Websense Manager ヘルプ

Websense®Web Security
Websense Web Filter

v7

©1996–2008, Websense Inc.
All rights reserved.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA

発行 2008
アメリカ合衆国およびアイルランドにて印刷

本マニュアルに記載されている製品および使用方法は、米国 特許番号 5,983,270、6,606,659、6,947,985、7,185,015、7,194,464、および RE40,187 およびその他の申請中の特許で保護されています。

本書の一部または全部を Websense Inc. からの書面による事前の同意なく、いかなる電子メディアまたはコンピュータに複写、複製、転載、翻訳することを禁じます。

本ガイドの内容の正確性については万全を期しています。しかしながら、Websense Inc., は、これを一切保証するものではなく、本製品の商品性および特定の用途に対する適合性についても同じ く一切保証していません。Websense Inc., は、本ガイドまたはガイドに含まれる例の提供、性能、または使用にかかわる偶発的、副次的ないかなる損害に対しても、責任を負いかねます。本書の情報は、通知なしに変更されることがあります。

商標について

Websense は Websense, Inc., の米国およびおよびその他の国際市場における登録商標です。Websense は米国および国際的に多数の他の未登録の商標を有しています。他のすべての商標は、それぞれの所有者の財産です。

Microsoft、Windows、Windows NT、Windows Server および Active Directory は、Microsoft Corporation の米国およびその他の国における商標または登録商標です。

Sun、Solaris、UltraSPARC、Sun Java System および すべての Sun Java System ベースの商標 および ロゴは Sun Microsystems, Inc., の米国 および その他の国における商標です。

Mozilla および Firefox は、Mozilla Foundation の米国および他の国における登録商標です。

eDirectory および Novel Directory Services は Novell, Inc. の米国および他の国における登録商標です。

Adobe、Acrobat および Acrobat Reader は、Adobe Systems Incorporated の米国および / もしくはその他の国における登録商標または商標です。

Pentium は Intel Corporation の登録商標です。

Red Hat は Red Hat, Inc., の米国および他の国における登録商標です。Linux は Linus Torvalds の米国およびその他の国における商標です。

本製品には Apache Software Foundation (http://www.apache.org) により配布されたソフトウェアが含まれています。
Copyright (c) 2000.The Apache Software Foundation.All rights reserved.

本マニュアルに記載されているその他の製品名はそれぞれの企業の登録商標であり、各メーカーにのみ所有権があります。

目次

1 使用開始にあたって

Websense ソフトウェアは、ビジネスから教育、政府など、あらゆる産業部門のネットワーク管理者に、インターネットへのネットワーク トラフィックを管理またはモニタする機能を提供します。

- いかがわしい、不適切な、または仕事に関連しないと考えられるインターネット データへのアクセスに費やされる従業員の仕事をしていない時間を最小にします。
- 不適切なアクセスによるネットワーク リソースの乱用や訴訟の脅威を最小にします。
- ネットワークにセキュリティの堅固な層を付加し、ネットワークをスパイウェア、マルウェア、ハッキングなどの侵入の可能性に対して保護します。

ここから以下に関する情報を見つけることができます:

Websense の基本構成	インターネット フィルタリングの実施
• Websense Manager での作業、15 ページ • サブスクリプション、26 ページ • Websense マスタ データベース、30 ページ • Network Agent 設定の確認、352 ページ	• カテゴリおよびプロトコルのフィルタリング、36 ページ • クライアントの追加、69 ページ • ポリシーに関する作業、75 ページ • クライアントへのポリシーの割り当て、80 ページ

また、以下を行う方法を知ることができます:

構成を評価する	インターネット フィルタリング ポリシーを調整する
• 今日: ヘルス、セキュリティ、および値 (AM 12:00 以降)、20 ページ • 履歴: 最終 30 日、23 ページ • プレゼンテーション レポート、98 ページ • 調査レポート、118 ページ	• カスタム カテゴリの作成、180 ページ • 特定のサイトのフィルタリングの再定義、184 ページ • ユーザのアクセスを指定したサイトのリストに制限、170 ページ • キーワードに基づくフィルタリング、182 ページ

構成を評価する	インターネット フィルタリング ポリシーを調整する
• ツールボックスによるフィルタリング動作の確認、200 ページ	• ファイル タイプに基づくトラフィックの管理、196 ページ • Bandwidth Optimizer による帯域幅の管理、194 ページ

概要

Websense ソフトウェアは、統合デバイス（プロキシ サーバー、ファイアウォール、ルーター、キャッシング アプライアンスを含む）とともに動作し、インターネット アクセス ポリシーを開発しモニタし強化するためのエンジンおよび構成ツールを提供します。

一連の Websense コンポーネント（Websense 製品コンポーネント、274 ページを参照）が協調して、インターネット フィルタリング、ユーザ識別、アラート、レポート、およびトラブルシューティング機能を提供します。

この Websense ソフトウェア バージョンに含まれている新機能の概要については、リリース ノートを参照してください。リリースノートは Websense サポート ポータルにあります。

インストール後は、Websense ソフトウェアは**デフォルト** ポリシーを適用し、要求をブロックせずにインターネット使用状況をモニタします。独自のポリシーが定義されクライアントに割り当てられるまでは、このポリシーがネットワーク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。カスタム フィルタリング設定が作成された後でも、他のポリシーに管理されないクライアントには常にデフォルト ポリシーが適用されます。詳細は、デフォルト ポリシー、74 ページ を参照してください。

フィルタの作成、クライアントの追加、ポリシーの定義、およびクライアントへのポリシーの適用のプロセスについては、以下に説明されています：

- インターネット使用のフィルタ、35 ページ
- クライアント、59 ページ
- インターネット フィルタリング ポリシー、73 ページ

単一のブラウザ ベース ツールである Websense Manager が、Websense ソフトウェアの全般的構成、ポリシー管理およびレポート機能に対する中央管理されたグラフィカル インターフェースを提供します。詳細は、Websense Manager での作業、15 ページ を参照してください。

Websense Manager へのアクセス権のレベルを定義して、特定の管理者が特定のクライアント グループのみを管理することや、個人が自分のインターネット使用状況に関するレポートを行うことを許可することができます。詳細は、指定済み管理、239 ページ を参照してください。

Websense Manager での作業

関連トピック :

- Websense Manager へのログオン、16 ページ
- Websense Manager の中での移動、18 ページ
- 今日 : ヘルス、セキュリティ、および値 (AM 12:00 以降)、20 ページ
- 履歴 : 最終 30 日、23 ページ

Websense Manager は、フィルタリング機能のカスタマイズ、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生成、ならびに Websense ソフトウェアの構成および設定に使用される中央設定インターフェースです。この Web ベース ツールは、サポートされている以下の 2 つのブラウザ上で動作します :

- Microsoft Internet Explorer 7
- Mozilla Firefox 2

一部の他のブラウザを使用して Websense Manager を起動することは可能ですが、完全な機能とアプリケーションの正しい表示を得るにはサポートされているブラウザを使用してください。

Websense Manager を起動するには、次のいずれかを行います :

- Windows の場合 :
  - **[スタート] > [すべてのプログラム] > [Websense]** を選択し、続いて **[Websense Manager]** を選択します。
  - Websense Manager のデスクトップ アイコンをダブルクリックします。
- ネットワークのコンピュータ上で、サポートされているブラウザを開き以下を入力します :

  ```
  https://<IP address>:9443/mng
  ```

  <IP address> を Websense Manager コンピュータの IP アドレスに置き換えてください。

デフォルト ポート上で Websense Manager に接続できない場合は、Websense Manager コンピュータ上の **tomcat.log** ファイル (デフォルトでは **C:¥Program Files¥Websense¥tomcat¥logs¥** または **/opt/Websense/tomcat/logs/** ディレクトリにあります) を参照してポートを確認してください。

正しいポートを使用しているのにリモート コンピュータから Websense Manager に接続できない場合には、ファイアウォールがそのポート上での通信を許可しているかどうかを確認してください。

Websense Manager との安全なブラウザ ベース通信を行うために SSL 接続を使用します。この接続では、Websense, Inc. が発行するセキュリティ証明書を使用します。サポートされているブラウザは Websense, Inc. を既知の認証機関として認識しないので、新しいブラウザから初めて Websense Manager を

起動すると、認証エラーが表示されます。このエラーが表示されないようにするには、ブラウザにこの証明書をインストールするかまたは証明書を恒久的に受け入れます。手順については、Websense Knowledge Base を参照してください。

セキュリティ証明書が受け入れられると、ブラウザ ウィンドウに Websense Manager のログオン ページが表示されます (Websense Manager へのログオンを参照)。

Websense Manager へのログオン

関連トピック :

- Websense Manager での作業
- Websense Manager の中での移動、18 ページ
- 今日 : ヘルス、セキュリティ、および値 (AM 12:00 以降)、20 ページ
- 履歴 : 最終 30 日、23 ページ

インストール後、Websense Manager に最初にログオンするユーザが完全な管理者アクセス権限を持ちます。ユーザ名は **WebsenseAdministrator** で、これを変更することはできません。インストール時に WebsenseAdministrator パスワードが設定されます。

ログオンするには、まず Websense Manager を起動します (Websense Manager での作業を参照)。ログオン ページで以下を行います :

1. 管理する **Policy Server** を選択します。

   使用している環境に Policy Server が 1 つしか存在しない場合は、デフォルトでそれが選択されます。
2. **アカウント タイプ**を選択します :
   - Websense ユーザ アカウント、たとえば WebsenseAdministrator、を使用してログオンするには、**[Websense アカウント]**(デフォルト) をクリックします。
   - ネットワーク資格情報を使用してログオンするには、**[ネットワーク アカウント]** をクリックします。
3. **ユーザ名**および**パスワード**を入力し、**[ログオン]** をクリックします。

これで Websense Manager にログオンできました。

- Websense Manager に初めてログオンすると、クイック スタート チュートリアルを起動するかどうかたずねられます。Websense ソフトウェアになれていない場合、または Websense ソフトウェアのこのバージョンになれていない場合は、クイック スタート チュートリアルを一通り見ることを強くおすすめします。

- 指定済み管理を使用して管理ロールを作成すると、管理するロールを選択するように要求される場合があります。詳細は、指定済み管理、239 ページ を参照してください。

Websense Manager のセッションは、そこで最後に行った操作（ページの中でのクリック、情報の入力、変更のキャッシュ、変更の保存）の 30 分後に終了します。セッションが終了する 5 分前に、警告メッセージが表示されます。

- そのページにキャッシュされていない変更や未反映のキャッシュされた変更がある場合、セッションが終了するとそれらの変更は失われます。変更を保存し適用するには、必ず [OK] をクリックして変更をキャッシュし、[**すべて保存**] をクリックしてください。
- 同じブラウザ ウィンドウの複数のタブで Websense Manager が開かれている場合は、すべてのインスタンスが同じセッションを共有しています。1 つのタブでセッションがタイムアウトになると、すべてのタブでタイムアウトになります。
- 同じコンピュータの複数のブラウザ ウィンドウで Websense Manager が開かれている場合、**次のような場合には**、それらのインスタンスは同じセッションを共有しています：
  - Microsoft Internet Explorer を使用していて、ショートカット [Ctrl-N] を使用して Websense Manager の新しいインスタンスを開いた場合。
  - Mozilla Firefox を使用している場合。

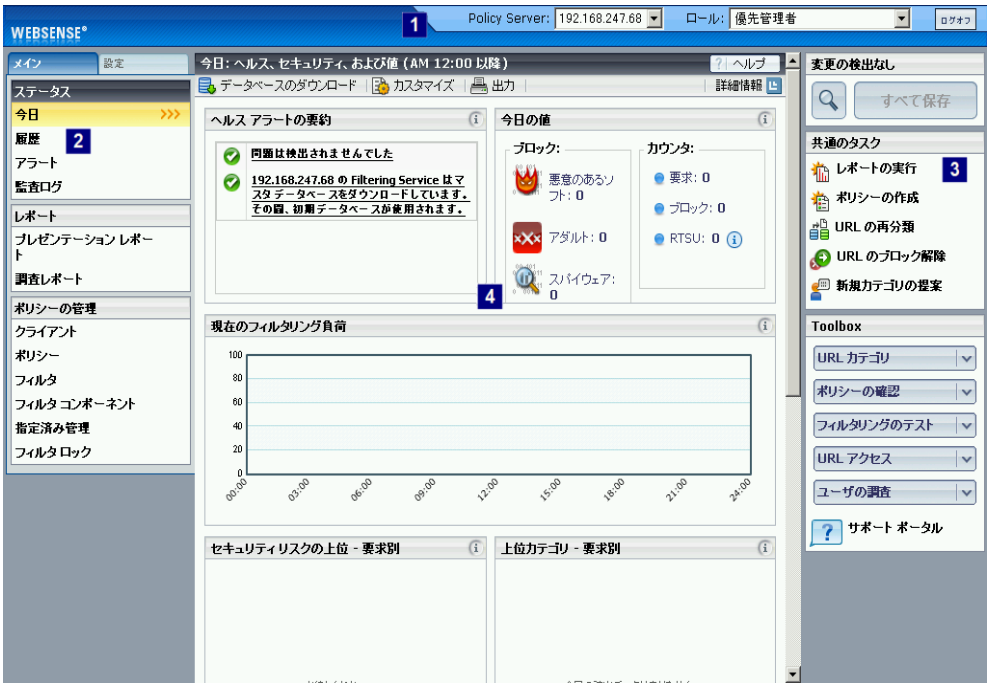
  1 つのタブでセッションがタイムアウトになると、すべてのタブでタイムアウトになります。
- 複数の Internet Explorer ウィンドウを互いに独立に開き、それらを使用して異なる Websense Manager 管理者としてログオンしている場合は、それらのウィンドウは 1 つのセッションを**共有してはいません**。1 つのウィンドウがタイムアウトしても、他のウィンドウは影響を受けません。

Websense Manager からログオフせずにブラウザを閉じた場合や、Websense Manager にアクセスしているリモートコンピュータの予期しないシャットダウンがあった場合は、一時的にロックアウトされる場合があります。Websense ソフトウェアは約 2 分以内にこの問題を検出し、中断したセッションを終了させ、ふたたびログオンできるようにします。

Websense Manager の中での移動

Websense Manager インターフェースは、以下の 4 つの主要領域に分けることができます：

1. Websense バナー
2. 左側のナビゲーション ペイン
3. 右側のショートカット ペイン
4. コンテンツ ペイン



Websense バナーには、以下が示されます：

- 現在ログオンしている **Policy Server**（Policy Server の動作、279 ページを参照）
- 現在の管理**ロール**（管理ロールの説明、240 ページを参照）
- 管理セッションを終了するための **[ログオフ]** ボタン

Websense Manager に表示されるコンテンツは、ログオンしたユーザに付与されている権限によって異なります。たとえば、「レポートのみ」権限を与えられているユーザには、サーバー構成設定やポリシー管理ツールは表示されません。詳細は、指定済み管理、239 ページ を参照してください。

このセクションでは、WebsenseAdministrator やその他の優先管理者特権を与えられているユーザが利用できるオプションについて説明します。

左側のナビゲーション ペインには、**[メイン]** と **[設定]** の 2 つのタブがあります。**[メイン]** タブを使用して、ステータス、レポート、およびポリシーの管理機能にアクセスします。**[設定]** タブを使用して、Websense アカウントを管理し、グローバルなシステム管理タスクを実行します。

右側のショートカット ペインには、役に立つツールや共通の管理タスクへのリンクが含まれています。また、ここで Websense Manager で行った変更を確認し、保存することができます。

- ナビゲーション ペインの最上部に、保存されるのを待っているキャッシュされた変更があるかどうかが示されます。Websense Manager で作業中には、[変更] バーに**未反映の変更点**があるかどうかが示されます。

  ほとんどの場合、Websense Manager でタスクを実行し、**[OK]** をクリックすると、変更点がキャッシュされます。(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変更点がキャッシュされない場合があります。)

  変更点をキャッシュした後、**[すべて保存]** をクリックして変更点を保存し、実施します。保存する前にキャッシュされた変更点を表示するには、**[未反映の変更点の表示]** をクリックします (変更点の確認、保存および破棄、19 ページを参照)。これは、[すべて保存] の左側の小さなボタンです。
- **[共通のタスク]** には、頻繁に実行される管理タスクへのショートカットが表示されます。リストの項目をクリックすると、そのタスクが実行されているページにジャンプします。
- **[Toolbox]** には、フィルタリング設定を確認するために使用できるクイック ルックアップ ツールが含まれています。詳細は、ツールボックスによるフィルタリング動作の確認、200 ページ を参照してください。

変更点の確認、保存および破棄

ほとんどの場合、Websense Manager でタスクを実行し、**[OK]** をクリックすると、変更点がキャッシュされます。**[未反映の変更点の表示]** ページを使用して、キャッシュされた変更点を確認します。

> **重要**
> [OK] ボタンを続けて 2 回も 3 回もクリックしないでください。同じボタンを短い間隔で 2 回以上クリックすると Mozilla Firefox の表示に問題が起こることがあり、問題を解決するためにはブラウザを終了してから再開しなければなりません。

機能の単一分野への変更は、一般に、キャッシュ リストでは単一のエントリにグループ化されます。たとえば、6 人のクライアントを追加し、2 人のクライアントを削除した場合、キャッシュ リストでは、[クライアント] に対してのみ変更が行われたことになります。他方では、1 つの [設定] ページに対する変更が、キャッシュ リストでは複数のエントリになる場合もあります。このようなことは、1 つの [設定] ページを使用して複数の Websense ソフトウェア機能を設定しているような場合に起こります。

- すべてのキャッシュされた変更を保存するには、**[すべての変更を保存する]** をクリックします。
- すべてのキャッシュされた変更を放棄するには、**[すべての変更を破棄する]** をクリックします。

すべて保存またはすべて破棄を選択すると、右側のショートカット ペインの変更バーがそれに応じて更新され、最後に選択したページに戻ります。すべて保存またはすべて破棄機能は、どちらも取り消しはできません。

[監査ログ] を使用して、Websense Manager で行われた変更の詳細を表示します。詳細は、監査ログの表示とエクスポート、286 ページ を参照してください。

今日 : ヘルス、セキュリティ、および値 (AM 12:00 以降)

関連トピック :

- Websense Manager の中での移動、18 ページ
- 履歴 : 最終 30 日、23 ページ
- 今日 ページのカスタマイズ、22 ページ
- アラート、289 ページ

Websense Manager にログオンすると、最初に **[ステータス] > [今日 : ヘルス、セキュリティ、および値 (AM 12:00 以降)]** ページが表示されます。このページには、フィルタリング ソフトウェアの現在の状態が表示され、ログ データベース コンピュータの時計に従って AM 12:01 から最大 24 時間のインターネット フィルタリング活動がグラフで表示されます。

このページの上部の 2 つの要約セクションには、現在の状態の概要が表示されます :

- **[ヘルス アラートの要約]** には、Websense ソフトウェアの状態が表示されます。要約でエラーや警告が表示された場合は、アラート メッセージをクリックすると [アラート] ページが開きます。このページにさらに詳しい情報が表示されます (現在のシステム ステータスの確認、296 ページ を参照)。

  [ヘルス アラートの要約] 情報は、30 秒ごとに更新されます。
- **[今日の値]** セクションには、たとえば、今日 Websense フィルタリングがネットワークをどのように保護したかを示す統計のほか、処理されたインターネット要求の数や他の重要なアクティビティの合計が表示されます。

要約情報の下には、最大 4 つの図によってフィルタリング活動に関する情報が示されます。これらの図は、優先管理者および [今日] ページでレポートを見る許可を与えられている指定済み管理者が利用可能です。ロールの編集、258 ページを参照してください。

これらの図の情報は、2 分ごとに更新されます。図をすべて見るには、スクロールする必要がある場合があります。

グラフの名前	説明
現在の フィルタリング負荷	処理されてログ データベースに記録された、フィルタされたインターネット トラフィックの数量。10 分間隔で表示されます。
上位セキュリティ リスク – 要求別	今日、どのセキュリティ リスク カテゴリが最も多く要求されたかを調べ、フィルタリング 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判別します。
上位カテゴリ – 要求別	今日、最も多くアクセスされたカテゴリを参照します。セキュリティ、帯域幅、生産性に関する潜在的問題について、高水準の概要が得られます。
ポリシーの実施状況 – リスク クラス別	各リスク クラスについて、今日許可されたおよびブロックされた件数を表示します（リスク クラス、40 ページを参照）。現在のポリシーが効果的か、それとも変更が必要かを評価できます。
上位プロトコル – 帯域幅別	今日、ネットワークで最も多くの帯域幅を使用したプロトコルを確認します。この情報を使用して、帯域幅のニーズとポリシーを変更する潜在的な必要があるかどうかを評価します。
セキュリティ リスク サイトを要求したコンピュータ	今日、セキュリティ リスク サイトにアクセスしたコンピュータを調べます。これらのコンピュータを点検して、ウィルスやスパイウェアに感染していないことを確認する必要があるかもしれません。
上位ブロックされたユーザ	今日、ブロックされたサイトをどのユーザが最も多く要求したかを調べ、組織のインターネット使用基準の順守状況を把握します。
上位未分類サイト	今日、Websense マスタ データベースで分類されていないサイトのうち、どのサイトが最も多くアクセスされたかを確認します。[**共通のタスク**] > [**URL の再分類**] にアクセスし、サイトをフィルタリングのためのカテゴリに割り当てます。

いずれかの棒グラフをクリックすると、詳細な調査レポートが表示されます。

ページの上に 3 つのボタンが表示されます：

- [**データベースのダウンロード**] 優先管理者だけが使用可能です。マスタ データベースのダウンロードの状況を表示しダウンロードを開始するためのページを開きます（マスタ データベース ダウンロード ステータスの確認、285 ページを参照）。
- [**カスタマイズ**] 優先管理者だけが使用可能です。ページに表示する図を変更できるページを開きます（今日 ページのカスタマイズ、22 ページを参照）。
- [**印刷**] すべての管理者が利用可能です。第 2 ウィンドウが開かれ、[今日] ページに表示されている図の印刷可能バージョンが表示されます。ブラウザ オプションを使用してこのページを印刷します。このページには

Websense Manager ウィンドウにあるようなナビゲーション オプションはすべて表示されません。

インターネット アクティビティ図やフィルタリング図の下に、**[Filtering Service の要約]** が表示され、現在の Policy Server に関連付けられた各 Filtering Service の状況が示されます。Filtering Service の IP アドレスをクリックすると、その Filtering Service インスタンスの詳細情報が表示されます。

セキュリティのために、Websense Manager セッションは何もしないと 30 分後に終了します。ただし、フィルタリング データやアラート データの監視の継続を選択することができます。これを行うには、[今日] ページの下部の **[タイムアウトなしで、今日、履歴、アラートのステータスをモニタする]** をオンにします。これらの 3 つのページの情報は、ブラウザを閉じるまで、または Websense Manager の別のページに移動するまで、継続的に正常に更新されます。

重要

この監視オプションを有効にし、[今日]、[履歴]、および [アラート] ページに 30 分以上留まっている場合、別の Websense Manager ページに移動しようとすると、[ログオン] ページに戻ります。

このオプションを有効にする場合は、必ず、30 分のタイムアウト期間が終わる前にキャッシュされた変更を保存してください。

今日 ページのカスタマイズ

関連トピック :

- 今日 : ヘルス、セキュリティ、および値 (AM 12:00 以降)、20 ページ
- 履歴 ページのカスタマイズ、25 ページ

[今日] > **[カスタマイズ]** ページを使用して、[ステータス] > [今日] ページ用に最大 4 つの図を選択します。無条件のポリシー権限を持つ優先管理者 (WebsenseAdministrator を含む) だけが、[今日] ページをカスタマイズできます。

選択した図が、すべての優先管理者に対して、および [今日] ページの図を見る権限を持っている指定済み管理者に対して、[今日] ページに表示されます。ロールの編集、258 ページを参照してください。

一部の図には、ユーザ名や IP アドレスのような、機密である可能性がある情報が表示されます。図を見ることができるすべての管理者に対して選択する図が適切であるように留意してください。

図を選択するには、図名のそばのチェックボックスをオンにし、またはオフにします。選択を終了したら、**[OK]** をクリックすると [今日] ページに戻り、図が表示されます。変更を行わずに [今日] ページに戻るには、**[キャンセル]** をクリックします。

各図に表示される情報の簡単な説明については、今日：ヘルス、セキュリティ、および値（AM 12:00 以降）、20 ページを参照してください。

履歴：最終 30 日

関連トピック：

- 今日：ヘルス、セキュリティ、および値（AM 12:00 以降）、20 ページ
- Websense Manager の中での移動、18 ページ
- 履歴 ページのカスタマイズ、25 ページ

[ステータス] > **[履歴：最終 30 日]** ページを使用して、過去 30 日間までのフィルタリング活動の概要を得ることができます。このページの図は、ログデータベース コンピュータの時計に従って毎日 AM 12:01 に、前日のデータを取り込んで更新されます。

図および要約表がカバーしている正確な期間は、Websense ソフトウェアがフィルタリングを行っていた時間に依存します。Websense ソフトウェアがインストールされた最初の 1 月間は、このページにはインストールからの日数の間のデータが表示されます。それ以降は、レポートは今日までの 30 日間をカバーします。

このページの上部の **[見積もり値]** には、Websense ソフトウェアがもたらす時間と帯域幅の節約量の見積もり、および多くの組織にとって重要なカテゴリーに対するブロックされた要求の要約が示されます。

見積もりを計算した方法の説明が必要な場合は、（[節約] の下の）**[時間]** または **[帯域幅]** の上にマウスを置きます（節約された時間と帯域幅、25 ページを参照）。**[カスタマイズ]** をクリックして、値を計算する方法を変更することができます。

さらに、**[ブロックされた要求数]** エリアでは、多くの組織にとって重要な複数のカテゴリのリストを示し、この期間中に各カテゴリに対するブロックされた要求数を示すことにより、Websense ソフトウェアがどのようにネットワークを保護したかを示します。

そのロールに対して与えられたレポート権限によっては、指定済み管理者には以下に説明する図が表示されない場合があります。ロールの編集、258 ページを参照してください。

また、このページには、フィルタリングの重要点に関する最大 4 つの図が含まれます。図をすべて見るには、スクロールする必要がある場合がありま

す。これらの図の情報は、1 日に 1 回更新されます。より詳細な情報をまとめた調査レポートを起動するには、図をクリックします。

グラフの名前	説明
インターネット アクティビティ – 要求別	毎日処理されてログ データベースに記録された、フィルタされたインターネット要求の数が表示されます。
上位セキュリティ リスク – 要求別	最近アクセスされたセキュリティ リスクのカテゴリを参照し、ネットワークに正しいフィルタリング ポリシーが適用されているか判別します。
上位カテゴリ – 要求別	最もアクセスの多かったカテゴリを表示します。セキュリティ、帯域幅、生産性に関する潜在的問題について、高水準の概要が得られます。
上位未分類サイト	Websense マスタ データベースで分類されていないサイトのうち、どのサイトが最も多くアクセスされたかを確認します。**[共通のタスク]** > **[URL の再分類]** にアクセスし、サイトをフィルタリングのためのカテゴリに割り当てます。
上位プロトコル – 帯域幅別	最近、ネットワークで最も多くの帯域幅を使用したプロトコルを確認します。この情報を使用して、帯域幅のニーズとポリシー変更の可能性を評価します。
ポリシーの実施状況 – リスク クラス別	各リスク クラスについて、最近許可されたおよびブロックされた件数を表示します（リスク クラス、40 ページを参照）。現在のポリシーが効果的か、それとも変更が必要かを評価できます。
上位ブロックされたユーザ	どのユーザのインターネット要求が最もブロックされたかを表示します。組織のインターネット使用基準が順守されているか状況を把握します。
ポリシーの実施状況の要約	セキュリティ リスク クラスに含まれるサイトについては最近の許可された要求とブロックされた要求について、その他のサイトについてはブロックされた要求について、概要が得られます。フィルタリングのどの点が詳細な評価を必要としているかを検討します。

ページの上に 2 つのボタンが表示されます：

- **[カスタマイズ]** 優先管理者だけが使用可能です。ページに表示する図を変更でき、節約量の見積もりを計算する方法を変更できるページを開きます（履歴 ページのカスタマイズ、25 ページを参照）。
- **[印刷]** すべての管理者が利用可能です。第 2 ウィンドウが開かれ、[履歴] ページに表示されている図の印刷可能バージョンが表示されます。ブラウザ オプションを使用してこのページを印刷します。このページには Websense Manager ウィンドウにあるようなナビゲーション オプションはすべて表示されません。

節約された時間と帯域幅

Websense フィルタリングが提供するセキュリティの改善のほかに、Websense フィルタリングは非生産的なインターネット アクティビティによって失われる時間と帯域幅を最小にするのに役立ちます。

[見積もり値] エリアの [節約] セクションには、これらの時間および帯域幅の節約量の見積もりが示されます。これらの値は、以下のようにして計算されます:

- 節約された時間: **「アクセス当りの一般的経過時間」**かける**「ブロックされたサイト数」**。最初は、Websense ソフトウェアは、ユーザが要求した Web サイトを見るのに費やす平均的秒数としてデフォルト値を使用します。ブロックされたサイト数の値は、その履歴ページがカバーしている時間範囲中にブロックされた要求の合計数です。
- 節約された帯域幅: **「アクセス当りの一般的帯域幅」**かける**「ブロックされたサイト数」**。最初は、Websense ソフトウェアは、平均的 Web サイトが消費する平均的バイト数としてデフォルト値を使用します。ブロックされたサイト数の値は、その履歴ページがカバーしている時間範囲中にブロックされた要求の合計数です。

これらの計算に使用する値を組織の使用状況を反映するように変更する方法の詳細については、履歴 ページのカスタマイズ、25 ページを参照してください。

履歴 ページのカスタマイズ

関連トピック:

- 履歴 : 最終 30 日、23 ページ
- 今日 ページのカスタマイズ、22 ページ

[履歴] > [カスタマイズ] ページを使用して、[ステータス] > [履歴] ページに表示する図を決定し、時間と帯域幅の節約量を計算する方法を決定します。

[履歴] ページに含めたい最大 4 つまでの各図名のそばのチェックボックスをオンにします。各図の簡単な説明については、履歴 : 最終 30 日、23 ページを参照してください。無条件のポリシー権限を持つ優先管理者 (WebsenseAdministrator を含む) だけが、[履歴] ページの図をカスタマイズできます。

一部の図には、ユーザ名のような、機密である可能性がある情報が表示されます。図を見ることができるすべての管理者に対して選択する図が適切であるように留意してください。

優先管理者および指定済み管理者は、時間と帯域幅の節約量の計算方法をカスタマイズできます。指定済み管理者は、節約された時間および帯域幅の計算を説明するポップアップ ウィンドウの中の **[カスタマイズ]** リンクをクリックすることによって、これらのフィールドにアクセスします。

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
ブロックされたページ当りの節約された平均秒数	1 人のユーザが個々のページを見るのに費やすと組織が推定する、平均的秒数を入力します。 Websense ソフトウェアは、この値にブロックされたページの数をかけることにより、履歴ページに示される時間の節約量を決定します。
ブロックされたページ当りの節約された平均帯域幅 (KB)	ページを表示するのに必要な平均帯域幅をキロバイト (KB) 単位で入力します。 Websense ソフトウェアは、この値にブロックされたページの数をかけることにより、履歴ページに示される帯域幅の節約量を決定します。

チェックボックスのマークの変更が終了したら、[OK] をクリックすると [履歴] ページに戻ります。新しい図または時間と帯域幅の見積もり値が表示されます。変更を行わずに [履歴] ページに戻るには、[**キャンセル**] をクリックします。

サブスクリプション

Websense サブスクリプションは、クライアント数をベースにして発行されます。クライアントとは、ネットワーク中のユーザまたはコンピュータです。

サブスクリプションを購入すると、サブスクリプション キーが電子メールで提供されます。各キーは、Websense Policy Server の 1 つのインストレーションに対して有効です。複数の Policy Server をインストールする場合は、それぞれについて別個のキーが必要です。

フィルタリングを開始する前に、有効なサブスクリプション キーを入力しなければなりません (アカウント情報の構成、28 ページを参照)。これによってマスタ データベースをダウンロードできるようになり (Websense マスタ データベース、30 ページを参照)、Websense ソフトウェアがクライアントをフィルタすることが可能になります。

初めてデータベースのダウンロードに成功すると、Websense Manager はサブスクリプションに含まれるクライアント数を表示します。

Websense ソフトウェアは、毎日フィルタしたクライアントに関するサブスクリプション テーブルを維持しています。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にクライアントが初めてインターネット要求を行うと、その IP アドレスがテーブルに入力されます。

テーブルにリストされたクライアントの数がサブスクリプション レベルに達した場合、それまでにリストされていないクライアントがインターネット アクセス要求を行うと、そのクライアントはサブスクリプションを超過することになります。このような場合、サブスクリプション レベルを超過するクライアントは、構成された設定に従って、インターネットから完全にブロック

されるか、またはフィルタされないインターネット アクセスを提供されることになります。同様に、サブスクリプションの期限が切れると、この設定に従って、すべてのクライアントが完全にブロックされるか、またはフィルタされません。

サブスクリプションが超過したか、または失効した場合のフィルタリング動作の構成については、アカウント情報の構成、28 ページを参照してください。

サブスクリプションが限界に近づいたか超過した場合に電子メール警告を送信するように Websense ソフトウェアを設定する方法については、システム アラートの設定、292 ページを参照してください。

フィルタされるカテゴリ数は、Websense サブスクリプションによります。Websense ソフトウェアは、購入時に有効化されたすべてのカテゴリのすべてのサイトをフィルタします。

MyWebsense ポータルによるアカウントの管理

Websense, Inc. は、www.mywebsense.com にカスタマ ポータルを維持しています。これを使用して、製品のアップデート、パッチ、製品ニュース、評価、および Websense ソフトウェアのテクニカル サポート リソースにアクセスすることができます。

アカウントを作成する際に、すべての Websense サブスクリプション キーを入力するように勧められます。これによって、使用している Websense 製品とバージョンに関連する情報、アラート、およびパッチにアクセスできるようになります。

MyWebsense アカウントを持っていれば、WebsenseAdministrator パスワードを忘れたために Websense Manager にログオンできなくなった場合でも、**[パスワードを忘れた場合]** をクリックするだけで済みます。MyWebsense にログオンするように促され、ログオンすると、新しいパスワードを生成し有効にするための指示が与えられます。

重要

新しいパスワードを要求する場合、MyWebsense ポータルで選択するサブスクリプション キーが Websense Manager の [アカウント] ページで入力したキーと一致していなければなりません。

組織の複数のメンバーが、同じサブスクリプション キーに関連して MyWebsense ログオンを作成できます。

Websense Manager から MyWebsense ポータルにアクセスするには、**[ヘルプ] > [MyWebsense]** を選択します。

Websense Web Protection Services™ の有効化

Websense Web Security サブスクリプションには、Websense Web Protection Services、すなわち、SiteWatcher™、BrandWatcher™、および

ThreatWatcher™ へのアクセスが含まれます。これらのサービスを有効化すると、これらのサービスは組織の Web サイト、ブランド、および Web サーバーを保護するために動作します。

サービス	説明
SiteWatcher	組織の Web サイトが悪意あるプログラムに感染した場合に、警告を発し、そのサイトにアクセスする可能性がある顧客、潜在顧客やパートナーを保護するためにただちに処置をとれるようにします。
BrandWatcher	• 組織の Web サイトやブランドがフィッシングや悪意あるキーロギング攻撃の標的になった場合に、警告を発します。 • インターネット セキュリティ インテリジェンス、攻撃の詳細、およびその他のセキュリティ関連情報を提供することにより、処置をとり、顧客に通知し、広報関係の影響を最小にできるようにします。
ThreatWatcher	• 組織の Web サーバーをハッカーの観点からチェックし、既知の脆弱性や潜在的脅威に関するスキャンを行います。 • リスク レベルを報告し、Web ベースのポータルを通じて勧告を提供します。 • Web サーバーに対する悪意ある攻撃が発生する前に防止することを手助けします。

MyWebsense ポータルにログオンして、Websense Protection Services を有効にします。ThreatWatcher が有効になったら、MyWebsense にログオンして、登録済み Web サーバーに関する脅威レポートにアクセスします。

アカウント情報の構成

関連トピック :

- サブスクリプション、26 ページ
- データベースのダウンロードの設定、32 ページ
- プロトコルの使用、187 ページ

[設定] > [アカウント] ページを使用して、サブスクリプション情報の入力、表示、Websense Manager へのアクセスに使用する WebsenseAdministrator パスワードの変更を行います。WebsenseAdministrator は、Websense ソフトウェアの管理に使用されるデフォルトのマスタ管理者アカウントです。

また、このページで、Websense ソフトウェアがプロトコル使用状況データを匿名で Websense, Inc. に送信することを有効にできます。この情報は、3600 万を超えるインターネット サイトと 100 を超えるプロトコル定義のコレクションである Websense マスタ データベースの更新に使用されます (詳細については、Websense マスタ データベース、30 ページを参照)。

1. Websense ソフトウェアを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には、**[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ます。

   新しいサブスクリプション キーを入力し、[OK] をクリックすると、マスタ データベースのダウンロードが自動的に開始されます。
2. 最初のマスタ データベースのダウンロード後、以下の情報が表示されます：

キーの有効期限	現在のサブスクリプションの終了日。この日付以降は、マスタ データベースのダウンロードとネットワークのフィルタリングを継続するには、サブスクリプションを更新しなければなりません。
サブスクリプション中のネットワーク ユーザ数	フィルタリングの対象とすることができるネットワーク ユーザ数。
サブスクリプション中のリモート ユーザ数	フィルタリングの対象とすることができるネットワークの外部のユーザ数（オプションの Remote Filtering 機能が必要）。

3. **[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]** を選択すると、以下のようになります：
   - サブスクリプションの有効期限が切れると、すべてのユーザのインターネット アクセスがブロックされます。
   - サブスクリプションに含まれるユーザ数を超過するユーザのすべてのインターネット アクセスがブロックされます。

   このオプションを選択しないと、上記の状況のユーザに対してはインターネット アクセスのフィルタリングは行われません。
4. WebsenseAdministrator のパスワードを変更するには、まず現在のパスワードを入力し、続いて新しい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。パスワードは大文字と小文字を区別し、文字、数字、特殊文字、スペースを含めることができます。
   - WebsenseAdministrator アカウントには強力なパスワードを作成することをお勧めします。パスワードは、最低 8 文字で、大文字、小文字、数字、特殊文字を 1 字以上含めるべきです。
5. **[カテゴリおよびプロトコルのデータを Websense, Inc に送信する]** をオンにすると、Websense ソフトウェアは、Websense 定義カテゴリーおよびプロトコルに関する使用状況データを収集し、匿名で Websense, Inc. に提出します。

   この使用状況データは、Websense, Inc. が Websense ソフトウェアのフィルタリング機能を継続的に強化するのに役立ちます。

Websense マスタ データベース

関連トピック：
- リアルタイム データベース更新、31 ページ
- Real-Time Security Updates ェ、31 ページ
- カテゴリおよびプロトコルのフィルタリング、36 ページ
- Filtering Service の動作、284 ページ
- マスタ データベース ダウンロード ステータスの確認、285 ページ
- レジューム可能なマスタ データベースのダウンロード、285 ページ

Websense マスタ データベースには、インターネット コンテンツのフィルタリングの基礎となるカテゴリーおよびプロトコル定義が収納されています（カテゴリおよびプロトコルのフィルタリング、36 ページを参照）。

- **カテゴリ**は、類似の内容を持つ Web サイト（URL および IP アドレスで識別）をグループ化するのに使用されます。
- **プロトコル**定義は、ファイルの転送やインスタント メッセージの送信のような、類似の目的に使用されるインターネット通信プロトコルをグループ化します。

Websense ソフトウェアのインストール時にはフィルタリング データベースの限定バージョンがインストールされますが、できるだけ早く完全なマスタ データベースをダウンロードして、総合的なインターネット フィルタリング機能を可能にすることをお勧めします。マスタ データベースを初めてダウンロードするには、**[設定]** > **[アカウント]** ページでサブスクリプション キーを入力します（アカウント情報の構成、28 ページを参照）。

Websense ソフトウェアがプロキシを通じてダウンロードを行わなければならない場合は、**[設定]** > **[データベースのダウンロード]** ページを使用してプロキシ設定を行ってください（データベースのダウンロードの設定、32 ページを参照）。

完全なデータベースのダウンロードには、インターネットの接続スピード、帯域幅、使用可能なメモリ、ディスクの空き容量に応じて、数分から場合によっては 1 時間以上かかることがあります。

最初のダウンロード後は、Websense ソフトウェアは、設定されたスケジュールに従って、データベースの変更分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、32 ページを参照）。マスタ データベースは頻繁に更新されるので、デフォルトでは、データベースのダウンロードは毎日行われるようにスケジュールされます。

マスタ データベースが 14 日を越えて古くなると、Websense ソフトウェアはインターネット要求のフィルタリングを行いません。

いつでもデータベースのダウンロードを開始するには、または最後のデータベース ダウンロードのステータス、最後のダウンロードの日付、もしくは現在のデータベースのバージョン番号を表示するには、**[ステータス] > [今日]** ページに移動し、**[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 データベース更新

スケジュールされたダウンロードのほかに、Websense ソフトウェアは必要に応じてデータベースの緊急更新を行います。リアルタイム更新は、たとえば、一時的に誤って分類されたサイトを分類しなおすために行われます。これらの更新によって、サイトやプロトコルが適切にフィルタされることが確保されます。

Websense ソフトウェアがデータベース更新を毎時間チェックします。

最新の更新は、**[ステータス] > [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、296 ページを参照）。

Real-Time Security Updates™

Websense Web Security のユーザは、標準のリアルタイム データベース更新を受け取ることのほかに、Real-Time Security Updates を有効にすることにより、マスタ データベースのセキュリティ関連更新が Websense, Inc. から発表されるとただちにそれを受け取ることができます。

Real-Time Security Updates は、インターネットに関連するセキュリティの脅威に対する保護の追加の層を提供します。これらの更新が発表されるとただちにそれらをインストールすることにより、新手のフィッシング詐欺（なりすまし詐欺）、不正なアプリケーション、主力 Web サイトやアプリケーションに感染する悪意あるプログラムに対する脆弱性を減らします。

Filtering Service は 5 分ごとにセキュリティ更新がないかチェックしますが、更新はセキュリティの脅威が発生したときにのみ送信されるので、実際の変更は随時、正常なネットワーク活動を混乱させないように行われます。

[設定] > [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 を有効にします（データベースのダウンロードの設定、32 ページを参照）。

データベースのダウンロードの設定

関連トピック：

- アカウント情報の構成、28 ページ
- Websense マスタ データベース、30 ページ
- マスタ データベース ダウンロード ステータスの確認、285 ページ

[設定] > **[データベースのダウンロード]** ページを使用して、マスタ データベースの自動ダウンロードのスケジュールを設定します。また、データベースをダウンロードするために Websense ソフトウェアが通過しなければならないプロキシ サーバーやファイアウォールに関する重要な情報を指定します。

1. 自動ダウンロードの **[ダウンロード日]** を選択します。

   Websense ソフトウェアが中断することなくフィルタリングを継続するには、最低 14 日ごとにマスタ データベースをダウンロードしなければなりません。すべてのダウンロード日の選択を解除すると、Websense ソフトウェアは自動的に、データベースが 7 日の古さになるとダウンロードを試みます。

   ご注意：
   Real-Time Security Updates が有効になっている場合には、ダウンロード日の設定は無効になります（ステップ 3 を参照）。セキュリティ更新のために最新の標準データベースが使用可能であることを確保するために、毎日自動的にダウンロードが実行されます。

2. **[ダウンロードの時間帯]** の **[開始時刻]** と **[終了時刻]** を選択します。時刻を選択しないと、データベースのダウンロードは 21:00（午後 9 時）と 06:00（午前 6 時）の間に行われます。

   Websense ソフトウェアは、この時間帯の間のランダムな時刻を選択して、マスタ データベース サーバーに接続します。ダウンロード失敗の場合のアラートの構成については、システム アラートの設定、292 ページを参照してください。

   ご注意：
   マスタ データベースまたはその更新のダウンロード後、データベースがローカル メモリー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。

3. (Websense Web Security) **[リアルタイム セキュリティ更新を有効にする]** を選択して、Websense ソフトウェアが 5 分ごとにマスタ データベースのセキュリティ更新がないかチェックするようにします。セキュリティ更新が検出されたら、ただちにそれをダウンロードします。

Real-Time Security Updates は、新手のフィッシング詐欺（なりすまし詐欺）、不正なアプリケーション、主力 Web サイトやアプリケーションに感染する悪意あるプログラムのような脅威に対する脆弱性から迅速にネットワークを保護します。

4. Websense ソフトウェアが、マスタ データベースをダウンロードするために、（Websense ソフトウェアが通信できる統合製品以外の）プロキシ サーバーやプロキシ ファイアウォールを介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は、**[プロキシ サーバーまたはファイアウォールを使用する]** を選択します。続いて、以下の設定を行います。

サーバーの IP または名前	プロキシ サーバーまたはファイアウォールのホスト コンピュータの IP アドレスまたは名前を入力します。
ポート	データベースのダウンロードに使用されるポート番号を入力します（デフォルトは 8080）。

5. ステップ 4 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要求する場合は、**[認証を使用する]** を選択し、Websense ソフトウェアがインターネット アクセス権を獲得するために使用する **[ユーザ名]** と **[パスワード]** を入力します。

> **ご注意：**
> [認証を使用する] を選択した場合は、マスタ データベースのダウンロードを可能にするには、プロキシ サーバーまたはファイアウォールはクリア 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。

デフォルトでは、ユーザ名およびパスワードは、Policy Server コンピュータのロケールのキャラクタ セットと一致するようにエンコードされます。このエンコードは、**[設定]** > **[ディレクトリ サービス]** ページで手動で設定できます（詳細ディレクトリ設定、66 ページを参照）。

ネットワーク構成のテスト

インターネット要求のフィルタリングを行うには、Websense ソフトウェアがネットワークのコンピュータへのおよびネットワークのコンピュータからのインターネット トラフィックを認識しなければなりません。ネットワーク トラフィック検出ツールを使用して、このインターネット通信がフィルタリング ソフトウェアにとって認識可能であることを確保します。その手順は、Network Agent 設定の確認、352 ページ を参照してください。

検出ツールがネットワークのすべてのセグメントを認識できない場合、構成手順の詳細については、ネットワークの構成、343 ページを参照してください。

Websense テクニカル サポート

Websense, Inc. は、お客様に満足していただくことに努めています。いつでも Websense Technical Support Web サイトにアクセスして、最新のリリース情報を知り、Knowledge Base にアクセスし、あるいはサポート要求を作成することができます。

www.websense.com/SupportPortal/

オンライン要求に対しては、営業時間中は約 4 時間で回答いたします。営業時間外のお問い合わせについては、次の営業日に回答します。

電話によるお問合せにも、対応いたします。電話によるご要求に速やかに効率的にお答えするために、以下についてご用意ください :

- Websense サブスクリプション キー
- Websense Manager にアクセスできること
- Filtering Service および Log Server、およびデータベース サーバー (Microsoft SQL Server または MSDE) を実行しているコンピュータへアクセスできること
- Websense ログ データベース へのアクセス許可
- ネットワークの構造を熟知しているか、熟知している担当者にすぐに連絡がつくこと
- Filtering ServiceおよびWebsense Managerが動作しているコンピュータの仕様
- Filtering Service マシンで実行している他のアプリケーションのリスト

重大な問題の場合は、追加情報が必要な場合があります。

標準の電話によるお問い合わせは、月曜から金曜までの営業時間中、次の番号で受け付けております :

- カルフォルニア州、サンディエゴ : **+1.858.458.2940**
- 英国、ロンドン : **+44 (0) 1932 796244**

営業時間およびその他のサポート オプションについては、上記のサポート Web サイトをご覧ください。

日本のお客様は、販売代理店を通じて迅速なサービスを受けることができます。

2 インターネット使用のフィルタ

関連トピック：

- カテゴリおよびプロトコルのフィルタリング、36 ページ
- フィルタに関する作業、47 ページ
- Websense フィルタリング設定の構成、56 ページ
- インターネット フィルタリング ポリシー、73 ページ
- フィルタリング ポリシーの調整、169 ページ

ポリシーが、ユーザのインターネット アクセスを管理します。ポリシーとは、Web サイトおよびインターネット アプリケーションへのアクセスを、どのようにしていつフィルタするかを Websense ソフトウェアに指示するスケジュールです。単純化すると、ポリシーは以下によって構成されます：

- **カテゴリ フィルタ** ウェブ サイト カテゴリに対してアクション（許可、ブロック）を適用するために使用されます。
- **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 プロトコルにアクションを適用するために使用されます。
- いつ各フィルタを実施するかを決定するスケジュール。

ポリシーに基づいたフィルタリングによって、クライアント（ネットワークの中のユーザ、グループ、およびコンピュータ）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。まず、フィルタを作成して明確なインターネット アクセス制限を定義し、次に、フィルタを使用してポリシーを構築します。

最初のインストレーションにおいては、Websense ソフトウェアは**デフォルト** ポリシーを作成し、これを使用して、サブスクリプション キーが入力されるとただちにインターネット要求の監視を開始します（デフォルト ポリ

シー、74 ページを参照)。最初は、デフォルト ポリシーはすべての要求を許可します。

> **ご注意 :**
> 以前の Websense ソフトウェア バージョンからアップグレードした場合は、既存のポリシー設定が保存されます。アップグレード後に、ポリシーを見直し、それらが依然として適切であることを確認してください。

異なるフィルタリング制限を異なるクライアントに適用するには、まずカテゴリ フィルタを定義します。以下を定義します :

- ビジネスおよび経済カテゴリ、教育カテゴリ、ならびにニュースおよびメディア カテゴリを除くすべての Web サイトへのアクセスをブロックする 1 つのカテゴリ フィルタ。
- セキュリティ リスクを示しているものおよびアダルト題材を含むものを除くすべての Web サイトを許可する第 2 のカテゴリ フィルタ。
- Webサイトへのアクセスをブロックせずに監視する第3のカテゴリ フィルタ (カテゴリ フィルタの作成、48 ページを参照)。

これらのカテゴリ フィルタとともに、以下を定義します :

- インスタント メッセージおよびチャット、P2P ファイル共有、プロキシ回避、ならびにストリーミング メディア プロトコル グループへのアクセスをブロックする 1 つのプロトコル フィルタ。
- プロキシ回避に関連するものを除くすべての非HTTP プロトコルを許可する第 2 のプロトコル フィルタ。
- すべての非HTTPプロトコルを許可する第3のプロトコル フィルタ(プロトコル フィルタの作成、51 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ら、これらをポリシーに追加し、クライアントに適用することができます (インターネット フィルタリング ポリシー、73 ページを参照)。

カテゴリおよびプロトコルのフィルタリング

Websense マスタ データベースは、類似の Web サイト (URL および IP アドレスによって識別) を**カテゴリ**に整理します。各カテゴリには、「アダルト」、「ギャンブル」、「P2P ファイル共有」のように、説明的な名前が付けられます。また、独自のカスタム カテゴリを作成して、組織が特に関心を持つサイトをグループ化することができます (カスタム カテゴリの作成、180 ページを参照)。マスタ データベースカテゴリとユーザ定義カテゴリがともに、インターネット フィルタリングの基礎を形成します。

Websense, Inc. は、マスタ データベースの中のカテゴリやサイトについて価値判断は行いません。カテゴリは、加入している顧客が関心を持つサイトを

うまくグループ化できるように工夫されています。カテゴリは、サイトもしくはサイトのグループ、またはそれらを公表している個人や集団を特徴付けることを意図したものではなく、そのように解釈すべきものではありません。同様に、Websense カテゴリに付けられたラベルは、便宜的略称であって、そのように分類された題材やサイトに対する意見もしくは態度、承認その他を伝えるものではなく、伝えていると解釈されるべきではありません。

マスタ データベース カテゴリの最新リストは、以下で入手できます：

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

サイトをマスタ データベースに追加することを提案するには、Websense Manager の右側のショートカット ペインの [**新規カテゴリの提案**] をクリックするか、または下記サイトにアクセスしてください：

www.websense.com/SupportPortal/SiteLookup.aspx

MyWebsense ポータルにログオン後、Site Lookup および Category Suggestion tool を選択してください。

Websense Manager で**カテゴリ フィルタ**を作成したら、どのカテゴリをブロックし、どのカテゴリを許可するかを選択します。

Websense マスタ データベースには、URL カテゴリのほかに、非 HTTP インターネット トラフィックの管理に使用するプロトコル グループが含まれています。各プロトコル グループには、類似のタイプのインターネット プロトコル (FTP や IRC) およびアプリケーション (AOL Instant Messenger や BitTorrent) が定義されます。定義は、頻繁に、毎晩のように検証され更新されます。

カテゴリの場合と同様に、インターネット フィルタリングに使用するためのカスタム プロトコルを定義できます。

マスタ データベース プロトコルの最新リストは、以下で入手できます：

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

プロトコル フィルタを作成したら、どのプロトコルをブロックし、どのプロトコルを許可するかを選択します。

ご注意：
プロトコルに基づいたフィルタリングを可能にするには、Network Agent がインストールされていなければなりません。

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。ポート番号を動的に割り当てる Websense 定義プロトコルだけを、アウトバウンド トラフィックとしてブロックすることができます。

新しいカテゴリおよびプロトコル

新しいカテゴリおよびプロトコルがマスタ データベースに追加されると、それぞれにデフォルトのフィルタリング アクション（**許可**または**ブロック**）が割り当てられます（フィルタリング アクション、43 ページを参照）。

- デフォルト アクションは、すべてのアクティブなカテゴリおよびプロトコルに適用されます（フィルタに関する作業、47 ページを参照）。アクティブなフィルタを編集して、カテゴリまたはプロトコルをフィルタする方法を変更します。
- デフォルト アクションは、問題のサイトまたはプロトコルが一般にビジネスに適しているとみなされているかどうかに関するフィードバックに基づいています。

新しいカテゴリまたはプロトコルがマスタ データベースに追加されたときはシステム アラートを生成し、通知するように、Websense ソフトウェアを構成できます。詳細は、アラート、289 ページ を参照してください。

特殊カテゴリ

マスタ データベースには、特殊なタイプのインターネット使用状況を管理するのに役立つ特殊カテゴリが含まれています。Websense ソフトウェアのすべてのエディションで、以下のカテゴリが使用可能です：

- 「**スペシャル イベント**」カテゴリは、ホット トピックとみなされるサイトを分類するために使用され、イベントに関連したインターネット トラフィックの急増に対処するのに役立ちます。たとえば、ワールドカップの公式サイトは、一般には「スポーツ」カテゴリに含まれますが、ワールドカップ本大会の期間中は「スペシャル イベント」カテゴリーに移されます。

  「スペシャル イベント」カテゴリの更新は、スケジュールされたダウンロード中にマスタ データベースに追加されます。サイトは短期間このカテゴリに追加され、その期間後は別のカテゴリに移されるか、マスタ データベースから削除されます。
- 「**生産性**」カテゴリは、時間を浪費する行動を防止することを重視したものです。
  - 広告宣伝
  - フリーウェア / ソフトウェアダウンロード
  - インスタント・メッセージ
  - オンライン証券＆トレーディング
  - 報酬サイト
- 「**帯域幅**」カテゴリは、ネットワーク帯域幅を節約することを重視したものです。
  - インターネット・ラジオと TV
  - インターネット電話
  - ピア・ツー・ピアによるファイル共有

- 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

Websense Web Security には、追加のセキュリティ カテゴリが含まれてます :

- 「**Websense Security Filtering**」(単に「**セキュリティ**」とも呼ばれます) 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ことができる悪意あるプログラムを含むインターネット サイトを重視したものです。このカテゴリのサイトは、デフォルトでブロックされます。
  - ボット ネットワーク
  - キーロガー
  - MMC 感染サイト
  - フィッシングとその他詐欺サイト
  - 潜在的に望ましくないソフトウェア
  - スパイウェア
- 「**より広範囲の危険性への対処**」は、悪意がある可能性がある Web サイトを重視したものです。サブカテゴリ「身元を偽装しているサイト」と「脆弱性をつく可能性のあるサイト」に含まれるサイトは、デフォルトでブロックされます。
  - 「**身元を偽装しているサイト**」には、真の性格や本性を隠したサイトや潜在的な悪意を示唆する要素を含むサイトが含まれます。
  - 「**脆弱性をつく可能性のあるサイト**」には、既知のエクスプロイトコードが存在することが分かっている、あるいはエクスプロイトコードが存在する可能性があるサイトが含まれます。
  - 「**潜在的な危険性を含むサイト**」には、ほとんどまたはまったく無用なコンテンツを含んでいると思われるサイトが含まれます。

「より広範囲の危険性への対処」グループは、レピュテーションに基づいて悪意がある可能性がある Web サイトをフィルタします。サイトのレピュテーションは、潜在的な悪意あるアクティビティの早期の兆候に基づいています。攻撃者は、たとえば一般的なミススペリングを含む URL や、他の点では正統な URL に似た URL をターゲットにする場合があります。そのようなサイトは、従来のフィルタが更新されてこれらのサイトを悪意があるサイトとして反映する前に、マルウェアをユーザに配布するために使用される可能性があります。

Websense セキュリティ リサーチが潜在的脅威を検出したら、Websense がサイトの最終分類に 100% 確信を持つまでの間、それは「より広範囲の危険性への対処」カテゴリに加えられます。

リスク クラス

関連トピック：
- カテゴリのリスククラスへの割り当て、308 ページ
- プレゼンテーション レポート、98 ページ
- 調査レポート、118 ページ

Websense マスタ データベースのカテゴリは、**リスク クラス**別にグループ化されています。リスク クラスは、カテゴリのグループに属するサイトがもたらす脆弱性のタイプもしくはレベルを示唆しています。

リスククラスは 主にレポートで使用されます。[今日] および [履歴] ページにはグラフが含まれていますが、そこではインターネット アクティビティがリスク クラス別に表示されます。また、リスク クラス別に整理されたプレゼンテーションや調査レポートを生成することができます。

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、最初は、「基本セキュリティ」カテゴリ フィルタが、「セキュリティ リスク」クラスのデフォルト カテゴリをすべてブロックします。独自のカテゴリ フィルタを作成する際には、リスク クラス グループをガイドラインとして使用して、カテゴリを許可するか、ブロックするか、または何らかの方法で制限するかの決定に役立てることができます。

Websense ソフトウェアには、以下に示す 5 つのリスク クラスが含まれています。デフォルトでは、Websense ソフトウェアは、以下のカテゴリを各リスクにグループ化します。

- 1 つのカテゴリーを複数のリスク クラスに入れることができ、あるいはどのリスク クラスにも割り当てないこともできます。
- マスタ データベースでは、グループ化は定期的に変更されます。

法的責任

アダルト (アダルト・コンテンツ、ランジェリー & 水着、ヌード、およびセックスを含む)
帯域幅 > ピア・ツー・ピアによるファイル共有
ギャンブル
違法行為
IT > ハッカー関連およびプロキシによるブロック回避
過激派グループ
人種差別
悪趣味
暴力
武器

ネットワーク帯域幅損失

帯域幅（インターネット・ラジオと TV、インターネット電話、ピア・ツー・ピアによるファイル共有、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・メディアを含む）

エンターテインメント > MP3 および音楽ダウンロードサービス

生産性 > 宣伝広告ならびにフリーウェア / ソフトウェアダウンロード

業務関連の使用

ビジネス & 経済（金融情報とサービスを含む）

教育 > 教材および参考資料

政府（軍隊を含む）

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、および URL 翻訳サイトを含む）

旅行

乗り物

セキュリティ リスク

帯域幅 > ピア・ツー・ピアによるファイル共有

より広範囲の危険性への対処（身元を偽装しているサイト、脆弱性をつく可能性のあるサイト、および潜在的な危険性を含むサイトを含む）[Websense Web Security]

IT > ハッカー関連およびプロキシによるブロック回避

生産性 > フリーウェア / ソフトウェアダウンロード

セキュリティ（ボット ネットワーク、キーロガー、MMC 感染サイト、フィッシングとその他詐欺サイト、潜在的に望ましくないソフトウェア、およびスパイウェアを含む）

生産性の損失

中絶（妊娠中絶賛成論および妊娠中絶反対論を含む）

アダルト > 性教育

主張グループ

帯域幅 > インターネット・ラジオと TV、ピア・ツー・ピアによるファイル共有、およびストリーミング・メディア

麻薬 / 医薬品（麻薬 / 医薬品の乱用、マリファナ、処方薬、および栄養補助食品 / 非規制化合物を含む）

教育（文化施設および教育機関を含む）

エンターテインメント（MP3 および音楽ダウンロードサービス）

ギャンブル

ゲーム

政府 > 政治団体

健康

IT > Web ホスティング

インターネット・コミュニケーション（一般の電子メール、組織の電子メール、テキストとメディアによるメッセージ配信、Web チャットを含む）

求人情報

生産性の損失

ニュース・メディア（娯楽雑誌を含む）

生産性（フリーウェア / ソフトウェアダウンロード、インスタント・メッセージ、掲示板、オンライン証券＆トレーディング、および報酬サイトを含む）

宗教（非伝統的な宗教 / オカルト / 民間伝承、および伝統宗教）

ショッピング（インターネット オークションおよび不動産を含む）

社会組織（専門家・従業員団体、奉仕・慈善事業団体、および社交・友好団体を含む）

社会 & ライフスタイル（アルコール & 煙草、ゲイ / レズビアン / バイセクシャル、趣味、出会い / 結婚 / お見合いサービス、レストラン & 食事、および SNS と個人のサイト）

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

乗り物

優先管理者は、各リスク クラスに割り当てられたカテゴリを、**[設定]** > **[リスク クラス]** ページで変更することができます（カテゴリのリスククラスへの割り当て、308 ページを参照）。

「セキュリティ」プロトコル グループ

「セキュリティ」および「より広範囲の危険性への対処」カテゴリのほかに、Websense Web Security には、インターネットを介して送信されるスパイウェアおよび悪意のあるプログラムもしくはコンテンツを検出しこれに対して保護することを手助けすることを目的とする 2 つのプロトコルが含まれています。

- **「悪質なトラフィック」**プロトコル グループには、**「ボット ネットワーク」**プロトコルが含まれます。これは、悪意のある目的で botnet に接続を試みる Bot が生成するコマンド アンド 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。
- **「悪質なトラフィック – モニタのみ」**プロトコル グループは、悪意のあるソフトウェアに関連しているかもしれないトラフィックを識別するために使用されます。
  - **「電子メールで運ばれるワーム」**は、電子メールで運ばれるワーム攻撃によって生成されたものかもしれないアウトバウンド SMTP トラフィックを追跡します。
  - **「その他の悪質なトラフィック」**は、悪意のあるアプリケーションとの関係が疑われ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。

