小にするように選択することを推奨します。

   IBT データベース ジョブは、リソースを集中的に消費することがあり、ほとんどのデータベース リソースに影響を与えます。このジョブを有効にする場合、スケジュールされたレポート処理または他の重要な動作のためのデータベース システムの能力に干渉しないように、開始時間を設定してください。また、すべての必要な処理を可能にするためには、更に強力なハードウェアが必要になるかを決定するために、ジョブをモニタしてください。

2. **[Average browse time per site（サイトごとの平均ブラウズ時間）]** に、ウェブ ページのコンテンツを読み込むための、分単位の平均値を設定します。

   この数値は、インターネット ブラウズ時間のレポートの目的のためのブラウズ セッションを指定します。ブラウザを開くと、HTTP トラフィックが発生します。これはブラウズ セッションの開始を表します。HTTP トラフィックがここで設定された時間内で連続的に発生する限り、セッションは開いています。HTTP トラフィックがなくなり、この時間を過ぎると、ブラウズ セッションは閉じられたと考えられます。再び HTTP トラフィックが発生するとすぐに、新しいブラウズ セッションが開始します。

   > **注意**
   > 可能な限りサイトごとの平均ブラウズ時間を変更しないようにし、変更した場合はいつでも、新しいデータベース パーティションを開始することを推奨します。
   >
   > レポート上のデータの整合性を保つために、同じサイトあたり平均ブラウズ時間を使用するデータベース パーティションから IBT レポートを作成してください。

   いくつかのウェブサイトは、情報を更新するために、自動リフレッシュ技術を使用していることに留意してください。1 つの例は 最新のニュース記事の表示を交代させるニュース サイトです。このリフレッシュは 新しい HTTP トラフィックを発生させます。そのため、この種のサイトが開いたままになっていると、サイトがリフレッシュする度に新しいログ レコードが作成されます。HTTP トラフィックに間隔はありません、そのため、ブラウズ セッションは閉じられません。

3. ブラウズ セッションの終了前に最後のウェブサイトを読み込むために費やされた時間を計算して、**[Browse time for last site read（最後のサイト読み込みのブラウズ時間）]** の値を設定します。

   HTTP トラフィックの時間間隔が平均 [サイトごとの] ブラウズ時間のしきい値より長い場合、セッションは終了します。[最終読み込み] ブラウズ時間の値は セッションタイムに加算されます。

4. 調査レポートを使用するブラウズ時間を含む詳細なレポートを有効化するには、**[Calculate detailed browse time for use in investigative detail reports（調査詳細レポートで使用するための詳細なブラウズ時間を計算）]** をオンにします。

   重要
   詳細なブラウズ時間の計算を有効化するとログ データベースのサイズが大きくなり、データベースのパフォーマンスに影響を与えることもあります。このオプションを使用する場合、ログ データベースの増加と全体的なレポーティング パフォーマンスを慎重にモニタしてください。

   詳細なブラウザ時間が無効化されたとき、要約のレポートにブラウザ時間を含めるために使用される計算を実行するために IBT ジョブは実行し続けます。

5. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで、変更は適用されません。

トレンドおよびアプリケーション データの保持の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Log Database 管理の設定、517 ページ*
- *データベース パーティション オプションの設定、518 ページ*
- *URL がログ記録される方法の設定、524 ページ*
- *Log Database メンテナンス オプションの設定、522 ページ*
- *インターネット ブラウズ時間の設定、525 ページ*

インターネット アクティビティのトレンドに関するプレゼンテーション レポーティングを有効化するために、オプションでログ データベースがトレンド データを保存できます。トレンド レポーティングを有効化したとき、ETL データベース ジョブ（*データベース ジョブ、516 ページ*を参照）は、毎日のトレンド データをカタログ データベースに追加し、トレンド ジョブが夜間に実行し、週間、月間、月間、年間のトレンド情報を保存します。

ログ データベースはまた、ブラウザの統計データ（帯域幅、カウントなど）、オペレーティング システム プラットフォーム、およびアプリケーション レーポートを有効化するためのユーザー エージェント文字列を保存します。

トレンド データの設定

トレンド データがログ データベース内の保持される期間を指定するために、[Settings] > [Reporting] > [Log Database] ページを順に選択し **[Trend Data Retention（トレンド データ保持）]** セクションを使用します。

1. Mark **[Store trend data（トレンド データを保存）]** をオンにして、ETL ジョブに トレンド データを保存して、毎晩のトレンド ジョブをアクティブ化するように指示します。

   トレンド データは、オプションが有効化されているときデータが収集された場合のみ計算されます。

   トレンド データ保持が有効化される前にデータベース内に保存されているデータ、またはこのオプションが無効化された後に収集されたデータは、トレンド レポートの含めることができません。

   このオプションが無効化されたとき、トレンド データベース ジョブは、AMT パーティションでの脅威に関連するデータの処理のためのみ実行します。

2. また週間、月間、および年間傾向データを保存する期間を指定します。トレンド データを保存される期間を長くすると、ログ データベースのサイズが大きくなります（*ログ データベースのサイズ設定のガイドライン、529 ページ*を参照）

> **注意**
> トレンド データはカタログ データベースに保存され、パーティション データベースには保存されませんから、トレンド データの格納期間はデータベース パーティションが保持される長さに左右されません。

トレンド データのデフォルトの格納期間は下記の表の通りです。

	SQL Server	SQL Server Express
毎日	90 日	60 日
毎週	26 週間	13 週間
毎月	18 カ月間	6 カ月間
毎年	5 年	3 年

毎晩のトレンド ジョブは、データが指定した保持期間よりも古くなった時、そのデータをパージします。

3. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで、変更は適用されません。

アプリケーション データの設定

[Settings] > [Reporting] > [Log Database] ページの **[Application Data（アプリケーション データ）]** セクションは、アプリケーションのレポート（[Application] ページの [Browser]、[Source Platform]、[Search] タブ）に入力するために使用する統計データの保持期間を決定します。

選択する期間は、実際のユーザー エージェント文字列が保存される期間には影響しません。それらは無期限に保存されます。これは帯域幅、要求の数、コンピュータの数などの統計情報にのみ影響します。

デフォルトでは、アプリケーション レポートの統計データは 30 日間保存されます。他の値を選択するには、下記の手順を実行します。

1. **[Keep data for（データを保持する期間）]** ドロップダウン リストから新しい期間を選択します。データーベース エンジンによっては、データを最大 90 日間保持できます。
2. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

ログ データベースのサイズ設定のガイドライン

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *データベース パーティション オプションの設定、518 ページ*
- *要求がログ記録される方法の設定、505 ページ*
- *URL がログ記録される方法の設定、524 ページ*

ログ データベースの正確なサイズ設定を行うのはむずかしいです。なぜならデータベースのサイズは、フィルタリングされるユーザーの数や 1 秒あたりの平均要求数などの多くの変数の影響を受けるからです。また、サイズはデータベースが下記のいずれの目的のために設定されているかによって影響されます。

- 各 Web 要求のヒット件数およびアクセス件数を記録する（*Log Server の設定、507 ページ*を参照）。

  ヒット件数を記録すると詳細な情報が得られますが、アクセス件数を記録すると約 40% までデータベースのサイズを小さくできます。

- ログ レコードを集約する（*Log Server の設定、507 ページ*を参照）。

  デフォルトでは、すべての要求が個別のヒット件数またはアクセス件数としてログ記録されます。集約をオンにしたとき、指定した時間内の同様の要求（同じユーザーによって、同じドメイン内のサイトに対して行われ、同じ処置が適用される要求）は、1 つのログ コードとして記録されます。それによってログ データベースのサイズを約 60 % 減らすことができます。

- 各ログ記録された要求の完全な URL を保存する（*URL がログ記録される方法の設定、524 ページ*を参照）。

  完全な URL を記録すると、ユーザーがアクセスしたサイトに関する正確な情報を提供しますが、ログ データベースのサイズが 2 倍以上になります。

- すべてのカテゴリのログの要求（*要求がログ記録される方法の設定、505 ページ*を参照）

  デフォルトでは、すべてのカテゴリ内のサイトの要求がログ記録されます。ログ データベースのサイズを減らすために、サイト（例、組織へのセキュリティ リスクや法的責任のないサイト）のログ記録の要求を停止できます。

  この変更の影響は、ログ記録されないカテゴリの数、およびユーザーがこれらのカテゴリ内のサイトに要求する頻度によって異なります。

- 詳細なブラウズ時間の計算を実行する（*インターネット ブラウズ時間の設定、525 ページ*を参照）。

  ブラウズ時間を含む調査詳細レポートを作成するために、IBT ジョブは詳細なブラウズ時間を計算しなければなりません。しかし、詳細なブラウズ時間データを保存すると、データベースのサイズが大きくなり、データベース パフォーマンスにも影響を与えることがあります。

- トレンド データを保存する（*トレンドおよびアプリケーション データの保持の設定、527 ページ*を参照）。

  トレンド データを保存すると、1 日、1 週間、またはそれ以上の長い期間の間のユーザーのインターネット アクティビティのトレンドに関するレポートを作成できます。データをより長く保存するほどデータベース サイズにより大きな影響を与えます。

アクティブおよび非アクティブの標準ロギング パーティションの毎日の平均サイズをモニタするには、[Settings] > [Reporting] > [Log Database page] ページを順に選択して、**[Growth Rates and Sizing（増加率とサイズ設定）]** チャートを使用します。この情報は、トラフィック量の経時的な傾向を把握するのに役立ち、将来の成長に備えることが容易になります。

平均サイズ設定情報を収集する際、（[Settings] > [Reporting] > [Log Database] ページの [Partition Management（パーティション管理）] セクション）のロールオーバー **[Initial Size（初期サイズ）]** および **[Growth（増加）]** の設定値を調整します。

最良の方法として、[Initial Size] の値をロール オーバー期間（週、月など）全体にわたる**平均パーティション サイズ**の約 80% に設定します。これは下記のことを目的としています。

- パーティションの拡張が必要になる回数を最小限にする。
- データをパーティションに入れる処理のためにリソースを解放する。
- パーティションを作成するときに、不必要なディスク スペースが割り当てられないようにする。

  パーティションに割り当てられた初期スペースの未使用の部分は、そのパーティションが削除されるまで復元することはできません。

ダッシュボードのレポーティング データの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[脅威]、[リスク]、[使用状況]、および [システム] ダッシュボードの要素で表示できる最大時間を設定するには、**[Settings] > [Reporting] > [Dashboard（ダッシュボード）]** ページを順に選択します。

Websense Web Security Gateway または Gateway Anywhere をインストールしている場合は、ネットワーク内で疑わしい脅威アクティビティに関連するファイルに関するデータを保存するためのフォレンシック リポジトリを作成するかどうかも設定できます。

ダッシュボード グラフの最大期間の設定

デフォルトでは、[Status] > [Dashboard] ページのすべてのタブ上のグラフ、カウンタ、およびテーブルは、データを最大 **30 日間**表示します。この制限は、ダッシュボードをロードするのにかかる時間を最小にし、TWeb Security manager の全体的なパフォーマンスを最適化し、ログ データベースの負荷を減らすために選択されました。

Microsoft SQL Server の標準バージョンと Enterprise バージョンの場合、ダッシュボード グラフをより長期間表示するように設定できます。しかし最大期間を拡張すると、Web Security manager とログ データベースの両方のパフォーマンスに重大な影響が及ぼすことがあります。

- [リスク]、[使用状況]、および[システム]ダッシュボードのグラフに表示できる最大期間を変更するには、**[Show a maximum of（最大を表示）]** ドロップダウリストから値を選択します。
  - 期間を増やしても、ログ データベースのサイズには影響しませんが、データベースを問い合わせる、情報を取得する、およびダッシュボードのグラフを更新するのに必要とされる時間が増えます。
  - Microsoft SQL Server Express を使用している場合、最大期間は、30 日間で、変更できません。

- [脅威] ダッシュボードおよび [Event Details（イベントの詳細）] ページの [Threats Data（脅威データ）] の下に表示されることがある最大期間を変更するには、**[Keep Threats data for（の間脅威データを保持）]** ドロップダウン リストから値を選択します。
  - 詳細な脅威データは、標準のロギング データとは別のパーティションに保存されますから、期間が増えるとログ データベースのサイズも大きくなります。
  - 脅威関連のフォレンシック データの格納が有効化されている場合（下記を参照）、フォレンシック リポジトリはここで選択した期間の間データを保存しようとします。しかし、最大リポジトリ サイズに達した場合、古いレコードが自動的に削除され新しいレコードを入れる空間をつくります。
  - Microsoft SQL Server Express を使用している場合、最大期間は、30 日間で、変更できません。

データは選択した全期間の間常に利用できるとは限りません。Websense Web Security ソリューションを 7 日間だけインストールしていた場合、例えば、30 日間のレポートはポリシーの実施が行われた 7 日間だけのデータを示します。

[脅威] ダッシュボードのサンプル データ

危険性の高いネットワーク トラフィックを生成せずに、[脅威] ダッシュボードで表示できるデータのタイプの例を確認したい場合、サンプル データをインポートできます。

サンプル データは Log Database にロードされており、そこでネットワーク内で生成された実際のデータと混合されますから、テスト環境または評価環境でのみサンプル データをロードすることを推奨します。

サンプル データであることを明確にするために、サンプル データベース内の各ユーザーには、**[Demo]** というミドル ネームが割り当てられます（例、Sam Demo Smith、Lisa Demo Brady）。さらに、ユーザー アクティビティのタイムスタンプの日付には、データを保持するログ データベースのパーティションの作成の日付よりも前の日付が使われます。

サンプル データをデータベースにインポートするには、**[Sample Data（サンプル データ）]** をクリックし、次に **[Import Sample Data（サンプル データをインポート）]** をクリックします。**[OK]** をクリックして、**[Save and Deploy]** をクリックしたとき、データがログ データベースにロードされます。数秒後、[脅威] ダッシュボードが新しいデータを示すように更新されます。

フォレンシック データの格納の設定

Websense Web Security Gateway および Gateway Anywhere 環境では、脅威に関連するフォレンシック データには下記の内容を含めることができます。

- データの送信を試みるソースに関する情報（IP アドレス、デバイス名、およびユーザー）。
- データが送信されるターゲットに関する情報（IP アドレス、URL、および地理的位置）。
- データの送信の試みに関連するヘッダー情報。
- 送信される実際のデータのコピー（例、テキスト ファイル、スプレッドシート、ZIP ファイル）。

フォレンシック データの格納を有効化した場合、**フォレンシック リポジトリ**が保存される場所、データベースを大きくできる最大サイズ、フォレンシック データを保存する期間も指定します。

1. [Incident Data for Forensic Investigation（フォレンシック調査のためのインシデント データ）] の下の **[Store forensic data about Threats incidents for further investigation（詳細な調査のために脅威インシデントに関するフォレンシック データを保存する）]** をオンにして、フォレンシック リポジトリを作成します。

   Websense Data Security ソリューションが配備されている場合、この新しいフォレンシック リポジトリは Data Security リポジトリに似ています。より小さな Web Security リポジトリでは、[脅威] ダッシュボードに表示されるインシデントについてのみ情報を保存します。

2. **[Blocked requests only（ブロックされている要求のみ）]**、か **[All requests（すべての要求）]**（ブロックされている要求と許可されている要求の両方）のどちらのフォレンシックの詳細を保存するかを指定します。
3. フォレンシック リポジトリをホストする場所への **[Path（パス）]** を指定します。
   - 指定されるディレクトリはすでに存在していなくてはなりません。
   - パスは、ローカル（TRITON 管理サーバー上）またはリモートにできます。
   - 選択した場所にリポジトリが下記で指定する最大サイズまで大きくなることができる十分なスペースがあることを確認してください。
4. アカウントの資格情報にフォレンシック リポジトリ ディレクトリの読取り、書込み、および削除の許可を与えます。
   - ディレクトリにアクセスするのにネットワーク アクセスも特別な許可も必要としない場合は、**[Use Local System account（ローカル システム アカウントを使用）]** を選択します。
   - ドメイン アカウントを使用し、次にアカウントの **[User name（ユーザー名）]**、**[Password（パスワード）]**、および **[Domain（ドメイン）]** を入力するには、**[Use this account（このアカウントを使用）]** を選択します。

   選択したアカウントがフォレンシック リポジトリの場所にアクセスできることを確認するには、**[Test Connection（テスト接続）]** をクリックします。

5. フォレンシック リポジトリの最大サイズを指定するには、フォレンシック リポジトリの **[Maximum size（最大サイズ）]** を単位 GB で入力します（デフォルト 20）。
   - SQL Server Express を使用している場合は、この値を変更できません。
   - 最大サイズに到達したとき、**または**レコードが脅威データに指定されている経過日数制限に到達したとき、レコードはリポジトリから自動的にパージされます。
6. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで、変更は適用されません。

調査レポートの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *データベース接続とレポートのデフォルト、535 ページ*
- *表示および出力のオプション、537 ページ*

調査レポートを使用して、組織のインターネット利用状況についての情報を対話形式で調査できます。*調査レポート、187 ページ*を参照してください。

メイン調査レポート ページのオプション リンクを使用して、レポート作成に使用されるログ データベースを変更できます。また、詳細レポートのデフォルト表示を変更することもできます。*データベース接続とレポートのデフォルト、535 ページ*を参照してください。

wse.ini ファイルを使用して、要約の表示 および マルチレベル レポートの特定のデフォルト値を設定できます。また、レポートが PDF に出力されるときに使用されるデフォルト ページ サイズを管理できます。*表示および出力のオプション、537 ページ*を参照してください。

データベース接続とレポートのデフォルト

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *調査レポートの設定、534 ページ*
- *表示および出力のオプション、537 ページ*
- *要約レポート、190 ページ*
- *マルチレベル要約レポート、196 ページ*

希望するログ データベースへ接続する、および調査レポートのデフォルト詳細表示を管理するには、**[Investigative Reports（調査レポート）] > [Options（オプション）]** ページを順に選択します。

このページの変更は レポートに影響を与えます。他の管理者、または セルフ レポートのためにログオンしているユーザーも、自身のレポート動作で、これらの値を変更することができます。

1. 調査レポートに使用するログ データベースを選択します。
   - Log Server がログ記録するログ データベースに接続するためには、**[View the catalog database（カタログ データベースを表示）]** をオンにします。ステップ 2 に進みます。
   - 別のログ データベースにアクセスするには、**[View the catalog database]** をオフにして、下記の情報を入力します。

フィールド	説明
Server（サーバー）	ログ データベースがあるコンピュータ名または IP アドレスを入力します。 お客様の環境で SQL Server クラスタ化を使用している場合、クラスタの仮想 IP アドレスを入力します。
Database（データベース）	ログ データベースの名前を入力します。
User ID（ユーザー ID）	データベースにアクセスする許可があるアカウントのユーザー ID を入力します。 Log Server が信頼関係接続で、ログ データベースにアクセスするように設定されている場合は、空白のままにします。
Password（パスワード）	指定されたアカウントのパスワードを入力してください。信頼関係接続の場合 空白のままにします。

2. 詳細レポートの下記のデフォルトの値を選択します。

フィールド	説明
Select default Investigative Reports date range（調査レポートのデフォルト日付範囲を選択）	初期表示の要約レポートの日付範囲を選択します。
Select the default detail report format（デフォルトの詳細レポート フォーマットを選択）	デフォルト列セットを使用して、レポートされる情報を詳細レポートに表示するためには、**[Smart columns selection（スマート列の選択）]** を選択します。 すべての詳細レポートの初期表示の正確な列を指定するためには、**[Custom columns selection（カスタム列の選択）]** を選択します。選択を行うために [Available Columns（使用可能な列）] リストを使用します。 レポートが作成された後で、ユーザーは表示された列を変更することができます。
Select report type（レポート タイプを選択）	最初に下記のどちらの詳細レポートを開くかを選択します： • **Detail（詳細）**：各レコードが別々の行に表示されます。時刻を表示できます。 • **Summary（要約）**：共通要素を共有するすべてのレコードを 1 つのエントリに結合します。この要素は、レポートされる情報によって異なります。一般に、測定基準の前の右端の列は要約された要素を示します。時刻は表示できません。
Available Columns / Current Report（使用可能な列 / 現在のレポート）	[Available Columns] リストで列名を選択し、[Current Report（現在のレポート）] リストに移動するために、適切な矢印をクリックします。最高 7 つの列を [Current Report] リストに載せることができます。 [Current Report] リストに最初の詳細レポートのすべての列を含めた後、列の順序を設定します。リストでエントリを選択し、上 / 下矢印ボタンでその位置を変更します。

3. **[Save Options（オプションの保存）]** をクリックし、すぐにすべての変更を保存します。

表示および出力のオプション

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *調査レポートの設定、534 ページ*
- *データベース接続とレポートのデフォルト、535 ページ*
- *調査レポートの出力のオプション、214 ページ*

特定のレポート選択とレポート結果が、要約およびマルチレベル調査レポートで表示される方法を調整することができ、PDF フォーマットにレポートが出力されるときのデフォルト ページ サイズを指定することができます。

これらの調査レポートの設定のオプションは、**wse.ini** ファイル（デフォルトでは、C:\Program Files（x86）\Websense\Web Security\webroot\Explorer\ ディレクトリにあります）で設定されます。

次の表は、調査レポートの表示と出力に影響を与えるパラメータ、管理するもの、デフォルト値をリストしています（wse.ini ファイルの他の設定を変更しないでください）。

パラメータ	説明
maxUsersMenu	[Internet Use by（インターネット使用状況）] リストのレポート選択としてユーザーを表示するためには、データベースはこの値より少ないユーザー（デフォルトは、5000）である必要があります。
maxGroupsMenu	[Internet Use by] リストのレポート選択としてグループを表示するためには、データベースはこの値より少ないグループ（デフォルトは、3000）である必要があります。 **注意：**[Internet Use by] リストにグループが表示されるためには、2 つ以上のグループがある必要があります。 また、[Internet Use by] リストにドメインが表示されるためには、2 つ以上のドメインがある必要があります。ドメインの最大値はありません。

パラメータ	説明
maxUsersDrilldown	これは、[User（ユーザー）] オプションがいつ赤色で表示されるかを管理するために、warnTooManyHits パラメータとともに動作します。赤色の文字は、[User] の選択が非常に大きいレポートを作成し、作成が遅くなることを示しています。 この値（デフォルトは、5000）より多くのユーザーがあり、warnTooManyHits 値より多くのヒット件数がある場合、種々のドロップダウンリストと値のリストで、[User] オプションは赤色に表示されます。 この値より多くのユーザーがあり、warnTooManyHits 値より少ないヒット件数の場合、結果のレポートは妥当なサイズであるとして、[User] オプションは通常の色で表示されます。
maxGroupsDrilldown	指定されたレポートがこの数（デフォルトは、2000）より多くのグループを含む場合、[Group（グループ）] オプションは絞り込み中に赤色で表示されます。赤色の文字は、[Group] の選択が非常に大きいレポートを作成し、作成が遅くなることを示しています。
warnTooManyHits	これは、[User] オプションがいつ赤色で表示されるかを管理するために、maxUsersDrilldown パラメータとともに動作します。 maxUsersDrilldown 値より多くのユーザーがあり、ヒット件数がこの値（デフォルトは、10000）より少ない場合、[User] オプションは赤色で表示*されません*。 maxUsersDrilldown 値より多くのユーザーがあり、この値より多くのヒット件数がある場合、[User] オプションは赤色で表示されます。赤色の文字は、[User] の選択が非常に大きいレポートを作成し、作成が遅くなることを示しています。
hitsPerPage	1 ページに表示される項目の最大数（デフォルトは、100）を決定します（これは 印刷レポートに影響を与えません）。

パラメータ	説明
maxOutputBufferSize	これは、メイン調査レポート ページに表示できる最大データ量（単位 バイト）です。要求されたデータがこの限度（デフォルトは、4000000 または 4 メガバイト）を超える場合、いくつかの結果が表示されないことを示すメッセージがレポートの終わりに赤色で表示されます。 問題がある場合、値をより大きくし、1 つのレポートでより大きい量のデータを表示することができます。しかし、メモリ エラーが発生する場合、この値を小さくすることを考慮してください。
sendMulti	このオプションはデフォルトでは無効（0）です。非常に大きい、スケジュールされた詳細レポートを、10,000 行の複数のファイルに分けるためには、このパラメータを 1（有効）にセットします。1 つのレポートに相当するファイルは、圧縮されて電子メール受信者に送信されます。レポート ファイルは、ほとんどのファイル圧縮ユーティリティで展開できます。 注意：この値の変更は、Explorer Report Scheduler サービスが再開されるまでは適用されません。
maxSlices	これは、個別のスライスがないすべての値を結合する [その他] のスライスを含めて、円グラフのスライスの最大数（デフォルトは、6）です。
timelineCompressionThreshold	[Group Similar Hits/View All Hits（類似グループ ヒット件数 / 全ヒット件数）] の表示オプションが有効な場合に、このオプションは、日別ユーザー活動詳細 および 月別ユーザー活動詳細でのみ使用されます。ここで設定された秒数（デフォルトでは、10）以内に発生した同じカテゴリのすべてのヒット件数は、レポートで折りたたまれます。
PageSize	調査レポート結果は、容易に配布または印刷できるよう、Portable Document Format（PDF）に出力することができます。ページ サイズ（デフォルトでは、レター）は、下記のサイズに設定できます。 • A4（8.27 X 11.69 インチ） • レター（8.5 X 11 インチ）

セルフレポーティング

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *レポートの優先設定、503 ページ*
- *セルフレポートへのアクセス、215 ページ*
- *調査レポート、187 ページ*

セルフレポーティングは、個人のインターネット アクティビティの調査レポートをユーザーに表示することを許可することができる機能です。これは、ユーザーにどんな種類の情報が収集され、モニタされているかを参照することを許可します。これは、多くの国の政府規制に適合しています。さらに、ユーザーに自分のアクティビティを見せるようにすれば、一部のユーザーは自分のブラウジング習性を見直して、組織のインターネット ポリシーに適合するようになるかも知れません。

セルフ レポーティングを有効にするには下記の手順を実行します。

1. **[Settings] > [General] > [Directory Services（ディレクトリ サービス）]** を順に選択し、ネットワーク資格証明で調査レポートにアクセスするユーザーを認証するために使用するディレクトリ サービスを設定します。これは、以前にユーザーおよびグループ名によるポリシー アプリケーションを有効化にするために、行われているかもしれません。*ディレクトリ サービス、93 ページ*を参照してください。
2. **[Settings] > [Reporting（レポーティング）] > [Preferences（優先設定）]**を順に選択し、**[Allow self-reporting（セルフ レポーティングを許可]** をオンにします。*レポートの優先設定、503 ページ*を参照してください。

オプションを有効にした後、必ずユーザーにレポートを実行するために必要な下記の情報を提供してください。

- セルフ レポーティング インターフェースにアクセスするための URL：

  ```
  https://<IP_address> :9443/mng/login/pages/
  selfReportingLogin.jsf
  ```

  <IP_address> を TRITON 管理サーバーの IP アドレスに置き換えます。

  後で使用できるように、URL をお気に入りまたはブックマークとして保存することができることをユーザーに通知してください。

  また、管理者とユーザは、TRITON コンソールのログオン ページを開いて、[TRITON（セルフ レポート）] リンクをクリックすることで、セルフ レポート ログオン ページにアクセスすることができます。

- ログオン時に使用するユーザー名とパスワード。

  セルフ レポーティング ユーザーは、ログオン時にネットワーク ユーザー名とパスワードを入力する必要があります。

18 ネットワークの構成

関連トピック：

- *Network Agent の設定*、542 ページ
- *Network Agent 設定の確認*、551 ページ

プロキシまたはファイアウォール製品と統合されていないスタンドアロン モードで、Websense Web Security または Websense Web Filter を実行した場合、Websense Network Agent は、下記の機能を有効化します。

- インターネット ポリシーの適用
- ネットワーク プロトコルおよびインターネット アプリケーション管理
- 帯域幅管理
- 転送バイト数のログ記録

Websense Web Security Gateway または Gateway Anywhere を使用しているとき、または Web Security または Web Filter がサードパーティのゲートウェイ、ファイアウォール、またはキャッシング製品と統合されている場合、Content Gateway またはサードパーティ製品はユーザー要求をポリシーの適用のために Filtering Service へルーティングし、ブロック ページをクライアントに返送します。この環境では、非 HTTP 要求を管理するため、インターネット アクティビティをログするを管理するために、またはその両方のために Network Agent が使用されることがあります。

また、Websense Web Security Gateway および Gateway Anywher は、Network Agent から独立して、HTTP をトンネリングするプロトコルを検出することができ（*トンネリング プロトコルの検出*、235 ページを参照）、また一部の帯域管理機能を提供します（*Bandwidth Optimizer による帯域幅の管理*、342 ページを参照）。

Network Agent は、ネットワーク上で転送されたバイト数を含む、全体的なネットワーク利用状況を絶えずモニタします。エージェントは、事前指定されている間隔で利用状況の要約をログ記録します。各要約には、開始時刻、終了時刻、全体の使用バイト数、プロトコル毎の使用バイト数が含まれます。

デフォルトでは、Network Agent は、Policy Server に帯域幅使用状況データを、Filtering Service にインターネット アクティビティ ログ データを提供します。

一般に、Network Agent は、ネットワーク上のすべてのトラフィックを確認するように設定されます。このエージェントは、下記の要求を識別します。

- 内部コンピュータから内部コンピュータへ送信された要求（例えば、イントラネット サーバーのヒット件数）。
- 社内コンピュータからウェブ サーバーなどの外部コンピュータに送信される要求（例、ユーザー インターネット要求）

従業員インターネット利用状況のモニタにおいては、後者が主要な関心事です。

Network Agent の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：
- *グローバル設定*、543 ページ
- *ローカル設定*、544 ページ
- *NIC の設定*、547 ページ
- *IP アドレスの追加と編集*、550 ページ

Network Agent をインストールした後、そのネットワークのモニタリング動作を設定するために、Web Security manager を使用します。Network Agent の設定は、下記の 2 つのメイン エリアに分かれています。

- **グローバル設定**は、Policy Server インスタンスに関連付けられているすべての Network Agent インスタンスに影響します。これらの設定を使用して下記の事柄を実行します。
  - ネットワーク内のコンピュータを指定します。
  - Network Agent が**着信**要求をモニタするネットワーク内のコンピュータ（例えば、内部 Web サーバー）をリストします。
  - 帯域幅の計算とプロトコル ログ記録の動作を指定します。
- **ローカル設定**は、選択された Network Agent のインスタンスにだけ適用します。これらの設定を使用して下記の事柄を実行します。
  - どの Filtering Service のインスタンスを各 Network Agent に関連付けるかを指定します。
  - この Network Agent がモニタするコンピュータによって使用されるプロキシとキャッシュを記録します。

- Network Agent コンピュータの各ネットワーク カード（NIC）の使用方法（要求のモニタ、または、ブロックページの送信、または その両方）を設定します。

  また、ネットワーク カードの設定は、各 Network Agent のインスタンスがどのネットワーク セグメントをモニタするか決定します。

グローバル設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *ローカル設定、544 ページ*
- *NIC の設定、547 ページ*
- *IP アドレスの追加と編集、550 ページ*

現在の Policy Server（Web Security ツールバーに表示される IP アドレスの Policy Server）接続されている Network Agent のすべてのインスタンスの基本的なモニタリングとログ記録の動作を定義するには、**[Settings] > [Network Agent] > [Global]** ページを使用します。

[Describe Your Network（使用しているネットワークを説明）] リストは、使用しているネットワークの一部である IPv4 または IPv6 フォーマットの IP アドレスを特定します。デフォルトでは、Network Agent は、これらの IP アドレス**間**で送信されたトラフィック（内部のネットワーク通信）をモニタしません。

Network Agent は、どの IP アドレスがインターネット要求のモニタ対象かを判断するときこのリストは使用しません。その動作は、各 NIC で別個に設定されます（*NIC の設定、547 ページ*を参照）。このリストは、モニタリングから内部トラフィック（LAN やイントラネット接続など）を除外するためにだけ使用されます。

デフォルトでは、エントリの初期セットが提供されています。さらにエントリを追加するか、既存のエントリを編集または削除することができます。

[Internal Traffic to Monitor（モニタ対象の内部トラフィック）] リストには、Network Agent にトラフィックをモニタ**させる**内部 IPv4 または IPv6 アドレス（[Describe Your Network] リストに含まれている）が含まれています。例えば、内部接続を追跡するために、内部 Web サーバーを含めることができます。

ネットワークのどこからでも指定された内部のコンピュータに送信された要求は、すべてモニタされます。デフォルトで、このリストは空白です。

- 適切なリストに IP アドレスまたは範囲を追加するには、**[Add（追加）]** をクリックします。IPv4 フォーマットと IPv6 フォーマットの両方がサポートされています。詳細は、*IP アドレスの追加と編集、550 ページ*を参照してください。

- リストのエントリを編集するには、IP アドレスまたは範囲をクリックします。詳細は、*IP アドレスの追加と編集、550 ページ*を参照してください。
- リストからエントリを削除するには、IP アドレスまたは範囲の隣のチェックボックスをオンにして、**[Delete（削除）]** をクリックします。

[Additional Settings（追加設定）] オプションで、Network Agent が帯域幅使用状況を計算する頻度、プロトコルト トラフィックをログ記録する頻度を決定できます .