「悪質なトラフィック」プロトコル グループは、デフォルトでブロックされ、プロトコル フィルタの中に構成することができます（プロトコル フィルタの編集、52 ページを参照）。「悪質なトラフィック – モニタのみ」プロトコルは、報告のために記録することはできますが、他のフィルタリング アクションは適用できません。

Instant Messaging Attachment Manager

Instant Messaging (IM) Attachment Manager は、オプション機能です。この機能に加入すると、AOL/ICQ、Microsoft (MSN)、および Yahoo を含む IM クライアントとのファイル共有を制限できます。これによって、IM トラフィックは許可しても、IM クライアントによる添付ファイルの転送はブロックすることができます。

「インスタントメッセージングファイルの添付」は、複数の IM クライアントの定義を含むプロトコル グループです。IM Attachment Manager を有効にすると、これらのプロトコルがすべてのアクティブなプロトコル フィルタのプロトコル リストおよび [プロトコルの管理] ページに表示されます。

IM 添付ファイル フィルタリングは、内部トラフィックと外部トラフィックの両方に適用できます。内部トラフィック フィルタリングを有効にするには、**[設定] > [Network Agent] > [グローバル設定]** ページで監視対象となるネットワークの部分を定義します (グローバル設定、346 ページを参照)。

フィルタリング アクション

カテゴリ フィルタおよびプロトコル フィルタは、各カテゴリまたはプロトコルに 1 つの**アクション**を割り当てます。これが、クライアントのインターネット要求に応答して Websense フィルタリング ソフトウェアが取る処置です。カテゴリおよびプロトコルの両方に適用されるアクションは、次のとおりです :

- 要求を**ブロック**します。ユーザはブロック ページまたはブロック メッセージを受け取り、サイトを見ることはできず、あるいはインターネット アプリケーションを使用できません。
- 要求を**許可**します。ユーザはサイトを見ることができ、あるいはインターネット アプリケーションを使用できます。
- 現在の**帯域幅**使用量を評価してから、要求をブロックまたは許可します。このアクションが有効になっている場合、帯域幅使用量が指定されたしきい値に達すると、特定のカテゴリまたはプロトコルに対するそれ以上のインターネット要求はブロックされます。Bandwidth Optimizer による帯域幅の管理、194 ページを参照してください。

カテゴリに対してのみ、追加のアクションを適用することができます。

ご注意 :
「確認」および「割り当て時間」オプションは、個々のクライアント (ユーザ、グループ、およびコンピュータ) が複数の Policy Server によって管理されている場合は使用すべきではありません。

これらの機能に関連する時間情報が Policy Server 間で共有されておらず、影響を受けるクライアントが、意図したより多いまたは少ないインターネット アクセスを許可される可能性があります。

- 「**確認**」– ユーザはブロック ページを受け取り、そのサイトに業務目的でアクセスすることの確認を求められます ユーザが **[継続]** をクリックすると、サイトを表示することができます。

  [継続] をクリックすると、タイマーがスタートします。設定された時間の間 (デフォルトでは 60 秒) に、ユーザは「確認」カテゴリの他のサイトを、ふたたびブロック ページを受け取ることなく、閲覧できます。この時間が終了すると、別の「確認」サイトを閲覧しようとすると、ふたたびブロック ページが送られてきます。

  デフォルト時間は、**[設定] > [フィルタリング]** ページで変更できます。
- 「**割り当て時間**」– ユーザはブロック ページを受け取り、割り当て時間を使用してサイトを表示するかどうかたずねられます。ユーザが **[割り当て時間の使用]** をクリックすると、サイトを表示することができます。

  [割り当て時間の使用] をクリックすると、2 つのタイマー、すなわち割り当て時間セッション タイマーと合計割り当て時間タイマーがスタートします。

  - デフォルトの**セッション**時間中に(デフォルトでは10分)ユーザが追加の「割り当て時間」サイトを要求した場合は、別のブロック ページを受け取ることなくそれらのサイトを表示できます。
  - **合計**割り当て時間は、毎日割り当てられます。それを使い切ると、各クライアントは翌日まで、「割り当て時間」カテゴリのサイトにアクセスするのを待たなければなりません。1 日当りの割り当て時間は (デフォルトでは 60 分)、**[設定] > [フィルタリング]** ページで設定します。1 日当りの割り当て時間は、個人ベースでクライアントに許可できます。詳細は、割り当て時間を使用したインターネット アクセスの制限、44 ページ を参照してください。
- 「**キーワードをブロック**」– キーワードを定義し、キーワードのブロックを有効にすると、サイトの URL にブロックされるキーワードが含まれている場合、そのサイトを要求するユーザは、サイトへのアクセスを許可されません。キーワードに基づくフィルタリング、182 ページを参照してください。
- 「**ファイル タイプをブロック**」– ファイル タイプのブロックを有効にすると、ブロックされるタイプのファイルをダウンロードしようとするユーザは、ブロック ページを受け取り、ファイルはダウンロードされません。ファイル タイプに基づくトラフィックの管理、196 ページを参照してください。

割り当て時間を使用したインターネット アクセスの制限

[割り当て時間の使用] をクリックすると、割り当て時間セッションが終了するまで、「割り当て時間」カテゴリのサイトを閲覧できます。デフォルト

の割り当て時間セッション時間（[**設定**] > [**フィルタリング**] ページで設定）は、10 分です。

> **ご注意：**
> 個々のクライアントが複数の Policy Server で管理されている場合は、「割り当て時間」オプションを使用すべきではありません。
>
> この機能に関連する時間情報が Policy Server 間で共有されておらず、影響を受けるクライアントが、意図したより多いまたは少ないインターネット アクセスを許可される可能性があります。

割り当て時間セッションが終了すると、「割り当て時間」サイトを要求すると別の割り当て時間ブロック メッセージが送られてきます。1 日の割り当て時間を使い切っていないユーザは、新しい割り当て時間セッションを開始することができます。

「割り当て時間」が設定されると、Websense ソフトウェアは優先順位リストを使用して、ユーザが「割り当て時間」カテゴリのサイトを要求した場合の対応の仕方を決定します。Websense ソフトウェアは、以下に対して設定された割り当て時間を参照します：

1. ユーザ
2. コンピュータまたはネットワーク クライアント
3. ユーザが所属するグループ

   ユーザが複数のグループに所属している場合は、Websense ソフトウェアは、[**設定**] > [**フィルタリング**] ページの [**より厳密な制限でブロックをする**] 設定に従って、割り当て時間を許可します（Websense フィルタリング設定の構成、56 ページを参照）。
4. デフォルト割り当て時間

Java や Flash アプレットのようなインターネット アプレットは、割り当て時間制限に期待通りに応答できない場合があります。割り当て時間の制限を受けるサイトからアクセスしている場合でも、ブラウザ内で動作しているアプレットは設定された割り当て時間セッション時間を超えて動作し続けることができます。

この理由は、こ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、元のホスト サーバーと通信することなくアプリケーションのように動作しているからです。しかし、ユーザがブラウザの [リフレッシュ] ボタンをクリックすると、Websense ソフトウェアはホスト サーバーへの通信を検出し、該当する割り当て時間制限に従って要求をブロックします。

パスワード アクセス

パスワード アクセスによって、有効なパスワードを持つユーザは、Websense ソフトウェアがブロックしたサイトにアクセスできます。パス

ワード アクセスは、個々のクライアント（ユーザ、グループ、コンピュータ、またはネットワーク）に対して許可されます。

パスワード アクセスが有効になっている場合は、Websense ブロック メッセージにパスワード フィールドが含まれます。有効なパスワードを入力したクライアントは、限定された時間の間、ブロックされたサイトにアクセスできます。

ご注意：
個々のクライアントが複数の Policy Server で管理されている場合は、パスワード アクセス オプションを使用すべきではありません。

この機能に関連する時間情報が Policy Server 間で共有されておらず、影響を受けるクライアントが、意図したより多いまたは少ないインターネット アクセスを許可される可能性があります。

パスワード アクセス オプションは、**[設定]** > **[フィルタリング]** ページで有効にします（Websense フィルタリング設定の構成、56 ページを参照）。

[ポリシーの管理] > **[クライアント]** ページで、特定のクライアントに対してパスワード アクセス権限を付与します（クライアントの追加、69 ページまたはクライアント設定の変更、70 ページを参照）。

検索フィルタリング

検索フィルタリングは、一部の検索エンジンが提供している機能で、ユーザ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。

本来、インターネット検索エンジンの検索結果には、検索基準に一致するサイトに関連するサムネール画像が含まれる場合があります。それらのサムネールがブロックされたサイトに関連するものである場合、Websense ソフトウェアは、ユーザが完全なサイトにアクセスするのを妨げますが、検索エンジンが画像を表示することは妨げません。

検索フィルタリングを有効にすると、Websense ソフトウェアは、ブロックされたサイトに関連するサムネール画像が検索結果の中に表示されるのを停止する検索エンジン機能を有効にします。検索フィルタリングを有効にすると、ローカルおよびリモートの両方のフィルタリング クライアントが影響を受けます。

Websense, Inc. は、検索フィルタリング機能を持つ検索エンジンのデータベースを維持しています。検索エンジンがデータベースに追加または削除されると、アラートが生成されます（アラート、289 ページを参照）。

検索フィルタリングは、**[設定]** > **[フィルタリング]** ページで有効にします。詳細は、Websense フィルタリング設定の構成、56 ページ を参照してください。

フィルタに関する作業

関連トピック：

- カテゴリおよびプロトコルのフィルタリング、36 ページ
- インターネット フィルタリング ポリシー、73 ページ
- カテゴリ フィルタの作成、48 ページ
- プロトコル フィルタの作成、51 ページ
- 制限付きアクセス フィルタの作成、172 ページ

Websense Manager の［**ポリシーの管理**］>［**フィルタ**］ページを使用して、カテゴリおよびプロトコル フィルタを表示、作成、および変更し、その他のフィルタリング ツールを使用して作業します。

［フィルタ］ページは、以下の 3 つのセクションに分かれています：

- ［**カテゴリ フィルタ**］では、ブロックするカテゴリと許可するカテゴリを決定します。
- ［**プロトコル フィルタ**］では、ブロックする、および許可する非 HTTP プロトコルを決定します。

  プロトコルに基づいたフィルタリングを可能にするには、Network Agent がインストールされていなければなりません。
- ［**制限付きアクセス フィルタ**］では、許可された Web サイトの限定リストを定義します（ユーザのアクセスを指定したサイトのリストに制限、170 ページを参照）。

カテゴリ フィルタ、プロトコル フィルタ、および制限つきアクセス フィルタは、**ポリシー**の基本的構成要素です。各ポリシーは、1 つ以上のカテゴリ フィルタまたは制限つきアクセス フィルタと 1 つのプロトコル フィルタで構成され、特定のスケジュールに基づいて選択され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、または制限つきアクセス 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、以下の項目を参照してください：
  - カテゴリ フィルタの編集、49 ページ
  - プロトコル フィルタの編集、52 ページ
  - 制限付きアクセス フィルタの編集、172 ページ
- 新しいカテゴリ フィルタ、プロトコル フィルタ、または制限つきアクセス フィルタを作成するには、［**追加**］をクリックします。詳細については、以下の項目を参照してください：
  - カテゴリ フィルタの作成、48 ページ
  - プロトコル フィルタの作成、51 ページ
  - 制限付きアクセス フィルタの作成、172 ページ

既存のフィルタを複製するには、フィルタ名のそばのチェックボックスをチェックし、[**コピー**]をクリックします。このコピーには、一意性を保つために元のフィルタの名前の後に数字を付加した名前が付けられ、フィルタのリストに追加されます。このコピーを、他のフィルタと同じように編集します。

指定済み管理ロールを作成した場合（指定済み管理、239 ページを参照）、優先管理者は自分が作成したフィルタを、指定済み管理者が使用するために他のロールにコピーすることができます。

フィルタを別のロールにコピーするには、まずフィルタ名のそばのチェックボックスをオンにし、[**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、175 ページ を参照してください。

カテゴリ フィルタの作成

関連トピック：

- フィルタに関する作業、47 ページ
- カテゴリ フィルタの編集、49 ページ

[**ポリシーの管理**] > [**フィルタ**] > [**カテゴリ フィルタの追加**] ページを使用して、新しいカテゴリ フィルタを作成します。事前定義されたテンプレートから作業するか、または新しいフィルタのベースとして使用するために既存のカテゴリ フィルタのコピーを作成することができます。

1. 一意的な**フィルタ名**を入力します。名前は長さが 1 ～ 50 字で、以下の文字を含めることはできません：

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

   フィルタ名にスペース、ダッシュ、およびアポストロフを含めることができます。
2. フィルタの簡単な**説明**を入力します。この説明は、[フィルタ] ページの [カテゴリ フィルタ] セクションのフィルタ名のそばに表示されるので、フィルタの目的を説明するものであるべきです。

   フィルタ名での文字に関する制限がこの説明にも適用されますが、例外として、説明にはピリオド (.) とカンマ (,) を含めることができます。
3. ドロップダウンリストからエントリを選択して、テンプレートを使用するか、既存のフィルタのコピーを作成するかを決定します。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、54 ページを参照してください。
4. 新しいフィルタを表示および編集するには、[OK] をクリックします。フィルタが [フィルタ] ページの [**カテゴリ フィルタ**] 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、続いて「カテゴリ フィルタの編集」の手順を行います。

カテゴリ フィルタの編集

関連トピック：

- カテゴリおよびプロトコルのフィルタリング、36 ページ
- フィルタリング アクション、43 ページ
- 割り当て時間を使用したインターネット アクセスの制限、44 ページ
- パスワード アクセス、45 ページ
- フィルタに関する作業、47 ページ
- カテゴリの使用、177 ページ

[ポリシーの管理] > **[フィルタ]** > **[カテゴリ フィルタ の編集]** ページを使用して、既存のカテゴリ フィルタを変更します。

重要

カテゴリ フィルタを編集すると、変更はそのフィルタを実施するすべてのポリシーに影響を与えます。

別の指定済み管理ロールの同じ名前のカテゴリ フィルタを実施するポリシーは、影響を受けません。

フィルタ名と説明が、ページの上部に表示されます。

- **[名前の変更]** をクリックして、フィルタ名を変更します。
- **[説明]** フィールドに入力して、フィルタの説明を変更します。

[このフィルタを使用しているポリシー] のそばの番号は、選択されているフィルタを現在使用しているポリシーの数を示しています。そのカテゴリ フィルタがアクティブになっている場合、**[ポリシーの表示]** をクリックすると、そのフィルタを実施しているポリシーのリストが表示されます。

ページの下部に、カテゴリのリストおよび現在それぞれのカテゴリに適用されているアクションが表示されます。

1. **カテゴリ** リストのエントリを選択して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付けられたフィルタリング アクションを変更します。
2. カテゴリに適用されているアクションを変更する前に、**[カテゴリの詳細]** セクションを使用してカテゴリに関連付けられた特殊な属性があれば検討します。
   - カテゴリに割り当てられた再分類された URL またはフィルタなし URL がある場合、これを検討するには、**[このカテゴリのカスタム URL を参照]** をクリックします。特定のサイトのフィルタリングの再定義、184 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を検討するには、[**このカテゴリのキーワードを参照**] をクリックします。キーワードに基づくフィルタリング、182 ページを参照してください。
- カテゴリのカスタム URL またはキーワードの定義に使用されている正規表現を検討するには、[**このカテゴリの正規表現を参照**] をクリックします。

3. カテゴリ リストの下部のボタンを使用して、選択されているカテゴリに適用されているアクションを変更します。使用可能なアクションの詳細については、フィルタリング アクション、43 ページを参照してください。

   指定済み管理者は、優先管理者がロックしたカテゴリに関連付けられたアクションを変更することはできません。詳細は、すべてのロールのフィルタリング制限の定義、268 ページ を参照してください。
4. カテゴリ リストの右側のチェックボックスを使用して、選択されているカテゴリに対して高度のフィルタリング アクションを適用します。:
   - キーワードをフィルタリングに使用する方法を変更するには、[**キーワードをブロック**] をオンまたはオフにします。キーワードに基づくフィルタリング、182 ページ
   - 選択されているカテゴリのサイトの特定タイプのファイルにユーザがアクセスできるようにするかどうかを決定するには、[**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、196 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、1 つまたは複数のファイル タイプを選択してください。
   - カテゴリのサイトへのアクセスを一定の帯域幅しきい値に基づいて制限するかどうかを指定するには、[**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、194 ページを参照してください。

     帯域幅に基づいてブロックすることを選択した場合は、使用するしきい値限界を指定してください。
5. 他のカテゴリに適用するフィルタリング アクションに対して、ステップ 1 ～ 3 を繰り返して変更を加えます。
6. フィルタの編集が完了したら、[OK] をクリックして変更をキャッシュし、[フィルタ] ページに戻ります。[**すべて保存**] 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にするには、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 フィルタリング ポリシー、73 ページを参照してください。

プロトコル フィルタの作成

関連トピック：
- カテゴリおよびプロトコルのフィルタリング、36 ページ
- フィルタリング アクション、43 ページ
- プロトコル フィルタの編集、52 ページ
- プロトコルの使用、187 ページ

[ポリシーの管理] > **[フィルタ]** > **[プロトコル フィルタの追加]** ページを使用して、新しいプロトコル フィルタを定義します。事前定義されたテンプレートから作業するか、または新しいフィルタのベースとして使用するために既存のプロトコル フィルタのコピーを作成することができます。

1. 一意的な**フィルタ名**を入力します。名前は長さが 1 ～ 50 字で、以下の文字を含めることはできません：

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

   フィルタ名にスペース、ダッシュ、およびアポストロフを含めることができます。
2. フィルタの簡単な**説明**を入力します。この説明は、[フィルタ] ページの [プロトコル フィルタ] セクションのフィルタ名のそばに表示されるので、フィルタの目的を説明するものであるべきです。

   フィルタ名での文字に関する制限がこの説明にも適用されますが、例外として、説明にはピリオド (.) とカンマ (,) を含めることができます。
3. ドロップダウンリストからエントリを選択して、テンプレートを使用するか（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、54 ページを参照）、または新しいフィルタのベースとして既存のフィルタをコピーするかを選択します。
4. 新しいフィルタを表示および編集するには、**[OK]** をクリックします。フィルタが [フィルタ] ページの **[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には、続いて「プロトコル フィルタの編集」の手順を行います。

プロトコル フィルタの編集

関連トピック：

- カテゴリおよびプロトコルのフィルタリング、36 ページ
- プロトコル フィルタの作成、51 ページ
- フィルタリング アクション、43 ページ
- プロトコルの使用、187 ページ
- Bandwidth Optimizer による帯域幅の管理、194 ページ

[ポリシーの管理] > **[フィルタ]** > **[プロトコル フィルタ の編集]** ページを使用して、既存のプロトコル フィルタを変更します。

重要
ここでの変更内容は、このフィルタを実施するすべてのポリシーに影響を与えます。

別の指定済み管理ロールの同じ名前のプロトコル フィルタを実施するポリシーは、影響を受けません。

フィルタ名と説明が、ページの上部に表示されます。

- **[名前の変更]** をクリックして、フィルタ名を変更します。
- **[説明]** フィールドに入力して、フィルタの説明を変更します。

[このフィルタを使用しているポリシー] のそばの番号は、選択されているフィルタを現在使用しているポリシーの数を示しています。そのプロトコル フィルタがアクティブになっている場合、**[ポリシーの表示]** をクリックすると、そのフィルタを実施しているポリシーのリストが表示されます。

ページの下部に、プロトコルのリストおよび現在それぞれのプロトコルに適用されているアクションが表示されます。

プロトコルをフィルタし記録する方法を変更するには、以下のようにします：

1. **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フィルタリング アクションが、リストの右側に表示されます。

2. プロトコル リストの下部の [**許可**] および [**ブロック**] ボタンを使用して、選択されているプロトコルに適用されるアクションを変更します。

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

   一部のアプリケーションは、TCP ベースのメッセージと UDP ベースのメッセージの両方を使用します。アプリケーションの最初のネットワーク要求が TCP で行われ、その後のデータが UDP を使用して送信される場合、Websense ソフトウェアは最初の TCP 要求をブロックし、したがってその後の UDP トラフィックもブロックします。

   UDP 要求は、許可された場合でもブロックされたものとして記録される場合があります。

   選択されているプロトコル グループの他のプロトコルに同じアクションを適用するには、[**グループに適用**] をクリックします。

3. 選択されているプロトコルの使用状況に関するデータをアラートやレポートに使用可能にしたい場合は、[**プロトコル データをログに記録**] チェックボックスをオンにします。
4. このプロトコルの使用に対して帯域幅の制限を課すには、[**Bandwidth Optimizer でブロック**] をクリックし、続いて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、194 ページ を参照してください。
5. フィルタの編集が完了したら、[**OK**] をクリックして変更をキャッシュし、[フィルタ] ページに戻ります。[**すべて保存**] 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にするには、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適用します（インターネット フィルタリング ポリシー、73 ページを参照）。

ご注意：
特定の時刻にプロトコル フィルタの実行を開始するポリシーを作成することができます。フィルタが有効になる前にプロトコル セッションを開始したユーザは、フィルタがブロックしても、そのセッションが続いている間は、そのプロトコルへのアクセスを継続することができます。ユーザがいったんセッションを終了すると、そのプロトコルへの追加の要求はブロックされます。

Websense 定義のカテゴリ フィルタおよびプロトコル フィルタ

Websense ソフトウェアには、複数のサンプル カテゴリ フィルタおよびプロトコル フィルタが含まれています。これらのフィルタをそのまま使用することも、必要に応じて変更することもできます。事前定義されたフィルタが不要の場合は、それらの多くを削除することもできます。

事前定義されたカテゴリ フィルタには、以下のようなものがあります:

- 基本
- 基本セキュリティ
- すべてブロック
- デフォルト
- モニタのみ
- すべて許可

「すべてブロック」および「すべて許可」カテゴリ フィルタは、[フィルタ] ページのリストには示されませんが、ポリシーに追加できます。これらのフィルタは、フィルタリングにおいて特別な役割を果たしますが、削除または編集することはできません。インターネット要求をフィルタする際には、Websense ソフトウェアは、まず「すべてブロック」または「すべて許可」フィルタが適用されるかどうかをチェックしてから、追加のフィルタリングのチェックを行います(サイトのフィルタリング、81 ページを参照)。

事前定義されたプロトコル フィルタには、以下のようなものがあります:

- 基本セキュリティ
- デフォルト
- モニタのみ
- すべて許可

「すべて許可」プロトコル フィルタは、カテゴリ フィルタの場合と同じように、[フィルタ] ページのリストには示されず、編集または削除することはできません。また、フィルタリングにおいては優先的に実行されます。

「デフォルト」カテゴリ フィルタおよびプロトコル フィルタは、編集はできますが、削除することはできません。アップグレード環境においては、「デフォルト」ポリシーにすき間が存在する場合は、「デフォルト」フィルタを使用してポリシーが適用されない要求をフィルタします。

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

新しいカテゴリ フィルタまたはプロトコル フィルタを作成する際には、[フィルタ] ページで既存のフィルタを コピーするか、[フィルタの追加] ページで既存のフィルタをモデルとして選択するか、またはフィルタ **テンプレート**を使用することから始めることができます。

Websense ソフトウェアには、5 つのカテゴリ フィルタ テンプレートが含まれています:

- 「**モニタのみ**」および「**すべて許可**」は、すべてのカテゴリを許可します。
- 「**すべてブロック**」は、すべてのカテゴリをブロックします。
- 「**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、その他は許可します。
- 「**デフォルト**」は、「ブロック」、「許可」、「継続」、および「割り当て時間」アクションをカテゴリに適用します。
- 「**基本セキュリティ**」は、セキュリティ リスク クラスのデフォルト カテゴリのみをブロックします（リスク クラス、40 ページを参照）。

Websense ソフトウェアには、3 つのプロトコル フィルタ テンプレートが含まれています：

- 「**モニタのみ**」および「**すべて許可**」は、すべてのプロトコルを許可します。
- 「**基本セキュリティ**」は、P2P ファイル共有およびプロキシ回避プロトコル、ならびにインスタントメッセージングファイルの添付（このオプションに加入している場合）および悪質なトラフィック（Websense Web Security）をブロックします。
- 「**デフォルト**」は、インスタント メッセージ / チャット プロトコル、ならびに P2P ファイル共有、プロキシ回避、インスタントメッセージング ファイルの添付（このオプションに加入している場合）および悪質なトラフィック（Websense Web Security）をブロックします。

ほとんどの Websense 定義カテゴリ フィルタおよびプロトコル フィルタは変更または削除できますが、テンプレートは編集または削除することはできません。同様に、必要に応じてカスタム フィルタはいくらでも作成できますが、新しいテンプレートを作成することはできません。

テンプレートを編集することはできないので、テンプレートは、Websense 定義フィルタが適用する元のフィルタリング アクションを参照するために常に利用可能な手段と言えます。たとえば、「通常」カテゴリ フィルタおよびプロトコル フィルタ テンプレートは、最初の「デフォルト」カテゴリ フィルタおよびプロトコル フィルタと同じアクションを適用しています。つまり、テンプレートのデフォルト設定を使用するフィルタを作成することにより、最初の Websense filtering 構成をいつでも復元することができます。

テンプレートを使用して新しいフィルタを作成する方法については、カテゴリ フィルタの作成、48 ページまたはプロトコル フィルタの作成、51 ページを参照してください。

Websense フィルタリング設定の構成

関連トピック：

- カテゴリおよびプロトコルのフィルタリング、36 ページ
- クライアント、59 ページ
- ブロック ページ、85 ページ
- フィルタリング アクション、43 ページ
- パスワード アクセス、45 ページ
- フィルタリング順序、80 ページ
- Bandwidth Optimizer による帯域幅の管理、194 ページ
- キーワードに基づくフィルタリング、182 ページ

[設定] > **[フィルタリング]** ページを使用して、種々のフィルタリング機能の基本設定を設定します。

[Bandwidth Optimizer] の下に、使用可能な帯域幅に基づいてインターネット使用をフィルタするのに必要な情報を入力します。帯域幅に基づいたフィルタリングの詳細については、Bandwidth Optimizer による帯域幅の管理、194 ページを参照してください。

1. **インターネット接続速度**を指定するには、次のいずれかを行います：
   - 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 kb/秒単位でネットワーク速度を入力する。
2. **[ネットワークのデフォルト帯域幅]** フィールドを使用して、ネットワーク帯域幅フィルタリングが有効になっている場合に使用するデフォルトのしきい値（総ネットワーク トラフィックに対するパーセンテージ）を入力します。
3. **[プロトコル別のデフォルト帯域幅]** フィールドを使用して、プロトコル帯域幅フィルタリングが有効になっている場合に使用するデフォルトのしきい値を入力します。

[一般的なフィルタリング] セクションを使用して、複数のグループ ポリシーが適用される場合にユーザをフィルタする方法を決定し、キーワード検索オプションを指定し、パスワード アクセス、継続、割り当て時間セッション動作について設定します。

1. 複数のグループ ポリシーが適用される場合にユーザをフィルタする方法を決定するには、**[最も厳しいグループ ポリシーを使用する]** をオンまたはオフにします（フィルタリング順序、80 ページを参照）。

- このオプションを選択すると、最も厳しいフィルタリング設定を適用するポリシーが適用されます。言い換えると、該当する 1 つのグループ ポリシーがあるカテゴリへのアクセスをブロックし、別のグループ ポリシーが許可する場合は、そのカテゴリーのサイトへのユーザ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は、最も許容的な設定が使用されます。

2. 以下の**キーワード検索オプション**のいずれかを選択します（キーワードに基づくフィルタリング、182 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、Websense ソフトウェアは、『?』の前のキーワードは検索しません。
URL のみ	URL にキーワードがある場合、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、Websense ソフトウェアは『?』までのキーワードを検索します。
URL および CGI	アドレスにキーワードがある場合、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、Websense ソフトウェアは『?』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	警告とともに使用します。**[キーワード ブロックの無効化]** は、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 ブロックをオフにします。

3. **[「パスワード アクセス」オプションのタイムアウト]** フィールドに、「パスワード アクセス」を選択した後にユーザがすべてのカテゴリのサイトにアクセスできる最大時間を秒単位で入力します（最大 3600、デフォルトは 60）（パスワード アクセス、45 ページを参照）。
4. **[継続のタイムアウト]** フィールドに、[継続] をクリックしたユーザが確認アクションが管理するカテゴリのサイトにアクセスできる最大時間を秒単位で入力します（最大 3600、デフォルトは 60）（フィルタリング アクション、43 ページを参照）。
5. **[「割り当て時間の使用」セッションの長さ]** フィールドに、ユーザが割り当て時間制限カテゴリのサイトを閲覧できる時間（最大 60 分、デフォルトは 10 分）を入力します（割り当て時間を使用したインターネット アクセスの制限、44 ページを参照）。

   セッションは、ユーザが [割り当て時間の使用] をクリックしたとき開始されます。
6. すべてのユーザに対する **[デフォルトの割り当て時間（日別）]**（最大240分、デフォルトは 60 分）を入力します。

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

[「割り当て時間の使用」セッションの長さ] および [デフォルトの割り当て時間 (日別)] を変更すると、[**デフォルトの割り当てセッション数 (日別)**] が計算され、表示されます。

[**ブロック メッセージ**] セクションを使用して、ブラウザ ベースのブロック メッセージの上部フレームのために作成した代替 HTML ブロック ページへの URL またはパスを入力します (代替ブロック メッセージの作成、92 ページを参照)。

- 種々のプロトコル用に、すなわち **FTP**、**HTTP** (**HTTPS** を含む)、および **Gopher** 用に、別個のページを使用できます。
- これらのフィールドを空白のままにしておくと、ソフトウェアが用意したデフォルトのブロック メッセージ、またはこのメッセージのカスタマイズされたバージョンが使用されます (ブロック メッセージのカスタマイズ、88 ページを参照)。

[**検索フィルタリング**] の下で [**検索フィルタリングを有効にする**] を有効にすると、Websense ソフトウェアは特定の検索エンジンに組み込まれている設定をアクティブにし、ブロックされたサイトに関連付けられたサムネール画像やその他の明示的コンテンツが検索結果に表示されなくなります (検索フィルタリング、46 ページを参照)。

この機能をサポートしている検索エンジンが、このセクションの下部に表示されています。

フィルタリングの構成を終了したら、[OK] をクリックして変更をキャッシュします。[**すべて保存**] をクリックするまで、変更は適用されません。

3 クライアント

Websense Manager で**クライアント**として追加することにより、Websense ソフトウェアが特定のユーザ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 アドレスによって定義される、ネットワークの個々のコンピュータ。
- **ネットワーク**：IP アドレスの範囲として集合的に定義される、コンピュータのグループ。
- **ユーザ**：ユーザ、グループ、またはサポートされているディレクトリ サービスのドメイン アカウント。

最初は、Websense ソフトウェアは**デフォルト** ポリシー（デフォルト ポリシー、74 ページを参照）を使用して、すべてのクライアントを同じようにフィルタします。Websense Manager の［クライアント］ページにクライアントを追加すると、そのクライアントに特定のフィルタリング ポリシーを割り当てることができます。

複数のポリシーを適用できる場合、たとえば、1 つのポリシーがユーザに大して割り当てられ、別のポリシーがコンピュータに対して割り当てられている場合には、Websense ソフトウェアはどのポリシーを実行するかを以下のようにして決定します：

1. 要求を行った**ユーザ**に割り当てられているポリシーを適用します。そのポリシーが、要求の時点にスケジュールされたフィルタを持っていない場合は、次に適用可能なポリシーを使用します。
2. 特定のユーザに対するポリシーが存在しない場合、またはポリシーが要求の時点でアクティブなフィルタを持っていない場合には、要求がそこから行われた（第 1 に）**コンピュータ**または（第 2 に）**ネットワーク**に割り当てられたポリシーを探します。
3. 特定のコンピュータまたはネットワークに対するポリシーが存在しない場合、またはポリシーが要求の時点でアクティブなフィルタを持っていない場合には、ユーザが所属する**グループ**に割り当てられたポリシーを探します。ユーザが複数のグループに所属している場合は、Websense ソフトウェアは該当するすべてのグループを検討します（フィルタリング順序、80 ページを参照）。
4. グループ ポリシーが存在しない場合は、ユーザの**ドメイン**に割り当てられたポリシーを探します（OU）。

5. 該当するポリシーが見つからない場合、またはポリシーが要求の時点でカテゴリ フィルタを実行していない場合には、クライアントが割り当てられているロールの**デフォルト** ポリシーを実行します。

Websense ソフトウェアがフィルタリング ポリシーをクライアントに適用する方法の詳細は、サイトのフィルタリング、81 ページを参照してください。

クライアントに関する作業

関連トピック：

- クライアント、59 ページ
- コンピュータおよびネットワークに関する作業、61 ページ
- ユーザおよびグループに関する作業、62 ページ
- クライアントの追加、69 ページ
- クライアント設定の変更、70 ページ

[ポリシーの管理] > [クライアント] ページを使用して、既存のクライアントに関する情報を表示し、クライアントを追加、編集、または削除し、あるいはクライアントを指定済み管理ロールに移動します。

指定済み管理者は、[クライアント] ページでクライアントを自分の処理対象クライアント リストに追加し、表示されるようにしなければなりません。その手順は、クライアントの追加、69 ページ を参照してください。

クライアントは、以下の 3 つのグループに分けることができます：

- **ディレクトリ**には、ユーザ、グループ、およびディレクトリ サービスのドメインが含まれます（ユーザおよびグループに関する作業、62 ページを参照）。
- **ネットワーク** は、単一のポリシーが管理することができるフィルタされるネットワーク内の IP アドレスの範囲です（コンピュータおよびネットワークに関する作業、61 ページを参照）。
- **コンピュータ**は、IP アドレスによって識別される、フィルタされるネットワーク内の個々のコンピュータです（コンピュータおよびネットワークに関する作業、61 ページを参照）。

クライアント タイプのそばのプラス記号 (+) をクリックすると、選択されたタイプの既存のクライアントのリストが表示されます。各クライアント リストには、以下が含まれます：

- クライアント名、IP アドレスまたは IP アドレス範囲。
- 現在このクライアントに割り当てられている**ポリシー**。別のポリシーが割り当てられるまでは、**デフォルト** ポリシーが使用されます（インターネット フィルタリング ポリシー、73 ページを参照）。

- ブロックされたサイトを閲覧するために、クライアントが**「パスワード アクセス」**オプションを使用できるかどうか（パスワード アクセス、45 ページを参照）。
- クライアントにカスタム量の**割り当て時間**が割り当てられているかどうか（割り当て時間を使用したインターネット アクセスの制限、44 ページを参照）。

特定のクライアントを見つけるには、ツリーの該当するノードをブラウズします。

クライアント ポリシー、パスワード アクセス、割り当て時間、および認証設定を編集するには、リストの 1 つまたは複数のクライアントを選択し、**[編集]** をクリックします。詳細は、クライアント設定の変更、70 ページ を参照してください。

クライアントを追加するには、または、[クライアント] ページに現在は表示されていない処理対象クライアントにポリシーを適用するには、**[追加]** をクリックします。詳細は、クライアントの追加、69 ページを参照してください。

指定済み管理ロールを作成すれば（指定済み管理、239 ページを参照）、優先管理者は自分のクライアントを他のロールに移動させることができます。まず、クライアント エントリのそばのチェックボックスをオンにし、続いて **[ロールに移動]** をクリックします。クライアントを指定済み管理ロールに移動すると、そのクライアントに適用されていたポリシーとフィルタが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、71 ページを参照してください。

Websense ソフトウェアが 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すると、ページの上部のツールバーに **[カスタム LDAP グループの管理]** ボタンが表示されます。このボタンをクリックして、LDAP 属性に基づいたグループを追加または編集します（カスタム LDAP グループに関する作業、67 ページを参照）。

Websense Manager からクライアントを削除するには、クライアントを選択し、**[削除]** をクリックします。

コンピュータおよびネットワークに関する作業

関連トピック：

- クライアントに関する作業、60 ページ
- ユーザおよびグループに関する作業、62 ページ
- クライアントの追加、69 ページ
- クライアントへのポリシーの割り当て、80 ページ

Websense Manager では、**コンピュータ**とは、フィルタされるコンピュータに関連付けられた IP アドレス（たとえば、10.201.3.1）です。**ネットワーク**とは、

フィルタされるコンピュータのグループに関連付けられた IP アドレスの範囲（たとえば、10.201.3.2 – 10.201.3.44）です。

ユーザ、グループ、またはドメイン クライアントの場合と同じように、コンピュータおよびネットワーク クライアントに対してポリシーを割り当てることができます。

- たとえば、ユーザがログオンすることを必要としない、またはユーザがゲスト アカウントでログオンできる**コンピュータ**にポリシーを割り当てます。
- **ネットワーク**にポリシーを割り当て、一度に複数のコンピュータに同じフィルタリング ポリシーを適用します。

コンピュータまたはネットワークにポリシーが割り当てられると、そのポリシーは、ログオン ユーザに対するポリシーを割り当て**ない限り**、フィルタされるコンピュータに誰がログオンしているかに関係なく実行されます。このコンピュータ ポリシーまたはネットワーク ポリシーは、ユーザに対して適用される**グループ** ポリシーよりも優先されます。

ユーザおよびグループに関する作業

関連トピック：

- クライアントに関する作業、60 ページ
- ディレクトリ サービス、63 ページ
- カスタム LDAP グループに関する作業、67 ページ
- コンピュータおよびネットワークに関する作業、61 ページ
- クライアントの追加、69 ページ
- クライアントへのポリシーの割り当て、80 ページ

ネットワーク内の個々のユーザおよびグループにポリシーを適用するために、Websense ソフトウェアがディレクトリ 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、グループ、ドメイン、および組織単位）情報を取得するように構成します。

Websense ソフトウェアは、Windows NT Directory / Active Directory（混在モード）と通信することができ、また Lightweight Directory Access Protocol (LDAP) によってアクセスされる Windows Active Directory、Novell eDirectory、および Sun Java System Directory と通信することができます。

ご注意：
LDAP ベースのディレクトリ サービスを使用する場合は、重複するユーザ名はサポートされません。複数のドメインで同じユーザ名が存在しない必要があります。

また、Windows Active Directory または Sun Java System Directory を使用する場合は、空白のパスワードを持つユーザ名はサポートされません。すべてのユーザにパスワードが割り当てられていることが必要です。

Websense User Service が、フィルタリング ポリシーを適用する際に使用するディレクトリ サービスからの情報を Policy Server および Filtering Service に伝達します。

Websense, Inc. は、User Service を Windows コンピュータ上にインストールすることを推奨します（ただし、Linux コンピュータ上にインストールすることもできます）。一般的には、これは Policy Server がインストールされているコンピュータです。

Websense ソフトウェアがディレクトリ サービスと通信するように構成する方法については、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

ディレクトリ サービスは、ネットワークのユーザおよびリソースに関する情報を格納するツールです。Websense Manager でユーザ クライアント（ユーザ、グループ、ドメイン、または組織単位）を追加する前に、Websense ソフトウェアがディレクトリ サービスから情報を取得するように設定しなければなりません。

[設定] > [ディレクトリ サービス] ページを使用して、ネットワークで使用するディレクトリ サービスを特定します。Policy Server ごとに 1 つのタイプのディレクトリ サービスだけを設定することができます。

まず、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。どれを選択したかによって、ページに表示される設定がきまります。

設定手順については、以下の該当する項を参照してください：

- Windows NT Directory / Active Directory（混在モード）、63 ページ
- Windows Active Directory（ネイティブ モード）、64 ページ
- Novell eDirectory および Sun Java System Directory、65 ページ

Windows NT Directory / Active Directory（混在モード）

使用するディレクトリ サービスが Windows NT Directory または Active Directory の混在モードである場合は、それ以上の設定は必要ありません。

まれな環境において、別のディレクトリを使用しようとする場合、この項の追加情報が必要になる場合があります。それは、以下の場合にのみ発生します：

- 透過的識別のために DC Agentを使用していて（DC Agent、216 ページを参照）、しかも、
- User Service が Linux コンピュータ上で実行されている場合です。

使用している構成がこれに該当する場合は、Windows NT Directory / Active Directory（混在モード）の下にリストされている管理者資格情報を提供する必要があります。使用しているインストレーションがこの構成でない場合は、管理者資格情報フィールドは無効になっています。

Windows Active Directory（ネイティブ モード）

Windows Active Directory は、1 つまたは複数のグローバル カタログにユーザ情報を格納します。このグローバル カタログにより、個人およびアプリケーションは Active Directory ドメインの中でオブジェクト（ユーザ、グループ、など）を見つけることが可能になります。

Websense ソフトウェアがネイティブ モードの Active Directory と通信するには、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しなければなりません。

1. グローバル カタログ サーバー リストのそばの **[追加]** をクリックします。[グローバル カタログ サーバーの追加] ページが表示されます。
2. **[サーバーの IP または名前]** フィールドを使用して、グローバル カタログ サーバーを指定します：
   - フェイルオーバーのために複数のグローバル カタログ サーバーが構成されている場合には、DNS ドメイン名を入力します。
   - グローバル カタログ サーバーのフェイルオーバーが構成されていない場合は、追加するサーバーの IP アドレスまたはホスト名（ネットワーク内のネーム レゾルーションができない場合）を入力します。
3. Websense ソフトウェアがグローバル カタログと通信するのに使用する **[ポート]** 番号を入力します（デフォルトでは **3268**）。
4. オプションで、Websense ソフトウェアがユーザ情報の検索に使用する **[ルート コンテクスト]** を入力します。値を指定する場合、それは使用しているドメインの中で有効なコンテクストでなければなりません。
   - 通信ポート 3268 または 3269 を指定した場合は、ルート コンテクストを指定する必要はありません。
   - 指定したポートが 389 または 636 の場合は、ルート コンテクストを指定しなければなりません。

- ［ルート コンテクスト］フィールドを空白のままにしておくと、Websense ソフトウェアはディレクトリ サービスの最上位レベルで検索を開始します。

  ご注意：
  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。Websense ソフトウェアが 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. Websense ソフトウェアがディレクトリ サービスからユーザ名およびパス情報を取得するために使用する管理者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 サービスの照会および読み取りを行うことができなければなりませんが、ディレクトリ サービスに対して変更を行うことができる必要はなく、ドメイン管理者である必要はありません。

   ［コンポーネント別の識別名］または **［完全識別名］**を選択して、アカウント情報を入力する方法を指定します。

   - ［コンポーネント別の識別名］を選択した場合は、管理者アカウントの **［表示名］**、アカウントの **［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。管理ユーザ名の共通名 (cn) 形式 を使用します。ユーザ ID (uid) 形式は使用しません。

     ご注意：
     ［アカウントフォルダ］フィールドでは、組織単位 (ou) タグ (たとえば、ou= 財務) を使用する値はサポートされません。管理アカウント名に ou タグが含まれる場合、管理アカウントの完全識別名を入力しなければなりません。

   - ［完全識別名］を選択した場合は、**[ユーザ識別名]** フィールドに単一文字列による識別名を入力し (たとえば、cn=Admin, cn=Users, ou=InfoSystems, dc=company, dc=net)、続いてそのアカウントの **［パスワード］**を入力します。

6. **[OK]** をクリックします。
7. 各グローバル カタログ サーバーについて、上記のプロセスを繰り返します。
8. **［詳細ディレクトリ設定］**をクリックし、続いて「詳細ディレクトリ設定、66 ページ」の手順を行います。

Novell eDirectory および Sun Java System Directory

ディレクトリ サービスから情報を取得するために、Websense ソフトウェアは管理権限を持つユーザ 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. **[サーバーIP]** フィールドに、ディレクトリ サーバー コンピュータの IP アドレスを入力します。

2. Websense ソフトウェアがディレクトリと通信するのに使用する [**ポート**] 番号を入力します。デフォルト値は 389 です。
3. 使用するディレクトリが読み取り専用アクセスのための管理者権限を要求する場合は、[**管理者識別名**] と [**パスワード**] を入力します。
4. オプションで、Websense ソフトウェアがユーザ情報の検索に使用する [**ルート コンテクスト**] を入力します。たとえば、o=domain.com と 入力します。

   コンテクストを狭めることは、ユーザ情報の検索の速度と効率を高めるのに役立ちます。

   > **ご注意：**
   > 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。Websense ソフトウェアが 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. [**詳細ディレクトリ設定**] をクリックし、続いて「詳細ディレクトリ設定、66 ページ」の手順を行います。

詳細ディレクトリ設定

関連トピック：

- Windows Active Directory（ネイティブ モード）、64 ページ
- Novell eDirectory および Sun Java System Directory、65 ページ

これらの設定は、以下の定義に使用できます：

- Websense ソフトウェアがユーザ、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。
- Websense ソフトウェアがディレクトリ サービスと通信するのに暗号化された接続を使用するかどうか。
- Websense ソフトウェアがどのキャラクタ セットを使用して LDAP 情報をエンコードするか。

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、[**カスタム フィルタを使用する**] をオンにします。[フィルタ] フィールドに、デフォルト フィルタ文字列が表示されます。
2. 既存のフィルタ 文字列を編集し、使用するディレクトリの特定のオブジェクト クラス タイプに置き換えます。たとえば、ディレクトリがオブジェクト クラス タイプとして **ou**（組織単位）ではなく **dept** を使用する場合は、新しい値を [ドメイン検索フィルタ] フィールドに挿入します。

   属性は、ディレクトリ サービスの内容の検索で使用される文字列です。カスタム フィルタは、以下の機能を提供します。

- **ユーザ検索フィルタ**は、User Service がユーザを検索する方法を決定します。
- **グループ検索フィルタ**は、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**は、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 グループ検索フィルタ**は、User Service がユーザをグループに関連付ける方法を決定します。

3. ソフトウェアとディレクトリ サービス間の通信のセキュリティを確保するために、**[SSL を使用する]** をオンにします。
4. Websense ソフトウェアが LDAP 情報のエンコードに使用するキャラクタ セットを決定するために、**[UTF-8]** または **[MBCS]** を選択します。

   MBCS もしくはマルチバイト キャラクタ セットは、中国語、日本語、韓国語などの東アジア言語のエンコードに一般に使用されます。
5. **[OK]** をクリックして、変更をキャッシュします。**[すべて保存]** をクリックするまで、変更は適用されません。

カスタム LDAP グループに関する作業

関連トピック :

- ユーザおよびグループに関する作業、62 ページ
- ディレクトリ サービス、63 ページ
- カスタム LDAP グループの追加または編集、68 ページ

[カスタム LDAP グループの管理] ページを使用して、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カスタム グループを管理します。このオプションは、Websense ソフトウェアが 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されている場合にのみ、使用可能です。

重要

カスタム LDAP グループを Websense Manager に追加すると、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 Server に追加するには、Websense Manager を使用して各 Policy Server にログオンし、情報を入力します。

カスタム LDAP グループを追加し、その後、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すると、既存のグループは無効になります。グループをふたたび追加し、続いてそれぞれをクライアントとして定義しなければなりません。

- グループを追加するには、**[追加]** をクリックします（カスタム LDAP グループの追加または編集、68 ページを参照）。
- リストのエントリを変更するには、グループ名をクリックします（カスタム LDAP グループの追加または編集を参照）。
- エントリを削除するには、まずそのエントリを選択し、続いて **[削除]** をクリックします。

カスタム LDAP グループに対する変更を終了したら、**[OK]** をクリックして変更をキャッシュし、前のページに戻ります。**[すべて保存]** をクリックするまで、変更は適用されません。

カスタム LDAP グループの追加または編集

Websense Manager の **[カスタム LDAP グループの追加]** ページを使用して、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します。**[カスタム LDAP グループの編集]** ページを使用して、既存の定義を変更します。

> **重要**
> カスタム LDAP グループを追加し、その後、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すると、既存のグループは無効になります。グループをふたたび追加し、続いてそれぞれをクライアントとして定義しなければなりません。

1. **[グループ名]** を入力または変更します。その LDAP グループの目的を明確に示すような説明的な名前を使用します。

   グループ名は、大文字と小文字を区別し、一意的な名前でなければなりません。
2. ディレクトリ サービスの中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**」は雇用状態を示すユーザの属性であり、「**parttime**」はユーザがパートタイム従業員であることを示す値です。
3. **[OK]** をクリックすると、[カスタム LDAP グループの管理] ページに戻ります。リストに新しいまたは修正されたエントリが表示されます。
4. 別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。**[すべて保存]** 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

関連トピック：

- クライアントに関する作業、60 ページ
- コンピュータおよびネットワークに関する作業、61 ページ
- ユーザおよびグループに関する作業、62 ページ
- ディレクトリ サービスの検索、70 ページ
- クライアント設定の変更、70 ページ

[ポリシーの管理] > **[クライアント]** > **[クライアントの追加]** ページを使用して、Websense Manager にユーザ、グループ、コンピュータ、およびネットワーク クライアントを追加し、それらにポリシーを割り当てられるようにします。

指定済み管理ロールにログオンした場合は、処理対象クライアント リストに表示されているクライアントのみを追加することができます。処理対象クライアントを [クライアント] ページに追加する過程で、クライアントにポリシーを割り当てなければなりません。

1. 1 つまたは複数のクライアントを識別します。
   - ユーザ、グループ、またはドメイン 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、ディレクトリ サービスのエントリを検索します。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、**[検索]** をクリックしてディレクトリ検索ツールを有効にすることができます（ディレクトリ サービスの検索、70 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**を入力します。2 つのネットワーク定義が重なり合うことはできませんが、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個別に識別される IP アドレスを含むことができます。このような重なり合いが生じた場合は、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優先されます。
2. 矢印ボタン (>) をクリックして、各クライアントを **[選択したクライアント]** リストに追加します。

   [選択したクライアント] 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、続いて **[削除]** をクリックします。
3. **ポリシー**を選択して、[選択したクライアント] リストのすべてのクライアントに割り当てます。
4. 作業が終了したら、**[OK]** をクリックして、変更をキャッシュします。**[すべて保存]** をクリックするまで、変更は適用されません。

クライアントが、**[ポリシーの管理]** > **[クライアント]** ページの該当するリストに追加されます。1 つまたは複数のクライアントに割り当てられたポリ

シーを変更するか、または追加のクライアント設定を構成するには、各クライアント エントリを選択し、[**編集**] をクリックします。詳細は、クライアント設定の変更、70 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

Websense ソフトウェアを 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たら、検索機能を使用してユーザを特定し、Websense Manager でクライアントとして追加することができます。検索機能は、処理対象クライアントや管理者を指定済み管理ロールに追加するためにも使用できます。

ディレクトリ サービスを検索して、ユーザ、グループ、および組織単位情報を取得するには、以下のようにします :

1. [**検索**] をクリックします。
2. ユーザ、グループ、または組織単位の**名前**の全部または一部を入力します。
3. [**タイプ**] リストを使用して、検索したいディレクトリ エントリのタイプ (ユーザ、グループ、OU、または全部) を指定します。

   大きなディレクトリ サービスの場合は、**全部**を選択すると、検索に非常に長い時間がかかる場合があります。
4. [**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。より正確にコンテクストを指定することは、検索の高速化に役立ちます。
5. [**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。
6. 検索結果の中の 1 つまたは複数のエントリを選択し、続いて右向き矢印 (>) をクリックして選択したものをクライアントまたは管理者として追加します。
7. [**新規検索**] をクリックして別の検索基準のセットを入力します。
8. [**参照**] をクリックすると、ディレクトリの参照に戻ります。
9. 変更が終了したら、[OK] をクリックして、変更をキャッシュします。[**すべて保存**] をクリックするまで、変更は適用されません。

クライアント設定の変更

[**ポリシーの管理**] > [**クライアント**] > [**クライアントの編集**] ページを使用して、1 つまたは複数のクライアントのポリシーおよび認証設定を変更します。[編集] 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は、[クライアントの編集] ページで行った構成の変更は、選択したクライアントのすべてに適用されます。

1. 選択したクライアントに適用する**ポリシー**を選択します。別のポリシーを割り当てるまでは、デフォルト ポリシーがクライアントを管理します。

2. パスワードを入力することによってWebsenseブロック ページを無効化できるようにするには、[パスワード アクセス] の下の [**オン**] をクリックし、続いてパスワードを入力し、確認します。

   クライアントのパスワード アクセス権限を削除するには、[**オフ**] をクリックします。

3. 選択したクライアントに**割り当て時間**のカスタマイズされた量を割り当てるには、[**カスタム**] をクリックし、割り当てる割り当て時間の分数を入力します。

   デフォルトの割り 当て時間設定に戻すには、[**デフォルト**] をクリックします。

4. 変更をキャッシュし、[クライアント] のページに戻るためには、[OK] をクリックします。[**すべて保存**] 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設定が、クライアント リストの一部として [**ポリシーの管理**] > [**クライアント**] ページに表示されます。

クライアントをロールに移動

優先管理者は、[**クライアントをロールに移動**] ページを使用して、1 つまたは複数のクライアントを指定済み管理ロールに移動することができます。クライアントを移動したら、そのクライアントはターゲット ロールの [クライアント] ページの処理対象クライアント リストに表示されます。

- 優先管理者ロールのクライアントに適用されるポリシーおよびそれが実施するフィルタは、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、自分の処理対象クライアントに適用されるポリシーを変更することができます。
- フィルタ ロックの制限は、優先管理者が管理するクライアントには影響を与えませんが、指定済み管理ロールの処理対象クライアントには影響を与えます。
- グループ、ドメイン、または組織単位が処理対象クライアントとしてロールに付加されると、そのロールの指定済み管理者は、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)が処理対象クライアントとしてロールに付加されると、そのロールの指定済み管理者は、そのネットワーク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することはできません。

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、以下のようにします :

1. [**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。
2. [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よって、選択したクライアントが移動したことが示されます。移動プロセスには、多少の時間がかかる場合があります。

3. [**すべて保存**] 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、Websense Manager をログアウトし、ログオンしなおさなければなりません。

4 インターネット フィルタリング ポリシー

関連トピック：

- インターネット使用のフィルタ、35 ページ
- クライアント、59 ページ
- デフォルト ポリシー、74 ページ
- ポリシーに関する作業、75 ページ
- フィルタリング順序、80 ページ

ポリシーが、ユーザのインターネット アクセスを管理します。ポリシーは、以下によって構成されます：

- カテゴリ フィルタ。ウェブ サイト カテゴリに対してアクション（許可、ブロック）を適用するために使用されます（カテゴリおよびプロトコルのフィルタリング、36 ページを参照）。
- 制限つきアクセス フィルタ。Web サイトの限定リストのみにアクセスを許可するために使用されます（ユーザのアクセスを指定したサイトのリストに制限、170 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されます（カテゴリおよびプロトコルのフィルタリング、36 ページを参照）。
- いつ各カテゴリ フィルタまたは制限つきアクセス フィルタ、およびプロトコル フィルタを実行するかを決定するスケジュール。

新しい Websense ソフトウェア 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：

- **デフォルト** ポリシーは、他のポリシーによって管理され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。Websense ソフトウェアは、サブスクリプション キーが入力されるとただちに、このポリシーの実施を開始します（デフォルト ポリシー、74 ページを参照）。
- **制限なし**ポリシーは、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、デフォルトでいずれかのクライアントに適用されることはありません。
- **例 – 標準ユーザ**は、ポリシーが複数のカテゴリ フィルタおよびプロトコル フィルタを適用し種々の時間に種々の度合いのフィルタリング制限を

提供する方法を示したものです。このポリシーは、ポリシーを編集しクライアントに適用するプロセスを示した『新しいユーザのクイック スタート チュートリアル』で使用されます。

これらのポリシーを現状のままで使用することも、組織に適合するようにそれらを編集することも、新しいポリシーを作成することも自由です。

デフォルト ポリシー

関連トピック：

- インターネット フィルタリング ポリシー、73 ページ
- ポリシーに関する作業、75 ページ
- フィルタリング順序、80 ページ

Websense ソフトウェアをインストールし、サブスクリプション キーを入力するとただちに、**デフォルト** ポリシーがインターネット使用のモニタリングを開始します。最初は、デフォルト ポリシーはすべての要求を許可します。

ご注意：
以前の Websense ソフトウェア バージョンからアップグレードした場合は、既存のポリシー設定が保存されます。アップグレード後に、ポリシーを見直し、それらが依然として適切であることを確認してください。

独自のフィルタリング ポリシーを作成し、適用したとき、デフォルト ポリシーは引き続きセーフティーネットの役割を果たし、他のポリシーによって管理されないクライアントに対してインターネット アクセスのフィルタリングを行います。

新しいインストレーションにおいては、デフォルト ポリシーは、1 日 24 時間、週 7 日間のインターネット フィルタリングを適用する必要があります（カテゴリ フィルタまたは制限つきアクセス フィルタの組合せの実行、該当する場合はプロトコル フィルタの実行）。

重要
Websense ソフトウェアの初期のバージョンからのアップグレードでは、デフォルト ポリシーが全時間範囲をカバーしない場合があります。デフォルト ポリシーを変更する必要はありません。ただし、将来編集を行った場合、Websense ソフトウェアは、全時間範囲がカバーされるまで、変更の保存を許可しません。

デフォルト ポリシーを必要に応じて編集し、組織の必要に適合させてください。デフォルト ポリシーを削除することはできません。

ポリシーに関する作業

関連トピック：

- インターネット フィルタリング ポリシー、73 ページ
- ポリシーの作成
- ポリシーの編集
- インターネット使用のフィルタ
- フィルタリング ポリシーの調整

[ポリシーの管理] > **[ポリシー]** ページを使用して、既存のポリシー情報を検討します。また、このページは、ポリシーの追加、編集、および削除、指定済み管理ロールへのポリシーのコピー（優先管理者のみ）、ならびにポリシー構成に関する詳細情報の印刷のための、出発点の役割も果たします。

[ポリシー] ページには、既存のポリシーのリストが含まれています。このリストには、各ポリシーの名前と説明、ならびにそのポリシーが割り当てられているユーザ、ネットワーク、およびコンピュータ クライアントの数が表示されます。

- ポリシーを追加するには、**[追加]** をクリックします。詳細については、ポリシーの作成、76 ページを参照してください。
- ポリシーを編集するには、リストのポリシー名をクリックします。詳細については、ポリシーの編集、77 ページを参照してください。
- ポリシーによってフィルタされる対象のクライアントを表示するには、ユーザ、ネットワーク、またはコンピュータ欄の数字をクリックします。ポップアップ ダイアログボックスにクライアント情報が表示されます。

すべてのポリシーとその構成要素（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、正規表現を含む）のリストを出力するには、**[ポリシーをファイルに出力]** をクリックします。この機能は、Microsoft Excel 形式でポリシー情報の詳細なスプレッドシートを作成します。この目的は、人事担当者、管理職、およびフィルタリング ポリシー情報を検討する監督権限を持つその他の人々のために便利な方法を提供することです。

指定済み管理ロールを作成した場合（指定済み管理、239 ページを参照）、優先管理者は自分が作成したポリシーを、指定済み管理者が使用するために他のロールにコピーすることができます。ポリシーによって実施されるフィルタもコピーされます。

ご注意：
指定済み管理者はフィルタ ロックで管理されるので、フィルタ ロックを実施する「すべて許可」フィルタおよびポリシーはロールにコピーすることはできません。

ポリシーを別のロールにコピーするには、まずポリシー名のそばのチェックボックスをオンにし、[**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、175 ページ を参照してください。

ポリシーの作成

関連トピック:

- インターネット フィルタリング ポリシー、73 ページ
- ポリシーに関する作業、75 ページ
- ポリシーの編集、77 ページ
- フィルタに関する作業、47 ページ
- ユーザのアクセスを指定したサイトのリストに制限、170 ページ

[**ポリシーの管理**] > [**ポリシー**] > [**ポリシーの追加**] ページを使用して、新しいカスタム ポリシーを作成します。

1. 一意的な**ポリシー名**を入力します。ポリシー名は長さが 1 ～ 50 字で、以下の文字を含めることはできません。:

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

   ポリシー名には、スペース、ダッシュ、およびアポストロフは含めることができます。
2. ポリシーの**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、明確で詳細であることが望ましいです。

   ポリシー名に適用される文字に関する制限が説明にも適用されますが、2 つの例外があります。すなわち、ピリオド (.) とコンマ (,) は含めることができます。
3. 新しいポリシーのベースとして、既存のポリシーを使用するには、[**既存のポリシーを基にする**] チェックボックスをオンにし、ドロップダウンリストからポリシーを選択します。

   空のポリシーから始めるには、このチェックボックスをオフにしておきます。
4. 変更をキャッシュし、[ポリシーを編集] のページに戻るには、[OK] をクリックします。

   [ポリシーを編集] ページを使用して、新しいポリシーの定義を終了します。ポリシーの編集、77 ページを参照してください。

ポリシーの編集

関連トピック：
- インターネット フィルタリング ポリシー、73 ページ
- ポリシーに関する作業、75 ページ
- ポリシーの作成、76 ページ
- フィルタに関する作業、47 ページ
- ユーザのアクセスを指定したサイトのリストに制限、170 ページ

[ポリシーの管理] > **[ポリシー]** > **[ポリシーを編集]** ページを使用して、既存のポリシーを変更し、または新しいポリシーの定義を仕上げます。

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：

- **[名前の変更]** をクリックして、ポリシー名を変更します。
- **[説明]** フィールドに入力して、フィルタの説明を変更します。

ポリシーの説明の下の [**クライアント**] フィールドに、このポリシーが現在フィルタしている各タイプのクライアント（ユーザ、コンピュータ、およびネットワーク）の数がリストされます。このポリシーが管理しているクライアントを表示するには、該当するクライアント タイプに対応するリンクをクリックします。

このポリシーに追加のクライアントを割り当てるには、ページの上部のツールバーの中の **[クライアントに適用]** をクリックし、続いて「クライアントへのポリシーの割り当て、80 ページ」の手順を行います。

[ポリシーの定義] エリアを使用して、このポリシーを種々の時間にどのフィルタに適用するかを定義します。：

1. スケジュールに時間帯を追加するには、**[追加]** をクリックします。
2. [スケジュール] テーブルの **[開始]** および **[終了]** 欄を使用して、この時間帯がカバーする時間を定義します。

   深夜をまたぐ時間（たとえば、PM5:00 ～ AM8:00）のフィルタリングを定義するには、2 つの時間帯をスケジュールに追加し、1 つは開始時刻から深夜までの時間をカバーし、もう 1 つは深夜から終了時刻までの時間をカバーするようにします。