フィールド	使用方法
Bandwidth calculation interval（帯域幅の計算の間隔）	Network Agent が帯域幅使用状況を計算する頻度（単位秒）を指定するために 1 から 300 までの数字を入力します。例えば、300 と入力した場合、Network Agent は 5 分ごとに帯域幅を計算します。 デフォルトは 10 秒です。
Log protocol traffic periodically（プロトコルのトラフィックを定期的にログ記録する）	このオプションをオンすると [Logging interval（ログ記録間隔）] フィールドが有効化します。
Logging interval（ログ記録間隔）	Network Agent がプロトコルをログ記録する頻度（単位分）を指定するには、1 から 300 までの数字を入力します。例えば、60 と入力した場合、Network Agent は 1 時間ごとにログファイルに書き込みます。 デフォルトは 1 分です。

変更を完了しとき、**[OK]** をクリックして変更をキャッシュします。**[Save and Deploy（保存と配備）]** をクリックするまで、変更は適用されません。

ローカル設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *グローバル設定、543 ページ*
- *NIC の設定、547 ページ*

Network Agent の選択したインスタンスのインターネット トラフィック管理、プロキシ情報、その他の設定を設定するには、**[Setting s] > [Network Agent] > [Local Settings（ローカル設定]** ページを順に選択します。

- Network Agent の [Local Settings] ページを表示するには、[Settings] > [Network Agent] を順に選択し、マウスを **[Global（グローバル）]** オプションの上に置きます。IP アドレスのリストが表示されます。設定するインスタンスの IP アドレスを選択します。
- 選択した Network Agent インスタンスの IP アドレスがコンテンツ ペインのタイトル バーに表示されます。

[Filtering Service Definition（Filtering Service の定義）] を使用して、どの Filtering Service が選択した Network Agent インスタンスと関連しているかを指定し、Filtering Service が利用可能でない場合にインターネット要求に対する応答方法を指定します。

フィールド	使用方法
Filtering Service IP address（Filtering Service の IP アドレス）	この Network Agent と関連付けられた Filtering Service を選択します。
If Filtering Service is unavailable（Filtering Service が使用できない場合）	Filtering Service が再び利用可能になるまで、すべての要求を許可するには **[Permit（許可）]** を選択し、すべての要求をブロックするには **[Block（ブロック）]** を選択します。デフォルトは Permit です。

正確に ユーザーの要求がモニタされ、管理され、ログ記録されるために、**[Proxies and Caches（プロキシとキャッシュ）]** リストを使用して、Network Agent と通信するすべてのプロキシまたはキャッシュ サーバーの IP アドレスを指定します。

- 適切なリストに IPv4 または IPv6 アドレスまたは範囲を追加するには、**[Add]** をクリックします（*IP アドレスの追加と編集、550 ページ*を参照）。
- リストのエントリを編集するには、IP アドレスまたは範囲をクリックします。
- リストからエントリを削除するには、IP アドレスまたは範囲の隣のチェックボックスをオンにして、**[Delete]** をクリックします。

個々の NIC を設定するには、**[Network Interface Cards（ネットワーク インターフェース カード）]** リストを使用します。**[Name（名前）]** 列にある NIC をクリックします。その後の手順については、*NIC の設定、547 ページ*を参照してください。

下記の場合に **[Advanced Network Agent Settings（Network Agent 詳細設定）]** オプションを使用します。

- ネットワーク内の HTTP 要求が非標準ポートを通過する場合。

  デフォルトでは、**[Ports used for HTTP traffic（HTTP トラフィックで使用されるポート）]** は、**[8080]**、**[80]**（Websense ソフトウェアがファイアウォール、プロキシ、またはキャッシュと統合されている場合）、または **[All（すべて）]**（スタンアロン環境の場合）です。

- Network Agent が特定のポート上のトラフィックを無視するように設定する場合。

  [Configure this Network Agent instance to ignore traffic on the following ports（下記のポート上のトラフィックを無視するようにこの Network Agent を設定）] をオンにし , 次に 1 つ以上のポートを入力します。

  Websense Content Gateway を配備している場合は、これを使用して HTTPS トラフィックの二重ログ記録を防ぐことができます。

- Websense テクニカル サポートがトラブルシューティングのためにデバッグ オプションを変更するように指示した場合。

  [Debug Settings（デバッグ設定）] のオプションは、テクニカル サポートの指示がない場合は変更してはいけません。

フィールド	説明
Mode（モード）	• なし（デフォルト） • 一般 • エラー • 詳細 • 帯域幅
Output（出力）	• ファイル（デフォルト） • ウィンドウ
Port（ポート）	55870（デフォルト）

Network Agent の設定の変更を完了したとき、**[OK]** をクリックして変更をキャッシュします。**[Save and Deploy]** をクリックするまで、変更は適用されません。

NIC の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *Network Agent の設定*、542 ページ
- *NIC のモニタリング設定*、549 ページ
- *IP アドレスの追加と編集*、550 ページ

ネットワーク利用状況をモニタし 管理するために、Network Agent が利用可能な各ネットワーク インターフェース カード（NIC）を使用する方法を指定するには、**[Network Agent] > [Local Settings（ローカル設定）] > [NIC Configuration（NIC の設定）]** ページを順に選択します。

[NIC Information（NIC 情報）] エリアには、変更内容のコンテクストが表示され、**IP アドレス**、簡単な NIC の**説明**、カード**名**を示します。正しい NIC を設定するためにこの情報を使用します。

モニタリング

複数の NIC 構成の場合、ネットワーク トラフィックをモニタする NIC とブロックページを配信する他の NIC を識別することができます。少なくとも 1 つの NIC をモニタリングのために使用する必要があります。また複数の NIC がトラフィックをモニタできます。

[Use this NIC to monitor traffic（トラフィックのモニタリングにこの NIC を使用）] オプションを使用するかどうか指定するには、**[Monitoring（モニタリング）]** セクションを使用します。

- モニタリングにこの NIC を使用しない場合は、チェックボックスの選択を取り消して、次のセクションに進みます。
- モニタリングに この NIC を使用する場合は、このチェックボックスを選択し、**[Configure（設定）]** をクリックします。[Configure Monitoring Behavior（モニタリング動作の設定）] ページが開きます。手順については、*NIC のモニタリング設定*、549 ページを参照してください。

その他の NIC のオプション

モニタリング オプションの設定に加えて、その他の NIC の動作を指定することができます：

1. [Blocking（ブロック中）] の下の **[Blocking NIC（ブロックする NIC）]** フィールドに適切な NIC がリストされていることを確認します。複数の NIC を指定している場合、このフィールドの各 NIC の設定は同じ値を示します。換言すれば、ブロックするために使用される NIC は 1 つだけです。
2. **スタンドアロン** モードで Websense ソフトウェアを実行している場合は、**[Filter and log HTTP requests（HTTP 要求のフィルタリングとログ記録）]** が選択され、変更できません。
3. Websense ソフトウェアをサードパーティのデバイスまたはアプリケーションと統合している場合は、Network Agent が HTTP 要求をフィルタリングする方法、および記録する方法を指定するには、**[Integrations（統合）]** のオプションを使用します。お客様の環境で適用できないオプションは無効になっています。
   - Network Agent がすべてのインターネット アクティビティ ログ レコードを生成するようにするには **[Log HTTP requests（HTTP 要求のログ記録）]** を選択します。

     このオプションを選択した場合、統合製品によって生成されたログ レコードは Filtering Service によって廃棄されます。Network Agent が作成するログ レコードだけが、ログ データベースに保存するために Log Server に転送されます。
   - Network Agent を使って統合製品経由で送信されていない要求だけをフィルタするには、**[Filter all requests not sent over HTTP ports（HTTP ポート以外で送信されたすべての要求をフィルタする）]** を選択します。
4. [Protocol Management（プロトコル管理）] で、Network Agent が非 HTTP プロトコルをフィルタするためにこの NIC を使用するかどうかを指定します。
   - プロトコル管理機能を有効にするには、**[Filter non-HTTP protocol requests（非 HTTP プロトコル要求をフィルタ）]** をオンにします。それによって、Websense ソフトウェアは、インスタント メッセージ送信、ストリーミング メディア、ファイル共有、インターネット メールなどに使用されるデータ転送方法やインターネット アプリケーションをフィルタすることができます。詳細については、*カテゴリおよびプロトコルへのアクセスの管理、59 ページ*と*プロトコルの使用、335 ページ*を参照してください。
   - Bandwidth Optimizer 機能を有効にするには、**[Measure bandwidth usage by protocol（プロトコル別に帯域幅使用状況を測定）]** をオンにします。Network Agent は、この NIC を使用して各プロトコルまたはアプリケーションによるネットワーク帯域幅利用状況を追跡します。詳細は、*Bandwidth Optimizer による帯域幅の管理、342 ページ*を参照してください。

NIC のモニタリング設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Network Agent が選択されたネットワーク インターフェース カード（NIC）を使用してモニタする IP アドレスを指定するには、**[Local Settings] > [NIC Configuration] > [Monitor List（モニタ リスト）]** ページを順に選択します。

1. [Monitor List] で、Network Agent がモニタする要求を指定します。
   - **All（すべて）**：Network Agent は、選択された NIC を使用して確認するすべての IP アドレスからの要求をモニタします。一般に、これは現在の Network Agent コンピュータまたは NIC と同じネットワーク セグメントにあるすべてのコンピュータを含みます。
   - **None（なし）**：Network Agent は、すべての要求をモニタしません。
   - **Specific（特定）**：Network Agent は、[Monitor List] に含められているネットワーク セグメントだけをモニタします。
2. [Specific] を選択した場合は、**[Add（追加）]** をクリックして、次に Network Agent が IPv4 または IPv6 フォーマットでモニタする IP アドレスを指定します。詳細は、*IP アドレスの追加と編集、550 ページ*を参照してください。

   > **注意**
   > 重複した IP アドレス範囲を入力することはできません。範囲が重複した場合、ネットワーク帯域幅の測定が正確ではない可能性があり、帯域幅ベースの制限が正確に適用されない可能性があります。

   IP アドレスまたはネットワーク範囲をリストから削除するには、適切なリスト項目をオンにし、**[Delete]** クリックします。
3. [Monitor List Exceptions（モニタ リスト例外）] で、Network Agent がモニタリングから除外するすべての内部コンピュータを指定します。

   例えば、Network Agent は CPM Server によって行われる要求を無視することができます。このようにすれば、CPM Server の要求が Websense ログ データやステータス モニタの出力を混乱させることはありません。
   a. コンピュータを指定するには、**[Add]** をクリックし、そのコンピュータの IP アドレスを IPv4 または IPv6 フォーマットで入力します。
   b. 追加のコンピュータを指定するには手順を繰り返します。
4. **[OK]** をクリックして変更をキャッシュし、[NIC Configuration] ページに戻ります。**[Save and Deploy]** をクリックするまで、変更は適用されません。

IP アドレスの追加と編集

Web Security Help | Web Security ソリューション | バージョン 7.8.x

関連項目：

- *グローバル設定、543 ページ*
- *ローカル設定、544 ページ*
- *NIC の設定、547 ページ*

下記の Network Agent のリストのいずれかに変更を行うには、**[Add IP Addresses（IP アドレスを追加）]** ページまたは **[Edit IP Addresses（IP アドレスを編集）]** ページを使用します。[Internal Network Definition（内部ネットワーク定義）]、[Internal Traffic to Monitor（モニタする内部トラフィック）]、[Proxies and Caches（プロキシとキャッシュ）]、[Monitor List]、[Monitor List Exceptions]。

- IPv4 と IPv6 の両方のアドレスおよび範囲がサポートされています。
- IP アドレス範囲を追加または編集する場合は、リスト内の既存のエントリ（単一の IP アドレスまたは範囲）と重複しないようにしてください。
- 単一の IP アドレスを追加または編集する場合は、それがリスト内ですでに表示されている範囲に含まれないようにしてください。

新しい IP アドレスまたは範囲を追加するには、下記の手順を実行します。

1. **[IP address（IP アドレス）]** または**[IP address range（IP アドレス範囲）]** ラジオボタンを選択します。
2. 有効な IP アドレスまたは範囲を入力します。
3. **[OK]** をクリックして、前の [Network Agent Settings] ページに戻ります。新しい IP アドレスまたは範囲が適当なテーブルに表示されます。

   変更をキャッシュしないで前のページに戻るには、**[Cancel（キャンセル）]** をクリックします。
4. 必要に応じて、他の IP アドレスに対してこの手順を繰り返します。

既存の IP アドレスまたは範囲を編集するとき、[Edit IP Addresses（IP アドレスを編集）] ページに、すでに選択されている正しいラジオ ボタンと選択項目が表示されます。必要な変更をすべて行い、**[OK]** をクリックして前のページに戻ります。

IP アドレスの追加または編集が完了したとき、[Network Agent Settings] ページで **[OK]** をクリックします。**[Save and Deploy]** をクリックするまで、変更は適用されません。

Network Agent 設定の確認

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Web Security manager で Network Agent を設定した後、サードパーティのパケット アナライザを使用して、ネットワーク上のコンピュータが Web Security ソリューションによって認識されることを確認します。

Network Agent モニタリング NIC として設定したネットワーク カードが、モニタリングのために Network Agent インスタンスが設定されているすべてのネットワーク セグメント内の IP アドレスからのトラフィックを把握できることを確認します。（この設定は、[Local Settings] > [NIC Configuration] > [Monitor List] ページで行われます。*NIC のモニタリング設定、549 ページ*を参照してください。）

いずれかの IP アドレスからのパケットがモニタリング用の NIC に認識されない場合、下記のどちらかの処置を実行します。

- ネットワーク構成および NIC 交換の要件を見直します（Deployment and Installation Center または Network Agent クイック スタートを参照）。
- モニタリング用 NIC を適切に設定していることを確認します（*NIC の設定、547 ページ*）。

19 トラブルシューティング

Web Security Help | Web Security ソリューション | バージョン 7.8.x

テクニカル サポートにお問い合わせされる前に、このセクションで、よく起きる問題の解決方法を見つけてください。

Websense Support ウェブサイトは、広範なナレッジ ベースとカスタマ フォーラムを備えており、support.websense.com から入手できます。キーワードまたはフレーズによってトピックを検索するか、または製品およびバージョンによってコンテンツを参照してください。

トラブルシューティングについての説明は、下記のセクションに分かれています。

インストールとサブスクリプションの問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

サブスクリプションの問題がある

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense マスタ データベースをダウンロードし、インターネット ポリシーの実施を実行するには、有効なサブスクリプション キーが必要です。サブスクリプションが期限切れまたは無効になっていて、マスタ データベースが 2 週間以上ダウンロードされていない場合、**[Status（ステータス）] > [Alerts]** ページに警告が表示されます。

- Websense サブスクリプション キーを受信したとおりに入力したことを確認してください。キーは大文字と小文字を区別します。
- サブスクリプションが期限切れになっていないことを確認します。*サブスクリプション キー、558 ページ*を参照してください。
- 最近の 2 週間の間にマスタ データベースが正常にダウンロードされていることを確認します。ダウンロード スタータスを確認するには、Web Security manager の [Status] > [Dashboard] ページを順に選択し、**[Database Download（データベースのダウンロード）]** をクリックします。

  データベースのダウンロードの問題のトラブルシューティングに役立てるために、*マスタ データベースがダウンロードしない、557 ページ*を参照してください。

キーを正しく入力したのに、まだステータス エラーが表示される、またはサブスクリプションが期限切れになっている場合は、Websense, Inc., または再販業者にお問い合わせください。

ライセンスが期限切れになっている場合、Web Security manager の設定に従って、すべてのユーザに無制限にインターネット アクセスが許可されるか、またはすべてのインターネット要求がブロックされます。詳細は、*サブスクリプション、27 ページ*を参照してください。

サブスクリプション キーを確認できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

サブスクリプション キーを入力した後、Filtering Service は、キーを確認し Master Database をダウンロードするために Websense データベース ダウンロード サーバーへの接続を試みます。

Filtering Service がデータベース ダウンロード サーバーに接続できない場合、サブスクリプション エラーとデータベース ダウンロード エラーの両方が Web Security manager に表示されます。

- データベース ダウンロード サーバーが停止した場合は、問題は短時間のうちに自動的に解決します。
- Filtering Service がダウンロード サーバーに接続できない場合は、*インターネット アクセス、558 ページ* および *ファイアウォールまたはプロキシ サーバーの設定の確認、559 ページ*を参照し、接続ができるように Filtering Service とネットワーク環境が適切に設定されていることを確認してください。

アップグレードの後、ユーザーが Web Security manager に表示されない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Web Security ソリューションをアップグレードした後、ディレクトリ サービスとして Active Directory を指定した場合、非 UTF-8 文字を含むユーザー名が Web Security manager に表示されない場合があります。

LDAP 3.0 をサポートするために、Websense インストーラはアップグレード時に文字セットを MBCS から UTF-8 に変更します。そのため、UTF-8 文字セットに含まれない文字を含む名前が正しく認識されません。

この問題を解決するには、下記の手順を実行して手動で文字セットを MBCS に変更します。

1. **[Settings（設定）] > [General（一般）] > [Directory Services（ディレクトリ サービス）]** を順に選択します。
2. ページ上部の [Directories（ディレクトリ）] の下で **[Active Directory（Native Mode）（Active Directory（ネイティブ モード））]** が選択されていることを確認します。
3. **[Advanced Directory Settings（ディレクトリの詳細設定）]** をクリックします。
4. [Character Set（文字セット）] の下の **[MBCS]** をクリックします。このオプションが表示されていない場合は、下にスクロールします。
5. **[OK]** をクリックして変更をキャッシュします。**[Save and Deploy]** をクリックするまで、変更は適用されません。

マスタ データベースの問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

初期フィルタリング データベースが使用されている

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense マスタ データベースには、インターネット コンテンツの管理の基礎となるカテゴリおよびプロトコル定義が格納されています。

Filtering Service がインストールされている各コンピュータには、Websense ソフトウェアと共に、マスタ データベースの縮小版がインストールされています。この縮小版データベースは、ユーザーがサブスクリプション キーを入力した時点から基本的な機能を有効化するために使用します。

完全なポリシーの適用を実行するには、完全なデータベースをダウンロードする必要があります。詳細は、*Websense マスタ データベース、32 ページ*を参照してください。

データベースをすべてのダウンロードするプロセスには数分から 60 分以上かかることがあります。インターネット接続速度、帯域幅、使用可能なメモリ、空き容量などにより異なります。

マスタ データベースが 1 週間以上経過して古くなっている

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense マスタ データベースには、インターネット コンテンツの管理の基礎となるカテゴリおよびプロトコル定義が格納されています。Websense ソフトウェアは、Web Security manager で指定されたスケジュールに従って、マスタ データベース に変更をダウンロードします。デフォルトでは、ダウンロードは 1 日 1 回行われるようにスケジュール設定されています。

手動でデータベースのダウンロードを開始するには、下記の手順を実行します。

1. **[Status（ステータス）] > [Dashboard（ダッシュボード）]**ページを順に選択し、**[Database Download]** をクリックします。
2. 該当する Filtering Service インスタンスの横の **[Update（更新）]** をクリックしてデータベースのダウンロードを開始するか、または **[Update All（すべて更新）]** をクリックして Filtering Service がインストールされているすべてのコンピュータへのダウンロードを開始します。

> **注意**
> マスタ データベースの更新のダウンロード後、データベースがローカル メモリにロードされている間は、CPU 使用率が 90% に達する場合があります。ダウンロードはピーク時間外に実行することを推奨します。

3. データベースのダウンロード中も作業を継続する場合は、**[Close（閉じる）]** をクリックします。

   いつでも、**[Database Download]** ボタンをクリックすることによってダウンロード ステータスを表示することができます。

マスタ データベースの新しいバージョンがカテゴリまたはプロトコルを追加または削除した場合は、ダウンロード時にカテゴリまたはプロトコル関連のポリシー管理タスク（カテゴリ セットの編集など）を実行している管理者はエラーを受け取ることがあります。そのような更新は比較的稀ですが、最善を期して、データベースの更新中はカテゴリ、プロトコル、フィルタに対する変更を行わないことを推奨します。

マスタ データベースがダウンロードしない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense マスタ データベースを正常にダウンロードできない場合は、下記のことを確認してください。

- Web Security manager でサブスクリプション キーを正しく入力していること、およびそのキーが期限切れになっていないことを確認します（*サブスクリプション キー、558 ページ*）。
- Filtering Service がインストールされているコンピュータがインターネットにアクセスできることを確認します（*インターネット アクセス、558 ページ*）。
- ファイアウォールまたはプロキシ サーバーの設定をチェックして、Filtering Service が Websense ダウンロード サーバーに接続できることを確認します（*ファイアウォールまたはプロキシ サーバーの設定の確認、559 ページ*）。

- ダウンロードに使用するコンピュータに十分なディスク スペースがあること（*Filtering Service をインストールしているコンピュータのディスク スペースが不足している、561 ページ*）およびメモリがあること（*Filtering Service をインストールしているコンピュータのメモリーが不足している、562 ページ*）を確認します。
- ネットワーク上にダウンロード接続を妨げる可能性があるアプリケーションまたはアプライアンス（アンチウィルス ソフトウェアなど）がないか調べます（*制限アプリケーション、563 ページ*）。

サブスクリプション キー

Web Security Help | Web Security ソリューション | バージョン 7.8.x

サブスクリプション キーが正しく入力されていて、期限切れになっていないことを確認するために、下記の手順を実行します。

1. **[Settings] > [General] > [Account（アカウント）]** ページを順に選択します。
2. Websense, Inc., または再販業者から受け取ったキーと **[Subscription key（サブスクリプション キー）]** フィールドに入力したキーを比較します。
3. **[Key expires（キーの有効期限）]** の横の日付を調べます。この日付を過ぎている場合、再販業者または Websense, Inc., に連絡して、サブスクリプションを更新してください。
4. [Settings（設定）] ダイアログボックスでキーを変更した場合は、**[OK]** をクリックしてキーを有効にし、データベースのダウンロードを有効化します。

手動でデータベースのダウンロードを開始したり、最新のデータベースのダウンロードの状況をチェックするには、[Status] > [Dashboard] ページの上部のツールバーにある **[Database Download]** をクリックします。

インターネット アクセス

Web Security Help | Web Security ソリューション | バージョン 7.8.x

マスタ データベースをダウンロードするために、Filtering Service がインストールされているコンピュータは下記の URL にあるダウンロード サーバーに **HTTP post** コマンドを送信します。

download.websense.com
ddsdom.websense.com
ddsint.websense.com
portal.websense.com
my.websense.com

Filtering Service を実行しているコンピュータでダウンロード サーバーと通信するために必要なインターネット アクセスが可能であることを確認するために、下記の手順を実行します。

- non-appliance インストールに対しては、Filtering Service を実行しているコンピュータ上でブラウザを開き、下の URL を入力します。

  http://download.websense.com/

  コンピュータがサイトへの HTTP 接続を開くことができる場合は、リダイレクト ページが表示され、次にブラウザに Websense ホーム ページが表示されます。
- コマンド プロンプトまたはシェルから下記のコマンドを入力します。

  ```
  ping download.websense.com
  ```

  ping コマンドに対してダウンロード サーバーから応答が返されることを確認します。
- telnet を使用して **download.websense.com 80** に接続します。カーソルが表示され、エラー メッセージが表示されない場合は、ダウンロード サーバーに接続できます。

Filtering Service を実行しているコンピュータがダウンロード サーバーと接続できない場合は、下記の手順を実行します。

- Filtering Service が使用するインターフェースのために、ポート 80 またはネットワーク内で HTTP トラフィックのために指定されているポート上での通信を有効化します。Websense アプライアンスでは、これは通常は C インターフェースです。
- Filtering Service ネットワーク インターフェースが正しい DNS 設定を使用していることを確認します。
- Filtering Service がインターネットに接続するために必要なすべてのプロキシ サーバーを使用するように設定されていることを確認します（*ファイアウォールまたはプロキシ サーバーの設定の確認、559 ページ*を参照）。

また、ゲートウェイ、またはファイアウォールに Filtering Service が実行しているコンピュータから HTTP トラフィックをブロックするようなルールが含まれていないことを確認します。

ファイアウォールまたはプロキシ サーバーの設定の確認

Web Security Help | Web Security ソリューション | バージョン 7.8.x

マスタ データベースが認証を必要とするファイアウォールまたはプロキシを通じてダウンロードされる場合、プロキシ認証の設定をチェックするために下記の手順を実行します。

1. **[Settings] > [General] > [Database Download]** を順に選択します。
2. **[Use proxy server or firewall（プロキシ サーバーまたはファイアウォールを使用する）]** が選択されていること、正しいサーバーおよびポートがリストされていることを確認します。

3. **[Authentication（認証）]** の設定が正しいことを確認します。ユーザー名およびパスワードを確認します。スペルや大文字 / 小文字に注意してください。

   Websense ソフトウェアが認証情報を提供しなければならない場合、ファイアウォールまたはプロキシ サーバーはクリア テキストまたは基本認証を受け入れるように設定されていなければなりません。基本認証の有効化に関する詳細は、support.websense.com から入手できます。