   Websense ソフトウェアに含まれている「**例 – 標準ユーザ**」ポリシーに、深夜をまたぐフィルタリング時間の定義方法が示されています。
3. **[曜日]** 欄を使用して、この時間帯にどの曜日を含めるかを定義します。リストから曜日を選択するには、欄の右端の下向き矢印をクリックします。曜日の選択が終わったら、上向き矢印をクリックします。
4. **[カテゴリ / 制限付きアクセス フィルタ]** 欄を使用して、この時間帯に実行するフィルタを選択します。

このポリシーで実施する新しいフィルタを追加するには、[**カテゴリ フィルタの作成**] または [**制限付きアクセス フィルタの作成**] を選択します。詳細は、カテゴリ フィルタの作成、48 ページまたは制限付きアクセス フィルタの作成、172 ページを参照してください。

5. [**プロトコル フィルタ**] 欄を使用して、この時間帯に実施するプロトコル フィルタを選択します。

   このポリシーで実行する新しいフィルタを追加するには、[**プロトコル フィルタの作成**] を選択します。その手順は、プロトコル フィルタの作成、51 ページ を参照してください。

6. スケジュールに追加の時間帯を追加するには、ステップ 1 ～ 5 を繰り返します。

スケジュールの中の時間帯を選択すると、[ポリシーを編集] ページの下部にこの時間帯に実行されるフィルタが示されます。各フィルタ リストには、以下が含まれます :

- フィルタ タイプ (カテゴリ フィルタ、制限付きアクセス 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 (カテゴリもしくはプロトコルおよび適用されるアクション、または許可されるサイトのリスト)
- 選択したフィルタを実施するポリシーの数
- 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すると、変更はそのフィルタを実施するすべてのポリシーに影響を与えます。複数のポリシーで実施されるフィルタを編集する前に、[**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、影響を受けるポリシーを正確に調べてください。

フィルタ リストの下部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:

フィルタ タイプ	ボタン
カテゴリ フィルタ	• **[許可]**、**[ブロック]**、**[確認]**、または **[割り当て時間]** ボタンを使用して、選択したカテゴリに適用するアクションを変更します(フィルタリング アクション、43 ページを参照)。 • 親カテゴリとすべてのそのサブカテゴリに適用されるアクションを変更するには、まず、親カテゴリに適用されるアクションを変更し、続いて **[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、または帯域幅に基づいたブロックを有効にするには、**[詳細]** をクリックします。
制限付きアクセス フィルタ	• **[サイトの追加]** および **[式の追加]** ボタンをクリックして、許可された URL、IP アドレス、または正規表現をフィルタに追加します(ユーザのアクセスを指定したサイトのリストに制限、170 ページを参照)。 • フィルタからサイトを削除するには、URL、IP アドレス、または式のそばのチェックボックスをオンにし、続いて **[削除]** をクリックします。
プロトコル フィルタ	• **[許可]** または **[ブロック]** ボタンを使用して、選択したプロトコルに適用されるアクションを変更します(フィルタリング アクション、43 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されるアクションを変更するには、グループのいずれかのプロトコルに適用されるアクションを変更し、**[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か、または帯域幅に基づいたブロックを有効にするには、**[詳細]** をクリックします。

ポリシーの編集を終了したら、[OK] をクリックして変更をキャッシュします。**[すべて保存]** をクリックするまで、変更は適用されません。

クライアントへのポリシーの割り当て

関連トピック：

- インターネット フィルタリング ポリシー、73 ページ
- ポリシーの作成、76 ページ
- ポリシーの編集、77 ページ
- クライアント、59 ページ
- クライアントの追加、69 ページ

[ポリシー] > [ポリシーを編集] > [クライアントにポリシーを適用] ページを使用して、選択したポリシーをクライアントに割り当てます。

クライアント リストに、すべての使用可能なユーザ、コンピュータ、およびネットワーク クライアント、ならびに各クライアントに現在割り当てられているポリシーが表示されます。

選択したポリシーがフィルタする各クライアントのそばのチェックボックスをオンにし、続いて **[OK]** をクリックすると、[ポリシーを編集] ページに戻ります。変更をキャッシュするために、再度 **[OK]** をクリックします。

[すべて保存] をクリックして、Websense ソフトウェアが新しいポリシーを使用して選択したクライアントからの要求のフィルタを開始することを促します。

フィルタリング順序

Websense ソフトウェアは、特定の順序で適用される複数のフィルタを使用して、要求されたインターネット データを許可するか、ブロックするか、または制限するかを決定します。

Websense ソフトウェアは、受け取った各要求に対して、以下を行います：

1. サブスクリプションが現在有効で、加入クライアント数を超過していないことを確認し、サブスクリプションが遵守されていることを確認します。
2. 以下の順序で検索して、適用するポリシーを決定します：
   a. **ユーザ**に割り当てられているポリシー。
   b. 使用されているコンピュータの **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。
   c. ユーザが所属する**グループ**に割り当てられているポリシー。
   d. ユーザの**ドメイン**に割り当てられているポリシー。
   e. **デフォルト** ポリシー。

   見つかった最初の該当するポリシーが使用されます。
3. ポリシーの制限にしたがって要求をフィルタします。

場合によっては、ユーザが複数のグループまたはドメインに所属しており、ユーザ ポリシー、コンピュータ ポリシー、ネットワーク ポリシーがどれも適用されない場合があります。このような場合には、Websense ソフトウェアは各ユーザ グループに割り当てられている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持っている場合は、Websense ソフトウェアはそのポリシーに従って要求をフィルタします。
- グループの 1 つが異なるポリシーを持っている場合には、Websense ソフトウェアは、**[設定]** > **[フィルタリング]** ページの **[より厳密な制限でブロックをする]** の設定にしたがって要求をフィルタします。

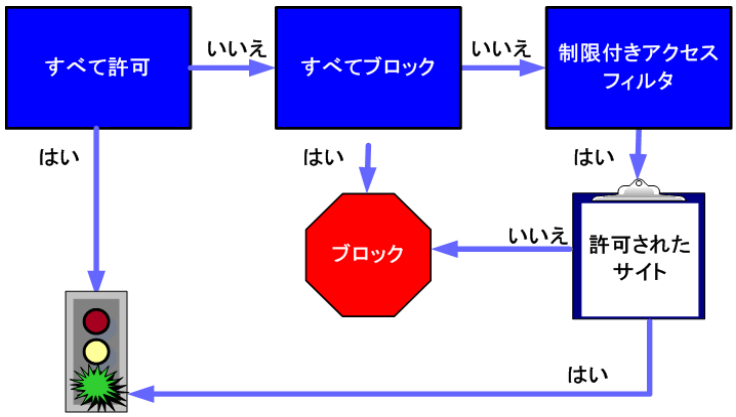
  [より厳密な制限でブロックをする] がオンになっていて、該当するポリシーのいずれかが要求されているカテゴリに対するアクセスをブロックする場合は、Websense ソフトウェアはサイトをブロックします。

  このオプションがオフになっていて、該当するポリシーのいずれかが要求されているカテゴリに対するアクセスを許可する場合は、Websense ソフトウェアはサイトを許可します。

該当するポリシーが制限付きアクセス フィルタを実施する場合は、**[より厳密な制限でブロックする]** オプションは期待とは異なる効果になる場合があります。制限付きアクセス フィルタとフィルタリングの優先順位、170 ページを参照してください。

サイトのフィルタリング

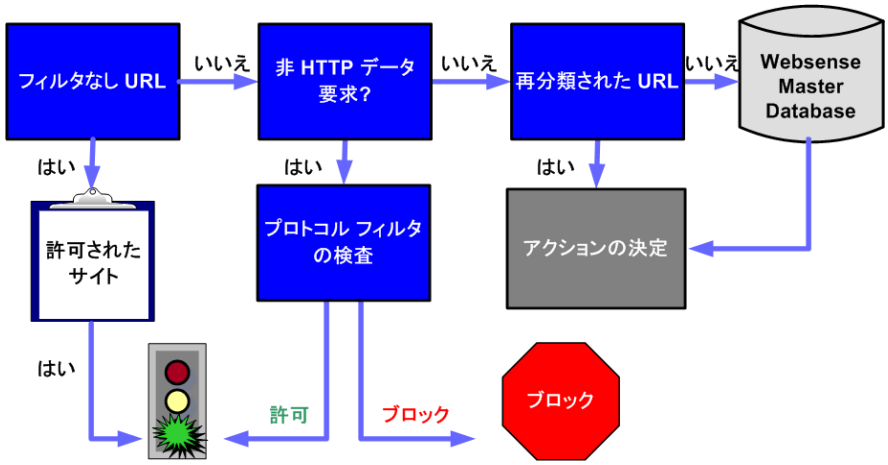
Websense ソフトウェアは、ポリシーの制限を以下のように評価して、要求されたサイトを許可するか、ブロックするかを決定します。



1. 現在の曜日および時間にどの**カテゴリ フィルタ**または**制限付きアクセス フィルタ**をポリシーが実施するかを決定します。
   - アクティブなカテゴリ フィルタが **[すべて許可]** である場合は、サイトを許可します。
   - アクティブなカテゴリ フィルタが **[すべてブロック]** である場合は、サイトをブロックします。

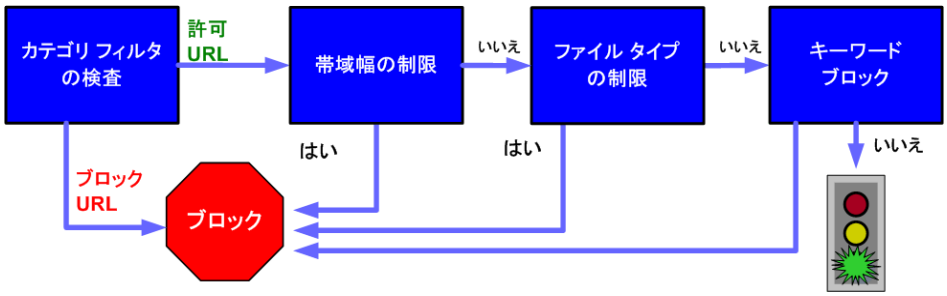
- フィルタが [**制限付きアクセス フィルタ**] である場合は、フィルタに URL または IP アドレスが含まれているかどうかをチェックします。含まれている場合は、サイトを許可します。含まれていない場合は、サイトをブロックします。
- 他のカテゴリ フィルタが適用される場合は、ステップ 2 に進みます。

> **ご注意：**
> Websense ソフトウェアは、インターネット検索エンジンのキャッシュからアクセスされる URL を、他の URL と同じようにフィルタします。このように格納されている URL は、URL カテゴリについてアクティブなポリシーに従ってフィルタされます。キャッシュされた URL のログ記録は、検索エンジン パラメータを含む完全なキャッシュされた URL を示します。



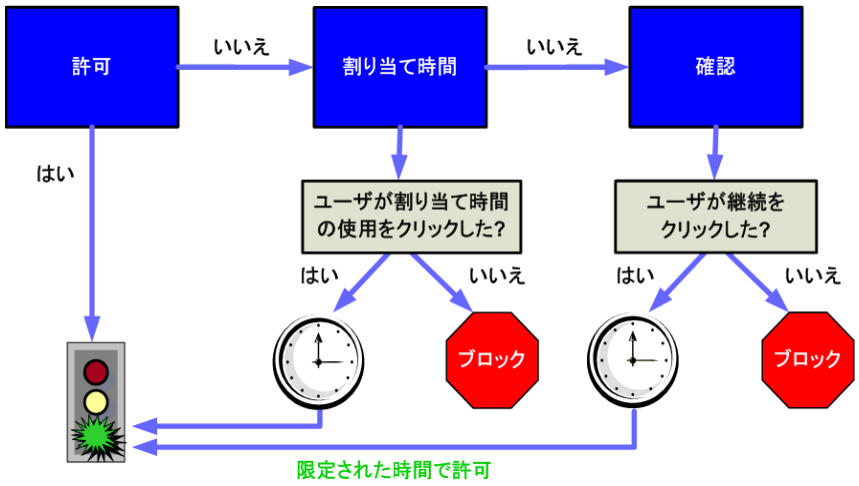
2. サイトと**フィルタなし URL** リストのエントリとの一致を調べます。
   - その URL がリストに存在する場合は、サイトを許可します。
   - その URL がリストに存在しない場合は、ステップ 3 に進みます。
3. アクティブな**プロトコル フィルタ**をチェックし、その要求に非 HTTP プロトコルが関連しているかどうかを判定します。
   - 関連している場合は、プロトコル フィルタ設定を送信されるデータに適用します。
   - 関連していない場合は、ステップ 4 に進みます。
4. サイトと**再分類された URL** リストのエントリとの一致を調べます。
   - 一致する場合は、サイトに対応するカテゴリを識別し、ステップ 6 に進みます。
   - 一致しない場合は、ステップ 5 に進みます。
5. サイトと**マスタ データベース**のエントリとの一致を調べます。
   - その URL がマスタ データベースに存在する場合は、サイトに対応するカテゴリを識別し、ステップ 6 に進みます。

- 一致しない場合は、そのサイトをその他 / 未分類として分類し、ステップ 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アクションを識別します。
   - アクションが**ブロック**である場合は、サイトをブロックします。
   - 他のアクションが適用されている場合は、ステップ 7 に進みます。
7. アクティブなカテゴリ フィルタの **Bandwidth Optimizer** 設定をチェックします (Bandwidth Optimizer による帯域幅の管理、194 ページを参照)。
   - 現在の帯域幅使用率が設定されている限界を超えている場合は、サイトをブロックします。
   - 現在の帯域幅使用率が指定された限界を超えていない場合、または帯域幅に基づいたアクションが適用されていない場合は、ステップ 8 に進みます。
8. アクティブなカテゴリ フィルタに適用される [**ファイル タイプ**] 制限をチェックします (ファイル タイプに基づくトラフィックの管理、196 ページを参照)。
   - サイトが、ブロック対象となる拡張子のファイルを含んでいる場合は、それらのファイルへのアクセスはブロックされます。サイト自体がブロック対象となるファイル タイプで構成されている場合は、サイトへのアクセスはブロックされます。
   - サイトが、ブロック対象となる拡張子のファイルを含んでいない場合は、ステップ 9 に進みます。
9. キーワード ブロックが有効になっている場合は、URL および CGI パスにブロックされる**キーワード**がないかチェックします (キーワードに基づくフィルタリング、182 ページを参照)。
   - ブロックされるキーワードが見つかった場合は、サイトをブロックします。

- ブロックされるキーワードが見つからなかった場合は、ステップ 10 に進みます。



10. カテゴリに適用されるアクションに従って、サイトを取り扱います。
    - **許可**: サイトを許可します。
    - **割り当て時間によって制限**: 割り当て時間を使用してサイトを閲覧するか、または前のページに戻るかを選択するオプション付きのブロック メッセージを表示します。
    - **確認**: 仕事上の目的でサイトを閲覧するのかどうかを確認するオプション付きのブロック メッセージを表示します。

Websense ソフトウェアは、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、処理を進めます。その時点で、Websense ソフトウェアはそれ以上のフィルタリングは行いません。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、Websense ソフトウェアは、カテゴリ レベルでサイトをブロックし、キーワード フィルタのチェックは行いません。したがって、Log Server は、(キーワードのためではなく) ブロックされるカテゴリのために要求がブロックされた、と記録します。

ご注意:
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係なく、インターネット サイトにアクセスできます。

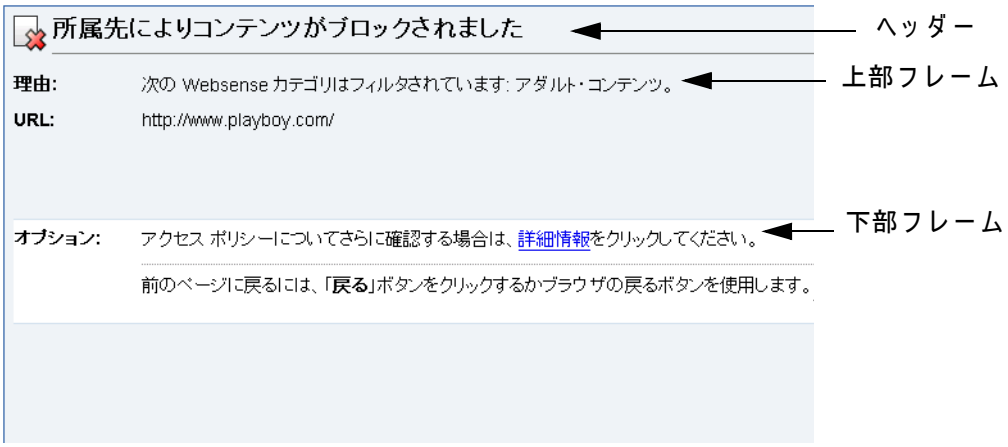
5 ブロック ページ

関連トピック：

- プロトコル ブロック メッセージ、86 ページ
- ブロック ページに関する作業、87 ページ
- 代替ブロック メッセージの作成、92 ページ
- 別のコンピュータ上の代替ブロック ページの使用、92 ページ

Websense ソフトウェアは Web サイトをブロックするとき、クライアントのブラウザにブロック ページを表示します。サイトがセキュリティ リスク クラス（リスク クラス、40 ページを参照）のカテゴリに属しているためにブロックされた場合には、ブロック ページの特別バージョンが表示されます。

デフォルトでは、ブロック ページは 3 つのメイン セクションで構成されています。



- **ヘッダー**では、サイトがブロックされたことが説明されます。
- **上部フレーム**には、要求された URL と、URL がブロックされた理由を示すメッセージが含まれます。
- **下部フレーム**には、前にページに戻るオプションや、[継続] ボタンもしくは [割り当て時間] ボタンをクリックしてサイトを閲覧するオプションのような、ユーザが使用可能なオプションが提示されます。

ブロック ページは、HTML ファイルで構成されます。デフォルトのブロック ページ ファイルが、Websense ソフトウェアに含まれています。これらのデフォルト ファイルを使用することも、独自のカスタム バージョンを作成することもできます。

- 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 ページに関する作業、87 ページを参照）。
- リモート Webサーバーに収容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、Websense ソフトウェアを構成します（別のコンピュータ上の代替ブロック ページの使用、92 ページを参照）。

プロトコル ブロック メッセージ

関連トピック：

- ブロック ページに関する作業、87 ページ
- 代替ブロック メッセージの作成、92 ページ
- 別のコンピュータ上の代替ブロック ページの使用、92 ページ

ユーザまたはアプリケーションがブロックされる非 HTTP プロトコルを要求すると、Websense ソフトウェアは一般にプロトコル ブロック メッセージを表示します。

ただし、ユーザがブラウザの中からブロックされる FTP、HTTPS、または Gopher サイトを要求し、要求がプロキシに受け渡される場合は、HTML ベースのブロック ページがブラウザに表示されます。

アプリケーションがブロックされるプロトコルを要求すると、実行できないことを示すエラー メッセージをユーザがアプリケーションから受け取る場合があります。アプリケーション エラー メッセージは、Websense ソフトウェアが生成したものではありません。

Windows コンピュータ上でプロトコル ブロック メッセージを表示するには、一定のシステム構成が必要な場合があります：

- Windows NT、XP、または 200x を実行しているクライアント コンピュータ上でプロトコル ブロック メッセージを表示するには、Windows Messenger サービスが有効になっていなければなりません。このサービスは、デフォルトでは有効になっていません。Windows サービス ダイアログボックスを使用して、使用しているコンピュータでこのサービスが実行されているかどうか、調べることができます（Windows のサービス ダイアログボックス、401 ページを参照）。
- Windows 98 コンピュータ上でプロトコル ブロック メッセージを表示するには、Windows ディレクトリにある **winpopup.exe** を起動しなければなりません。コマンド プロンプトからこのアプリケーションを実行するか、

このアプリケーションを [スタートアップ] フォルダにコピーして自動的に起動するように設定して下さい。

プロトコル ブロック メッセージは、Linux コンピュータ上では表示されません。HTML ブロック ページは、オペレーティングシステムに関係なく表示されます。

プロトコル フィルタリングが有効になっている場合、プロトコル ブロック メッセージがクライアント コンピュータ上に表示されるように設定されているかどうかに関係なく、Websense ソフトウェアはプロトコル要求をフィルタします。

ブロック ページに関する作業

関連トピック :

- プロトコル ブロック メッセージ、86 ページ
- ブロック メッセージのカスタマイズ、88 ページ
- 代替ブロック メッセージの作成、92 ページ
- 別のコンピュータ上の代替ブロック ページの使用、92 ページ

Websense ブロック ページの作成に使用するファイルは、**Websense¥BlockPages¥en¥Default** ディレクトリに格納されています :

- **master.html** は、ブロック ページの情報フレームを構築し、ボタン フレームに該当するオプションを表示するために以下のファイルのいずれかを使用します。

ファイル名	内容
blockFrame.html	ブロックされるカテゴリのサイトのためのテキストとボタン ([戻る] オプション)
continueFrame.html	**確認**アクションが適用されるカテゴリのサイトのためのテキストとボタン
quotaFrame.html	**割り当て時間**アクションが適用されるカテゴリのサイトのためのテキストとボタン
moreInfo.html	ユーザがブロック ページの **[詳細情報]** リンクをクリックすると表示されるページのコンテンツ

- **block.html** には、ブロック メッセージの上部フレームのテキストが含まれています。これは、アクセスが制限されることを説明し、要求されたサイトのリストを示し、サイトが制限される理由を記述するものです。

ブロック メッセージのカスタマイズ

関連トピック：

- メッセージ フレームのサイズの変更、89 ページ
- ブロック ページに表示されるロゴの変更、89 ページ
- ブロック ページ コンテンツ変数の使用、90 ページ
- デフォルト ブロック ページに戻す、91 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、このコピーを使用してユーザが受け取るブロック ページの上部フレームをカスタマイズすることができます。

- 組織のインターネット使用ポリシーに関する情報を追加します。
- 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。

1. Websense ブロック ページ ディレクトリに移動します：

   ```
   <installation path>\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：

   ```
   <installation path>\BlockPages\en\Custom
   ```

   ご注意：
   BlockPages¥en¥Default ディレクトリの元のブロック メッセージ ファイルを変更**しないでください**。それらを **BlockPages¥en¥Custom** ディレクトリにコピーし、コピーを変更してください。

3. メモ帳や Vi などの、テキストエディタでファイルを開きます。

   警告
   ブロック メッセージ ファイルの編集には、プレーン テキストエディタを使用してください。一部の HTML エディタは、HTML コードを変更し、それによってファイルがこわれ、ブロック メッセージ表示問題を引き起こす可能性があります。

4. テキストを編集します。ファイルには、変更の仕方を案内するコメントが含まれています。

   トークン（「$*」と「*$」で囲まれた部分）や HTML コードの構造を変更**しないでください**。これによって、Websense ソフトウェアがブロック メッセージの中に特定情報を表示することが可能になります。

5. ファイルを保存します。

6. Filtering Service を再起動します (詳細については、Websense サービスの停止と起動、288 ページを参照)。

メッセージ フレームのサイズの変更

ブロック メッセージに表示したい情報によっては、ブロック メッセージのデフォルトの幅や上部フレームの高さが適切でない場合があります。**master.html** ファイルのこれらのサイズ パラメータを変更するには、以下を行います :

1. **master.html** を、**Websense¥BlockPages¥en¥Default** ディレクトリから **Websense¥BlockPages¥en¥Custom** ディレクトリにコピーします。
2. メモ帳や vi のような (HTML エディタではない) テキストエディタで、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、以下の行を編集します :

   ```
   <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. 追加情報を表示するためにメッセージの上部フレームをスクロールさせるには、以下の行を編集します。

   ```
   <iframe src="$*WS_BLOCKMESSAGE_PAGE*$*WS_SESSIONID*$" ...
   scrolling="no" style="width:100%; height: 6em;">
   ```

   scrolling パラメータの値を **auto** に変更して、メッセージ テキストがフレームの高さを超過する場合にスクロールバーを表示します。

   また、**height** パラメータの値を変更して、フレーム高さを変更することができます。
5. ファイルを保存して閉じます。
6. Filtering Service を再起動して変更を実行します (Websense サービスの停止と起動、288 ページを参照)。

ブロック ページに表示されるロゴの変更

master.html ファイルには、ブロック ページに Websense ロゴを表示するために使用される HTML コードも含まれています。代わりに組織のロゴを表示するには、以下を行います :

1. それらがすでにコピーされていない場合、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** ディレクトリにコピーします。
2. 組織のロゴを含んでいる画像ファイルを同じ場所にコピーします。
3. メモ帳や vi のような (HTML エディタではない) テキストエディタで **master.html** を開き、以下の行を編集して Websense ロゴを組織のロゴに置き換えます。:

   ```
   <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画像ファイルの名前に置き換えます。
- **title** パラメータの値を、組織の名前を反映するように変更します。

4. ファイルを保存して閉じます。
5. Filtering Service を再起動して変更を適用します（Websense サービスの停止と起動、288 ページを参照）。

ブロック ページ コンテンツ変数の使用

コンテンツ変数は、HTML ブロック ページに表示される情報を制御します。デフォルトのブロック メッセージ コードには、以下の変数が含まれています。

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（ドメイン名を除く）
WS_USERDOMAIN	現在のユーザのドメイン名
WS_IPADDR	要求元コンピュータの IP アドレス
WS_WORKSTATION	ブロックされたコンピュータの名前（名前がない場合は IP アドレスが表示されます）

変数を使用するには、該当する HTML タグの「$*」と「*$」の間に変数名を挿入します：

```
<p id="UserName">$*WS_USERNAME*$</p>
```

この場合、WS_USERNAME が変数です。

ブロック メッセージ コードには、以下のような追加の変数が含まれています。これらの変数の中には、独自のカスタム ブロック メッセージの構築に役立つものがあるでしょう。ただし、Websense 定義ブロック メッセージ ファイルの中にこれらの変数を見つけた場合、これらを変更**しないでください**。Filtering Service がブロックされた要求を処理する際にこれらの変数を使用するので、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 を表示します。
WS_BLOCKREASON	サイトがブロックされた理由（すなわち、どのフィルタリング アクションが適用されたか）を表示します。
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デフォルト カテゴリに属しているかどうかを示します。TRUE（属している）の場合、セキュリティ ブロック ページが表示されます。

変数名	目的
WS_PWOVERRIDECGIDATA	ブロック ページ HTML コードの入力フィールドに、[**パスワード アクセス**] ボタンの使用に関する情報を取り込みます。
WS_QUOTA_CGIDATA	ブロック ページ HTML コードの入力フィールドに、[**割り当て時間の使用**] ボタンの使用に関する情報を取り込みます。
WS_PASSWORDOVERRID_BEGIN, WS_PASSWORDOVERRID_END	パスワード アクセス機能の有効化に関係します。
WS_MOREINFO	要求されたサイトがブロックされた理由に関する詳細情報を（[**詳細情報**] リンクがクリックされた後に）表示します。
WS_POLICYINFO	要求元のクライアントを管理するポリシーを示します。
WS_MOREINFOCGIDATA	[**詳細情報**] リンクの使用について、Filtering Service にデータを送信します。
WS_QUOTATIME	要求元クライアントに残されている割り当て時間の量を表示します。
WS_QUOTAINTERVALTIME	要求元クライアントに対して構成されている割り当て時間セッションの長さを表示します。
WS_QUOTABUTTONSTATE	特定の要求について [**割り当て時間の使用**] ボタンを有効にするかどうかを指示します。
WS_SESSIONID	要求に関連する内部識別子の役割を果たします。
WS_TOPFRAMESIZE	カスタム ブロック サーバーが設定されている場合、カスタム ブロック サーバーが送信するブロック ページの上部のサイズ（パーセンテージ）を指示します。
WS_BLOCKMESSAGE_PAGE	ブロック ページの上部フレームに使用されるソースを指示します。
WS_CATEGORY	ブロックされた URL のカテゴリを表示します。
WS_CATEGORYID	要求された URL のカテゴリの一意的な識別子。

デフォルト ブロック ページに戻す

カスタム ブロック メッセージを実施した後にエラーを経験した場合、以下の手順でデフォルト ブロック メッセージを復元できます：

1. **Websense¥BlockPages¥en¥Custom** ディレクトリからすべてのファイルを削除します。デフォルトで、Websense ソフトウェアはデフォルト ディレクトリのファイルを使用するように戻ります。
2. Filtering Service を再起動します（Websense サービスの停止と起動、288 ページを参照）。

代替ブロック メッセージの作成

関連トピック：

- ブロック ページに関する作業、87 ページ
- ブロック メッセージのカスタマイズ、88 ページ

独自の HTML ファイルを作成して、ブロック ページの上部フレームに表示するテキストを提供することができます。既存の HTML ファイルを使用して最初から代替ファイルを作成するか、または **block.html** をコピーしてテンプレートとして使用します。

- HTTP、FTP、および Gopher の 3 つのプロトコルのそれぞれについて、異なるメッセージを作成します。
- それらのファイルを、Websense コンピュータまたは内部 Web サーバーに収容します（別のコンピュータ上の代替ブロック ページの使用、92 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ら、Websense ソフトウェアが新しいメッセージを表示するように構成する必要があります（Websense フィルタリング設定の構成、56 ページを参照）。この過程で、構成可能なプロトコルのそれぞれにどのメッセージを使用するかを指定できます。

別のコンピュータ上の代替ブロック ページの使用

関連トピック：

- ブロック ページに関する作業、87 ページ
- ブロック メッセージのカスタマイズ、88 ページ
- 代替ブロック メッセージの作成、92 ページ

Websense ブロック ページを使用し、上部フレーム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、それらを内部 Web サーバーに収容することができます。

ご注意：
ブロック ページを外部 Web サーバーに格納することが可能です。ただし、そのサーバーがマスタ データベースにリストされているサイトを収容していて、そのサイトがブロックされるカテゴリに属する場合は、ブロック ページ自体がブロックされます。

一部の組織は、Websense サーバー コンピュータのアイデンティティを隠すために、代替リモート ブロック ページを使用しています。

リモート ブロック ページは、どんな HTML ファイルでもかまいません。デフォルト Websense ブロック ページの形式に従う必要はありません。ただし、ブロック ページの作成にこの方法を使用すると、Websense 定義のブロック ページ（デフォルトまたはカスタム）で使用可能な［継続］、［割り当て時間の使用］、および［パスワード アクセス］機能が使用できなくなります。

ファイルをしかるべき場所に置いたら、**eimserver.ini** ファイルを編集して新しいブロック ページを指示するようにします。

1. Websense Filtering Service と Policy Server サービスを、この順序で、停止させます（Websense サービスの停止と起動、288 ページを参照）。
2. Filtering Service コンピュータ上で、Websense **bin** ディレクトリに移動します（デフォルトでは、¥Program Files¥Websense¥bin または /opt/websense/bin）。
3. **eimserver.ini** ファイルのバックアップ コピーを作成し、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]** セクションを見つけます（ファイルの先頭にあります）。
5. 以下の形式で、ホスト名またはブロック ページを収容しているサーバーの IP アドレスを入力します：

   ```
   UserDefinedBlockPage=http://<host name or IP address>
   ```

   URL のプロトコル部分（http://）が必要です。
6. ファイルを保存し、テキスト エディタを閉じます。
7. Websense Policy Server と Filtering Service を、この順序で、再起動します。

サービスが開始されると、ユーザは代替コンピュータに収容されているブロック ページを受け取ります。

6 レポートを使用したフィルタリング ポリシーの評価

関連トピック :

- レポートの概要、96 ページ
- プレゼンテーション レポート、98 ページ
- 調査レポート、118 ページ
- セルフレポートへのアクセス、145 ページ

Websense Manager は、使用しているフィルタリング ポリシーの効果を評価するために、いくつかのレポーティング ツールを提供します (Websense Manager と Websense reporting コンポーネントが Windows サーバ上にインストールされていなければなりません)。

- Websense Manager を開いたとき、最初に [**今日**] ページが表示されます。このページには Websense ソフトウェアの運用ステータスが表示されます (今日 : ヘルス、セキュリティ、および値 (AM 12:00 以降)、20 ページ を参照。)
- [**履歴**] ページは、ログ データベースに保存されている情報の量に応じて、最大 30 日分のフィルタリング アクティビティのグラフを表示します。これらのグラフには今日のアクティビティは含まれません。(履歴 : 最終 30 日、23 ページ を参照。)
- **プレゼンテーション レポート**および**調査レポート**では、レポートの生成、カスタマイズ、スケジュール設定のための多くのオプションを利用できます。詳細は、レポートの概要、96 ページ を参照してください。

組織がすでに Linux サーバ上に Websense Manager をインストールしているか、または Windows 上で実行するプログラムではなく Websense Explorer for Linux Reporting プログラムを選択した場合、Websense Manager にレポート オプションは表示されません。[今日] および [履歴] ページにインターネット フィルタリングのグラフは表示されません。このプログラムをインストールし、レポートを実行する方法については、『Explorer for Linux 管理者用ガイド』を参照してください。

レポートの概要

関連トピック：

- レポートを使用したフィルタリング ポリシーの評価、95 ページ
- プレゼンテーション レポート、98 ページ
- 調査レポート、118 ページ
- セルフレポートへのアクセス、145 ページ

[今日] および [履歴] ページに表示されるグラフのほかに、Websense ソフトウェアはプレゼンテーション レポートと調査レポートの 2 つのレポート オプションを提供します。

ご注意：
指定済み管理を使用する組織では、一部の管理者はすべてのレポート機能にはアクセスできません。指定済み管理、239 ページを参照してください。

プレゼンテーション レポートレポートはレポート定義のリストを提供します。表形式のレポートと、棒グラフと表を組み合わせたレポートがあります。プレゼンテーション レポートを生成するには、以下の手順を実行します。

1. リストからレポートを選択します。
2. **[実行]** をクリックします。
3. 日付範囲を選択します。
4. **[すぐに実行]** をクリックします。

事前定義されたグラフを生成するほかに、それをコピーし、レポートに含めるべきクライアント、カテゴリ、プロトコル、またはアクションを識別するカスタマイズされたレポート フィルタを適用することができます。頻繁に使用するレポート定義に「使用頻度の高いレポート」を表すマークをつけ、見つけやすくします。

任意のプレゼンテーション レポートを、特定の時刻に、または繰り返し実行するようにスケジュール設定できます。詳細については、プレゼンテーション レポート、98 ページを参照してください：

調査レポートによって、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レベルの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、そのデータの異なるビューを表示することができます。

- リスク クラス名をクリックし、次にそのリスク クラスに関係するより詳細なレベルを選択します。たとえば、「法的責任」リスク クラスのユーザ別アクティビティを表示することを選択できます。

- 生成されるグラフでユーザ名をクリックして、そのユーザに関する詳細を表示します。
- [**インターネット使用状況**] リストから異なるオプションを選択して、ようやく棒グラフを切り替えます。
- 2 つのレベルの情報を同時に表示するには、棒グラフの上のフィールドに入力します。たとえば、上位 10 件のカテゴリの上位 5 人のユーザのアクティビティを表示する場合は、カテゴリの要約グラフから、**[10](ユーザ)** を選択し、次に **[5]** を選択します。
- 棒または番号をクリックして、その項目 (リスク クラス、カテゴリ、ユーザなど) の詳細レポートを開きます。
- [**使用頻度の高いレポート**] をクリックして、特によく使用するレポート フォーマットを将来の使用のために保存したり、前に保存した使用頻度の高いレポートを生成します。

可能性は無限です。インターネット使用状況データを表示する多くの方法の詳細については、調査レポート、118 ページを参照してください。

インターネット ブラウズ時間について

関連トピック :

- データベース ジョブ、324 ページ
- インターネット ブラウズ時間の設定、330 ページ

インターネット ブラウズ時間 (IBT)、つまり個人が Web サイトのアクセスで消費した時間の量をもとに、プレゼンテーション レポートと調査レポートの両方を生成できます。どのソフトウェア プログラムでも、個人が特定のサイトを実際に見ていた時間を正確に知ることはできません。サイトを開き数秒間見てから電話に応対し、その後で他のサイトを要求する場合があります。各サイトを数分をかけて熟読してから次のサイトへ進む場合もあります。

Websense ソフトウェアのログ データベース ジョブでは、いくつかの設定可能な値を基にした公式を使ってインターネット ブラウズ時間 (IBT) を計算します。このジョブは 1 日 1 回実行されますから、ブラウズ時間情報と実際のログ データには時間差が生じることがあります。

ブラウズ時間の計算では、インターネット セッションはユーザがブラウザを開いた時点で開始します。このセッションは、ユーザが少なくとも 3 分ごとに別の Web サイトを要求している間は継続します (このデフォルトの読み込み時間しきい値は設定可能です)。

このインターネット セッションは、ユーザが別のサイトを要求する前に 3 分を経過したとき終了します。Websense ソフトウェアは最初の要求から、最後の要求の 3 分後までの時間を計算します。

3 分以上を経過した後でユーザが別の要求を行ったとき、新しいセッションが開始します。一般的にはユーザのブラウズ時間は 1 日のうちの複数のセッションから成ります。

インターネット ブラウズ時間ジョブおよび関連する設定のオプションの詳細についてはデータベース ジョブ、324 ページおよびインターネット ブラウズ時間の設定、330 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

関連トピック：

- プレゼンテーション レポートのコピー、101 ページ
- 使用頻度の高いレポートの使用、109 ページ
- プレゼンテーション レポートの作成、109 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、111 ページ
- スケジュールされたジョブのリストの表示、115 ページ

[レポート] > [プレゼンテーション レポート] ページには事前定義されているグラフや表形式のレポートのリストが表示されます。これらのレポートはそれぞれ、ログ データベースからの特定の情報を示します（ログ データベースの説明、323 ページを参照）。このレポート カタログからレポートを選択すると、レポートの簡単な説明が表示されます。

事前定義されたレポートをコピーし、レポートに含めるクライアント、カテゴリ、プロトコル、およびアクションを指定するレポート フィルタをカスタマイズすることができます。頻繁に使用するレポートは、すばやく 見つけられるように、「 使用頻度の高いレポート」を表すマークを付けることができます。

レポートをすぐに実行するか、または後で、もしくは定期的に実行するためにスケジュール設定します。出力フォーマットを選択し、スケジュール設定されたレポートを選択した受信者のグループに配布します。

レポートを [プレゼンテーション レポート] ページで直接に、HTML フォーマットで生成した場合は、別のページに移動したときにそのレポートは保存されません。レポートを PDF または XLS フォーマットで生成し、すぐに表示した場合、レポートを表示したプログラム（Adobe Reader または Microsoft Excel）を閉じるときにレポートは保存されません。

代わりに、PDF または XLS ファイルを表示する前にファイルを保存することを選択するか、レポートを表示するプログラムの [保存] オプションを使用することができます。この場合、ディスク スペースの問題が起こらないように、定期的にレポート ファイルを削除または移動してください。

スケジュール設定されたレポートは、次のディレクトリに自動的に保存されます。