Websense ソフトウェアが正常にソフトウェアをダウンロードするときにファイアウォールによってインターネット アクセスが制限される場合、または HTTP を通じて転送できるファイルのサイズが制限される場合、Websense ソフトウェアはデータベースをダウンロードできません。ファイアウォールがダウンロードの失敗の原因であるかどうかを調べるには、ダウンロードをブロックしている可能性があるファイアウォール規則を探し、必要なら Web Security manager でダウンロードの時刻を変更します（*データベースのダウンロードの設定、34 ページ*を参照）。

Filtering Service が Websense アプライアンス上で実行していない場合、Filtering Service プロキシ設定をコンピュータ上のブラウザ プロキシ設定と照合します。最初に Filtering Service サービスを実行しているコンピュータ上のブラウザがウェブ ページを適切にダウンロードできることを確認します。ページが正常に開くにもかかわらずマスタ データベースがダウンロードされない場合は、ブラウザのプロキシ サーバーの設定を調べてください。

- Microsoft Internet Explorer の場合は下記の手順を実行します。
  1. **[Menu（メニュー）]** バーを表示し、次に **[Tools（ツール）] > [Internet Options（インターネット オプション）]** を順に選択し、**[Connections（接続）]** タブを選択します。
  2. **[LAN Settings（LAN の設定）]** をクリックし、**[Proxy server（プロキシ サーバー）]** の下に表示される設定値をメモしておきます。
- Mozilla Firefox の場合は、下記の手順を実行します。
  1. **[Tools] > [Options（オプション）] >** を順に選択し、**[Advanced（詳細）]** タブを選択します。
  2. **[Network（ネットワーク）]** タブ（デフォルトでは通常選択済み）で、**[Settings（設定）]** をクリックします。

     [Connection Settings（接続の設定）] ダイアログボックスに、ブラウザがプロキシ サーバーに接続するように設定されているかどうかが示されます。プロキシの設定をメモしておきます。

Filtering Service をインストールしているコンピュータのディスク ス ペースが不足している

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Filtering Service は、圧縮されたマスタ データベースの更新を Websense **bin** ディレクトリ（デフォルトでは C:\Program Files、*または* Program Files（x86）\Websense\Web Security\bin、もしくは /opt/Websense/bin/）にダウンロードするために、適切なスーペースが必要です。また、データベースを展開およびロードするためにもスペースが必要です。一般的な目安として、Websense, Inc., では、ダウンロード先のドライブに 4 GB 以上の空きディスク スペースを確保しておくことを推奨します。

ディスク スペースの警告は、Filtering Service をインストールしているコンピュータのディスク スペースが 4 GB を割り込んでいることを示しています。

Windows システムでは、ディスク スペースを確認するために Windows Explorer を使用して下記の手順を実行します。

1. Windows Explorer（Internet Explorer ではありません）で **[My Computer（マイコンピュータ）]** を選択します。
2. Websense ソフトウェアがインストールされているドライブを選択します。デフォルトでは、Websense ソフトウェアは C ドライブに置かれています。
3. ドライブを右クリックし、**[Properties（プロパティ）]** を選択します。
4. [General（一般）] タブで、空きスペースが 4 GB 以上あることを確認します。ドライブ上の空きスペースが足りない場合は、不必要なファイルを削除して、必要なスペースを解放してください。

Linux システムでは、**df** コマンドを使用して、Websense ソフトウェアがインストールされているファイル システムの空きスペースの量を確認します。

1. ターミナル セッションを開きます。
2. プロンプトで、下記のように入力します。

   ```
   df -h /opt
   ```

   Websense ソフトウェアは通常、/opt/Websense/bin ディレクトリにインストールされます。別の場所にインストールされている場合は、そのパスを指定します。
3. 4 GB 以上の空きディスク スペースがあることを確認します。ドライブ上の空きスペースが足りない場合は、不必要なファイルを削除して、必要なスペースを解放してください。

ディスク スペースの問題に対処した後、マスタ データベースをダウンロードできない場合は、下記の手順を実行します。

1. Filtering Service をインストールしているコンピュータ上のすべての Websense サービスを停止します（*Websense サービスの停止と起動、477 ページ*を参照）。
2. Websense **bin** ディレクトリから **Websense.xfr** および **Websense**（拡張子なし）ファイルを削除します。
3. Websense サービスを再起動します。
4. 手動でデータベースのダウンロードを開始します（Web Security manager の **[Status] > [Dashboard]** ページを順に選択し、**[Database Download]** をクリックします）。

Filtering Service をインストールしているコンピュータのメモリーが不足している

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense ソフトウェアを実行し、マスタ データベースをダウンロードし、マスタ データベースの更新を適用するために必要なメモリは、ネットワークのサイズによって異なります。

- 小規模なネットワークでは、少なくとも 2 GB のメモリを推奨します（Windows および Linux）。
- システムの推奨事項については、Deployment and Installation Center を参照してください。

Filtering Service をインストールしているコンピュータで空きメモリが 512 MB 未満に低下したとき、ヘルス アラート メッセージが生成されます。この計算にはバッファおよびキャッシュ スペースが含まれていません。

コンピュータが Deployment and Installation Center の要件に一致するかまたは上回り、Filtering Service がマスタ データベースをロードできる場合は、低メモリの条件は問題を起こす可能性が低いです。

しかし、Filtering Service がマスタ データベースをロードできない場合は、コンピュータ上でメモリを解放するか、または追加の RAM を追加する必要があります。

Windows システムのメモリをチェックするには、下記の手順を実行します。

1. [Task Manager（タスク マネージャ）] を開きます。
2. **[Performance（パフォーマンス）]** タブを選択します。
3. 利用可能な **[Physical Memory（物理メモリ）]** の合計を確認します。

また Windows Performance モニタ（[Start（スタート）] > [Administrative Tools（管理ツール）] > [Performance（パフォーマンス）]）を使用して、情報を取得します。

Linux システムのメモリをチェックするには、下記の手順を実行します。

1. ターミナル セッションを開きます。
2. プロンプトで、下記のように入力します。

   ```
   top
   ```

3. **Mem: av** と **Swap: av** を加算することによって利用可能なメモリの合計を計算します。

メモリの不足の問題に対処するために、コンピュータの RAM をアップグレードするか、またはメモリ使用量の大きいアプリケーションを他のコンピュータに移動することができます。

制限アプリケーション

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ウィルス スキャナ、サイズ制限アプリケーション、または侵入検出システムなどの制限アプリケーションまたはアプライアンスがデータベースのダウンロードを妨げることがあります。Websense ソフトウェアがそのようなアプリケーションまたはアプライアンスに接続せずに直接に最終的なゲートウェイに接続するように構成できれば理想的です。代わりの方法として、下記の手順を実行します。

1. Filtering Service がインストールされているコンピュータおよびマスタ データベースのダウンロード場所と関係する制限を無効にします。

   デバイスの設定を変更する方法については、アプライアンスまたはソフトウェアのマニュアルを参照してください。
2. マスタ データベースをダウンロードします。

この変更によっても問題が解決しない場合は、Filtering Service を実行しているコンピュータを含めるようにアプリケーションまたはアプライアンスの構成を変更します。

設定した時間にマスタ データベースのダウンロードが行われない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Filtering Service がインストールされているコンピュータ上でシステム日付および時刻が正しく設定されていない可能性があります。Filtering Service はシステム クロックを使用してマスタ データベースをダウンロードする適当な時刻を判断します。

ダウンロードがまったくできない場合は、*マスタ データベースがダウンロードしない、557 ページ*を参照してください。

データベース ダウンロードの問題に関するテクニカル サポートへのお問い合わせ

Web Security Help | Web Security ソリューション | バージョン 7.8.x

このヘルプ セクションで示しているトラブルシューティングの手順を実行してもまだマスタ データベースのダウンロードの問題が解決しない場合は、Websense テクニカル サポートに下記の情報を送信してください。

1. [Database Download] ダイアログ ボックスに表示されるエラー メッセージ（正確に）
2. データベースをダウンロードしようとしたコンピュータの外部 IP アドレス
3. Websense サブスクリプション キー
4. 最後にダウンロードを試みた日付と時刻
5. 転送されたバイト数（もしあれば）
6. コマンド プロンプトを開き、**download.websense.com** に対して **nslookup** を実行します。ダウンロード サーバーに接続した場合は、返送された IP アドレスをテクニカル サポートに送信してください。
7. コマンド プロンプトを開き、**download.websense.com** に対して **tracert** を実行します。ダウンロード サーバーに接続した場合は、ルート トレースをテクニカル サポートに送信してください。
8. ダウンロードの試行中に Filtering Service を実行しているコンピュータ上で実行されたパケット トレースまたはパケット キャプチャ。
9. 同じダウンロードの試行中にネットワーク ゲートウェイ上で実行されたパケット トレースまたはパケット キャプチャ。
10. Websense **bin** ディレクトリ（デフォルトでは C:\Program Files、*または* Program Files（x86）\Websense\Web Security\bin、もしくは /opt/Websense/bin/）からの下記のファイル。**websense.ini**、**eimserver.ini**、および **config.xml**。

テクニカル サポートの連絡先については、support.websense.com/ を参照してください。

ポリシー実施の問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

- *Filtering Service が実行していない、565 ページ*
- *User Service を使用できない、566 ページ*
- *サイトが間違って [Information Technology（情報技術）] に分類されている、567 ページ*

- *キーワードがブロックされない、568 ページ*
- *カスタムまたは制限付きアクセス フィルタ URL が指定どおりに処理されない、568 ページ*
- *Websense ソフトウェアがユーザーまたはグループ ポリシーを適用しない、569 ページ*
- *リモート ユーザーが正しいポリシーを受け取らない、569 ページ*

Filtering Service が実行していない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Filtering Service が実行していない場合、ポリシー実施およびログ記録を行うことができません。

下記の場合に Filtering Service が停止することがあります。

- Filtering Service をインストールしているコンピュータのディスク スペースが不足している（*Filtering Service をインストールしているコンピュータのディスク スペースが不足している、561 ページ*を参照）。
- マスタ データベースのダウンロードが、ディスク スペースの不足のために失敗した（*マスタ データベースがダウンロードしない、557 ページ*を参照）。
- **websense.ini** ファイルが不明または壊れている
- サービスを停止して（たとえば、カスタム ブロック ページを作成した後）、再開していない。

また、複数の Websense サービスを再開し、それが正しい順序で開始されなかった場合に、Filtering Service が停止したように見える場合があります。複数のサービスを再開する場合は、先に Policy Database、Policy Broker、Policy Server を開始してから他の Websense サービスを開始してください。

これらの問題のトラブルシューティングを行うには、下記の手順を実行します。

- Filtering Service がインストールされているコンピュータに 3GB 以上の空きディスク スペースがあることを確認します。必要な場合、不要なファイルを削除して、空きスペースを増やします。
- Websense **bin** ディレクトリ（デフォルトでは C:\Program Files または Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）に移動し、テキスト エディタで **eimserver.ini** ファイルを開くことができるか確認します。このファイルが壊れている場合は、バックアップ ファイルに置き換えます。
- Windows イベント ビューワまたは **websense.log** ファイルで Filtering Service からのエラー メッセージをチェックします（*トラブルシューティングのヒントとツール、650 ページ*を参照）。

- TRITON コンソールからログオフし、Policy Server を再開し、次に Websense Filtering Service を再開します（*Websense サービスの停止と起動、477 ページ*を参照）。

  1 分間待ってから、再び TRITON コンソールにログオンします。

User Service を使用できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ユーザー ベースのポリシーが適切に適用されるためには、User Service が実行している必要があり、また Policy Server が User Service と通信できる必要があります。

他の Websense サービスを再開した後で Policy Server を再開した場合、User Service が停止したように見える場合があります。この問題を解決するには、下記の手順を実行します。

1. TRITON コンソールを閉じます。
2. Websense Policy Server サービスを再開します（*Websense サービスの停止と起動、477 ページ*を参照）。
3. Websense User Service を開始、または再開します。
4. 1 分間待ってから、再び TRITON コンソールにログオンします。

まだ問題が解決しない場合は、下記の手順を実行します。

- Windows イベント ビューワまたは **websense.log** ファイルで User Service からのエラー メッセージをチェックします（*トラブルシューティングのヒントとツール、650 ページ*を参照）。
- Websense **bin** ディレクトリ（デフォルトでは C:\Program Files または Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）に移動し、テキスト エディタで **eimserver.ini** ファイルを開くことができるか確認します。このファイルが壊れている場合は、バックアップ ファイルに置き換えます。

Filtering Service をインストールしているコンピュータで CPU 使用率が高い

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Filtering Service をインストールしているコンピュータの CPU が過負荷状態になっている場合（Filtering Service が実行している処理によってか、他のソフトウェアからの要求によってかに関わりなく）、サイトへのアクセス要求の処理に時間がかかり、サイトの参照が遅くなることがあります。

CPU 使用率のピーク時（95% を超える）には、Filtering Service が要求をまったく処理できず、ポリシーの適用に異常をきたすことがあります。

この問題を対処するために、Task Manager（Windows）または **top** コマンド（Linux）を使用して、コンピュータ上のどの処理が CPU 使用率をピークにさせているかを判断します。

- 他のコンピュータから実行できるアプリケーションはありますか。
- Filtering Service を専用コンピュータに移動できますか。

Filtering Service が大幅な処理時間を使用している場合、下記の処置を実行します。

- Filtering Service によって処理されるトラフィックの量を評価します。DNS 検索はかなりの処理時間を必要とすることがあります。ロード バランシングのために追加の Filtering Service インスタンスをインストールすることができます。
- キーワードおよび正規表現の使用を評価します。多数の表現やキーワードを使っていませんか、また非常に複雑な正規表現を使っていませんか。

  キーワードおよび正規表現の数を減らすか、または複雑な正規表現を削除するか簡略化すると、Filtering Service のパフォーマンスを向上させることができます。

サイトが間違って [Information Technology（情報技術）] に分類されている

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Internet Explorer バージョン 4.0 以上では、[Address（アドレス）] バーからの検索を受け付けます。このオプションが有効にされていて、ユーザが [Address] バーにドメイン名だけを入力した場合（たとえば、**http://www.websense.com** の代わりに **websense**）、Internet Explorer はこのエントリをサイト要求ではなく検索要求とみなします。検索対象である可能性がもっとも大きいサイトと、検索条件に近いサイトのリストが表示されます。

その結果、Filtering Service は、要求されたサイトのカテゴリーとは関係なく、アクティブなポリシーでの [Information Technology/Search Engines and Portals（情報技術 / 検索エンジンおよびポータル）] カテゴリのステータスを基に要求を許可、ブロック、または制限します。正しいポリシーが実施されるように、[Address] バーからの検索機能をオフにします。

1. **[Tools（ツール）] > [Internet Options（インターネット オプション）]** を順に選択します。
2. **[Advanced（詳細）]** タブを開きます。
3. **[Search from the Address bar（アドレス バーからの検索）]** で、**[Do not submit unknown addresses to your auto-search provider（未知のアドレスを自動検索プロバイダーに送信しない）]** を選択します。
4. **[OK]** をクリックします。

キーワードがブロックされない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

この問題の原因として下記の 2 つのことが考えられます：**[Disable keyword blocking（キーワード ブロックの無効化）]** が選択されているか、URL にキーワードが含まれているサイトが **post** を使ってデータをユーザーのウェブ サーバーに送信したことです。

キーワードのブロックが有効になっていることを確認するには、下記の手順を実行します。

1. **[Settings] > [General] > [Filtering（フィルタリング）]** を順に選択します。
2. [Filtering（一般的なフィルタリング）] の下の **[Keyword search options（キーワード検索のオプション）]** リストをチェックします。**[Disable keyword blocking]** が表示されている場合、リストから別のオプションを選択します。使用可能なオプションの詳細については、*フィルタリング設定値の設定*、81 ページを参照してください。
3. **[OK]** をクリックして変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

サイトがウェブ サーバーにデータを送信するために **post** を使用している場合は、Filtering Service はその URL に対するキーワード設定を実施しません。ご使用の統合製品が post を通じて送信されたデータを認識しない限り、ユーザーはブロックされているキーワードを含む URL にアクセスできます。

URL が post コマンドを使用するかどうかを調べるには、ブラウザで URL のソースを表示します。ソース コードに [<method=post>] のような文字列が含まれる場合は、その URL をロードするために post が使用されています。

カスタムまたは制限付きアクセス フィルタ URL が指定どおりに処理されない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

制限付きアクセス フィルタまたはカスタム UR L リスト（再分類またはフィルタリングされていない）の中の HTTPS URL が指定どおりにブロックまたは許可されない場合は、統合製品がその URL を Filtering Service によって認識できない形式に変換している可能性があります。

非プロキシ統合製品はドメイン形式の URL を IP 形式に変換します。たとえば、URL **https://<domain.com>** は、**https://<IP_address> :443** と読み取られます。この場合に、Filtering Service は統合製品から受信した URL とカスタム URL または制限付きアクセス フィルタとを照合できず、サイトを正しく処理しません。

この問題を回避するには、カスタム URL として指定するまたは制限付きアクセス フィルタで使用するサイトの IP アドレスと URL の両方を追加します。

Websense ソフトウェアがユーザーまたはグループ ポリシーを適用しない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ユーザー要求が種々の理由により割り当てたユーザーまたはグループ ポリシーによって処理されないことがあります。下記のトピックをチェックし、また詳細については、Knowledge Base で検索してください。

- *User Service を使用できない*、566 ページ
- *リモート ユーザーが正しいポリシーを受け取らない*、569 ページ
- *ディレクトリ サービスの接続と設定*、581 ページ
- *ディレクトリ サービスの設定*、582 ページ
- *ユーザー識別と Windows Server*、582 ページ
- *Websense アプライアンスまたは Linux サーバーに配備された User Service*、585 ページ
- *リモート ユーザーが正しくフィルタリングされない*、587 ページ

リモート ユーザーが正しいポリシーを受け取らない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

リモート ユーザーがキャッシュされたドメイン資格情報（ネットワーク ログオン情報）を使用してログオンすることによってネットワークにアクセスした場合は、Filtering Service はそのユーザー、そのユーザのグループ、またはドメインに割り当てられているポリシーを割り当てます。ユーザー、グループ、またはドメインにポリシーが割り当てられていない場合、またはユーザーがローカル ユーザー アカウントを使ってコンピュータにログオンした場合は、デフォルト ポリシーが適用されます。

ユーザーがユーザー ポリシー、グループ ポリシー、またはデフォルト ポリシーを受け取らない場合があります。これは、ユーザーがローカル ユーザー アカウントを使ってリモート コンピュータにログオンした場合や、リモート コンピュータの Media Access Control（MAC）アドレスの末尾の部分がポリシーが割り当てられているネットワーク内の IP アドレスと重なる場合に起こります。そのような場合、その IP アドレスに割り当てられているポリシーが、リモート ユーザに対して適用されます。

Network Agent の問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Network Agent がインストールされていない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Network Agent は HTTP、HTTPS、および FTP 以外のインターネットプロトコルのポリシーの実施を可能にするために必要とされます。また、一部の統合環境では、Network Agent を使用することによって、より正確なログ記録を行うことができます。

統合製品と共に実行していて、Network Agent によるプロトコル管理またはログ記録を必要としない場合は、[No Network Agent is installed（Network Agent がインストールされていません）] というステータス メッセージを非表示にすることができます。手順については、*現在のシステム ステータスの確認*、490 ページを参照してください。

スタンドアロン型インストールの場合は、ネットワーク モニタリングおよびポリシーの実施を行うために Network Agent がインストールされている必要があります。Deployment and Installation Center および *Network Agent の設定*、542 ページを参照してください。

Network Agent が実行していない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Network Agent では、HTTP、HTTPS、および FTP 以外のプロトコルの完全処理を有効化する必要があります。また、一部の統合環境では、Network Agent を使用することによって、より正確なログ記録を行うことができます。

スタンドアロン型インストールの場合は、ネットワーク トラフィックをモニタおよび管理するために Network Agent が実行している必要があります。

この問題のトラブルシューティングを行うには、下記の事柄を確認します。

1. Network Agent を実行しているコンピュータ上での低メモリの問題がサービスまたはデーモンの開始を妨げている可能性を調べます。
2. 下記の該当するいずれかの手順に従い Network Agent サービスまたはデーモンのステータスをチェックします。

- Windows の場合：Windows Services ツールを使用して **Websense Network Agent** サービスが開始しているかどうかを確認します。
- Linux の場合：**/opt/Websense/WebsenseDaemonControl** コマンドを使用して、**Network Agent** のステータスをチェックします。
- Appliance の場合：Appliance Manager を使用して **Network Agent** モジュールのステータスをチェックします。

3. すべての管理者が TRITON コンソールからログ オフしていることを確認し、**Websense Policy Broker** サービスと **Websense Policy Server** サービスを再開します（*Websense サービスの停止と起動*、477 ページを参照）。
4. **Websense Network Agent** サービスを開始、または再開します。
5. 1 分間待ってから、再び TRITON コンソールにログオンします。

それでも問題が解決しない場合は、下記の手順を実行します。

- **Windows イベント ビューワ**で Network Agent からのエラー メッセージをチェックします（*Windows イベント ビューア*、651 ページを参照）。
- **Websense.log** ファイルで Network Agent からのエラー メッセージをチェックします（*Websense ログ ファイル*、652 ページを参照）。

Network Agent が NIC をモニタしていない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ネットワークのトラフィックをモニタするために、Network Agent を 1 つ以上のネットワーク インターフェース カード（NIC）に関連付ける必要があります。

Network Agent コンピュータにネットワーク カードを追加または削除した場合は、Network Agent の設定を更新しなければなりません。

1. Web Security manager で、**[Settings]** を選択します。
2. 左側のナビゲーションペインの [Network Agent] の下で、Network Agent をインストールしているコンピュータの IP アドレスを選択します。
3. 選択したコンピュータのすべての NIC がリストされていることを確認します。
4. 1 つ以上の NIC がネットワーク トラフィックをモニタするように設定されていることを確認します。

詳細は、*Network Agent の設定*、542 ページを参照してください。

Network Agent が Filtering Service と通信できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

インターネット使用状況ポリシーを強制するために、Network Agent は Filtering Service と通信できなければなりません。

- Filtering Service がインストールされているコンピュータの IP アドレスを変更するか、Filtering Service を再インストールしましたか。

  そうである場合は、*Filtering Service の IP アドレスまたは UID 情報を更新する、572 ページ*を参照してください。
- Network Agent がインストールされているコンピュータ上に、2 つ以上のネットワーク インターフェイス カード (NIC) がありますか？

  そうである場合は、*ネットワークの構成、541 ページ*を参照して Websense ソフトウェアの設定を確認してください。
- Network Agent に接続しているスイッチを再構成しましたか

  再構成した場合は、ハードウェアのセットアップを確認するには Network Agent Quick Start を参照してください。また Websense の設定を確認するには、*Network Agent の設定、542 ページ*を参照してください。

どれも適用しない場合は、関連する Network Agent および Filtering Service の詳細については、*ローカル設定、544 ページ*を参照してください。

Filtering Service の IP アドレスまたは UID 情報を更新する

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Filtering Service をアンインストールしてから再インストールしたとき、Network Agent は自動的には Filtering Service の内部識別子（UID）を更新しません。Web Security manager は、古い UID（すでに存在しない）を使用して Filtering Service のクエリーを試みます。

同様に、Filtering Service がインストールされているコンピュータの IP アドレスを変更したとき、この変更は自動的には登録されません。

Filtering Service への接続を再確立するには、下記の手順を実行します。

1. RITON コンソールにログ オンし、Web Security manager を開きます。

   ステータス アラートは、Network Agent のインスタンスが Filtering Service に接続できないことを知らせます。
2. 左側のナビゲーションペインの上部の **[Settings]** をクリックします。
3. 左側のナビゲーションペインの [Network Agent] の下で、Network Agent をインストールしているコンピュータの IP アドレスを選択します。

4. ページ上部の [Filtering Service Definition（Filtering Service の定義）] の下の **[Server IP address（サーバーの IP アドレス）]** リストを展開し、次に Filtering Service をインストールしているコンピュータの IP アドレスを選択します。
5. ページ下部の **[OK]** をクリックして更新をキャッシュします。**[Save and Deploy]** をクリックするまで、変更は適用されません。

Network Agent をインストールしているコンピュータのメモリが不足している

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Network Agent は、起動時に必要な動作メモリを割り当てます。Network Agent をインストールしているコンピュータに厳格なメモリの制限がある場合は、Network Agent は下記のいずれかの状態になります。

- 起動できない [きどうできない]
- トラフィックをモニタできなくなる

どちらの場合でも、Network Agent からの情報に基づくポリシーの実施およびログ記録は行われません。そのため、ユーザーは通常はブロックされるサイトまたはアプライアンスへのアクセスが許可されることがあります。

Task Manager（Windows）または **top** コマンド（Linux）を使用して Network Agent をインストールしているコンピュータのメモリ使用率を評価してください。問題を解決するために、下記の処置を実行できます。

- コンピュータの RAM をアップグレードする。
- 高いメモリ要件をもつアプリケーションまたはコンポーネントを他のコンピュータに移動する。
- 必要なメモリーを減らすために Network Agent の設定を簡単にする。

Network Agent をインストールしているコンピュータで CPU 使用率が高い

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Network Agent をインストールしているコンピュータの CPU がそのコンピュータで実行している他のソフトウェアからの要求によって過負荷状態になった場合、Network Agent はトラフィックを検出できずログ記録できない場合があります。スタンドアロン型環境では、それによって、通常はブロックされるウェブサイトおよびインターネット アプリケーションへのすべてのユーザー要求が許可されることがあります。

この問題を対処するために、Task Manager（Windows）または **top** コマンド（Linux）を使用して、コンピュータ上のどの処理が CPU 使用率をピークにさせているかを判断します。

- 他のコンピュータから実行できるアプリケーションはありますか。
- Network Agent を専用コンピュータに移動できますか。

ユーザー設定およびユーザー識別の問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

- *ユーザーベースおよびグループベースのポリシーが適用されない*、574 ページ
- *異常に長いディレクトリ サーバー接続の遅延*、576 ページ
- *Filtering Service が透過的識別エージェントと通信できない*、576 ページ
- *DC Agent の許可が不十分*、577 ページ
- *DC Agent が必要なファイルにアクセスできない*、578 ページ
- *ユーザーおよびグループを Web Security manager に追加できない*、580 ページ
- *Websense アプライアンスまたは Linux サーバーに配備された User Service*、585 ページ

ユーザーベースおよびグループベースのポリシーが適用されない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ユーザーベースまたはグループベースのポリシーを割り当てた後でも Filtering Service がインターネット要求のフィルタリングにコンピュータ、ネットワーク ポリシー、または**デフォルト ポリシー**を適用する場合には、下記の手順を実行して問題の原因を調べます。

- Windows Active Directory でネストされたグループを使用している場合、親グループに割り当てられているポリシーは親グループの直接に適用されるのではなく、サブグループに所属するユーザーに適用されます。ユーザーおよびグループの階層の詳細については、ディレクトリ サービスのマニュアルを参照してください。
- User Service キャッシュが古くなっている可能性があります。User Service はユーザー名の IP アドレスへのマッピングを 3 時間の間キャッシュします。キャッシュをクリアして再作成するには、Web Security manager で [Settings] > [General] > [Directory Services（ディレクトリ サービス）] ページの [User Service Cache（User Service Cache ）] セクションを選択し、**[Clear Cache（キャッシュをクリア）]** をクリックします。

- User Service が Guest アカウントを使用するサービスとしてインストールされている可能性があります。これはドメイン コントローラから見れば匿名ユーザーと同じです。ドメイン コントローラが匿名ユーザーにユーザおよびグループのリストを提供しないように設定されている場合は、User Service はリストをダウンロードすることを許可されません。*DC Agent、Logon Agent、および User Service の許可の変更、584 ページ*を参照してください。
- User Service が Websense アプライアンスまたは Linux サーバーに配備されている場合、ユーザーを識別するために DC Agent（任意のモードの Active Directory と共に）または Logon Agent（ネーティブ モードの Active Directory と共に）を使用しているとき、WINS サーバーの設定を確認します。*Websense アプライアンスまたは Linux サーバーに配備された User Service、585 ページ*を参照してください。
- Windows XP SP2 を実行しているコンピュータ上のユーザーが不適切なポリシーを受け取った場合、Windows Internet Connection Firewall（ICF）が原因である可能性があります。ICF は Windows XP SP2 に含まれ、デフォルトでは有効化されています。Windows ICF の詳細については、Microsoft Knowledge Base Article #320855 を参照してください。

  DC Agent または Logon Agent が Windows XP SP2 を実行しているコンピュータからユーザー ログオン情報を取得できるようにするには、下記の手順を実行します。

  1. クライアント コンピュータで **[Start（スタート）] > [Settings（設定）] > [Control Panel（コントロール パネル）] > [Security Center（セキュリティ センター）] > [Windows Firewall（Windows ファイアウォール）]** を順に選択します。
  2. **[Exceptions（例外）]** タブを選択します。
  3. **[File and Printer Sharing（ファイルとプリンタの共有）]** をオンにします。
  4. **[OK]** をクリックして [ICF] ダイアログ ボックスを閉じ、他の開いているウィンドウを閉じます。

上記の手順のどれもが問題に対処しない場合は、下記のトピックをチェックするか、または詳細について support.websense.com を検索してください。

- *ディレクトリ サービスの接続と設定、581 ページ*
- *ディレクトリ サービスの設定、582 ページ*
- *ユーザー識別と Windows Server、582 ページ*

異常に長いディレクトリ サーバー接続の遅延

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense User Service は、以下の処理のためにネットワーク内のユーザー ディレクトリと通信します。

- [Clients] ページおよび他の Web Security manager のページにユーザー、グループ、および OU 情報を入力する。
- Websense Filtering Service が正しいポリシーを実施できるように、ユーザーのグループ情報を検索する。
- ポリシーの適用、レポート、およびアラートの一貫性を確保するために、ユーザーおよびグループ情報を他の Websense コンポーネントに提供する。
- ブラウザ ベースのログオン プロンプトを通じて手動認証を提供する。

User Service でのディレクトリのクエリーで異常に長い接続遅延が起こった時、ユーザーには下記のことが起こります。

- ブラウズが遅くなる
- 適切なユーザーまたはグループ ポリシーではなく、IP アドレス ベースのポリシーまたはデフォルト ポリシーを受け取る

管理者が Web Security manager のクライアントにアクセスしようとした時、遅延が起こる場合があります。

この問題を解決するためには、以下のことを調べます。

- ヘルス アラート メッセージで通知された User Service コンピュータと各ディレクトリ サーバー コンピュータの間のネットワークの問題
- ディレクトリの接続または検索の速度を低下させる可能性があるドメイン コントローラ関連の問題

Filtering Service が透過的識別エージェントと通信できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

透過的ユーザー識別のために、DC Agent、Logon Agent、eDirectory Agent、または RADIUS Agent 使用する場合は、ユーザーベースのポリシーを正しく適用するために Filtering Service がエージェントと通信できるうにしなければなりません。この通信ができない場合は、ユーザーは IP アドレスベースのポリシーまたはデフォルト ポリシーによってフィルタリングされます。

この問題に対処するために、下記の手順を実行します。

1. エージェント サービスまたはデーモンが実行していることを確認します。
   - **Windows** の場合：Windows の [Services] ツールを使用して、Websense DC Agent、Websense Logon Agent、Websense eDirectory Agent、または Websense RADIUS Agent が実行していることを確認します。

- **Linux** の場合：**/opt/Websense/** ディレクトリに移動し、下記のコマンドを使用して Logon Agent、eDirectory Agent、または RADIUS Agent が実行していることを確認します。

  ```
  ./WebsenseAdmin -status
  ```

2. Filtering Service をインストールしているコンピュータから透過的識別エージェントをインストールしているコンピュータを **ping** できます。透過的識別エージェントをインストールしているコンピュータの IP アドレスとホスト名の両方を ping し、DNS が適切に設定されていることを確認します。例：

   ```
   ping 10.55.127.22
   ping transid-host
   ```

3. 透過的識別エージェント通信ポートが Filtering Service コンピュータとエージェント コンピュータの間の接続を確立します。デフォルト ポートは、下記の通りです。
   - DC Agent：30600
   - Logon Agent：30602
   - eDirectory Agent：30700
   - RADIUS Agent：30800
4. Web Security manager の **[Settings] > [General] > [User Identification（ユーザー識別）]** ページに正しいエージェントの IP アドレスまたはホスト名、およびポートが表示されます。

実行されるサービスが正常に表示され、Filtering Service をインストールしているコンピュータとエージェントをインストールしているコンピュータの間でネットワーク通信問題が示されない場合は、下記の処置を行います。

- Windows の [Services] ツールまたは /opt/Websense/WebsenseDaemonControl コマンドを使用して、エージェントを再起動します。
- エージェントがインストールされているコンピュータの Windows イベント ビューア（*Windows イベント ビューア*、651 ページを参照）、または **websense.log** ファイル（*Websense ログ ファイル*、652 ページを参照）で透過的識別エージェントからのエラー メッセージがないかチェックします。

DC Agent の許可が不十分

Web Security Help | Web Security ソリューション | バージョン 7.8.x

DC Agent が Guest アカウントを使用するサービスとしてインストールされている可能性があります。これはドメイン コントローラから見れば匿名ユーザと同じです。

ドメイン検出（DC Agent の場合に dc_config.txt ファイルを作成し保持するために必要です）を実行するため、またはコンピュータ ポーリングを実行するために、Websense DC Agent は、**domain admin** の許可を必要とします。一部の環境（通常は非常に大規模な企業ネットワーク）では、DC Agent は、**enterprise admin** の許可を必要とします。

ドメイン検出およびコンピュータ ポーリングを無効化しており、手動で dc_config.txt ファイルを保持しながらドメイン コントローラ ポーリングを使用しようとしたとき、DC Agent は、ドメイン コントローラへの読み取りアクセス権限をもつユーザーとして実行することがあります。

DC Agent に domain admin の権限を与えるには、下記の手順を実行します。

1. DC Agent をインストールしているコンピュータで、**WsUserID** など解り易い名前のユーザー アカウントを作成します。このアカウントは、DC Agent がディレクトリ サービスからの情報を要求した際に DC Agent のセキュリティ コンテクストを提供するためにのみ存在します。
   - すべてのドメインで新しいアカウント **domain admin** の権限を割り当てます。
   - すべてのドメインのこのアカウントに同じパスワードを割り当てます。
   - パスワードを [never expire（期限なし）] に設定します。

   ユーザー名およびパスワードをメモします。
2. 下記のどちらかの Windows のサービス ツールを開きます。
   - Windows Server 2012：[Server Manager] > [Tools] > [Services]
   - Windows Server 2008 R2：[Start] > [Administrative Tools] > [Services]
3. **Websense DC Agent** サービスにスクロールし、サービス名を右クリックして、[Stop（停止）] を選択します。
4. サービス名を再び右クリックして、**[Properties（プロパティ）]** を選択し、次に **[Log On]** タブをクリックします。
5. **[This account（このアカウント）]** を選択し、DC Agent 用に作成したアカウント名およびパスワードを入力します。一部のドメインでは、アカウント名をドメイン \ ユーザー名の形式で入力する必要があります。
6. **[OK]** をクリックして [Services] ツールに戻ります。
7. サービス名を再び右クリックし、**[Start]** を選択します。
8. [Services] ツールを閉じます。

また User Service に DC Agent と同じ管理権限を割り当てる必要がある場合があります。

DC Agent が必要なファイルにアクセスできない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

DC Agent はネットワーク内のドメイン コントローラを識別し、次にドメイン コントローラに対してユーザー ログオン セッションについての照会を行います。デフォルトでは、エージェントは自動的に既存のドメイン コントローラを確認し、ネットワークに追加された新しいドメインまたはドメイン コントローラを検出します。この情報を DC Agent がインストールされているコンピュータの **Websense bin** ディレクトリにある **dc_config.txt** というファイルに保存します。

下記の場合に、DC Agent がこのファイルにアクセスできないことを示すアラートが発生することがあります。

- DC Agent が読み取り許可または書き込み許可を得ているファイルを開くことができない場合。
  - DC Agent を実行するために使用されているドメイン アカントがそのファイルおよびディレクトリへの読み取り許可と書き込み許可を得ていることを確認します。
  - そのファイルが存在し、書き込み禁止にされていない場合、ファイルが手動で開くことができること、および破損していないことを確認します。
- DC Agent ファイルを作成できないのは、ドメイン コントローラ情報を見つけることができないからです。
  - User Service が Websense アプライアンスまたは Linux コンピュータにインストールされている場合は、必要な WINS セットアップ の手順を実行したことを確認します。詳細については、*Websense アプライアンスまたは Linux サーバーに配備された User Service*、585 ページを参照してください。
  - User Service が Windows Server 2008 コンピュータにインストールされている場合は、サービスが **domain admin** 資格情報を使用して実行していることを確認します。*DC Agent、Logon Agent、および User Service の許可の変更*、584 ページを参照してください。
  - NetBIOS for TCP/IP が有効化されていること、および NetBIOS のポート（137、138、139、および 445）が DC Agent をインストールしているコンピュータとドメイン コントローラの間で開かれていることを確認します。

    User Service が Windows で実行している場合は、NetBIOS のポートが User Service をインストールしているコンピュータとドメインポートの間で開かれていることを確認します。
  - Computer Browser Service が DC Agent、User Service、または Active Directory をホストする Windows 2008 Server コンピュータで実行していることを確認します。*Computer Browser サービスをオンにする*、583 ページを参照してください。
- DC Agent がファイル内で有効なエントリを検出しない
  - ファイル内の 1 つ以上のドメイン コントローラ エントリが有効化にされていることを確認します。すべてのエントリが無効化されている場合、DC Agent は j 事実上機能を停止するように指示されています。
  - ファイル内のすべてのエントリが有効な形式にされていることを確認します。例：

    ```
    [WEST_DOMAIN]
    dcWEST1=on
    dcWEST2=on
    [EAST_DOMAIN]
    dcEAST1=on
    dcEAST2=off
    ```

[DC Agent Domains and Controllers（DC Agent ドメインおよびコントローラ）] ページが空白

Web Security Help | Web Security ソリューション | バージョン 7.8.x

デフォルトでは、DC Agent は自動**ドメイン検出**を実行し、ネットワーク内のドメイン コントローラを識別します。ドメインおよびコントローラの情報は、**dc_config.txt** という名前のファイルに保存されます。dc_config.txt ファイルからの情報は、Web Security manager に収集され、[Settings] > [User Identification] > [DC Agent Domains and Controllers] ページに表示されます。

このページは、下記の場合にエラー テキストのみ表示することがあります。

- DC Agent が最近インストールされ、ドメイン検索がまだ進行中である場合。
- ネットワーク内のすべてのドメイン コントローラのポーリングをオフにするために、管理者が **dc_config.tx** ファイルを変更した場合。
- 何かによって DC Agent がドメイン検出を実行できないようにしている場合。

下記のことを確認してください。

- ネットワーク内の各 DC Agent について DC Agent ドメイン検出が **[Settings] > [User Identification] > [DC Agent]** ページで有効にされていること。
- DC Agent がドメイン検出プロセスを完了するために十分な時間が確保されていたこと。
- [Status（ステータス）] > [Alerts（アラート）]ページに DC Agent アラートが表示されていなこと。

DC Agent アラートが表示れている場合は、*DC Agent の許可が不十分、577 ページ*および *DC Agent が必要なファイルにアクセスできない、578 ページ*を参照してください。これらの項目は、DC Agent がドメイン検出プロセスを完了し、dc_config.txt ファイルを作成するために必要な許可およびネットワーク アクセス得るようにするための手順を示しています。

ユーザーおよびグループを Web Security manager に追加できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

いくつかの問題によって、Web Security manager にクライアントを追加しようとした時、ユーザーおよびグループのリストを表示できない場合があります。下記のトピックをチェックし、また詳細については、Knowledge Base で検索してください。

- *ディレクトリ サービスの接続と設定、581 ページ*
- *ディレクトリ サービスの設定、582 ページ*
- *ユーザー識別と Windows Server、582 ページ*

ディレクトリ サービスの接続と設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense User Service をインストールしているコンピュータとディレクトリ サーバーが実行していること、およびネットワーク上で通信できることを確認してください。ディレクトリ サービス通信に使用するデフォルト ポートは、下記の通りです。

139	NetBIOS 通信：Active Directory
389	LDAP 通信：Active Directory、Novell eDirectory、Oracle（旧 Sun Java）Directory Server
636	SSL ポート：Novell eDirectory、Oracle（旧 Sun Java）Directory Server
3268	Active Directory
3269	SSL ポート：Active Directory

さらに、下記の事柄について検討してください。

- Windows Active Directory を**混在**モードで使用しており、User Service が Windows Server コンピュータ上で実行している場合、User Service を実行するために使用するアカウントには、ディレクトリに対する管理権限が必要とされる場合があります。

  User Service アカウントを確認または変更するには、*DC Agent、Logon Agent、および User Service の許可の変更、584 ページ*を参照してください。

- Active Directory を**ネイティブ モード**で実行している場合は、User Service をローカル システム アカウントとして実行するように設定します。実際のサービスにはアカウントは割り当てられません。

  User Service は、Web Security manager の [Settings] > [General] > [Directory Services] > [Add Global Catalog Server（グローバル カタログ サーバーを追加）] ページで設定された管理者のユーザー名およびパスワードを使ってディレクトリと接続します。

- Linux コンピュータで User Service を実行し、Windows ベースのディレクトリ サービスと通信している場合は、WINS をセットアップしており、必要なすべての設定手順の実行を完了していることを確認してください（*Websense アプライアンスまたは Linux サーバーに配備された User Service、585 ページ*を参照）。

- ファイアウォールがポート 55815 上での Web Security manager と User Service との通信をブロックしているかどうか判断します。ブロックしている場合は、ブロックされたポートを開きます。

ディレクトリ サービスの設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Web Security manager でユーザーおよびグループを追加する際に問題が発生した場合、下記の手順を実行して、ディレクトリ サービスに完全で正確な設定を行っていることを確認します。

1. **[Settings] > [General] > [Directory Services]** ページを順に選択します。
2. 組織によって使用されているディレクトリ サービスを選択します。
3. 設定を確認します。詳細については、*ディレクトリ サービス*、93 ページとそのサブトピックを参照してください。

Websense User Service が Linux コンピュータにインストールされており、Active Directory と通信するように設定されている場合は、追加の設定の要件については、*Websense アプライアンスまたは Linux サーバーに配備された User Service*、585 ページを参照してください。

ユーザー識別と Windows Server

Web Security Help | Web Security ソリューション | バージョン 7.8.x

サポートされている Windows Server バージョン に下記のいずれか 1 つ以上のコンポーネントをインストールする場合に、Web Security manager でユーザーおよびグループを追加する際に問題が発生することがあります。

- Websense User Service
- Windows Active Directory

ネットワークが Active Directory を混在モードで使用している場合、Windows Computer Browser は、User Service がインストールされているコンピュータと Active Directory を実行しているコンピュータでも実行していなければなりません。このサービスは、Windows の以前のバージョンではデフォルトでオンにされていましたが、Windows Server 2008 および 2012 ではデフォルトでは無効化されています。

さらに User Service が Windows Server にインストールされており、Active Directory を混在モードで使用している場合は、User Service が Active Directory からの情報にアクセスするためのドメイン権限を持つように設定する必要があります。

User Service を Linux で実行し、Active Directory を使用している場合は、追加の設定が必要です。*Websense アプライアンスまたは Linux サーバーに配備された User Service*、585 ページを参照してください。

当該のコンピュータで Computer Browser を有効化するには、*Computer Browser サービスをオンにする*、583 ページを参照してください。

User Service がディレクトリ情報へのアクセス権限を持つように設定するには、*DC Agent、Logon Agent、および User Service の許可の変更、584 ページ*を参照してください。

Computer Browser サービスをオンにする

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense セットアップは、Windows Server での下記のコンポーネントのインストール時に Computer Browser をオンにするオプションを提供します。

- Websense User Service
- Websense DC Agent
- Websense Logon Agent

そのサービスを開始しないように選択した場合、またはインストーラが正常でなかった場合、このサービスを手動でオンにする必要があります。

影響を受けたコンポーネントを実行している各コンピュータで下記の手順を実行します。

1. 下記の手順を実行して、Windows Network File Sharing が有効化されていることを確認します。
   - Windows Server 2012：
     a. デスクトップで、マウスを画面の右上端に移動し、次に **[Settings（設定）] > [Control Panel（コントロール パネル）]** を順に選択します。
     b. [Control Panel] で **[Network and Internet（ネットワークとインターネット）]** をクリックし、次に **[Network and Sharing Center（ネットワークと共有センター）]** をクリックします。
     c. 左ナビゲーション ペインで **[Change advanced sharing settings（共有の詳細設定の変更）]** をクリックし、その後 **[Turn on file and printer sharing（ファイルとプリンターの共有を有効にする）]** を選択します。
     d. **[Save Changes（変更の保存）]** をクリックし、保存して終了します。
   - Windows Server 2008 R2：
     a. **[Start（スタート）] > [Network（ネットワーク）]** を順に選択し、**[Network and Sharing Center（ネットワークおよび共有センター）]** をクリックします。
     b. **[Advanced Sharing Settings（共有詳細設定）]** をクリックし、**[Turn on file and print sharing（ファイルおよびプリントの共有をオンにする）]** を選択します。

2. 下記のどちらかの Windows のサービス ツールを開きます。
   - Windows Server 2012：[Server Manager] > [Tools] > [Services]
   - Windows Server 2008 R2：[Start] > [Administrative Tools] > [Services]
3. **[Computer Browser（コンピュータ ブラウザ）]** をダブルクリックし、[Properties（プロパティ）] ダイアログ ボックスを開きます。
4. スタートアップ タイプを **[Manual（手動）]** に選択します。
5. **[Start（開始）]** をクリックします。
6. スタートアップ タイプを **[Automatic（自動）]** に変更します。これによって、コンピュータが再起動するたびにサービスが自動で開始されるようにします。
7. **[OK]** をクリックして変更内容を保存し、[Services] ツールを閉じます。
8. 影響を受けたコンポーネントをホストする Windows Server を実行している各コンピュータでこれらの手順を繰り返します。

DC Agent、Logon Agent、および User Service の許可の変更

Web Security Help | Web Security ソリューション | バージョン 7.8.x

DC Agent、Logon Agent、または User Service は、ディレクトリ サービスへのアクセス許可を得たアカウントとして実行する必要がある場合があります。

1. ドメイン コントローラを実行しているコンピュータで、ユーザー アカウント（例、**Websense**）を作成します。既存のアカウントを使用することもできますが、Websense アカウントを使用すれば、パスワードを無期限に設定できるので便利です。特別の権限は必要ありません。

   パスワードを [never to expire（無期限に有効）] に設定します。このアカウントは、ディレクトリ オブジェクトにアクセスするためのセキュリティ コンテクストを提供するだけです。

   このアカウントのために設定したユーザ名とパスワードは手順 6 と 7 で必要になりますから、メモしておいてください。
2. 影響を受けたコンポーネントを実行しているコンピュータで、**[Start] > [Programs] > [Administrative Tools] > [Services]** を順に選択します。
3. 下記のリストから適切な Websense サービス エントリを選択し、次に **[Stop（停止）]** をクリックします。
   - Websense DC Agent
   - Websense Logon Agent
   - Websense User Service
4. Websense サービス エントリをダブルクリックします。
5. **[Log On（ログオン）]** タブで **[This account（このアカウント）]** オプションを選択します。

6. 手順 1 で作成した Websense アカウントのユーザー名を入力します。例、**DomainName\websense**。
7. このアカウントの Windows パスワードを入力し確認してください。
8. **[OK]** をクリックし、ダイアログ ボックスを閉じます。
9. [Services] ツールで Websense サービス エントリを選択し、**[Start]** をクリックします。
10. ネットワーク内の Websense DC Agent、Logon Agent、および User Service の各インスタンスについてこの手順を繰り返します。

Websense アプライアンスまたは Linux サーバーに配備された User Service

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ネットワーク内の個別のユーザーおよびグループにポリシーを適用することを計画していて、User Service が Websense アプライアンスまたは Linux サーバー上で実行している場合、下記のときに特別の設定が必要になります。

- Active Directory を混在モードで使用する
- Websense Logon Agent を使用してネイティブ モードの Active Directory ディレクトリを通じて透過的にユーザーを識別することを希望する場合
- DC Agent を使用して透過的にユーザを識別することを希望する場合

これらの環境では、ドメイン名をドメイン コントローラ IP アドレスに解決するために、Websense ソフトウェアを Windows Internet Name Server（WINS）と通信するように設定する必要があります。正確な手順は、環境によって異なります。

ネットワークが Windows Active Directory を混在モードで使用している場合、下記の手順を実行します。

1. Web Security manager で、**[Settings] > [General] > [Directory Services]** ページに移動します。
2. **[Windows Active Directory（Mixed Mode）（Windows Active Directory（混在モード））]** を選択します。これは、デフォルトのオプションです。
3. 管理ユーザーの名前とパスワードを入力してください。
4. **[Domain（ドメイン）]** 名を入力します。

   組織が複数のドメインを使用している場合は、ユーザーを認証するすべてのドメインによって信頼されているドメインの名前を入力します。
5. 先に入力したドメイン名をドメイン コントローラ IP アドレスに解決できる Windows Internet Name Server（WINS）の IP アドレスを入力します。
6. **[OK]** をクリックして変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

ネットワークが Active Directory（ネイティブ モード）を使用し、WINS を設定する必要がある場合は、下記の手順を実行します。

1. **[Settings] > [General] > [Directory Services]** ページを順に選択します。
2. 管理資格情報を提供し、下記のように Windows Internet Name Server（WINS）を指定します。
   a. **[Windows Active Directory（Mixed Mode）]** を選択します。これはデフォルトのオプションです。
   b. 管理ユーザーの名前とパスワードを入力してください。
   c. **[Domain（ドメイン）]** 名を入力します。
      組織が複数のドメインを使用している場合は、ユーザーを認証するすべてのドメインによって信頼されているドメインの名前を入力します。
   d. 先に入力したドメイン名をドメイン コントローラ IP アドレスに解決できる Windows Internet Name Server（WINS）の IP アドレスを入力します。
   e. **[OK]** をクリックして、変更をキャッシュします。
   f. **[Save and Deploy]** をクリックし、変更を適用します。
3. [Directory Service] ページで、**[Active Directory（Native Mode）]** を選択します。
4. グローバル カタログ サーバーとディレクトリ サービスの他の設定を設定します。詳細については、*Windows Active Directory（ネイティブ モード）、95 ページ*を参照してください。
5. **[OK]** をクリックして、変更をキャッシュします。**[Save and Deploy]** をクリックするまで変更は適用されません。

リモート ユーザが手動認証の入力を要求されない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

リモート ユーザがインターネット アクセス時に手動で認証するように設定したにもかかわらず、個別のユーザが認証の入力を要求されない場合があります。これは、一部のネットワーク内の IP アドレスが手動認証をバイパスするように設定されている場合に起こります。

リモート ユーザーがネットワークにアクセスするとき、Websense ソフトウェアはコンピュータの Media Access Control（MAC）アドレス の最後の部分を読み取ります。これが手動認証をバイパスするように設定されたネットワーク内の IP アドレスと一致した場合、リモート ユーザーはインターネット アクセス時に手動での認証を要求されません。

この問題の解決方法の 1 つは、ネットワーク内 IP アドレスが手動認証を使用するように再設定することです。もう 1 つの方法は、当該のリモート ユーザーの手動認証の要件を無効にすることです。

リモート ユーザーが正しくフィルタリングされない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

リモート ユーザーが正しいポリシーを受け取っていない場合、RADIUS Agent ログをチェックして、**[Error receiving from server: 10060（サーバーからエラーを受信：10060）]**（Windows の場合）または **[Error receiving from server: 0（サーバーからエラーを受信：0 ）]**（Linux の場合）というメッセージがないか調べます。

これは通常は、RADIUS サーバ - が RADIUS Agent をクライアント（RADIUS 要求のソース）として認識しないために起こります。RADIUS サーバーが適切に構成されていることを確認します（テクニカル ペーパー『Using RADIUS Agent for Transparent User Identification』を参照）。

リモート フィルタリング ソフトウェア（*オフサイト ユーザーの管理*、303 ページを参照）をインストールしている場合は、Remote Filtering Client がネットワーク内の Remote Filtering Server と通信できない場合にはオフサイト ユーザーをフィルタリングできません。

リモート フィルタリング ソフトウェアの設定の手順については、テクニカル ペーパー『Remote Filtering Software』を参照してください。

ブロック メッセージの問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

- *ブロックされたファイル タイプのブロック ページが表示されない*、587 ページ
- *ブロック ページの代わりにブラウザ エラーが表示される*、588 ページ
- *ブロック ページの代わりに空白のホワイト ページが表示される*、589 ページ

ブロックされたファイル タイプのブロック ページが表示されない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ファイル タイプのブロックを使用しているとき、ブロック メッセージがユーザーの画面に表示されない場合があります。たとえば、許可されたサイト上の内部フレーム（iframe））にダウンロード可能なファイルが含まれている場合は、そのフレームに送信されるブロック メッセージは表示されません。これはフレーム サイズが 0 だからです。

これは単に表示の問題です。ユーザーがブロックされたファイルにアクセスしたり、ファイルをダウンロードすることはできません。

ブロック ページの代わりにブラウザ エラーが表示される

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ユーザがブロック ページの代わりにエラー メッセージを受け取った場合、もっとも一般的な原因は次の 2 つです。

- ユーザーのブラウザが外部プロキシを使用するように設定されている。ほとんどのブラウザに、外部プロキシの使用を有効にする設定があります。ブラウザが外部プロキシを使用するように設定されていないことを確認します。
- Filtering Service がインストールされているコンピュータの識別またはそのコンピュータとの通信に問題がある。

ユーザーのブラウザの設定が正しい場合、Filtering Service がインストールされているコンピュータの IP アドレスが **eimserver.ini** ファイルに正しくリストされていることを確認します。

1. **Websense Filtering Service** を停止します（*Websense サービスの停止と起動、477 ページ*を参照）。
2. Websense **bin** ディレクトリ（デフォルトでは C:\Program Files、*または* Program Files（x86）\Websense\Web Security\bin、もしくは /opt/Websense/bin/）に移動します。
3. **eimserver.ini** ファイルをテキスト エディタで開きます。
4. **[WebsenseServer]** の下に空白の行を追加し、下記のように入力します。

   ```
   BlockMsgServerName = <Filtering Service IP address>
   ```

   たとえば、Filtering Service の IP アドレスが 10.201.72.15 である場合、下記のように入力します。

   ```
   BlockMsgServerName = 10.201.72.15
   ```

5. ファイルを保存し、閉じます。
6. Filtering Service を再起動します。

Filtering Service がインストールされているコンピュータに複数の NIC があり、**eimserver.ini** ファイルを編集した後でもブロック ページが正しく表示されない場合は、**BlockMsgServerName** パラメータで他の NIC の IP アドレスの入力を試みてください。

それでもブロック ページが表示されない場合、ユーザが下記の Websense ブロック ページ ディレクトリ内のファイルへの読み取りアクセス権限を持っていることを確認してください。

- Websense\BlockPages\en\Default
- Websense\BlockPages\en\Custom

ブロック ページの問題が解決しない場合は、その他のトラブルシューティングのヒントについて support. websense.com を検索してください。

ブロック ページの代わりに空白のホワイト ページが表示される

Web Security Help | Web Security ソリューション | バージョン 7.8.x

広告がブロックされた場合、またはブラウザがブロック ページに関連付けられているエンコードを正しく検出しなかった場合は、ユーザの画面にブロック ページの代わりに空白のホワイト ページが表示されることがあります。これは下記のの理由によって起こります。

- [広告] カテゴリがブロックされている場合は、Websense ソフトウェアは、グラフィック ファイルの要求を広告サイトの要求として解釈し、ブロック メッセージの代わりに空白のイメージを表示します（これは広告をブロックする場合の通常の方法です）。要求された URL が .gif または同様の拡張子で終わる場合は、ユーザに *.gif の部分を省いて URL を再入力するよう要求します。*グラフィック広告のブロック、145 ページ*を参照してください。
- 一部の古いブラウザは、ブロック ページのエンコードを検出できない場合があります。適切に文字コードを検出できるように、ブラウザが適当な文字セット（フランス語、ドイツ語、イタリア語、スペイン語、ブラジル ポルトガル語、簡体中国語、繁体中国語、韓国語の場合は UTF-8、日本語の場合は Shift_JIS）を表示するように設定します。そのための手順、またはブラウザを新しいバージョンにアップグレードする方法については、ブラウザのマニュアルを参照してください。

ログ、ステータス メッセージ、およびアラートの問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

- *Websense コンポーネントのエラー メッセージを探す方法、590 ページ*
- *Websense のヘルス アラート、590 ページ*
- *1 つの要求に対して 2 つのログ レコードが生成される、593 ページ*
- *Usage Monitor を使用できない、593 ページ*
- *Usage Monitor が実行していない、593 ページ*

Websense コンポーネントのエラー メッセージを探す方法

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense のコア コンポーネントに関連するエラーまたは警告がある場合は、Web Security manager. の **[Status] > [Alerts]** ページにアラート メッセージがリストされます。また、デフォルトでは **[Status] > [Dashboard]** ページの [System（システム）] タブの上部の **[Health Alert Summary（ヘルス アラートの要約）]** リストに、短いアラート メッセージが表示されます（*Websense のヘルス アラート、590 ページ*を参照）。

- ダッシュボードのアラートの要約をクリックすると、[Status] > [Alerts] ページに詳細な情報が表示されます。
- [Status] > [Alerts]ページのメッセージの隣の **[Solutions（ソリューション）]** をクリックすると、トラブルシューティングに役立つ情報が表示されます。

Websense ソフトウェア コンポーネントからのエラー、警告、メッセージ、およびデータベース ダウンロード ステータス メッセージは、Websense **bin** ディレクトリ の **websense.log** ファイルに記録されます（*Websense ログ ファイル、652 ページ*を参照）。

Windows コンピュータにインストールされている Websense ソフトウェア コンポーネントでは、Windows イベント ビューアをチェックすることもできます。*Windows イベント ビューア、651 ページ*を参照してください。