```
<install_path>\ReportingOutput
```

デフォルト設定では、<install_path> は C:¥Program Files¥Websense です。

スケジュール設定されたプレゼンテーション レポートが実行されたとき、レポート ファイルは **presentationreport_0** という名前の電子メール添付ファイル

として受信者に送信されます。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。添付ファイルの名前は ReportingOutput ディレクトリに保存されているファイルの名前と一致しません。このディレクトリで特定のレポートを検索するには、スケジュール設定されたジョブが実行された日付で作成されているファイルを検索します。

レポートは 15 日後に、自動的に ReportingOutput ディレクトリから削除されます。レポートを長期間保存したい場合、それをバックアップ ルーチンに含めるか、またはレポートをスケジュール設定して電子メールで送信されたファイルを、保存期間が長い場所に保存します。

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。Websense Manager をインストールしているコンピュータに十分なディスクスペースがあることを確認してください。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。

Websense ソフトウェアは、PDF (Adobe Reader)、XLS (Microsoft Excel)、または HTML のいずれかの、ユーザが指定するフォーマットでレポートを生成できます。HTML フォーマットを選択した場合、レポートは Websense Manager コンテンツペインに表示されます。そのレポートを印刷したり、ファイルに保存することはできません。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。

PDF または XLS フォーマットを選択した場合、レポート ファイルをディスクに保存するか、または別のウィンドウに表示することを選択できます。

重要

プレゼンテーション レポートを PDF フォーマットで表示するには、Websense Manager 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。

プレゼンテーション レポートを XLS フォーマットで表示するには、Websense Manager をアクセスしているコンピュータに Excel 2003 以上がインストールされていなければなりません。

[プレゼンテーション レポート] ページでレポート カタログを参照して、関心があるレポートを選択します。次に、このページのコントロールを使用し

てレポートを実行し、コピーを作成し、このコピーのレポート フィルタ等をカスタマイズできます。

ボタン	アクション
使用頻度の高いレポートのみを表示	このオプションを選択すると、レポート カタログは「使用頻度の高いレポート」というマークが付いているレポートだけを表示します。 レポートの完全なリストを表示するには、このオプションをオフにします。
レポート フィルタの編集	このオプションは、事前定義されているレポートが選択されている時にだけ利用でき、レポートに含めるカテゴリ、プロトコル、ユーザ、アクションを選択できます。プレゼンテーション レポートのコピー、101 ページを参照してください。
コピー	選択したレポートのコピーにマークを付け、それをカスタム レポートとしてレポート カタログに追加します。プレゼンテーション レポートのコピー、101 ページを参照してください。 カスタム レポートを選択し、次に、**[レポート フィルタの編集]** をクリックすることによって特定のパラメータを設定します。
使用頻度の高いレポート	選択したレポートに「使用頻度の高いレポート」のマークを付けるか、または「使用頻度の高いレポート」のマークを除去します。使用頻度の高いレポートの使用、109 ページを参照してください。 レポート カタログでは「使用頻度の高いレポート」のマークが付いているレポートのレポート名の横に星印が表示されます。**[使用頻度の高いレポートのみを表示]** チェックボックスを使用して、レポート カタログにどのレポートを表示するかをコントロールします。
削除	レポートから、選択したレポートのコピーを削除します。ソフトウェアにあらかじめインストールされている事前定義レポートは削除できません。 削除されたレポートがスケジュール設定されているジョブの中に含まれている場合、そのレポートはそのジョブで引き続き生成されます、
実行	日付範囲と出力フォーマットを設定した後、選択したレポートを生成します。プレゼンテーション レポートの作成、109 ページを参照してください。 カスタム レポート（事前定義されたレポートのコピー）の他の側面を制御する方法については、プレゼンテーション レポートのコピー、101 ページを参照してください。 レポートを、特定の時刻に、または繰り返し実行するようにスケジュール設定するには [スケジューラ] をクリックします。

ページの上部のボタンには、プレゼンテーション レポートのための追加のオプションがあります。

ボタン	アクション
ジョブ キュー	作成されたスケジュール設定されているジョブと各ジョブのステータスを表示します。スケジュールされたジョブのリストの表示、115 ページを参照してください。
スケジューラ	特定の時刻に、またはスケジュールに従って繰り返し実行する 1 つ以上のレポートを含む含むジョブを定義できます。プレゼンテーション レポートのスケジュール設定、111 ページを参照してください。

プレゼンテーション レポートのコピー

関連トピック:

- レポート フィルタの定義、102 ページ
- プレゼンテーション レポート、98 ページ

[プレゼンテーション レポート] ページには当初、ソフトウェアと共にインストールされているすべての事前定義されたレポートを示すレポート カタログが表示されます。これらのレポートのいずれかについて、特定の期間のレポートを生成するには、レポートを選択し、[実行] をクリックします。

また、これらの事前定義されたレポートをテンプレートとしてコピーし、カスタムのレポート フィルタを作成することもできます。コピーからレポートを作成するときに、どのユーザ、カテゴリ、プロトコル、アクションをレポートに含めるか等の要素を制御するために、レポート フィルタを作成します。

レポートをコピーし、レポート フィルタを編集した後、新しいレポートをコピーして、そのコピーを基にした種々のレポートを作成できます。

1. レポート カタログの中の任意のレポートを選択します。
2. **[コピー]** をクリックします。

   レポート カタログにレポート名の複製が表示され、それがコピーであることを示すコードが付加されます。
3. レポート カタログでそのコピーを選択し、次に **[レポート フィルタの編集]** をクリックしてレポートの要素を変更します。レポート フィルタの定義、102 ページを参照してください。

レポート フィルタの定義

関連トピック：

- プレゼンテーション レポートのコピー、101 ページ
- プレゼンテーション レポートの作成、109 ページ

レポート フィルタを使用して、レポートに含める情報を制御できます。たとえば、選択したクライアント、カテゴリ、リスク クラス、プロトコル、または選択したフィルタリング アクション（許可、ブロックなど）のみをレポートに含めることを選択できます。また、レポート フィルタを通じてレポート カタログのエントリに新しい名前と説明を割り当てたり、カスタム ロゴを表示するようにしたり、他の一般的なオプションを設定することもできます。

ご注意：
カスタムロゴを使用するには、レポート フィルタを定義する前に若干の準備が必要です。希望するグラフィックをサポートされているグラフィック形式で作成し、ファイルを適当な場所に置かなければなりません。レポート ロゴのカスタマイズ、107 ページを参照してください。

フィルタで使用できるオプションは、選択したレポートによって異なります。たとえば、「ブロックされたグループの上位 - 要求別」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。

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。事前定義されているレポートのコピーのフィルタを変更することはできます。

1. レポート カタログの中の任意のレポートを選択します。

   [レポート フィルタの編集] ボタンが無効になっている場合は、ステップ 2 に進みます。

   [レポート フィルタの編集] ボタンが有効になっている場合は、ステップ 3 に進みます。

2. **[コピー]** をクリックして、カスタマイズするためのコピーを作成します。

   レポート カタログにレポート名の複製が表示され、それがコピーであることを示すコードが付加されます。

3. **[レポート フィルタの編集]** ボタンをクリックします。

   [レポート フィルタ] 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、適当な項目を選択し、**[次へ]** をクリックして次のタブへ移動します。詳細な手順は、次を参照してください：

   - レポート対象のクライアントの選択、103 ページ
   - レポート対象のカテゴリの選択、104 ページ

- レポート対象のプロトコルの選択、105 ページ
- レポート対象のアクションの選択、105 ページ
- レポートのオプションの設定、106 ページ

4. [**確認**] タブで、レポート フィルタを保存するほかに、レポートをすぐに実行するか、またはスケジュール設定するかを選択します。レポート フィルタ定義の確認、108 ページを参照してください。

レポート対象のクライアントの選択

関連トピック:

- レポート対象のカテゴリの選択、104 ページ
- レポート対象のプロトコルの選択、105 ページ
- レポート対象のアクションの選択、105 ページ
- レポートのオプションの設定、106 ページ
- レポート フィルタ定義の確認、108 ページ

[プレゼンテーション] > [レポート フィルタ] ページの [**クライアント**] タブでは、レポートにどのクライアントを含めるかを制御できます。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、同じレポートで特定のユーザと特定のグループを選択することはできません。

レポート定義で特定のクライアント タイプが指定されている時、そのタイプのクライアント、またはそれよりも大きいグループを表しているクライアントを選択することができます。たとえば、[ブロックされたグループの上位 - 要求別] を基にレポートのフィルタを定義するとき、そのレポートのグループ、ドメインまたは組織単位を選択できますが、個別ユーザ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. [**検索の制限**] リストからの検索結果の最大数を設定します。

   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 つ以上の文字を入力し、次に [**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. 結果リストの 1 つ以上のエントリをハイライトし、右矢印ボタン (>) をクリックしてそれを [**選択済み**] リストへ移動します。
5. 必要に応じてステップ 2-4 を実行し、追加の検索を行い、さらにクライアントを [選択済み] リストに追加します。
6. 選択が終了したら、[**次へ**] をクリックして [カタログ] タブを開きます。レポート対象のカテゴリの選択、104 ページを参照してください。

レポート対象のカテゴリの選択

関連トピック :

- レポート対象のクライアントの選択、103 ページ
- レポート対象のプロトコルの選択、105 ページ
- レポート対象のアクションの選択、105 ページ
- レポートのオプションの設定、106 ページ
- レポート フィルタ定義の確認、108 ページ

[プレゼンテーション レポート] > [レポート フィルタ] ページの [**カテゴリ**] タブで、カテゴリまたはリスク クラスを基に、レポートに含める情報を制御できます。リスク クラス、40 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. 分類として、[**カテゴリ**] または [**リスク クラス**] を選択します。

   親カテゴリを展開して、その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にリストを表示します。

   関連付けられているレポートが特定のリスク クラスのレポートなら、該当するリスク クラスおよびそれに対応するカテゴリだけが選択可能です。

   > **ご注意 :**
   > レポートの中で指定されているリスク クラスのカテゴリのサブセットを選択した場合、その選択を反映するようにレポートのタイトルを変更することを検討してください。

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 [**すべてを選択**] および [**すべてクリア**] ボタンを使用して、必要とされる選択の回数を最小限にします。
3. 右矢印 (>) ボタンをクリックして、選択した項目を [**選択済み**] 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 [選択済み] リストに入れられます。

4. すべての選択が終了したら、**[次へ]** をクリックして [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、105 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

関連トピック :

- レポート対象のクライアントの選択、103 ページ
- レポート対象のカテゴリの選択、104 ページ
- レポート対象のアクションの選択、105 ページ
- レポートのオプションの設定、106 ページ
- レポート フィルタ定義の確認、108 ページ

[プレゼンテーション] > [レポート フィルタ] ページの **[プロトコル]** タブでは、レポートにどのプロトコルを含めるかを制御できます。

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 **[すべてを選択]** および **[すべてクリア]** ボタンを使用して、必要とされる選択の回数を最小限にします。
3. 右矢印 (>) ボタンをクリックして、選択した項目を **[選択済み]** リストに追加します。
4. すべての選択が終了したら、**[次へ]** をクリックして [プロトコル] タブを開きます。レポート対象のアクションの選択、105 ページを参照してください。

レポート対象のアクションの選択

関連トピック :

- レポート対象のクライアントの選択、103 ページ
- レポート対象のカテゴリの選択、104 ページ
- レポート対象のプロトコルの選択、105 ページ
- レポートのオプションの設定、106 ページ
- レポート フィルタ定義の確認、108 ページ

[プレゼンテーション]>[レポート フィルタ]ページの**[アクション]**タブでは、レポートにどのフィルタリング アクションを含めるか(「制限付きアクセス フィルタにより許可」、「割り当て時間によりブロック」など)を制御できます。レポートが特定のタイプのアクション(たとえば「ブロック」)を指定している場合、レポートにはそのタイプのアクションのみを選択できます。

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. アクション 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アクションのチェックボックスをオンにします。

   リストの下の**[すべてを選択]**および**[すべてクリア]**ボタンを使用して、必要とされる選択の回数を最小限にします。
3. 右矢印(>)ボタンをクリックして、選択した項目を**[選択済み]**リストに追加します。
4. すべての選択が終了したら、**[次へ]**をクリックして[プロトコル]タブを開きます。レポートのオプションの設定、106 ページを参照してください。

レポートのオプションの設定

関連トピック:

- レポート ロゴのカスタマイズ、107 ページ
- レポート対象のクライアントの選択、103 ページ
- レポート対象のカテゴリの選択、104 ページ
- レポート対象のプロトコルの選択、105 ページ
- レポート対象のアクションの選択、105 ページ
- レポートのオプションの設定、106 ページ
- レポート フィルタ定義の確認、108 ページ

[プレゼンテーション]>[レポート フィルタ]ページの[**オプション**]タブでは、レポートのいくつかの側面を制御できます。

1. レポート カタログに表示される**レポートのカタログ名**を変更します。名前の最大の長さは 85 文字です。

   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. レポートに表示される**レポート タイトル**を変更します。名前の最大の長さは 85 文字です。
3. レポート カタログに表示される**説明**を変更します。名前の最大の長さは 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、107 ページを参照してください。

5. **[使用頻度の高いレポートとして保存]** チェックボックスにマークを付けて、レポートを使用頻度の高いレポートとしてリストします。

   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。[レポート カタログ] ページで **[使用頻度の高いレポートのみを表示]** を選択して、リストされるレポートの数を減らすことができます。それによってより迅速に特定のレポートにアクセスすることができます。

6. 報告される項目の数を制限するには、**[最初のみを表示]** チェックボックスにマークを付け、1 ～ 20 の範囲の数字を入力します。

   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。たとえば、「上位カテゴリ - アクセス件数別」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終了したら、**[次へ]** をクリックして [確認] タブを開きます。レポート フィルタ定義の確認、108 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

事前定義されたプレゼンテーション レポートは、左上隅に Websense のロゴを表示します。事前定義されたレポートをコピーし、そのレポート フィルタを定義する場合、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 ファイルを次のディレクトリに保存します。

   ```
   <install_path>\Manager\ReportingTemplates\images
   ```

   デフォルト設定では、<install_path> は C:¥Program Files¥Websense です。

このディレクトリ内のすべてのサポートされているイメージ ファイルは、自動的に [レポート フィルタ] ページの [オプション] タブのドロップダウン リストに表示されます。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（レポートのオプションの設定、106 ページ を参照。）

> **ご注意：**
> レポート フィルタの中でアクティブになっているイメージを削除してはいけません。指定されたロゴがない場合、レポートを生成できません。

レポート フィルタ定義の確認

関連トピック：

- レポート対象のクライアントの選択、103 ページ
- レポート対象のカテゴリの選択、104 ページ
- レポート対象のプロトコルの選択、105 ページ
- レポート対象のアクションの選択、105 ページ
- レポートのオプションの設定、106 ページ

[プレゼンテーション] > [レポート フィルタ] ページの **[確認]** タブでは、レポート カタログに表示される名前と説明が表示され、処理方法を選択できます。

1. **名前**と**説明**を確認します。

   変更が必要なとき、**[戻る]** をクリックして [オプション] タブに戻り、そこで変更を行うことができます。（レポートのオプションの設定、106 ページ を参照。）
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、98 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、[レポートの実行] ページを開きます。プレゼンテーション レポートの作成、109 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、[レポートのスケジュール] 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、111 ページを参照してください。

3. **[完了]** をクリックして、ステップ 2 で行った選択を適用します。

使用頻度の高いレポートの使用

関連トピック：

- プレゼンテーション レポート、98 ページ
- プレゼンテーション レポートの作成、109 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、111 ページ

事前定義レポートかカスタム レポートかに関わらず、どのプレゼンテーション レポートにでも「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。このオプションは、頻繁に生成するレポートをレポート カタログの中ですばやく検索できるようにするために使用します。

1. **[プレゼンテーション レポート]** ページで、頻繁に生成するレポート、またはすばやく検索できるようにしたいレポートをハイライトします。
2. **[使用頻度の高いレポート]** 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 カタログの上の **[使用頻度の高いレポートのみを表示]** チェックボックスをオンにすると、リストを「使用頻度の高いレポート」というマークが付いているレポートに制限します。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。

変更が必要になり、使用頻度の高いレポートが頻繁には使用されなくなった場合、「使用頻度の高いレポート」のマークを除去できます。

1. 使用頻度の高いレポートの星印が付いているレポートをハイライトします。
2. **[使用頻度の高いレポート]** をクリックします。

   レポート カタログ内のそのレポート名から星印が削除されます。**[使用頻度の高いレポートのみを表示]** を選択した場合、そのレポートはリストに表示されなくなります。

プレゼンテーション レポートの作成

関連トピック：

- プレゼンテーション レポート、98 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、111 ページ

1 つのレポートを作成するとき、下記の一連のステップを実行する必要があります。

> **ご注意：**
> レポートを PDF フォーマットで表示するには、Websense Manager 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。
>
> レポートを XLS フォーマットで表示するには、Websense Manager 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。
>
> 必要なソフトウェアがインストールされていない場合でも、ファイルを保存することを選択できます。

1 つ以上のレポートを実行するジョブを作成し、プレゼンテーション レポート スケジュール設定機能を使ってそれを 1 回または繰り返し実行するには、以下の手順を実行します。プレゼンテーション レポートのスケジュール設定、111 ページを参照してください。

1. **[プレゼンテーション レポート]** ページで、[レポート カタログ] ツリー内のレポートをハイライトし、**[実行]** をクリックします。
2. レポート データの **[開始日]** と **[終了日]** を選択します。
3. レポートの**出力フォーマット**を選択します。

フォーマット	説明
PDF	Portable Document Format。PDF ファイルは Adobe Reader に表示されます。
HTML	HyperText Markup Language。HTML ファイルは、Internet Explorer または Firefox ブラウザで直接に表示できます。
XLS	Excel スプレッドシート。XLS ファイルは Microsoft Excel に表示されます。

4. **上位 N 件**レポートを選択した場合は、レポートする項目の数を選択します。
5. **[実行]** をクリックします。

   HTML レポートがコンテンツペインに表示されます。PDF または XLS 出力を選択した場合、レポートを別のウィンドウに表示するか、レポートをディスクに保存するかを選択することができます。
6. レポートを印刷するには、レポートを表示するプログラムの印刷オプションを使用します。

最も適切な印刷を行うには、印刷用に PDF または XLS 出力を生成します。次に、Adobe Reader または Microsoft Excel の印刷オプションを使用します。

PDF または XLS フォーマットで出力されるレポートを保存するには Adobe Reader または Microsoft Excel の保存機能を使用します。

プレゼンテーション レポートのスケジュール設定

関連トピック：

- プレゼンテーション レポート、98 ページ
- プレゼンテーション レポートの作成、109 ページ
- スケジュールされたジョブのリストの表示、115 ページ
- プレゼンテーション レポートのコピー、101 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するか、または **[プレゼンテーション レポート] > [スケジューラ]** ページを使用して、1 つ以上のレポートを実行するためのスケジュールを定義するジョブを作成できます。

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。

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。

- [プレゼンテーション レポート]ページ(レポート カタログの上) の上部の**[スケジューラ]** ボタンをクリックします。
- レポートのレポート フィルタを追加または編集するとき、[確認] タブで **[保存してスケジュール]** を選択し、**[終了]** をクリックします。(プレゼンテーション レポートのコピー、101 ページ を参照。)
- ジョブを編集するには、[ジョブ キュー] ページのジョブ名リンクをクリックします。
- 新しいジョブを追加するには、[ジョブ キュー] ページの **[追加]** をクリックします。

[スケジューラ] ページには、実行するレポートと、レポートを実行するスケジュールを選択するための一連のタブがあります。詳細な手順は、次を参照してください：

- スケジュールの設定、112 ページ
- スケジュールするレポートの選択、113 ページ
- 出力オプションの選択、115 ページ
- 日付範囲の設定、114 ページ

ジョブを作成した後、ジョブのステータスおよび他の有益な情報を示すジョブのリストを表示できます。スケジュールされたジョブのリストの表示、115 ページを参照してください。

スケジュールの設定

関連トピック：

- プレゼンテーション レポートのスケジュール設定、111 ページ
- スケジュールするレポートの選択、113 ページ
- 出力オプションの選択、115 ページ
- 日付範囲の設定、114 ページ

[プレゼンテーション レポート] > [スケジューラ] ページの **[スケジュール]** タブで、1 回または繰り返し実行するレポート ジョブを定義します。

ご注意：
ログ データベースの過負荷とロギングおよび対話形式レポート作成のパフォーマンス低下を避けるために、レポート ジョブを実行する曜日と時間帯を分散することを推奨します。

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. ジョブの **[繰り返しパターン]** と **[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	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. **[時刻のスケジュール]** で、ジョブの実行の開始時刻を設定します。

ジョブは、Websense Manager を実行しているコンピュータ上の時刻に従って開始します。

> **ご注意：**
> 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. **[期間のスケジュール]** で、ジョブを開始する日付とジョブを終了するためのオプションを選択します。

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、115 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、115 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. **[次へ]** をクリックして [レポート] タブを開きます。スケジュールするレポートの選択、113 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

関連トピック：

- プレゼンテーション レポートのスケジュール設定、111 ページ
- スケジュールの設定、112 ページ
- 出力オプションの選択、115 ページ
- 日付範囲の設定、114 ページ

[プレゼンテーション レポート] > [スケジューラ] ページの **[レポートの選択]** タブを使用して、ジョブのレポートを選択します。

1. [レポート カタログ] ツリーでこのジョブで実行するレポートをハイライトします。
2. 右矢印 (>) ボタンをクリックして、そのレポートを **[選択済み]** リストに移動します。

3. このジョブで実行するすべてのレポートが**[選択済み]**リストに表示されるまで、ステップ 1 ～ 2 を繰り返します。
4. **[次へ]** をクリックして [日付範囲] タブを開きます。日付範囲の設定、114 ページを参照してください。

日付範囲の設定

関連トピック :
- プレゼンテーション レポートのスケジュール設定、111 ページ
- スケジュールの設定、112 ページ
- スケジュールするレポートの選択、113 ページ
- 出力オプションの選択、115 ページ

[プレゼンテーション レポート] > [スケジューラ] ページの **[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。使用できるオプションは、**日付の範囲**の選択によって異なります。

日付の範囲	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 (今、最新、最新 2 など)、および期間のタイプ (日数、週数、または月数) を指定します。たとえば、「最近 2 週間」あるいは「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、[今週] は、日曜から今日までのレポートを作成します。[今月] は、月の初めから今日までのレポートを作成します。[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。

ジョブの日付範囲を設定した後、**[次へ]** をクリックして [出力] タブを表示します。出力オプションの選択、115 ページを参照してください。

出力オプションの選択

関連トピック：

- プレゼンテーション レポートのスケジュール設定、111 ページ
- スケジュールの設定、112 ページ
- スケジュールするレポートの選択、113 ページ
- 日付範囲の設定、114 ページ

ジョブで実行するレポートを選択した後、[**出力**] タブを使用して出力フォーマットおよび配信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	Portable Document Format。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. 必要な場合、[**電子メールの件名と本文をカスタマイズ**] チェックボックスをオンにします。次に、このジョブの配信電子メールのカスタム**件名** と**本文**テキストを入力します。
4. [**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、[ジョブ キュー] 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、115 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

関連トピック：

- プレゼンテーション レポート、98 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、111 ページ
- 出力オプションの選択、115 ページ
- 調査レポートのスケジュール設定、139 ページ

[プレゼンテーション レポート] > **[ジョブ キュー]** ページは、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されたジョブをリストします。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、スケジュールされた調査レポート ジョブの管理、142 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。
状態	次のどちらかを示します。 • [有効] は、指定された繰り返しパターンに従って実行するジョブを示します。 • [無効] は、アクティブでなく、実行しないジョブを示します。
繰り返し	このジョブの繰り返しパターン（[1 回]、[毎日]、[毎週]、[毎月]）を設定します。
履歴	選択したジョブの [ジョブ履歴] ページを開くには、**[詳細]** リンクをクリックします。ジョブ履歴の表示、117 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	[スケジューラ] ページを開きます。そこでジョブ定義を編集できます。プレゼンテーション レポートのスケジュール設定、111 ページを参照してください。
ジョブの追加	[スケジューラ] ページを開きます。そこで新しいジョブを定義できます。プレゼンテーション レポートのスケジュール設定、111 ページを参照してください。
削除	[ジョブ キュー] 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、**[無効にする]** ボタンを使用します。
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。

オプション	説明
有効にする	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。
無効にする	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

関連トピック：

- プレゼンテーション レポートのスケジュール設定、111 ページ
- スケジュールされたジョブのリストの表示、115 ページ

[プレゼンテーション レポート] > [ジョブ キュー] > [ジョブ履歴] ページを使用して、選択したジョブの最近における試行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
レポート名	レポートに表示されるタイトル。
開始日	レポートの実行を開始した日付と時刻。
終了日	レポートが完了した日付と時刻。
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。
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。

調査レポート

関連トピック：

- 要約レポート、120 ページ
- マルチレベル要約レポート、125 ページ
- 柔軟な詳細レポート、126 ページ
- ユーザの活動詳細レポート、131 ページ
- 標準レポート、135 ページ
- 使用頻度の高い調査レポート、137 ページ
- 調査レポートのスケジュール設定、139 ページ
- 外れ値レポート、143 ページ
- ファイルへの出力、144 ページ
- データベース接続とレポートのデフォルト、336 ページ

[レポート] > [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形式で分析します。

最初に、調査レポートのメイン ページに、リスク クラス別のアクティビティの要約レポートが表示されます。要約レポート ビューに表示されているリンクおよび要素をクリックすることによって、関心のある領域の詳細を表示し、組織のインターネット使用状況の一般的な動向を把握します。要約レポート、120 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、125 ページを参照）および柔軟な詳細レポート（柔軟な詳細レポート、126 ページを参照）によって、情報を種々の観点から分析できます。

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
日 / 月別ユーザ	特定のユーザのアクティビティについて、1 日または 1 カ月のレポートを定義するダイアログボックスが表示されます。詳細は、ユーザの活動詳細レポート、131 ページ を参照してください。
標準レポート	特定のデータの組み合わせをすばやく参照できるように、事前定義されたレポートのリストが表示されます。標準レポート、135 ページを参照してください。

オプション	アクション
使用頻度の高いレポート	現在のレポートを「使用頻度の高いレポート」として保存でき、また、生成またはスケジュール設定できる既存の使用頻度の高いレポートのリストを表示します。使用頻度の高い調査レポート、137 ページを参照してください。
ジョブ キュー	スケジュールされた調査レポート ジョブのリストを表示します。調査レポートのスケジュール設定、139 ページを参照してください。
外れ値の表示	平均と大幅に異なるインターネット使用状況を示すレポートを表示します。外れ値レポート、143 ページを参照してください。
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。[オプション] ページを使用して特定のレポート機能をカスタマイズすることもできます。たとえば、要約レポート上に最初に表示される時間や詳細レポートのデフォルト列などです。データベース接続とレポートのデフォルト、336 ページを参照してください。
	[検索] フィールドの右側にあるこのボタンをクリックして、現在のレポートを Microsoft Excel に適合するスプレッドシート ファイルにエクスポートします。 ファイルを開くかまたは保存するかを尋ねられます。ファイルを開くには、Microsoft Excel 2003 以降がインストールされている必要があります。ファイルへの出力、144 ページを参照してください。
	[検索] フィールドの右側にあるこのボタンをクリックして、現在のレポートを Adobe Reader に適合する PDF ファイルにエクスポートします。 ファイルを開くかまたは保存するかを尋ねられます。ファイルを開くには、Adobe Reader 7.0 以降がインストールされている必要があります。ファイルへの出力、144 ページを参照してください。

レポートはログ データベースで記録されている情報に限定されます。ユーザ名、IP アドレス、または選択したカテゴリ (ログ記録のための Filtering Service 設定、310 ページを参照) のロギングを無効にした場合、その情報を含めることはできません。同様に、特定のプロトコル (プロトコル フィルタの編集、52 ページを参照) のロギングを無効にした場合、これらのプロトコルの情報は使用できません。レポートにドメイン名 (www.domain.com) とドメイン内の特定のページへのパス (/products/productA) の両方を表示したい場合、完全な URL (完全 URL によるログ記録の設定、328 ページを参照) をログする必要があります。

Websense 調査レポートは、Websense Manager を実行しているコンピュータのプロセッサと使用可能なメモリ、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。大きなレポートは、生成するのに非常に長い時間がかかることがあります。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し、別の日時に実行するようにスケジュール設定できるオ

プションが含まれます。調査レポートのスケジュール設定、139 ページを参照してください。

要約レポート

関連トピック：

- マルチレベル要約レポート、125 ページ
- 柔軟な詳細レポート、126 ページ
- ユーザの活動詳細レポート、131 ページ
- 標準レポート、135 ページ
- 使用頻度の高い調査レポート、137 ページ
- 調査レポートのスケジュール設定、139 ページ
- 外れ値レポート、143 ページ
- ファイルへの出力、144 ページ

調査レポート ページは最初に、ログ データベースからの、すべてユーザの今日のアクティビティを示すリスククラス別の使用状況の要約レポートを示します。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。この最初の要約レポートの対象となる時間を設定する方法については、データベース接続とレポートのデフォルト、336 ページを参照してください。

ページに表示される種々のリンクおよびオプションをクリックすることによって、レポートされる情報をすばやく変更したり、レポートの詳細に絞り込むことができます。

1. **[測定]** リストから、次のいずれかのオプションを選択します。

オプション	説明
ヒット件数	URL が要求された回数。 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。ログ キャッシュ ファイルの設定、317 ページを参照してください。
帯域幅 [KB]	ユーザからの最初の要求および Web サイトからの応答の両方に含まれるデータの量 (単位はキロバイト)。この値は、送信および受信の両方の帯域幅の合計です。 一部の統合製品は、この情報を Websense ソフトウェアに送信しません。この 2 つの例として、Check Point FireWall-1 と Cisco PIX Firewall があります。統合製品がこの情報を送信せず、Websense Network Agent がインストールされている場合、帯域幅情報に関するレポートを有効にするためには、該当する NIC の **Log HTTP 要求 (拡張ログ)** オプションをアクティブにします。NIC 設定、349 ページを参照してください。
送信バイト数 [KB]	インターネット要求として送信されるキロバイト数。これは送信されたデータの量を表します。これには単純な URL 要求、または大量の送信を含む (たとえばユーザが Web サイトへの登録を行った) 場合があります。
受信バイト数 [KB]	要求に対する応答で受信したキロバイト数。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、キロバイト数は、ログ レコードを作成しているソフトウェアによって異なります。Websense Network Agent がレコードをログしている場合は、ブロックされたサイトの受信バイト数は Websense ブロック ページのサイズを表します。 リアルタイム 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、受信キロバイト数はスキャンされたページのサイズを表します。リアルタイム スキャンの詳細については、リアルタイム オプションによるコンテンツの分析、147 ページを参照してください。 他の統合製品によってログ レコードが作成された場合、ブロックされたサイトの受信キロバイト数は 0 か、ブロック ページのサイズか、または要求されたサイトから取得した値のいずれかです。
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 ブラウズ時間について、97 ページを参照してください。

2. レポートの上の**[インターネット使用状況]**リストからオプションを選択することによって、レポートのプライマリ分類を変更します。

   オプションは、ログ データベース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、ログ データベース内に 1 つのグループまたはドメインしかない場合、グループおよびドメイン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。表示および出力オプション、338 ページ を参照。)

3. 左列の名前 (または名前の横の矢印) をクリックして、[ユーザ別]、[ドメイン別]、[アクション別] などオプションのリストを表示します。

   リストされるオプションは、[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。

   > **ご注意 :**
   > [ユーザ] や [グループ] などのオプションは赤文字で表示されることがあります。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。

   たとえば、リスククラス要約レポートで、「法的責任」リスククラスの下の [ユーザ別] をクリックして、「法的責任」リスククラス内の各ユーザの使用状況のレポートを生成します。

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. 列見出しの横の矢印を使用して、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
レポート・パス （ユーザ > 日付）	**[インターネット使用状況]** リストの横には、現在のレポートに選択した条件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。
表示	レポートの期間を選択します。[1 日]、[1 週間]、[1 カ月]、または [すべて]。レポートは、選択した期間のデータを表示するように更新されます。 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、**[対象期間開始]** フィールドは、表示される期間を反映するように更新されます。 [対象期間 / 開始] フィールドまたは [使用頻度の高いレポート] ダイアログボックスで特定の日付を選択した場合、**[表示]** 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。
対象期間開始 ... 終了 ...	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。
円グラフ / 棒グラフ	棒グラフが表示されているとき、**[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。 棒グラフが表示されているとき、**[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。
全画面表示	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。

オプション	アクション
匿名 / 名前	[**匿名**] をクリックすると、レポートの中のユーザ名を表示する箇所に、内部的に割り当てられたユーザ ID 番号が表示されます。 名前が隠されているとき、[**名前**] をクリックするとその場所にユーザ名が表示されます。 ユーザ名を表示できない場合もあります。詳細は、ログ記録のための Filtering Service 設定、310 ページ を参照してください。 [匿名] をクリックしてからデータの別のビュー（詳細ビュー、外れ値など）に移動した場合、新しいレポートでもユーザ名は隠されたままです。しかし、名前を隠したまま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、レポートの上部のリンクを使用します。 個別の管理者がレポート内のユーザ名を表示できないようにするには、その管理者に、調査レポート内のユーザ名の表示およびプレゼンテーション レポートへのアクセスを禁止するようなレポート権限を持つロールを割り当てます。
検索対象	リストからレポート要素を選択し、隣のテキスト ボックスに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。

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、125 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、126 ページを参照してください。

マルチレベル要約レポート

関連トピック：
- 調査レポート、118 ページ
- 要約レポート、120 ページ
- 柔軟な詳細レポート、126 ページ
- ユーザの活動詳細レポート、131 ページ
- 標準レポート、135 ページ
- 使用頻度の高い調査レポート、137 ページ
- 調査レポートのスケジュール設定、139 ページ
- 外れ値レポート、143 ページ
- ファイルへの出力、144 ページ

マルチレベル要約レポートは、表示されているプライマリ情報を補う第 2 レベルの情報を表示します。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. **[上位]** リストで、レポートするプライマリ・エントリ（左列）の数を指定する数値を選択します。生成されるレポートには、上位の値を持つプライマリ エントリが表示されます（「日」がプライマリ エントリである場合、このレポート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。**[上位]** フィールドには「**カスタム**」という語が表示されます。
2. **[ソート キー]** リストから、レポートする 2 番目の情報を選択します。
3. **[表示]** フィールドで、各プライマリ エントリに対してレポートするセカンダリ結果の数を選択します。
4. **[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. 列見出しの横の矢印を使用して、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、**[インターネット使用状況]** の下の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

関連トピック：

- 調査レポート、118 ページ
- 要約レポート、120 ページ
- マルチレベル要約レポート、125 ページ
- 使用頻度の高い調査レポート、137 ページ
- 調査レポートのスケジュール設定、139 ページ
- 外れ値レポート、143 ページ
- ファイルへの出力、144 ページ
- データベース接続とレポートのデフォルト、336 ページ
- 柔軟な詳細レポートの列、128 ページ

詳細レポートは、ログ データベース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、Websense Manager を実行しているコンピュータのプロセッサと使用可能なメモリ、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、120 ページまたはマルチレベル要約レポート、125 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。

   詳細レポートをロードしているあいだ、ポップアップ メッセージに進捗が表示されます。

   ご注意：
   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、137 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、336 ページ を参照。）
5. ページの上部の **[レポートの変更]** をクリックします。

   [レポートの変更] ダイアログボックスの **[現在のレポート]** リストに、現在の詳細レポートに表示される列が示されます。
6. **[使用可能な列]** または **[現在のレポート]** リストで列名を選択し、右矢印 (>) または左矢印 (<) ボタンをクリックすると、その列が反対側のリストに移動します。

   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。

   使用可能な列のリストおよび各列の説明を柔軟な詳細レポートの列、128 ページに示しています。
7. **[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。

   [現在のレポート] 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. レポートの上の**[要約]**または**[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 [時間] 列を削除する必要があります。要約レポートでは、共通の要素を共有するすべてのレコードが 1 つのエントリに集められます。専用の要素は、レポートされる情報によって変化します。一般に、基準の前の一番右の列は 要約された要素を示します。
詳細	[詳細] 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。[時間] 列を表示できます。

9. **[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**[表示]**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**[次]**および**[前]**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。表示および出力オプション、338 ページを参照してください。
    - 要求した Web 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、**[使用頻度の高いレポート]**をクリックします。(使用頻度の高いレポートの保存、137 ページを参照してください)。

柔軟な詳細レポートの列

関連トピック :

- 柔軟な詳細レポート、126 ページ
- 使用頻度の高い調査レポート、137 ページ
- 調査レポートのスケジュール設定、139 ページ

下の表は、詳細レポートに使用できる列を示しています (柔軟な詳細レポート、126 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、[ユーザ] 列が表示される場合、[グループ] 列は使用できません。[カテゴリ] 列が表示される場合、[リスク クラス] 列は使用できません。

列名	説明
ユーザ	要求を行ったユーザの名前。ユーザ情報をレポートに含めるためには、それがログ データベースからアクセスできなければなりません。ユーザ ベースのレポートではグループ情報は使用できません。
日付	要求が発行された日付。
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)。
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、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。
グループ	要求者が所属するグループの名前。グループ ベースのレポートには個々のユーザ名は表示されません。サイトを要求したユーザがディレクトリ サービス内の複数のグループに所属している場合、レポートのこの列には複数のグループがリストされます。
リスク クラス	要求したサイトが所属するカテゴリに関連付けられたリスク クラス。カテゴリが複数のリスク クラスに所属する場合は、関連するすべてのリスク 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、308 ページを参照してください。
ディレクトリ オブジェクト	要求を行ったユーザのディレクトリ パス (ユーザ名を含まない)。一般的には各ユーザは複数のパスに属していますから、同じトラフィックについて複数の行が生成されます。 非 LDAP ディレクトリ サービスを使用する場合は、この列は使用できません。
フィルタの種類	Websense ソフトウェアが要求に対して行ったアクション (「許可されたカテゴリ」、「ブロックされたカテゴリ」など)。
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。このコンピュータは、統合製品または Websense Network Agent のどちらかを実行しているコンピュータです。
プロトコル	要求のプロトコル。
プロトコル グループ	要求されたプロトコルが含まれるマスタ データベースのグループ。
送信元 IP	要求の発行元のコンピュータの IP アドレス。
宛先 IP	要求されたサイトの IP アドレス。
完全 URL	要求されたサイトのドメイン名およびパス (例 : http://www.mydomain.com/products/itemone/)。完全 URL をログしていない場合、この列は空白になります。完全 URL によるログ記録の設定、328 ページを参照してください。

列名	説明
月	要求が発行された暦月。
ポート	ユーザがサイトとの通信に使用する TCP/IP ポート。
帯域幅	ユーザからの最初の要求および Web サイトからの応答の両方に含まれるデータの量（単位はキロバイト）。この値は、送信および受信の両方の帯域幅の合計です。 一部の統合製品は、この情報を Websense ソフトウェアに送信しません。この 2 つの例として、Check Point FireWall-1 と Cisco PIX Firewall があります。統合製品がこの情報を送信せず、Websense Network Agent がインストールされている場合、帯域幅情報に関するレポートを有効にするためには、該当する NIC の **Log HTTP 要求（拡張ログ）**オプションをアクティブにします。NIC 設定、349 ページを参照してください。
送信バイト数	インターネット要求として送信されるデータのキロバイト数。これは送信されたデータの量を表します。これには単純な URL 要求、または大量の送信を含む（たとえばユーザが Web サイトへの登録を行った）場合があります。
受信バイト数	要求に対する応答で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、キロバイト数は、ログ レコードを作成しているソフトウェアによって異なります。Websense Network Agent がレコードをログしている場合は、ブロックされた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。 リアルタイム 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。リアルタイム スキャンの詳細については、リアルタイム オプションによるコンテンツの分析、147 ページを参照してください。 他の統合製品によってログ レコードが作成された場合、ブロックされたサイトの受信キロバイト数は 0 か、ブロック ページのサイズか、または要求されたサイトから取得した値のいずれかです。
時刻	サイトが要求された時刻が 24 時間時計を使って HH:MM:SS 形式で表示されます。
カテゴリ	要求をフィルタリングする基準となったカテゴリ。このカテゴリは、Websense 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。

ユーザの活動詳細レポート

関連トピック：

- 調査レポート、118 ページ

1 人のユーザの「ユーザの活動詳細」レポートを生成するには、**[日 / 月別ユーザ]** リンクをクリックします。このレポートは、そのユーザの 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、特定のユーザの選択した日のレポートを生成します。そのレポートをもとに、同じユーザの 1 カ月間の活動のレポートを生成できます。詳細な手順は、次を参照してください：

- 日別ユーザ活動詳細、131 ページ
- 月別ユーザ活動詳細、132 ページ

日別ユーザ活動詳細

関連トピック：

- 調査レポート、118 ページ
- ユーザの活動詳細レポート、131 ページ
- 月別ユーザ活動詳細、132 ページ

日別のユーザ活動詳細レポートによって、特定のユーザの 1 日の活動をより詳しく調べることができます。

1. メインページの上部の **[日 / 月別ユーザ]** を選択します。[日別ユーザ詳細] ダイアログボックスが表示されます。
2. **[検索するユーザ]** フィールドにユーザの名前、または名前の一部を入力し、**[検索]** 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. **[ユーザの選択]** リストからユーザを選択します。
4. **[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. **[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、[月別ユーザ活動] レポートに表示されるリスク グループに対応します。月別ユーザ活動詳細、132 ページ を参照。）

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
前の日付 / 次の日	このユーザ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。
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、実行されたアクション（ブロック、許可、その他）と共に表示します。
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。
類似グループ ヒット件数 / 全ヒット件数の表示	10 秒以内の間隔で行われ、同じドメイン、カテゴリ、およびアクションも関係しているすべての要求を 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。この値を変更する必要がある場合は、表示および出力オプション、338 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、[全ヒット件数の表示] に戻り、各要求の元のリストが復元されます。
カテゴリ表示制御	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、**[適用]** 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. レポートの上の **[月別ユーザ活動詳細]** をクリックし、同じユーザの 1 カ月間の活動を表示します。詳細は、月別ユーザ活動詳細、132 ページを参照してください。

月別ユーザ活動詳細

関連トピック：

- 調査レポート、118 ページ
- ユーザの活動詳細レポート、131 ページ
- 日別ユーザ活動詳細、131 ページ
- カテゴリ マッピング、133 ページ

[日別ユーザ活動詳細]レポートが開いているとき、そのユーザの月別の活動を確認するためにレポートを切り替えることができます。

1. [日別ユーザ活動詳細]レポートを開きます。日別ユーザ活動詳細、131 ページを参照してください。
2. 上部の**[月別ユーザ活動詳細]**をクリックします。

   新しいレポートにカレンダの画像が表示され、それぞれの日付の領域には、その日のユーザのインターネット アクティビティを表す小さな色ブロックが表示されます。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**[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。カテゴリ マッピング、133 ページを参照してください。
4. **[前]**または**[次]**をクリックし、このユーザの先月または翌月のインターネット アクティビティを表示します。

カテゴリ マッピング

関連トピック:

- 調査レポート、118 ページ
- ユーザの活動詳細レポート、131 ページ
- 月別ユーザ活動詳細、132 ページ

下のリストは、[日別ユーザ利用状況]レポートおよび[月別ユーザ利用状況]レポートで、それぞれの色がどのカテゴリに対応しているかを示しています。

マスタ データベース内のカテゴリ名は変更されることがあります。また、カテゴリをいつでも追加または削除することができます。

色	カテゴリ
グレイ	カスタム カテゴリ 非 HTTP トラフィック
ダークブルー	**「ビジネス & 経済」**とそのすべてのサブカテゴリ **「教育」**とそのすべてのサブカテゴリ **健康** **「IT」**(検索エンジンおよびポータル、および Web ホスティング サブカテゴリを含む) **「その他」**サブカテゴリ(「コンテンツデリバリーネットワーク」、「ダイナミックコンテンツ(CGI-BIN)」、「イメージ(メディア)」、「イメージサーバー」、および「私的 IP アドレス」) **「生産性**/広告宣伝」

色	カテゴリ
ライトブルー	**麻薬 / 医薬品** / 処方薬 **「政府」**とそのサブカテゴリ「軍隊」 **「IT**/URL 翻訳サイト」 **「その他」**（親カテゴリのみ） **「ニュース・メディア」**（親カテゴリのみ） **スペシャル・イベント**
黄色 緑	**「中絶」**とそのすべてのサブカテゴリ **「アダルト** / 性教育」 **「帯域幅」**とそのサブカテゴリ「インターネット・ラジオと TV」、「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」 **「エンターテイメント」**とそのサブカテゴリ「MP3」 **ゲーム** **「政府** / 政治団体」 **「IT**/ コンピュータセキュリティ情報」 **「インターネット・コミュニケーション** /Web ベース電子メール」 **「その他** / ファイル·ダウンロード·サーバー」 **「その他** / ネットワークエラー」 **「ニュース・メディア** / 娯楽雑誌」 **「生産性」**とそのサブカテゴリ「インスタント・メッセージ」、「掲示板とフォーラム」、「オンライン証券 & トレーディング」 **「宗教」**とそのサブカテゴリ「非伝統的な宗教 , オカルト、民間伝承」、「伝統宗教」 **「セキュリティ」**（親カテゴリのみ） **「ショッピング」**とそのすべてのサブカテゴリ **「社会組織」**とそのすべてのサブカテゴリ **「社会 & ライフスタイル」**とそのサブカテゴリ「ゲイ、レズビアン、バイセクシャルル」、「趣味」、「個人 Web サイト」、「レストラン & 食事」 **「スポーツ」**とそのすべてのサブカテゴリ **旅行** **「ユーザー定義」** **乗り物**

色	カテゴリ
オレンジ	**「アダルト** / ヌード」 **主張グループ** **「帯域幅** / インターネット電話」 **「麻薬 / 医薬品」**とそのサブカテゴリ「麻薬 / 医薬品の乱用」、「マリファナ」、「栄養補助薬品 / 非規制化合物」 **「IT**/ プロキシによるブロック回避」 **「インターネット・コミュニケーション」**とそのサブカテゴリ「Web チャット」 **求人情報** **「その他** / 未分類」 **「生産性」**とそのサブカテゴリ「フリーウェア / ソフトウェアダウンロード」、「報酬サイト」 **「宗教」** **「社会 & ライフスタイル」**とそのサブカテゴリ「アルコール & 煙草」、「出会い、結婚 / お見合いサービス」 **悪趣味** **武器**
赤	**「アダルト」**とそのサブカテゴリ「アダルト・コンテンツ」、「ランジェリー & 水着」、「セックス」 **「帯域幅** / ピア・ツー・ピアによるファイル共有」 **ギャンブル** **違法行為** **「IT**/ ハッカー関連」 **過激派グループ** **人種差別** **「セキュリティ」**とそのサブカテゴリ「キーロガー」、「MMC 感染サイト」、「フィッシング」、「スパイウェア」 **暴力**

標準レポート

関連トピック :

- 調査レポート、118 ページ
- 使用頻度の高い調査レポート、137 ページ
- 調査レポートのスケジュール設定、139 ページ

標準レポートを使用すれば、絞り込み処理なしにすばやく特定の情報のセットを表示できます。

1. 調査レポートのメイン ページの**[標準レポート]**リンクをクリックします。

2. 参照したい情報を含んでいるレポートを選択します。以下のレポートがあります。

最高アクティビティ レベルを基準に絞り込みます
• アクセス回数が最も多かったユーザ • アクセス件数上位 10 件の URL のユーザ上位 10 名 • ショッピング、エンターテイメント、スポーツに分類されたサイトを閲覧した上位 5 ユーザ • アクセス件数上位 5 カテゴリの上位 5 URL
帯域幅消費が最も高かったものを基準に絞り込みます
• 帯域幅を最も消費しているグループ • ストリーミング メディアで最も多く帯域幅を消費したグループ • ネットワーク帯域幅損失として検出されたユーザが閲覧していた URL の詳細レポート • 帯域幅カテゴリの上位 10 グループ
最も長い間オンラインだったユーザを基準に絞り込みます
• 最も長い時間オンラインで作業していたユーザ • 最も長い時間生産性カテゴリに含まれるサイトで作業していたユーザ
ブロックされた回数を基準に表示します
• ブロックされた回数が最も多かったユーザ • ブロックされた回数が最も多かったサイト • ユーザがブロックされた URL の詳細レポート • ブロックされたカテゴリの上位 10 カテゴリ
セキュリティ リスクが最も高かったものを基準に絞り込みます
• セキュリティ リスクの原因になりうる上位カテゴリ • P2P プロトコルの最多使用ユーザ • セキュリティ カテゴリに含まれるサイトの上位ユーザ • スパイウェア アクティビティが最も多かったコンピュータの上位 10 台で閲覧された URL
法的責任を基準に絞り込みます
• 法的責任を問われる対象になりうるアクセス（カテゴリ別） • アダルト カテゴリの上位ユーザ

3. 表示されるレポートを検討します。
4. 繰り返し実行する場合、こ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、137 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

関連トピック：

- 調査レポート、118 ページ
- 調査レポートのスケジュール設定、139 ページ

ほとんどの調査レポートを**使用頻度の高いレポート**として保存できます。これには、特定の情報に絞り込むことによって生成したレポート、標準レポート、特定のニーズに対応するように変更した詳細レポートが含まれます。その後、この使用頻度の高いレポートを随時実行するか、または、特定の日時に実行するようにスケジュール設定します。

指定済み管理を使用する組織では、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の許可は、優先管理者によって設定されます。この許可を与えられている管理者は、自分が保存した使用頻度の高いレポートのみを実行およびスケジュール設定できます。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アクセスする権限はありません。

使用頻度の高いレポートの使用の詳細については、以下の項を参照してください。

- 使用頻度の高いレポートの保存、137 ページ
- 使用頻度の高いレポートの生成または削除、138 ページ
- 使用頻度の高いレポートの修正、138 ページ

使用頻度の高いレポートの保存

関連トピック：

- 使用頻度の高い調査レポート、137 ページ
- 使用頻度の高いレポートの修正、138 ページ

以下の手順を使って、レポートを使用頻度の高いレポートとして保存します。

1. 必要な情報を含む希望する形式の調査レポートを生成します。
2. **[使用頻度の高いレポート]**をクリックします。
3. Websense Manager によって表示される名前を受け入れるか、変更します。

   名前には、文字、数字、および下線文字 (_) を含めることができます。空白やその他の特殊文字は使用できません。
4. **[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。

5. このリスト上でレポートを選択し、レポートを管理するためのオプションを選択します。選択するオプションに従って、以下のどちらかの項を参照してください。
   - 使用頻度の高いレポートの生成または削除、138 ページ
   - 調査レポートのスケジュール設定、139 ページ

使用頻度の高いレポートの生成または削除

関連トピック：
- 使用頻度の高い調査レポート、137 ページ
- 使用頻度の高いレポートの修正、138 ページ

いつでも、使用頻度の高いレポートを生成することができ、また、使用しなくなった使用頻度の高いレポートを削除できます。

1. **[使用頻度の高いレポート]** 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。

   ご注意：
   組織で指定済み管理を使用する場合、このリストは、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を含みません。

2. このリストから希望するレポートを選択します。

   希望するレポートが使用頻度の高いレポートとして保存されていない場合、使用頻度の高いレポートの保存、137 ページを参照してください。
3. 下記のいずれかの手順を実行します。
   - 選択したレポートをすぐに生成および表示するには、**[すぐに実行]** をクリックします。
   - レポートを後で実行するか、または定期的に実行するようにスケジュール設定するには、**[スケジュール]** をクリックします。詳細については、調査レポートのスケジュール設定、139 ページを参照してください。
   - 使用頻度の高いレポートのリストからレポートを削除するには、**[削除]** をクリックします。

使用頻度の高いレポートの修正

関連トピック：
- 調査レポート、118 ページ
- 使用頻度の高い調査レポート、137 ページ

下記の手順によって、既存の使用頻度の高いレポートをもとに、新しい使用頻度の高いレポートを簡単に作成できます。

1. **[使用頻度の高いレポート]** 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。

   ご注意：
   組織で指定済み管理を使用する場合、このリストは、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を含みません。

2. 作成する新しいレポートに最も近い既存の使用頻度の高いレポートを選択し、実行します（使用頻度の高いレポートの生成または削除、138 ページ を参照。）
3. 表示されたレポートを必要に合わせて修正します。
4. **[使用頻度の高いレポート]** をクリックして、修正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。（使用頻度の高いレポートの保存、137 ページ を参照。）

調査レポートのスケジュール設定

関連トピック：

- 使用頻度の高い調査レポート、137 ページ
- 使用頻度の高いレポートの保存、137 ページ
- スケジュールされた調査レポート ジョブの管理、142 ページ

調査レポートをあとで実行する、または繰り返し実行するためにスケジュール設定するには、その前にそれを「使用頻度の高いレポート」として保存しなければなりません。スケジュールされたレポート ジョブが実行されたとき、生成されたレポートは指定した受信者に電子メールで送信されます。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。

スケジュールされたレポート 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>\
```

デフォルト設定では、<install_path> は C:¥Program Files¥Websense です。スケジュールされたジョブの受信者が 1 人だけである場合、<name> が電子メー

ル アドレスの最初の部分 (@ の前) になります。受信者が複数である場合、レポートは「Other」という名前のディレクトリに保存されます。

> **ご注意 :**
> 繰り返し実行するジョブによって保存されるレポートは、常に同じ名前で保存されます。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。
>
> スケジュールされたレポートのサイズと数によっては、このディレクトリは非常に大きくなる場合があります。ディレクトリを定期的にクリアして、不必要なレポート ファイルを消去してください。

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。(使用頻度の高いレポートの保存、137 ページを参照)。

2. **[使用頻度の高いレポート]** 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。

   > **ご注意 :**
   > 組織で指定済み管理を使用している場合、このリスト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を含みません。

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. **[スケジュール]** をクリックしてスケジュール設定されたレポート ジョブを作成し、次に、[レポートのスケジュール] ページで要求される情報を入力します。

   ログ データベースの過負荷とロギングおよび対話形式レポート作成のパフォーマンス低下を避けるために、レポート ジョブを実行する曜日と時間帯を分散することを推奨します。

フィールド	説明
実行頻度	レポート ジョブを実行する頻度 ([1 回]、[毎日]、[毎週]、[毎月]) を選択します。
開始日	ジョブを最初に実行する日の曜日または暦日を選択します。
実行時刻	レポートを実行する時刻を設定します。
電子メール送信先	**[追加の電子メール アドレス]** フィールドを使用して、レポート受信者のアドレスをこのリストに追加します。 ジョブのレポートを受信する 1 つ以上の電子メール アドレスをハイライトしてください (レポートの受信者以外の選択を解除してください)。

フィールド	説明
追加の電子メール アドレス	電子メール アドレスを入力してから [**追加**] をクリックして、このアドレスを [**電子メール送信先**] リストに追加します。 新しい電子メール アドレスが自動的に、他の選択されている電子メール アドレスと共にハイライトされます。
電子メールの件名と本文をカスタマイズする	電子メール通知の件名と本文をカスタマイズするには、このチェックボックスにマークを付けます。 このボックスにチェックが付いていない場合、デフォルトの件名と本文が使用されます。
電子メールの件名	スケジュールされたレポートを配布するときに電子メールの件名として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の件名は、次のようになっています。 「調査レポートのスケジュール ジョブ」
電子メールの本文	スケジュールされたレポートを配布するときの電子メール メールの本文に追加するテキストを入力します。 電子メールは次のようになります。<CUSTOM TEXT> の代わりに、ここで入力したテキストが表示されます。 添付のファイルは Report Scheduler により生成されました。作成日時 : <CUSTOM TEXT> 生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。 ご注意 : このリンクは、受信者がジョブの送信元の Web サーバへのアクセスを許可されていない場合は機能しません。
スケジュール ジョブ名	スケジュールされているジョブに一意な名前を割り当てます。この名前は、ジョブ キューの中でこのジョブを識別します。スケジュールされた調査レポート ジョブの管理、142 ページを参照してください。

フィールド	説明
出力フォーマット	スケジュールされたレポートのファイル形式を選択します。 **PDF**: Portable Document Format ファイルは Adobe Reader に表示されます。 **Excel**: Excel スプレッドシート ファイルは Microsoft Excel に表示されます。
日付の範囲	このジョブのレポートの対象となる日付の範囲を設定します。 **[すべての日付]**: ログ データベースに含まれるすべての日付 **[日付範囲を指定]**: 期間 (日数、週数、月数) と、期間に含める特定の日、週または月 (今日、先週、過去 2 カ月等)。 **[特定の日付]**: このジョブのレポートの対象となる日付 (1 つまたは複数) を設定します。

5. **[次へ]** をクリックして [スケジュールの確認] ページを表示します。
6. **[保存]** をクリックして選択を保存し、[ジョブ キュー] ページへ進みます (スケジュールされた調査レポート ジョブの管理、142 ページを参照)。

スケジュールされた調査レポート ジョブの管理

関連トピック :

- 調査レポート、118 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、111 ページ

調査レポートのスケジュールされたジョブを作成したとき、**[ジョブ キュー]** ページが表示され、新しいジョブと、既存のスケジュールされたジョブのリストを示します。また、調査レポートのメイン ページの **[ジョブ キュー]** リンクをクリックすることによってこのページにアクセスすることもできます。

ご注意 :
組織で指定済み管理を使用している場合、このページは、他の管理者によってスケジュールされたジョブを表示しません。

[レポートのスケジュール - 詳細] セクションは、スケジュールされた各ジョブを作成順にリストし、定義されているスケジュールの概要とジョブ ステータスを示します。また、次のオプションが利用可能です。

オプション	説明
編集	このジョブに定義されているスケジュールを表示し、必要に応じて編集できるようにします。
削除	ジョブを削除し、[ステータス ログ] セクションに「削除済み」のジョブを表すエントリを追加します。

[ステータス ログ] セクションには何らかの変更があった各ジョブがリストされ、そのジョブのスケジュールされている開始時刻と実際の終了時刻、およびステータスが表示されます。

[ステータス ログ] セクションのすべてのエントリを削除するには、**[ステータス ログのクリア]** をクリックします。

外れ値レポート

関連トピック :

- 調査レポート、118 ページ
- 要約レポート、120 ページ

外れ値レポートは、データベースの情報をもとに、どの従業員がもっとも多くの異常なインターネット アクティビティを行っているかを示します。Websense ソフトウェアはすべてのユーザのカテゴリ別、日別、アクション (フィルタの種類) 別、プロトコル別の平均アクティビティを計算します。次に、統計的に平均からもっとも大きく逸脱しているユーザ アクティビティを表示します。外れ値は、平均値からの標準偏差として計算されます。

1. 調査レポートのメイン ページで、外れ値を調べたい情報の要約レポートを生成します。下線が付いていて、[インターネット使用状況] フィールドの横に青で表示されているレポートが、外れ値レポートに反映されます。

   たとえば、特定のカテゴリのヒット件数別の外れ値を表示するには、**[インターネット使用状況]** リストで **[カテゴリ]** を選択し、**[測定基準]** に **[ヒット件数]** を選択します。

   ご注意 :
   ブラウズ時間を基準とする外れ値レポートを生成することはできません。ブラウズ時間を示す要約情報から開始した場合、外れ値レポートはヒット件数を基準として生成されます。

2. **[外れ値の表示]** をクリックします。

行は降順にソートされ、最も値が大きいものが最初に表示されます。各行には次の情報が表示されます。

- ユーザ、カテゴリ、プロトコル、日、アクション別の合計（ヒット件数または使用帯域幅）
- そのカテゴリ、プロトコル、日、アクションの全ユーザの平均（ヒット件数または使用帯域幅）
- ユーザの平均からの差

3. このカテゴリに対する特定のユーザの一定期間内のアクティビティを見るには、ユーザ名を選択します。

   たとえば、あるユーザのアクティビティが特定の日に著しく高い場合、そのユーザの名前をクリックして、そのユーザの全体的なアクティビティをより詳しく示すレポートを表示します。

ファイルへの出力

関連トピック：

- 調査レポート、118 ページ
- 調査レポートの印刷、145 ページ

調査レポートを生成した後、レポートの上部のボタンを使って、そのレポートをファイルに保存できます。クリックするボタンによって、ファイルの形式が決まります。

オプション	説明
	レポートを XLS 形式で保存します。 Websense Manager をアクセスしているコンピュータに Microsoft Excel 2003 以降がインストールされている場合は、レポートを表示または保存するように要求されます。そうでない場合は、保存するレポートのディレクトリおよびファイル名を選択するように要求されます。 レポートを印刷、保存、または電子メール送信するには、Microsoft Excel のオプションを使用します。
	レポートを PDF 形式で生成します。 Websense Manager をアクセスしているコンピュータに Adobe Reader v7.0 以降がインストールされている場合は、レポートを表示または保存するように要求されます。そうでない場合は、保存するレポートのディレクトリおよびファイル名を選択するように要求されます。 レポートを印刷、保存、または電子メール送信するには、Adobe Reader のオプションを使用します。

調査レポートの印刷

関連トピック：

- 調査レポート、118 ページ
- ファイルへの出力、144 ページ

次のいずれかの方法によって調査レポートを印刷できます。

- レポートが表示されているときに、Web ブラウザ印刷機能を使用する。
- PDF または XLS ファイルを作成し、次に Adobe Reader または Microsoft Excel の印刷機能を使用する（ファイルへの出力、144 ページを参照）。

レポートは、ブラウザから正常に印刷されるように設定されていますが、結果を確認するために、印刷テストを実行することもできます。

「月別ユーザ利用状況」レポートは、横方向モードで印刷されるように設定されます。他のすべてのレポートは、縦方向モードに設定されています。

カスタム レポートを設計するとき（柔軟な詳細レポート、126 ページを参照）、列の幅はレポートに含まれる情報によって異なります。レポートの幅が 8 1/2 インチよりも広い場合、ページ方向は横方向に変わります。

ページの印字面の幅は、7 1/2 インチまたは 10 インチです。A4 の場合、余白は少し狭くなりますが、印刷範囲に収められます（デフォルト用紙サイズは、Letter、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。表示および出力オプション、338 ページ を参照。）

セルフレポートへのアクセス

関連トピック：

- 調査レポート、118 ページ
- レポートの優先設定、310 ページ
- セルフ レポート、341 ページ

Websense セルフレポートを使って自分のインターネット ブラウジング アクティビティを評価し、必要に応じてそれを組織のガイドラインに対応するように調整できます。この機能はまた、組織がユーザに関して収集している情報をユーザに開示することを求める国家の法規への適合をサポートします。

組織の中でセルフレポートが有効にされている場合、ブラウザからそのレポートにアクセスします。

1. Websense 管理者によって提供された URL を入力するか、Websense Manager メイン ログオン ページの [セルフレポート] 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** がドロップダウンリストを表示する場合、ユーザのインターネット アクティビティに関する情報のログがある Policy Server の IP アドレスを選択します。

   詳細については Websense 管理者に問い合わせてください。
3. ネットワークへのログオンに使用する**[ユーザ名]**および**[パスワード]**を入力します。
4. **[ログオン]** をクリックします。

Websense Manager は、リスククラス別にインターネット アクティビティを示す調査レポートを表示します。ページ上の種々のリンクおよび要素をクリックして他のオプションにアクセスすることによって、ユーザのアクティビティに関して保存されている情報を別のビューで見ることができます。レポートの操作時に、わからないことがあれば **[ヘルプ]** システムにアクセスしてください。

7 リアルタイム オプションによるコンテンツの分析

関連トピック：

- スキャン オプション、149 ページ
- コンテンツの分類と脅威のスキャン、150 ページ
- ファイルのスキャン、151 ページ
- コンテンツのストリッピング、153 ページ
- リアルタイム スキャン アクティビティのレポート、156 ページ

Websense フィルタリング ソフトウェアは、アクティブになっているポリシーとマスタ データベースに格納されている情報に基づいて、インターネット アクティビティをフィルタします。Websense Content Gateway または Websense Web Security Gateway に加入している場合は、さらに、Web サイトおよびファイルの内容の分析をリアルタイムで行うことができます。

サブスクリプションの内容によっては、2 つのリアルタイム分析オプション、すなわち、コンテンツの分類とセキュリティ リアルタイム スキャンが使用可能です。

- **コンテンツの分類**を使用して、（アクティブなポリシーとマスタ データベースの URL 分類に基づいて）まだブロックされていない URL のコンテンツを検討し、フィルタリングで使用するカテゴリを返します。
- Websense Web Security Gateway に加入している場合は、3 つの**セキュリティ リアルタイム スキャン** オプションが使用可能です。
  - **コンテンツのスキャン**は、Web コンテンツを調べて、フィッシング、URL リダイレクション、Web エクスプロイト、プロキシ回避などのセキュリティの脅威を見つけます。
  - **ファイルのスキャン**は、ファイルのコンテンツを検査して、ウイルス、トロイの木馬、ワームなどの脅威のカテゴリを決定します。
  - **コンテンツのストリッピング**は、要求された Web ページからアクティブなコンテンツを削除します。

これらのオプションのいずれかが有効になっている場合は、アクティブなポリシーと Websense マスタ データベース分類に基づいてまだブロック**されて**

いないサイトのみが、分析の対象になります。詳細は、スキャン オプション、149 ページ を参照してください。

> **重要**
> 制限付きアクセス フィルタおよびフィルタなし URL は、リアルタイム分類を無効にします。
>
> ユーザが、アクティブになっている制限付きアクセス フィルタ（ユーザのアクセスを指定したサイトのリストに制限、170 ページを参照）またはフィルタなし URL リスト（特定のサイトのフィルタリングの再定義、184 ページを参照）に含まれているサイトを要求した場合には、リアルタイム スキャンが行われ脅威が見つかった場合でも、要求は許可されます。

これらのリアルタイム セキュリティ機能を活用するには、以下の 2 つの場所で、Websense Content Gateway または Websense Web Security Gateway のサポートを含んでいるサブスクリプション キーを入力します：

- Websense Manager（**[設定]** > **[アカウント]** に移動）。
- Websense Content Gateway 管理インターフェース（**[構成]** > **[プロキシ]** > **[サブスクリプション]** > **[サブスクリプションの管理]** タブに移動）。

2 つの製品が必要なデータベースをダウンロードし、両方の管理ツールにおけるすべてのリアルタイム機能を同期させ、表示するには、数分かかります。

Websense リアルタイム オプション

Websense リアルタイム オプションは、ネットワーク セキュリティを確保するのに役立ちます。これらのオプションを使用してインターネット コンテンツをスキャンし、フィルタリング カテゴリを割り当てます。リアルタイムな結果は Filtering Service に送信され、Filtering Service はアクティブなポリシーにおいてリアルタイム分類に割り当てられているアクションに基づいてそのサイトをフィルタします。

データベースのダウンロード

リアルタイム オプションは、Websense Web Security Gateway とともにインストールされた小さなデータベースに依拠しており、Websense Web Security Gateway は定期的にデータベース更新をチェックします。これらのデータベースの更新は、すべてのマスタ データベースの更新とは独立に行われます（リアルタイム データベース更新および Real-Time Security Updates を含む）。

./WCGAdmin start コマンドを使用して Websense Security Gateway を起動するたびに、データベース ダウンロードが開始されます。ダウンロードに失敗す

ると、ダウンロードに成功するまで、15 分ごとに新たなダウンロードが試みられます。

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。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、こ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ら、コマンド ラインから Websense Content Gateway を終了し、再起動しなければなりません。

- 終了するには、**/opt/WCG/WCGAdmin stop** と入力します。
- 再起動するには、**/opt/WCG/WCGAdmin start** と入力します。

スキャン オプション

[設定] > **[リアルタイム スキャン]** ページを使用して、リアルタイム オプションを有効にし、構成します。個々のスキャン オプションについて、以下の項で詳しく説明します。

- コンテンツの分類と脅威のスキャン、150 ページ
- ファイルのスキャン、151 ページ
- コンテンツのストリッピング、153 ページ

各オプションについて、少なくとも 2 つの選択肢があります:

- **[オフ]**。リアルタイム スキャンやブロックは行われません。このオプションは、追加のセキュリティを提供しません。
- **[推奨]** または **[オン]**。サイトがリアルタイム スキャンを行うように構成されている場合、この設定は最善のパフォーマンスを提供します。2 つの要素に基づいてスキャンが行われます:
  - **[設定]** > **[リアルタイム スキャン]** > **[例外]** タブの [常にスキャンする] リストと [スキャンしない] リスト (スキャンの調整、154 ページを参照)。
  - Websense ソフトウェアが、サイトがダイナミック コンテンツを含んでいると認識したかどうか。ダイナミック コンテンツを含んでいるというフラグが付けられたサイトは、スキャンされます。ダイナミック コンテンツを含んでいるサイトを識別するマーカーは、ユーザが設定できません。

    ダイナミック コンテンツを含むサイトで [スキャンしない] リストに含まれているものは、スキャンされません。
- **[すべて]** すべての要求された Web ページがスキャンされます。唯一の例外は、[スキャンしない] リストに含まれているサイトです。

このオプションは最高のセキュリティを提供しますが、システム パフォーマンスがかなり遅くなる場合があります。

警告

[スキャンしない] 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。[スキャンしない] リストのサイトが危険なものであっても、リアルタイム オプションは悪意あるコードの分析や検出を行いません。

コンテンツの分類と脅威のスキャン

関連トピック:

- スキャン オプション、149 ページ
- ファイルのスキャン、151 ページ
- コンテンツのストリッピング、153 ページ
- スキャンの調整、154 ページ
- リアルタイム スキャン アクティビティのレポート、156 ページ

Web コンテンツの変化は急速です。統計は、Web コンテンツのかなり多くがダイナミックであることを示しています。さらに、インターネットには、ソーシャル ネットワーキング サイトに見られるように、多くのユーザが生成したコンテンツがあります。これらは、企業の Web サイトを管理しているようなコンテンツおよびスタイルのガイドラインに従っていません。

[コンテンツの分類] が有効になっていると、選択したサイトはリアルタイムで分類され、結果のカテゴリが Websense フィルタリング ソフトウェアに転送され、アクティブなポリシーに基づいてブロックまたは許可されます。

重要

リアルタイム スキャン アクティビティのレポートの生成を予定している場合は、[完全な URL によるログ記録] を有効にします (完全 URL によるログ記録の設定、328 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 の設定、320 ページを参照)、[コンテンツの分類] 機能によって分類された URL は、マスタ データベースに含めるために転送されます。

サブスクリプションに Websense Security Gateway が含まれている場合は、セキュリティの脅威についてサイトをスキャンするように指定できます。

[設定] > **[リアルタイム スキャン]** > **[共通オプション]** ページを使用して、[コンテンツの分類] および [コンテンツのスキャン] をいつ使用するかを指定します。

1. [コンテンツの分類] エリアで、**[オフ]** または **[オン]**（デフォルト）を選択し、スキャンを行うかどうかを決定します。スキャン オプション、149 ページを参照してください。

   カテゴリが決まると、構成済みの他のリアルタイム オプションが適用され、追加のセキュリティが提供されます。

2. (Websense Security Gateway) [コンテンツのスキャン] エリアで、**[オフ]**（デフォルト）、**[推奨]**、または **[すべて]** を選択して、スキャンのレベルを決定します。
3. 次のどちらかを実行します。
   - サイトを [スキャンしない] リストまたは [常にスキャンする] リストに追加するには、**[例外]** タブを選択します。スキャンの調整、154 ページを参照してください。
   - 他のリアルタイム オプションの設定を変更するには、**[共通オプション]** ページに移ります。ファイルのスキャン、151 ページおよびコンテンツのストリッピング、153 ページを参照してください。
4. 作業が終了したら、**[OK]** をクリックして、変更をキャッシュします。**[すべて保存]** をクリックするまで、変更は適用されません。

プレゼンテーション レポートは、脅威を含んでいるサイトへのアクセスの試みに関する詳細を提供します。Websense レポート機能の詳細については、プレゼンテーション レポート、98 ページを参照してください。

ファイルのスキャン

関連トピック：

- スキャン オプション、149 ページ
- コンテンツの分類と脅威のスキャン、150 ページ
- コンテンツのストリッピング、153 ページ
- スキャンの調整、154 ページ
- リアルタイム スキャン アクティビティのレポート、156 ページ

ファイルのスキャンは、ユーザがダウンロードしようとしている、またはリモートで開こうとしている着信アプリケーション ファイルのコンテンツを調べます。このリアルタイム オプションは、Websense フィルタリング ソフトウェアにカテゴリを返し、それに従ってファイルを許可またはブロックできるようにします。

最善のやり方は、すべての**実行可能**ファイル（たとえば **.exe** ファイルや **.dll** ファイル）をスキャンすることです。また、スキャンする追加のタイプを指定することができ、スキャンする最大サイズを設定することができます。

> **ご注意：**
> Windows 32 ビット ポータブル アプリケーション ファイルだけがスキャンされます。

[設定] > **[リアルタイム スキャン]** > **[共通オプション]** タブを使用して、ファイルのスキャンをいつ使用するかを指定します。

1. [ファイルのスキャン] エリアで、**[オフ]**、**[推奨]**（デフォルト）、または **[すべて]** を選択して、スキャンのレベルを決定します。スキャン オプション、149 ページを参照してください。
2. **[詳細設定]** をクリックします。
3. **[実行可能な内容を含むファイル タイプすべてをスキャン]** がデフォルトで選択されています。スキャンする個々のファイル拡張子のリストを指定したい場合は、このチェックボックスをオフにします。
4. スキャンする追加のファイル タイプを指定するには、ファイル拡張子（たとえば、**ppt** や **wmv**）を入力し、続いて **[追加]** をクリックします。ファイル拡張子には、英数字、アンダースコア（_）、ダッシュ（-）しか含むことはできません。拡張子の前のドットは、含めません。

   [選択されたファイル拡張子] リストからファイル拡張子を削除するには、その拡張子を選択し、**[削除]** をクリックします。
5. [オプション] の下に、スキャンするファイルの最大サイズを入力します（デフォルトは 10 MB）。**[カスタム]** を選択し、4096 MB (4 GB) までのサイズを入力します。指定したサイズより大きなファイルは、スキャンされません。
6. 次のどちらかを実行します。
   - サイトを [スキャンしない] リストまたは [常にスキャンする] リストに追加するには、**[例外]** タブを選択します。スキャンの調整、154 ページを参照してください。
   - 他のリアルタイム オプションの設定を変更するには、**[共通オプション]** タブに移ります。コンテンツの分類と脅威のスキャン、150 ページ および コンテンツのストリッピング、153 ページ を参照してください。
7. 作業が終了したら、**[OK]** をクリックして、変更をキャッシュします。**[すべて保存]** 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。Websense レポート機能の詳細については、プレゼンテーション レポート、98 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、196 ページを参照してください。

コンテンツのストリッピング

関連トピック：

- スキャン オプション、149 ページ
- コンテンツの分類と脅威のスキャン、150 ページ
- ファイルのスキャン、151 ページ
- スキャンの調整、154 ページ
- リアルタイム スキャン アクティビティのレポート、156 ページ

システムへの脅威が、Web 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。システムの完全性を保全する 1 つの方法は、そのようなコンテンツが決して持ち込まれないようにすることです。

Websense リアルタイム 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 Web 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になっていると、ダイナミック コンテンツを含んでいるというフラグの付いたサイト、または [常にスキャンする] リストに含まれているサイトから、指定されたスクリプト言語によるすべてのコンテンツが除去されます (スキャン オプション、149 ページを参照)。

コンテンツの削除は、リアルタイム オプションによってサイトが分類され、Websense フィルタリング ソフトウェア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。

重要
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にするか、サイトを [スキャンしない] 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。

[設定] > [リアルタイム スキャン] > [共通オプション] タブを使用して、ダイナミック コンテンツを含むサイトからいつコンテンツをストリップするかを指定します。

1. [コンテンツのストリッピング] エリアで、着信 Web ページから削除する必要があるアクティブ コンテンツのタイプを選択します。

2. 他のリアルタイム オプションの設定の変更については、以下を参照してください:
   - コンテンツの分類と脅威のスキャン、150 ページ
   - ファイルのスキャン、151 ページ.
3. 作業が終了したら、**[OK]** をクリックして、変更をキャッシュします。**[すべて保存]** をクリックするまで、変更は適用されません。

いずれかの選択されている言語のコンテンツ ストリッピングを無効にするには、関連するチェックボックスをオフにします。

スキャンの調整

関連トピック:

- スキャン オプション、149 ページ
- コンテンツの分類と脅威のスキャン、150 ページ
- ファイルのスキャン、151 ページ
- コンテンツのストリッピング、153 ページ

[常にスキャンする] リストおよび [スキャンしない] リストを使用して、[推奨] および [すべて] スキャン オプションの動作をカスタマイズします。

- リアルタイム オプションが [推奨] または [オン] に設定されている場合には、ダイナミック コンテンツを含むサイトおよび [常にスキャンする] リストに含まれるサイトはスキャンされます (スキャン オプション、149 ページを参照)。[スキャンしない] リストに含まれるサイトは、無視されます。
- リアルタイム オプションが [すべて] に設定されている場合には、[スキャンしない] リストに含まれるサイトは無視されます。これによって、パフォーマンスを改善できます。

[スキャンしない] 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 はそのサイトをスキャンしてセキュリティ問題を捕捉することができません。

[設定] > [リアルタイム スキャン] > [例外] ページを使用して、[常にスキャンする] リストおよび [スキャンしない] リストに追加し編集します。

[常にスキャンする] リストまたは [スキャンしない] リストにサイトを追加するには、以下のようにします:

1. **[URL]** ボックスにサイト名を入力します。

   ホスト名のみを入力します (たとえば、**thissite.com**)。完全な URL を入力する必要はありません。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、区別されるエントリです。

   一度に複数のホスト名を入力できます。

2. **[オプション]** 欄で、入力したすべてのサイトにどのリアルタイム オプションを適用するかを選択します。1 つまたは複数のオプションを選択できます。**[セキュリティの脅威]** が対象とするのは、コンテンツのスキャンだけで、ファイルのスキャンは対象になりません。ファイルのスキャンは、[常にスキャンする] リストおよび [スキャンしない] リストの影響を受けません。

   異なるサイトに異なるオプションを適用するには、サイトを別個に入力します。
3. **[常にスキャンするに追加]** または **[スキャンしないに追加]** を選択します。

   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、同じサイトを、脅威に関して常にスキャンし、コンテンツのストリッピングに関してスキャンしないように指定することはできません。

   - サイトが表示されるリストを変更するには、まずサイトを選択し、続いて右向き矢印 (>) ボタンおよび左向き矢印 (<) ボタンを使用してサイトを新しいリストに移動させます。
   - どちらかのリストからサイトを削除するには、サイトを選択し、つづいて **[削除]** をクリックします。
4. 作業が終了したら、**[OK]** をクリックして、変更をキャッシュします。**[すべて保存]** 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 オプションを変更するには、以下のようにします :

1. [常にスキャンする] リストまたは [スキャンしない] リストのサイトを選択し、続いて **[編集]** をクリックします。
2. [ルールの編集] ボックスで、そのホスト名についての新しいオプションを選択します :
   - **[変更なし]** は、現在の設定を維持します。
   - **[オン]** は、指定されているオプション (たとえば、コンテンツの分類) についてコンテンツをスキャンすることを指示します。
   - **[オフ]** は、指定されているオプションについてスキャンを行わないことを指示します。オプションをオフにすると、パフォーマンスは改善されますが、セキュリティが危険にさらされる可能性があります。
3. 変更を終了したら、[ルールの編集] ボックスの **[OK]** をクリックして [例外] タブに戻ります。
4. 変更をキャッシュするために、再度 **[OK]** をクリックします。**[すべて保存]** をクリックするまで、変更は適用されません。

リアルタイム スキャン アクティビティのレポート

関連トピック：

- スキャン オプション、149 ページ
- コンテンツの分類と脅威のスキャン、150 ページ
- ファイルのスキャン、151 ページ
- コンテンツのストリッピング、153 ページ

サブスクリプションにリアルタイム スキャン機能が含まれている場合、プレゼンテーション レポートや調査レポートを使用してこれらの機能の効果を分析することができます。

[プレゼンテーション レポート] ページで、[リアルタイム セキュリティの脅威] という名前のレポートのグループが使用可能です。これらのレポートは、特に脅威に関連するアクティビティに重点を置いています。すべてのプレゼンテーション レポートと同じように、セキュリティの脅威レポートをコピーし、レポート フィルタを編集してそのコピーからレポートを生成する際に、含める情報を調整することができます。

一部のセキュリティの脅威レポートには、[脅威 ID] 欄が含まれています。個々の脅威 ID をクリックすると、識別された脅威のタイプについて説明した Websense Secirity Labs ページを開くことができます。

さらに、他のプレゼンテーション レポートには、リアルタイム スキャン アクティビティや標準フィルタリング アクティビティに関する情報が含まれています。事前定義されたレポートをコピーし、そのフィルタを編集して、特にリアルタイム スキャン アクティビティ用のレポートを作成できます。

重要

[完全な URL によるログ記録] を有効にして、リアルタイム スキャン アクティビティのレポートが意味のあるものになることを確保します（完全 URL によるログ記録の設定、328 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。

たとえば、[レポート カタログ] の [インターネット アクティビティ] グループの中の [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 URL の詳細なリストが示されます。リアルタイム スキャンに特有のレポートを作成するには、[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 フィルタを編集します。[アクション] タブで、リアルタイム スキャンに関連する許可およびブロック アクションのみを選択します。[オプション] タブで、レポート カタログのタイトルおよびレポート名を変更し、これがリアルタイム スキャン 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、名前とタイトルを、「リアルタイム : カテゴリ別完全な URL の詳細」に変更することができます。

また、調査レポートを使用して、リアルタイム スキャン アクティビティの状況を把握できます。

1. **[インターネット使用状況]** ドロップダウンリストで [アクション] を選択します。
2. 結果のレポートの中で、リアルタイム アクション、たとえば [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させます。
3. 必要なドリルダウン オプションを、たとえば [カテゴリ] または [ユーザ] をクリックします。
4. [ヒット件数] 値またはいずれかの行のバーをクリックすると、関連する詳細が表示されます。
5. ページの上部の **[レポートの変更]** をクリックして、[完全 URL] 欄をレポートに追加します。

   すべての調査レポート機能の使用に関する詳細については、調査レポート、118 ページを参照してください。

リアルタイム スキャンをログ記録する方法

リアルタイム スキャン オプションを使用する際には、標準 Web フィルタリング アクティビティとリアルタイム スキャン アクティビティでは、ログ記録を行う方法に違いがあることに留意してください。

標準 Web フィルタリングの場合は、ログ データベースのサイズを小さくする複数のオプションがあります。

- **[アクセス件数]** を有効にすると、要求された Web サイトごとに 1 つのレコードだけがログ記録されます。ログ キャッシュ ファイルの設定、317 ページを参照してください。
- **[集約]** を有効にすると、特定の共通要素を持つ複数の要求が 1 つのログ記録に結合されます。集約オプションの設定、318 ページを参照してください。
- **[完全な URL によるログ記録]** を無効にすると、各要求についてドメイン名 (www.domain.com) のみがログ記録され、ドメインの特定ページへのパス (/products/productA) は記録されません。完全 URL によるログ記録の設定、328 ページを参照してください。
- **[選択可能なカテゴリのログ記録]** を有効にすると、ログ記録を、組織にとって決定的に重要な選択されたカテゴリに限定します。ログ記録のための Filtering Service 設定、310 ページを参照してください。

しかし、リアルタイム スキャン機能は、これらの設定では部分的にしか限定されません。リアルタイム スキャンによって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。

- **[Web フィルタ記録]** 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。すべての Web フィルタ レポートに使用可能です。
- **[リアルタイム記録]** 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記録され、すべてのカテゴリへの要求が記録され、レコードは集約されません。サイトがブロックされたか、または許可されたかに関係なく、リアルタイム スキャンの結果としてリアルタイム レコードが生成されます。リアルタイム記録では、[完全な URL によるログ記録] に関する設定のみが尊重されます。

いずれかのログ データベースのサイズ削減オプションを有効にした場合、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、リアルタイム レポートで報告される数が標準フィルタリング 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、リアルタイム 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フィルタリング レポートでは 1 件のアクセスとして表示されますが、リアルタイム レポートでは複数のヒットとして表示される可能性があります。

標準フィルタリングとリアルタイム フィルタリング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 サイズ削減設定を**無効**にします。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、ログ データベース 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、305 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、98 ページおよび調査レポート、118 ページを参照してください。

8 リモート クライアントのフィルタ

関連トピック：

- リモート フィルタリングの動作、160 ページ
- Remote Filtering 設定の構成、166 ページ

多くの組織が、時どきネットワークの外部でノート パソコンを使用するユーザを抱えています。Microsoft Windows オペレーティングシステムを使用しているリモート ユーザに対しては、Websense Web Security と Websense Web Filter の両方で使用可能なオプション機能である Websense Remote Filtering を実施することにより、インターネット要求をフィルタできます。

Remote Filtering は、HTTP、SSL、および FTP トラフィックをモニタし、ユーザがリモート コンピュータにログオンした方法によって、個々のユーザもしくはグループに割り当てられたポリシー、またはデフォルト ポリシーを適用します。Remote Filtering は、コンピュータまたはネットワーク範囲に割り当てられたポリシーに基づくフィルタは行いません。詳細は、リモート ユーザの識別、163 ページを参照してください。

リモート クライアントに対しては、帯域幅に基づいたフィルタリングはサポートされていません（Bandwidth Optimizer による帯域幅の管理、194 ページを参照）。リモート クライアントが生成する帯域幅は、帯域幅測定値およびレポートには含まれません。

FTP 要求および HTTPS のような SSL 要求のリモート フィルタリングは、ブロックのみ、または許可のみが可能です。たとえば、リモート ユーザが割り当て時間アクションもしく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 サイトを要求した場合は、Remote Filtering Client によってこのサイトはブロックされます。これらのコンピュータがネットワークの内部からアクセスする場合は、割り当て時間および確認フィルタリング アクションは正常に適用されます。

Remote Filtering を実行するには、以下のコンポーネントをインストールしなければなりません：

- Remote Filtering Server は、一番外側のファイアウォールの内側に置かれ、リモート コンピュータがそれと通信することが許可されなければなりません。一般に、ネットワークの非武装地帯あるいは DMZ の中の、ネットワークの残りの部分を保護するファイアウォールの外側にインストール

されます。最大 3 つの Remote Filtering Server をインストールして、フェイルオーバー機能を提供することができます。

- Remote Filtering Client は、Windows オペレーティングシステムを実行し、ネットワークの外部で使用される各コンピュータにインストールされなければなりません。

> **ご注意：**
> 『配備ガイド』の推奨事項に慎重に従って、これらのコンピュータを配置してください。これらのインストールの手順については、『インストール ガイド』を参照してください。
>
> Websense ソフトウェアをスタンドアロン モードで使用する場合（統合製品を使用しない場合）は、Network Agent が Remote Filtering Server コンピュータをモニタ**しない**ように設定します（グローバル設定、346 ページを参照）。

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。

リモート フィルタリングの動作

関連トピック：

- ネットワークの内部、161 ページ
- ネットワークの外部、162 ページ
- リモート ユーザの識別、163 ページ
- サーバー通信が失敗した場合、164 ページ
- 仮想プライベート ネットワーク (VPN)、165 ページ
- Remote Filtering 設定の構成、166 ページ

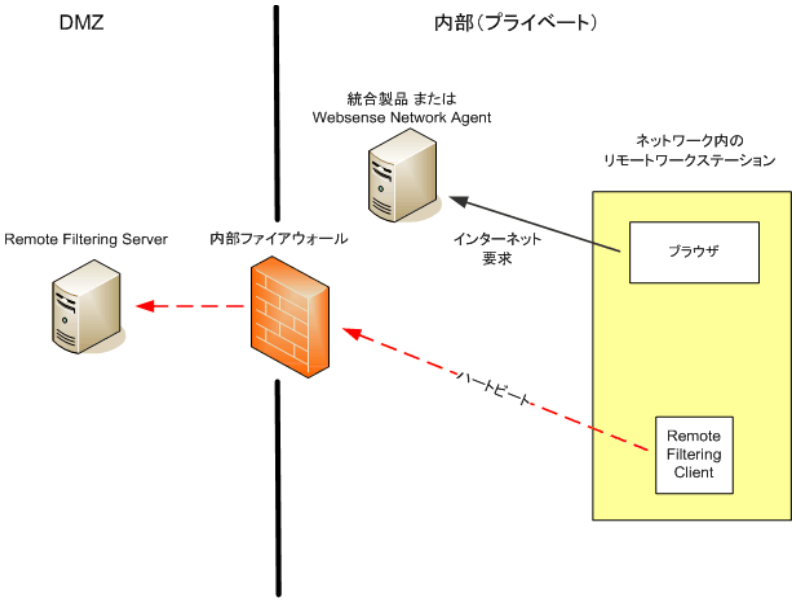
リモート コンピュータが HTTP、SSL または FTP 要求を行うと、リモート コンピュータ上の Remote Filtering Client が Remote Filtering Server と通信します。Remote Filtering Server は、Websense Filtering Service と通信して、どのアクションを適用するかを決定します。次に、Remote Filtering Server は、Remote Filtering Client に応答し、サイトを許可するか、または該当するブロック メッセージを送信します。

Remote Filtering Client を実行しているコンピュータ上のブラウザが HTTP、SSL または FTP による要求を行うと、Remote Filtering Client は、その要求について Remote Filtering Server に照会するかどうか決定しなければなりません。この決定は、そのコンピュータが所在する、ネットワークとの相対的な位置によって制御されます。

ネットワークの内部

関連トピック：
- リモート フィルタリングの動作、160 ページ
- ネットワークの外部、162 ページ
- リモート ユーザの識別、163 ページ
- サーバー通信が失敗した場合、164 ページ
- 仮想プライベート ネットワーク (VPN)、165 ページ
- Remote Filtering 設定の構成、166 ページ

ネットワークの内部でコンピュータが起動すると、Remote Filtering Client は DMZ の中の Remote Filtering Server に**ハートビート**の送信を試みます。ハートビート ポートは内部ファイアウォール上に開かれているので、ハートビートは成功します。

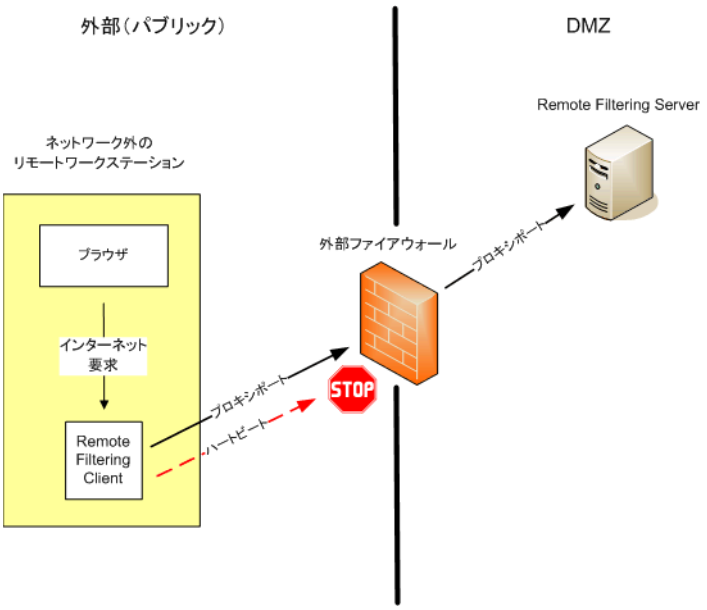


この場合は、Remote Filtering Client は受動的になり、Remote Filtering Server へのインターネット要求についての照会は行いません。その代わり、これらの要求は統合製品（たとえば、Cisco Pix、Microsoft ISA Server）または Websense Network Agent に直接受け渡されます。この要求は、他の内部要求と同じようにフィルタされます。

ネットワークの外部

関連トピック：
- リモート フィルタリングの動作、160 ページ
- ネットワークの内部、161 ページ
- リモート ユーザの識別、163 ページ
- サーバー通信が失敗した場合、164 ページ
- 仮想プライベート ネットワーク (VPN)、165 ページ
- Remote Filtering 設定の構成、166 ページ

ネットワークの外部でコンピュータが起動すると、Remote Filtering Client は Remote Filtering Server にハートビートの送信を試みます。ハートビート ポートは外部ファイアウォールでブロックされているので、ハートビートは成功しません。



このハートビートの失敗によって、Remote Filtering Client は、HTTP、SSL、または FTP 要求ごとに、設定されているポート（デフォルトでは 80）を介して、DMZ の中の Remote Filtering Server に宛てて照会を送信することになります。続いて、Remote Filtering Server は、ネットワーク内部の Websense Filtering Service にフィルタリング要求を転送します。Filtering Service は要求を評価し、応答を Remote Filtering Server に送信します。続いて、この応答がリモート コンピュータに送信されます。サイトがブロックされた場合は、Remote Filtering Client は該当するブロック ページを要求し、受信し、ブロック ページがユーザに対して表示されます。

Remote Filtering Client は、Remote Filtering Server からの応答を受信するまで、フィルタされる各要求を表示します。受信した応答に応じて、Remote Filtering Client は、サイトを許可するか、またはブロック ページを表示します。

ログ ファイルは、ネットワークへの参加および退出、フェイル オープンやフェイル クローズ状態、およびクライアントの再起動などの、リモート フィルタリング アクティビティを追跡します。Remote Filtering Client は、最初に起動したときに、ログ ファイルを作成します。ログ ファイルの存在およびサイズは、お客様が管理します。Remote Filtering 設定の構成、166 ページを参照してください。

リモート ユーザの識別

関連トピック：

- リモート フィルタリングの動作、160 ページ
- ネットワークの内部、161 ページ
- ネットワークの外部、162 ページ
- サーバー通信が失敗した場合、164 ページ
- 仮想プライベート ネットワーク (VPN)、165 ページ
- Remote Filtering 設定の構成、166 ページ

ユーザがリモート コンピュータにログオンした方法によって、どのポリシーを実施するかが決まります。

ユーザが、キャッシュされたドメイン資格情報（ネットワーク ディレクトリ ログオン情報）を使用してログオンした場合は、Websense Filtering Service はユーザ名を解決することができ、該当するユーザおよびグループに基づいたポリシーをリモート コンピュータに適用します。さらに、インターネット アクティビティは、ネットワーク ユーザ名の下にログ記録されます。

ユーザが、コンピュータにとってローカルなユーザ アカウントを使用してログオンした場合は、Filtering Service はユーザ名を解決できず、代わりにデフォルト ポリシーを適用します。インターネット アクティビティは、ローカル ユーザ名の下にログ記録されます。Remote Filtering は、コンピュータまたはネットワーク範囲に割り当てられたポリシーに基づくフィルタは行いません。

ご注意：
リモート ユーザは、ここで説明したように、必ずログオン資格情報に従ってフィルタされます。選択認証設定は、これらのユーザには適用されません。

サーバー通信が失敗した場合

関連トピック：
- リモート フィルタリングの動作、160 ページ
- ネットワークの内部、161 ページ
- ネットワークの外部、162 ページ
- リモート ユーザの識別、163 ページ
- 仮想プライベート ネットワーク (VPN)、165 ページ
- Remote Filtering 設定の構成、166 ページ

ネットワークの外部の Remote Filtering Client がネットワークの DMZ の中の Remote Filtering Server との通信に成功したとき、フィルタリングが行われます。しかし、この通信がうまく行かない場合があります。

Remote Filtering Client が Remote Filtering Server と通信できない場合に、Remote Filtering Client がとる処置は、設定可能です。デフォルトでは、Remote Filtering Client は**フェイル オープン**設定を使用します。この設定では、これらのコンポーネント間の通信が確立できなかった場合にはすべての HTTP、SSL、および FTP 要求が許可されます。Remote Filtering Client は、引き続き Remote Filtering Server との連絡を試みます。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**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、Remote Filtering Client が Remote Filtering Server に接続するまでは、フィルタリングは行われません (すべての要求が許可されます)。この場合は、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)。

ご注意：
何らかの理由で Remote Filtering Server が Websense 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、フィルタリングは必ずフェイル オープンになります。

このタイムアウト期間は、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、そのセッション中は Web アクセスを確立することはできません。このような場合には、ユーザはコンピュータを再起動して、タイムアウト期間を再開する必要があります。

フェイル オープン / フェイル クローズ設定の変更、およびタイムアウト値の変更については、Remote Filtering 設定の構成、166 ページを参照してください。

仮想プライベート ネットワーク (VPN)

関連トピック :

- リモート フィルタリングの動作、160 ページ
- ネットワークの内部、161 ページ
- ネットワークの外部、162 ページ
- リモート ユーザの識別、163 ページ
- サーバー通信が失敗した場合、164 ページ
- Remote Filtering 設定の構成、166 ページ

Websense Remote Filtering は、スプリット トンネル VPN を含む VPN 接続をサポートしています。リモート コンピュータが VPN (非スプリット トンネル) を介して内部ネットワークに接続すると、Remote Filtering Client は Remote Filtering Server にハートビートを送信することができます。その結果、Remote Filtering Client は受動的になり、リモート コンピュータからのすべての HTTP、SSL、および FTP 要求は、内部統合製品または Network Agent によって、他のネットワーク内のコンピュータの場合と同じようにフィルタされます。

リモート コンピュータがスプリット トンネル VPN クライアントを介して内部ネットワークに接続する場合は、Remote Filtering Client はそのことを検出し、Remote Filtering Server にハートビートを送信しません。Remote Filtering Client は、外部で動作していることを想定して、Remote Filtering Server に要求を提出してフィルタリングを求めます。

Websense ソフトウェアは、以下の VPN クライアントに対するスプリット トンネルをサポートしています :

- Checkpoint SecureClient
- Cisco
- Juniper/Netscreen
- Microsoft PPTP
- Nokia
- Nortel
- SonicWALL

Remote Filtering 設定の構成

関連トピック：

- リモート フィルタリングの動作、160 ページ
- ネットワークの内部、161 ページ
- ネットワークの外部、162 ページ
- リモート ユーザの識別、163 ページ
- サーバー通信が失敗した場合、164 ページ
- 仮想プライベート ネットワーク (VPN)、165 ページ

条件無し優先管理者は、[**設定**] > [**一般**] > [**Remote Filtering**] ページを使用して、このインストレーションに関連付けられたすべての Remote Filtering Client に影響を与えるオプションを構成することができます。

Remote Filtering の動作の詳細については、リモート フィルタリングの動作、160 ページを参照してください。

1. [**フェイル クローズ**] チェックボックスをオンにすると、Remote Filtering Client コンピュータが Remote Filtering Server と通信しない限り、Remote Filtering Client のすべてのインターネット アクセスはブロックされます。

   デフォルトでは、このチェックボックスはオンになっていません。つまり、コンピュータが Remote Filtering Server と通信できない場合、リモート ユーザはフィルタされずにインターネットにアクセスできます。
2. [フェイル クローズ] オプションをオンにしたら、[**フェイル クローズまでのタイムアウト**] フィールドを使用して最大 60 分までの分単位の時間 (デフォルトは 15 分) を選択するか、または [**タイムアウトなし**] を選択します。

   タイムアウト時間中は、すべての HTTP、SSL、および FTP 要求が許可されます。

   タイムアウト時間中に Remote Filtering Client が Remote Filtering Server と通信できないと、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)。

   [**タイムアウトなし**] を選択すると、ユーザがホテルやその他の有料プロバイダからのインターネット接続を確立する前に、リモート コンピュータをロックアウトできます。さらに、Remote Filtering Client は、Remote Filtering Server との通信を試行し続けます。

   警告

   Websense, Inc. は、[**タイムアウトなし**] を選択することや、非常に短いタイムアウト時間を設定することは、推奨しません。
3. [**ローカル ログ キャッシュの最大サイズ**] (MB 単位、最大 10 MB) を選択します。[**ログなし**] を選択すると、ログ記録が無効になります。

これによって、リモート コンピュータが最初に Remote Filtering Server から切断されたときにリモート コンピュータが作成するログ ファイルのサイズと存在を制御します。このログ ファイルは、以下のイベントを追跡します :

- コンピュータのネットワークからの切断
- コンピュータのネットワークへの再接続
- Remote Filtering Client の再起動
- フェイル オープン条件の発生
- フェイル クローズ条件の発生
- Remote Filtering Client のポリシー アップデートの受信

コンピュータは最後の 2 つのログを保持します。これらのログは、リモート フィルタリングに関する接続問題やその他の問題のトラブルシューティングに使用できます。

9 フィルタリング ポリシーの調整

インターネット利用のフィルタリングのもっとも単純な方法では、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、Websense ソフトウェアは、この基本的なフィルタリングをはるかに超えて、ユーザがインターネット使用状況を管理するために必要とする詳細レベルのフィルタリングを可能にす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（ユーザのアクセスを指定したサイトのリストに制限、170 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、177 ページを参照）。
- **URL を再分類し**、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（URL の再分類、186 ページを参照）。
- **フィルタなし URL** を定義し、サイトがアクティブ カテゴリ フィルタでブロックされたカテゴリに割り当てられている場合でも、ユーザがそのサイトにアクセスできるようにする（フィルタなし URL の定義、185 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のアクセスをブロックする。
- **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（キーワードに基づくフィルタリング、182 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、196 ページを参照）。

ユーザのアクセスを指定したサイトのリストに制限

関連トピック：

- 制限付きアクセス フィルタとフィルタリングの優先順位、170 ページ
- 制限付きアクセス フィルタの作成、172 ページ
- 制限付きアクセス フィルタの編集、172 ページ

制限付きアクセス フィルタは、インターネット アクセスをフィルタリングするための非常に正確な方法です。それぞれの制限付きアクセス フィルタは、個別の Web サイトのリストです。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。

重要

制限付きアクセス フィルタが有効になっているとき、Websense ソフトウェアは、要求されたサイトがフィルタ内にあるかどうかだけを調べます。他のチェックは実行されません。

したがって、フィルタによって許可されたサイトが不正コードに感染した場合でも、サイトのマスタ データベースまたは Real-Time Scanning の分類に関係なく、そのサイトのユーザ要求は許可されます。

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 フィルタとフィルタリングの優先順位

場合によっては、1 人のユーザに複数のフィルタリング 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。また、1 つの URL が制限付きアクセス フィルタに含まれ、同時にフィルタなし URL として定義される場合があります。

1 人のユーザに複数のグループ ポリシーが適用されるとき、[**より厳密な制限でブロックをする**] の設定（フィルタリング順序、80 ページを参照）によって、ユーザをフィルタリングする方法が決まります。デフォルトでは、この設定はオフにされています。

Websense ソフトウェアは、どのフィルタリング設定がフィルタ レベルで、より緩やかであるかを判断します。ユーザが複数のポリシーによってフィルタリングされ、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」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。

[**より厳密な制限でブロックをする**] 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。

[**より厳密な制限でブロックをする**] 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、[**より厳密な制限でブロックする**] の設定のフィルタリングへの影響を要約しています。

	[より厳密な制限でブロックする] がオフ	[より厳密な制限でブロックする] 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 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 + フィルタなし URL	フィルタなし URL（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 フィルタの作成

関連トピック：

- フィルタに関する作業、47 ページ
- ユーザのアクセスを指定したサイトのリストに制限、170 ページ
- 制限付きアクセス フィルタの編集、172 ページ

[制限付きアクセス フィルタの追加] ページ（**[フィルタ]** または **[ポリシーを編集]** 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. 一意的な**フィルタ名**を入力します。名前は長さが 1 ～ 50 字で、以下の文字を含めることはできません：

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

   フィルタ名にスペース、ダッシュ、およびアポストロフを含めることができます。
2. フィルタの簡単な**説明**を入力します。この説明は、[フィルタ] ページの [制限付きアクセス フィルタ] 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。

   フィルタ名での文字に関する制限がこの説明にも適用されますが、例外として、説明にはピリオド (.) とカンマ (,) を含めることができます。
3. 新しいフィルタを表示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、[フィルタ] ページに戻るには、**[キャンセル]** 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 **[ポリシー管理]** > **[フィルタ]** > **[制限付きアクセス フィルタ]** 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

関連トピック：

- ユーザのアクセスを指定したサイトのリストに制限、170 ページ
- 制限付きアクセス フィルタとフィルタリングの優先順位、170 ページ
- 制限付きアクセス フィルタの作成、172 ページ
- ポリシーの編集、77 ページ

制限付きアクセス フィルタは Web サイト（URL または IP アドレス）と正規表現から成るリストで、ユーザがアクセスできる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 フィルタが有効になっているとき、Websense ソフトウェアは、要求されたサイトがフィルタ内にあるかどうかだけを調べます。他のチェックは実行されません。

したがって、フィルタによって許可されたサイトが不正コードに感染した場合でも、サイトのマスタ データベースまたは Real-Time Scanning の分類に関係なく、そのサイトのユーザ要求は許可されます。

[ポリシーの管理] > [フィルタ] > [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、どのサイト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、**[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. **[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、**[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. [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。1 行に 1 件の URL または IP アドレスを入力します。

   接頭語 「HTTP://」 を含める必要はありません。

   サイトがそのマスタ データベースのカテゴリに従ってフィルタリングされるとき、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。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。
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、**[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、[**テスト**] をクリックします。
- フィルタリングでの正規表現の使用の詳細については、正規表現の使用、199 ページを参照してください。

6. [**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、[**編集**] 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、[**削除**] をクリックします。
7. フィルタの編集が完了したら、[OK] をクリックして変更をキャッシュし、[フィルタ] ページに戻ります。[**すべて保存**] をクリックするまで、変更は適用されません。

ポリシーを編集ページからのサイトの追加

関連トピック :

- ユーザのアクセスを指定したサイトのリストに制限、170 ページ
- 制限付きアクセス フィルタとフィルタリングの優先順位、170 ページ
- 制限付きアクセス フィルタの作成、172 ページ
- ポリシーの編集、77 ページ

制限付きアクセス フィルタにサイトを追加するには、[**ポリシー**] > [**ポリシーを編集**] > [**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、[ポリシーを編集] ページに戻ります。変更をキャッシュするために、[ポリシーを変更] ページでも [OK] をクリックする必要があります。[**すべて保存**] 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

関連トピック：

- カテゴリ フィルタの作成、48 ページ
- プロトコル フィルタの作成、51 ページ
- 制限付きアクセス フィルタの作成、172 ページ
- ポリシーの作成、76 ページ

優先管理者は、[**フィルタ**] > [**ロールにフィルタをコピー**] ページおよび [**ポリシー**] > [**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使用して、管理対象のクライアントをフィルタリングできます。

- ターゲット ロールには、「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。
- 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 カテゴリのフィルタリング アクションを許可に設定します。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. [ロールにフィルタをコピー] または [ロールにポリシーをコピー] 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. [**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。

[**すべて保存**] 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、ロール内の指定済み管理者が次回 Websense Manager 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選択して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

[**ポリシー管理**] > [**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調整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 4 つのボタンは、下記のタスクに関連付けられています。

カテゴリを編集	• URL を再分類します（特定のサイトのフィルタリングの再定義、184 ページを参照）。たとえば、「ショッピング」カテゴリがインターネット フィルタリング 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またはパートナー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、180 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(キーワードに基づくフィルタリング、182 ページを参照）。URL が特定の文字列を含むサイトへのアクセスを再分類し、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、199 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。
プロトコルの編集	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、191 ページおよびカスタム プロトコルの編集、189 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。

ファイル タイプ	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、196 ページを参照）。
フィルタなし URL	特定のサイトが、ブロックされるカテゴリに属している場合でも、すべてのクライアントに対して許可されるように定義します（フィルタなし URL の定義、185 ページを参照）。URL をこのリストに追加しても、「すべてブロック」カテゴリ フィルタまたは制限付きアクセス フィルタは上書きされません。

カテゴリの使用

関連トピック：

- カテゴリとその属性の編集、177 ページ
- カスタム カテゴリの作成、180 ページ
- キーワードに基づくフィルタリング、182 ページ
- 特定のサイトのフィルタリングの再定義、184 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フィルタリングしたり、マスタ データベース内の個別のサイトのフィルタリング方法を変更するための種々の方法を利用できます。

- より詳細なフィルタリング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。
- **再分類された 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再分類するために**キーワード**を定義する。

カテゴリとその属性の編集

関連トピック：

- カスタム カテゴリの作成、180 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、179 ページ
- グローバル カテゴリのフィルタリングの変更、179 ページ
- キーワードに基づくフィルタリング、182 ページ
- 特定のサイトのフィルタリングの再定義、184 ページ

[ポリシーの管理] > **[フィルタ コンポーネント]** > **[カテゴリの編集]** ページを使用して、カスタム カテゴリ、再分類された URL、キーワードを作成および変更します。

既存のカテゴリ (Websense 定義およびカスタムの両方) が、コンテンツペインの左側にリストされます。カテゴリに関連付けられた現在のカスタム 設定を表示するか、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たすべてのカスタム URL、キーワード、および正規表現のリストを表示するには、ページの上部のツールバー内の **[すべてのカスタム URL/ キーワードを表示]** 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、179 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、**[追加]** をクリックし、次に、カスタム カテゴリの作成、180 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ためには、カテゴリを選択し、**[削除]** をクリックします。Websense 定義の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、**[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、180 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、**[アクションの優先設定]** をクリックします (グローバル カテゴリのフィルタリングの変更、179 ページを参照)。
- **[再分類された URL]** リストは、このカテゴリに割り当てられた再分類されたサイト (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、**[URL の追加]** をクリックします。その後の手順については、URL の再分類、186 ページ を参照してください。
  - 既存の再分類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、**[編集]** をクリックします。
- **[キーワード]** 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、**[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、キーワードに基づくフィルタリング、182 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、**[編集]** 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、**[詳細]** をクリックします。
  - 正規表現を定義するには、[式の追加] をクリックします (正規表現の使用、199 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、**[編集]** をクリックします。

- 再分類された 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、**[削除]** をクリックします。

[カテゴリを編集] 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、[フィルタ コンポーネント] ページに戻ります。**[すべて保存]** 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

[フィルタ コンポーネント] > [カテゴリを編集] > [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、**[削除]** をクリックします。

[カテゴリを編集] ページに戻るには、**[閉じる]** をクリックします。[すべてのカスタム URL/ キーワードを表示] ページのいずれかの項目を削除した場合、[カテゴリを編集] ページで **[OK]** をクリックして変更をキャッシュします。**[すべて保存]** をクリックするまで、変更は適用されません。

グローバル カテゴリのフィルタリングの変更

[フィルタ コンポーネント] > [カテゴリの編集] > [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フィルタリング設定を変更する前に、**[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、フィルタリング アクション、43 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 **[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、キーワードに基づくフィルタリング、182 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、196 ページ を参照してください。

4. **[高度なフィルタリング]**で、Bandwidth Optimizer を使用して 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、194 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、[カテゴリを編集] ページに戻ります (カテゴリとその属性の編集、177 ページを参照)。[カテゴリを編集] 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

[フィルタ コンポーネント] > [カテゴリを編集] > [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、**[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、**[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。

  フィルタ名での文字に関する制限がこの説明にも適用されますが、例外として、説明にはピリオド (.) とカンマ (,) を含めることができます。

変更を完了したら、**[OK]** をクリックし、[カテゴリを編集] ページに戻ります。[カテゴリを編集] 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

関連トピック :

- カテゴリとその属性の編集、177 ページ
- キーワードに基づくフィルタリング、182 ページ
- 特定のサイトのフィルタリングの再定義、184 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 定義カテゴリのほかに、より詳細なフィルタリングおよびレポート作成のためにユーザ固有の**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。

[ポリシー管理] > **[フィルタ コンポーネント]** > **[カテゴリを編集]** > **[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。

   フィルタ名での文字に関する制限がこの説明にも適用されますが、例外として、説明にはピリオド (.) とカンマ (,) を含めることができます。

3. **[次に追加]** リストから親カテゴリを選択します。デフォルトでは、**[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、URL の再分類、186 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、キーワードに基づくフィルタリング、182 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 フィルタでこのプロトコルに適用するデフォルトのフィルタリング **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。

   > **ご注意**：
   > 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 カテゴリのフィルタリング アクションを [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、[カテゴリを編集] ページに戻ります。**[すべて保存]** 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 [カテゴリ] 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。

キーワードに基づくフィルタリング

関連トピック：

- URL の再分類、186 ページ
- Websense フィルタリング設定の構成、56 ページ
- カテゴリ フィルタの作成、48 ページ
- カテゴリ フィルタの編集、49 ページ
- カテゴリの使用、177 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サイト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（Websense フィルタリング設定の構成、56 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、183 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、49 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、URL にそのキーワードが含まれるサイトをブロックし、そのサイトを指定されたカテゴリに属しているサイトとしてログ記録します。このサイトは、そのカテゴリ内の他の URL が許可されている場合でもブロックされます。

たとえば、アクティブ カテゴリ フィルタで「スポーツ」カテゴリが許可されていて、バスケットボール サイトへのアクセスをブロックしたい場合、キーワード「nba」を「スポーツ」に関連付け、キーワード ブロックを有効にします。これにより以下の URL がブロックされ、「スポーツ」カテゴリに属しているサイトとしてログ記録されます。

- sports.espn.go.com/**nba**/
- moder**nba**kery.com
- moder**nba**biesandchildren.com
- fashio**nba**r.com

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**
> Websense Web Security を使用している場合、キーワードをいずれかの「より広範囲の危険性への対処」サブカテゴリに関連付けないようにしてください。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

関連トピック：

- カテゴリ フィルタの編集、49 ページ
- カテゴリの使用、177 ページ
- キーワードに基づくフィルタリング、182 ページ
- 正規表現の使用、199 ページ

キーワードは、URL に含まれる文字（語、句、頭字語など）から成る文字です。

[ポリシーの管理] > **[フィルタ コンポーネント]** > **[カテゴリの編集]** > **[キーワードの追加]** 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、**[キーワードの編集]** 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。
- Websense Web Security を使用している場合、キーワードをいずれかの「より広範囲の危険性への対処」サブカテゴリに関連付けないようにしてください。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、[カテゴリを編集] ページに戻ります。**[すべて保存]** 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. **[設定] > [フィルタリング]** ページでキーワード ブロックを有効にします（Websense フィルタリング設定の構成、56 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、49 ページを参照 ）。

特定のサイトのフィルタリングの再定義

関連トピック :

- カスタム カテゴリの作成、180 ページ
- キーワードに基づくフィルタリング、182 ページ
- フィルタなし URL の定義、185 ページ
- URL の再分類、186 ページ

カスタム URL を使って、以下の操作を行うことができます。

- Websense マスタ データベースにないサイトに対して、より詳細なフィルタリングを適用する。デフォルトでは、これらのサイトをフィルタリングするために、**「その他 ¥ 未分類」** カテゴリに適用されるアクションが使用されます。
- サイトをそのマスタ データベースのカテゴリと異なる方法でフィルタリングする。

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、そのカスタム 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。

カスタム URL には、フィルタなし URL と再分類された URL の 2 つのタイプがあります。

- フィルタなし URL は、「すべてブロック」カテゴリ フィルタまたは制限付きアクセス フィルタによって管理されていないすべてのユーザに対して許可されます（ フィルタなし URL の定義、185 ページを参照 ）。
- 再分類された URL は、そのマスタ データベースカテゴリから他の Websense 定義のカテゴリまたはカスタム カテゴリに移動されました（URL の再分類、186 ページを参照 ）。

  デフォルトでは再分類された 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。

サイトがそのマスタ データベースのカテゴリに従ってフィルタリングされるとき、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。カスタム URL の場合はそうではありません。サイトのフィルタリング方法を変更するには、その URL と IP アドレスの両方をカスタム URL として定義します。

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。

サイトが新しいドメインに移動され、HTTP リダイレクトを使ってユーザが新しい URL に転送される場合、新しい URL は自動的には転送元のサイトと同じ方法ではフィルタリングされません。サイトが新しいアドレスで適切にフィルタリングされるようにするためには、新しいカスタム URL を作成します。

フィルタなし URL の定義

関連トピック：

- カテゴリの使用、177 ページ
- 特定のサイトのフィルタリングの再定義、184 ページ
- URL の再分類、186 ページ

[ポリシー管理] > [フィルタ コンポーネント] > [フィルタなし URL] ページを使用して、「すべてブロック」カテゴリ フィルタまたは制限付きアクセス フィルタによって管理される場合を除きすべてのユーザがアクセスできるサイトのリストを定義します。

コンテンツペインの右側の **[許可されたサイト]** リストに、フィルタなしサイト（URL および IP アドレス）とユーザが定義した正規表現がリストされます（正規表現の使用、199 ページを参照）。各サイトはカテゴリに関連付けられています。

- URL をそのマスタ データベース カテゴリに関連付けるか、または再分類することができます。
- ユーザがフィルタなし URL へのアクセスを要求したとき、その要求はその URL が割り当てられているカテゴリで、許可されたカスタム URL としてログ記録されます。

フィルタなし URL を追加するには、以下の手順を実行します。

1. **[フィルタなし URL の定義]** で、URL または IP アドレスを 1 行に 1 件ずつ入力し、右向き矢印（>）をクリックします。

   Websense ソフトウェアは、カスタム URL をその同等の IP アドレスと照合しません。サイトの URL と IP アドレスの両方を許可するには、その両方を [フィルタなし URL] リストに追加します。

2. 複数のサイトに一致する正規表現を追加するには、[**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、その正規表現を [フィルタなし URL] リストに移動します。パターンが想定しているサイトと一致することを確認するには、[**テスト**] をクリックします。

   詳細については、正規表現の使用、199 ページを参照してください。

3. 完了したとき、[OK] をクリックして変更をキャッシュし、[カテゴリを編集] ページに戻ります。[**すべて保存**] 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 URL] リストからサイトを削除するには、URL、IP アドレス、または正規表現を選択し、[**削除**] をクリックします。

URL の再分類

関連トピック :

- カテゴリの使用、177 ページ
- 特定のサイトのフィルタリングの再定義、184 ページ
- フィルタなし URL の定義、185 ページ

[**ポリシーの管理**] > [**フィルタ コンポーネント**] > [**カテゴリの編集**] > [**URL の再カテゴリ**] 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。既存の再分類されたサイトの変更は、[**URL の編集**] ページで行います。

URL を再分類することによって、個別のサイトがフィルタリングおよびログ記録される方法を変更します。再分類されたサイトを追加するとき、以下の手順を実行します。

- URL またはアドレスを 1 行に 1 件ずつ入力します。
- 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再分類した場合、このサイトはユーザ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** を再分類した場合、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。

再分類したサイト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、[カテゴリを編集] ページに戻ります。[**すべて保存**] をクリックするまで、変更は適用されません。

再分類した URL を保存した後、右側のショートカットペインの [**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フィルタリング動作の確認、200 ページを参照してください。

プロトコルの使用

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。

ご注意：
プロトコルに基づいたフィルタリングを可能にするには、Network Agent がインストールされていなければなりません。

Websense 定義のプロトコル定義を使用するだけでなく、フィルタリングのためにカスタム 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 [**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、[**ポリシー管理**] > [**フィルタ コンポーネント**] を選択し、[**プロトコル**] 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、189 ページおよびカスタム プロトコルの作成、191 ページを参照してください。

プロトコルのフィルタリング

関連トピック：

- プロトコルの使用、187 ページ
- カスタム プロトコルの編集、189 ページ
- カスタム プロトコルの作成、191 ページ
- プロトコル ID の追加または編集、189 ページ
- Websense によって定義されたプロトコルへの追加、193 ページ

Network Agent がインストールされているとき、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。

ご注意：
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、Websense ソフトウェアは、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。

Websense ソフトウェアがこの情報を見つけられなかった場合、このプロトコルに関連付けられているすべてのコンテンツが許可されます。

カスタム プロトコルの編集

関連トピック：

- プロトコルの使用、187 ページ
- カスタム プロトコルの作成、191 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

[ポリシーの管理] > **[フィルタ コンポーネント]** > **[プロトコルの編集]** 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、**[プロトコルの追加]** をクリックして、カスタム プロトコルの作成、191 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ィルタリング アクションを変更するために、**[アクションの無効化]** をクリックします（プロトコル フィルタリングのグローバル変更、191 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、**[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、189 ページを参照）。
4. リストの中の ID を選択し、次に **[編集]** 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. 作業が終了したら、**[OK]** をクリックして、変更をキャッシュします。**[すべて保存]** 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、**[削除]** をクリックします。

プロトコル ID の追加または編集

[フィルタ コンポーネント] > **[プロトコルの編集]** > **[プロトコル ID の追加]** 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。[**プロトコル ID の編集**] 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。
   - [**すべてのポート**] 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 8080 のプロトコルを定義するときには注意が必要です。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。

     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。
   - [**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、[プロトコルの編集] ページに戻ります。[**すべて保存**] 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

[**フィルタ コンポーネント**] > [**プロトコルの編集**] > [**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、[**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] をクリックして、[プロトコルの編集] ページに戻ります。変更をキャッシュするために、[プロトコルの編集] ページでも [OK] をクリックしなければなりません。

プロトコル フィルタリングのグローバル変更

[フィルタ コンポーネント] > **[プロトコルの編集]** > **[アクションの無効化]** 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フィルタリング 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**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、**[変更なし]**が選択されています。詳細は、フィルタリング アクション、43 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、194 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]** と **[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、189 ページを参照)。変更をキャッシュするために、[プロトコルの編集] ページでも **[OK]** をクリックしなければなりません。

カスタム プロトコルの作成

関連トピック:

- プロトコルの使用、187 ページ
- プロトコルのフィルタリング、188 ページ
- カスタム プロトコルの編集、189 ページ
- Websense によって定義されたプロトコルへの追加、193 ページ

[フィルタ コンポーネント] > **[プロトコル]** > **[プロトコルの追加]** 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、193 ページ を参照してください。

2. **[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 [プロトコルの編集] 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。
   - **[すべてのポート]** または **[すべての外部IP アドレスポート]** 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。

   > **ご注意：**
   > ポート 80 または 8080 のプロトコルを定義するときには注意が必要です。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。
   >
   > 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「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. [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、194 ページを参照)。
5. 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。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. 変更をキャッシュするために、再度 **[OK]** をクリックします。**[すべて保存]** 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

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

関連トピック：
- カテゴリの使用、177 ページ
- プロトコルの使用、187 ページ
- デフォルトの Bandwidth Optimizer 制限の設定、195 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。

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。

帯域幅ベースのフィルタリング オプションがアクティブのとき、Websense ソフトウェアは、最初の設定から 10 分後、および Websense Policy Server が再開されたときにその 10 分後に、帯域幅ベースのフィルタリングを開始します。この遅延は、帯域幅の正確な計算と、フィルタリングでのこのデータの使用を保証するためです。

帯域幅制限のために要求がブロックされたとき、その情報が Websense ブロック ページの [**理由**] フィールドに表示されます。詳細は、ブロック ページ、85 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

関連トピック :

- カテゴリ フィルタの編集、49 ページ
- プロトコル フィルタの編集、52 ページ
- Bandwidth Optimizer による帯域幅の管理、194 ページ

ポリシーの中で帯域幅設定を指定する前に、帯域幅ベースのフィルタリング設定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。Websense によって定義されている値は次の通りです。

- ネットワークのデフォルト帯域幅 : **50%**
- プロトコルあたり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. Websense Manager で、[**設定**] > [**フィルタリング**] を選択します。
2. 帯域幅によるフィルタリングを有効にしているときに帯域幅を基にしたフィルタリング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、[**ネットワークのデフォルト帯域幅**] でデフォルトのフィルタリング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、[**プロトコル別のデフォルト帯域幅**] でデフォルトのフィルタリング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. 作業が終了したら、[OK] をクリックして、変更をキャッシュします。[**すべて保存**] 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

カテゴリ フィルタを作成するとき、ファイル拡張子を基にフィルタリングを定義し、特定のカテゴリに含まれるサイトからの特定のファイル タイプへのアクセスを制限することができます。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ビデオ ファイルをブロックするという設定が可能です。

Websense ソフトウェアは、いくつかの事前定義されたファイル タイプ、または特定の目的に使用するファイル拡張子のグループを提供します。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を適用するか、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。しかし、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。

ユーザがサイトを要求したとき、Websense ソフトウェアは最初にサイト カテゴリを判断し、次に、フィルタリングされるファイル拡張子をチェックします。

ご注意：
ビデオおよびオーディオ インターネット メディアに完全なフィルタリングを適用するには、プロトコル ベースのフィルタリングとファイル タイプによるフィルタリングを組み合わせます。この場合、プロトコル フィルタリングはストリーミング メディアを処理し、ファイル タイプによるフィルタリングはダウンロードしてから再生できるファイルを処理します。

ユーザがアクセスしようとしているファイルの拡張子がブロックされている場合、Websense ブロック ページの [**理由**] フィールドは、そのファイル タ

イプがブロックされたことを示します。詳細は、ブロック ページ、85 ページ を参照してください。

> **ご注意：**
> ブロックされた GIF または JPEG 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 タイプの定義には、フィルタリング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、Websense によって定義されるファイル タイプには、以下のファイル拡張子が含まれます。

オーディオ	圧縮 ファイル		実行ファイル	ビデオ	
.aif	.ace	.mim	.bat	.asf	.mpg
.aifc	.arc	.rar	.exe	.asx	.mpv2
.aiff	.arj	.tar		.avi	.qt
.m3u	.b64	.taz		.ivf	.ra
.mid	.bhx	.tgz		.m1v	.ram
.midi	.cab	.tz		.mov	.wm
.mp3	.gz	.uu		.mp2	.wmp
.ogg	.gzip	.uue		.mp2v	.wmv
.rmi	.hqx	.xxe		.mpa	.wmx
.snd	.iso	.z		.mpe	.wxv
.wav	.jar	.zip			
.wax	.lzh				
.wma					

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。

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、カスタム ファイル タイプを作成するには、**[ポリシー管理]** > **[フィルタ コンポーネント]** を選択し、**[ファイル タイプ]** をクリックします。詳細は、ファイル タイプの扱い、198 ページ を参照してください。

ファイル タイプの扱い

関連トピック：
- ファイル タイプに基づくトラフィックの管理、196 ページ
- カテゴリ フィルタの編集、49 ページ
- サイトのフィルタリング、81 ページ

[ポリシーの管理] > **[フィルタ コンポーネント]** > **[ファイル タイプの編集]** ページを使用して最大 32 の **ファイル タイプ** を作成および管理できます。ファイル タイプは、カテゴリ フィルタで明示的にブロックできるファイル拡張子のグループです（ファイル タイプに基づくトラフィックの管理、196 ページを参照）。

- 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、**[拡張子を追加]** 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、199 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、**[ファイル タイプを追加]** をクリックし、次にカスタム ファイル タイプの追加、198 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、**[削除]** 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。**[すべて保存]** 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

[フィルタ コンポーネント] > **[ファイル タイプの編集]** > **[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。

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. **ユーザ定義のファイル拡張子** 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、[ファイル タイプの編集] 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、[ファイル タイプの編集] ページで [OK] をクリックします。**[すべて保存]** 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

[フィルタ コンポーネント] > [ファイル タイプの編集] > [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。

1. **[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、[ファイル タイプの編集] 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、[ファイル タイプの編集] ページで [OK] をクリックします。**[すべて保存]** 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

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 Websense フィルタリングは、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。正規表現は強力なフィルタリング 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、フィルタリングのオーバーヘッドを過度に大きくします。

> **重要**
> 正規表現をフィルタリング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。

Websense ソフトウェアは、一部の例外を除いて、大部分の Perl 正規表現構文をサポートします。一部の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。

`(?<=pattern)string`	`(?<!pattern)string`
`\N{name}`	`(?imsx-imsx)`
`(?(condition)pat1)`	`\pP`
`(?(condition)pat1|pat2)`	`\pP`
`(?{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フィルタリング動作の確認

Websense 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、フィルタリング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、201 ページ
- ポリシーの確認、201 ページ
- フィルタリングのテスト、201 ページ
- URL アクセス、202 ページ
- ユーザの調査、202 ページ

また**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 Web サイトが表示されます。サポート ポータルから、Knowledge Base を使用してチュートリアル、ヒント、関連記事、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

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 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. **[実行]** 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 が再分類された場合は、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

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 **[ポリシーの確認]** 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、**[ユーザの検索]** 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の指定、202 ページを参照）。
   - IP アドレス
3. **[実行]** 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、ユーザに割り当てられているポリシーがなく、ユーザ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（フィルタリング順序、80 ページを参照）。

フィルタリングのテスト

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 **[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、[**ユーザの検索**] 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の指定、202 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. [**実行**] 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

ユーザが過去 2 週間の間に（今日を含む）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 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. [**実行**] 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。

セキュリティ関連のアラートを受け取ったときに、このツールを使って、組織がフィッシング サイトやウィルスに感染したサイトに接触していないかを調べることができます。

ユーザの調査

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 [**ユーザの調査**] をクリックします。
2. ユーザ名またはコンピュータの IPアドレスの全部または一部を入力します。
3. [**実行**] を クリックします。

調査レポートにクライアントの使用状況の履歴が表示されます。

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の指定

[**ユーザの検索**] ページを使用して、ポリシーの確認ツールまたはフィルタリングの テストツールの対象となるユーザ（ディレクトリ）クライアントを指定します。

このページが開かれ、[**ユーザ**] オプションが選択された状態になります。「**ディレクトリ エントリ**」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 サービスを利用している場合にだけ利用できます。

ディレクトリを検索してユーザを見つけるには、以下の手順を実行します。

1. ユーザ**名**またはその一部を入力します。
2. **ディレクトリ エントリ**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. [**検索**] をクリックします。検索条件に一致するエントリが [**検索結果**] の下にリストされます。
4. ユーザ名をクリックしてユーザを選択するか、または [**再建策**] 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。

   [**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名が [**ユーザ**] フィールドに表示されたとき、[**実行**] をクリックします。

フィルタリングのテスト ツールを使用している場合、[**実行**] 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。をクリックすると、ディレクトリの参照に戻ります。

ユーザ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 アドレス**] をクリックします。

10 ユーザ識別

ポリシーをユーザ 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 アドレスが与えられ、要求を行ったユーザを識別する必要があります。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を識別 および 認証し、Websense ソフトウェアにユーザ情報を渡します。詳細は、『インストールガイド』を参照してください。
- Websense 透過的識別エージェントは、ディレクトリ サービスと通信し、ユーザを識別するためにバックグラウンドで動作します (透過的識別 を参照)。
- Web ブラウザを開くとき、Websense ソフトウェアが ログオンを要求し、ネットワーク資格情報の入力をユーザに促します (手動認証、207 ページを参照)。

透過的識別

関連トピック :

- 手動認証、207 ページ
- ユーザ識別方法の設定、208 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 サービスでユーザを識別するために使用するすべての方法を 言います。これは、フィルタリングで使用するためにユーザ情報を 提供するデバイス または アプリケーション と 統合された Websense ソフトウェア、または オプション の Websense 透過的識別エージェント の使用を 含みます。

- Websense DC Agent、216 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 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、219 ページは、Windows ドメインにログインするユーザ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ます。しかし、連携するログオン アプリケーションは、Windows コンピュータ上でのみ動作します。
- Websense RADIUS Agent、222 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、227 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手順は、『インストールガイド』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（複数のエージェントの設定、233 ページ を参照）。

ご注意：
統合された NetCache アプライアンスを使用している場合、透過的識別が動作するために、NetCache は、WinNT、LDAP、または RADIUS フォーマットでユーザ名を Websense ソフトウェアに送信する必要があります。

プロキシ サーバーを使用し、透過的識別エージェントを使用する場合、プロキシ サーバーで匿名認証を使用することが最良です。

一般のユーザ識別の設定と特定の透過的識別エージェントの両方は、Websense Manager で設定されます。左ナビゲーションペインで、**[設定]** タブをクリックし、**[ユーザ識別]** をクリックします。

詳細な 設定方法は、ユーザ識別方法の設定、208 ページ を参照してください。

特定の場合に、Websense ソフトウェアは透過的識別エージェントからユーザ情報を得ることができない場合があります。これは、1 人以上のユーザが同じコンピュータに割り 当てられている、ユーザが匿名ユーザ または ゲストである、またはその他の理由で発生します。これらの場合、ユーザにブラウザでログオンするよう 促すことができます（手動認証、207 ページ を参照）。

リモート ユーザの透過的識別

ある特定の設定で、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を透過的に識別することができます：

- Websense Remote Filtering Server および Remote Filtering Client を配備すると、Websense ソフトウェアがドメイン アカウントを使用してキャッシュされたドメイン上にログオンするすべてのリモート ユーザを識別することができます。詳細は、リモート クライアントのフィルタ、159 ページ を参照してください。

- DC Agent を配備すると、リモート ユーザ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、216 ページ を参照)。
- リモートの場所からログオンするユーザを認証するために RADIUSサーバーを使用している場合、RADIUS Agent が透過的にこれらのユーザを識別することができ、ユーザ または グループに基づいてフィルタリング ポリシーを適用することができます (RADIUS Agent、222 ページ を参照)。

手動認証

関連トピック :

- 透過的識別、205 ページ
- 特定のコンピュータの認証ルールの設定、210 ページ
- セキュア手動認証、212 ページ
- ユーザ識別方法の設定、208 ページ

透過的識別は、すべての環境で常に利用可能ではなく、また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のために、または 透過的識別が利用可能でない場合に、ユーザ および グループ ベースのポリシーに基づいてフィルタするために、**手動認証**を使用することができます。

ブラウザを介してインターネットにアクセスする最初のときに、手動認証によりユーザ名とパスワードを入力するようユーザに促します。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、そのユーザのポリシー情報を検索します。

透過的識別が利用できない場合 (ユーザ識別方法の設定、208 ページ を参照)、または ブラウザを開くとき、ユーザがログオンするよう促すカスタム認証の設定で指定するコンピュータのリストを作成した場合、手動認証を有効にするよう Websense ソフトウェアを設定することができます (特定のコンピュータの認証ルールの設定、210 ページ を参照)。

手動認証が有効で 次の場合は、ユーザが HTTP エラーを受信し インターネットにアクセスできません :

- パスワードの入力に 3 回失敗した。ユーザ名 または パスワードが無効なときに これは起こります。
- 認証要求を回避するために [**キャンセル**] 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。

ユーザ識別方法の設定

関連トピック：

- 透過的識別、205 ページ
- 手動認証、207 ページ
- ユーザおよびグループに関する作業、62 ページ

ユーザおよびグループ ベースのポリシーを適用するために、Websense ソフトウェアが、いつ、どのようにネットワークのユーザを識別するかを管理するために、**[設定]** > **[ユーザ識別]** のページを使用します。

- 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 **[透過的識別エージェント]** にリストされます：

- **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。
- **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。
- **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、205 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、**[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、217 ページ
- Logon Agent の設定、220 ページ
- RADIUS Agent の設定、225 ページ
- eDirectory Agent の設定、229 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、**[削除]** をクリックします。

[追加の認証オプション] で、ユーザが（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、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 ポリシーを優先する場合、**[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に要求するためには、**[ログオン情報についてユーザにプロンプトを表示する]** をクリックします。ユーザ 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、207 ページ を参照）。
- ユーザ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 [例外] 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。

ユーザが、いつ、どのように Websense ソフトウェアによって識別されるか決定する一般ルールを確立した後で、ルールの例外を作成することができます。

例えば、透過的識別エージェント または 統合製品をユーザを識別するために使用し、透過的に識別することができないとき 資格情報の入力をユーザに促すために、手動認証を有効にした場合、次のいずれかを特定のコンピュータに指定することができます：

- 識別できないユーザは、資格情報の入力を要求されない。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。
- 利用可能な場合でも、ユーザ情報は常に無視され、ユーザは 常に資格情報の入力を促される。
- 利用可能な場合でも、ユーザ情報は常に無視され、ユーザは 常に資格情報の入力を促されない（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 ポリシーが常に適用されます）。

例外を作成するためには、**[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、210 ページ を参照してください。

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。変更を保存しない場合は、**[キャンセル]** をクリックします。

特定のコンピュータの認証ルールの設定

関連トピック：

- ユーザ識別方法の設定、208 ページ
- 手動認証、207 ページ
- セキュア手動認証、212 ページ

選択認証を使用すると、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）からのインターネット アクセスを要求するユーザが、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。これは、次の目的で使用できます：

- キオスクを提供している組織の従業員用に、公共のキオスク コンピュータと異なる認証ルールを設定する。
- 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が、常に識別されることを保証する。

コンピュータが適用されている指定されたユーザ識別の設定は、[**設定**] > [**ユーザ識別**] の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ユーザ識別の設定を行う、または 特定のコンピュータの指定された設定を表示するためには、[**例外**] 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、[**追加**] をクリックします。その後の手順は、ユーザ識別設定例外の定義、210 ページ を参照してください。

リストにコンピュータ 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。[**すべて保存**] をクリックするまで、変更は適用されません。

ユーザ識別設定例外の定義

関連トピック：

- 透過的識別、205 ページ
- 手動認証、207 ページ
- ユーザ識別方法の設定、208 ページ

特定のユーザ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、[**設定**] > [**ユーザ識別**] > [**IP アドレスの追加**] の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 [**IP アドレス範囲**] を入力し、[**選択済み**] リストにそれらを追加するために、右矢印ボタンをクリックします。

   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を透過的に識別するかどうかを指定するために、[**ユーザ識別**] 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情報を要求するためには、[**ユーザの透過的識別を試行**] を選択します。
   - ユーザを識別するためのすべての透過的方法を使用しない場合は、[**ユーザ情報を無視**] を選択します。
3. ユーザ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。ユーザ情報が有効でない、他の識別が失敗した、または ユーザ情報が無視された場合に、この設定は適用されます。
   - ユーザにログオン資格情報を提供するように要求するためには、[**ログオン情報についてユーザにプロンプトを表示する**] 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、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。
   - ユーザがログオン資格情報を提供するように要求されないためには、[**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。
4. [ユーザ識別] のページに戻るためには、[OK] をクリックします。
5. [例外] 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。[**すべて保存**] をクリックするまで、変更は適用されません。

ユーザ識別設定例外の修正

関連トピック:

- 透過的識別、205 ページ
- 手動認証、207 ページ
- ユーザ識別方法の設定、208 ページ

[例外] リストの項目を変更するためには、[**設定**] > [**ユーザ識別**] > [**IP アドレスの編集**] のページを使用します。このページで行われた変更は、[選択済み] 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を透過的に識別するかどうかを指定するために、[**ユーザ識別**] 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情報を要求するためには、[**ユーザの透過的識別を試行**] を選択します。

- ユーザを識別するためのすべての透過的方法を使用しない場合は、[**ユーザ情報を無視する**] を選択します。

2. ユーザ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。
   - ユーザにログオン資格情報を提供するように要求するためには、[**ログオン情報についてユーザにプロンプトを表示する**] 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、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。
   - ユーザがログオン資格情報を提供するように要求されないためには、[**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。
3. [ユーザ識別] のページに戻るためには、[OK] をクリックします。
4. [例外] 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。[**すべて保存**] 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

関連トピック:

- ユーザ識別方法の設定、208 ページ
- 手動認証、207 ページ
- 特定のコンピュータの認証ルールの設定、210 ページ
- セキュア手動認証の有効化、214 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。

ご注意:
セキュア手動認証は リモート フィルタリング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、213 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、214 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、215 ページ を参照）。

キーと 証明書の 作成

関連トピック：

- 手動認証、207 ページ
- 特定のコンピュータの認証ルールの設定、210 ページ
- セキュア手動認証、212 ページ
- セキュア手動認証の有効化、214 ページ
- クライアント ブラウザ内での証明書の適用、215 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（www.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 Server 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

関連トピック:

- 手動認証、207 ページ
- 特定のコンピュータの認証ルールの設定、210 ページ
- セキュア手動認証、212 ページ
- キーと証明書の作成、213 ページ
- クライアント ブラウザ内での証明書の適用、215 ページ

1. Websense Filtering Service を停止します (Websense サービスの停止と起動、288 ページを参照)。
2. Filtering Service コンピュータの Websense インストール ディレクトリに移動します (デフォルトで、**C:¥Program Files¥Websense¥bin** または **/opt/Websense/bin/**).
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、**[設定]** > **[ディレクトリ サービス]** のページで **[SSL を使用する]** が選択されていることを確認します。詳細は、詳細ディレクトリ設定、66 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

関連トピック:

- 手動認証、207 ページ
- 特定のコンピュータの認証ルールの設定、210 ページ
- セキュア手動認証、212 ページ
- キーと証明書の作成、213 ページ
- セキュア手動認証の有効化、214 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 (バージョン 7)

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. **[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、**[キャンセル]** 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 **認証エラー** ボックスをクリックし、次に **[証明書の表示]** をクリックします。
4. [証明書] ダイアログ ボックスの一般タブ上で、**[証明書のインストール]** をクリックします。
5. **[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、**[次へ]** をクリックします。
6. **[終了]** 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、**[はい]** をクリックします。

ユーザは、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 (バージョン 2.x)

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. **[常にこの証明書を受け入れる]** をクリックします。
3. 要求されたら、資格情報を入力します。
4. **[ツール]** > **[オプション]** に移動し、**[詳細]** をクリックします。
5. **[暗号化]** タブを選択し、**[証明書の表示]** をクリックします。
6. **[ウェブサイト]** タブを選択し、証明書がリストされていることを確認します。

ユーザは、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 (バージョン 3.x)

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. **[例外を追加することができます]** をクリックします。
3. **[例外の追加]** をクリックします。
4. **[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、**[セキュリティ例外の確認]** をクリックします。

ユーザは、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

関連トピック :

- 透過的識別、205 ページ
- DC Agent の設定、217 ページ
- エージェントのインスタンスごとの設定、235 ページ

Websense DC Agent は Windows 上で動作し、NetBIOS、WINS、または DNS などの各種ネットワーク サービスで機能する Windows ネットワークでユーザを検出します。

DC Agent と User Service が ネットワーク ユーザ 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。詳細は、『インストール ガイド』の「Websense コンポーネントのインストール」の項を参照してください。

   ご注意 :
   ドメイン管理者権限を使用して DC Agent を実行します。また、ドメイン管理者アカウントは DC Agent コンピュータで 管理者グループのメンバーである必要があります。

   これは、DC Agent がドメインコントローラからユーザ ログオン情報を取得するために必要になります。この権限で DC Agent をインストールすることができない場合、インストール後にこれらのサービスの管理者権限を設定してください。詳細は、Websense ソフトウェアがユーザまたはグループ ポリシーを適用しない、368 ページ を参照してください。

2. DC Agent をネットワーク内の他の Websense 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. Websense Manager を使用して、フィルタにユーザとグループを追加します (クライアントの追加、69 ページ を参照)。

DC Agent が透過的にユーザを識別できない場合、Websense ソフトウェアが識別のためのプロンプトを表示することができます。詳細は、手動認証、207 ページ を参照してください。

DC Agent の設定

関連トピック :

- 透過的識別
- 手動認証
- ユーザ識別方法の設定
- DC Agent
- 複数のエージェントの設定

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、および DC Agent の新しいインスタンスを設定するために、**[設定] > [ユーザ識別] > [DC Agent]** の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. [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 **サーバー** の IP アドレスまたは名前を入力します。

   ご注意：
   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. 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 間で認証接続を確立するために、**[認証を有効にする]** をチェックし、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、アスタリスク マーク (*) 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 (エージェントのインスタンスごとの設定、235 ページ を参照)。

1. **[DC Agent の通信]** に、DC Agent と他の Websense コンポーネント間の通信に使用する通信ポートを入力します。デフォルトは 30600 です。

   Websense テクニカル サポートによって指示された場合を除き、**[診断ポート]** の設定は 変更しないでください。デフォルトは 30601 です。
2. [ドメイン コントローラのポーリング] で、DC Agent が ユーザ ログオン セッションをドメイン コントローラにクエリーすることを有効にするために、**[ドメイン コントローラのポーリングを有効にする]** にマークを付けます。

   エージェント設定ファイルで、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。詳細は、複数のエージェントの設定、233 ページ を参照してください。
3. **[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。
4. **[ユーザ 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。

5. ユーザ 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、[コンピュータ ポーリング] で **[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。

6. ユーザ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、**[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。

7. DC Agent が コンピュータ ポーリングで取得したユーザ 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、**[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名を保持しますので、ユーザ マップの正確性を低くすることがあります。

   ご注意 :
   ユーザ エントリのタイムアウト間隔を ユーザ マップの確認間隔より短くしないでください。これは、ユーザ名が確認される前に、ユーザマップから削除される原因になります。

8. 変更をすぐに保存し、実行するために [OK] をクリックします。

Logon Agent

関連トピック :

- 透過的識別、205 ページ
- Logon Agent の設定、220 ページ
- エージェントのインスタンスごとの設定、235 ページ

Websense Logon Agent はユーザがドメインにログオンすると、リアル タイムでユーザを識別します。これは、クエリー タイミングの問題でユーザ ログオンを見落とす可能性を除去します。

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.exe）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。詳細は、『インストールガイド』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 コンピュータと Websense Filtering Service と通信するように設定します（Logon Agent の設定 を参照）。

ご注意：
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、Linux 上の User Service の実行、375 ページ を参照してください。

Logon Agent の設定

関連トピック：

- 透過的識別、205 ページ
- 手動認証、207 ページ
- ユーザ識別方法の設定、208 ページ
- Logon Agent、219 ページ
- 複数のエージェントの設定、233 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、**[設定] > [ユーザ識別] > [Logon Agent]** の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. [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**サーバー**の IP アドレスまたは名前を入力します。

   ご注意：
   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。デフォルトは 30602 です。
3. Filtering Service と Logon Agent 間で認証接続を確立するために、**[認証を有効にする]** をチェックし、接続のための**パスワード**を入力します。
4. 変更を保存するために [OK] をクリックするか、追加の設定情報を入力するために、画面の次のセクションに移動します。

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 Agent の通信]** に、Logon Agent と他の Websense コンポーネント間の通信に使用する通信ポートを入力します。デフォルトは 30602 です。
2. Websense テクニカル サポートによって指示された場合を除き、**[診断ポート]** の設定は 変更しないでください。デフォルトは 30603 です。
3. [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 **[接続ポート]** を指定します。デフォルトは 15880 です。
4. 各 Logon Agent インスタンスが許容する **[接続最大数]** を入力します。デフォルトは 200 です。

   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。
5. 変更を保存するために [OK] をクリックするか、追加の設定情報を入力するために、画面の次のセクションに移動します。

ユーザ 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）で動作するかを決定する必要があります。

LogonApp.exe を実行するとき、/NOPERSIST パラメータを含めて起動すると、非永続モードで動作します。（詳細情報は、Logon Agent のインストールに含まれている **LogonApp_ReadMe.txt** ファイル 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 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、[**クエリー間隔**] を指定します。

> **ご注意**：
> 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、クエリーが 5 分ごとに発生する前に、現在の 15 分の間隔が終了する必要があります。

- 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 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、[**ユーザ 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 エントリはユーザ マップから削除されます。

設定の変更が完了したとき、設定を保存するために [OK] をクリックします。

RADIUS Agent

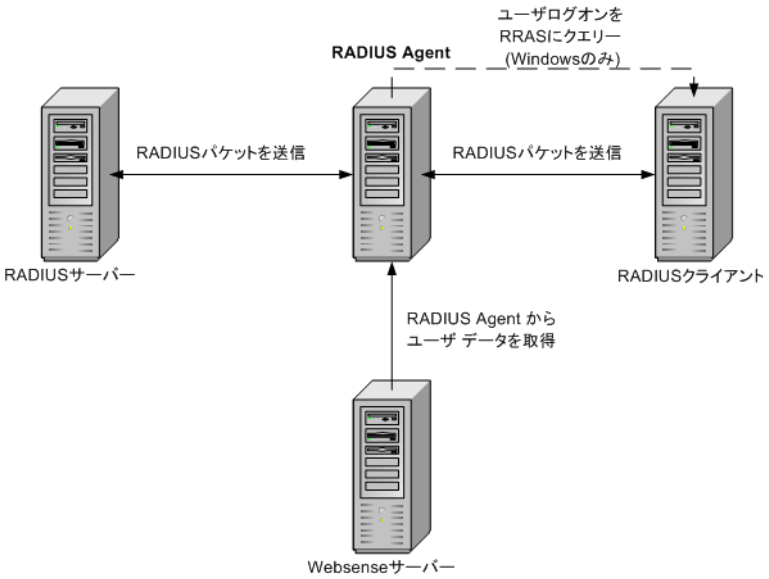
関連トピック：

- 透過的識別、205 ページ
- RADIUS トラフィック処理、223 ページ
- RADIUS 環境の設定、224 ページ
- RADIUS Agent の設定、225 ページ
- RADIUS クライアントの設定、226 ページ
- RADIUS サーバーの設定、227 ページ
- エージェントのインスタンスごとの設定、235 ページ