Websense のヘルス アラート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

デフォルトでは、

- 初期フィルタリング データベースが使用されている。
- マスタ データベースを初めてダウンロードしている
- マスタ データベースが 1 週間以上経過して古くなっている
- WebCatcher が無効化されている
- Log Server が実行していない
- プレゼンテーション レポートのスケジューラが Log Database に接続されていない
- Log Database ETL ジョブが 4 時間後に完了していない。
- Log Server が実行していない
- マスタ データベースが更新中
- マスタ データベースのダウンロードが失敗した
- TRITON 管理サーバーがインストールされているコンピュータのディスク スペースが不足している
- プライマリ Policy Broker は現在使用可能
- Log Database を使用できない
- 1 つ以上のプレゼンテーション レポートのジョブが失敗した
- Policy Server のための Log Server が設定されていない
- Log Database を使用できない

- Log Server がインストールされているコンピュータ上のディスク スペースが不足している
- Log Server は、1 時間以上、Filtering Service からデータを受け取っていない。
- Network Agent にモニタリング用の NIC が設定されていない
- Network Agent をインストールしているコンピュータのメモリーが不足している
- Filtering Service が実行していない
- Filtering Service をインストールしているコンピュータのディスクス ペースが不足している
- Filtering Service をインストールしているコンピュータで CPU 使用率が高い
- DC Agent の許可が不十分
- Filtering Service が Logon Agent と通信できない。
- Filtering Service が eDirectory Agent と通信できない。
- Usage Monitor が実行していない
- フォレンシック リポジトリの位置に到達できなかった
- 設定の問題によって脅威フォレンシック データを収集できない
- Log Server のキャッシュ ディレクトリがキャッシュ ファイルを 100 以上含んでいる。
- Network Agent に Filtering Service が設定されていない
- Network Agent をインストールしているコンピュータで CPU 使用率が高い
- Policy Server に Network Agent が設定されていない
- Network Agent が実行していない
- Filtering Service をインストールしているコンピュータのメモリーが不足している
- DC Agent インスタンスが必要なファイルにアクセスできない
- Filtering Service が DC Agent と通信できない
- Filtering Service が RADIUS Agent と通信できない。
- Policy Broker レプリカが 24 時間以上プライマリ Policy Broker と同期化していない
- Usage Monitor を使用できない
- フォレンシック リポジトリがその最大サイズの 90 % に達した
- フォレンシック リポジトリ内の一部のレコードが 1 週間以内に削除するようにスケジュール設定されている

Websense Web Security Gateway または Gateway Anywhere のライセンス契約をしている場合は、Websense ソフトウェアは Content Gateway をモニタして、下記の条件に関するアラートを表示します。

- Content Gateway が実行していない
- Content Gateway を使用できない

Websense Web Security Gateway Anywhere のライセンス契約をしている場合、またはサブスクリプションが Web セキュリティ コンポーネントとデータ セキュリティ コンポーネントの両方を含んでいる場合は、Websense ソフトウェアは、相互運用性のコンポーネントをモニタし、下記の条件に関するアラートを表示します。

- Sync Service が実行していない。
- Policy Server インスタンスと関連付けられた Sync Service がない。
- オンプレマイズのコンポーネントがハイブリッド サービスに接続できない。
- Sync Service をホストするパーティションでディクス スペースが不足している。
- Sync Service がハイブリッド サービスからログ ファイルをダウンロードしてから 24 時間経過した。
- ハイブリッド フィルタリングをアクティブにするために必要な情報が見つからない。
- Directory Agent が実行していない。
- Policy Server インスタンスと関連付けられた Directory Agent がない。
- ハイブリッドサービスからアラートを受け取った。
- Sync Service がログ ファイルを Log Server に送信してから 24 時間経過した。

アラート メッセージの隣のアイコンは、関連する条件の潜在的な影響を示します。

メッセージが通知メッセージであり、インストールによる問題を反映しません（例、WebCatcher が有効化されていない、または Filtering Service がマスタ データベースの更新をダウンロード中）。

アラート条件は、問題を起こす可能性がありますが、すぐにはポリシーの実施やレポーティングを妨げません（例、マスタ データベースは 1 週間以上経過している、またはサブスクリプション キーが有効期限切れが近づいている）。

Websense ソフトウェア コンポーネントが機能していない（構成されていないか、実行していない）ためにポリシーの実施またはレポーティングができない、またはサブスクリプションの有効期限が切れています。

[Health Alerts Summary] のアラート メッセージをクリックし、[Status] > [Alerts] ページを順に選択します。ここに現在のアラート条件に関する追加の情報が表示されます。詳細トラブルシューティングのヒントを表示するには、通知のアラートの場合は **[Learn More（詳しく知る）]**、エラーまたは警告の場合は **[Solutions]** をクリックします。

ヘルス アラートが、メッセージをハイブリッド サービスから受け取ったことを示す場合は、その詳細について [Hybrid Filtering Alerts（ハイブリッド フィルタリングのアラート）] テーブルをチェックします。

使用していないコンポーネントや無効にしているコンポーネントに関するエラーまたはステータス メッセージを受け取った場合は、そのアラート メッセージを非表示にするよう設定できます。詳細は、*現在のシステム ステータスの確認、490 ページ*を参照してください。

1 つの要求に対して 2 つのログ レコードが生成される

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Windows QoS Packet Scheduler を Network Agent と同じコンピュータにインストールした場合は、Network Agent コンピュータからの 1 つの HTTP またはプロトコル要求に対して 2 つの要求がログ記録されます（この重複は、ネットワーク内のクライアント コンピュータからの要求では起こりません）。

問題を解決するには、Network Agent コンピュータ上の Windows QoS Packet Scheduler を無効化します。

すべてのロギングに対して Network Agent を使用する場合は、この問題は発生しません。詳細については、*NIC の設定、547 ページ*を参照してください。

Usage Monitor を使用できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

カテゴリおよびプロトコル使用状況アラート機能、および Real-Time Monitor を有効化するために、Websense Usage Monitor をインストールする必要があります。通常は、ネットワーク内の各 Policy Server に 1 つの Usage Monitor インスタンスがインストールされます。Usage Monitor を Policy Server がインストールされているコンピュータにインストールすることもできます。

Usage Monitor をインストールするとき、Usage Monitor が下記のコンポーネントと通信できることを確認してください。

- ポート 55806 と 40000 上の Policy Server
- ポート 55880 上の Policy Broker
- ポート 55809 上の Filtering Service と Real-Time Monitor

Usage Monitor はまた、リッスン用ポート 55813 上で Policy Server および Filtering Service からの情報を受信できなければなりません。55813.

Usage Monitor が実行していない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Usage Monitor が停止している場合、下記の問題が発生します。

- アラートのためのカテゴリおよびプロトコル アクセス情報を収集できません。
- カテゴリおよびプロトコル使用状況アラートを生成できません。
- Real-Time Monitor は、インターネット アクティビティ データを受け取りません。

Usage Monitor を起動するには、下記のどちらかの手順を実行します。

- Windows の場合：Windows の [Services] ツールを開き、Websense Usage Monitor にスクロールし、そのサービスを右クリックして、**[Start（開始）]** を選択します。
- Linux の場合：**/opt/Websense/WebsenseDaemonControl** コマンドを使用します。

Usage Monitor が起動しない場合は、Windows Event Viewer または **websense.log** ファイルでサービスからのエラー情報がないかチェックしてください。

Policy Server と Policy Broker の問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

- *パスワードを忘れた、594 ページ*
- *Websense Policy Database サービスが開始しない、595 ページ*
- *Policy Server が突然に停止する、595 ページ*
- *Policy Broker レプリカがデータを同期化できない、596 ページ*

パスワードを忘れた

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ユーザが優先管理者または指定済み管理者であり、ローカル アカウントを使用して TRITON Unified Security Center にログオンしている場合は、グローバル セキュリティ管理者はパスワードをリセットできます。グローバル優先管理者は、[TRITON Settings（TRITON の設定）] > [Administrators（管理者）] ページでアカウントとパスワードを管理できます。

グローバル セキュリティ管理者が利用できない場合、ローカル アカウントを使用している管理者が TRITON ログオン ページの **[Forgot my password（パスワードを忘れた）]** リンクを通じて新しいパスワードを要求できます。

- 一時パスワードが管理者アカウントに関連付けられた電子メール アドレスに送信されます。
- 一時パスワードは、30 分間だけ有効です。一時パスワードでログオンする前に 30 分以上が経過した場合は、もう一度新しいパスワードを要求する必要があります。
- 一時パスワードを使ってログオンした後、新しいパスワードを入力するように求められます。

Websense Policy Database サービスが開始しない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Policy Database は、特別なアカウント **WebsenseDBUser** として実行します。このアカウントでログオンの問題が起こった場合、Policy Database は起動できません。

この問題を解決するには、WebsenseDBUser パスワードを変更します。

1. ローカル管理者として Policy Database がインストールされているコンピュータにログオンします。
2. **[Start] > [Programs] > [Administrative Tools] > [Computer Management（コンピュータ管理）]** を順に選択します。
3. ナビゲーションペインの [System Tools（システム ツール）] の下の **[Local Users and Groups（ローカル ユーザおよびグループ）]** を 展開し、**[Users（ユーザ）]** を選択します。コンテンツ ページにユーザ情報が表示されます。
4. **[WebsenseDBUser]** を右クリックし、**[Set Password（パスワードを設定）]** を選択します。
5. このユーザ アカウントの新しいパスワードを入力および確認して、**[OK]** をクリックします。
6. [Computer Management] ダイアログ ボックスを閉じます。
7. 下記のどちらかの Windows のサービス ツールを開きます。
   - Windows Server 2012：[Server Manager] > [Tools] > [Services]
   - Windows Server 2008 R2：[Start] > [Administrative Tools] > [Services]
8. **[Websense Policy Database]** を右クリックし、**[Properties（プロパティ）]** を選択します。
9. [Properties] ダイアログ ボックスの [Log On（ログオン）] タブに新しい WebsenseDBUser パスワード情報を入力し、**[OK]** をクリックします。
10. [Websense Policy Database] を再度右クリックし、**[Start]** を選択します。

    サービスが開始したとき、[Services] ツールを閉じます。

Policy Server が突然に停止する

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Policy Server がインストールされているコンピュータのハード ディスクの空きスペースがなくなった場合は、Websense Policy Server サービスまたはデーモンが停止します。ディスク スペースの不足が一時的な状況（他のアプリケーションが大きな一時ファイルを作成し、それらを削除する場合）であっても、Policy Server は自動的には再起動されません。

- Policy Server がインストールされているコンピュータに Filtering Service または Network Agent がインストールされた場合は、Web Security manager のヘルス アラート メッセージがディスク スペースが少なくなっているという警告を示します。
- Policy Server が停止したとき、Web Security manager にヘルス アラート メッセージが表示されます。

当面の問題に対処するには、Policy Server を手動で再起動します。つぎに、コンピュータでどのアプリケーションが利用可能なすべてのディスク スペースを塞いでいるのかを判断します。次に、最良のソリューションがそのアプリケーションを他のコンピュータに移動することなのか、Policy Server がインストールされているコンピュータにディスク スペースを追加することなのかを判断します。

Policy Broker レプリカがデータを同期化できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

複製された Policy Broker が配備されている環境では、環境内のすべてのコンポーネントが最新の情報を利用できるように、各レプリカは定期的にそのポリシーおよび設定データをプライマリ Policy Broker と同期化します。

レプリカが 24 時間以上プライマリ Policy Broker に接続できない場合、ヘルス アラートが表示されます。この問題を解決するには、下記の手順を実行します。

- プライマリ Policy Broker がインストールされているコンピュータとレプリカ Policy Broker がインストールされているコンピュータの間で、ポート **6432** 上での双方向ネットワーク通信が可能であることを確認します。（ファイアウォールがこのポート上でのインバウンド接続とアウトバウンド接続の両方を許可する必要があります）。
- プライマリ Policy Broker コンピュータが稼働していて、Policy Broker サービスまたはデーモンが実行していることを確認します。
- Policy Broker レプリカ コンピュータが作動していて、Policy Broker サービスまたはデーモンが実行していることを確認します。
- レプリカ Policy Broker はプライマリ Policy Broker の設定中に設定された同期化パスワードを使用する必要があります。最近プライマリ Policy Broker を交換した場合は、正しい同期化パスワードが使用されていることを確認してください。

指定済み管理の問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

管理されたクライアントをロールから削除できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

下記の場合に、[Delegated Administration（代理管理）] > [ロールを編集（Edit Role）] ページの管理対象のクライアント リストからクライアントを直接に削除できません。

- 管理者がポリシーをクライアントに適用している
- 管理者が、ネットワーク、グループ、ドメイン、または組織単位の 1 つ以上のメンバーにポリシーを適用している。

優先管理者が接続している Policy Server が、削除されるはずのクライアントを含むディレクトリ サービスと通信している Policy Server ではない場合、問題が発生するかもしれません。この場合、現在の Policy Server およびディレクトリ サービスはクライアントを認識しません。

管理対象のクライアントの削除の方法については、*処理対象クライアントの削除、434 ページ*を参照してください。

ログオン エラー メッセージによると、他のユーザが私のコンピュータにログオンしている

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Manager にログオンしようとしたとき、[ログオンに失敗しましたロール *role_name* は *user_name* により、*date, time* 以降、コンピュータ 127.0.0.1. で使用されています。]IP アドレス 127.0.0.1 は、[ループバック アドレス] とも呼ばれ、一般的にはローカル コンピュータを表します。

このメッセージは、他の誰かが、ユーザーが要求しているのと同じロールで TRITON 管理サーバー コンピューターから Web Security manager にログオンしていることを示します。別のロールを選択し（複数のロールを管理している場合）、レポート用にのみログオンするか、または他の管理者がログオフするまで待ちます。

再分類されたサイトが誤ったカテゴリに従ってフィルタリングされる

Web Security Help | Web Security ソリューション | バージョン 7.8.x

再分類された URL は、その URL を追加したロールによって管理されるクライアントにのみ影響します。たとえば、優先管理者が URL を再カテゴリ化した場合、指定済み管理ロールによって管理されているクライアントは、引き続きこれらのサイトのマスタ データベースカテゴリに従ってフィルタリングされます。

再分類を他のロールのクライアントに適用するために、優先管理者は各ロールに切り替え、そのロールでそのサイトを再分類することができます。

カスタム プロトコルを作成できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

優先管理者だけがカスタム プロトコルを作成できます。しかし、指定済み管理者は、カスタム プロトコルのアクションを設定できます。

優先管理者がカスタム プロトコルを作成するとき、ほとんどのクライアントに適応するデフォルト動作を設定する必要があります。次に、指定済み管理者に新しいプロトコルを伝え、指定済み管理者が必要に応じて自分のロールでのフィルタを更新できるようにします。

Log Server と Log Database の問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

- *Log Server が実行していない*、599 ページ
- *Log Server が Filtering Service からログ ファイルを受け取らなかった*、600 ページ
- *Log Server がインストールされているコンピュータ上のディスク スペースが不足している*、603 ページ
- *Policy Server に Log Server がインストールされていない*、604 ページ
- *ログ データベースが作成されなかった*、606 ページ
- *Log Database を使用できない*、607 ページ
- *ログ データベースのサイズがレポーティングの遅延を起こしている*、608 ページ
- *Log Server キャッシュ ディレクトリに 101 個以上のファイルがある*、609 ページ
- *最後に成功した ETL ジョブが 4 時間以上前に実行された*、611 ページ

Log Server が実行していない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Log Server が実行していない場合、または他の Websense コンポーネントが Log Server と通信できない場合は、インターネット使用状況の情報が保存されません。**[Status] > [Dashboard]** ページのグラフがアップグレードを停止し、レポートを生成できないことがあります。

下記の場合に Log Server を使用できません。

- 20 回の試行の後、Log Database に接続できない。

  Log Database がインストールされているコンピュータが実行していること、Microsoft SQL Server が適切に動作していること、Log Server コンピュータと Log Database コンピュータの間のネットワーク通信が中断されていないことを確認してください。
- Log Server がインストールされているコンピュータのディスク スペースが足りない。

  Log Server がインストールされているコンピュータの空きディスク スペースを確認し、必要に応じて、不要なファイルを削除します。
- Microsoft SQL Server パスワードを変更したが、ODBC または Log Server の接続を更新していない。

  この問題の対処の方法については、*Log Server 接続アカウントまたはパスワードの更新、613 ページ*を参照してください。
- マスタ データベースが正常にダウンロードされてから 14 日を超えている。

  この問題の対処の方法については、*マスタ データベースが 1 週間以上経過して古くなっている、556 ページ*および*マスタ データベースがダウンロードしない、557 ページ*を参照してください。
- **logserver.ini** ファイルが見つからないか壊れている。

  Websense **bin** ディレクトリ（デフォルトでは C:\Program Files または Program Files（x86）\Websense\Web Security\bin）に移動し、テキスト エディタで **logserver.ini** ファイルを開くことができるか確認します。このファイルが壊れている場合は、バックアップ ファイルに置き換えます。

- インターネット使用状況の情報をログ記録しないように、Log Server を停止した。

  Windows の [Services] ツールで Log Server が起動していることを確認し、必要に応じてそのサービスを再起動します（*Websense サービスの停止と起動*、477 ページを参照）。

これらの処置のどれもが問題に対応しない場合、問題をよりよく把握するために、Windows イベント ビューア と **websense.log** ファイルで Log Server からのエラー メッセージ（*トラブルシューティングのヒントとツール*、650 ページを参照）がないかチェックします。

Log Server が Filtering Service からログ ファイルを受け取らなかった

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Log Server は、Filtering Service からインターネット使用状況の情報を受け取って、Log Database に保存します。Log Server が Filtering Service からファイルを受け取らなかった場合は、データがログ記録されず、最新のデータが **[Status] > [Dashboard]** ページに表示されず、そのため最新のデータを含むインターネット使用状況レポートを作成できません。

下記の場合に Log Server が Filtering Service からファイルを受け取らないことがあります。

- Filtering Service が実行していない。

  この問題の対処の方法については、*Filtering Service が実行していない*、565 ページを参照してください。
- 2 つのサービスがネットワークを通じて通信できない。
  - ファイアウォール ルールに最近変更がなかったか確認します。このルール変更があれば、ポート 55805（デフォルト）または組織が使用しているカスタム ポート上のコンピュータ間でのトラフィックに影響を与えることがあります。
  - **telnet** または **ping** などのユーティリティを使用して、コンピュータ間で通信できることを確認します。
  - Web Security manager の **[Settings] > [General] > [Logging]** ページで Log Server IP アドレスおよびポート（デフォルトでは 55805）が正しいことを確認します。

    ループバック アドレス（127.0.0.1）または [localhost] が表示された場合は、Log Server がインストールされているコンピュータの実際の IP アドレスを入力します。
  - [Settings] > [General] > [Logging（ログ記録）] ページを順に選択し、**[Check Status（ステータスを確認）]** ボタンを使用して、Log Server に接続できることを確認します。

ステータスの確認ができなかった場合、下記の処置を実行します。

a. ポートをブロックしているファイアウォールがないことを確認します。

b. 下記のコマンドを Log Server がインストールされているコンピュータで実行して Log Server がそのポートでリッスンしていることを確認します。

```
netstat -ban > port.txt
```

- Network Agent、Content Gateway、またはサードパーティの統合製品が正しく構成しておらす、インターネット トラフィックを受け取っていません。
  - Network Agent 構成の問題の対処の方法については、*Network Agent の問題、570 ページ*および*ネットワークの構成、541 ページ*を参照してください。
  - Content Gateway 構成の問題の対処の方法については、Deployment and Installation Center および Content Gateway Help を参照してください。
  - 他のサポートされている統合製品の詳細については、Deployment and Installation Center およびベンダーのマニュアルを参照してください。
- Log Server に新しいキャッシュ ファイルを作成するための十分なディスク スペースがありません。

  この問題の対処の方法については、*Log Server がインストールされているコンピュータ上のディスク スペースが不足している、603 ページ*を参照してください。
- Filtering Service がログ記録用に設定されいない Policy Server に関連付けられているか、またはログを TestLogServer に送信しています。

  この問題の対処の方法については、*Policy Server に Log Server がインストールされていない、604 ページ*および*要求がログ記録される方法の設定、505 ページ*を参照してください。
- ファイルをキャッシュまたは BCP フォルダに書き込みできません。

  [Settings] > [Reporting（レポーティング）] > [Log Server] ページを順に選択し、ODBC キャッシュ ファイルまたは BCP ファイルに対してパスが正しく定義されていること、およびパスへの書き込み許可を持つ Log Server サーバーを実行するためのアカウントが使用されていることを確認してください。
- Log Server が適切にインストールされていませんでした。

  下記の手順を実行し、Log Server が Windows オペレーティング システムに適切に登録されていることを確認します。

  1. Windows の [Services] ツールを使用して Websense Log Server サービスを停止します。
  2. コマンド プロンプトを開き（**Run > cmd**）、Websense **bin** ディレクトリ（デフォルトでは C:\Program Files または C:\Program Files（X86）\Websense\Web Security\bin）に移動します。

3. 下記のコマンドを入力します。

   ```
   LogServer .exe -c
   ```

   - エラーが表示されなかった場合は、サービスは適切に登録されています。
   - エラーが表示された場合は、次のステップに進みます。

4. Log Server サービスを削除するために、下記のコマンドを入力します。

   ```
   LogServer.exe -u
   ```

5. 実行可能ファイルを登録するために、下記のコマンドを入力します。

   ```
   LogServer.exe -i
   ```

6. 再度、下記のコマンドを入力します。エラーが表示されないことを確認します。

   ```
   LogServer .exe -c
   ```

上記の項目のどれもが問題に対象しない場合は、下記の事柄について確認してください。

- Log Server の実行可能ファイルのバージョンがインストールしている製品バージョンに対応していることを確認してください。Log Server のバージョンを見つけるには、下記の手順を実行します。

  1. Log Server がインストールされているコンピュータで Windows コマンド プロンプトを開きます。
  2. Websense **bin** ディレクトリ（デフォルトでは C:\Program Files、*または* Program Files（x86）\Websense\Web Security\bin）に移動します。
  3. 下記のコマンドを入力します。

     ```
     logserver -v
     ```

  この Log Server のバージョンは、TRITON Unified Security Center の **[Help（ヘルプ）] > [About the TRITON Console（TRITON Console について）]** ページの **[Web Security build（Web Security のビルド）]** の隣に表示されるバージョンと一致している必要があります。

- Websense アプライアンス上の Filtering Service が設定を変更した後、指定どおりに再起動しないことがあります。アプライアンス上の Filtering Service が実行を停止した場合は、**[Status] > [Modules（モジュール）]** を順に選択し、Websense Web Security モジュール全体を再起動します。
- Log Server が再起動の後すぐに実行を停止し、実行時エラー[C error（Visual C Runtime Error（ビジュアル C 実行時エラー））] を表示した場合、Log Server の **[Cache（キャッシュ）]** フォルダ（デフォルトでは C:\Program Files または Program Files（x86）\Websense\Web Security\bin\Cache）にある **LogServer.state** ファイルを削除し、**[Websense Log Server]** サービスを再開します。
- TestLogServer を使用している場合は、このツールがログ データを Log Server に転送するように設定されていることを確認してください。

  TestLogServer の詳細については、support.websense.com を参照してください。

Log Server がインストールされているコンピュータ上のディスク スペースが不足している

Websense Log Server は、インターネット アクティビティのレコードをそれらがログ データベースに処理されるまで Log Server がインストールされているコンピュータの一時ログ キャッシュ ファイルまたは BCP（Bulk Copy Program）のファイルに保存します。

Websense ソフトウェアはログ キャッシュ ファイルと BCP ファイルに利用可能なスペースを監視します。デフォルトでは：

- ログ キャッシュ ファイルは、**C:\Program Files または Program Files (x86)\Websense\Web Security\bin\Cache** ディレクトリに保存されます。
- BCP ファイルは、**C:\Program Files または Program Files (x86)\Websense\Web Security\bin\Cache\BCP** ディレクトリに保存されます。

ログ キャッシュ ファイル と BCP ファイルの場所の変更は、Web Security manager の **[Settings] > [Reporting] > [Log Server]** ページで行うことができます。*Log Server の設定*、507 ページを参照してください。

> **注意**
> データを一次 Log Server に転送する複数の Log Server がある場合は、一次 Log Server のディスク スーペースのみが追跡されます。

これらのどちらかの場所で利用可能なスペースが少なすぎる場合は。[Status] > [Status] ページの [System] タブにヘルス アラート メッセージが表示されます。ディスク スペースが不足している場合は、ログ記録は停止します。

- ログ キャッシュ ファイルまたは BCP ファイルが保存されているドライブの空きディスク スペースが 10% 未満になったとき、警告メッセージが表示されます。ログ記録は続行しますが、ログ データの損失を避けるためにできる限り速やかにコンピュータ上のディスク スペースをクリアする必要があります。
- ログ キャッシュ ファイルまたは BCP ファイルが保存されているドライブの空きディスク スペースが 4 MB 未満になったとき、エラー メッセージが表示されます。

  ディスク スペースが 4 MB 未満になったとき、ログ記録が断続的になるか、完全に停止するかもしれません。ログ データの損失を最小限に抑えるために、エラー メッセージが表示されたら、できる限り速やかに Log Server がインストールされているコンピュータのディスク スペースをクリアしてください。

Policy Server に Log Server がインストールされていない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Log Server は、インターネット使用状況の情報を収集し、その情報をログ データベースに保存して、調査レポート、プレゼンテーション レポート、および Web Security manager の [Dashboard] ページのグラフおよび要約で使用できるようにします。

レポートを作成するためには、Log Server がインストールされている必要があります。

このメッセージは下記の場合に表示されます。

- Log Server が Policy Server とは別のコンピュータにインストールされており、Log Server の IP アドレスが誤って Web Security manager のローカルホストに設定されている。
- Websense レポーティング ツールを使用していません。
- Log Server が別の Policy Server インスタンスに関連付けられています。

Web Security manager で Log Server の IP アドレスが正しく設定されていることを確認するには、下記の手順を実行します。

1. 左側のナビゲーション ペインの **[Settings]** タブを選択し、**[General（一般）] > [Logging（ロギング）]** を順に選択します。
2. **[Log Server IP address or name（Log Server の IP アドレスまたは名前）]** フィールドに、Log Server がインストールされているコンピュータの IP アドレスを入力します。
3. **[OK]** をクリックして変更をキャッシュし、**[Save and Deploy]** をクリックします。

Websense のレポーティング ツールを使用していない場合、または Log Server を別の Policy Server インスタンスに関連付けている場合は、Web Security manager のアラート メッセージを非表示にできます。

1. 左側のナビゲーション ペインの [Main（メイン）] タブで **[Status] > [Alerts（アラート）]** を順に選択します。
2. [Active Alerts（アクティブなアラート）] の下の **[Advanced（詳細）]** をクリックします。
3. メッセージ [No Log Server installed（Log Server がインストールされていません）] の **[Hide this alert（このアラートを非表示）]** をオンにします。
4. **[Save Now（すぐに保存）]** をクリックします。変更が即座に実行されます。

Policy Server に 2 つ以上の Log Server がインストールされている

Web Security Help | Web Security ソリューション | バージョン 7.8.x

各 Policy Server インスタンスは Web Security Log Server の 1 つのインスタンスにだけ接続できます。Log Server の複数のインスタンスが同じ Policy Server に接続しようと試みた場合、ログ データが適切に記録されず、複数のレポーティング ツールに問題が発生します。

この問題を解決するには、下記の手順を実行します。

- 複数のアクティブな Log Server インスタンスが実行している場合、エラーを報告している Policy Server に接続している 1 つの Log Server インスタンスを除いて他のすべての Log Server インスタンスをアンインストールします。

  データをログ データベースに記録する中央 Log Server と通信するために複数の Log Server インスタンスを構成する場合は、Log Server の[Extending your Web Security deployment（Web Security 環境の拡張）] を参照してください。
- このエラーが表示されたが、Log Server の 1 つのインスタンスだけがアクティブである場合は、下記のいすれかのことが原因である可能性があります。
  - Log Server インスタンスをアンインストールされたとき Policy Server を実行していなかった。
  - Log Server をインストールした後、Policy Server の IP アドレスを変更した。
  - インストール時に、Log Server が他のコンピュータ上の Policy Server インスタンスに接続していた。Log Server がインストールされているコンピュータに後で、Policy Server インスタンスがインストールされた。

  これらのすべての場合、問題に対処するための最も安全な方法は、下記の手順を実行することです。

  1. エラーを表示している Policy Server インスタンスに現在接続されている Log Server（1 つまたは複数）をアンインストールします。
  2. Websense Policy Server を停止します（Windows の [Services] ツールまたは /opt/Websense/WebsenseDaemonControl コマンドを使用）。
  3. Websense **bin** ディレクトリ（C:\Program Files **または** Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin）に移動し、他の場所に **config.xml** ファイルのバックアップ コピーを作成します。**この手順をスキップしてはいけません**。
  4. 基本テキスト エディタ（XML エディタや HTML エディタではない）で元の **config.xml** ファイルを開きます。

5. ファイルの上部近くで、WebsenseLogServer コンテナを見つけます。このコンテナには [ghost]Log Server インスタンスの ID が含まれています。

   ```
   <container name="WebsenseLogServer">
   ```

6. コンテナ全体（終了タグを含む）を削除します。例：

   ```
   <container name="WebsenseLogServer">
        <data name="0c65012f-93af-11e1-8616-
   f215ee9c7d9d"> 10.201.136.34</data>
   </container>
   ```