Websense RADIUS Agent によって、RADIUS サーバーによって提供された認証を使用し、ユーザと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 または グループ、およびローカル ユーザに対して、特定のフィルタリング 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。しかし、RADIUS Agent、RADIUS サーバー、RADIUS クライアントは、適切に設定される必要があります (RADIUS Agent の設定、225 ページ を参照)。

RADIUS トラフィック処理

Websense RADIUS Agent は、RADIUS クライアントと RADIUS サーバー (または 複数のクライアントとサーバー) 間の RADIUS メッセージを転送するプロキシの役割を務めます。

RADIUS Agent は 直接ユーザを認証しません。代わりに、エージェントは リモート ユーザを識別し、RADIUS サーバーがそれらのユーザを認証することができるように、IP アドレスと関連付けます。理想的には、RADIUS サーバーは LDAP ベースのディレクトリ サービスに認証要求を送信します。

RADIUS Agent は、ユーザ名対 IP アドレスの組合せをユーザ マップに保存します。RADIUS クライアントが、アカウンティング (またはユーザ ログオン追跡) をサポートし、アカウンティングが使用可能である場合、RADIUS Agent は、受信する RADIUS メッセージからユーザ ログオン セッションについてのより詳細な情報を収集します。

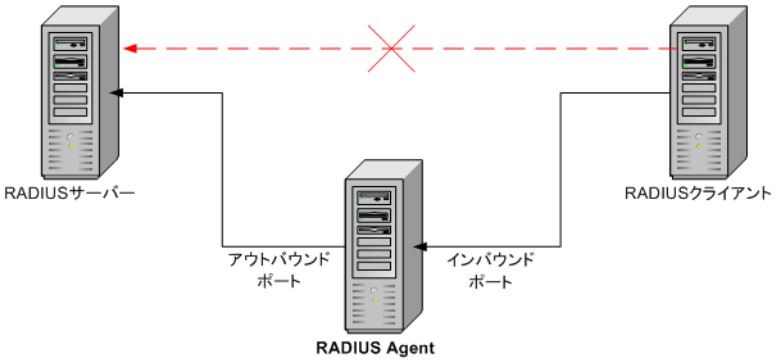
適切に設定されたら、Websense RADIUS Agent は、次のタイプのすべての RADIUS プロトコル パケットを取得し、処理します :

- **認証要求** : RADIUS クライアントによって送信されるネットワーク アクセス接続試行の認証要求。
- **アクセス許可** : 認証要求に応答して RADIUS サーバーによって送信されます。接続を試みた RADIUS クライアントが許可され、認証されることを伝達します。

- **アクセス拒否**：認証要求に応答して RADIUS サーバーによって送信されます。接続を試みた RADIUS クライアントが拒否されたことを伝達します。
- **アカウンティング中止要求**：RADIUS サーバーにユーザの追跡を停止するよう伝達するために、RADIUS クライアントから送信されます。

RADIUS 環境の設定

Websense RADIUS Agent は、RADIUS クライアントと RADIUS サーバー間のプロキシの役割を務めます。この図は、標準の RADIUS 構成と比較して、RADIUS Agent を使用する場合の違いを単純化して表示しています。



RADIUS Agent と RADIUS サーバーは別個のコンピュータにインストールする必要があります。エージェントとサーバーは、同じ IP アドレスを持つことはできなく、異なったポートを使用する必要があります。

RADIUS Agent をインストールした後、Websense Manager で RADIUS Agent を設定します（RADIUS Agent の設定、225 ページ を参照）。また、次のことが必要になります：

- RADIUS クライアント（一般に Network Access Server ［NAS］）を直接 RADIUS サーバーに接続するのではなく、RADIUS Agent と通信するよう設定します。
- RADIUS Agent をプロキシとして使用するように、RADIUS サーバーを設定します（RADIUS サーバー マニュアルを参照してください）。複数の RADIUS サーバーがある場合、個別にそれぞれを設定します。

ご注意：
Lucent RADIUS Server および RRAS を使用している場合、RADIUS サーバーを Password Authentication Protocol（PAP）を使用するように設定し、RRAS サーバーが PAP 要求だけを受け入れるよう設定する必要があります。詳細は、関連する製品マニュアルを参照してください。

RADIUS Agent の設定

関連トピック：

- 透過的識別、205 ページ
- 手動認証、207 ページ
- ユーザ識別方法の設定、208 ページ
- RADIUS Agent、222 ページ
- 複数のエージェントの設定、233 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、[**設定**] > [**ユーザ識別**] > [**RADIUS Agent**] の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. [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**サーバー**の IP アドレスまたは名前を入力します。

   ご注意：
   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. 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。デフォルトは 30800 です。
3. Filtering Service と RADIUS Agent 間で認証接続を確立するために、[**認証を有効にする**] をチェックし、接続のための**パスワード**を入力します。
4. 変更を保存するために [**OK**] をクリックするか、追加の設定情報を入力するために、画面の次のセクションに移動します。

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 マーク (*) 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（エージェントのインスタンスごとの設定、235 ページ を参照）。

1. RADIUS Agent と他の Websense コンポーネント間の通信に使用する**通信ポート**を入力します。デフォルトは 30800 です。

2. Websense テクニカル サポートによって指示された場合を除き、[**診断ポート**] の設定は 変更しないでください。デフォルトは 30801 です。
3. RADIUS Server で、[**RADIUS サーバーの IP または名前**] を入力します。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。
4. Microsoft RRAS を使用している場合、[**RRAS コンピュータ**] の IP アドレスを入力します。Websense ソフトウェアは、ユーザ ログオン セッションをこのコンピュータにクエリーします。
5. RADIUS Agent がユーザ マップを更新する頻度を決定するために、[**ユーザ エントリのタイムアウト**] 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。
6. 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、[**認証ポート**] および [**アカウンティング ポート**] を使用します。各タイプの通信で、通信のためにどのポートが使用されるかを指定します :
   - RADIUS Agent と RADIUS サーバー
   - RADIUS Agent と RADIUS クライアント
7. 変更が完了したとき、設定をすぐに保存するために [OK] をクリックします。

RADIUS クライアントの設定

RADIUS Agent を介して、RADIUS クライアントが RADIUS サーバーに認証とアカウンティングの要求を送信するように設定する必要があります。

RADIUS クライアントの設定を修正します :

- RADIUS Agent が認証要求をリッスンしているコンピュータとポートに、RADIUS クライアントは 認証要求を送信します。これは、RADIUS Agent 設定中に指定された [**認証ポート**] です。
- RADIUS Agent がアカウンティング要求をリッスンしているコンピュータとポートに、RADIUS クライアントは アカウンティング要求を送信します。これは、RADIUS Agent 設定中に指定された [**アカウンティング ポート**] です。

RADIUS クライアントを設定する正しい手順は、クライアントのタイプによって異なります。詳細は、RADIUS クライアントのマニュアルを参照してください。

ご注意 :
RADIUS クライアントは、認証およびアカウンティングのメッセージに、**User-Name** 属性と **Framed-IP-Address** 属性を含める必要があります。RADIUS Agent は、ユーザ名 /IP アドレスのペアを判定し、保存するために、これらの属性値を使用します。デフォルトで、RADIUS クライアントがこの情報を作成しない場合、作成するように設定してください (RADIUS クライアントのマニュアルを参照してください)。

RADIUS サーバーの設定

Websense RADIUS Agent と RADIUS サーバー間の通信が適切になるように、次を実行します :

- RADIUS サーバーのクライアント リストに、RADIUS Agent コンピュータの IP アドレスを追加します。手順は、RADIUS サーバーのマニュアルを参照してください。
- エージェントが RADIUS サーバーと通信するために使用する、RADIUS サーバーと RADIUS クライアント間の共有暗号鍵を定義します。通常、共有暗号鍵は 認証セキュリティ オプションとして指定されます。

  RADIUS クライアントと RADIUS サーバーに共有暗号鍵を設定すると、RADIUS メッセージはセキュア通信されます。一般に、共有暗号鍵は普通のテキスト文字列です。手順は、RADIUS サーバーのマニュアルを参照してください。

ご注意 :
RADIUS サーバーは、認証およびアカウンティングのメッセージに、**User-Name** 属性と **Framed-IP-Address** 属性を含める必要があります。RADIUS Agent は、ユーザ名 /IP アドレスのペアを判定し、保存するために、これらの属性値を使用します。デフォルトで、RADIUS サーバーがこの情報を作成しない場合、作成するように設定してください (RADIUS サーバーのマニュアルを参照してください)。

eDirectory Agent

関連トピック :

- 透過的識別、205 ページ
- eDirectory Agent の設定、229 ページ
- エージェントのインスタンスごとの設定、235 ページ

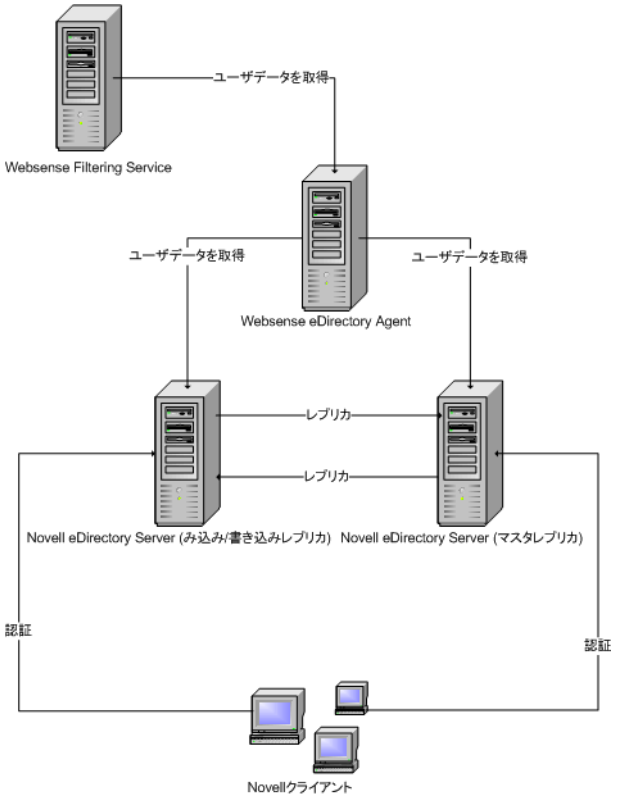
Websense ソフトウェアがユーザ、グループ、ドメイン、組織単位に割り当てられたポリシーに従ってフィルタできるようにするために、Websense eDirectory Agent は 透過的にユーザを識別するために Novell eDirectory と共に動作します。

eDirectory Agent は、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。エージェントは、各認証されたユーザを IP アドレスと関連づけ、ローカルなユーザマッ

プにユーザ名対 IP アドレスの組合せを記録します。eDirectory Agent は、この情報を Filtering Service に送信します。

> **ご注意：**
> 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。これは 1 つの IP アドレスを複数のユーザと関連づけます。この場合、その IP アドレスからログオンした最後のユーザのユーザ名 /IP アドレスのペアが、eDirectory Agent のユーザ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。



設定上の注意

- Cisco Content Engine v5.3.1.5以降とWebsenseソフトウェアを統合している場合：
  - Cisco Content Engine と同じコンピュータ上で、次の Websense サービスを実行してください：

Websense eDirectory Agent
Websense User Service
Websense Filtering Service
Websense Policy Server

- すべての Novell eDirectory レプリカが、同じコンピュータの **wsedir.ini** ファイルに追加されていることを確認してください。
- **eDirAgent.bak** ファイルを削除します。

Websense Reporting Tools サービスは、Cisco Content Engine と Websense ソフトウェアとは**別の**コンピュータ上で実行してください。

- Websense ソフトウェアは、eDirectory Agent を NMAS と共に使用することをサポートしています。NMAS と共に eDirectory Agent を使用するためには、Novell Client が動作しているコンピュータに eDirectory Agent をインストールする必要があります。

eDirectory Agent の設定

関連トピック：

- 透過的識別、205 ページ
- 手動認証、207 ページ
- ユーザ識別方法の設定、208 ページ
- eDirectory Agent、227 ページ
- eDirectory Agent が LDAP を使用するための設定、231 ページ
- 複数のエージェントの設定、233 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、**[設定] > [ユーザ識別] > [eDirectory Agent]** の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. [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**サーバー**の IP アドレスまたは名前を入力します。

   ご注意：
   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. 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。デフォルトは 30700 です。
3. Filtering Service と eDirectory Agent 間で認証接続を確立するために、**[認証を有効にする]** をチェックし、接続のための**パスワード**を入力します。
4. 変更を保存するために [OK] をクリックするか、追加の設定情報を入力するために、画面の次のセクションに移動します。

次に、グローバル eDirectory Agent 通信設定をカスタマイズします。デフォルトでは、ここでの変更は すべての eDirectory Agent インスタンスに影響を与えます。しかし、アスタリスク マーク (*) 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 (エージェントのインスタンスごとの設定、235 ページ を参照)。

1. eDirectory Agent と他の Websense コンポーネント間の通信に使用するデフォルト**通信ポート**を入力します。デフォルトは 30700 です。
2. Websense テクニカル サポートによって指示された場合を除き、**[診断ポート]** の設定は 変更しないでください。デフォルトは 30701 です。
3. [eDirectory Server] で、ディレクトリでユーザ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。
4. 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 アカウント情報を指定します :
   a. Novell eDirectory の管理ユーザ 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される **[パスワード]** を入力します。
   c. エージェントのユーザ 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 エントリのタイムアウト]** 間隔を指定します。

   一般的なユーザ ログオン セッションより、この間隔をおよそ 30%長くするべきです。これは、ユーザがブラウズを完了する前に、ユーザ 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。

   > **ご注意 :**
   > 特定の環境では、[ユーザ エントリのタイムアウト] 間隔を使用して eDirectory Agent がユーザ マップを更新する頻度を決定するより、ユーザ ログオンを更新するために、一定間隔で eDirectory Server にクエリーすることが適切な場合があります。eDirectory Server の完全クエリーの有効化、232 ページを参照してください。

5. **[eDirectory レプリカ]** 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、**[追加]** をクリックし、eDirectory サーバー レプリカの追加、231 ページ の手順に従ってください。

設定の変更が完了したとき、設定を保存するために [OK] をクリックします。

eDirectory サーバー レプリカの追加

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 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 レプリカの追加] の画面で eDirectory **Server**（マスタ または レプリカ）の IP アドレス または名前を入力します。
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。
3. [eDirectory] のページに戻るためには、[OK] をクリックします。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. [OK] をクリックして変更をキャッシュし、[**すべて保存**] をクリックします。
6. 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。その手順は、Websense サービスの停止と起動、288 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

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、288 ページを参照）。
3. eDirectory Agent インストール ディレクトリ（デフォルトで、**¥Program Files¥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** 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

小さなネットワークでは、すべてのログオンするユーザを一定間隔で 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と最後のクエリーからログオフしたユーザの両方を検出することができ、ローカル ユーザ 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 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はクエリーによって識別されるため、[**ユーザ エントリのタイムアウト**] 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の名前を検索するために必要な時間。
- ユーザ名情報を処理する時間、ローカルユーザ 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 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 コンピュータで、Websense **bin** ディレクトリに移動します（デフォルトで、C:¥Program Files¥Websense¥bin または /opt/Websense/bin）。
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を考慮して、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。

   > **ご注意：**
   > 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、適切に **PollInterval** の値を編集します。

   間隔は **ミリ秒** 単位で設定することに注意してください。
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、288 ページを参照）。

複数のエージェントの設定

関連トピック：

- DC Agent、216 ページ
- Logon Agent、219 ページ
- RADIUS Agent、222 ページ
- eDirectory Agent、227 ページ

同じネットワーク内で、複数の透過的識別エージェントを組み合せることができます。お客様のネットワークが、複数のエージェントを必要とする場合、別個のコンピュータにそれぞれのエージェントをインストールすることが最良です。しかし、特定の場合に、1 つのコンピュータで複数のエージェントが動作するように、Websense ソフトウェアを設定することができます。

次の透過的識別エージェントの組み合せがサポートされています :

組み合せ	同一コンピュータ？	同一ネットワーク？	必要な設定
複数の DC Agent	いいえ	はい	DC Agent のすべてのインスタンスが、Filtering Service と通信できることを確認してください。
複数の RADIUS Agent	いいえ	はい	各インスタンスを Filtering Service と通信するように設定してください。
複数の eDirectory Agent	いいえ	はい	各インスタンスを Filtering Service と通信するように設定してください。
複数の Logon Agent	いいえ	はい	各インスタンスを Filtering Service と通信するように設定してください。
DC Agent + RADIUS Agent	はい	はい	これらのエージェントを別個のディレクトリにインストールしてください。各エージェントを異なった通信ポートを使用して Filtering Service と通信するように設定してください。
DC Agent + eDirectory Agent	いいえ	いいえ	Websense ソフトウェアは 同じ配置で Windows と Novell 両方のディレクトリ サービスと通信することをサポートしていません。しかし、両方のエージェントをインストールすることはでき、1 つだけエージェントをアクティブにできます。
DC Agent + Logon Agent	はい	はい	両方のエージェントを Filtering Service と通信するように設定してください。デフォルトで、各エージェントは ユニークなポートを使用します。そのため、ポートを変更しない場合、ポートの競合の問題はありません。

組み合せ	同一コンピュータ？	同一ネットワーク？	必要な設定
eDirectory Agent + Logon Agent	いいえ	いいえ	Websense ソフトウェアは 同じ配置で Windows と Novell 両方のディレクトリ サービスと通信することをサポートしていません。しかし、両方のエージェントをインストールすることはでき、1 つだけエージェントをアクティブにできます。
RADIUS Agent + eDirectory Agent	はい	はい	各エージェントを異なった通信ポートを使用して Filtering Service と通信するように設定してください。
DC Agent + Logon Agent + RADIUS Agent	はい	はい	この組み合わせは めったに必要とされませんが、サポートされます。 各エージェントを別個のディレクトリにインストールしてください。すべてのエージェントを異なった通信ポートを使用して Filtering Service と通信するように設定してください。

エージェントのインスタンスごとの設定

Websense Manager の透過的識別エージェントの設定はグローバルであり、インストールされたエージェントのすべてのインスタンスに適用されます。しかし、どれかのエージェントの複数のインスタンスがある場合、他とは無関係に 1 つのインスタンスを設定することができます。

特定のエージェントのインスタンスのために指定するユニークな設定は、設定ダイアログ ボックスのグローバル設定より優先されます。上書きできる設定は アスタリスク (*) のマークが付いています。

1. 透過的識別エージェント サービスを停止します (Websense サービスの停止と起動、288 ページを参照)。
2. エージェントのインスタンスを実行しているコンピュータで、エージェント インストール ディレクトリに移動し、テキスト エディタで適切なファイルを開きます :
   - DC Agent: **transid.ini**
   - Logon Agent: **authserver.ini**
   - eDirectory Agent: **wsedir.ini**
   - RADIUS Agent: **wsradius.ini**
3. このエージェントのインスタンスで変更するパラメータを見つけます (INI ファイル パラメータ、237 ページ を参照)。

たとえば、このエージェントのインスタンスと他の Websense サービス間で認証接続を有効にします。このためには、INI ファイルで **password** パラメータの値を入力します：

```
password=[xxxxxx]
```

4. 必要なら、他の値も変更します。
5. INI ファイルを保存して、閉じます。
6. **DC Agent** 設定を変更した場合、Websense **bin** ディレクトリ（デフォルトで、C:¥Program Files¥Websense¥bin）から 2 つのファイルを削除する必要があります。
   a. DC Agent コンピュータのすべての Websense サービスを停止します（Websense サービスの停止と起動、288 ページ を参照）。
   b. 次のファイルを削除します：

      ```
      Journal.dat
      XidDcAgent.bak
      ```

      Websense DC Agent サービスを起動するとき、これらのファイルは再生されます。
   c. Websense サービス（DC Agent を含む）を再起動し、**ステップ 8** に移動します。
7. 透過的識別エージェント サービスを再起動します。
8. Websense Manager で、エージェント設定を更新します：
   a. **[設定]** > **[ユーザ識別]** に移動します。
   b. **[透過的識別エージェント]** で、エージェントを選択し、**[編集]** をクリックします。

      > **ご注意：**
      > エージェント インスタンスの**ポート**番号を変更した場合、エージェントを削除し、再度追加します。最初に既存のエージェント エントリを選択し、**[削除]** をクリックし、次に **[エージェントの追加]** をクリックします。

   c. このエージェント インスタンスが使用する **[サーバーの IP または名前]** と **[ポート]** を確認します。INI ファイルで固有のポート番号を指定している場合、エントリがその値と一致していることを確認してください。
   d. INI ファイルで固有の認証パスワードを指定した場合、ここで表示される **[パスワード]** エントリが正しいことを確認してください。
   e. **[OK]** をクリックして、変更をキャッシュします。**[すべて保存]** をクリックするまで、変更は適用されません。

INI ファイル パラメータ

Websense Manager フィールド ラベル	.ini パラメータ名	説明
通信ポート (すべてのエージェント)	port	エージェントが他の Websense サービスと通信するポート。
診断ポート (すべてのエージェント)	DiagServerPort	エージェント トラブルシューティング ツールがエージェントからのデータをリッスンするポート。
パスワード (すべてのエージェント)	password	エージェントが他の Websense サービスに認証接続するために使用するパスワード。認証を有効にするためのパスワードを指定します。
クエリー間隔 (DC Agent)	QueryInterval	DC Agent がドメインコントローラーにクエリーする間隔。
サーバーの IP または名前 ポート (eDirectory Agent)	Server=IP:port	eDirectory Agent を実行しているコンピュータの IP アドレスとポート番号。
検索基準 (eDirectory Agent)	SearchBase	Novell eDirectory サーバーのルート コンテクスト。
管理者識別名 (eDirectory Agent)	DN	Novell eDirectory サーバーの管理ユーザ名。
パスワード (eDirectory Agent)	PW	Novell eDirectory サーバーの管理ユーザ パスワード。
RADIUS サーバーの IP または名前	RADIUSHost	RADIUS サーバーコンピュータの IP アドレス または 名前。
RRAS コンピュータの IP アドレス (Windows のみ) (RADIUS Agent)	RRASHost	RRAS を実行しているコンピュータの IP アドレス。Websense は、ユーザ ログオン セッションをこのコンピュータにクエリーします。
認証ポート : RADIUS Agent と RADIUS サーバー間	AuthOutPort	RADIUS サーバーが認証要求をリッスンするポート。
認証ポート : RADIUS クライアントと RADIUS Agent 間	AuthInPort	RADIUS Agent が認証要求をアクセプトするポート。
認証ポート : RADIUS Agent と RADIUS サーバー間	AccOutPort	RADIUS サーバーが RADIUS アカウンティング メッセージをリッスンするポート。
認証ポート : RADIUS クライアントと RADIUS Agent 間	AccInPort	RADIUS Agent が アカウンティング要求をアクセプトするポート。

特定のユーザ名を無視するエージェントの設定

透過的識別エージェントを、実際のユーザ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。ドメイン コントローラと接続するために、**computerA/ServiceName** と識別されるユーザのコンピュータが起動した場合、フィルタリング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** ポリシーによってこのユーザをフィルタします。

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、288 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 ソフトウェアがこれらのユーザ名を無視します。

   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名を無視します。Websense ソフトウェアは、フィルタリングにこれらの名前を含めません。

11 指定済み管理

関連トピック：

- 管理ロールの説明、240 ページ
- 管理者の説明、240 ページ
- 管理ロールの開始、245 ページ
- Websense Manager へのアクセスの有効化、253 ページ
- 指定済み管理の使用、257 ページ
- 複数の管理者の Websense Manager へのアクセス、267 ページ
- すべてのロールのフィルタリング制限の定義、268 ページ

指定済み管理は、クライアントの特定のグループのインターネット フィルタリングとレポートを管理するための強力で、柔軟性のある手段を提供します。すべてのユーザが中央に位置している場合、これはインターネット アクセス管理とレポートの責務を個々のマネージャーに配分する効果的な方法です。複数の場所と地域をもつ大規模な組織においては、ローカル管理者が、その地域のユーザのインターネット アクセスとフィルタリング活動のレポートを管理するために非常に効果的な方法です。

指定済み管理を実行することは、同じ管理者によって管理されるクライアントの各グループのための管理ロールを作成することになります。各ロールの個々の管理者に、クライアントのためのポリシーを管理、レポートの作成、または その両方の許可を与えることができます。管理ロールの開始、245 ページを参照してください。

優先管理者ロールは、事前にインストールされ、デフォルトの次の管理ユーザを含みます：WebsenseAdministrator。優先管理者は、他のロールの管理者より広範囲のポリシーと構成設定へのアクセス権を持っています。優先管理者、241 ページを参照してください。

管理ロールの説明

関連トピック：

- 管理者の説明、240 ページ
- 管理ロールの開始、245 ページ

管理ロールは、管理されたクライアント（1 人以上の管理者によって管理されたユーザ、グループ、ドメイン、組織単位、コンピュータ、ネットワーク範囲）のコレクションです。ポリシーをロールのクライアントに適用する、レポートを作成する、または その両方の許可を個々の管理者に与えます。

Websense ソフトウェアでは、優先管理者ロールが事前定義されています。また、自動的な優先管理者ロールのメンバーであるデフォルト ユーザ WebsenseAdministrator が存在します。このロールに管理者を追加することはできますが、デフォルト管理者を削除することはできません。

重要
事前定義された優先管理者ロールを削除することはできません。デフォルト ユーザの WebsenseAdministrator は、優先管理者ロールの管理者ですが、ロールにはリストされません。WebsenseAdministrator の許可を変更 または削除することはできません。

お客様の組織で適切な数のロールを作成してください。例えば、部門のマネージャーを管理者とし、部門のメンバーを管理されたクライアントとする各部門のロールを作成するかもしれません。地理的に分散された組織では、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をそのロールの管理されたクライアントとして割り当てるかもしれません。その後、その所在地で 1 人以上の個人を管理者に割り当てます。

管理者の定義で利用可能なオプションについての情報は、管理者の説明、240 ページ を参照してください。

ロールの作成と許可の設定手順は、指定済み管理の使用、257 ページ を参照してください。

管理者の説明

管理者は、クライアントのグループのポリシーを管理するために または レポートを作成するために、Websense Manager にアクセスすることができる個人です。利用可能な許可は ロールのタイプに依存します。

- 優先管理者は Websense Manager で事前定義された特別なロールです。このロールは、アクセス許可の定義に対して、最も柔軟性があります。優先管理者、241 ページを参照してください。
- 指定済み管理ロールは 優先管理者によって作成される必要があります。このロールの管理者は より限定されたアクセス許可を持っています。指定済み管理者、243 ページを参照してください。

さらに、ポリシー管理の責務を与えずにレポートを作成することを許可する、レポート専用の指定済み管理ロールを作成することができます。

ネットワーク ログオン資格証明を使用するロールを管理者に割り当てるか、または Websense Manager にアクセスすることだけに使用する専用のアカウントを作成することができます。Websense Manager へのアクセスの有効化、253 ページを参照してください。

優先管理者

関連トピック :

- 管理者の説明、240 ページ
- 指定済み管理者、243 ページ
- 複数のロールの管理者、244 ページ

優先管理者ロールは インストール中に作成されます。デフォルトユーザ、WebsenseAdministrator は 自動的にこのロールに割り当てられます。そのために、インストール中に最初にこのユーザ名とパスワードでログオンするとき、すべてのポリシー、レポート、および Websense Manager の設定に対する完全な管理上のアクセス権を持っています。

このアカウントの完全なアクセスを維持するために、WebsenseAdministrator は 優先管理者ロールの管理者のリストに表示されません。これは 削除できません。許可を変更することができません。

必要な場合に、優先管理者ロールに管理者を追加することができます。各管理者に 次の許可を与えることができます :

- **ポリシー**許可は、優先管理者 に指定済み管理ロールを作成 / 編集し、これらのロールにフィルタとポリシーをコピーすることを許可します。また、これは、フィルタリング コンポーネント、フィルタ、ポリシーを作成 / 編集し、ポリシーを他のロールによって管理されないクライアントに適用することができます。

  さらに、ポリシー許可をもつ優先管理者は監査ログを見ることができ、Websense の設定へアクセスすることができ、次の他のオプションも与えられます :

  - **条件無し**許可は、アカウント、Policy Server、Remote Filtering Server 設定、リスククラス割り当て、ログ記録オプションなどのすべての Websense インストールのシステム設定に対して、優先管理者がアクセスすることを許可します。

条件無し優先管理者は、指定済み管理ロールによって管理されたすべてのユーザに対して、特定のカテゴリとプロトコルをブロックするフィルタ ロックを作成するオプションを持っています。詳細は、すべてのロールのフィルタリング制限の定義、268 ページ を参照してください。

必要に応じて、条件無し優先管理者は、管理者を追加 / 削除し、優先管理者ロールを変更することができます。また、指定済み管理ロールを削除するか、それらのロールから管理者 または クライアントを削除することができます。

- **条件有り**許可は、データベースのダウンロード、ディレクトリ サービス、ユーザ識別、Network Agent の設定に対して、優先管理者がアクセスすることを許可します。また、レポート許可を持っている条件有り優先管理者は、レポート ツールの設定にアクセスすることができます。

  条件有り優先管理者は、Websense ユーザ アカウントを追加することができますが、削除することはできません。彼らは、指定済み管理を作成 / 編集することができますが、ロール、管理者、または それらに割り当てられている管理されたクライアントを削除することはできません。また、優先管理者ロールから管理者を削除することはできません。

- **レポート**許可は、すべてのレポート機能とすべてのユーザのレポートに対して、優先管理者がアクセスすることを許可します。条件無し優先管理者には、自動的にレポート許可が与えられます。

  管理者がレポート許可のみを与えられている場合、[共通のタスク] リストの [ポリシーの作成]、[URL の再分類]、[URL のブロック解除] オプションは利用できません。さらに、ツールボックスの中の [ポリシーの確認] オプションは利用できません。

複数の条件無し優先管理者を作成することは、主要な優先管理者が利用できない場合に、他の管理者がすべての Websense ポリシーと構成設定へアクセスできることを保証します。

2 人の管理者が、同じロールのポリシーを管理するために同時にログオンすることはできないことに注意してください。競合を防止するための情報は、複数の管理者の Websense Manager へのアクセス、267 ページ を参照してください。

優先管理者ロールの独自の権限は、ロールの管理者がすべてのロールへアクセスすることを許可されていることです。ログオンの後に他のロールに変更するためには、バナーの**ロール** ドロップダウンリストに移動し、ロールを選択します。

ロールの変更後、ポリシー許可は 指定済み管理ロールで利用可能なロールに制限されます。作成するフィルタとポリシーはそのロールの管理者のみが利用可能です。そのロールで管理されたクライアントにだけ適用することができます。指定済み管理者、243 ページを参照してください。

レポート許可は累積されます。すなわち、管理者は、管理者であるすべてのロールの組み合わされた許可をもっています。条件無し優先管理者は、アクセスしているロールにかかわらず完全なレポート許可を持っています。

指定済み管理者

関連トピック：

- 管理者の説明、240 ページ
- 優先管理者、241 ページ
- 複数のロールの管理者、244 ページ

指定済み管理者は 特定のロールに割り当てられたクライアントを管理します。各管理者にポリシー許可、レポート許可、または その両方を割り当てます。

ポリシー許可をもつ指定済み管理者は、ロールに割り当てられたクライアントにポリシーを適用し、それによって各クライアントの利用可能なインターネット アクセスを決定します。この役割の一部として、指定済み管理者は、優先管理者によって設定されたフィルタ ロックの制限を受けるポリシーおよびフィルタを作成 / 編集 / 削除することができます。すべてのロールのフィルタリング制限の定義、268 ページを参照してください。

ご注意：
指定済み管理者は、管理しているクライアントのインターネット活動に関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、優先管理者は、管理者によって行われた変更をモニタするために監査ログのページを使用するべきです。監査ログの表示とエクスポート、286 ページを参照してください。

指定済み管理者は デフォルト ポリシーを削除することはできません。

指定済み管理者は ある制限付きでフィルタコンポーネントを編集することができます。詳細は、ポリシーとフィルタの作成、251 ページ を参照してください。

また、Websense ユーザ アカウントで Websense Manager にログオンしているポリシー許可の管理者は、自身の Websense パスワードを変更することができます。(Websense ユーザ アカウント、255 ページ を参照。)

レポート許可に関する指定済み管理者の使用可能なオプションは、ロールが設定されている方法によって変化します。彼らのロールによって管理されたクライアントだけについてレポートすることが可能である場合もあり、すべてのクライアントに関するレポートが許可される場合もあります。彼らは、すべてのレポート機能へのアクセス権を持つ場合もあり、より限定されたレポート アクセス権を持つ場合もあります。詳細は、ロールの編集、258 ページ を参照してください。

レポート許可だけを持つ管理者は、右側のショート カットペイン（共通のタスクとツールボックス）で利用可能なオプションを制限されます。

複数のロールの管理者

関連トピック：

- 管理者の説明、240 ページ
- 優先管理者、241 ページ
- 指定済み管理者、243 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もできます。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 つのロールを選択する必要があります。

ログオン後の許可は次の通りです：

- **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 / 編集し、そのロールが管理するクライアントにポリシーを適用することができます。[指定済み管理] のページは、割り当てたすべてのロールをリストし、ロールの管理された各クライアントとレポート許可を表示することができます。
- **レポート**：すべてのロールの組み合わされたレポート許可をもちます。例えば、次のようなレポート許可をもつ 3 つのロールに割り当てられているとします：
  - ロール 1: レポート許可なし
  - ロール 2: 管理しているクライアントのみをレポート、調査レポートのみ
  - ロール 3: すべてのクライアントをレポート、すべてのレポート機能への完全なアクセス

  この場合、ログオン時にどのロールを選択したかにかかわらず、[今日] と [履歴] のページのすべてのレポートの表示が許可され、すべてのクライアントをレポートすることができ、すべてのレポート機能を使用することができます。
  レポートのためにのみログオンしている場合、バナー バーの [ロール] フィールドに 完全レポート（すべてのクライアントに関するレポート）許可を持つか、制限付きレポート（管理するクライアントのみに関するレポート）許可を持つかどうかが表示されます。

管理ロールの開始

関連トピック：

- 管理ロールの説明、240 ページ
- 管理者への通知、247 ページ
- 指定済み管理タスク、248 ページ

指定済み管理を開始するためには、優先管理者が次のタスクを完了する必要があります：

- 管理者がどのように Websense Manager にログオンするかを決定します。Websense Manager へのアクセスの有効化、253 ページを参照してください。
- ロールを追加し、それらを設定します。指定済み管理の使用、257 ページを参照してください。
- 管理者にその役割とオプションを知らせます。管理者への通知、247 ページを参照してください。

これらの必要とされるタスクに加えて、指定済み管理と関連付けられたいくつかのオプションのタスクがあります。

フィルターロックの作成

条件無し優先管理者は フィルタ ロックを作成することができます。それは、すべての指定済み管理ロールで管理されたクライアントをブロックする特定のカテゴリとプロトコルを指定します。これらの制限は、指定済み管理ロールで作成された、または コピーされたすべてのフィルタに自動的に実行され、指定済み管理者が変更することはできません。

ご注意：
フィルタ ロックは、優先管理者ロールによって管理されているクライアントには割り当てられません。

また、フィルタ ロックは、選択されたカテゴリに関連したファイル タイプとキーワードをブロック および ロックすることができ、選択されたプロトコルのログ記録を行うことができます。フィルタ ロックの作成、269 ページを参照してください。

クライアントの移動

優先管理者としてログオンしているときに、[クライアント] のページでクライアントを追加すると、そのクライアントは優先管理者ロールに割り当てられます。[ロールの編集] ページで、そのクライアントを指定済み管理ロールに追加することはできません。理想的には、優先管理者ロールでポリ

シーを割り当てるより、直接ロールにクライアントを追加するべきです。しかし、これは常に可能ではありません。

優先管理者ロールから他のロールにクライアントを移動するためには、[クライアント] のページで **[ロールに移動]** オプションを使用します。クライアントをロールに移動、71 ページを参照してください。

移動するときに、優先管理者ロールで適用されたポリシーは指定済み管理ロールにコピーされます。また、ポリシーを実行するフィルタもコピーされます。このコピー処理中に、もしあれば、フィルタ ロックの制限を行うためにフィルタは更新されます。

ターゲット ロールには、「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。管理者は、そのロールで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。

ご注意：
フィルタ または ポリシーが同じロールにコピーされるたびに、「コピー済み」タグは新しいコピーを受け取った回数だけ増加します：「コピー済み 1」、「コピー済み 2」など。それぞれは ロールの中で別個のフィルタ または ポリシーになります。

ロールの管理者がフィルタおよびポリシーをリネームし、必要な場合それらを編集し、それらの設定を明確にし、重複を最小にする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単純化することができます。

優先管理者ロールの [すべて許可] フィルタは、すべてのカテゴリ または プロトコルへのアクセスを許可し、編集できません。フィルタ ロック を実行する優先管理者の能力を維持するために、これらのフィルタは指定済み管理ロールにコピーすることができません。

移動されるクライアントに割り当てられたポリシーが [すべて許可] フィルタを実行している場合、[すべて許可] フィルタを使用しないポリシーを適用するまで、クライアントは移動できません。

クライアントが新しいロールに移動された後は、そのロールの管理者だけが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。優先管理者ロールのオリジナルのポリシー または フィルタの変更は、指定済み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。

フィルタとポリシーのコピー

優先管理者によって作成されたフィルタとポリシーは、優先管理者ロールの管理者にだけ利用可能です。クライアントをロールを移動させないで、指定済み管理ロールにフィルタとポリシーをコピーするためには、**[ロールにコピー]** オプションを使用します。ロールへのフィルタおよびポリシーのコピー、175 ページを参照してください。

直接フィルタとポリシーをコピーすると、クライアントの移動でコピーされたフィルタとポリシーに適用される同じ制限が行われます。

- フィルタ ロックの制限がコピー中に実行されます。
- [すべて許可]のカテゴリ および プロトコル フィルタは、コピーされません。
- 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「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がわかり易いように、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。

残りのクライアントに対するポリシーの適用

指定済み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。優先管理者ロールに [処理対象クライアント] リストはありません。

ポリシーをクライアントに適用するためには、[ポリシーの管理] > [クライアント] のページでそれらを追加します。クライアントの追加、69 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、そのロールのデフォルト ポリシーで管理されます。

[クライアント] の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たネットワーク、グループ、ドメイン、組織単位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あるい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優先管理者ロールに追加することはできません。

管理者への通知

関連トピック :

- 管理ロールの説明、240 ページ
- 管理ロールの開始、245 ページ

どの管理ロールでも個人を管理者に割り当てた後で、彼らに次の情報を通知してください。

- Websense Manager のログオン URL。デフォルト :

  ```
  https://<ServerIP>:9443/mng/
  ```

  <ServerIP> の代わりに Websense Manager を実行しているコンピュータの IP アドレスを使用します。
- 当てはまる場合、ログオン中にどの Policy Server を選択するべきか 複数の Policy Server 環境では、ログオン中に管理者は Policy Server を選択する必要があります。管理された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た Policy Server を選択する必要があります。

- Websense Manager にログオンするとき、ネットワーク ログオン アカウント または Websense ユーザ アカウントのどちらを使用するか。管理者が Websense ユーザ アカウントでログオンする場合、ユーザ名とパスワードを提供してください。
- 許可。ロール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、または その両方。

  ポリシーとレポート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てください。レポートを作成することのみを計画している場合、バナーの [**ロール**] フィールドに移動し、[**ポリシー許可のリリース**] を選択するよう推奨してください。これは、ロールのポリシー許可を解放し、他の管理者が Websense Manager にアクセスし、そのロールのポリシーを管理することができるようにします。
- ロールによって管理されているクライアントのリストを見つける方法。管理されたクライアントのリストを含む [ロールの編集] ページを表示するためには、管理者が [ポリシーの管理] > [指定済み管理] に移動し、ロール名をクリックします。
- カテゴリ または プロトコルがブロックされていて、ロックされている場合、フィルタ ロックによって制限されていること。
- 管理者の一般的なタスク 指定済み管理タスク、248 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 / 変更したときは、指定済み管理者に必ず通知してください。これらのコンポーネントはすべてのロールのフィルタとポリシーで自動的に表示されます。従って、各管理者にとって、変更がいつ行われたかを知ることは重要です。

指定済み管理タスク

関連トピック :

- 管理ロールの説明、240 ページ
- 管理ロールの開始、245 ページ
- 管理者への通知、247 ページ

ポリシー許可を持つ指定済み管理者は 次のタスクを行なうことができます。

- ユーザ アカウントの表示、249 ページ
- ロール定義の表示、249 ページ
- クライアント ページにクライアントを追加、250 ページ
- ポリシーとフィルタの作成、251 ページ
- クライアントに対するポリシーの適用、252 ページ

細かいレベルで **レポート**許可を与えることができます。ロールに与えられた指定されたレポート許可によって、レポート許可をもつ管理者に次のどのタ

スクが利用可能であるかが決定されます。レポートの作成、252 ページを参照してください。

ユーザ アカウントの表示

関連トピック:
- 指定済み管理タスク、248 ページ
- ロール定義の表示、249 ページ
- クライアント ページにクライアントを追加、250 ページ
- ポリシーとフィルタの作成、251 ページ
- クライアントに対するポリシーの適用、252 ページ

ネットワーク資格情報で Websense Manager にログオンしている場合、パスワードの変更はネットワーク ディレクトリ サービスを使用して処理されます。詳細についてはシステム管理者に問い合わせてください。

Websense ユーザ名とパスワードが割り当てられている場合、アカウントの情報を表示し、Websense Manager 内でパスワードを変更します。

1. **[ポリシーの管理]** > **[指定済み管理]** に移動します。
2. ページ上部の **[Websense ユーザ アカウントの管理]** をクリックします。
3. パスワードを変更する場合、**[パスワードの変更]** をクリックします。Websense ユーザ パスワードの変更、256 ページを参照してください。
4. 管理者であるロールのリストを表示するためには **[表示]** をクリックします。

ロール定義の表示

関連トピック:
- 指定済み管理タスク、248 ページ
- ユーザ アカウントの表示、249 ページ
- クライアント ページにクライアントを追加、250 ページ
- ポリシーとフィルタの作成、251 ページ
- クライアントに対するポリシーの適用、252 ページ

ロールに管理されているクライアントをリストする [ロールの編集] ページを表示するためには、[指定済み管理] のページを開き、ロール名をクリックします。また、このページはこのロールでレポート許可を持つ管理者に、利用可能なレポート機能を表示します。

レポート許可だけを持つ管理者には このページは表示されません。管理者に指定されたレポート機能のみが利用可能です。

クライアント ページにクライアントを追加

関連トピック：

- 指定済み管理タスク、248 ページ
- ユーザ アカウントの表示、249 ページ
- ロール定義の表示、249 ページ
- ポリシーとフィルタの作成、251 ページ
- クライアントに対するポリシーの適用、252 ページ

優先管理者は ロールに管理されたクライアントを割り当てます。しかし、指定済み管理者は ポリシーを適用する前に、[クライアント] のページでクライアントを追加する必要があります。その手順は、クライアントの追加、69 ページ を参照してください。

クライアントが ロールの処理対象クライアント リストに追加されるとすぐに、そのロールのデフォルト ポリシーでフィルタされます。優先管理者の [クライアント] ページからロールに移動されたクライアントは、クライアントが移動したとき、ロールにコピーされた優先管理者が適用したポリシーによって管理されます。

[指定済み管理] > [ロールの編集] のページにリストされたすべてのクライアントは、[クライアント] のページに追加し、ポリシーを割り当てることができます。また、ロールの処理対象クライアントとして割り当てられている、個々のユーザ または グループ、ドメイン、組織単位、ネットワーク範囲のメンバーであるコンピュータを追加することができます。

ユーザは 複数のグループ、ドメイン、組織単位に含まれている場合があるので、異なったロールが 共通のメンバーとしてのグループ、ドメイン、組織単位を管理するときに、より大きいクライアント グループから個人を追加すると、競合を発生させる可能性があります。異なったロールの管理者が同時に Websense Manager にアクセスし、[クライアント] 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）を追加するかもしれません。この状況では、そのクライアントのインターネット フィルタリングは、[クライアント] ページでそれぞれのロールに指定された優先権によって管理されます。ロールの競合管理、265 ページを参照してください。

ポリシーとフィルタの作成

関連トピック：

- 指定済み管理タスク、248 ページ
- ユーザ アカウントの表示、249 ページ
- ロール定義の表示、249 ページ
- クライアント ページにクライアントを追加、250 ページ
- クライアントに対するポリシーの適用、252 ページ

ロールが作成されたとき、事前にインストールされているデフォルト ポリシー、カテゴリ フィルタ、プロトコル フィルタを自動的に継承します。また、優先管理者がロールにコピーすることを選択したポリシーとフィルタがあるかもしれません。

また、ポリシーとフィルタのほかに、優先管理者によって作成されたカスタム ファイル タイプ および プロトコルを継承します。

優先管理者から継承したポリシーとフィルタを編集することは自由です。行う変更は 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優先管理者が行った変更は、あなたのロールには影響を与えません。

ご注意：
優先管理者が カスタム ファイル タイプとプロトコルに行った変更は、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。

優先管理者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を確認してください。

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。指定済み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は、ポリシーに関する作業、75 ページ を参照してください。フィルタを作成する手順は、フィルタに関する作業、47 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。

- **カテゴリ**：カスタム カテゴリの追加、マスタ データベースとカスタム カテゴリ両方の編集、ロール内で使用する再分類された URL とキーワードの定義、作成するカテゴリ フィルタでデフォルトで適用されるアクションと高度なフィルタリング オプションの変更。（カテゴリが フィルタ ロックによってロックされていない場合に限り、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。）

- **プロトコル**: 作成するプロトコル フィルタでデフォルトで適用されるアクションと高度なフィルタリング オプションの変更。(プロトコルがフィルタ ロックによってロックされていない場合に限り、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。) 指定済み管理者は プロトコル定義を追加 / 削除することはできません。
- **ファイル タイプ**: ファイル拡張子の表示、ファイル タイプの割り当て。指定済み管理者は ファイル タイプを追加するか、ファイルタイプに割り当てられた拡張子を変更することはできません。
- **フィルタなし URL**: URL の追加、そのロールのみで管理されているすべてのクライアントに対して許可されるサイトを表す正規表現の追加。

詳細は、フィルタ コンポーネントの作成、176 ページ を参照してください。

優先管理者が フィルタ ロック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 / 編集したフィルタを変更できない場合があります。すべてのロールのフィルタリング制限の定義、268 ページ を参照してください。

クライアントに対するポリシーの適用

関連トピック:

- 指定済み管理タスク、248 ページ
- ユーザ アカウントの表示、249 ページ
- ロール定義の表示、249 ページ
- クライアント ページにクライアントを追加、250 ページ
- ポリシーとフィルタの作成、251 ページ

ポリシーを作成した後で、[**クライアントに適用**] をクリックすることで、[クライアント] のページにすでに追加されているクライアントに、そのポリシーを直接適用することができます。クライアントへのポリシーの割り当て、80 ページを参照してください。

または、[クライアント] のページに移動し、このポリシーによって管理されるクライアントを追加することもできます。クライアントに関する作業、60 ページを参照してください。

レポートの作成

レポート許可を持っている場合、利用可能な特定のレポート オプションが優先管理者によって設定されます。どの機能を使用することができるかを知るためには、[指定済み管理] のページに移動し、ロール名をクリックします。[ロールの編集] のページに、許可を持っているレポート機能が表示されます。詳細は、ロールの編集、258 ページ を参照してください。

Websense Manager へのアクセスの有効化

指定済み管理ロールの構成を設定するとき、管理者がどの Websense Manager 機能にアクセスすることができるかを決定します。Websense Manager にログオンしているユーザが、右側の機能を利用できるためには、それぞれのユーザがユーザ名とパスワードでログオンしている必要があります。2 つのタイプのアカウントが使用できます :

- **ネットワーク アカウント**はネットワーク ディレクトリ サービスですでに設定された資格情報を使用します (ディレクトリ アカウント、253 ページ を参照)。
- **Websense ユーザ アカウント**は Websense Manager内で使用するユーザ名とパスワードを作成します (Websense ユーザ アカウント、255 ページ を参照)。

ディレクトリ アカウント

関連トピック :

- Websense Manager へのアクセスの有効化、253 ページ
- Websense ユーザ アカウント、255 ページ

条件無し優先管理者は、[**設定**] > [**一般**] > [**ログオン ディレクトリ**] のページを使用して、管理者がネットワーク資格情報で Websense Manager にログオンすることを許可するため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。

ご注意 :
この情報は、Websense Manager ユーザのみを認証するために使用されます。フィルタリング クライアントには適用されません。クライアント ディレクトリ サービス情報は、[設定] > [ディレクトリ サービス] のページで設定されます (ディレクトリ サービス、63 ページ を参照)。

Websense Manager ユーザ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 サービスを含む場合、Websense Manager で設定するログオン ディレクトリ サービスと他との間に信頼関係が存在する必要があります。

Websense Manager 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、管理者に対して Websense ユーザ アカウントを作成することを考えてください (Websense ユーザ アカウント、255 ページ を参照)。

Websense Manager が管理者を認証するために使用するディレクトリ サービスを定義するためには、最初に管理者を認証するディレクトリ サービスを使

用するためのチェックボックスが選択されていることを確認し、次にリストから**ディレクトリサービス タイプ**を選択します。

デフォルトの **[Windows NT Directory / Active Directory (混在モード)]** を選択する場合、それ以上の設定は必要ありません。**[OK]** をクリックして、変更をキャッシュします。**[すべて保存]** をクリックするまで、変更は適用されません。

[Active Directory (ネイティブ モード)] または **[その他の LDAP ディレクトリ]** を選択した場合、次の追加情報を入力してください :

1. ディレクトリ サービス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 名前を入力します。

   Active Directory (ネイティブ モード) を使用し、フェイルオーバーのためにグローバル カタログ サーバーを配置している場合、その代わりに DNS ドメイン名を入力することができます。
2. ディレクトリ サービス通信に使用する**ポート**を入力します。
3. ディレクトリ サービスとの通信を暗号化するためには、**[SSL を使用する]** にマークを付けます。
4. Websense ソフトウェアがディレクトリ サービスに接続するために使用する **[ユーザ識別名]** と **[パスワード]** を入力します。
5. Websense ソフトウェアが管理者を認証するときに使用する **[デフォルト ドメイン コンテクスト]** を入力します。
   - Active Directory (ネイティブ モード) を使用している場合、設定は完了です。**[OK]** をクリックして、変更をキャッシュします。**[すべて保存]** をクリックするまで、変更は適用されません。
   - その他の LDAP ディレクトリを使用している場合、継続してください。
6. **[ユーザ ログイン ID の属性]** および もしあれば Websense ソフトウェアのユーザ認証を速めるために使用する **[ユーザ検索フィルタ]** を提供します。

   また、この情報は、**[設定]** > **[ディレクトリ サービス]** のページの **[詳細ディレクトリ設定]** にも現れます。必要なら、値をコピーし、ペーストすることができます。
7. [グループ オプション] で、LDAP スキーマが **memberOf** 属性を含むかどうか指定します :
   - memberOf が使用されない場合、Websense ソフトウェアが管理者を認証するために適用する **[ユーザ グループ検索フィルタ]** を指定します。
   - memberOf が使用される場合、適用されるべき**「グループ」属性**を指定します。
8. LDAP スキーマが ネストされたグループを含む場合、**[別のネストされたグループ検索を実行]** にマークを付けます。
9. ディレクトリ サービスが LDAP 照会を使用する場合、Websense ソフトウェアが照会を使用するか、無視するかを指定します。
10. **[OK]** をクリックして、変更をキャッシュします。**[すべて保存]** をクリックするまで、変更は適用されません。

Websense ユーザ アカウント

関連トピック：

- Websense Manager へのアクセスの有効化、253 ページ
- Websense ユーザアカウントの追加、255 ページ

管理者がネットワーク ディレクトリ資格情報を入力しないで Websense Manager にアクセスできるようにするアカウントを作成するためには、優先管理者は [**指定済み管理**] > [**Websense ユーザ アカウントの管理**] のページを使用します。また、このページで、優先管理者は、Websense ユーザ アカウントのパスワードを変更し、管理者として割り当てられている Websense ユーザのロールを表示することができます。

また、条件無し優先管理者は、このページで Websense ユーザ アカウントを削除することができます。

指定済み管理者は、Websense パスワードを変更し、管理者として割り当てられているロールを表示するために、このページを使用できます。

オプション	説明
追加	新しい Websense ユーザ アカウントを作成するためのページを開きます。Websense ユーザアカウントの追加、255 ページを参照してください。
パスワードの変更	関連するアカウントのパスワードを変更するためのページを開きます。Websense ユーザ パスワードの変更、256 ページを参照してください。
表示	ユーザが管理者として割り当てられているロールのリストを表示します。
削除	1 つ以上の不必要なユーザ アカウントのチェックボックスにマークを付け、削除するためにこのボタンをクリックします。
閉じる	指定済み管理のページに戻ります。

Websense ユーザアカウントの追加

関連トピック：

- Websense Manager へのアクセスの有効化、253 ページ
- Websense ユーザ アカウント、255 ページ
- Websense ユーザ パスワードの変更、256 ページ

Websense ユーザアカウントを追加するためには、[**指定済み管理**] > [**Websense ユーザ アカウントの管理**] > [**Websense ユーザの追加**] のページを使用します。

1. 50 文字以内で固有の**ユーザ名**を入力してください。

   名前は長さが 1 ～ 50 字で、以下の文字を含めることはできません :

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

   ユーザ名に スペースとダッシュを含めることができます。
2. このユーザの**パスワード** (4 – 255 文字) を入力し、確認します。

   強固なパスワードが推奨されます : 8 文字以上で、少なくとも次のそれぞれ 1 つずつを含む。

   - 大文字
   - 小文字
   - 数字
   - 特殊文字 (ハイフン、アンダースコア、空白 など)
3. 変更を完了したら、変更をキャッシュし、[Websense ユーザ アカウントの管理] のページに戻るために、[OK] をクリックします。**[すべて保存]** をクリックするまで、変更は適用されません。

Websense ユーザ パスワードの変更

関連トピック :

- Websense Manager へのアクセスの有効化、253 ページ
- Websense ユーザ アカウント、255 ページ
- Websense ユーザアカウントの追加、255 ページ

[指定済み管理] > [Websense ユーザ アカウントの管理] > [パスワードの変更] のページで、指定済み管理者は 自身の Websense ユーザ アカウントのパスワードを変更できます。優先管理者は、すべての Websense ユーザ アカウントのパスワードを変更するために、このページを使用することができます。

1. 正しい **ユーザ名**が、ページ上部に表示されていることを確認してください。
2. このユーザの新規**パスワード** (4 – 255 文字) を入力し、確認します。

   強固なパスワードが推奨されます : 8 文字以上で、少なくとも次のそれぞれ 1 つずつを含む。

   - 大文字
   - 小文字
   - 数字
   - 特殊文字 (ハイフン、アンダースコア、空白 など)
3. 変更を完了したら、変更をキャッシュし、[Websense ユーザ アカウントの管理] のページに戻るために、[OK] をクリックします。**[すべて保存]** をクリックするまで、変更は適用されません。

指定済み管理の使用

関連トピック：

- 管理ロールの説明、240 ページ
- ロールの競合管理、265 ページ

優先管理者 または 指定済み管理者が表示しているかによって、**[ポリシーの管理] > [指定済み管理]** のページは、異なったオプションを提供します。

優先管理者は、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、次のオプションが利用可能です。

オプション	説明
追加	新しいロールを追加するために クリックします。 ロールの追加、258 ページを参照してください。
ロール	ロールを表示 / 設定するために クリックします。 ロールの編集、258 ページを参照してください。
削除	リストでマークが付けられているロールを削除するために クリックします。このオプションは 条件無し優先管理者のみ利用可能です。 ロールが削除された後、ロールのクライアントがどのように管理されるかについての情報は、留意事項、266 ページ を参照してください。
詳細	ロールの優先順位の管理機能にアクセスするためにクリックします。
ロールの優先順位の管理	異なったロールで管理される複数のグループに同じクライアントが属するとき、使用されるロールのポリシー設定を指定するためにクリックします。ロールの競合管理、265 ページを参照してください。
Websense ユーザアカウントの管理	Websense Manager にアクセスするためにだけ使用するアカウントのユーザ名とパスワードを追加、編集、削除するために クリックします。Websense ユーザアカウント、255 ページを参照してください。
カスタム LDAP グループの管理	指定済み管理ロールで処理対象クライアントとして割り当てられているカスタム LDAP グループを追加、編集、削除するために クリックします。カスタム LDAP グループに関する作業、67 ページを参照してください。 設定されたディレクトリ サービスが Windows NT Directory / Active Directory (混在モード) である場合、このオプションは利用できません。

指定済み管理者は、自身が管理者のロールだけを参照し、より限定されたオプションへアクセスします。

オプション	説明
ロール	ロールに割り当てられたクライアント、指定されたレポート許可を表示するために クリックします。ロールの編集、258 ページを参照してください。
Websense ユーザ アカウントの管理	Websense Manager パスワードを変更し、割り当てられているロールを表示するオプションにアクセスするために クリックします。Websense ユーザ アカウント、255 ページを参照してください。

ロールの追加

関連トピック：

- ロールの編集、258 ページ
- 留意事項、266 ページ

新しいロールで名前と説明を指定するためには、**[指定済み管理]** > **[ロールの追加]** のページを使用します。

1. 新しいロールの**名前**を入力します。

   名前は長さが 1 ～ 50 字で、以下の文字を含めることはできません：

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

   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**説明**を入力します。

   説明は 最高 255 文字までです。ロール名に適用される文字に関する制限が説明にも適用されますが、2 つの例外があります。すなわち、ピリオド (.) とコンマ (,) は含めることができます。
3. **[ロールの編集]** のページを 表示し、このロールの特性を 定義するためには、[OK] をクリックします。ロールの編集、258 ページを参照してください。

   次に Websense Manager にログオンしたときに、新しいロールはバナーのロール ドロップダウンリストに追加されます。

ロールの編集

関連トピック：

- 指定済み管理の使用、257 ページ
- ロールの追加、258 ページ
- ロールの競合管理、265 ページ

指定済み管理者は、ロールで管理されているクライアントのリストと、与えられている特定のレポート許可を表示するために、**[指定済み管理]** > **[ロールの編集]** のページを使用することができます。

優先管理者は、ロールの管理者およびクライアントを選択し、下記の管理者許可を設定するために、このページを使用することができます。条件無し優先管理者だけが、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. 必要なら、**ロール名**と**説明**を変更します。

   ご注意：
   優先管理者ロール名は 変更できません。

2. このロールの管理者を追加 または 削除します。（優先管理者のみが 利用可能です。指定済み管理者としてログオンしている場合、この項は表示されません。）

項目	説明
ユーザ名	管理者ユーザ名
アカウント タイプ	ユーザがネットワーク ディレクトリ サービス（ディレクトリ）として定義されているか、Websense ユーザ アカウント（Websense）として定義されているかを示します。
レポート	管理者にレポート ツールを使用する許可を与えるためには、このチェックボックスにマークを付けます。
ポリシー	フィルタとポリシーを作成し、ロールで管理されているクライアントにポリシーを適用する許可を管理者に与えるためには、このチェックボックスにマークを付けます。 また、優先管理者ロールで、ポリシー許可をもつ管理者は、特定の Websense 構成設定を管理することができます。優先管理者、241 ページを参照してください。
無制限	優先管理者ロールのみが利用可能です。すべての Websense 構成設定とフィルタ ロックを管理する許可を管理者に与えるためには、このチェックボックスにマークを付けます。 条件無し優先管理者だけが、新しい管理者に無制限の許可を与えることができます。
追加	**[管理者の追加]** ページを開きます。管理者の追加、262 ページを参照してください。
削除	管理者リストでマークが付いたすべての管理者をロールから削除します。（条件無し優先管理者だけが 利用可能です。）

3. ロールの [**処理対象クライアント**] を追加 / 削除します。(優先管理者だけが変更できます。指定済み管理者は、ロールに割り当てられたクライアントを表示することができます。)

項目	説明
名前	明示的にロールに割り当てられた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、[クライアント] のページでクライアントを追加する必要があります。指定済み管理タスク、248 ページを参照してください。
追加	[**処理対象クライアントの追加**] のページを開きます。処理対象クライアントの追加、264 ページを参照してください。
削除	条件無し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 リストでマークが付いたすべてのクライアントをロールから削除します。 特定のクライアントは 処理対象クライアント リストからすぐに削除することができません。詳細は、留意事項、266 ページ を参照してください。

4. レポートアクセスを持つこのロールの管理者に利用可能な機能を選択するためには、[**レポート作成の許可**] のエリアを使用します。
   a. レポート許可の一般レベルを選択します :

オプション	説明
すべてのクライアントのレポート	管理者がすべてのネットワーク ユーザのレポートを作成する許可を与えるためには、このオプションを選択します。 このロールの管理者に特定の許可を設定するためには、[レポート作成の許可] エリアの他のオプションを使用します。
処理対象クライアントのみのレポート	このロールに割り当てられた処理対象クライアントのみをレポートするように管理者を制限するためには、このオプションを選択します。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にレポートを限定された管理者は、プレゼンテーション レポート、または [今日] および [履歴] のページでユーザベースのレポートにアクセスすることはできません。また、ログ データベース設定を管理することができません。

b. ロールの適切な管理者に使用を許可するために、各レポート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
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のレポートを行うときだけ、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、98 ページを参照してください。
今日および履歴ページでのレポートの参照	これらのページで インターネット利用状況を示す図の表示を有効にします。今日 : ヘルス、セキュリティ、および値 (AM 12:00 以降)、20 ページ および 履歴 : 最終 30 日、23 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、管理者は、[今日] のページのヘルス アラートと値のエリア、および [履歴] のページの見積もり値のみを表示できます。
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たとき、追加の調査レポート機能を選択することができます。調査レポート、118 ページを参照してください。
調査レポートでのユーザ名の参照	記録されている場合、このロールの管理者がユーザ名を表示することを可能にします。ログ記録のための Filtering Service 設定、310 ページを参照してください。 名前の代わりにシステムによって作成された識別コードだけを表示するためには、このオプションの選択を取り消します。 このオプションは、管理者が調査レポートにアクセスできる場合にだけ利用可能です。
調査レポートをお気に入りに保存	このロールの管理者が使用頻度の高い調査レポートを作成することを可能にします。使用頻度の高い調査レポート、137 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にアクセスできる場合にだけ利用可能です。

オプション	説明
調査レポートのスケジュール	このロールで管理者が、後で、または 繰り返し実行するために、調査レポートをスケジュールすることを可能にします。 調査レポートのスケジュール設定、139 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与えられているときだけ、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 [設定] > [ログ データベース] のページにアクセスすることを可能にします。 ログ データベース管理の設定、326 ページを参照してください。 管理者がすべてのクライアントのレポートを行うときだけ、このオプションは利用可能です。

5. 変更を終了したら、変更をキャッシュし、[指定済み管理] のページに戻るために、[OK] をクリックします。**[すべて保存]** 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

関連トピック :

- ロールの編集、258 ページ
- Websense Manager へのアクセスの有効化、253 ページ

優先管理者が ロールの管理者を指定するために、**[指定済み管理] > [ロールの編集] > [管理者の追加]** のページを使用します。

ご注意 :
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 ログオン中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の組み合わされたレポート許可を持ちます。

指定済み管理者は、管理しているクライアントのインターネット活動に関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、優先管理者は、管理者によって行われた変更をモニタするために監査ログのページを使用するべきです。監査ログの表示とエクスポート、286 ページを参照してください。

1. ディレクトリ アカウントを指定済み管理者に追加する場合、そのディレクトリサービス設定（ディレクトリ サービス、63 ページを参照）がログオン ディレクトリ 設定（ディレクトリ アカウント、253 ページを参照）に一致している Policy Server にログオンしていることを確認してください。

   Websense ユーザ アカウントだけを管理者に追加する場合、どの Policy Server にもログオンできます。

2. **[ディレクトリ アカウント]** で、1 人以上のユーザのチェックボックスにマークを付け、彼らを**選択済み**リストに移動するために、右矢印 (>) ボタンをクリックします。

   > **ご注意：**
   > カスタム LDAP グループは 管理者を追加することはできません。

   お客様の環境が、Active Directory（ネイティブ モード）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、グループ、ドメイン、組織単位名を見つけるために、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、70 ページを参照してください。

3. **[Websense アカウント]** で、1 人以上のユーザのチェックボックスにマークを付け、ハイライトされたユーザを [選択済み] リストに移動するために、右矢印 (>) ボタンをクリックします。

4. このロールの管理者に**許可**を設定します。

オプション	説明
ポリシー	このロールの管理者がポリシーを処理対象クライアントに適用するためには、このオプションをチェックします。また、これは特定の Websense 設定へのアクセス権を与えます。
無制限	すべての Websense 設定へのアクセス権を与えるためには、このオプションをチェックします。 条件なし優先管理者がポリシー許可をもつ優先管理者ロールを管理者に追加するときだけ、このオプションは有効です。
レポート	レポートツールへのアクセス権を与えるためには、このオプションをチェックします。許可された特定のレポート機能を設定するためには、[ロールの編集] のページを使用します。

5. 変更が完了したら、**[OK]** をクリックし、[ロールの編集] のページに戻ります。

6. 変更をキャッシュするために、[ロールの編集] のページで **[OK]** をクリックします。**[すべて保存]** 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

関連トピック：

- 指定済み管理の使用、257 ページ
- ロールの編集、258 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、グループ、ドメイン、組織単位）、コンピュータ、ネットワークは、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。

優先管理者が必要なロールにクライアントを追加するためには、**[指定済み管理] > [ロールの編集] > [処理対象クライアントの追加]** のページを使用します。各クライアントは 1 つのロールにだけ割り当てることができます。

1 つのロールにネットワーク範囲を処理対象クライアントとして割り当てる場合、その範囲内の個々の IP アドレスを他のどのロールにも割り当てることはできません。さらに、ユーザ、グループ、ドメイン、組織単位を、2 つの異なったロールに割り当てることはできません。しかし、ユーザを 1 つのロールに割り当て、ユーザがメンバーであるグループ、ドメイン、組織単位に異なったロールを割り当てることはできます。

ご注意：
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、後でそのグループの個々のユーザをもう 1 つ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、どのクライアント タイプを含めるかを考慮してください。ロールに IP アドレスを追加する場合、このロールの管理者は 指定されたコンピュータの**すべて**の利用状況に関するレポートを作成することができます。ロールにユーザを追加する場合、どのコンピュータが利用されたかにかかわらず、管理者は そのユーザのすべての利用状況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。自身のポリシーを設定することができます。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 レポートを有効にしてください（セルフ レポート、341 ページ を参照）。

お客様の組織が複数の Policy Server を配備し、Policy Server が異なったディレクトリと通信している場合、必ず追加するクライアントを含むディレクトリに接続している Policy Server を選択してください。

ご注意：
同じロールのすべての処理対象クライアントは、同じディレクトリ サービスであることが最善です。

1. ロールのクライアントを選択します：
   - **[ディレクトリ]** で、1 人 または 複数のユーザのチェックボックスにマークを付けます。

     お客様の環境が、Active Directory（ネイティブ モード）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、グループ、ドメイン、組織単位名を見つけるために、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、70 ページを参照してください。
   - **[コンピュータ]** に、このロールに追加するコンピュータの IP アドレスを入力します。
   - **[ネットワーク]** に、ユニットとして追加するコンピュータの範囲の最初と最後の IP アドレスを入力します。
2. クライアントを **[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、[ロールの編集] のページに戻ります。
4. 変更をキャッシュするために、[ロールの編集] のページで **[OK]** をクリックします。**[すべて保存]** をクリックするまで、変更は適用されません。

ロールの競合管理

関連トピック：
- 指定済み管理の使用、257 ページ
- 処理対象クライアントの追加、264 ページ

ディレクトリ サービスでは 同じユーザが複数のグループに属することができます。結果として、複数の指定済み管理ロールによって管理されるグループ内に 1 人のユーザが存在する可能性があります。同じ状況は ドメインと組織単位でも存在します。

さらに、ユーザが 1 つのロールによって管理され、異なったロールによって管理されるグループ、ドメイン、組織単位に属する可能性があります。ロールの両方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、ユーザの管理者がポリシーをそのユーザに適用することがあります。

重複があるために、異なったポリシーが同じユーザ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、**[指定済み管理]** > **[ロールの優先順位の設定]** の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フィルタリング ポリシーを適用します。

1. 優先管理者以外のリスト上のロールを選択します。

   ご注意：
   優先管理者ロールは 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、**[上に移動]**または **[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、変更をキャッシュし、[指定済み管理] のページに戻るために、**[OK]** をクリックします。**[すべて保存]** をクリックするまで、変更は適用されません。

留意事項

関連トピック：

- 指定済み管理の使用、257 ページ
- ロールの編集、258 ページ

指定済み管理ロールを削除する、または ロールから処理対象クライアントを削除する前に、次の情報を確認してください。

ロールの削除

[指定済み管理] のページで、条件無し優先管理者は、使用しないロールを削除することができます。

また、ロールを削除すると、ロールの管理者が [クライアント] のページに追加したすべてのクライアントが削除されます。ロールが削除された後は、それらのクライアントが他のロールによって管理されたネットワーク、グループ、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（フィルタリング順序、80 ページ を参照）。そうでない場合、優先管理者デフォルト ポリシーによって管理されます。

1. **[指定済み管理]** のページで、削除する各ロールの横のチェックボックスにマークを付けます。

   ご注意：
   優先管理者ロールを削除することはできません。

2. **[削除]** をクリックします。
3. [指定済み管理] のページから 選択されたロールが削除されたことを確認してください。**[すべて保存]** をクリックするまで、変更は保持されません。

   次に Websense Manager 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

次の場合、処理対象クライアント リスト（[指定済み管理] > [ロールの編集]）から直接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、ドメイン、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。

Websense Manager にログオンするときに、優先管理者が削除するクライアントを含むディレクトリ サービスと通信する Policy Server と異なった Policy Server を選択した場合、問題が発生する場合があります。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、条件なし優先管理者は、適切なクライアントが削除されることを保証することができます。

1. 削除される処理対象クライアントを含むディレクトリ サービスの Policy Server を選択して、Websense Manager にログオンします。条件なし優先管理者の許可でログオンする必要があります。
2. バナーの**ロール** リストを開き、削除される処理対象クライアントからロールを選択します。
3. 指定済み管理者がポリシーを割り当てたすべてのクライアントのリストを表示するために、**[ポリシーの管理] > [クライアント]** に移動します。

   これには、ロールの処理対象クライアント リストの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、組織単位のメンバーであるクライアント両方が含まれます。
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**ロール**リストを開き、**[優先管理者ロール]** を選択します。
7. **[ポリシーの管理] > [指定済み管理] > [ロールの編集]** 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、[ロールの編集] のページで [OK] をクリックします。**[すべて保存]** をクリックするまで、変更は適用されません。

複数の管理者の Websense Manager へのアクセス

関連トピック：

- 管理者の説明、240 ページ
- Websense Manager へのアクセスの有効化、253 ページ

異なったロールの管理者は、彼らのロール許可が許可するどの作業を行なうためにでも、同時に Websense Manager にアクセスすることができます。例えば、共にポリシー許可を持つロール A と ロール B の管理者が、同時に Websense Manager にログオンすることができます。彼らは異なったクライアントを管理していますから、競合なしでポリシーを作成し、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管理者が同時にログオンする場合、状況は異なります。ポリシー構造と割り当ての一貫性を保持するために、どんな時でも、ポリシー許可で Websense Manager にアクセスすることができるのは、1 つのロールに対して 1 人の管理者だけです。1 番目の管理者がまだログオンしている間に、同じロールのポリシー許可の 2 番目の管理者がログオンしようとする場合、2 番目の管理者は選択することができません。

- 管理者がレポート許可を持っている場合、レポートのためのみに、ログオンしてください。
- 管理者が他のロールに割り当てられている場合、異なったロールにログオンしてください。
- 最初の管理者がログオフした後、再試行してください。

ポリシーとレポートの両方の許可をもつ管理者がレポートを作成するためにログオンしている場合、ロールの他の管理者がポリシー管理作業を行なうことができるように、すぐにポリシー許可を解放するべきです。

▶ バナーで **[ロール]** ドロップダウン リストに移動し、**[ポリシー許可のリリース]** を選択します。

代わりの方法は、それぞれのロールに特別な Websense ユーザ アカウント (Websense ユーザ アカウント、255 ページ を参照) を作成し、そのユーザにレポート許可だけを与えることです。ポリシーとレポートの両方の許可を持つロールの管理者に、それらのログオン資格情報 (ユーザ名とパスワード) を提供します。管理者がレポートを実行する必要があるとき、異なった管理者のためにポリシー アクセスを解放したままにして、レポート管理者としてログオンすることができます。

すべてのロールのフィルタリング制限の定義

関連トピック:

- 管理者の説明、240 ページ
- フィルタ ロックの作成、269 ページ

条件無し優先管理者は、Websense ソフトウェアで、指定済み管理ロールに管理されたすべてのクライアントに対して、カテゴリとプロトコルをブロックする フィルタ ロックを指定することができます。詳細は、フィルタ ロックの作成、269 ページ を参照してください。

これらのロールの管理者は、ポリシーの他のカテゴリとプロトコルにフィルタリング アクションを自由に適用できますが、フィルタ ロックでブロックされているカテゴリとプロトコルは許可されません。

変更が保存されるとすぐに、フィルタ ロックの変更がすべての処理対象クライアントに対して実行されます。変更が有効になったとき、Websense Manager で作業している指定済み管理者は、次にログオンするときまで、フィルタの変更を参照できません。

> **ご注意：**
> 優先管理者ロールから他のロールにフィルタをコピーすると、コピーは フィルタ ロックの制限を引き継ぎます。

優先管理者は フィルタ ロックによって制限されません。彼らは、指定済み管理ロールでブロック および ロックされたカテゴリとプロトコルへのアクセスを許可するポリシーを定義することができます。従って、特別なアクセス権を必要とする個人は、優先管理者ロールによって管理されるべきです。

フィルタ ロックの作成

関連トピック：

- すべてのロールのフィルタリング制限の定義、268 ページ
- カテゴリのロック、270 ページ
- プロトコルのロック、271 ページ

[ポリシーの管理] > [フィルタ ロック] のページで、指定済み管理ロールですべての処理対象クライアントをブロックするカテゴリ または プロトコルを編集するかどうか選択できます。フィルタ ロックでブロックされるすべてのカテゴリ または プロトコルの機能は、**ブロックされ、ロック**されます。

- 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するためには、**[カテゴリ]** ボタンをクリックします。カテゴリのロック、270 ページを参照してください。
- プロトコルをブロックおよびロックし、プロトコルをログ記録するためには、**[プロトコル]** ボタンをクリックします。プロトコルのロック、271 ページを参照してください。

カテゴリのロック

関連トピック:

- すべてのロールのフィルタリング制限の定義、268 ページ
- フィルタ ロックの作成、269 ページ
- プロトコルのロック、271 ページ

指定済み管理ロールのすべてのメンバーに対してブロックおよびロックするカテゴリを選択するためには、[**ポリシーの管理**] > [**フィルタ ロック**] > [**カテゴリ**] のページを使用します。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ができます。

1. ツリーで、カテゴリを選択します。

   指定済み管理ロールでは、優先管理者によって作成されたカスタム カテゴリへアクセスできません。従って、カスタム カテゴリは このツリーに表示されません。
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
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。
キーワードのロック	各ロールのこのカテゴリに定義されたキーワード ベースのアクセスを ブロック および ロックします。
ファイル タイプの ロック	このカテゴリのサイトで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 ロックされる各ファイル タイプのチェックボックスにマークを付けます。 優先管理者によって作成されたカスタム ファイル タイプは、指定済み管理ロールで利用できるため、このリスト上に含められます。
サブカテゴリに適用	同じ設定を このカテゴリのすべてのサブ カテゴリに適用します。

   適切であるなら、すぐにすべてのカテゴリの選択された要素をブロック および ロックすることができます。ツリーで [**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。その後、[**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、変更をキャッシュし、[フィルタ ロック] のページに戻るために、[OK] をクリックします。[**すべて保存**] 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

関連トピック：

- すべてのロールのフィルタリング制限の定義、268 ページ
- フィルタ ロックの作成、269 ページ
- カテゴリのロック、270 ページ

指定済み管理ロールで管理されるすべての処理対象クライアントに対して、選択されたプロトコルへのアクセスをブロック および ロックし、ログ記録をロックするためには、**[ポリシーの管理]** > **[フィルタ ロック]** > **[プロトコル]** のページを使用します。

ご注意：
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しています。ログ記録に少なくとも 1 つのプロトコル フィルタが設定されていない場合、プロトコル使用状況アラートを作成することができません。フィルタ ロックで **[プロトコルのロックのログ記録]** 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作成されます。プロトコル使用状況アラートの設定、295 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。

   指定済み管理ロールから、優先管理者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。従って、カスタム プロトコルはこのツリーに表示されます。
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
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と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。
プロトコルのロックのログ記録	このプロトコルへのアクセス情報をログ記録し、指定済み管理者がログ記録を無効にすることを防止します。
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。

3. 変更を終了したら、変更をキャッシュし、[フィルタ ロック] のページに戻るために、[OK] をクリックします。**[すべて保存]** をクリックするまで、変更は適用されません。

12 Websense サーバーの管理

関連トピック：

- Websense 製品コンポーネント、274 ページ
- Policy Server の動作、279 ページ
- 監査ログの表示とエクスポート、286 ページ
- Websense サービスの停止と起動、288 ページ
- アラート、289 ページ
- Websense データのバックアップと復元、297 ページ

インターネット使用フィルタリングは、複数の Websense ソフトウェア コンポーネント間の対話を必要とします：

- インターネット アクセスのユーザ要求が、Network Agent または サードパーティ社統合製品によって受信されます。
- 要求を処理するために Websense Filtering Service に送信されます。
- Filtering Service は、要求に応答するとき、適切なポリシーを適用するために、Policy Server および Policy Broker と通信します。

ほとんどの環境では、1 つの Policy Server があるか、または 複数の Policy Server があるかに関わらず、1 つの Policy Database がクライアント、フィルタ、ポリシー、一般設定情報を保持します。

Websense Manager の各インスタンスが、1 つの Policy Database と関連付けられており、そのデータベースと関連付けられた Policy Server を設定するために使用することができます。

Websense Manager で行われたポリシーの設定は、中央のデータベースに保存され、ポリシー情報はその Policy Database と関連付けられたすべての Policy Server で自動的に有効になります。

Websense 製品コンポーネント

関連トピック：

- Filtering コンポーネント、275 ページ
- レポートコンポーネント、277 ページ
- ユーザ識別コンポーネント、278 ページ
- Policy Server の動作、279 ページ
- Websense サービスの停止と起動、288 ページ
- 現在のシステム ステータスの確認、296 ページ

Websense ソフトウェアは、ユーザ識別、インターネット フィルタリング、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、お客様がフィルタリング環境を理解し、管理するための手助けとなるために、そのコンポーネントの概要を提供します。

主な Websense コンポーネントは 次のとおりです：

- Policy Database
- Policy Broker
- Policy Server
- Filtering Service
- Network Agent
- マスタ データベース
- Websense Manager
- Usage Monitor
- User Service
- Log Server
- ログ データベース

また、Websense ソフトウェアはオプションの次の透過的識別エージェントを含みます：

- DC Agent
- RADIUS Agent
- eDirectory Agent
- Logon Agent

追加のオプション コンポーネントには 次が含まれます：

- Remote Filtering Server
- Remote Filtering Client
- Websense Content Gateway

Filtering コンポーネント

コンポーネント	説明
Policy Database	Websense ソフトウェア設定とポリシー情報を保存します。
Policy Broker	ポリシーおよび一般設定情報のために、Websense コンポーネントからの要求を管理します。
Policy Server	• 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。 • フィルタリング インターネット要求で使用するための、設定データを Filtering Service に連絡します。 Websense Manager で、Policy Server を設定します (Policy Server の動作、279 ページ を参照)。 ポリシーおよびほとんどの設定は、Policy Database を共有する Policy Server 間で共有されます (複数の Policy Server 環境での動作、281 ページ を参照)。
Filtering Service	Network Agent または サードパーティ社統合製品と接続し、インターネット フィルタリングを提供します。ユーザがあるサイトを要求したとき、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がフィルタされ、記録されるためには、Filtering Service が実行されている必要があります。 • 各 Filtering Service のインスタンスが、Websense マスタ データベースの自身のコピーをダウンロードします。 Websense Manager で フィルタリングと Filtering Service の動作を設定します (インターネット使用のフィルタ、35 ページ および Websense フィルタリング設定の構成、56 ページ を参照)。
Network Agent	• フィルタリングとログ記録機能を拡張 • プロトコル管理の有効化 • スタンドアロン環境でのフィルタリングの有効化 詳細は、ネットワークの構成、343 ページ を参照してください。

コンポーネント	説明
マスタ データベース	• 90 以上のカテゴリとサブカテゴリに分類された、3 千 6 百万以上のウェブサイトを含みます。 • フィルタリング プロトコルに使用するための100以上のプロトコル定義を含みます。 インターネット フィルタリングを有効化するためには、Websense マスタ データベースをダウンロードし、データベースが最新版であることを確認してください。マスタ データベースが 2 週間以上古くなると、フィルタリングが行われません。詳細は、Websense マスタ データベース、30 ページ を参照してください。
Websense Manager	Websense ソフトウェアへの設定および管理インターフェースを提供します。 インターネット アクセス ポリシーを定義 および カスタマイズし、フィルタリング クライアントを追加 または 削除し、Websense ソフトウェア コンポーネントを設定するためなどに、Websense Manager を使用します。 詳細は、Websense Manager での作業、15 ページ を参照してください。
Usage Monitor	インターネット使用状況に基づいたアラートを有効にします。 Usage Monitor が、URL カテゴリとプロトコルのアクセスを追跡し、設定したアラート動作に従い、アラート メッセージを作成します。 詳細は、アラート、289 ページ を参照してください。
Remote Filtering Client	• ネットワーク ファイアウォールの外側のクライアント コンピュータに配置します。 • フィルタされるクライアントであるコンピュータを識別し、Remote Filtering Server と通信します。 詳細は、リモート クライアントのフィルタ、159 ページ を参照してください。
Remote Filtering Server	• ネットワーク ファイアウォールの外側のクライアントをフィルタリング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、リモート クライアントのフィルタ、159 ページ を参照してください。

コンポーネント	説明
Websense Content Gateway	• 強固なプロキシとキャッシュ プラットホームを提供します。 • 以前は分類されていなかった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。 リアルタイム オプションによるコンテンツの分析、147 ページを参照してください。
Websense Security Gateway	標準的な Websense Content Gateway 機能の他に、次の機能があります : • 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、プロキシ回避)。 • 脅威のカテゴリを割り当てるために、ファイル コンテンツを検査します (例えば、ウイルス、トロイの木馬、ワーム)。 • ある特定の Web ページからアクティブなコンテンツを取り除きます。 リアルタイム オプションによるコンテンツの分析、147 ページを参照してください。

レポートコンポーネント

コンポーネント	説明
Log Server	次を含むインターネット要求データを記録します : • 要求ソース • 要求に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、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を保存します。 調査レポート、プレゼンテーション レポート、および Websense Manager 内で [今日] および [履歴] のページの図を有効にするためには、Log Server を Windows コンピュータにインストールする必要があります。 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 (ログ記録のための Filtering Service 設定、310 ページ を参照)。
ログ データベース	Websense レポート 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。

ユーザ識別コンポーネント

コンポーネント	説明
User Service	• ディレクトリ サービスと通信します。 • フィルタリング ポリシーを適用するときに使用するために、「グループ対ユーザ」と「ユーザ対ドメイン」の関係を含めて、ユーザ関連の情報を Policy Server と Filtering Service に伝達します。 Websense 透過的識別エージェントをインストールし、構成している場合（透過的識別、205 ページ を参照）、User Service がユーザ ログオン セッション情報の判定を補助し、この情報は Filtering Service にユーザ名と IP アドレスの関係を提供するために使用します。 Websense クライアントとしてユーザおよびグループを追加するとき（クライアントの追加、69 ページ を参照）、User Service がディレクトリ サービスから Websense Manager に名前とパス情報を提供します。 ディレクトリ サービス アクセスを設定するための情報は、ディレクトリ サービス、63 ページ を参照してください。
DC Agent	• Windows ベースのディレクトリ サービスのユーザに対して、透過的ユーザ識別を行います。 • Websense ソフトウェアに、フィルタリング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。 詳細は、DC Agent、216 ページ を参照してください。
Logon Agent	• Linux と Windows ネットワーク上での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。 • 発生したときに、ユーザ ログオン セッションを検出します。 個々のユーザ ログオン セッションが Websense ソフトウェアによって取得され、直接処理されることを保証するために、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ます。 詳細は、Logon Agent、219 ページ を参照してください。

コンポーネント	説明
eDirectory Agent	• 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 アドレスを関連づけ、Filtering Service に情報を提供するために、User Service と共に動作します。 詳細は、eDirectory Agent、227 ページ を参照してください。
RADIUS Agent	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に対して、透過的識別を有効にします。 詳細は、RADIUS Agent、222 ページ を参照してください。

Policy Database について

Websense Policy Database 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、指定済み管理設定を含む) および Websense Manager で指定されたグローバル設定の両方を保存します。1 つの Policy Server インスタンス専用の設定は別に保存されます。

ほとんどの複数の Policy Server 環境では、1 つの Policy Database がポリシーと複数の Policy Server の一般設定データを保持します。

1. 起動時に、各 Websense コンポーネントは、Policy Broker を介して Policy Database からの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、しばしば Policy Database に対して変更を調査します。
3. 管理者が Websense Manager で変更を行い、[すべて保存] をクリックするたびに、Policy Database は更新されます。
4. Policy Database の変更の後、各コンポーネントはその機能に影響する変更を要求し、受信します。

重要な設定とポリシー情報を保護するために、通常の Policy Database のバックアップをとってください。詳細は、Websense データのバックアップと復元、297 ページ を参照してください。

Policy Server の動作

Policy Server は、ポリシー情報を管理し、ポリシーの実行を支援するために Filtering Service と通信する Websense ソフトウェア コンポーネントです。ま

た、Policy Server は、他のコンポーネントを識別し、それらの位置とステータスを追跡します。

Websense 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。

- Websense Manager が Policy Server と通信するように設定されるまで、Websense Manager にログオンすることはできません。
- インストールされたWebsenseソフトウェアに複数のPolicy Serverが含まれる場合、ログオン時に Policy Serverインスタンスを選択することができます。
- Websense 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。

デフォルトで、Websense Manager と中央の Policy Server インスタンス間の通信が、Websense Manager インストール中に確立されます。

ほとんどの環境では、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 と 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、Policy Server の複数のインスタンスをインストールすることは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、Websense Manager で各インスタンスを追加します (Policy Server インスタンスの追加と編集、280 ページ を参照)。

Policy Server インスタンスの追加と編集

Websense Manager に、Policy Server のインスタンスを追加するか既存の Policy Server を設定するか、削除するためには、**[設定]** > **[Policy Server]** のページを使用します。

Policy Server のインスタンスを追加する方法は、次のとおりです :

1. **[追加]** をクリックします。[Policy Server の追加] のページが開きます。
2. **[サーバーの IP または名前]** フィールドに、Policy Server コンピュータの IP アドレスまたはホスト名を入力します。
3. Websense Managerがそのpolicy Serverインスタンス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 **55806** です。
4. Policy Server のページに戻るために、**[OK]** をクリックします。新しい Policy Server インスタンスがリストに表示されます。
5. Policy Server のページに対するすべての変更をキャッシュするために、**[OK]** をクリックします。**[すべて保存]** をクリックするまで、変更は適用されません。

Policy Server インスタンスを編集するためには (例えば、Policy Server コンピュータ IP アドレスまたは名前を変更する場合)、Policy Server リストから IP アドレスまたはホスト名を選択し、**[編集]** をクリックします。

Policy Server のインスタンスを削除するためには、Policy Server リストから IP アドレスまたはホスト名を選択し、**[削除]** をクリックします。[削除] をクリックすると、Websense Manager から Policy Server インスタンスを削除し

ますが、Websense Policy Server サービスをアンインストールするか、または停止することはありません。リストされた Policy Server のインスタンスが 1 つだけである場合、そのインスタンスを削除することはできません。

複数の Policy Server 環境での動作

多数のユーザの分散環境では、複数の Policy Server 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。

- 現在の負荷に依存して、同じクライアントが異なった Policy Server によって管理されることを許可する設定を実行している場合、時間ベースのポリシー アクションを実行**しないでください**:
  - パスワード アクセス
  - 確認
  - 割り当て時間

  これらの機能と関連したタイミング情報は、Policy Server 間で共有されません。クライアントに、意図したインターネット アクセスを与えることができません。

  他のポリシーがクライアントに適用されない場合、デフォルト ポリシーが実行されます。クライアントが 1 つ以上の Policy Server によって管理されている場合、デフォルト ポリシーで時間ベースのアクションを適用するカテゴリ フィルタを実行していないことを確認してください。
- ポリシー情報は Policy Database に保存されるため、**[すべて保存]** をクリックしたとき、ポリシーの変更は すべての Policy Server 間で自動的に共有されます。
- また、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) が Policy Server 間で共有されます。
- 1つのPolicy Serverに指定された設定 (Filtering Serviceと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。

1 つの Policy Server インスタンスに適用される 設定を確認するか、設定するために、Websense Manager で Policy Server を切り 替えるためには、次を 行います :

1. Websense バナーで **Policy Server** リストを展開し、IP アドレスを選択します。
2. 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、変更リストが表示されます。次のどちらかを実行します。
   - 変更を保存し、現在の Policy Server からログアウトするためには、**[すべて保存とログアウト]** をクリックします。
   - 変更を破棄し、現在の Policy Server からログアウトするためには、**[変更を破棄とログアウト]** をクリックします。
   - Policy Server の設定を継続するためには、**[戻る]** をクリックします。

   保存された変更がない場合、直接ログオン スクリーンに移動します。
3. ログオン画面で、選択された Policy Server にログオンするために、ユーザ名とパスワードを入力し、**[ログオン]** をクリックします。

Policy Server IP アドレスの変更

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**。また、Websense Manager がコンピュータにインストールされている場合、これには Apache2Websense サービスと ApacheTomcatWebsense サービスが含まれます。

IP アドレスを変更した後、フィルタリングを再開する前に、Websense Manager、Policy Server、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: Websense Manager 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、Websense Manager を更新します。

1. Websense Manager コンピュータ上で、**Apache2Websense** サービスと **ApacheTomcatWebsense** サービスを停止します（必要な場合）。

   Websense Manager 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、Apache サービスはすでに停止されているはずです。
2. 次のディレクトリに移動します：
   - Windows:

     `C:\Program Files\Websense\tomcat\conf\Catalina\localhost\`
   - Linux:

     `/opt/Websense/tomcat/conf/Catalina/localhost/`
3. **mng.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（メモ帳 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 度現れます：**ps/default/host** の値 および **psHosts** の値。
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、Apache サービスを再起動しないでください。

ステップ 2: Policy Server 設定を更新します

Policy Server 設定ファイル および Websense コンポーネント間の通信を設定するために使用する初期化ファイルを更新します。

1. もし行っていない場合、Policy Server 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、288 ページ を参照）。
2. Websense **bin** ディレクトリに移動します。
   - Windows:

     `C:\Program Files\Websense\bin`

- Linux

  `/opt/Websense/bin`

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: ログ データベース接続の確認

ログ データベースに対する 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. **[スタート] > [設定] > [コントロール パネル] > [管理ツール] > [データ ソース (ODBC)]** に移動します。
2. **[システム DSN]** タブ上で、適切なデータソース名（デフォルトは、**wslogdb70**）を選択し、**[構成]** 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、**[次へ]** をクリックします。
4. データベースに接続するために使用される資格証明を入力し、**[次へ]** 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 **[データソースのテスト]** をクリックします。

ご注意：
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た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。正常にコンピュータ上のすべての Websense サービスが再起動されたことを確認します。

2. Policy Server を設定するために使用される Websense Manager が他のコンピュータにインストールされている場合、そのコンピュータで **Apache2Websense** サービスと **ApacheTomcatWebsense** サービスを再起動します。

ご注意：
Websense Manager 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

Filtering Service は、インターネット活動をフィルタするために、Network Agent またはサードパーティ社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き、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、サイトがどのようにフィルタされるかを決定する適用可能なポリシーを使用します。

各 Filtering Service のインスタンスは、どのようにインターネット要求をフィルタするべきかを決定するために、Websense マスタ データベースの自身のコピーをダウンロードします。

また、記録され、レポートで使用できるように、Filtering Service は Log Server にインターネット活動についての情報を送信します。

Websense Manager にログオンするとき、[ステータス] > [今日] のページの **[Filtering Service の要約]** に、現在の Policy Server に関連付けられた各 Filtering Service のインスタンスの 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

各 Filtering Service インスタンスのステータスを確認するためには、**[ステータス] > [今日] > [Filtering Service の詳細]** のページを使用します。

ページに次がリストされます：

- 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には無関係
- Filtering Service のバージョン

  適用されたすべてのホットフィックスも含めて、これは、Websense ソフトウェア バージョンと一致している必要があります。
- Filtering Service コンピュータ上で稼働しているオペレーティング システム
- Websense ソフトウェア プラットホーム

これは、Websense ソフトウェアがスタンド アローン モードで実行しているか、サードパーティ社製品と統合されているかを示します。

- 選択された Filtering Service と通信するすべての Network Agent インスタンスの IP アドレスとステータス。

[今日] のページに戻るためには、**[閉じる]** をクリックします。

マスタ データベース ダウンロード ステータスの確認

ネットワーク内の各 Filtering Service のインスタンスは、マスタ データベースの自身のコピーをダウンロードします。Websense Manager で作業しているとき、[ステータス] > [今日] のページの [ヘルス アラートの要約] に、マスタ データベースのダウンロードが進行中であるか、ダウンロードに失敗した場合、ステータス メッセージが表示されます。

最近の または 進行中のデータベースのダウンロードの詳細情報を見るためには、[今日] のページのツールバー上で **[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 ページには、現在の Policy Server に関連付けられた Filtering Service のインスタンスの項目が含まれます。

最初に、[データベースのダウンロード] のページには、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、ダウンロードが成功したかどうかを示す簡単なダウンロード要約を表示します。この要約の表示から、次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 (**[更新]** をクリック)。
- リストされたすべての Filtering Service インスタンスのためにデータベースのダウンロードを開始する (**[すべて更新]** をクリック)。
- 1 つ または すべての進行中の更新をキャンセルする。

選択された Filtering Service で更に詳細なデータベース ダウンロードの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。

- 選択された 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。
- 選択された Filtering Service のデータベースのダウンロードを手動で開始するためには、**[更新]** をクリックします。

データベースのダウンロード中に、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、Websense Manager で作業を続けるためには、**[閉じる]** をクリックします。

レジューム可能なマスタ データベースのダウンロード

マスタ データベースの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を再開するよう試みます。Filtering Service がダウンロード サーバーと再接続可能である場合、それが中断されたところからダウンロードを再開します。

失敗した、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ダウンロードを再開しません。その代わりに、最初から処理を再開します。

1. Websense Manager で **[ステータス]** > **[今日]** に移動し、**[データベースのダウンロード]** を選択します。
2. 中断している処理を停止するためには、**[すべて更新の中止]** をクリックします。
3. 最初からダウンロード処理を再起動するためには、Filtering Service インスタンスを選択し、**[更新]** または **[すべて更新]** をクリックします。

監査ログの表示とエクスポート

Websense ソフトウェアは、どの管理者が Websense Manager にアクセスしたか、ポリシーおよび設定を変更したか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（優先管理者、241 ページ を参照）。

指定済み管理者は、管理しているクライアントのインターネット活動に関して重要な管理ができます。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、必要である場合に、その選択された部分を 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、**[ステータス]** > **[監査ログ]** のページを使用します。

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削除することはありません。

[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上のページング ボタンを使用します。

ログは次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 ダイアログ ボックス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
日付	タイムゾーンで調整された変更の日付と時間。 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、日付と時間の設定が同期していることを確認してください。
ユーザ	変更を行った管理者ユーザ名。

列	説明
サーバー	変更で影響を受けた 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 [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表示されます。
ロール	変更の影響を受けた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た処理対象クライアントとして割り当てられたクライアントに明示的に影響を与える場合、その変更は 優先管理者ロールに影響を与えると表示されます。変更が、ロールに割り当てられたネットワーク範囲、グループ、ドメイン、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されます。
タイプ	ポリシー、カテゴリ フィルタ、ログオン / ログオフのような変更された設定項目。
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ための識別名。
アクション	追加、削除、変更、ログオン などの行われた変更の種類。
前回	変更前の値。
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 レコードには表示されません。

監査ログレコードをエクスポートするためには、次を行います :

1. **[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ためには、**[最新 60 日間]** を選択します。

2. **[実行]** をクリックします。

   Websense Manager を実行しているコンピュータに 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。ファイルとして保存 または 印刷するためには、Excel のオプションを使用します。

   Websense Manager を実行しているコンピュータに 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

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。

> **ご注意：**
> 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は、ダウンロードが完了するまで、実行を停止しません。

すべての Websense サービスを停止する場合、常に次に示される順序で、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 と関連がない場合、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、常に次に示される順序で、サービスを起動してください：

1. Websense Policy Database
2. Websense Policy Broker
3. Websense Policy Server

Windows

1. Windowsサービス ダイアログボックスを開きます（**[スタート]**>**[設定]**>**[コントロールパネル]**>**[管理ツール]**>**[サービス]**）。
2. Websenseサービスの名前を右クリックし、**[停止]**または**[開始]**を選択します。

Linux

Linux コンピュータでは、次の手順を使用することで、すべてのサービスは一緒に停止し、起動します。

1. **/opt/Websense** ディレクトリに移動します。
2. 次のコマンドで Websense サービス ステータスをチェックします：
   - `./WebsenseAdmin status`
3. 次のコマンドで、すべての Websense サービスを停止、起動、再起動します：
   - `./WebsenseAdmin stop`
   - `./WebsenseAdmin start`

- `./WebsenseAdmin restart`

警告
kill を Websense サービスを停止するために使用しないでください。サービスを破損する場合があります。

アラート

関連トピック：

- 制限の管理、290 ページ
- 一般のアラート オプションの設定、290 ページ
- システム アラートの設定、292 ページ
- カテゴリ使用状況アラートの設定、293 ページ
- プロトコル使用状況アラートの設定、295 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使用状況の両方についての追跡および管理を容易にするために、優先管理者は、選択されたイベントが発生したとき、アラートを送信するように設定することができます。

- **システム アラート**：サブスクリプションの状態とマスタ データベースの動作に関する通知。
- **使用状況アラート**：特定のカテゴリまたはプロトコルのインターネット使用状況が、設定された閾値に到達した場合の通知。

アラートは、電子メール、スクリーン上のポップアップ メッセージ (Windows Messenger **net send**)、または SNMP メッセージによって、選択された受信者に送信することができます。

ご注意：
スクリーン上のポップアップ アラートは Linux コンピュータに送信することはできません。しかし、Samba クライアントが Linux コンピュータ上にインストールされている場合は、Policy Server を実行している Linux コンピュータから Windows コンピュータに送信することができます。『配備ガイド』を参照してください。

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対して作成することができます。

制限の管理

関連トピック：

- アラート、289 ページ
- 一般のアラート オプションの設定、290 ページ
- カテゴリ使用状況アラートの設定、293 ページ
- プロトコル使用状況アラートの設定、295 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作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のユーザ要求によって送信されるアラート数の制限を指定するためには、**[使用状況タイプごとの日次アラートの最大数]** を使用します。詳細は、一般のアラート オプションの設定、290 ページ を参照してください。

また、閾値限界を各カテゴリおよびプロトコルの使用状況アラートごとに設定できます。例えば、10 の閾値限界をあるカテゴリに設定した場合、そのカテゴリの要求が 10 になった後に、アラートは作成されます（すべてのクライアントの合計）。詳細は、カテゴリ使用状況アラートの設定、293 ページ および プロトコル使用状況アラートの設定、295 ページ を参照してください。

日次アラートの最大数は 20、カテゴリ アラートの閾値は 10 とした場合を考えてください。管理者は、カテゴリ 要求が閾値を超えた最初の 20 回だけ アラートを受け取ります。これは、最初の 200 回の発生だけがアラート メッセージを発生させることを意味します（アラートの最大数 20 と 閾値 10 の掛け算）。

一般のアラート オプションの設定

関連トピック：

- アラート、289 ページ
- システム アラートの設定、292 ページ
- カテゴリ使用状況アラートの設定、293 ページ
- プロトコル使用状況アラートの設定、295 ページ

マスタ データベース カテゴリの更新などの種々のシステム イベント、および インターネットの使用が定義された閾値を超えたなどのサブスクリプション問題を、Websense ソフトウェアは 管理者に通知することができます。

下記の希望する通知方法を選択し、設定するために、**[設定]** > **[アラートと通知]** > **[アラート]** のページを使用します。その後、[設定] > [アラートと通知] の他のページを使用して、受信するアラートを有効にします。

1. 各カテゴリおよびプロトコルの使用状況アラートの毎日作成されるアラートの合計数を制限するためには、**[使用状況タイプごとの日次アラートの最大数]** に値を入力します。

   例えば、スポーツ カテゴリのサイトに誰かが 5 回要求した毎に送信されるように、使用状況アラート（閾値）を設定します。ユーザ数とインターネット使用パターンによっては、毎日何百というアラートを作成することがあります。

   [使用状況タイプごとの日次アラートの最大数] に 10 を入力した場合、スポーツ カテゴリのためのアラート メッセージは毎日 10 回だけ作成されます。この例で、これらのメッセージはスポーツ サイトのために最初の 50 回の要求に対して警告します（アラート毎に 5 の要求 と 10 のアラートの掛け算）。

2. 電子メールによってアラートと通知を配信するためには、**[電子メール アラートを有効にする]** チェックボックスにマークを付けます。その後、これらの電子メール設定を行います。

SMTP サーバーの IP または名前	電子メールのアラートをルーティングする SMTP サーバーの IP アドレス または 名前。
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。
管理者の電子メール アドレス (To)	電子メール アラートの受信者の電子メールアドレス。
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 別個のラインにある必要があります。

3. 特定のコンピュータ上にポップアップ メッセージを表示するためには、**[ポップアップ アラートを有効にする]** チェックボックスにマークを付けます。その後、最高 50 人までの**受信者**の IP アドレス または コンピュータ名を、別個のラインにそれぞれ入力します。

   ご注意：
   ポップアップ アラートは Linux コンピュータに送信することはできません。しかし、Samba クライアントが Linux コンピュータ上にインストールされている場合は、Policy Server を実行している Linux コンピュータから Windows コンピュータに送信することができます。『配備ガイド』を参照してください。

4. 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、**[SNMP アラートの有効化]** チェックボックスにマークを付けます。その後、SNMP Trap システムの情報を提供します。

コミュニティ名	SNMP Trap サーバー上のコミュニティ名。
サーバーの IP または名前	SNMP Trap サーバーの IP アドレス または 名前。
ポート	SNMP メッセージが使用するポート番号。

5. 作業が終了したら、**[OK]** をクリックして、変更をキャッシュします。**[すべて保存]** 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

関連トピック：

- アラート、289 ページ
- 一般のアラート オプションの設定、290 ページ
- 現在のシステム ステータスの確認、296 ページ

Websense Manager は、**[ステータス] > [アラート]**（詳細情報）のページで、詳細なシステム ヘルスとステータス情報を表示します（現在のシステム ステータスの確認、296 ページ に記述）。

管理者が Websense Manager にログオンしていないときに、データベースのダウンロードの失敗 または 期限が切れようとしているサブスクリプションなどの重要なシステムイベントを通知するために、Websense システム アラートを、電子メール、ポップアップ メッセージ、または SNMP Trap システムを使用して、配信されるように設定してください。

Websense 管理者に対してこれらのアラートを送信する方法 および 送信するアラートを選択するためには、[設定] タブの **[アラートと通知] > [システム]** のページを使用します。

1. 各アラートで使用される配信方法にマークを付けます。[アラート] ページでどの方法が有効化されているかに依存して、**電子メール**、**ポップアップ**、**SNMP** を選択することができます。

> **ご注意：**
> アラートの作成とともに、マスタ データベースのダウンロード失敗、および サブスクリプション レベルの超過についての情報は Windows Event Viewer (Windows のみ) および Websense.log ファイル (Windows および Linux) に記録されます。

アラートは次のイベントで利用可能です：

- 1 週間以内にサブスクリプションが失効します。
- Search Filtering でサポートされたサーチ エンジンが変更されました。
- Websense マスタ データベースのダウンロードが失敗しました。
- マスタ データベースからカテゴリ または プロトコルが追加されたか、削除されました。
- 現在のユーザはサブスクリプションで既定されているユーザ数を超えています。
- 現在のユーザ数がサブスクリプションで規定されているユーザ数の 90% に到達しました。
- 1ヶ月以内にサブスクリプションが失効します。
- Websense マスタ データベースが更新されました。

2. 作業が終了したら、[OK] をクリックして、変更をキャッシュします。[**すべて保存**] 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

関連トピック：

- アラート、289 ページ
- 制限の管理、290 ページ
- 一般のアラート オプションの設定、290 ページ
- カテゴリ使用状況アラートの追加、294 ページ

特定の URL カテゴリのインターネット使用状況が定義された閾値に達したとき、Websense ソフトウェアは お客様に通知することができます。カテゴリに対する 許可要求 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、カテゴリに対して制限を与えるかどうかを決定するために、許可されたショッピング カテゴリのサイトに対する 50 回の要求毎に、アラートを発生させる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を調べるために、ブロックされる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。

すでに設定されたアラートを表示するか、使用状況アラートを追加 / 削除するためには、[設定] タブの [**アラートと通知**] > [**カテゴリ使用状況**] の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、それぞれの閾値、選択されたアラート手段を知るためには、[**許可されたカテゴリの使用状況アラート**] および [**ブロックされたカテゴリの使用状況アラート**] を表示します。

2. [カテゴリ使用状況アラートの追加] のページ（カテゴリ使用状況アラートの追加、294 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ためには、下の適切なリストで **[追加]** をクリックします。
3. そのリストから希望するカテゴリを削除するためには、そのチェックボックスにマークを付け、適切なリストの下で **[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、[カテゴリの使用状況アラート] のページに戻ります。**[すべて保存]** 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

関連トピック：

- アラート、289 ページ
- 一般のアラート オプションの設定、290 ページ
- カテゴリ使用状況アラートの設定、293 ページ

[カテゴリの使用状況アラート] のページで [追加] をクリックすると、**[カテゴリ使用状況アラートの追加]** のページが表示されます。ここで、使用状況アラートで使用する新しいカテゴリを選択し、これらのアラートの閾値を設定し、アラート手段を選択することができます。

1. 同じ閾値とアラート手段を追加するためには、各カテゴリの横のチェックボックスにマークを付けます。

   ご注意：
   ログ記録から除外されているカテゴリの使用状況アラートは追加できません。ログ記録のための Filtering Service 設定、310 ページを参照してください。

2. アラートが作成される要求数を選択することで、**[しきい値]** を設定します。
3. これらのカテゴリの希望するアラート手段（**電子メール**、**ポップアップ**、**SNMP**）のチェックボックスにマークを付けます。

   アラート ページで有効にしたアラート手段（一般のアラート オプションの設定、290 ページ を参照）だけが選択できます。
4. 変更をキャッシュし、[カテゴリ 使用状況アラート] のページ（カテゴリ使用状況アラートの設定、293 ページ 参照）に戻るためには、**[OK]** をクリックします。**[すべて保存]** 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

関連トピック：
- アラート、289 ページ
- 制限の管理、290 ページ
- 一般のアラート オプションの設定、290 ページ
- プロトコル使用状況アラートの追加、295 ページ

特定のプロトコルのインターネット使用状況が定義された閾値に達したとき、Websense ソフトウェアは お客様に通知することができます。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与えるかどうかを決定するために、許可されている特定のインスタント メッセージ送信プロトコルの 50 回の要求毎に、アラートを発生させる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の使用ポリシーに適合しているかを調べるために、ブロックされている特定の P2P ファイル共有プロトコルの 100 回の要求毎に、アラートを受信することを希望されるかもしれません。

すでに設定されたアラートを表示するか、使用状況アラートのプロトコルを追加 / 削除するためには、[設定] タブの **[アラートと通知]** > **[プロトコル使用状況アラート]** の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、それぞれの閾値、選択されたアラート手段を知るためには、**[許可されたプロトコルの使用状況アラート]** および **[ブロックされたプロトコルの使用状況アラート]** を表示します。
2. [プロトコル使用状況アラートの追加] のページ (プロトコル使用状況アラートの追加、295 ページ を参照) を開いて アラートにプロトコルを追加するためには、下の適切なリストで **[追加]** 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、適切なリストの下で **[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、[プロトコル使用状況アラート] のページに戻ります。**[すべて保存]** 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

関連トピック：
- アラート、289 ページ
- 一般のアラート オプションの設定、290 ページ
- プロトコル使用状況アラートの設定、295 ページ

使用状況アラートに使用する新しいプロトコルを選択し、これらのアラートの閾値を設定し、アラート手段を選択するためには、**[プロトコル使用状況アラート]** > **[プロトコル使用状況アラートの追加]** のページを使用します。

1. 同じ閾値とアラート手段を追加するためには、各プロトコルの横のチェックボックスにマークを付けます。

   ご注意：
   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す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、プロトコルを記録するプロトコル フィルタによって管理されたクライアントの使用状況を反映するだけです。

2. アラートが作成される要求数を選択することで、**[しきい値]** を設定します。
3. これらのプロトコルで希望するアラート手段（**電子メール**、**ポップアップ**、**SNMP**）のチェックボックスを選択します。

   アラート ページで有効にしたアラート手段（一般のアラート オプションの設定、290 ページ を参照）だけが選択できます。
4. 変更をキャッシュし、[プロトコル使用状況アラート] のページ（プロトコル使用状況アラートの設定、295 ページ を参照）に戻るためには、**[OK]** をクリックします。**[すべて保存]** 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

Websense ソフトウェアの健全性に影響を与える問題の情報を発見するために、**[ステータス]** > **[アラート]** のページを使用し、トラブルシューティング ヘルプを参照し、Websense マスタ データベースの最近のリアルタイム更新の詳細を確認します。

[アクティブなアラート] リストには、モニタされた Websense ソフトウェア コンポーネントのステータスが表示されます。

- 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 **[現在モニタ中の内容]** をクリックします。
- 問題を解決するためには、エラーあるいは警告メッセージの隣りの **[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ためには、**[詳細]** をクリックします。お客様の組織で、Log Server、Network Agent、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、関連するアラートを非表示にするようにチェックボックスにマークを付けます。完了したら、変更を実行するために **[OK]** をクリックします。

詳細 オプションを非表示にするためには、再度 [**詳細**] をクリックします。

[**リアルタイム データベース更新**] リストは、Websense マスタ データベースの緊急更新についての情報を提供し、次を表示します :

- 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マスタ データベース更新に追加して発生し、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毎時間チェックします。

Websense Web Security ユーザのために、アラート ページの 3 番目のリストに次が含まれます : **リアルタイム セキュリティ更新** このリストは リアルタイム データベース更新 リストと同じ形式ですが、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。

これらのセキュリティ更新が作成されるとただちにそれらをインストールすることにより、新手のフィッシング詐欺 (なりすまし詐欺)、不正なアプリケーション、主力 Web サイトやアプリケーションに感染する悪意のあるプログラムに対する脆弱性を除去します。

リアルタイム セキュリティ更新についての詳細情報は、Real-Time Security Updates ェ、31 ページ を参照してください。

アラート 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ためには、ページ上部の [**印刷**] ボタンを使用します。ブラウザ オプションを使用してこのページを印刷します。このページには Websense Manager ウィンドウにあるようなナビゲーション オプションはすべて表示されません。

Websense データのバックアップと復元

関連トピック :

- バックアップのスケジューリング、300 ページ
- バックアップの即時実行、301 ページ
- バックアップ ファイルの管理、302 ページ
- Websense データの復元、302 ページ
- スケジュールされたバックアップの中止、303 ページ
- コマンド リファレンス、304 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をバックアップし、以前の設定に復元することを容易にします。また、ユーティリティによって保存されたデータは、アップグレード後の Websense 設定情報をインポートするために使用することができます。

Backup Utility は次を保存します :

- Policy Database に保存された クライアントおよびポリシー データを含むグローバル設定情報。
- 各 Policy Server によって保存された Filtering Service と Log Server 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化および設定ファイル。

バックアップ処理は次のように機能します :

1. 即時バックアップ（バックアップの即時実行、301 ページ を参照）を開始するか、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リング、300 ページ を参照）。
   - いつでも手動でバックアップを開始してください。
   - 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したディレクトリに、バックアップ ファイルは 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。ファイル名は次の形式になります :

   ```
   wsbackup_yyyy-mm-dd_hhmmss.tar.gz
   ```

   ここで、yyyy-mm-dd_hhmmss は、バックアップの日付と時間を表します。**tar.gz** は ポータブル圧縮ファイル形式です。

   root (Linux) と Administrators 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 Backup Utility を Websense コンポーネントが動作している各コンピュータ上で実行します。ツールは、現在のコンピュータ上で発見された次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¥Websense¥bin または **/opt/Websense/bin**	authserver.ini BrokerService.cfg config.xml eimserver.ini LogServer.ini netcache.conf 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	すべてのカスタム ブロック ページ設定
tomcat/conf/Catalina/Localhost	mng.xml
Windows¥system32	isa_ignore.txt
Windows¥system32¥bin	ignore.txt
/etc/wsLib	wsSquid.ini

Websense バックアップ ファイルは 安全で確実な場所に保存してください。これらのファイルは お客様の組織のレギュラーバックアップ手順の一部であるべきです。

以前の設定に復元するには 次を行います :

1. 保存場所からバックアップ ファイルを取り出します。
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。

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リング

関連トピック:

- バックアップの即時実行、301 ページ
- バックアップ ファイルの管理、302 ページ
- Websense データの復元、302 ページ
- スケジュールされたバックアップの中止、303 ページ
- コマンド リファレンス、304 ページ

バックアップをスケジュールするためには、コマンド シェルを開き、Websense bin ディレクトリに移動します (デフォルトで、**C:¥Program Files¥Websense¥bin** または **opt/Websense/bin**)。次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。

例で表示されている変数の代わりに、次の情報を提供してください:

変数	情報
<m>	0 – 59 バックアップを開始する正確な 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。

変数	情報
<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 日にスケジュールした場合、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 週の曜日を指定します。0 は 日曜日を表します。

各フィールドは 数値、アスタリスク、パラメータ リストを使用できます。詳細は **crontab** のリファレンスを参照してください。

バックアップの即時実行

関連トピック:

- バックアップのスケジューリング、300 ページ
- バックアップ ファイルの管理、302 ページ
- Websense データの復元、302 ページ
- スケジュールされたバックアップの中止、303 ページ
- コマンド リファレンス、304 ページ

即時バックアップを実行するためには、コマンド シェルを開き、Websense bin ディレクトリに移動します (デフォルトで、**C:¥Program Files¥Websense¥bin** または **opt/Websense/bin**)。次のコマンドを入力します。

```
wsbackup -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場合、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

関連トピック：
- バックアップのスケジューリング、300 ページ
- バックアップの即時実行、301 ページ
- Websense データの復元、302 ページ
- スケジュールされたバックアップの中止、303 ページ
- コマンド リファレンス、304 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。この設定ファイルは次が指定されています：

- どのくらいの間バックアップ 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

これらのパラメータを変更するためには、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 ディレクトリに保持される日数。デフォルトは 365 です。
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。

KeepDays の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作成するためにバックアップ ディレクトリから削除されます。

Websense データの復元

関連トピック：
- バックアップのスケジューリング、300 ページ
- バックアップの即時実行、301 ページ
- バックアップ ファイルの管理、302 ページ
- スケジュールされたバックアップの中止、303 ページ
- コマンド リファレンス、304 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ていることを確認してください。

復元処理を開始するためには、コマンド シェルを開き、Websense bin ディレクトリに移動します（デフォルトで、**C:¥Program Files¥Websense¥bin** または **opt/Websense/bin**）。次のコマンドを入力します。

```
wsbackup -r -f archive_file.tar.gz
```

重要

復元処理は 数分かかる場合があります。復元が進行している間は、処理を停止しないでください。

復元処理中は、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、288 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、サードパーティ社統合製品との通信に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に位置するため、正しいディレクトリに各ファイルをコピーすることで、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には 次が含まれます：

ファイル名	復元先
isa_ignore.txt	**Windows¥system32**
ignore.txt	**Windows¥system32¥bin**
wsSquid.ini	**/etc/wsLib**

スケジュールされたバックアップの中止

関連トピック：

- バックアップのスケジューリング、300 ページ
- バックアップの即時実行、301 ページ
- バックアップ ファイルの管理、302 ページ
- Websense データの復元、302 ページ
- コマンド リファレンス、304 ページ

バックアップ スケジュールをクリアし、現在実行中のスケジュールされたバックアップを停止するためには、コマンドシェルを開き、Websense bin ディレクトリに移動します（デフォルトで、**C:¥Program Files¥Websense¥bin** または **opt/Websense/bin**）。次のコマンドを入力します：

```
wsbackup -u
```

コマンド リファレンス

関連トピック：

- バックアップのスケジューリング、300 ページ
- バックアップの即時実行、301 ページ
- バックアップ ファイルの管理、302 ページ
- Websense データの復元、302 ページ
- スケジュールされたバックアップの中止、303 ページ

root (Linux) または Administrators グループのメンバー (Windows) だけが Backup Utility を実行できます。

いつでも Backup Utility コマンド オプションの完全なリストを見るには、次を入力します：