7. **config.xml** ファイルを保存し、閉じます。
8. Websense **bin** ディレクトリから **config.xml.bak** ファイルを削除します。
9. Windows の [Services] ツールまたは /opt/Websense/ WebsenseDaemonControl コマンドを使用して、Websense Policy Server を起動します。

ログ データベースが作成されなかった

インストーラがログ データベースを作成できなかった場合は、下記の事柄を確認してください。

- インストールのためにログオンするときに使用したアカウントが、データベースを作成するために必要な SQL Server の許可を割り当てられていない。必要な許可は、Microsoft SQL Server のバージョンによって異なります。
  - SQL Server Standard または Enterprise は **dbcreator** サーバー ロール メンバーシップ、**db_datareader** ロール メンバーシップ、および以下のいずれかのロールのメンバーシップを必要とします。
    - SSQLAgentUserRole
    - SQLAgentReader ロール
    - SQLAgentOperator ロール
  - SQL Server Express：**sysadmin** の許可が必要

  ログオン アカウントを更新するか、すでに必要な許可を割り当てられているアカウントを使ってログオンし（*Microsoft SQL Server のユーザ許可の設定、613 ページ*を参照）、インストーラを再度実行します。
- デフォルトのログ データベース名（wslogdb70 および wslogdb70_1）のファイルが存在するが、そのファイルがデータベース エンジンに適切に接続されていないために、Websense インストーラがそれを使用できない。

  この問題は、下記のように対処します。
  - 既存のデータベース ファイルを更新しない場合は、それらのファイルを削除するかまたは名前を変更し、次にインストーラを再度実行します。

- 既存のデーターベース ファイルがアップグレード可能なバージョンからのファイルであり、引き続きそれらのファイルを使用する場合、SQL Server Management Studio を使用して、それらのファイルをデータベース エンジンに接続し、インストーラを再度実行します。

- インストーラを実行するとき使用したアカウントが、データベースのインストール先ドライブへの必要なアクセスを許可されていない。

  ログオン アカウントがインストール場所への読み取り / 書き込みを許可されるように更新するか、または、すでにそのようなアクセスを許可されている別のアカウントを使ってログオンします。次に、インストーラを再度実行します。

- 指定されたインストール先に、ログ データベースを作成および保持するための十分なディスク スペースがない。

  ログ データベースをインストールおよび保持するために選択したディスク上で、十分な空きスペースを確保します。次に、インストーラを再度実行します。代わりに、他の場所を選択します。

Log Database を使用できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense ログ データベースは、インターネット使用状況の情報を保存して、プレゼンテーション レポート、調査レポートや、Web Security manager の [Dashboard] ページのグラフおよび要約で使用できるようにします。

Websense ソフトウェアがログ データベースに接続できない場合は、最初に、データベース エンジン（Microsoft SQL Server または Microsoft SQL Server Express）がログ データベースがインストールされているコンピュータで実行していることを確認します。

1. Windows の [Services] ツール（*Windows Services ツール、651 ページ*を参照）を開き、**MSSQLSERVER** サービスが実行していることを確認します。

   Microsoft SQL Server Standard または Enterprise（Express でない）を実行している場合は、**SQLSERVERAGENT** が実行していることも確認します。

2. サービスが停止している場合、サービス名を右クリックし、**[Start]** をクリックします。

   サービスが再開しない場合は、Windows イベント ビューア（*Windows イベント ビューア、651 ページ*を参照）で Microsoft SQL Server のエラーおよび警告をチェックします。

3. Microsoft SQL Server Standard または Enterprise（Express でない）を実行している場合は、SQLSERVERAGENT サービスをダブルクリックし、[Properties（プロパティ）] ダイアログ ボックスを開き、**スタートアップ タイプ**が **[Automatic（自動）]** に設定されていることを確認します。それによって Microsoft SQL Server またはデータベース エンジンがインストールされているコンピュータが再起動されるたびに、SQL Server Agent が再起動することを確認します。

スタートアップ タイプ が [Manual（手動）] または [Disabled（無効化）] である場合は、**[Automatic（自動）]** に変更し、**[OK]** をクリックします。

データベース エンジンおよび（該当する場合は）SQL Server Agent サービスが実行している場合は、下記の事柄を確認します。

- Windows の [Services] ツールを使って、**Websense Log Server** サービスが実行していることを確認します。
- Log Server と Log Database が別のコンピュータで実行している場合は、両方のコンピュータが実行しており、両方のコンピュータ間のネットワーク接続に障害がないことを確認します。
- Log Database コンピュータに十分なディスク スペースがあり、ログ データベースに十分なディスク スペースが割り当てられていることを確認します（*Log Server が Log Database にデータを記録しない*、612 ページを参照）。
- Microsoft SQL Server のパスワードが変更されていないことを確認します。パスワードが変更された場合は、Log Server がデータベースへの接続に使用するパスワード情報を更新する必要があります。*Log Server 接続アカウントまたはパスワードの更新*、613 ページを参照してください。
- Web Security manager がログ データベースと通信するのを妨げるネットワークの中断がないことを確認します。

データベース エンジンおよび関連サービスが実行していること、およびネットワーク上の問題が解決されたことを確認した後、Windows の [Services] ツールを使用して Websense TRITON - Web Security サービスを再開します。それによってプレゼンテーション スケジューラがジョブの定義を保存できるようにします（*Policy Server に Log Server がインストールされていない*、604 ページを参照）。

ログ データベースのサイズがレポーティングの遅延を起こしている

Web Security Help | Web Security ソリューション | バージョン 7.8.x

常にログデータベースのサイズに注意する必要があります。Websense レポートが正常に生成された場合でも、レポートの表示に時間がかかるようになったり、Web ブラウザから [timeout（タイムアウト）] メッセージが表示される場合は、一部のデータベース パーティションを無効にすることを検討してください。

1. Web Security manager で、**[Settings] > [Reporting] > [Log Database（ログ データベース）]** を順に選択します。
2. このページの **[Available Partitions（使用可能なパーティション）]** セクションを見つけます。
3. 現在のレポーティングの操作に必要ないパーティションの隣のチェック ボックスをオンにして、**[Disable（無効化）]** をクリックします。

4. **[OK]** をクリックし、**[Save and Deploy]** をクリックして変更を適用します。

データベースのサイズを推定する方法については、*ログ データベースのサイズ設定のガイドライン、529 ページ*を参照してください。

Log Server キャッシュ ディレクトリに 101 個以上のファイルがある

Web Security Help | Web Security ソリューション | バージョン 7.8.x

通常、Log Server ODBC キャッシュ ファイルまたは BCP ファイルは一定のペースで Log Database へ移動されます。Log Server コンピュータに一時ファイルが蓄積している場合、現在のインターネット使用状況情報はログ データベースに送信されません。

Log Server は、下記の場合に一時ファイルを処理できないことがあります。

- ログ データベースが実行していないか、Microsoft SQL Server がインストールされているコンピュータへの接続がダウンしているか、またはデータベースが使用中である場合。*Log Database を使用できない、607 ページ*を参照してください。
- ログ データベースが適切にインストールされていないか、誤ったバージョンである場合。*ログ データベースが作成されなかった、606 ページ*を参照してください。
- ETL ジョブが実行を停止し、着信バッファが一杯になっている場合。
- ログデータベースに割り当てられたデスク スペースがいっぱいになった場合。*Log Server が Log Database にデータを記録しない、612 ページ*を参照してください。
- データベース作成パスが無効である場合。
- 現在のアクティブなパーティションがない場合。
- BCP 挿入に問題がある場合。
- **tempdb** のサイズに問題がある場合。

問題を解決するには、下記のいずれかの手順を実行します。

- Microsoft SQL Server が実行していること（*Log Database を使用できない、607 ページ*を参照）、および大量のリソースを使用する他のプロセス（フル バックアップ、アンチウィル スキャンなど）が実行していないことを確認します。

  ディスク IO を調べて、コンピュータがデータベースへの高速挿入を処理できることを確認します。
- Microsoft SQL Server の認証されているバージョンを使用していることを確認します。
  - SQL Server 2012
  - SQL Server 2008 または 2008 R2 Enterprise または Standard

- SQL Server 2008 R2 Express

  SQL Server Express を使用している場合は、TRITON Unified Installer を使用してデータベース エンジンをインストールする必要があります。

- SQL Server Management Studio を使用して、ETL ジョブが実行していることを確認します。

  SQL Server Enterprise または Standard を使用しており、ETL ジョブが実行していない場合は、コンピュータで SQL Server Agent が実行していることを確認します。

  SQL Server Agent が実行している場合は、下記のことを行います。

  - カタログ データベース（wslogdb70）を展開し、INCOMINGBUFFER にレコードがあることを確認します。INCOMINGBUFFER が一杯になっている場合は、Log Server は追加のレコードを追加できません。
  - [INCOMINGBUFFER] テーブルにレコードがある場合は、下記の手順を実行します。
    a. **[wse_etl_config]** テーブルを見つけます。
    b. 右クリックして、**[Open Table（テーブルを開く）]** を選択します。
    c. **[max_buffer_size]** の値を **40000** に変更します。

- SQL Server Management Studio を使用して、カタログ データベースの **[Auto Growth（自動増加）]** オプションが有効化されていることを確認します。
- Web Security manager の **[Settings] > [Reporting] > [Log Database]** ページを順に選択し、下記の事柄を確認します。
  - **[Partition Management（パーティション管理）]** の下の **[File Path（ファイル パス）]** のエントリが有効であること。
  - **[Available Partitions]** の下に少なくとも 1 つのパーティションがリストされていること。
- Log Server が BCP 挿入を使用するために設定されているが、BPC ファイルが処理されない場合は、挿入方法を ODBC に変更し、新しいキャッシュ ファイルが処理されるかどうか確認します。
  1. Web Security manager の **[Settings] > [Reporting] > [Log Server]** ページを順に選択します。
  2. **[Log Record Creation（ログ レコード作成）]** セクションを展開します。
  3. **[ODBC（Open Database Connectivity）]** ラジオ ボタンを選択します。
  4. **[OK]** をクリックして変更をキャッシュし、**[Save and Deploy]** をクリックしてそれらの変更を適用します。

  デフォルトでは、ODBC キャッシュ ファイルは、**C:\Program Files または Program Files（x86）\Websense\Web Security\bin\Cache** ディレクトリに作成されます。
- データベース **tempdb** のログ（ldf）ファイルが一杯になっている場合があります。Microsoft SQL Server（MSSQLSERVER）サービスを再開し、tempdb データベースをクリアします。

最後に成功した ETL ジョブが 4 時間以上前に実行された

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ETL（Extract（抽出）、Transform（変換）、および Load（ロード））ジョブがパーティション データベースにデータを取り込まねばなりません。このジョブが定期的に実行しない場合は、ログ データベースへのデータの書き込みが遅れ、その結果、レポートおよびダッシュボードのグラフが最新でなくなります。

一般的に、ETL ジョブはすばやく実行し、最後の処理の完了から 10 秒後に再び開始されるようにスケジュール設定されます。ただし、レコードがデータベースに渡されていない場合（たとえばネットワーク関連の問題のため、または Filtering Service もしくは Log Server が実行していないため）、再びデータの受け取りが開始するまでそのジョブは実行しません。

ジョブが最近実行していない場合は、下記のことを確認してください。

- Microsoft SQL Server が実行していること（*Log Database を使用できない、607 ページ*を参照）、および大量のリソースを使用する他のプロセス（フル バックアップ、アンチウィル スキャンなど）が実行していないことを確認します。
  - ディスク IO を調べて、コンピュータがデータベースへの高速挿入を処理できることを確認します。
  - リンクされている手順を使ってログ データベースの問題のチェックします。
- 使用している Microsoft SQL Server が下記のいずれかのの認証済みバージョンであることを確認します。
  - SQL Server 2012 Enterprise または Standard
  - SQL Server 2008 または 2008 R2 Enterprise または Standard
  - SQL Server 2008 R2 Express

    SQL Server Express を使用している場合は、TRITON Unified Installer を使用してデータベース エンジンをインストールする必要があります。
- （*Microsoft SQL Server Standard および Enterprise*）ＳＱＬ Ｓｅｒｖｅｒ がインストールされているコンピュータ上の Windows Services ツールを使用して、SQL Server Agent サービスが実行していることを確認します。
- SQL Server Management Studio を使用して、ETL ジョブが実行していることを確認します。ETL ジョブが実行していない場合は、ジョブ履歴でエラーがないか確認し、ジョブを再開するか、ジョブを手動で実行します。
- 下記の手順を使用します。
  - FiltFiltering Service がデータを送信していることを確認する
  - Log Server をインストールしているコンピュータ上で問題が発生していないか調べる

また、TestLogServer ユーティリティを使用してログ記録動作を確認することもできます。Using TestLogServer for Web Security Troubleshooting（Web Security のトラブルシューティングに TestLogServer を使用する）を参照してください。

データベース アカウントを使用するように Log Server を構成する

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ログ データベースに接続するためにデータベース アカウント（**sa** など）を使用するように Log Server を設定するには、下記の手順を実行します。

1. Web Security manager で、**[Settings] > [Reporting] > [Log Server]** を順に選択します。
2. **[Log Database Connection（ログデータベース接続）]** の下で **[SQL Server authentication（SQL Server 認証）]** ラジオ ボタンを選択します。
3. 作成、読み取り、および書き込み許可をもつ SQL Server アカウントの **[Account** name（アカウント名）]（例、**sa**）および **[Password（パスワード）]** を入力します。詳細は、*Microsoft SQL Server のユーザ許可の設定*、613 ページを参照してください。
4. Click **[Test Connection]** をクリックし、Log Server が選択したアカウントを使用してログ データベースに接続できること、およびそのアカウントが適切な許可を持っていることを確認します。
5. **[OK]** をクリックして変更をキャッシュし、**[Save and Deploy]** をクリックしてそれらの変更を適用します。
6. Windows の [Services] ツールで **Websense TRITON - Web Security** サービスを再開します。

Log Server が Log Database にデータを記録しない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Log Server がログ データベースにデータを書き込めない場合は、通常はデータベースに割り当てられたディスク スペースがいっぱいになったことが考えられます。これはディスク ドライブがいっぱいになった場合、または、Microsoft SQL Server の場合にはデータベースの最大サイズが設定されている場合に起こります。

Log Database が置かれているディスク ドライブがいっぱいになった場合、ログ記録を再開するためにはコンピュータにディスク スペースを追加する必要があります。

SQL Server Database 管理者が Microsoft SQL Server 内の個別のデータベースの最大サイズを指定している場合、以下のどちらかの方法で対処します。

- SQL Server Database 管理者に連絡して、最大サイズを大きくするよう依頼する。
- 最大サイズを調べ、**[Settings] > [Reporting] > [Log Database]** を順に選択して、ログ データベースが最大サイズの約 90% に達したときロール オーバーするように構成する。*データベース パーティション オプションの設定*、518 ページを参照してください。

IT 部門が SQL Server 運用のためのディスク スペースの最大量を設定している場合は、IT 部門に連絡してください。

Log Server 接続アカウントまたはパスワードの更新

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Log Server がログ データベースに接続するとき使用するアカウントまたはパスワードを変更するには、下記の手順を実行します。

1. Web Security manager で、**[Settings] > [Reporting] > [Log Server]** を順に選択します。
2. **[Log Database Connection（ログ データ t ベースの接続）]** の下の **[Data source name（DSN）（データ ソース名（DNS））]** フィールドに正しいデータベース（デフォルトでは、wslogdb70）が表示されていかどうか確認します。
3. 接続方法として **[SQL server authentication（SQL サーバー認証）]** が選択されており、**[Account（アカウント）]** フィールドに有効なアカウント名（例、**sa**）が表示されていることを確認してください。
4. 接続アカウントの現在のパスワードを入力します。
5. **[Test Connection]** をクリックして、Log Server がそのアカウントを使用できることを確認してください。
6. **[OK]** をクリックして変更をキャッシュし、**[Save and Deploy]** をクリックしてそれらの変更を適用します。
7. Windows の [Services] ツールで **Websense TRITON - Web Security** サービスを再開します。

Microsoft SQL Server のユーザ許可の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Microsoft SQL Server Standard および Enterprise エディションは、ジョブ フレームワークのアクセス可能性を管理する SQL Server Agent のロールを定義します。SQL Server Agent のジョブは、SQL Server **msdb** データベースに保存されます。

Websense Log Server を正常にインストールするには、Websense データベースを所有するユーザ アカウントは、下記の要件を満たす必要があります。

1. **dbcreator** 固定 サーバー ロールのメンバーであること。
2. msdb データベースで：
   - **db_datareader** ロールのメンバーシップが割り当てられていること。
   - 以下のいずれかのロールのメンバーシップが割り当てられていること：
     - SQLAgentUser ロール
     - SQLAgentReader ロール
     - SQLAgentOperator ロール

正常に Log Server をインストールするために下記の手順を実行し、Microsoft SQL Server Management Studio を使用してデータベース ユーザー アカウントに必要な許可を与えます。

1. SQL Server がインストールされているコンピュータで、**[Start] > [Programs] > [Microsoft SQL Server 2008]** または **[Microsoft SQL Server 2012] > [Microsoft SQL Server Management Studio（Microsoft SQL Server 管理スタジオ）]** の順に選択します。
2. **[Object Explorer]** ツリーを選択し、**[Security（セキュリティ）] > [Logins（ログイン）]** を順に選択します。
3. インストール時に使用するログイン アカウントを選択します。
4. ログイン アカウントを右クリックし、このユーザの **[Properties（プロパティ）]** を選択します。
5. **[User Mapping（ユーザ マッピング）]** を選択し、下記の手順を実行します。
   a. データベース マッピングで **msdb** を選択します。
   b. メンバーシップに下記のいずれかのロールを割り当てます。
      - SQLAgentUser ロール
      - SQLAgentReader ロール
      - SQLAgentOperator ロール
   c. メンバーシップに **db_datareader** ロールを割り当てます。
   d. **[OK]** をクリックして、変更を保存します。
6. **[Server Roles（サーバ ロール）]** を選択し、次に **[dbcreator]** を選択します。dbcreator ロールが作成されます。
7. **[OK]** をクリックして、変更を保存します。

Log Server がディレクトリ サービスに接続できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

下記のどちらかのエラーが発生した場合、Log Server はディレクトリ サービスにアクセスできません。このアクセスは、レポートのユーザとグループの間のマッピングを更新するために必要です。これらのエラーは、Windows イ

ベント ビューア（*Windows イベント ビューア、651 ページ*を参照）に表示されます。

- EVENT ID：4096 - ディレクトリ サービスを初期化できません。Websense サーバが停止しているか、サーバに到達できません。
- EVENT ID：4096 - ディレクトリ サービスに接続できませんでした。この場合、このユーザのグループは解決されません。このプロセスがディレクトリ サービスにアクセスできることを確認してください。

最も一般的な原因は、Log Server と User Service が、アクセスを制限しているファイアウォールの反対側に置かれていることです。この問題を解決するには、ポート 55815 上のアクセスを許可するようにファイアウォールを設定します。

ディレクトリ サービス通信に使用するデフォルト ポートは、下記の通りです。

139	NetBIOS 通信：Active Directory
389	LDAP 通信：Active Directory、Novell eDirectory、Oracle（旧 Sun Java）Directory Server
636	SSL ポート：Novell eDirectory、Oracle（旧 Sun Java）Directory Server
3268	Active Directory
3269	SSL ポート：Active Directory

誤ったレポーティング ページが表示される

Web Security Help | Web Security ソリューション | バージョン 7.8.x

V シリーズのアプライアンスを開発した場合は、TRITON 管理サーバーがインストールされているコンピュータと Log Server がインストールされているコンピュータのタイム ゾーン設定がアプライアンスのタイム ゾーンと一致しなければなりません。

これらのタイム ゾーン設定が同期されていない場合、管理者が Web Security manage で **[Reporting] > [Investigative Reports（調査レポート）]** ページまたは **[Settings] > [Reporting] > [Log Database]** ページを開こうとした時、誤ったページが表示されます。想定していた機能の代わりに、ログオン ページまたは [login failed（ログインが失敗しました）] メッセージが表示されます。

この問題を解決するには、TRITON 管理サーバー と Log Server がインストールされている各コンピュータのタイム ゾーンをアプライアンスのタイム ゾーンに一致させるように更新し、次にオフボックス サービスを再開します。

調査レポートとプレゼンテーション レポートの問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Presentation Reports Scheduler がログ データベースに接続されていない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ヘルス アラートによって Presentation Reports Scheduler がログ データベースから切断されていると警告された場合は、この問題を解決するまでプレゼンテーション レポートにスケジュール設定されているすべてのジョブを作成しては**いけません**。

この接続が切断された時にプレゼンテーション レポートで作成したスケジュール設定されたジョブは一時的にのみ保存されますが、ログ データベースには書き込むことができず、永久的には保存されません。そのため、TRITON コンピュータを再起動する時、または Websense TRITON - Web Security サービスを再開する時にジョブ定義は失われます。

データベース エンジンが実行していること、ネットワーク上の問題が解決されたことを確認してください。次に、Websense TRITON - Web Security サービスを再開します。

1. TRITON がインストールされているコンピュータで、Windows の [Services] ツールを開きます。
2. サービスのリストから **[Websense TRITON - Web Security]** を選択します。
3. ツールバーの [Restart（リスタート）] ボタンをクリックします。
4. サービスが開始した後、[Services] ツールを閉じます。

プレゼンテーション レポートを作成するときディスク スペースが足りない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

デフォルトでは、プレゼンテーション レポートを作成するために、Websense ソフトウエアは、TRITON コンピュータ上の下記のフォルダのスペースを使用します。

```
C:\Program Files (x86)\Websense\Web Security\ReportingOutput
```

この場所で利用できるスペースが 1 GB 未満になった場合は、[Status] > [Dashboard] ページの [System] タブの [Health Alert Summary（ヘルス アラートの要約）] に警告メッセージが表示されます。

このメッセージが表示された場合は、プレゼンテーション レポートの作成上の問題または他のシステム パフォーマンス上の問題を避けるために、TRITON がインストールされているコンピュータの適切なディスクでディスク スペースをクリアします。

プレゼンテーション レポートでスケジュール設定したジョブが失敗

Web Security Help | Web Security ソリューション | バージョン 7.8.x

プレゼンテーション レポートで 1 つ以上のスケジュール設定したジョブが正常に実行できなかった場合は、[Status] > [Dashboard] ページの [System] タブの [Health Alert Summary] に警告メッセージが表示されます。

スケジュール設定されたジョブは、下記のように、様々な理由で失敗することがあります。

- 電子メール サーバー情報が [Settings] > [Reporting] > [Preferences（優先設定）] ページで設定されていなかった。手順については、*レポートの優先設定、503 ページ*を参照してください。
- プレゼンテーション レポートを作成するには TRITON がインストールされているコンピュータ上のディスク スペースが足りない。詳細は、*プレゼンテーション レポートを作成するときディスク スペースが足りない、617 ページ*を参照してください。

- ログ データベースとの接続が失われている。詳細は、*Policy Server に Log Server がインストールされていない、604 ページ*を参照してください。
- 構成された電子メール サーバーが実行していない。システム管理者と共にこの問題を解決してください。

どのジョブが失敗したかを見つけるために、**[Presentation Reports（プレゼンテーション レポート）] > [Job Queue（ジョブ キュー）]** ページを順に選択します。

- 既知の問題が解決した場合は、失敗したジョブのチェック ボックスをオンにして、**[Run Now（すぐに実行）]** をクリックしジョブを再度実行します。
- 失敗したジョブの **[Details（詳細）]** リンクをクリックして、[Job History（ジョブ履歴）] ページを表示します。このページは選択したジョブの最近の実行履歴に関する情報を表示します。

インターネット ブラウズ時間のレポートのデータが不正確である

Web Security Help | Web Security ソリューション | バージョン 7.8.x

集約の結果、インターネット ブラウズ時間レポートのデータが不正確になることがあります。これらのレポートはユーザーがインターネット アクセスに費やした時間を示し、各サイトで費やした時間の詳細を含めることもできます。インターネット ブラウザ時間は特別なアルゴリズムを使って計算されますが、集約を有効にすると、これらのレポートの計算の正確さが損なわれることがあります。

帯域幅が予想より大きい

Web Security Help | Web Security ソリューション | バージョン 7.8.x

多くの Websense 統合製品は、帯域幅情報を提供します。統合製品が帯域幅情報を提供しない場合、Network Agent が帯域幅データを含むログ記録を実行するように設定することができます。

ユーザーが許可されたファイルのダウンロードを要求したとき、統合製品または Network Agent は完全なファイル サイズを送信し、Websense ソフトウェアはそれを受信バイト数としてログ記録します。

ユーザーがその後、実際のダウンロードをキャンセルした場合、またはファイルが完全にはダウンロードされなかった場合でも、ログ データベースに保存される受信バイト数は完全なファイル サイズを表します。このような場合、報告される受信バイト数は、実際の受信バイト数よりも大きくなります。

これは報告される帯域幅の値にも影響します。報告される帯域幅は受信バイト数と送信バイト数の組み合わせです。

トレンド データがログ データベースからなくなっている

Web Security Help | Web Security ソリューション | バージョン 7.8.x

トレンド データは最初は ETL ジョブ（毎日のトレンド データを生成）によって、次にトレンド ジョブ（週間、月間、年間テーブルを生成）によってログ データベースに挿入されます。それによってこのデータはプレゼンテーション トレンド レポートで使用されます。

データベースのトレンド データがない、または一部のトレンド データが欠落している場合は、下記の事柄を確認します。

- Web Security manager の [Settings] > [Reporting] > [Log Database] ページでトレンド データーの保持を有効化していたかどうか確認します。トレンド データを作成および保存するためには、**[Store trend data（トレンド データを保存）]** チェック ボックス（[Trend Data Retention（トレンド データ保持）] の下）をオンにしなければなりません。
- Microsoft SQL Server **Standard** または **Enterprise** を使用している場合は、SQL Server Agent サービスが実行していること、またそれが正しいユーザーとして実行していることを確認してください。*Microsoft SQL Server のユーザ許可の設定、613 ページ*および *SQL Server Agent のジョブ、621 ページ*を参照してください。

  Windows の [Services] ツールを使って、**SQL Server Agent** サービスが実行していることを確認します。
- **ETL** および **trend** データベースのジョブが実行していることを確認してください。

  ETL j ジョブは毎日のトレンド データを生成し、またトレンド ジョブは夜間に実行し、週間、月間、月間、年間のトレンド値を生成します。SQL Server Management Studio を使用して、両方のジョブが実行していることを確認します。それらのジョブが実行していない場合は、ジョブ履歴でエラーがないか確認し、ジョブを再開するか、ジョブを手動で実行します。詳細は*最後に成功した ETL ジョブが 4 時間以上前に実行された、611 ページ*を参照してください。

トレンド レポートがデータを表示しない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

プレゼンテーション レポートを使用している場合は、日別、月別、年別のトレンド情報を表示するトレンド レポートを作成できます。これらの各期間のトレンド データを保持するログ データベースには個別のテーブルがあります。

作成するトレンド レポートにデータが含まれていない場合は、最初に下記の事柄について確認してください。

- *すべてのレポートが空白である、620 ページ*
- *プレゼンテーション レポート作成エラー、またはレポートが表示されない、624 ページ*
- *トレンド データがログ データベースからなくなっている、619 ページ*

これらのトピックが問題を突き止めるのに役立たない場合は、下記の事柄について確認してください。

- 実行しているレポートが有効なデータを保持するトレンド期間として定義されていること。

  トレンド データの保持期間は 4 つの期間から選択でき、それによって 1 日、1 週間、1 カ月、1 年間のレポートを定義できます。実行しているトレンド レポートとして選択した期間オプションのトレンド データがあることを確認してください。
- プレゼンテーション レポートがログ データベースに接続さていること。

  ログ データベースへの接続が失われた場合、プレゼンテーション レポートのツールはレポートを作成できません。*Log Database を使用できない、607 ページ*を参照してください。
- レポートを作成および保存するために使用できるディスク スペースがあること。

  プレゼンテーション レポート ツールはレポートを生成する時、ディスクに書き込みます。*プレゼンテーション レポートを作成するときディスク スペースが足りない、617 ページ*を参照してください。

一部のプロトコル要求がログ記録されない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

一部のプロトコル、たとえば ICQ や AOL が使用するプロトコルは、ユーザーに対して 1 つの IP アドレスを使ってサーバーにログインし、次に、クライアントに対してメッセージングのために異なる識別用 IP アドレスおよびポート番号を送信することを要求します。この場合、送信および受信されたメッセージの一部は Websense Network Agent によって監視およびログ記録されません。なぜなら、メッセージの交換時に、メッセージを送信しているサーバーが認識されていないからです。

その結果、ログ記録された要求の数と実際に送信された要求の数が一致しないことがあります。これは Websense レポーティング ツールによって生成されるレポートの正確さに影響します。

すべてのレポートが空白である

Web Security Help | Web Security ソリューション | バージョン 7.8.x

すべてのレポートにデータがない場合、下記のことを確認してください。

- アクティブなデータベース パーティションが、レポートに含まれる日付の情報を含んでいること。*データベースのパーティション、621 ページ*を参照してください。
- Microsoft SQL Server がインストールされているコンピュータで SQL Server Agent ジョブがアクティブであること（このサービスは SQL Server Express では使用されません）。*SQL Server Agent のジョブ、621 ページ*を参照してください。
- Log Server が Filtering Service からログ情報を受信するために正しく設定されていること。*Log Server の設定、622 ページ*を参照してください。

データベースのパーティション

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense ログ レコードは、データベース内のパーティションで保存されます。データベース エンジンおよび構成に従って、サイズまたは日付を基準にして新しいパーティションを作成できます。

Web Security manager で個別のパーティションをアクティブにしたり非アクティブにすることができます。非アクティブにされたパーティションに保存されている情報を基にしてレポートを生成しようとすると、情報が見つからず、レポートは空白になります。

必要なデータベース パーティションがアクティブになっていることを確認するには、下記の手順を実行します。

1. **[Settings] > [Reporting] > [Log Database]** を順に選択します。
2. **[Available Partitions（使用可能なパーティション）]** セクションにスクロールします。
3. レポートに含めるデータを含む各パーティションの **[Enable（有効化）]** チェック ボックスをオンにします。
4. **[Save Now]** をクリックし、変更を適用します。

SQL Server Agent のジョブ

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Microsoft SQL Server の Standard または Enterprise エディションを使用している場合は、SQL Server Agent データベース ジョブが無効化されている可能性があります。ETL データベース ジョブによってログ レコードをデータベースに保存するためには、このジョブが実行している必要があります。

1. **[Start] > [Administrative Tools] > [Services]** を順に選択します。
2. MSSQLSERVER と SQLSERVERAGENT の両方のサービスが開始されていることを確認します。

3. SQLSERVERAGENT のスタートアップ タイプが **[Automatic]** に設定されていることを確認します（**スタートアップ タイプ**情報を含む [Properties（プロパティ）] ダイアログ ボックスを開くには、[Services] リストのサービス名をダブルクリックします）。

   それによって Microsoft SQL Server またはデータベース エンジンがインストールされているコンピュータが再起動されるたびに、SQL Server Agent が再起動することを確認します。

SQL Server がインストールされているコンピュータにアクセスできない場合は、データベース管理者に、SQL Server Agent ジョブが実行していること、および自動スタートアップとして設定されていることを確認するよう依頼してください。

Log Server の設定

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Log Server が Filtering Service サービスからログ情報を受信するには、Web Security manager と Log Server の両方で設定が正しく設定されていなければなりません。そうでない場合は、ログ データはログ データベースに保存されません。

最初に、Web Security manager が Log Server に正常に接続されていることを確認します。

1. 無条件の優先管理者の許可を使って Web Security manager にログオンします。
2. **[Settings] > [General] > [Logging（ログ記録）]** ページを順に選択します。
3. Log Server がインストールされているコンピュータの IP アドレスまたはホスト名を入力してください。
4. Log Server をリッスンするポートを入力します（デフォルトでは **55805**）。
5. Web Security manager が指定された Log Server と通信可能かを判断するためには、**[Check Status（ステータスを確認）]** をクリックします。

   接続テストを成功したかどうかを知らせるメッセージが表示されます。必要なら、テストが成功するまで、IP アドレスまたはコンピュータ名とポートを更新します。
6. 完了したら、**[OK]** をクリックして変更をキャッシュします。**[Save and Deploy]** をクリックするまで、変更は適用されません。

次に Log Server の設定を確認します。

1. **[Settings] > [Reporting] > [Log Server]** ページを順に選択します。
2. **[Location（場所）]** の下の **[Port（ポート）]** が [Settings] > [General] > [Logging] ページの値と一致することを確認します。

3. **[OK]** をクリックして変更を確認およびキャッシュし、**[Save and Deploy]** をクリックしてそれらの変更を適用します。
4. Log Server ポートの設定を変更した場合は、Windows の [Services] ツールを使用して、**Websense Log Server** サービスと **Websense TRITON - Web Security** サービスを再開します。

Microsoft Excel 出力に一部のレポート データがない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Microsoft Excel ワークシートで開けることができる最大の行数は、65,536 行です。65,536 を超えるレポートを Microsoft Excel フォーマットにエクスポートする場合、65,537 行目以降のレコードはワークシートに表示されません。

エクスポートしたレポートのすべての情報にアクセスできるようにするには、下記のいずれかの手順を実行します。

- プレゼンテーション レポートでは、より小さなレポートを定義するようにレポート フィルタを編集します。そのためには、より短い日付範囲を設定するか、より少ないユーザーおよびグループを選択するか、またはより少ないアクションを選択します。
- 調査レポートでは、より小さなレポートを定義するようにデータを絞り込みます。
- 別のエクスポート形式を選択します。

プレゼンテーション レポート出力を HTML ファイルに保存する

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Reporting] > [Presentation Reports] ページから直接にレポートを生成する場合、表示形式を HTML、PDF、XLS の 3 種類から選択できます。HTML 表示形式を選択した場合、レポートを Web Security manager に表示できます。

ブラウザからプレゼンテーション レポートを印刷および保存することは推奨されません。印刷出力にブラウザ ウィンドウ全体が含まれ、保存されているファイルを開くと TRITON コンソールが起動します。

レポートをより効率的に印刷または保存するには、出力フォーマットとして PDF または XLS を選択してください。表示ソフトウェア（Adobe Reader または Microsoft Excel）がローカル コンピュータにインストールされている場合は、即座にこれらの形式のファイルを開くことができます。また、ファイルをディスクに保存することもできます（適切な表示ソフトウェアがインストールされていない場合は、これが唯一のオプションです）。

Adobe Reader または Microsoft Excel でレポートを開いた後、そのプログラムの印刷および保存オプションを使用して、希望する最終出力を作成できます。

プレゼンテーション レポート作成エラー、またはレポートが表示されない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

プレゼンテーション レポートにはレポートを即時実行するために、レポートをバックグラウンドで実行するようにスケジュール設定する（デフォルト）、とスケジュール設定せずにレポートを実行する（デフォルトのオプションを選択解除した場合）の 2 つのオプションがあります。

スケジュール設定せずに（フォアグラウンドで）レポートを実行し、HTML 形式を選択している場合、レポートはコンテンツ ペインに表示されます。PDF または XLS 形式を選択した場合、レポートを開くか保存することを選択できます。場合によっては、完全なレポートが表示される代わりに下記のどちらかのメッセージが表示されます。

- メッセージ [error generating report（レポート作成エラー）] が表示されます。
- [report complete（レポート完了）] メッセージが表示されますが、レポートは表示されません。

この問題が発生した場合は、Web Security manager の [Presentation Reports] ページから移動して、レポートを再び実行します。それによってレポートを表示しなかった場合は、TRITON コンソールからログ オフしてから再度ログオンし、レポートを再び実行します。

問題が解決しない場合は、下記の処置を行うことができます。

- **[Schedule the report to run in the background（レポートをバックグラウンドで実行するようにスケジュール設定する）]** オプションを使用し、[Review Reports（レポートを確認）] ページからレポートを開きます。
- レポートを作成するとき、Internet Explorer ではなく、Firefox または Chrome を使用します。

調査レポートの検索の問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

[Investigative Reports] のメイン ページの棒グラフの上の [Search（検索）] フィールドを使用して、選択したグラフの要素内の特定の語またはテキスト文字列を検索できます。調査レポートの検索に関連して、次の 2 つの問題が起きる可能性があります。拡張 ASCII 文字と検索パターン マッチング。

- Linux コンピュータ上で Mozilla Firefox を使用して Web Security manager にアクセスしている場合は、これらのフィールドに拡張 ASCII 文字を入力できません。これは、Linux 上の Firefox の既知の制限です。

調査レポートで拡張 ASCII 文字を含む文字列を検索する必要がある場合は、サポートされているブラウザを使って Windows コンピュータから Web Security manager にアクセスしてください。

- 調査レポートでは、調査レポートのメイン ページの [Search] フィールドに入力されたパターンに関連付けられた URL を検索できない場合があります。そのような場合は、レポートされた URL 内にそのパターンが存在することが確実であれば、その URL を検索できる別のパターンの入力を試みます。

調査レポートに関する一般的な問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

- 一部のクエリに非常に長い時間がかかる空白画面が表示されたり、クエリがタイムアウトになったことを知らせるメッセージが返されることがあります。この問題には、下記の原因が考えられます。
  - Web サーバーのタイムアウト
  - Microsoft SQL Server のタイムアウト
  - プロキシまたはキャッシング サーバのタイムアウト

  手動でこれらのコンポーネントのタイムアウト制限値を大きくする必要があります。
- ユーザーがどのグループにも属していない場合、ドメインにも表示されません。グループとドメインの両方の選択が非アクティブになります。
- Log Server がヒット件数の代わりにアクセス数をログ記録している場合でも、調査レポートでこの情報に付けられるラベルは **[Hits（ヒット件数）]** です。

他のレポーティングの問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

- *Real-Time Monitor がインストールされているコンピュータのメモリが不足している、626 ページ*
- *Real-Time Monitor が実行しない、626 ページ*
- *Real-Time Monitor が応答しない、627 ページ*
- *特定のレポート作成機能にアクセスできない、628 ページ*
- *[Status] > [Dashboard] ページにグラフが表示されない、628 ページ*
- *フォレンシック データ構成の問題がある、628 ページ*
- *フォレンシック リポジトリの位置に到達できなかった、629 ページ*
- *フォレンシック データがまもなくサイズ制限または経過日数制限を超える、629 ページ*
- *Websense Multiplexer が実行しない、または利用できない、629 ページ*

Real-Time Monitor がインストールされているコンピュータのメモリが不足している

Web Security Help | Web Security ソリューション | バージョン 7.8.x

このアラートは、Real-Time Monitor がインストールされているコンピュータ上の使用可能なメモリが全メモリ 15% 以下になったときに表示されます。メモリの不足によって Real-Time Monitor が一部またはすべてのレコードを受信、表示、および保存するのを妨げられることがあります。

それによってモニタに表示されるデータに空白ができたり、モニタのサーバーおよびデータベース コンポーネントが実行できなくなることがあります。

Windows Task Manager を使用して、Real-Time Monitor がインストールされているコンピュータのメモリ使用率を評価します。問題を解決するために、下記の処置を実行できます。

- コンピュータの RAM をアップグレードする。
- 高いメモリ要件をもつアプリケーションまたはコンポーネントを他のコンピュータに移動する。

Real-Time Monitor をより多くの使用可能なメモリを備えたコンピュータに移動する。

Real-Time Monitor が実行しない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

このアラートは、Websense RTM Server サービスが停止した時に表示されます。

Real-Time Monitor の 3 つのすべてのサービスが開始されたこと、および停止していた下記のいずれかのサービスが開始することを確認するとき、Windows の [Services] ツールを使用します。

- Websense RTM Database
- Websense RTM Server
- Websense RTM Client

いすれかのサービスが開始しない場合は、下記の事柄を確認します。

- Windows Event Viewer で Websense RTM Server からエラーや警告がないかチェックします。
- **WebsenseRTMMemoryOutput0.log** ファイル（デフォルトでは C:\Program Files **または** Program Files（x86）\Websense\Web Security\rtm\logs directory ディレクトリにあります）で Real-Time モニタのメモリ使用率に関する情報をチェックします。
- サービスを実行するために使用できる十分なリソース（メモリ、ハードディスク、および CPU）があることを確認します。

サービスは実行しているが、アラートが表示され続ける場合は、Real-Time Monitor が Policy Server に登録できなかったことを示す場合があります。この Real-Time Monitor インスタンスに関連付けられた Policy Server が実行していること、Real-Time Monitor がインストールされているコンピュータ と Policy Server がインストールされているコンピュータがポート 55836（暗号化通信）上または 55856（非暗号化通信）上で通信できることを確認します。

サービスが開始しない場合は、それらのサービスが **[Automatic]**（Manual でない）スタートアップとして設定されていることを確認します。

Real-Time Monitor が応答しない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Real-Time Monitor が、TRITON Unified Security Center がインストールされているコンピュータとは別のコンピュータにインストールされている場合は、ping コマンド を使用して 2 つのコンピュータがネットワークを通じて通信できることを確認します。また TRITON がインストールされているコンピュータと Real-Time Monitor がポート 9445 上（ユーザー インタフェース表示用）で通信できることを確認します。

また、Real-Time Monitor は下記のポートと通信できる必要があります。

- Usage Monitor のポート 55835
- Policy Server のポート 55836（暗号化通信の場合）、またはポート 55856（非暗号化通信の場合）

ネットワーク通信の問題がない場合は、Real-Time Monitor にリソース上の制限がある場合があります。

- Real-Time Monitor がインストールされているコンピュータのメモリ、CPU 使用率、使用可能なディスク スペースをチェックしてください。

  RTM Database は最大 10,000 個のレコードを保持でき、使用可能なディスクス ペースへの影響を制限するのに役立ちます。
- データベースが過度に多くの要求を受け取るか、または追加の接続を受け入れることができないことがあります。

  Windows Event Viewer が Websense RTM Database のエラーを示す場合は、その問題に対処するためにサービスを再開できます。

  データベースが再起動したとき、すべてのレコードがクリアされますから、古いデータは失われます。Real-Time Monitor で表示できないデータもログ データベースには保存されており、調査およびプレゼンテーション レポートでは表示できます。

特定のレポート作成機能にアクセスできない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Web ブラウザでポップアップ ブロッキングが非常に厳格に設定されているとき、特定のレポート作成機能がブロックされることがあります。これらの機能を使用するには、ブロッキング レベルを低くするか、ポップアップ ブロッキングを完全に無効化する必要があります。

[Status] > [Dashboard] ページにグラフが表示されない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

一般的に、[Status] > [Dashboard] ページは、Web Security 配備のステータスを示すグラフおよび他の要素を表示します。

- Websense Web Security ソリューションを配備した直後には、表示するレポート データがない可能性があります。トラフィックが現在ログ記録されているかどうかを確認するには、TestLogServer などのツールを使用します。その手順については、技術関連記事『Using TestLogServer for Web Security Troubleshooting』を参照してください。
- 指定済み管理を使用する組織では、指定済み管理者のロールに対するレポート作成許可を確認します。**[View dashboard charts（ダッシュボード グラフを表示）]** が選択されていない場合は、そのロールの指定済み管理者の画面にはこれらのグラフは表示されません。
- TRITON コンソールがログ データベースとの接続を失った場合（たとえば、ネットワーク関連の問題のため、またはデータベースをホストしている Microsoft SQL Server がダウンしたため）、データを表示できません。ログ データベースに関連するアラートについて [Status] > [Alerts] ページをチェックします。

フォレンシック データ構成の問題がある

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Web Security manager の **[Settings] > [Reporting] > [Dashboard]** ページでフォレンシック データ収集が有効化されている場合、ネットワーク外へのデータ送信の試みに関連するトランザクションの詳細、および関連する実際のデータ ファイルがフォレンシック リポジトリに記録されます。

稀に、このフォレンシック データの収集および格納に使用されるファイルが損傷または破損していることがあります。そのような問題を解決するには、Websense テクニカル サポートの支援が必要です。

フォレンシック リポジトリの位置に到達できなかった

Web Security Help | Web Security ソリューション | バージョン 7.8.x

フォレンシック データ収集が Web Security manager の **[Settings] > [Reporting] > [Dashboard]** ページで有効化されている場合、管理者は、ファイルを保存するための場所（ローカル ディレクトリまたは UNC パス）、および指定したディレクトリへの読み取り、書き込み、および削除の許可をもつアカウントの資格情報を提供します。

ヘルス アラートがフォレンシック リポジトリの場所の到達に関する問題を示す場合は、下記の事柄を確認します。

- [Settings] > [Reporting] > [Dashboard] ページのパスおよび資格情報が正しいこと。
- 指定したアカウントがディレクトリへの読み取り、書き込み、および削除の許可を持っていること。
- TRITON Management Server とリモート コンピュータの間いの通信を妨げるネットワーク上の問題がないこと。

フォレンシック データがまもなくサイズ制限または経過日数制限を超える

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Web Security manager の **[Settings] > [Reporting] > [Dashboard]** ページでフォレンシック データ収集を有効化した場合、管理者は、リポジトリの最大サイズ（単位 GB）とフォレンシック データを保存する最大時間（単位 日数）の両方を設定します。

フォレンシック リポジトリのサイズが制限に到達した時、ヘルス アラートが表示されます。制限に達した時、新しい着信レコードを保存するためのスペースができるまで、最も古いレコードが 1 日分ずつ削除されます。ます。

サイズ制限に達していないが、レコードが最大レコード経過日数に近づいている場合も、ヘルス アラートが表示されます。経過日数制限に達したとき、その制限を超えるレコードが削除されます。

削除されたフォレンシック データを復元する方法はありません。

Websense Multiplexer が実行しない、または利用できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Web Security のソリューションとして SIEM の統合を有効化した場合、Websense Multiplexer は、インターネット アクティビティ データを Filtering Service から Log Server と 構成された SIEM 製品の両方に送信します。

Multiplexer が実行していないか、または利用可能でない場合は、フェイルオーバー機能によって、Filtering Service がログ データを Log Server に送信するようにします。しかし SIEM 製品にはデータが送信されません。

Websense アプライアンスベースの環境でこの問題を解決するには、下記の手順を実行します。

1. Multiplexer サービスを有効化していなかった場合は、Appliance Manager の **[Administration（管理）] > [Toolbox（ツールボックス）] > [Command Line Utility（コマンド ライン ユーティリティ）]** を順に選択します。

   [multiplexer] を選択し、**enable** コマンドを使用します。
2. Multiplexer サービスを有効化しているが、実行していない場合は、Appliance Manager の **[Status] > [General]** ページを順に選択し、Websense Web Security モジュールを再起動します。

ソフトウェアのみを配備している場合に、この問題を解決するには下記の手順を実行します。

1. 下記のどちらかの該当する手順を実行し、Multiplexer サービスまたはデーモンを開始または再開します。
   - Windows の場合：[Services] ツールを使用して、**Websense Multiplexer** サービスを開始（または再開）します。
   - Linux の場合：/opt/Websense/**WebsenseDaemonControl** コマンドを使用して、**Multiplexer** を開始（または再開）します。
2. サービスを再開できない場合は、Multiplexer Controller 実行可能ファイルが反応しなくなっている可能性があります。
   - Windows の場合：Task Manager を使用して **MuxCtrl.exe** プロセスを停止し、[Services] ツールを使用して **Websense Multiplexer** を再開します。
   - Linux の場合：**MuxCtrl** プロセスを停止し、/opt/Websense/**WebsenseDaemonControl** コマンドを使用して **Multiplexer** を開始します。

相互運用性の問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Content Gateway が実行していない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Content Gateway インスタンスが Policy Server に登録するとき、接続は Web Security manager で追跡されます。Content Gateway インスタンスに関する情報は、[Settings] > [General] > [Content Gateway Access（Content Gateway アクセス）] ページ、および [Status] > [Dashboard] ページの [System] タブの [Filtering Service Summary（Filtering Service の要約）] に表示されます。

登録されたインスタンスが停止した場合または削除された場合は、ヘルス アラート メッセージが Web Security manager に表示されます。

- インスタンスが突然指定した場合は、Content Gateway がインストールされているコンピュータの **syslog** ファイルで障害の原因に関する情報をチェックしてください。
- Content Gateway を他の IP アドレスまたは他の物理的コンピュータに移動した場合、または不必要なインスタンスを削除した場合、ヘルス アラートを表示させないために、[Settings] > [Genera] > [Content Gateway Access] ページからインスタンスを手動で削除できます。

Content Gateway を使用できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Content Gateway インスタンスが Policy Server に登録するとき、接続は Web Security manager で追跡されます。Content Gateway インスタンスに関する情報は、[Settings] > [General] > [Content Gateway Access（Content Gateway アクセス）] ページ、および [Status] > [Dashboard] ページの [System] タブの [Filtering Service Summary（Filtering Service の要約）] に表示されます。

Web Security のコンポーネントが登録されているインスタンスと通信できなくなる場合、Web Security manager にヘルス アラート メッセージが表示されます。

- Content Gateway がインストールされているコンピュータが起動していること、および Content Gateway が実行していることを確認してください。
- このアラートはネットワーク上の問題を示すことがあります。Content Gateway が Policy Server（ポート 55806 および 55880）および Filtering Service（ポート 15868）がインストールされているそれぞれのコンピュータと通信できることを確認してください。

Content Gateway のクリティカルでないアラート

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Content Gateway からクリティカルでないアラートを受け取りましたという通知を受け取った場合は、下記のいずれかのエラーまたは状態が発生した可能性があります。どのエラーが発生したかを判断するために、影響を受けた Content Gateway インスタンスに関連付けられている Content Gateway manager をチェックします。

下記の表を使用してエラー状態の概要を把握します。詳細については、Content Gateway がインストールされているコンピュータのシステム ファイル、エラー ファイル、およびイベント ログ ファイルを参照してください。

アラート	説明
Content Gateway process reset（Content Gateway のプロセスがリセットしました）	Content Gateway を再起動せる問題が発生しました。 リセットさせた原因については、Content Gateway syslog ファイルを参照してください。
Cache configuration issue（キャッシュ構成の問題）	Content Gateway がキャッシュを構成できなくなりました。 詳細については、Content Gateway Manager Help の [Configuring the Cache（キャッシュの構成）] を参照してください。

アラート	説明
Unable to create cache partition （キャッシュ パーティションを作成できません）	キャッシュ構成中にエラーが発生しました。 Content Gateway Manager Help の [Configuring the Cache] を参照してください。
Unable to initialize cache （キャッシュを初期化できません）	キャッシュ エラーが発生しました。 Content Gateway は、キャッシュ ディスク上のディスク障害を許容します。ディスクが完全に壊れた場合、Content Gateway はそのディスクに [破損] を表すマークを付け、残りのディスクを引き続き使用します。 Content Gateway Manager Help の [Configuring the Cache] を参照してください。
Unable to open configuration file （設定ファイルを開くことができません）	設定ファイルに問題があります。 • 影響を受けたファイルの詳細については、システム ログをチェックしてください。 • ファイルまたはディレクトリにアクセスする許可が変更された可能性があります。 • ファイルが Content Gateway manager の外部で編集された場合、無効な構文や他の問題のためにファイルの読み取りができなくなる可能性があります。
Invalid fields in configuration file （設定ファイルに無効なフィールドがあります）	設定ファイルの 1 つ以上のパラメータまたはパラメータ値が不適切です。 影響を受けたファイルの詳細については、システム ログをチェックしてください。
Unable to update configuration file （設定ファイルを更新することができません）	設定ファイルを保存するのを妨げる問題があります。 影響を受けたファイルの詳細については、システム ログをチェックしてください。
Clustering peer operating system mismatch （クラスタ内のピア オペレーティング システムのミスマッチ）	クラスタ内のノードは均質で、下記の要素が同じである必要があります。 • ハードウェア プラットフォーム • オペレーティング システム バージョン

アラート	説明
Could not enable virtual IP addressing（仮想 IP アドレス指定を有効化できませんでした）	Content Gateway は、仮想 IP アドレス フェイルオーバーを有効化しようとしましたが、できませんでした。 この問題は、指定された仮想 IP アドレスがネットワークですでに使用されている場合に発生します。 仮想 IP アドレスは、他のすべての IP と同様に、Content Gateway に割り当てる前に事前予約されていなければなりません。
Connection throttle too high（接続スロットルが高すぎます）	クライアントまたはオリジン サーバーの接続が設定された接続制限値の半分の 90 %（デフォルトでは 45000）に到達したとき、接続スロットル イベントが発生します。 接続スロットル制限を高くする場合、システムは必要なクライアント接続を処理するために十分なメモリを備えている必要があります。RAM の制約があるシステムでは、スロットル制限値をデフォルト値より低くしなければならない場合があります。
Host database disabled（ホスト データベースが無効化されています）	ホスト データベースは、プロキシが接続するオリジン サーバーの Domain Name Server（DNS）エントリを保存します。ホスト データベースは、下記の情報を追跡します。 • DNS 情報（ホスト名を IP アドレスにすばやく変換するため） • 各ホストの HTTP バージョン（最新のプロトコル機能を、種々のサーバーを実行しているホストで使用できるようにするため） • ホストの信頼性および可用性情報（機能していないサーバーからの応答待ちを避けるため）
Logging configuration error（ログ記録設定エラー）	トランザクション、エラー、またはその両方を指定した場所にログ記録するように Content Gateway を設定できます。 ログ記録の詳細については、Content Gateway Manager Help の [Working with Log Files（ログ ファイルの処理）] を参照してください。

アラート	説明
Unable to open Content Gateway Manager （Content Gateway Manager を開くことができません）	Content Gateway が Web インタフェースを起動するための管理 API 呼び出しを処理するためのソケットをセットアップできません。
ICMP echo failed for a default gateway （デフォルト ゲートウェーの ICMP エコーが失敗しました）	クラスタの仮想 IP アドレスの割り当て中に Content Gateway ノードがそのデフォルト ゲートウェイと通信できませんでした。ノードがシャット ダウンします。
HTTP origin server is congested （HTTP オリジン サーバーが輻輳状態です）	Content Gateway が Web プロキシ キャッシュとして配備されているとき、ユーザーによる Web コンテンツ要求は、宛先 Web サーバー（オリジン サーバー）への転送の途中で Content Gateway を通過します。 クライアントがキャッシュ内の古くなった HTTP オブジェクトを要求した場合、Content Gateway はそのオブジェクトを再確認し、オブジェクトが変更されていないかどうかをオリジン サーバーに問い合わせます。 オリジン サーバーが輻輳状態になり（追加の接続を受け入れることができなくなり）再確認の問い合わせに応答しない場合、プロキシは確認を実行せず、キャッシュから古くなったオブジェクトを提供します。
Congestion alleviated on the HTTP origin server（輻輳が HTTP オリジン サーバーで緩和されました）	以前に接続の試みを拒否したオリジン サーバーが現在要求を再び受け入れるようになっています。
Content scanning skipped （コンテンツのスキャンがスキップしました）	Content Gateway は、通常スキャンされるはずの要求されたサイトのコンテンツのスキャンをしませんでした。 この問題は、Content Gateway への接続が過度に多く、システム リソース（CPU およびメモリ）が不十分であるとき発生することがあります。
WCCP configuration error （WCCP 設定エラー）	設定パラメータの詳細については、Content Gateway Manager Help の [WCCP Configuration（WCCP の設定）] のセクションを参照してください。

管理者が他の TRITON モジュールにアクセスできない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

TRITON コンソールで **[Data Security]** または **[Email Security]** をクリックしたとき、エラーを受け取った場合は、TRITON コンソールにログ オンするときに使用するローカルまたはネットワーク アカウントに、Data Security または Email Security へのアクセス許可が付与されていませんでした。

グローバル セキュリティ管理者は、管理者が TRITON モジュール間で切り替えできるように、[TRITON Settings] > [Administrators（管理者）] ページで管理者に各モジュールへの管理者アクセス権限を与える必要があります。

デフォルトの TRITON Unified Security Center 管理者アカウント **admin** にはすべてのインストールされているモジュールへの完全なアクセス権限があります。

詳細については、TRITON Console Help（TRITON の [Settings] ページの [Help] メニューから開くことができます）を参照してください。

User Service を使用できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Web Security Gateway Anywhere 環境では、Websense Sync Service がオンプレマイズ サービスとハイブリッド サービスの間の通信を行います。Sync Service は下記のことを行います。

- ポリシー設定データをハイブリッド サービスに送信する
- Directory Agent によって収集されたユーザー情報をハイブリッド サービスに送信する
- ハイブリッド サービスからレポーティング ログ レコードを受け取る。

まだハイブリッド サービス アカウントを有効にしていない場合、またはハイブリッド サービスのアクティブ化を試みたが成功しなかった場合、ローカル Websense ソフトウェア コンポーネントはハイブリッド サービスへの接続を確立する前に、Sync Service と通信できる必要があります。

この問題を解決するために、下記の事柄を確認してください。

- Sync Service が実行していること。
- Sync Service が正しい IP アドレスおよびポートに正常にバインドしていること。
  - Sync Service が使用する IP アドレスおよびポートは、Sync Service がインストールされているコンピュータの Websense **bin** ディレクトリにある **syncservice.ini** ファイルにリストされています。

- Web Security manager の [Settings] > [Hybrid Configuration（ハイブリッド設定）] > [Shared User Data（共有ユーザー データ）] ページに表示される IP アドレスおよびポートは、**syncservice.ini** ファイルにリストされる IP アドレスおよびポートと一致する必要があります。設定ファイルを更新した場合は、手動で [Settings] ページも更新します。
- **syncservice.ini** ファイルの IP アドレスおよびポートは、**das.ini** ファイル（Directory Agent がインストールされているコンピュータの Websense **bin** ディレクトリにあります）の Sync Service IP アドレスおよびポートの値と一致しなければなりません。

Sync Service がインストールされているコンピュータ上の他のどのサービスも、Sync Service が使用しようとしている IP アドレスおよびポートにバインドしていないことを確認してください。Sync Service が正しい IP アドレスおよびポートにバインドできないと思う場合は、サービスを停止し、コマンド プロンプトを開き、下記のコマンドを入力し、コンソール モードでサービスを再度開始してください。

```
syncservice -c
```

コンソール モードでは、Sync Service は、使用している IP アドレスおよびポートを表示するか、または IP アドレスおよびポートにバインドできなかった場合はエラーを表示します。

- Sync Service がインストールされているコンピュータは、ポート 55880 上で Policy Broker がインストールされているコンピュータと通信できます。
- Sync Service がインストールされているコンピュータは、ポート 55806 および 40000 上では Policy Broker がインストールされているコンピュータと通信できず、ポート 55830 および 55831 上で Policy Server からのデータを受信します。
- TRITON 管理サーバーがインストールされているコンピュータは ポート 55832 上で Sync Service がインストールされているコンピュータへの HTTP 接続を確立できます。

また Windows イベント ビューワまたは **websense.log** ファイルで Sync Service からのエラーをチェックします。

Sync Service をログ ファイルにダウンロードすることができなかった

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Sync Service は、設定した間隔でレポーティング ログ ファイルをダウンロードするためにハイブリッド サービスに接続しようとします（*ハイブリッド サービスとの通信のスケジュール設定、290 ページ*を参照）。Sync Service が接続できなかった場合、または Sync Service が接続の後ログ ファイルを取得できなかった場合、下記の問題が発生することがあります。

- ハイブリッド サービスは、ログ ファイルを 14 日間だけ保存します。その期間の後、そのファイルは削除され、復元することができません。そうなった場合は、組織はこれらのログに記録されたハイブリッド ポリシーの実施アクティビティに関して報告できなくなります。
- 組織がハイブリッド サービスを通じて送信するインターネット アクティビティの量に応じて、レポーティング ログ ファイルのサイズがすぐに大きくなることがあります。Sync Service が 1 日以上の間ログ ファイルをダウンロードできない場合、ファイルをダウンロードするために必要な帯域幅およびそれらを一時的に保存するために必要なディスク スペースがかなり大きくなります。

この問題に対処するには、**[Status] > [Hybrid Service（ハイブリッド サービス）]** ページで Sync Service がハイブリッド サービスに接続できるかどうか確認します。詳しいトラブルシューティングの手順については、*ハイブリッド サービスに接続できない、647 ページ*を参照してください。

Sync Service がハイブリッド サービスに接続しているが、ログ レコードを取得できない場合は、ハイブリッド サービスからの情報について、**[Status] > [Alerts（アラート）]** ページをチェックします。またハイブリッド サービス アカウントに関連付けられている管理電子メール アドレスもチェックします。

Sync Service が Log Server にデータを送信できなかった

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Sync Service は、ハイブリッド サービスからレポーティング ログ ファイルをダウンロードした後、そのファイルを Log Server に送信し、それらのファイルがログ データベースに送信されてレポートに含められるようにします。Sync Service が Log Server にデータを送信できなかった場合は、ログ ファイルが Sync Service がインストールされているコンピュータに集積し、多量のディスク スペースが消費される可能性があります。

- **telnet** コマンドを使用して、Sync Service がインストールされているコンピュータがポート **55885** 上で Log Server がインストールされているコンピュータに接続できることを確認します。
- Log Server が実行していること、および [Status] > [Alerts] ページに Log Server エラーが表示されていないことを確認してください。

ハイブリッド ポリシーの実施データがレポートに表示されない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ハイブリッド サービスによって処理されたインターネット アクティビティ情報がレポートに表示されない場合は、最初に下記の事柄を確認します。

- ハイブリッド ロギング ポートは、[Settings] > [General] > [Logging] ページで構成されていること。*要求がログ記録される方法の設定、505 ページ*を参照してください。
- **[Have the hybrid service collect reporting data for the clients it filters（ハイブリッド サービスがフィルタリング対象のクライアントのレポーティング データを収集するように設定する]）**チェック ボックスが [Settings] > [Hybrid Configuration] > [Scheduling（スケジュール設定）] ページで選択されていること。*ハイブリッド サービスとの通信のスケジュール設定、290 ページ*を参照してください。
- The **[Status（ステータス）] > [Hybrid Service]** ページに Sync Service がハイブリッド サービスに正常に接続されたこと、およびログ レコードが取得されたことが示されていること。*モニタのハイブリッド サービスとの通信、298 ページ*を参照してください。
- **[Status] > [Dashboard]** ページの [System] タブに Sync Service 通信の問題または Log Server のエラーを示すヘルス アラートが表示されていないこと。*Sync Service が Log Server にデータを送信できなかった、638 ページ*を参照してください。

分散ロギングを使用していて、複数の、リモート Log Server がデータを中央管理されている Log Server のインスタンスに送信する場合、Sync Service が中央の Log Server と通信するように設定されていることを確認します。ハイブリッド ログ記録データは、リモート Log Server インスタンスから中央 Log Server に送信することはできません。

Sync Service がインストールされているコンピュータでディスク スペースが不足している

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Sync Service がハイブリッド サービスによって収集されたレポーティング ログ ファイルを適時に送信できなかった場合は、ログ ファイルが Sync Service がインストールされているコンピュータに集積し、多量のディスク スペースが消費される可能性があります。この問題を避けるために、下記の事柄を行ってください。

- Sync Service が適切な間隔でハイブリッド サービスからレポーティング データを収集していることを確認します。組織がハイブリッド サービスを通じて送信するインターネット アクティビティが多ければ多いほど、より頻繁にログ ファイルをダウンロードして、バックログが大きくなるのを避ける必要があります。
- Sync Service がインストールされているコンピュータが Log Server が インストールされているコンピュータとポート **55885** で通信できることを確認します。
- 多量のレポーティング データが処理されるために Sync Service がインストールされているコンピュータに十分なリソースを割り当てます。

Sync Service 設定ファイル

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Web Security manager で設定できない Sync Service の動作を設定するには、**syncservice.ini** ファイルを使用します。

syncservice.ini ファイルは、Websense **bin** ディレクトリ（デフォルトでは C:\Program Files **または** Program Files（x86）\Websense\Web Security\bin）にあります。

- このファイルを編集するには、テキスト エディタを使用します。
- 変更を完了したとき、ファイルを保存して閉じ、Sync Service を再起動します。変更は、サービスが再開するまで有効になりません。

このファイルは下記の情報が含まれます。

- **SyncServiceHTTPAddress**：Sync Service が Directory Agent および Web Security manager と通信するためにバインドする IP アドレス。[Settings] > [Hybrid Configuration] > [Shared User Data] ページの Sync Service IP アドレスと一致しなければなりません。
- **SyncServiceHTTPPort**：Directory Agent および Web Security manager からの通信に対して Sync Service がリッスンする ポート（デフォルト 55832）。[Settings] > [Hybrid Configuration] > [Shared User Data] ページに表示される Sync Service ポートと一致しなければなりません。
- **UseSyncServiceProxy**：Sync Service がプロキシを通じてハイブリッド サービスに接続するかどうかを示します。値は、**true**（真）または **false**（偽）です。
  - **SyncServiceProxyAddress**：Sync Service がハイブリッド サービスに接続するとき通過するプロキシの IP アドレス。
  - **SyncServiceProxyPort**：Sync Service がホスト サービスに接続するとき通過するプロキシのポート。
  - **SyncServiceProxyUsername**：Sync Service がハイブリッド サービスとの通信するためにプロキシに接続するとき使用するユーザー名（必要な場合）。
  - **SyncServiceProxyPassword**：Sync Service がハイブリッド サービスと通信するためにプロキシに接続するとき使用するパスワード（必要な場合）。

Directory Agent が実行していない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Web Security Gateway Anywhere 環境では、Websense Directory Agent は、ディレクトリ サービスからユーザー情報を収集し、それを適用されているポリシーで使用するためにハイブリッド サービスに送信します。

Directory Agent が使用可能でない場合、ハイブリッド サービスのユーザー データが最新でなくなることがあります。

Make sure that Directory Agent がインストールされていること（ソフトウェア）または有効化されていること（アプライアンス）、およびサービスまたはデーモンが実行していることを確認します。

- Appliance の場合：Appliance Manager の **[Status] > [General]** ページを順に選択し、Websense Directory Agent が実行中のサービスとして示されていることを確認します。
  - Directory Agent が無効化されたサービス（薄いグレイ）としてリストされている場合は、**[Administration] > [Toolbox] > [Command Line Utility（コマンド ライン ユーティリティ）]** ページを順に選択し、**[directory-agent-service]** を選択し、次に **[enable]** を選択します。
  - Directory Agent は有効化されているが、実行していない場合は、Websense Web Security モジュールを再起動します。
- Windows の場合：Windows の [Services] ツールを使用して、サービスを開始するか、サービスが実行していることを確認します。
- Linux の場合：Use the **/opt/Websense/WebsenseDaemonControl** コマンドを使用してデーモンを起動するか、このデーモンが実行していることを確認します。

Directory Agent は実行しているが、アラート メッセージが引き続き表示される場合は、下記の事柄を確認します。

- Directory Agent がインストールされているコンピュータは Policy Server がインストールされているコンピュータと（ポート 40000 および 55806 で）通信できること。
- Directory Agent がインストールされているコンピュータは Sync Service がインストールされているコンピュータと（ポート 55832 で）通信できること。
- ファイアウォールが Directory Agent ポート（55900）で通信できること。

サービスは開始したが、まだ実行しない場合は、下記の事柄を確認します。

- [Administration] > [Logs（ログ）] ページ（アプライアンス）、イベント ビューア（Windows）、または websense.log ファイル（Linux）でエラーがないかチェックします。
- ソフトウェア インストールの場合は、Websense **bin** ディレクトリ（デフォルトでは C:\Program Files **または** Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）に移動し、**das.ini** ファイルがあること、および破損したり切り捨てられていないことを確認します。
- Directory Agent がインストールされているコンピュータにディレクトリの完全なスナップショットを保存するための十分なディスク スペースがあることを確認します。たとえば、200,000 個のユーザー ディレクトリのスナップショットは、約 100 MB のディスク スペースを必要とします。

- Directory Agent がその現在のスナップショットと以前のスナップショットを比較するために使用できる十分なメモリがあることを確認します。たとえば、200,000 個のユーザー ディレクトリのスナップショットを比較するには、約 100 MB のメモリを必要とします。

Directory Agent がドメイン コントローラに接続できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Directory Agent は、ディレクトリ サービスから情報を収集するためにドメイン コントローラに接続できなければなりません。Directory Agent がインストールされているコンピュータとドメイン コントローラがインストールさているコンピュータの間で通信上の問題がある場合は、ハイブリッド サービスのユーザー データが陳腐化し、ポリシーの実施が異常をきたすかもしれません。

この問題のトラブルシューティングを行うには、下記の事柄を確認します。

- Directory Agent がインストールされているコンピュータがドメインにバインドされていること、およびファイアウォールがディレクトリ サービス ポート上での通信を許可していることを確認します。

ポート	用途：
139	NetBIOS 通信：Active Directory
389	LDAP 通信：Active Directory、Novell eDirectory、Oracle（旧 Sun Java）Directory Server
636	SSL ポート：Novell eDirectory、Oracle（旧 Sun Java）Directory Server
3268	Active Directory
3269	SSL ポート：Active Directory

- Web Security manager の **[Settings] > [General] > [Directory Services]** ページを順に選択し、Directory Agent の設定を最後に更新して以降、ディレクトリ サービスの設定が変更されてないことを確認します。
- **[Settings] > [Hybrid Configuration] > [Shared User Data]** ページを順に選択し、Directory Agent がユーザーおよびグループ情報の有効なコンテクスト（パス）を検索しようとしていることを確認します。そのために下記の手順を実行します。
  - Windows Active Directory を使用している場合は、ディレクトリ名または IP アドレスをクリックし、[Test Context] をクリックします。各グローバル カタログ サーバーについて上記の手順を繰り返します。
  - Oracle（旧 Sun Java）Directory Server または Novell eDirectory を使用している場合は、[Test Context] をクリックします。

- [Shared User Data]ページで、コンテクストが有効であり、かつ適切であることを確認します。コンテクストは、ハイブリッド サービスによってフィルタリングされるユーザーおよびグループだけを含むように制限する必要があります。
- さらに[Shared User Data]ページで、Directory Search オプションが正しく設定されていることを確認します。正しく設定されていれば Directory Agent はディレクトリ サービスの該当する部分だけを検索します。
- Directory Agent がインストールされているコンピュータからディレクトリ サービス IP アドレスおよびポートに接続できることを確認します。

Directory Agent の通信上の問題

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Directory Agent がユーザー情報を収集するときディレクトリ サービスとの通信を妨げられた場合、または Directory Agent が Sync Service と通信できない場合は、更新されたユーザーおよびグループ情報をハイブリッド サービスに送信できません。

通信上の問題は下記の場合に発生することがあります。

- ネットワークに問題がある場合。
- The ports used for ディレクトリ サービス（表を参照）または Sync Service（55832）通信に使用されるポートが Directory Agent がインストールされているコンピュータとターゲット コンピュータの間でブロックされている場合。

Port（ポート）	用途：
139	NetBIOS 通信：Active Directory
389	LDAP 通信：Active Directory、Novell eDirectory、Oracle（旧 Sun Java）Directory Server
636	SSL ポート：Novell eDirectory、Oracle（旧 Sun Java）Directory Server
3268	Active Directory
3269	SSL ポート：Active Directory

- Directory Agent が不適当な資格情報を使用していか、ターゲット サービスが接続を認証できない場合。
- サービスが利用できない場合（例、サービスの再開またはコンピュータの再起動のため）

通信上の問題の原因を突き止めために、詳細について Windows イベントファイルまたは **websense.log** ファイルを参照してください。

Directory Agent がこのディレクトリ サービスをサポートしない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Directory Agent は、LDAP ベースのディレクトリ サービスからのみユーザーおよびグループ情報を取得できます。Windows Active Directory（混在モード）は、サポートされていません。下記のディレクトリ サービスがサポートされています。

- Windows Active Directory（ネイティブ モード）
- Oracle（旧 Sun Java System）Directory
- Novell eDirectory
- サポートされているディレクトリ サービスを使用していない場合でも、ハイブリッド サービスはフィルタリング対象の場所を管理することができます。しかし、ユーザーおよびグループ ベースのポリシーの実施は実行できません。

Directory Agent 設定ファイル

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Directory Agent の動作の設定のうち Web Security manager で設定できない動作を設定するには、**das.ini** ファイルを使用します。これらの設定には、エージェントが使用できる最大メモリ、作成できる最大スレッド、ユーザー情報スナップショットを保存するディレクトリなどが含まれます。

das.ini ファイルは、Websense **bin** ディレクトリ（デフォルトでは C:\Program Files **または** Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）にあります。

- このファイルを編集するには、テキスト エディタを使用します。
- 複数の値を取るパラメータに対して、エントリを区切るためにパイプ記号（[|]）を使用します。
- 有効化されるまたは無効化されるパラメータの場合、唯一有効な値は、**0**（無効化の場合）と **1**（有効化の場合）です。このファイルでは、値 [on] と [off] を使用できません。
- 変更を完了したとき、ファイルを保存して閉じ、Directory Agent サービスまたはデーモンを再開します。変更は、サービスが再開するまで有効になりません。

下記の主要な値をファイルで設定できます。

- Directory Agent が使用できるメモリの最大量、単位メガバイト（MB）。Directory Agent が非常に膨大な数のディレクトリ エージェント（200,000 個より以上のユーザーまたはグループの定義）を収集するように設定された場合は、この数値を大きくする必要があります。

```
MaxMemory=100
```

- Directory Agent がディレクトリ サービス スナップショット（ディレクトリの完全なビュー。2 つのクエリーの間での変更を調べるために使用します）を保存する場所を示す完全なディレクトリ パス。

  ```
  SnapshotDir=./snapshots/
  ```

  この相対パスを C:\Program Files **または** Program Files（x86）\Websense\bin\snapshots（Windows）もしくは /opt/Websense/bin/snapshots/（Linux）に変えます。

- Sync Service がハイブリッド サービスに送信する LDIF ファイルを Directory Agent が保存する場所を示すフル ディレクトリ パス。

  ```
  DiffDir=./diffs/
  ```

- Directory Agent が LDAP レコードで電子メール アドレスを検証するために使用する正規表現。そのパターンと一致しない電子メール アドレスをもつレコードは破棄されます。例えば、[a-z0-9!#$%&'*+/=?^_`{|}~-]+（?:\.[a-z0-9!#$%&'*+/=?^_`{|}~-]+）*@（?:[a-z0-9]（?:[a-z0-9-]*[a-z0-9]）?\.）+[a-z0-9]（?:[a-z0-9-]*[a-z0-9]）?

  Directory Agent が電子メール アドレスの検証を行わないようにする場合は、パラメータを空白（デフォルト）のままにしておきます。

  ```
  EmailValidateRegex=
  ```

- Sync Service に接続しようと試みて失敗した後の Directory Agent の再試行の回数 1 から 65535 の整数値をとります。

  ```
  SyncServiceRetryCount=5
  ```

- Sync Service への接続を確立しようとしているとき、Directory Agent が再試行と再試行の間待つ秒数。1 から 65535 の整数値をとります。

  ```
  SyncServiceRetryDelay=60
  ```

- ディレクトリ サービスに接続しようと試みて失敗した後の Directory Agent の再試行の回数 1 から 65535 の整数値をとります。

  ```
  DirServiceRetryCount=5
  ```

- ディレクトリ サービスへの接続を確立しようとしているとき、Directory Agent が再試行と再試行の間待つ秒数。1 から 65535 の整数値をとります。

  ```
  DirServiceRetryDelay=60
  ```

- Sync Service に再接続するために Directory Agent バックアップ サブシステムが再試行と再試行の間待つ秒数。バックアップ サブシステムは、ユーザー データが Sync Service によって正常に受信されるかどうか、およびハイブリッド サービスに送信されるかどうかを確認します。エラーの場合、バックアップ サブシステムは、送信できなかった LDIF ファイルが後の再試行のために保存されるようにします。

  1 から 65535 の整数値をとります。

  ```
  BackupPollPeriod=60
  ```

- 最後のトランザクションのステータスを判断するために、Directory Agent バックアップ サブシステムが Sync Service に再接続を試みる回数。1 から 65535 の整数値をとります。

```
BackupRetryCount=60
```

- Sun Java System Directory または Oracle Directory Server を使用してユーザーおよびグループ情報をハイブリッド サービスに送信する場合の設定値。これらの行の先頭から記号 # を削除して下記のパラメータを有効化します。

  ```
  # GroupMembershipAttribute=uniqueMember
  # MemberOfAttribute=memberOf
  ```

- Directory Agent が LDAP 照会に従うかどうか。値 1（有効化）または 0（無効化）をとります。

  ```
  EnableLDAPReferrals=1
  ```

Directory Agent コマンドライン パラメータ

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Directory Agent には、必要な場合にエージェントをインストール、アンインストール、起動、および停止するために停止できるコマンドライン インタフェースがあります。またエージェンに関するバージョンおよび使用状況の情報も印刷できます。

Directory Agent をコンソール モードで（アプリケーションとして）起動するには、コマンド プロンプトを開き、Websense **bin** ディレクトリ（デフォルトでは C:\Program Files **または** Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）に移動し、下記のコマンドを入力します。

```
DAS.exe -c
```

Directory Agent は、下記のコマンドライン パラメータを受け入れます。一部のパラメータは、Microsoft Windows 環境でのみ使用できます。

パラメータ	説明
-i	Directory Agent サービスをインストールします。これは自動的にオペレーティング システムに登録します（Windows のみ）。
-u	Directory Agent サービスをアンインストールします（Windows のみ）。
-c	Directory Agent をコンソール モードで実行します。
-r	Directory Agent をデーモンまたはサービスとして実行します。
-s	Websense eDirectory Agent サービスを停止します（Windows のみ）。

パラメータ	説明
-v	Directory Agent サービスに関するバージョン情報を印刷します。
-h -? -help <no option（オプションなし）>	Directory Agent サービスに関する使用状況の情報を印刷します。

ハイブリッドサービスからアラートを受け取った

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ハイブリッド サービスは、組織に影響を及ぼす可能性がある問題が発生すると、アラートを Sync Service がインストールされてるコンピュータに送信します。ハイブリッド サービス全体に影響する問題、またはアカウントに固有の問題についてのアラートが送信されます。アラートを受け取った時、下記のようになります。

- 一般的なアラートは、Web Security manager の [Status] > [Dashboard] ページの [System] タブの [Health Alerts（ヘルス アラート）] の下に表示されます。
- より特定のアラートは [Status] > [Status] ページの [Hybrid Filtering Alerts（ハイブリッド フィルタリング アラート）] の下に表示されます

問題を是正するために行うことができる処置（例、Directory Agent にユーザー情報を再送信するように要求 s る、または [Save and Deploy] をクリックして Sync Service にポリシー情報を再送信するように要求する）は、[Status] > [Alerts] ページの詳細なアラート メッセージに含まれています。

多くの場合、ハイブリッド サービスからのアラームは通知アラームであり、一時的な問題によってユーザーまたはポリシー情報の受信やレポーティング データの送信が妨げられる可能性があることを知らせます。お客様の側ではそのような問題に対処するための処置は必要ありません。

問題の原因となった条件が解決された時、System ダッシュボードの要約アラートと [Status] > [Alerts] ページのアラートの両方が解除されます。

ハイブリッド サービスに接続できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Web Security Gateway Anywhere ソリューションのオンプレマイズの部分とハイブリッドの部分は、一貫したポリシーの実施と正確なレポーティングを確保するために定期的に通信しなければなりません。

Sync Service は、ネットワーク上の問題のためにハイブリッド サービスへのアクセスを妨げられ、インターネット接続または内部ネットワーク接続に影響することがあります。

- Sync Service がインストールされているコンピュータがインターネットに接続できるかどうか確認するためにブラウザまたは **ping** ユーティリティを使用します。
- Sync Service がインストールされているコンピュータからインターネットへの HTTPS 接続が確立できることを確認してください。Sync Service は、ポート 443 を使用してハイブリッド サービスに接続します。
- Sync Service がネットワーク内の他のオンプレマイズ コンピュータとポート 55830 および 55831 を通じて通信できることを確認してください。

また、ハイブリッド サービスが Sync Service の接続を受け入れるの妨げる問題がないことも確認 s てください。

- ハイブリッド サービスからの情報については、[Status] > [Alerts]ページの [Hybrid Filtering Alerts] テーブルをチェックしてください。
- 管理者が [Settings] > [General] > [Account] ページで Websense テクニカル サポートからのメッセージのコンタクト アドレスとして指定されている電子メール アカウントをモニタしていたことを確認してください。

ハイブリッド サービスが接続を認証できない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ハイブリッド サービスを使用する環境では、Sync Service は、情報を送信または取得するためにハイブリッド サービスに接続するたびに、アカウント識別子を提供します。この識別子は、組織に固有の識別子であり、**admin** パスワードが変更するたびに更新されます。

稀な事例では、Policy Database に関連する重大な問題になることがあり、オンプレマイズ ソフトウェアとハイブリッド サービスの間の接続が失われることがあります。これらの場合は、ハイブリッド サービス アカウントとして新しい識別子を生成するために使用するセキュリティ トークンを要求しなければなりません。セキュリティ トークンは、Web Security manager の [Settings] > [General] > [Account] ページで指定されている**コンタクト電子メール アドレス**に送信されます。

新しいトークンを要求するには、下記の手順を実行します。

1. Web Security manager の [Status]] > [Alerts] ページの [unable to authenticate connection（接続を認証できません）] の隣に表示されている **[Get Token（トークンを取得）]** ボタンをクリックします。
2. 要求がハイブリッド サービスに送信されましたという成功メッセージを受け取ることを確認します。

3. ハイブリッド サービス アカウントに関連付けられている管理電子メール アカウントをモニタします。新しいトークンの要求が処理される間少し時間がかかります。
4. ハイブリッド サービスから電子メール メッセージを受け取った時、Web Security manager の [Settings] > [General] > [Account] ページに移動します。
5. このページの [Hybrid Filtering（ハイブリッド フィルタリング）] セクションにスクロール ダウンし、電子メール メッセージで指定されている**セキュリティ トークン**を入力します。
6. **[Connect（接続）]** をクリックします。

一時トークンが検証され、Sync Service とハイブリッド サービスの通信を再開するために使用されます。

重要なハイブリッド設定情報がない

Web Security Help | Web Security ソリューション | バージョン 7.8.x

ハイブリッド サービスを使用する環境では、Sync Service は、情報を送信または取得するためにハイブリッド サービスに接続するたびに、アカウント識別子を提供します。この識別子は、組織に固有の識別子であり、**admin** パスワードが変更するたびに更新されます。

稀な事例では、Policy Database に関連する重大な問題になることがあり、オンプレマイズ ソフトウェアとハイブリッド サービスの間の接続が失われることがあります。これらの場合は、ハイブリッド サービス アカウントとして新しい識別子を生成するために使用するセキュリティ トークンを要求しなければなりません。セキュリティ トークンは、[Settings] > [General] > [Account] ページで指定されている**コンタクト電子メール アドレス**に送信されます。

アラート メッセージ [Missing configuration information; connection to hybrid filtering lost（設定情報がありません、ハイブリッド フィルタリングへの接続が失われました）] を受け取った場合、コンタクト電子メール アドレスが提供されていないか、コンタクト電子メール アドレスが有効ではなくなっています。

この場合、組織のプライベート データのセキュリティを最大限にするために、*Websense テクニカル サポート* に直接連絡して、ハイブリッド サービス アカウントを更新する必要があります。

ハイブリッド フェイルオーバー プロキシが明示的プロキシのリストから削除された

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense Web Security Gateway Anywhere バージョン 7.6 では、ハイブリッド サービスへのフェイルオーバーは、手動で、ハイブリッド プロキシ アドレスを明示的プロキシのリストに追加し、そのプロキシをフィルタ対象の場所のリストの最後の明示的プロキシとして含めることによって設定されていました。バージョン 7.7 および 7.8 ではフェイルオーバ - は別の方法で設定されます。つまり、ハイブリッドプロキシが v 7.6 からのアップグレード時に明示的プロキシ リストから削除されます。

ハイブリッド プロキシへのファイルオーバーは、現在では各フィルタリング対象の場所で有効され、ハイブリッド サービスによって承認される必要があります。*ハイブリッド サービスのフェイルオーバの設定*、268 ページを参照してください。

トラブルシューティングのヒントとツール

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense [bin] ディレクトリの場所

Web Security Help | Web Security ソリューション | バージョン 7.8.x

多くの Websense Web Security の実行可能ファイルおよび設定ファイルは Websense **bin** ディレクトリにインストールされています。トラブルシューティングの処置がこのディレクトリに移動するように要求した場合、そのディレクトリの場所はオペレーティング システムおよびインストールされているコンポーネントによって異なります。

Linux プラットフォームの場合

```
/opt/Websense/bin/
```

Windows プラットフォームの場合

C:\Program Files または Program `Files(x86)\Websense\Web Security\bin`

Windows Services ツール

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Microsoft Windows がインストールされているコンピュータでは、Filtering Service、Network Agent、Policy Server、User Service、および他の Web Security コンポーネントはサービスとして実行します。Windows Services ツールを使って、これらのサービスのステータスを確認できます。

1. ツールを起動するには、以下の手順を行います。
   - Windows Server 2012：**[Server Manager] > [Tools] > [Services]** を順に選択します。
   - Windows Server 2008 R2：**[Start] > [Administrative Tools] > [Services]** を順に選択します。
2. トラブルシューティングするサービスを見つけるために、サービスのリストをスクロールします。

   サービスのエントリには、サービス名、サービスの簡単な説明、サービス ステータス（起動または停止）、サービスの開始方法、サービスがタスクを実行するために使用するアカウントが含まれます。
3. サービス名をダブルクリックすると、そのサービスに関するより詳細な情報を含む [Properties（プロパティ）] ダイアログ ボックスが開きます。

Windows イベント ビューア

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Windows イベント ビューアは、サービス アクティビティを含む、Windows イベントに関するエラー メッセージを記録します。これらのメッセージは、インターネット ポリシーの実施やユーザー識別の問題の原因となるネットワークまたはサービス エラーを特定するのに役立ちます。

1. 以下のいずれかの手順を行います。
   - Windows Server 2012：**[Server Manager] > [Tools] > [Event Viewer]** を順に選択します。
   - Windows Server 2008 R2：**[Start] > [Administrative Tools] > [Event Viewer]** を順に選択します。
2. イベント ビューアで下記のどちらか該当する手順を実行します。
   - Windows Server 2012：Expand the **[Windows Logs（Windows のログ）]** ツリーを展開し、**[Application]** を選択します。
   - Windows Server 2008 R2：イベント ビューアで **[Application（アプリケーション）]** をクリックして、エラー メッセージ、警告、および情報メッセージのリストを表示します。
3. リストをスクロールして、Websense サービスからのエラーまたは警告を見つけます。

Websense ログ ファイル

Web Security Help | Web Security ソリューション | バージョン 7.8.x

Websense ソフトウェアは、エラー メッセージを Websense **bin** ディレクトリ（デフォルトでは、C:\Program Files **または** Program Files（x86）\Websense\Web Security\bin もしくは /opt/Websense/bin/）にある、**websense.log** ファイルに書き込みます。

このファイルに含まれる情報は、Windows イベント ビューアで見つかった情報と同じです。Windows 環境では、イベント ビューアはメッセージをわかりやすい形式で表示します。しかし、**websense.log** ファイルは Linux システム上で使用でき、問題のトラブルシューティングの支援が必要なとき、そのファイルを Websense テクニカル サポートに送信することができます。

索引

E

F

H

I

J

L

M

N

O

P

T

U

W

X

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

た

て

と

な

に

ね

は

ひ

へ

わ