```
wsbackup -h
```

または

```
wsbackup --help
```

wsbackup コマンドには次の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`, `--help` または `-?`
- `-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]`

13 レポート管理

関連トピック：

- 構成のプランニング、306 ページ
- レポートツールへのアクセスの管理、306 ページ
- 基本構成、307 ページ
- Log Server 構成ユーティリティ、312 ページ
- ログ データベースの管理、325 ページ
- 調査レポートの設定、336 ページ
- セルフ レポート、341 ページ

Websense のプレゼンテーション レポートと調査レポートを使用するためには、Windows サーバーに Websense Manager とレポート コンポーネントの両方をインストールする必要があります。また、Websense ソフトウェアをインターネット フィルタリング状況を記録するように設定する必要があります。

ログ記録は、レコードを Websense Log Server に送信します。Websense Log Server は、ログ データベースに、それらの処理を渡します。ログ データベースは、次のサポートされているデータベース エンジン上にインストールされている必要があります：Microsoft SQL Server Desktop Engine（一般にこのドキュメントの中で MSDE と記述されています）または Microsoft SQL Server Enterprise または Standard Editions（また、一般に Microsoft SQL Server と記述されています）。これらのレポート コンポーネントのインストールに関する詳細情報は、『Websense インストール ガイド』を参照してください。

レポートを作成する際、Websense Manager はレポートのために定義するフィルタに従って、ログ データベースからの情報を表示します。

Linux サーバーに Websense Manager をインストールしている組織、または レポートに Linux を使用することを希望する組織は、レポートを作成するために、Websense Explorer for Linux 製品を別個にインストールすることができます。この製品は Websense Manager とは別に動作します。このプログラムのインストール手順、使用手順は、『Explorer for Linux 管理者用ガイド』を参照してください。

構成のプランニング

ネットワーク内のインターネット トラフィック量によって、ログ データベース は非常に大きくなることがあります。お客様の組織の効果的なログ記録とレポート戦略を決定するために、これらの質問を考慮してください :

- ネットワーク トラフィックはいつ最も混雑しますか ?

  トラフィックがより低いとき、集中的にデータベース ジョブとレポート ジョブをスケジュールするように考慮してください。これはピーク期間中のログ記録とレポートのパフォーマンスを改善します。インターネット ブラウズ時間の設定、330 ページ および ログ データベース メンテナンス オプションの設定、331 ページ を参照してください。
- 過去のレポートを維持するために、ログデータをどのくらいの期間保存すべきですか ?

  その期間に達した後、自動的にパーティションを削除することを考慮してください。これは ログ データベース のために必要とされるディスク スペースの量を減らします。ログ データベース メンテナンス オプションの設定、331 ページを参照してください。
- どれぐらいの詳細な情報が本当に必要とされますか ?

  どのログ記録 オプションを有効にするべきか考慮してください : 完全 URL とヒット件数 のログ記録はログ データベースのサイズを増加させます。ログ データベースのサイズを減少させるためには、次を考慮してください :

  - 完全 URL ログ記録を無効にする (完全 URL によるログ記録の設定、328 ページ を参照)。
  - ヒット件数の代わりにアクセス件数をログ記録する (ログ キャッシュ ファイルの設定、317 ページ を参照)。
  - 集約を有効にする (集約オプションの設定、318 ページ を参照)。
  - 選択可能なカテゴリのログ記録 を有効にする (ログ記録のための Filtering Service 設定、310 ページ を参照)。

レポートの実行が成功するためには、予想される負荷と過去のデータ蓄積要件に合致するか、それを超えるハードウェア上に配備されている必要があります。

レポートツールへのアクセスの管理

Websense Manager とレポート コンポーネントを Windows サーバー上にインストールする際、レポート オプションが Websense Manager と Log Server 構成ユーティリティに表示されます。

レポート コンポーネントをインストールすると、Log Server は 指定の Policy Server と接続します。Websense Manager にログオン中に、レポート機能にアクセスするためには、その Policy Server を選択する必要があります。別の Policy Server にログオンした場合、メイン タブのプレゼンテーション レポート または 調査レポートにアクセスすることはできません。また、[設定] タブのすべてのレポート セクションにアクセスすることはできません。

WebsenseAdministrator ログオン アカウントだけを使用する組織では、Websense Manager を使用するすべての人々は、プレゼンテーション レポート、調査レポート、レポートツールの設定を含む、Websense Manager 内のすべてのレポート オプションにアクセスできます。

指定済み管理を使用する組織では、Websense Manager 内のレポート ツールに対するアクセスは、WebsenseAdministrator と優先管理者ロールのメンバーによって管理されます。ロールを作成するときに、優先管理者はそのロールが特定のレポート オプションへのアクセス権を持つかどうかを指定します。

レポートツールへのアクセスの設定に関する情報は、ロールの編集、258 ページ を参照してください。

Log Server の構成ユーティリティは Windows スタートメニューからアクセスできます。インストール コンピュータへのアクセス権を持つ人々だけがこのユーティリティを開き、Log Server 設定を変更することができます。Log Server 構成ユーティリティ、312 ページを参照してください。

組織がすでに Linux サーバ上に Websense Manager をインストールしているか、または Windows 上で実行するプログラムではなく Websense Explorer for Linux Reporting プログラムを選択した場合、Websense Manager にレポート オプションは表示されません。[今日] および [履歴] のページに、インターネットフィルタリングの図は表示されません。このプログラムをインストールし、レポートを実行するための情報は、『Explorer for Linux 管理者用ガイド』を参照してください。

基本構成

関連トピック :

- ログ記録のための Filtering Service 設定、310 ページ
- カテゴリのリスククラスへの割り当て、308 ページ
- レポートの優先設定、310 ページ
- Log Server 構成ユーティリティ、312 ページ
- ログ データベースの管理、325 ページ

お客様の環境に合わせてレポートをカスタマイズするために、様々な設定オプションを使用することができます。

Websense マスタ データベースはカテゴリを**リスククラス**に整理します。リスククラスは 各カテゴリのサイトのもつ可能性があるタイプ または 脆弱性のレベルを提示します。お客様の組織用にリスククラスをカスタマイズするためには、[設定] タブから [一般] > [リスク クラス] の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、308 ページを参照してください。

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 レポートを有効にするためには、[設定] タブから [レポート] > [優先設定] のページを使用します。レポートの優先設定、310 ページを参照してください。

ログ記録は、レポートを作成することができるようにするために、Websense フィルタリング状況についての情報を、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、ログされるカテゴリを選択し、どんなユーザ情報を記録するかを決定するためには、[設定] タブから [一般] > [ログ記録] のページを使用します。詳細は、ログ記録のための Filtering Service 設定、310 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とログ データベースへの接続を管理するために、Log Server の構成ユーティリティを使用します。詳細は、Log Server 構成ユーティリティ、312 ページ を参照してください。

インターネット ブラウズ時間の管理、データベース パーティション オプション、エラー ログを含むログ データベースの管理を行うためには、[設定] タブから [レポート] > [ログ データベース] のページを使用します。詳細は、ログ データベースの管理、325 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

関連トピック :

- リスク クラス、40 ページ
- ブロック ページ、85 ページ
- レポートを使用したフィルタリング ポリシーの評価、95 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**に整理します。リスククラスは 各カテゴリのサイトのもつ可能性があるタイプ または 脆弱性のレベルを提示します。

リスククラスは 主にレポートで使用されます。[今日] および [履歴] のページはインターネット利用状況がリスククラスによって追跡された図を表示します。そして、リスククラスによって分類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することができます。

条件無し 優先管理者は、**[設定] > [リスククラス]** のページで、各リスククラスを構成するカテゴリを表示 / 変更することができます。例えば、ある業務では、ユーザによってポストされたビデオ サイトが「 法的責任」のリスククラス、「 ネットワーク帯域幅損失」、「 生産性の損失」に含まれると 考えられるか

もしれません。しかし、お客様の会社が統計的な市場調査をしている場合は、「業務関連の使用」のリスククラスの一部であると考えられるでしょう。

> **ご注意：**
> セキュリティ ブロック ページは、セキュリティ リスククラスのデフォルト カテゴリでブロックされたサイトに表示されます。セキュリティ リスククラスのカテゴリの変更は、レポートに影響を与えます。しかし、ブロックページには影響を与えません。ブロック ページ、85 ページを参照してください。

Websense レポートのリスククラス情報は、このページの割り当てを反映します。

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、**カテゴリ** リストを確認します。

   チェックマークは、カテゴリが現在選択された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. 選択されたリスククラスからカテゴリを含める、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
すべて選択	ツリーのすべてのカテゴリを選択します。
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。
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。[**すべて保存**] 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

関連トピック：

- セルフ レポート、341 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、111 ページ
- 調査レポートのスケジュール設定、139 ページ

プレゼンテーション レポート または 調査レポートで、後で実行するようスケジュールするか、繰り返し実行するようスケジュールした場合、レポートは 電子メールによって指定された受信者に配信されます。これらの電子メール メッセージのキー情報を指定するためには、[設定] タブから **[レポート] > [優先設定]** のページを使用します。

また、このページは、個人が自身のインターネット利用状況の調査レポートを作成することができる、セルフ レポートを有効にするためにも使用されます。

1. スケジュールされたレポートが電子メールによって配信されるときに、送信元フィールド を表示するために、**[電子メール アドレス]** を入力します。
2. 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ために使用される電子メール サーバーを、**[SMTP サーバーの IP または名前]** に入力します。
3. お客様の組織のエンド ユーザが Websense Manager にアクセスし、個人の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、**[セルフ レポートを許可する]** チェックボックスにマークを付けます。セルフ レポート、341 ページを参照してください。
4. 変更を適用するために **[すぐに保存]** をクリックします。

ログ記録のための Filtering Service 設定

関連トピック：

- ログ データベースの説明、323 ページ
- Log Server 構成ユーティリティ、312 ページ

Log Server にログ レコードを送信するための IP アドレスとポートを指定するには、[設定] タブの **[一般] > [ログ記録]** のページを使用します。また、このページで、Websense Filtering Service が Log Server にどんなユーザ情報と URL カテゴリを送信するか、レポートとカテゴリの使用状況アラートを有効にするかを選択できます (カテゴリ使用状況アラートの設定、293 ページ を参照)。

複数の Policy Server 環境では、それぞれ別個に [一般] > [ログ記録] のページで設定する必要があります。アクティブな Policy Server と関連付けられた

すべての Filtering Service は、このページで指定された Log Server にログ レコードを送信します。

複数の Policy Server が動作している場合、次のことを念頭においてください：

- Policy Server のための Log Server の IP アドレスとポートが空白である場合、その Policy Server と関連付けられた Filtering Service は、レポート または アラートのためのトラフィックを記録することができません。
- Policy Server の接続設定に従って、各 Filtering Service はトラフィックを記録します。異なった Policy Server のユーザ情報またはカテゴリ ログ記録の選択を変更した場合、異なった Policy Server に関連付けられたユーザのために作成されたレポートは整合性を失うことがあります。

複数の Policy Server と複数の Log Server 両方を含む環境の場合、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. コンピュータのインターネット アクセスの識別情報を記録するためには、**[IP アドレスのログ記録]** にマークを付けます。
2. ユーザのインターネット アクセスの識別情報を記録するためには、**[ユーザ名のログ記録] にマークを付けます。**

   ご注意：
   IP アドレス または ユーザ名を記録しない場合、レポートにユーザ データは表示されません。これは、時々 **匿名ログ**と呼ばれます。

3. **[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 IP アドレスまたはコンピュータ名を入力します。

   重要
   Log Server が Policy Server と別のコンピュータにインストールされている場合、このエントリは デフォルトで localhost になっているかもしれません。この場合、[今日] および [履歴] のページ上の図の表示を有効にするために、また他のレポート機能を有効にするために、Log Server コンピュータの正しい IP アドレスを入力します。

4. Log Server にログ レコードを送信する**ポート**番号を入力します。
5. Websense Manager が指定された Log Server と通信可能かを判断するためには、**[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 アドレスまたはコンピュータ名とポートを更新します。
6. どの URL カテゴリを記録するかを指定するエリアを開くために、**[選択可能なカテゴリのログ記録]** ボタンをクリックします。

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。

ご注意：
使用状況アラート設定を含む（カテゴリ使用状況アラートの設定、293 ページ を参照）カテゴリのログ記録を無効にすると、使用状況アラートは 送信されません。

レポートに 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。

a. 関心のあるカテゴリを参照するためには、親カテゴリを展開するか、折りたたみます。
b. 各カテゴリのチェックボックスにマークを付けることで、記録されるカテゴリを選択します。

   個々にカテゴリを選択するか、選択解除する必要があります。親カテゴリを選択しても、自動的にそのサブ カテゴリは選択されません。選択の補助に [**すべて選択**] および [**すべてクリア**] を使用してください。

7. [OK] をクリックして、変更をキャッシュします。[**すべて保存**] をクリックするまで、変更は適用されません。

Log Server 構成ユーティリティ

関連トピック：

- レポートツールへのアクセスの管理、306 ページ
- 基本構成、307 ページ
- Log Server の起動と停止、323 ページ

インストール中に、Log Server がどのように Websense フィルタリング 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。

Log Server の構成ユーティリティを使用して、必要な場合にこれらの設定を変更し、Log Server の動作の他の詳細な設定を行うことができます。このユーティリティは、Log Server と同じコンピュータにインストールされます。

1. Windows スタートメニューから、[**プログラム**] > [**Websense**] > [**ユーティリティ**] > [**Log Server の構成**] を選択します。

   Log Server の構成ユーティリティが開きます。
2. オプションを表示し、変更を行うタブを選択します。詳細な手順は、次を参照してください：
   - Log Server 接続の設定、313 ページ

- Log Server データベース オプションの設定、314 ページ
- ログ キャッシュ ファイルの設定、317 ページ
- 集約オプションの設定、318 ページ
- WebCatcher の設定、320 ページ

3. 変更を保存するには、[**適用**] をクリックします。
4. 変更を有効にするために、Log Server を停止し再起動するためには、[**接続**] タブを使用します。

重要
すべての Log Server の構成 タブに対して変更を行った後は、[**適用**] をクリックします。その後、変更を有効にするために、Log Server を停止し、再起動する**必要があります**。Log Server の複数回の再起動を避けるために、Log Server を再起動する前に、すべての Log Server の設定変更を完了してください。

Log Server 接続の設定

関連トピック:

- Log Server 構成ユーティリティ、312 ページ
- Log Server データベース オプションの設定、314 ページ
- ログ キャッシュ ファイルの設定、317 ページ
- 集約オプションの設定、318 ページ
- WebCatcher の設定、320 ページ
- Log Server の起動と停止、323 ページ

Log Server と Websense フィルタリング コンポーネント間に接続を作成し、維持するためのオプションが、Log Server 構成ユーティリティの [**接続**] タブにあります。

1. デフォルトの **Log Server 入力ポート (55805)** を受け入れるか、別の利用可能なポートを入力します。

   これは Log Server が Filtering Service と通信するポートです。ここで入力されたポートは、Websense Manager の [一般] > [ログ記録] のページ (設定タブ) に入力されたポートと一致する必要があります。
2. Log Server が更新のためにディレクトリ サービスと通信する頻度を指定するためには、[**ユーザ / グループの更新間隔**] に時間単位の値を入力します。

   完全ユーザ名、グループの割り当てのようなログ データベースレコードのユーザに関する更新情報を取得するために、Log Server はディレクトリ サービスと通信します。

次の更新が発生するまで、グループを変更されたユーザの活動は、前のグループのものとしてレポートされ続けます。ディレクトリ サービスを頻繁に更新するか、多数のユーザを持つ組織では、ユーザ / グループの更新間隔を 12 時間のデフォルト値より、頻度を上げるべきです。

3. 変更を保存するには、[**適用**] をクリックします。
4. Log Server を**起動** / **停止**するためには、[サービス状況] エリアのボタンを使用します。クリックするときに生じるアクションを反映するように、ボタンのラベルは変化します。

> **ご注意 :**
> Log Server が停止している場合、インターネットアクセス状況は記録されません。

Log Server を停止し、再起動するまで、Log Server 構成ユーティリティで行った変更は有効になりません。

Log Server データベース オプションの設定

関連トピック :

- Log Server 構成ユーティリティ、312 ページ
- Log Server 接続の設定、313 ページ
- データベース接続の設定、316 ページ
- ログ キャッシュ ファイルの設定、317 ページ
- 集約オプションの設定、318 ページ
- WebCatcher の設定、320 ページ
- Log Server の起動と停止、323 ページ

Log Server がログ データベースと動作する方法を設定するためには、Log Server 構成ユーティリティの [**データベース**] タブを開きます。

1. 次のオプションから [**ログの挿入メソッド**] を選択します。
   - データベース接続 (ODBC) を開く : データベース ドライバを Log Server とログ データベース間のデータを管理するために使用し、個々に記録をデータベースに挿入します。
   - バルク コピー プログラム (BCP) (推奨): バッチと呼ばれるグループで、ログ データベースに記録を挿入します。ODBC より効率的であるので、この選択が推奨されます。

     > **ご注意 :**
     > Log Server コンピュータに、SQL Server Client Tools をインストールしている場合に限り、BCP オプションは利用可能です。

2. Websense からの新しいインターネット ア クセス情報を保存するための、ログ データベース を選択するために、[**接続**] ボタンをクリックします。データベース接続の設定、316 ページを参照してください。

   データベースとの接続を確立するための設定 [**ODBC データ ソース名 (DSN)**] と [**ODBC ログイン名**] が表示されます。

3. ステップ 1 のログの挿入方法として、BCP を選択した場合、次のオプションを設定します。ログの挿入方法として ODBC を選択した場合、このステップはスキップしてください。

オプション	説明
BCP ファイル パスの位置	BCP ファイルを保存するディレクトリ パスです。これは、Log Server が読み込み / 書き込みアクセスを行うパスです。 Log Server がログ データベースコンピュータにインストールされている場合、または SQL Server Client Tools が Log Server コンピュータにインストールされている場合、このオプションは利用可能です。
BCP ファイルの作成レート	バッチファイルを閉じ、新しいバッチファイルを作成するまで、Log Server がバッチファイルにレコードを挿入する最大時間 (分) です。 この設定は、最大バッチ サイズ設定と共に機能します : いずれかの限界に達したらすぐに、Log Server は新しいバッチファイルを作成します。
BCP 最大バッチ サイズ	新しいバッチファイルを作成するまでのログ レコードの最大数です。 この設定は、作成レート設定と共に機能します : いずれかの限界に達したらすぐに、Log Server は新しいバッチファイルを作成します。

4. Log Server とデータベース エンジン間を接続する内部接続数を、[**許可された最大接続数**] に設定します。利用可能なオプションは、使用されるデータベース エンジンによって異なります。
   - **MSDE**: 4 にあらかじめセットされています。変更できません。
   - **SQL Server**: SQL Server ライセンスに合わせて、4 から 50 までの値を設定します。接続の最小値は、選択されたログ挿入方法に依存します。

   > **ご注意 :**
   > 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 以下に設定するべきです。データベース管理者と相談してください。

5. Log Server が停止した後、ログ記録を再開する方法を制御するオプションを有効 / 無効にするためには、[**拡張ログを使用する**] をチェック / アンチェックします。

このオプションが選択されていない場合（デフォルト）、Log Server が停止した後、最も古いログキャッシュファイルの最初から処理を開始します。これにより、ログ データベースに若干の重複エントリが発生することがありますが、Log Server の処理を高速化します。

このオプションがチェックされている場合、Log Server はアクティブなログ キャッシュ ファイルのその位置を調べます。再起動後、Log Server は、それが停止したところの処理を再開します。拡張ログは、Log Server 処理を遅くすることがあります。

6. すべての変更を保存するために、**[適用]** をクリックし、Log Server を停止し、再起動します（Log Server の起動と停止、323 ページ を参照）。

データ ベース接続の設定

関連トピック：

- Log Server 接続の設定、313 ページ
- Log Server データベース オプションの設定、314 ページ

Log Server 構成ユーティリティの［データベース］タブの **[接続]** ボタンで、Websense から入ってくるインターネット アクセス情報を保存するログ データベースを選択できます。これはインストール中に、自動的に設定されます。しかし、ログ記録するデータベースを変更する必要があるときはいつでも、変更できます。（接続を確立するためには、すでにデータベースが存在している必要があります。）

1. ［データソース］ダイアログボックスで、**[コンピュータ データソース]** タブを選択します。
2. 新しい情報が記録されるデータベースの ODBC 接続を選択します。
3. SQL Server ログオン ダイアログボックスを表示するために、**[OK]** をクリックします。
4. **[信頼関係接続を使用]** のオプションが有効な場合、お客様の環境で、それが適切に設定されていることを確認してください。

   MSDE ユーザ：信頼関係接続オプションのチェックを外します。

   SQL Server ユーザ：データベース管理者に相談してください。

   > **ご注意：**
   > SQL Server との通信に信頼関係接続を使用する場合、信頼ユーザ名とパスワードで、いくつかの Websense サービスを設定する必要があります。詳細は 『Websense インストール ガイド』を参照してください。

5. データベースを作成したときに確立した**ログイン ID** と**パスワード**を入力します。通常、これは Log Server のインストールとデータベースの作成中に、入力したログオン ID とパスワードと同じです。

6. この変更を行った後、および Log Server 構成ユーティリティの他の変更を行った後、[**接続**] タブで Log Server を停止し、再起動します。

ログ キャッシュ ファイルの設定

関連トピック:

- Log Server 構成ユーティリティ、312 ページ
- Log Server 接続の設定、313 ページ
- Log Server データベース オプションの設定、314 ページ
- 集約オプションの設定、318 ページ
- WebCatcher の設定、320 ページ
- Log Server の起動と停止、323 ページ

Log Server 構成ユーティリティの [**設定**] タブで、ログ キャッシュ ファイル作成オプションを管理し、Log Server に各ウェブサイト要求 または ウェブサイトのみを各ファイルに追跡させるかを指定できます。

1. [**ログファイルパスの位置**] フィールドにログ キャッシュ ファイルを保存するパスを入力します。デフォルトパスは <**インストール ディレクトリ**>**¥bin¥Cache** です。(デフォルト インストール ディレクトリは C:¥Program Files¥Websense¥ です。)
2. [**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 ファイルを閉じ、新しいファイルを作成するまで、ログ キャッシュ ファイル (**logn.tmp**) にインターネット アクセス情報を送り続ける時間 (分) の最大値を指定します。

   この設定は、最大サイズ設定と共に機能します: いずれかの限界に達したらすぐに、Log Server は新しいログキャッシュ ファイルを作成します。
3. [**キャッシュ ファイルの最大ファイル サイズ**] に、Log Server が ログ キャッシュ ファイルを閉じ、新しいファイルを作成するまでのファイルのサイズを指定します。

   この設定は、作成レート設定と共に機能します: いずれかの限界に達したらすぐに、Log Server は新しいログキャッシュ ファイルを作成します。
4. ウェブサイトのアクセス件数ごとにログレコードを作成するためには、[**アクセス件数の有効化**] をチェックします。

ご注意:
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。アクセス件数のロギングを有効にすることは、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。

このオプションが選択されていない場合、各 HTTP 要求に対して、画像および広告のような異なったページ要素を表示する別個のログ レコードが作成されます。また、ヒット件数のロギングのオプションを使用すると、急速に、はるかに大きいログ データベースが作成されます。

このオプションを選択すると、Log Server は 1 つのログ レコード中に、(画像および広告のような) Web ページを作成する個々の要素を結合します。

Websense Web Security Gateway をインストールしている場合、アクセス件数のログ記録が有効化されている場合でも、リアルタイム スキャンは、常にヒット件数でレポートします。この状況では、リアルタイム スキャンによってブロックされたトラフィックを含むウェブ フィルタリング レポートに表示される数は、リアルタイム スキャン レポートで表示される数より少なくなります。

ご注意:
アクセス件数とヒット件数間でロギング方法を変更する前に、新しいデータベース パーティションを作成することが最良です。新しいデータベース パーティションを作成する方法は、Websense Manager の [レポート] > [ログ データベース] のページ (設定タブ) を参照してください。

5. すべての変更を保存するために、**[適用]** をクリックし、Log Server を停止し、再起動します (Log Server の起動と停止、323 ページ を参照)。

集約オプションの設定

関連トピック:

- Log Server 構成ユーティリティ、312 ページ
- Log Server 接続の設定、313 ページ
- Log Server データベース オプションの設定、314 ページ
- ログ キャッシュ ファイルの設定、317 ページ
- WebCatcher の設定、320 ページ
- Log Server の起動と停止、323 ページ

集約を有効にし、集約の環境設定を行うためには、Log Server 構成ユーティリティの **[集約]** タブを使用します。

ご注意:
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。集約を有効にすることは、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。

次の要素を共有するインターネット要求を結合することによって、集約は ログ データベースのサイズを減少させます :

- 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 / ワークステーション

ログ データベースが小さい場合、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
集約を有効にすると、インターネット ブラウズ時間の計算等のいくつかのレポート データが正確性を損なわれる場合があります。

1. 複数の類似のインターネット要求を 1 つのログ レコードに結合する集約を有効にするには、**[ログ レコードの集約]** をチェックします。

   このオプションが選択されていない場合、デフォルトで、ログ データベース は、各インターネット要求のヒット件数 または アクセス件数の詳細を保存します ([設定] タブの選択に依存します。ログ キャッシュ ファイルの設定、317 ページ を参照)。これはより大規模なレポートの詳細を提供しますが、ログ データベースも大きくなります。

   このオプションを選択すると、レポートの詳細は小さくなり、ログ データベースも小さくなります。

   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 がインストールされている場合、集約が有効化されている場合でも、リアルタイム スキャンは、常に個々のヒット件数でレポートします。この状況では、リアルタイム スキャンによってブロックされたトラフィックを含むウェブ フィルタリング レポートに表示される数は、リアルタイム スキャン レポートで表示される数より少なくなります。

2. **[集約時間の間隔]** は、結合される最初と最後のレコード間の最大時間を指定します。

   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最大の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。

Websense Manager の [レポート] > [ログ データベース] のページ ([設定] タブ) の [完全 URL] オプションを有効にした場合、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、ユーザが次の場所を訪問し、すべてが ショッピング カテゴリに分類されるとします。

- www.domain.com/shoeshopping
- www.domain.com/purseshopping
- www.domain.com/jewelryshopping

完全 URL が有効な場合、集約により、URL www.domain.com/shoeshopping の下に、1 つのログ エントリが作成されます。

3. すべての変更を保存するために、**[適用]** をクリックし、Log Server を停止し、再起動します (Log Server の起動と停止、323 ページ を参照)。

WebCatcher の設定

関連トピック :

- Log Server 構成ユーティリティ、312 ページ
- Log Server 接続の設定、313 ページ
- Log Server データベース オプションの設定、314 ページ
- ログ キャッシュ ファイルの設定、317 ページ
- 集約オプションの設定、318 ページ
- WebCatcher の認証、322 ページ
- Log Server の起動と停止、323 ページ

WebCatcher は、未分類の URL とセキュリティ関連の URL を収集するオプション機能であり、Websense にそれらを提出します。そして、Websense は、分類するために、潜在的なセキュリティと責任リスクを調査します。(完全 URL ロギングは、WebCatcher 処理のためには必要ありません。) Websense は、情報を調査し、フィルタリングを改良するために、新しく分類された URL で マスタ データベース を更新します。

Log Server 構成ユーティリティの [**WebCatcher**] タブで、送信する URL タイプを選択し、ファイルのサイズと処理時間を設定します。

> **ご注意：**
> 複数の Log Server 環境では、WebCatcher は 1 つの Log Server だけで有効にできます。有効にすると、他の Log Server インスタンスの Log Server 構成ツールでこのタブは利用できません。

Websense に送信される情報は、URL のみを含み、ユーザ情報は含みません。

次の例は、WebCatcher を有効にした場合に、送信される情報を示しています。この例の IP アドレスは、要求者の IP アドレスではなく、URL ホスト コンピュータのアドレスです。

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

WebCatcher データは、HTTP Post で Websense に送信されます。ロールを作成するか、または外向きの HTTP トラフィックを許可するように、プロキシサーバーまたはファイアウォールの設定を変更する必要がある場合があります。手順は、プロキシサーバー または ファイアウォールのマニュアルを参照してください。

1. 次のオプションの 1 つを選択します：
   - [**はい、指定した URL のみ Websense に送信します**] は、WebCatcher 処理を行います。送信する URL を指定します。続けて、手順 2 を行います。
   - [**いいえ、Websense に情報を送信しません**] は、WebCatcher 処理を行いません。このオプションを選択した場合、これ以上の入力は必要ありません。
2. ログ データベースの中のすべての分類されていない URL リストを送信するためには、[**分類されていない URL の送信**] をチェックします。

   Websense は、それを受信し、分類されていない URL を解析し、マスタ データベース カテゴリに追加します。これにより、すべての組織でフィルタリングの正確性が改善されます。

   > **ご注意：**
   > イントラネット サイトは、WebCatcher によって送信されません。これには、10.xxx.xxx.xxx、172.16.xxx.xxx、192.168.xxx.xxx の範囲の IP アドレスのすべてのサイトが含まれます。

3. ログ データベースの中のセキュリティ URL リストを送信するためには、[**セキュリティ URL の送信**] をチェックします。

   受信されたセキュリティ URL は、Websense によって解析され、そのサイトの活動が、キーロガー、悪意のあるウェブサイト、フィッシングおよびその他の詐欺サイト、スパイウェア カテゴリ であるかを決定します。

4. **[ご利用の環境に最も近い国名 / 地域名を選択してください]** で、おもな活動が記録されている国を選択します。
5. Websense に送信されるデータのコピーを保存するためには、**[Websense に送信されるデータのコピーを保存する]** をチェックします。

   このオプションを有効にすると、WebCatcher は、Websense¥Reporter ディレクトリにデータを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、日付と時間が挿入されます。
6. **[アップロード ファイルの最大サイズ (KB)]** で、Websense に送信する前に、ファイルの大きさを指定します (4096KB から 8192KB まで)。

   お客様のシステムで、HTTP Post によって、このサイズのファイルをポストすることができることを確認してください。
7. **[処理開始時刻 (毎日最低 1 回)]** に、その日限界サイズに到達しなかった場合に、WebCatcher がファイルを送信する開始時間を指定します。

   これにより、少なくとも 1 日 1 回、情報が送信され、システムからクリアされます。
8. Log Server コンピュータがインターネットにアクセスするために認証を必要とする場合、**[認証]** ボタンをクリックします。

   表示される **[認証]** ダイアログボックスについての情報は、WebCatcher の認証、322 ページ を参照してください。
9. すべての変更を保存するために、**[適用]** をクリックし、Log Server を停止し、再起動します (Log Server の起動と停止、323 ページ を参照)。

WebCatcher の認証

関連トピック :

- Log Server 構成ユーティリティ、312 ページ
- WebCatcher の設定、320 ページ
- Log Server の起動と停止、323 ページ

[WebCatcher] タブ上で認証をクリックすると、**[認証]** ダイアログボックスが表示されます。

1. Log Server コンピュータがプロキシサーバーを介してインターネットにアクセスする場合、**[プロキシ サーバーを使用する]** オプションをチェックし、要求される情報を入力します。

フィールド	説明
プロキシ サーバー名	Log Server がインターネットにアクセスするために使用する、プロキシサーバーのコンピュータ名または IP アドレスを入力します。
プロキシ サーバー ポート	プロキシサーバーが通信するポート番号を入力します。

2. Log Server コンピュータがインターネットにアクセスするために認証を必要とする場合、**[基本認証を使用する]** オプションをチェックし、次に認証のためのユーザ名とパスワードを入力します。
3. 変更を保存し、[WebCatcher] タブに戻るために、**[OK]** をクリックします。

Log Server の起動と停止

関連トピック：

- Log Server 構成ユーティリティ、312 ページ
- Log Server 接続の設定、313 ページ

Log Server は、Filtering Service から情報を受け取って、レポート作成に使用するために、ログ データベースに保存します。一般に、インストール中に開始し、Windows サービスとして動作し、コンピュータを再起動したときはいつでも起動します。

Log Server を停止し、再起動した後だけ、Log Server 構成ユーティリティの変更が有効になります。これは、Log Server 構成ユーティリティの [接続] タブで、簡単に行えます。

1. Windows スタートメニューから、**[プログラム] > [Websense] > [ユーティリティ] > [Log Server の構成]** を選択します。
2. **[接続]** タブで、**[停止]** をクリックします。
3. 数秒待って、Log Server サービスを再起動するために、**[開始]** をクリックします。
4. Log Server 構成ユーティリティを閉じるために、**[OK]** をクリックします。

ご注意：
Log Server が停止している間は、Websense はインターネット アクセスを記録しません。

ログ データベースの説明

関連トピック：

- データベース ジョブ、324 ページ
- ログ データベースの管理、325 ページ

ログ データベースは、インターネット利用状況と関連付けられた Websense フィルタリング アクションのレコードを保存します。インストール時に、カタログ データベースと 1 つのデータベース パーティションを、ログ データベース に作成します。

カタログ データベースは、ログ データベース にアクセスする必要がある種々の Websense コンポーネントに、1 つの接続ポイントを提供します : ステータス ページ、Log Server、プレゼンテーション レポート、調査レポート。これは、カテゴリ名のリスト、リスククラス定義、グループへのユーザ マップ、データベース ジョブなどを含むデータベース パーティションの補助情報を含みます。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 リストを管理します。

データベース パーティションは、インターネット利用状況についての個々のログ レコードを保存します。MSDE ユーザの場合、Websense ソフトウェアによって指定されたサイズ ロールオーバー ルールに基づいて、新しいパーティションが作成されます。Microsoft SQL Server ユーザは、パーティション サイズ または 日付間隔に基づいて (詳細は、ロールオーバー オプションの設定、327 ページ を参照) 新しいパーティションを開始するように、ログ データベースを設定することができます。

> **ご注意 :**
> Websense ソフトウェアが Microsoft SQL Server を データベース エンジンとして使用している場合のみ、日付ベースのパーティションが利用可能です。

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 パーティションは 柔軟性と パフォーマンス上の利点を 提供します。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

次のデータベース ジョブは ログ データベース とともにインストールされます。SQL Server Agent は、データベース エンジン (MSDE または Microsoft SQL Server) が稼働しているコンピュータ上で実行する必要があります。

- Extract、Transform、Load (ETL) ジョブは 連続して実行されます。Log Server からデータを受信し、それを処理し、そして、パーティション

データベースに挿入します。ETL ジョブはログ レコードをログ データベース内へ処理するために実行されます。

- 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。

これらのデータベース ジョブの特定の設定は、[設定] > [ログ データベース] のページで設定できます。詳細は、ログ データベース管理の設定、326 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。

ログ データベースの管理

関連トピック:

- ログ データベース管理の設定、326 ページ
- ロールオーバー オプションの設定、327 ページ
- インターネット ブラウズ時間の設定、330 ページ
- 完全 URL によるログ記録の設定、328 ページ
- ログ データベース メンテナンス オプションの設定、331 ページ
- ログ データベースパーティション作成の設定、333 ページ
- 使用可能なパーティションの設定、334 ページ
- エラーログの表示、335 ページ

ログ データベースの管理には、データベース動作の複数の側面の制御を伴います。これには次が含まれます:

- データベース ジョブが何の動作を実行し、いつ実行するか。
- 新しいデータベース パーティションを作成するための条件。
- どのパーティションがレポートで利用可能であるか。

ログ データベースの管理者にとって、これらとその他のオプションは重要な制御です。ログ データベース管理の設定、326 ページを参照してください。

優先管理者は、ロールを作成するときに、ログ データベースの管理者を指定できます。ロールの編集、258 ページを参照してください。

> **ご注意：**
> ログ データベース設定を変更する許可を持つ管理者の数を制限することを推奨します。

ログ データベース管理の設定

関連トピック：

- ログ データベースの管理、325 ページ

[設定] タブからアクセスできる **[レポート]** > **[ログ データベース]** のページで、ログ データベース動作の種々の側面を管理できます。オプションは別途解説されている論理セクションにグループ化されています。

そのセクションの変更を有効にするためには、セクション内で [すぐに保存] をクリックする必要があります。**[すぐに保存]** をクリックすると、すぐにそのセクションの変更を保存します。([すべて保存] をクリックする必要はありません。)

ページ上部にアクティブなログ データベース名と **リフレッシュ** リンクが表示されます。このリフレッシュ リンクは ログ データベースページで現在の情報を再表示します。適切な [すぐに保存] ボタンによって適用されなかったすべての変更は失われます。

各セクションを使用する詳細な手順は、下記の適切なリンクをクリックしてください。

- データベース ロールオーバーのオプション：ロールオーバー オプションの設定、327 ページ
- 完全 URL によるログ記録：完全 URL によるログ記録の設定、328 ページ
- インターネット ブラウズ時間の設定：インターネット ブラウズ時間の設定、330 ページ
- メンテナンスの構成：ログ データベース メンテナンス オプションの設定、331 ページ
- データベース パーティションの作成：ログ データベースパーティション作成の設定、333 ページ
- 使用可能なパーティション：使用可能なパーティションの設定、334 ページ
- エラー ログのアクティビティ：エラーログの表示、335 ページ

ロールオーバー オプションの設定

関連トピック：

- ログ データベース管理の設定、326 ページ
- インターネット ブラウズ時間の設定、330 ページ
- 完全 URL によるログ記録の設定、328 ページ
- ログ データベース メンテナンス オプションの設定、331 ページ
- ログ データベースパーティション作成の設定、333 ページ
- 使用可能なパーティションの設定、334 ページ
- エラーログの表示、335 ページ

いつログ データベースに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）かを指定するためには 、[レポート] > [ログ データベース]（設定タブ）のページの **[データベース ロールオーバーのオプション]** を使用します。

1. 使用しているデータベース エンジンに依存して、データベース パーティションがサイズ（MB）に基づいて ロールオーバーするか、日付（週 または 月）に基づいて ロールオーバーするか、を指定するために、**[ロールオーバーの頻度]** オプションを使用します。

   MSDE ユーザは サイズ ロールオーバー オプションを使用する必要があります。Microsoft SQL Server ユーザは サイズまたは日付を選択することができます。

   - 日付ベースのロールオーバーでは、**週** または **月** の基準単位を 選択し、新しいデータベース パーティションが作成されるまで、データベース パーティションを保持する、完全な暦上の週 または月 を指定します。
   - サイズベースのロールオーバーでは、**MB** を選択し、ロールオーバーを開始するためにデータベースが達しなくてはならないメガバイト数を指定します。

     Microsoft SQL Server ユーザは 204800MB までサイズを設定することができます。

MSDE ユーザは 100MB と 1536MB の間でサイズを設定する必要があります。

ご注意：
ロールオーバーが 1 日の混雑した時間に開始される場合、ロールオーバー プロセスの間のパフォーマンス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は、ある環境では、自動ロールオーバーを長期間または最大サイズに設定します。その後、自動ロールオーバーが発生することを阻止するために、通常の手動ロールオーバーを実行します。手動ロールオーバーに関する情報は、ログ データベースパーティション作成の設定、333 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、レポートパ フォーマンス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（使用可能なパーティションの設定、334 ページ を参照）。

2. データベース ロールオーバー オプションに対する変更を有効にするためには、[**すぐに保存**] をクリックします。

完全 URL によるログ記録の設定

関連トピック：

- ログ データベース管理の設定、326 ページ
- ロールオーバー オプションの設定、327 ページ
- インターネット ブラウズ時間の設定、330 ページ
- ログ データベース メンテナンス オプションの設定、331 ページ
- ログ データベースパーティション作成の設定、333 ページ
- 使用可能なパーティションの設定、334 ページ
- エラーログの表示、335 ページ

[レポート] > [ログ データベース] のページ (設定タブ) の **[完全 URL によるログ記録]** のセクションは、各インターネット要求で URL のどの部分を記録するかを決定します。

ご注意 :
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、全部の URL を記録するためには、**[要求された各サイトの完全 URL を記録します]** にマークを付けます。

   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、[URL によるログ記録] を有効にします (リアルタイム スキャン アクティビティのレポート、156 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。

   完全 URL を保存することで、ログ データベースのサイズは大きくなりますが、詳細なレポートが得られます。

   集約が有効であるときに、[完全 URL によるログ記録] 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、集約オプションの設定、318 ページ を参照してください。
2. [完全 URL によるログ記録] オプションに対する変更を有効にするためには、**[すぐに保存]** をクリックします。

インターネット ブラウズ時間の設定

関連トピック：

- ログ データベース管理の設定、326 ページ
- ロールオーバー オプションの設定、327 ページ
- 完全 URL によるログ記録の設定、328 ページ
- ログ データベース メンテナンス オプションの設定、331 ページ
- ログ データベースパーティション作成の設定、333 ページ
- 使用可能なパーティションの設定、334 ページ
- エラーログの表示、335 ページ

インターネットブラウズ時間 (IBT) は、ユーザ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。[設定] > [ログ データベース] のページの **[インターネット ブラウズ時間の設定]** で、ブラウズ時間オプションを設定します。

1. IBT データベース ジョブの **[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動作させるよう、ネットワーク上が混雑していない時間を選択するよう、レポート作成に対する影響を最小にするよう選択することが最良です (ログ データベース メンテナンス オプションの設定、331 ページ を参照)。

   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。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. **[読み込み時刻のしきい値]** に、特定のウェブサイトを読み込むための、分単位の平均値を設定します。

   [読み込み時刻のしきい値] は、インターネット ブラウズ時間レポートの目的のためのブラウズ セッションを定義します。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。

ご注意：
可能な限り［読み込み時刻のしきい値］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が最良です。

レポート上のデータの整合性を保つために、同じ読み込み時刻のしきい値 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、**［最終読み込み時刻］**を設定します。

   HTTP トラフィックの時間間隔が［読み込み時刻のしきい値］より長い場合、セッションは終了します。［最終読み込み時刻］は セッションタイムに加算されます。

4. インターネットブラウズ時間の設定変更を有効にするためには、**［すぐに保存］**をクリックします。

ログ データベース メンテナンス オプションの設定

関連トピック：

- ログ データベース管理の設定、326 ページ
- ロールオーバー オプションの設定、327 ページ
- インターネット ブラウズ時間の設定、330 ページ
- 完全 URL によるログ記録の設定、328 ページ
- ログ データベースパーティション作成の設定、333 ページ
- 使用可能なパーティションの設定、334 ページ
- エラーログの表示、335 ページ

データベース メンテナンス ジョブの実行時間、実行する特定のタスク、データベース パーティションの削除、エラーログのような、データベース処理の特定の側面を管理するためには、［レポート］>［ログ データベース］のページ（設定タブ）の**［メンテナンスの構成］**のセクションを使用します。

1. **[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 1 日の中の時刻を選択します。

   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、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、330 ページ を参照）。

2. **[パーティションを自動的に削除する]** をチェックし、パーティションが削除されるべき日数（2 から 365 まで）を指定します。

   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、使用可能なパーティションの設定、334 ページ を参照してください。

3. **[索引自動再作成を有効にする]** をチェックし、各週でこの処理を自動的に実行する週の中の 1 日を選択します。

   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. **[失敗したバッチを削除するまでの日数]** をチェックし、すべての失敗したバッチを削除する日数（0 から 90 まで）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、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。

   不十分なディスク スペースまたはログ レコードをデータベースに挿入するための不適当なデータベース許可があった場合、レコードには **バッチ失敗** というマークが付けられます。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。さらに、**[未処理のバッチを処理する]** が選択されていない場合、失敗したバッチは再処理されません。これは ここで指定された時間後に削除されます。

5. 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、**[未処理のバッチを処理する]** をチェックします。

   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。もしあれば、上で指定された時間後に削除されます。

6. **[エラー ログを削除するまでの日数]** をチェックし、カタログ データベースからデータベース エラー ログを削除する日数 (0 から 90 まで) 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. メンテナンスの構成オプションに対する変更を有効にするためには、**[すぐに保存]** をクリックします。

ログ データベースパーティション作成の設定

関連トピック:

- ログ データベース管理の設定、326 ページ
- ロールオーバー オプションの設定、327 ページ
- インターネット ブラウズ時間の設定、330 ページ
- 完全 URL によるログ記録の設定、328 ページ
- ログ データベース メンテナンス オプションの設定、331 ページ
- 使用可能なパーティションの設定、334 ページ
- エラーログの表示、335 ページ

場所またはサイズ オプションなどの新しいデータベース パーティションの特性を定義するためには、[レポート] > [ログ データベース] のページ (設定タブ) の **[データベース パーティションの作成]** のセクションを使用します。また、このエリアで、指定したロールオーバー (ロールオーバー オプションの設定、327 ページ を参照) を待つより前に、すぐに新しいパーティションを作成できます。

1. 新しいデータベース パーティションの**データとログ** ファイル両方を作成するための、**ファイル パス** を入力します。
2. **[初期サイズ]** に、新しいデータベース パーティションの**データとログ** ファイル両方の初期ファイル サイズ (100 から 204800MB まで) を設定します。

   Microsoft SQL Server ユーザ: 可能な範囲 100 – 204800

   MSDE ユーザ: 可能な範囲 100 – 1500

   > **ご注意:**
   > ある期間を通して平均のパーティションのサイズを計算することが推奨されます。その後、その値に初期サイズを更新します。このアプローチは、パーティションが拡張される回数を最小にし、パーティション内へデータを処理するリソースを解放します。

3. **[増加]** に、追加のスペースが要求されるときの、パーティションの**データとログ** ファイルのメガバイト (MB) 単位の増加分を設定します。

Microsoft SQL Server ユーザ：可能な範囲 1 – 999999

MSDE ユーザ：可能な範囲 1 – 450

4. 入力されたパス、サイズ、増加 の変更を有効にするためには、**[すぐに保存]** をクリックします。

   これらの変更後作成されたデータベース パーティションは、新しい設定を使用します。

5. 自動ロールオーバーの設定にかかわらず、データベース ジョブ、324 ページ ETL ジョブ (を参照) の実行後、新しいパーティションを作成するためには、**[すぐに作成]** 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がこのセクションで行われた変更を使用するようにするためには、必ず、**[すぐに作成]** をクリックする前に、**[すぐに保存]** をクリックしてください。

   繰り返しコンテンツペインで [リフレッシュ] リンクをクリックします。作成処理が完了すると、[使用可能なパーティション] エリアに新しいパーティションが表示されます。

使用可能なパーティ ショ ンの設定

関連トピック：

- ログ データベース管理の設定、326 ページ
- ロールオーバー オプションの設定、327 ページ
- インターネット ブラウズ時間の設定、330 ページ
- 完全 URL によるログ記録の設定、328 ページ
- ログ データベース メンテナンス オプションの設定、331 ページ
- ログ データベースパーティション作成の設定、333 ページ
- エラーログの表示、335 ページ

[レポート] > [ログ データベース] のページ (設定タブ) の **[使用可能なパーティション]** のセクションはレポートで利用可能なすべてのデータベース パーティションをリストします。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。

どのデータベース パーティションをレポートに含めるかを管理するために、および 削除する個々のパーティションを選択するために、このリストを使用します。

1. レポートに含める各パーティションの横の **[有効にする]** をチェックします。

   適切に、リストで **[すべて選択]** および **[選択解除]** を使用します。

   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。いくつかのパーティションだけを有効にすることができるように、一度にすべてのパーティションを無効にするためには、**[選択解除]** を使用します。

レポート作成時に解析すべきデータ量とレポート処理速度を管理するために、これらのオプションを使用します。例えば、6 月の一連のレポートを作成する場合、6 月の日付があるもの以外のすべてのパーティションを選択解除します。

重要
この選択は、対話的に実行されるレポートと同様に、スケジュールされたレポートにも影響を与えます。データのないレポートが作成されることを避けるために、レポートをスケジュールするときに、適切なパーティションが使用可能であることを確認してください。

2. パーティションが必要ない場合、パーティション名の横の **[削除]** オプションをクリックします。毎晩のデータベース メンテナンス ジョブが次に実行されるときに、パーティションは実際に削除されます。

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、ログ データベース 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、ログ データベース メンテナンス オプションの設定、331 ページ を参照してください。

3. 使用可能なパーティションの変更を有効にするためには、**[すぐに保存]** をクリックします。

エラーログの表示

関連トピック :

- ログ データベース管理の設定、326 ページ
- ロールオーバー オプションの設定、327 ページ
- インターネット ブラウズ時間の設定、330 ページ
- 完全 URL によるログ記録の設定、328 ページ
- ログ データベース メンテナンス オプションの設定、331 ページ
- ログ データベースパーティション作成の設定、333 ページ
- 使用可能なパーティションの設定、334 ページ

Websense ログ データベース上で実行されたジョブの間に発生したエラーレコードを表示するには、[レポート] > [ログ データベース] のページ (設定タブ) の **[エラー ログのアクティビティ]** セクションを使用します (データ

ベース ジョブ、324 ページ を参照)。この情報は、トラブルシューティングにおいて有用です。

次のオプションの 1 つを選択します。

- エラーログ エントリを表示する数をドロップダウン リストから選択します。
- すべてのエラーログ エントリを表示するためには、[**すべて表示**] を選択します。
- すべてのエラーログ エントリを非表示にするためには、[**非表示**] を選択します。

調査レポートの設定

関連トピック :

- データベース接続とレポートのデフォルト、336 ページ
- 表示および出力オプション、338 ページ

調査レポートを使用して、対話的に、組織のインターネット利用状況についての情報を調査できます。調査レポート、118 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、336 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。表示および出力オプション、338 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

関連トピック :

- 調査レポートの設定、336 ページ
- 表示および出力オプション、338 ページ
- 要約レポート、120 ページ
- マルチレベル要約レポート、125 ページ

希望するログ データベースへ接続するために、および 調査レポートのデフォルト詳細表示を管理するためには、[**調査レポート**] > [**オプション**] のページを使用します。

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、[**カタログ データベースの表示**] をチェックします。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ためには、次を行います :
     a. [**カタログ データベースの表示**] のチェックを外します。
     b. 希望するログ データベースを指定するために、次の情報を入力します。(調査レポートは v6.3.x または v7.0 のデータベースから作成できます。)

フィールド	説明
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。
データベース	ログ データベース名を入力します。
ユーザ ID	データベースにアクセスする許可を持つアカウントのユーザ 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インストールされている場合は、空白のままにします。 不明の場合は、**sa** と入力します。これは、MSDE のデフォルト ユーザ ID であり、Microsoft SQL Server のデフォルト管理者 ID です。
パスワード	指定されたユーザ ID のパスワードを入力します。信頼関係接続の場合 空白のままにします。

2. 詳細レポートの次のデフォルト値を選択します。

フィールド	説明
調査レポートのデフォルト日付範囲の選択	初期表示の要約レポートの日付範囲を選択します。
デフォルトの詳細レポート フォーマットの選択	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、[**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列を指定するためには、[**カスタム列の選択**] を選択します。選択をするために [使用可能な列] を使用します。 レポートが作成された後で、ユーザは表示された列を変更することができます。

フィールド	説明
レポート タイプの選択	最初に詳細レポートを開くかどうかを選択します： • **詳細**：各レコードが別個の行に表示されます。時間が表示されます。 • **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。専用の要素は、レポートされる情報によって変化します。一般に、基準の前の一番右の列は 要約された要素を示します。時間は表示されません。
使用可能な列 / 現在のレポート	[使用可能な列] リストで列名を選択し、[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 [現在のレポート] リストに載せることができます。 [現在のレポート] 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、アップ / ダウン矢印 ボタンでその位置を変更します。

3. すぐにすべての変更を保存するためには、**[オプションの保存]** をクリックします。

表示および出力オプション

関連トピック：

- 調査レポートの設定、336 ページ
- データベース接続とレポートのデフォルト、336 ページ
- ファイルへの出力、144 ページ

特定のレポート選択とレポート結果が、要約または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設定オプションは **wse.ini** ファイルに設定されます。デフォルトで次の場所にあります：

```
C:\Program Files\Websense\webroot\Explorer\wse.ini
```

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	[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 (デフォルトは、5000) である必要があります。
maxGroupsMenu	[インターネット使用状況] 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。 **ご注意**:[インターネット使用状況] 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、[インターネット使用状況] 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。
maxUsersDrilldown	これは、[ユーザ] 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、[ユーザ] 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リストで、[ユーザ] 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、[ユーザ] 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、[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、[グループ] 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、[ユーザ] 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 (デフォルトは、10000) より多くのユーザがあり、ヒット件数がこの値より少ない場合、[ユーザ] 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があり、この値より多くのヒット件数がある場合、[ユーザ] オプションは赤色で表示されます。赤色の文字は、[ユーザ] 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。

パラメータ	説明
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。)
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 (バイト単位) 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、この値を減少させ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、これを 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。
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	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、日別ユーザ活動詳細 および 月別ユーザ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 (デフォルトは、レター) は 次が可能です : • A4 (8.27 X 11.69 インチ) • レター (8.5 X 11 インチ)

セルフ レポート

関連トピック：

- レポートの優先設定、310 ページ
- セルフレポートへのアクセス、145 ページ
- 調査レポート、118 ページ

セルフ レポートは、個人のインターネット活動の調査レポートをユーザ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、自身の活動を見せることは、ユーザに自身のブラウジング習性の変更を促し、組織のインターネット ポリシーに適合させます。

ご注意：
Websense Manager とレポート コンポーネントが Windows オペレーティング システムにインストールされているときだけ、セルフ レポートは利用可能です。詳細は 『配備ガイド』を参照してください。

セルフ レポートを有効にする方法は次のとおりです：

1. **[設定]** > **[一般]** > **[ディレクトリ サービス]** に移動し、ネットワーク資格証明で Websense Manager にアクセスするユーザを、認証するために使用されているディレクトリ サービスを設定します。これは、以前にユーザとグループ名によるフィルタリングを有効にするために、行われているかもしれません。ディレクトリ サービス、63 ページを参照してください。

   インストールに複数の Policy Server が含まれる場合、それぞれにログオンし、適切なディレクトリ サービスのための情報で [ディレクトリサービス] のページを設定する必要があります。
2. **[設定]** > **[レポート]** > **[優先設定]** に移動し、**[セルフ レポートを許可する]** チェックボックスにマークを付けます。レポートの優先設定、310 ページを参照してください。

オプションを有効にした後で、必ずユーザにレポートを実行するために必要な情報を連絡してください：

- セルフ レポート インターフェースにアクセスするための URL。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に通知してください。

  URL についての詳細情報は、後述しています。
- ログオン中にどの Policy Server を選択するべきか。

  ネットワークで Policy Server が 1 つしかない場合、これは必要ありません。ネットワークに複数の Policy Server が含まれる場合、ネットワーク

ログオンを認証するディレクトリ サービスと通信するよう設定された Policy Server の IP アドレスを、ユーザに通知してください。これは、Log Server をインストールしたとき、指定された Policy Server と同じです。

- ログオン時にどんなユーザ名とパスワードを使用するべきか。

  セルフ レポート ユーザは、ログオン時にネットワーク ユーザ名とパスワードを入力する必要があります。

セルフ レポート インターフェースにアクセスするための **URL** は 次のとおりです。

```
https://<ServerIP>:9443/mng/login/pages/
   selfReportingLogin.jsf
```

<ServerIP> の代わりに Websense Manager を実行しているコンピュータの IP アドレスを使用します。

また、管理者とユーザは、Websense Manager ログオン ページを開いて、[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。

ネットワークに**複数の Policy Server** が含まれている場合、セルフ レポート ログオン時に、どれを選択するべきかをユーザに通知する必要があります。

14 ネットワークの構成

関連トピック：

- ハードウェア構成、344 ページ
- Network Agent の構成、345 ページ
- Network Agent 設定の確認、352 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）スタンドアロンのモードで、Websense ソフトウェアを実行している場合、Websense Network Agent を有効にします：

- インターネット コンテンツ フィルタリング
- 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

統合された Websense ソフトウェアの配備では、サードパーティ製品が、フィルタリングのために Websense ソフトウェアに対してユーザ要求をルーティングし、ブロック ページをクライアントに返すためにルーティングすることがあります。この環境でも、非 HTTP 要求のフィルタリングのために Network Agent が使用されることがあり、拡張ログの詳細を提供するために使用されることもあります。

Network Agent は、ネットワーク上の転送バイト数を含む、絶えず全体的なネットワーク利用状況をモニタします。エージェントは事前定義された間隔で、Websense ソフトウェアに利用状況の要約を送ります。各要約には、開始時間、終了時間、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 に帯域幅使用状況を、Filtering Service にフィルタリング 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参照するように設定されます。エージェントは、次を識別します：

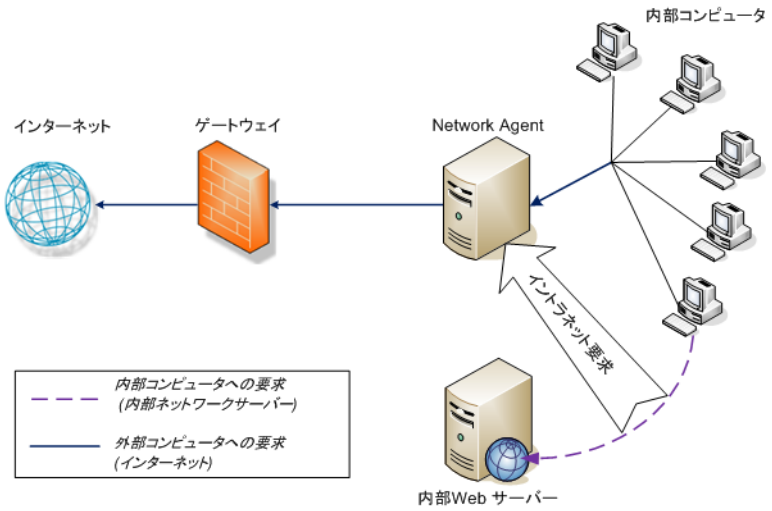
- 内部コンピュータから内部コンピュータへ送信された要求（例えば、イントラネット サーバーのヒット件数）。
- 内部のコンピュータから Web サーバーなどの外部のコンピュータに送信された要求（例えば、ユーザ インターネット要求）。

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。

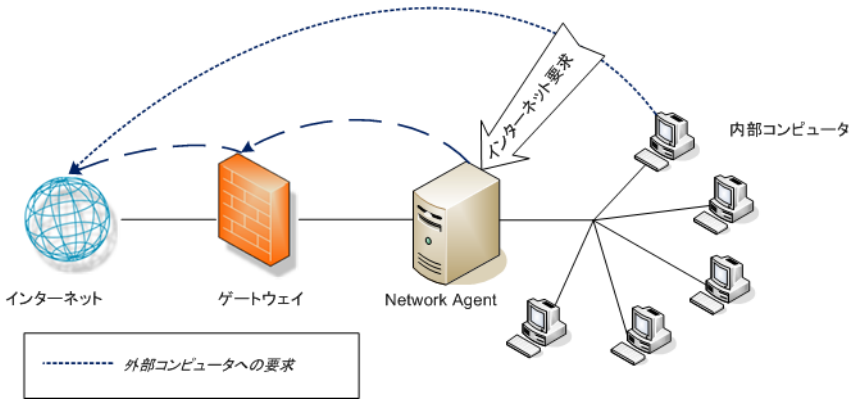
ハードウェア構成

各 Network Agent のインスタンスは、ネットワーク内の指定されたコンピュータ**からの**トラフィックをモニタします。デフォルトでは、指定された内部コンピュータ（例えば、内部 Web サーバー）**への**トラフィックのみをモニタします。

Network Agent インスタンスによって、どの内部コンピュータ（ネットワークセグメント）をモニタするか、Network Agent コンピュータ上のどのネットワーク インターフェース カード（NIC）でモニタするか、をカスタマイズすることができます。



内部コンピュータへのモニタリング要求



外部コンピュータへのモニタリング要求

各 Network Agent のインスタンスに、次のことが必要になります：

- モニタされるすべてのコンピュータに対する両方向のトラフィックを検出するために、適切にネットワーク内に配置されていること。
- トラフィックをモニタするための専用の少なくとも1つのNICがあること。

Network Agent は、複数の NIC をもつコンピュータにインストールすることができ、複数の NIC を要求のモニタ、およびブロック ページの送信に使用することができます。Network Agent コンピュータに新しい NIC を追加する場合、Network Agent サービスを再起動し、新しい NIC を設定します（NIC 設定、349 ページ を参照）。

> **ご注意：**
> Network Agent が、ネットワーク セグメントのトラフィックを参照することができるかどうか決定するためには、ネットワーク トラフィック検出ツールを使用します。Network Agent 設定の確認、352 ページ を参照してください。

Network Agent の配置と NIC 要件についての詳細は、『配備ガイド』を参照してください。

Network Agent で内部ネットワーク要求をモニタし、特定の NIC を使用して拡張ログを行うように設定する方法は、Network Agent の構成、345 ページ を参照してください。

Network Agent の構成

関連トピック：

- ハードウェア構成、344 ページ
- グローバル設定、346 ページ
- ローカル設定、347 ページ
- NIC 設定、349 ページ
- IP アドレスの追加と編集、351 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動作を設定するために、Websense Manager を使用します。Network Agent の設定は、2つのメインエリアに分かれます：

- **グローバル設定**は すべての Network Agent のインスタンスに影響を与えます。次のように設定します：
  - 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をリストします（例えば、内部 Web サーバー）。
  - 帯域幅の計測とプロトコル 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されます。次のように設定します：
  - 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 コンピュータのネットワーク カード（NIC）の使用方法を設定します（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）。

    また、ネットワーク カード設定で、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

関連トピック：

- ハードウェア構成、344 ページ
- ローカル設定、347 ページ
- NIC 設定、349 ページ
- IP アドレスの追加と編集、351 ページ

すべての Network Agent インスタンスの基本的なモニタリングとログ記録動作を定義するためには、**[設定]** > **[Network Agent]** > **[グローバル]** のページを使用します。

[内部ネットワーク定義] リストには ネットワーク内のコンピュータを指定します。デフォルトで、Network Agent は、これらのコンピュータ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。

エントリの初期セットがデフォルトで提供されています。追加エントリを追加するか、既存の項目を編集 / 削除することができます。

[モニタする内部トラフィック] リストには、[内部ネットワーク定義] 内で Network Agent にトラフィックをモニタ **させる**コンピュータを含めます。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。

- リストに適切な IP アドレス または 範囲を追加するためには、**[追加]** をクリックします。詳細は、IP アドレスの追加と編集、351 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ためには、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、351 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ためには、IP アドレス または 範囲の隣のチェックボックスにマークを付けて、[**削除**] をクリックします。

[**追加設定**] オプションで、Network Agent が帯域幅使用状況を計測する間隔、プロトコルト トラフィックを記録する頻度を決定できます :

フィールド	使用方法
帯域幅計測間隔	Network Agent が帯域幅使用状況を計測する頻度を、秒単位で、1 から 300 までの数字で入力します。例えば、300 と入力した場合、Network Agent が 5 分ごとに帯域幅を計測することを表します。 デフォルトは 10 秒です。
プロトコルのトラフィックを定期的にログに記録する	このオプションにマークを付けると、ログ記録間隔フィールドが有効になります。
ログ記録間隔	Network Agent がプロトコルを記録する頻度を、分単位で、1 から 300 までの数字で入力します。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。

変更を完了したら、変更をキャッシュするために [OK] をクリックします。[**すべて保存**] 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

関連トピック :

- ハードウェア構成、344 ページ
- グローバル設定、346 ページ
- NIC 設定、349 ページ

選択された Network Agent のインスタンスのフィルタリング動作、プロキシ情報、その他を設定するためには、[**設定**] > [Network Agent] > [**ローカル設定**] のページを使用します。選択された Network Agent のインスタンスの IP アドレスは、コンテンツペインのタイトルバーに表示され、左ナビゲーションペインでハイライトされます。

[Filtering Service の定義] は、選択された Network Agent インスタンスと Filtering Service の関連付けと、Filtering Service が利用可能でない場合の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 の IP アドレス	Network Agent と関連付けられた Filtering Service を選択します。
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 **[許可]** を選択し、すべての要求をブロックするには **[ブロック]** を選択します。デフォルトは 許可です。

正確に ユーザ要求がモニタされ、フィルタされ、記録されるために、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 アドレスを指定するために、**[プロキシとキャッシュ]** を使用します。

- リストに IP アドレス または 範囲を追加するためには、**[追加]** をクリックします。詳細は、IP アドレスの追加と編集、351 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ためには、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ためには、IP アドレス または 範囲の隣のチェックボックスにマークを付けて、**[削除]** をクリックします。

個々の NIC を設定するためには、**[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。**[名前]** コラムで NIC をクリックします。手順は、NIC 設定、349 ページ を参照してください。

ネットワークの HTTP 要求が非標準のポートを通過する場合、Network Agent がモニタするべき正しいポートを指定するために、**[Network Agent 詳細設定]** をクリックします。デフォルトで **HTTP トラフィックが使用するポート**は **8080、80** です。

Websense Technical Support によって指示された場合を除き、このセクションの他の設定を変更してはいけません。

フィールド	説明
モード	• なし（デフォルト） • 一般 • エラー • 詳細 • 帯域幅
出力	• ファイル（デフォルト） • ウィンドウ
ポート	55870（デフォルト）

Network Agent の設定の変更を完了したら、変更をキャッシュするために、[OK] をクリックします。[**すべて保存**] をクリックするまで、変更は適用されません。

NIC 設定

関連トピック :

- ハードウェア構成、344 ページ
- Network Agent の構成、345 ページ
- NIC のモニタリング設定、350 ページ
- IP アドレスの追加と編集、351 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]** > **[ローカル設定]** > **[NIC の構成]** のページを使用します。

NIC 情報エリアには、**IP アドレス**、**簡単な NIC の説明**、**カード名**を表示する変更可能なコンテクストが提供されています。この情報を正しい NIC を設定するために 使用してください。

モニタリング

複数の NIC 構成で、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。1 つ以上の NIC をトラフィックをモニタするために使用することもできます。

[トラフィックのモニタにこの NIC を使用する] を指定するために、**モニタリング** セクションを使用します。

- NIC をモニタリングのために使用しない場合、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。
- NIC をモニタリングのために使用する場合、チェックボックスを選択し、**[構成]** をクリックします。モニタリング動作の設定のページが開きます。その手順は、NIC のモニタリング設定、350 ページ を参照してください。

その他の NIC オプション

また、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. [ブロック中] で、**[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 ソフトウェアを動作させている場合、**[HTTP 要求のフィルタとログ記録]** 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 デバイス または アプリケーションと 統合している 場合、Network Agent が HTTP 要求をフィルタする 方法、および 記録する 方法を 指定するためには、**[統合]** 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。
   - Websense レポートで正確性を改善するためには、**[HTTP 要求をログ記録]** を選択します。
   - 統合製品を通して送信されない HTTP 要求だけをフィルタするために Network Agent を使用するためには、**[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. [プロトコル管理] で、Network Agent がこの NIC を非 HTTP プロトコルをフィルタするために使用するかを指定します :
   - プロトコル管理機能を動作させるためには、**[非 HTTP プロトコル要求をフィルタする]** をチェックします。これにより、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。詳細は、カテゴリおよびプロトコルのフィルタリング、36 ページ および プロトコルの使用、187 ページ を参照してください。
   - Bandwidth Optimizer 機能を有効にするためには、**[プロトコル別に帯域幅使用状況を測定する]** をチェックします。Network Agent は、この NIC を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するために使用します。詳細は、Bandwidth Optimizer による帯域幅の管理、194 ページ を参照してください。

NIC のモニタリング設定

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 どのコンピュータをモニタするかを指定するためには、**[ローカル設定] > [NIC の構成] > [モニタ リスト]** のページを使用します。

1. モニタ リストで、Network Agent が どの要求をモニタするか指定します :
   - **すべて** : Network Agent は、選択された NIC を使用して参照されるすべてのコンピュータ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 セグメントのすべてのコンピュータを含みます。
   - **なし** : Network Agent は 要求をモニタしません。
   - **指定** : Network Agent は、[モニタ リスト] に含められたネットワーク セグメントだけをモニタします。

2. [指定] を選択した場合、[**追加**] をクリックし、Network Agent がモニタするコンピュータの 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、351 ページ を参照してください。

   ご注意 :
   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ます。帯域幅ベースのフィルタリング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ためには、適切なリスト項目をチェックし、[**削除**] をクリックします。

3. [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 によって作成さ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 要求が Websense ログデータ または ステータス モニタ出力に含められません。

   a. コンピュータを指定するために、[**追加**] をクリックし、その IP アドレスを入力します。
   b. 追加のコンピュータを指定する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 の構成] ページに戻ります。[**すべて保存**] 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

関連トピック :

- グローバル設定、346 ページ
- ローカル設定、347 ページ
- NIC 設定、349 ページ

次の Network Agent リストを変更するためには、**[IP アドレスの追加]** または **[IP アドレスの編集]** のページを使用します : 内部ネットワーク定義、モニタする内部トラフィック、プロキシとキャッシュ、モニタ リスト、モニタ リスト例外。

- IP アドレス範囲を追加 / 編集する場合、リスト内の既存のエントリ (単一 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 / 編集する場合、それがリスト内に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方法は、次の通りです :

1. **[IP アドレス]** または **[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. 前の [Network Agent 設定] のページに戻るためには、**[OK]** をクリックします。新しい IP アドレス または 範囲が適切な表に表示されます。

   変更をキャッシュしないで前のページに戻るためには、**[キャンセル]** をクリックします。
4. 必要に応じて、IP アドレスの追加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、[IP アドレスの編集] のページに、すでに選択された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、前のページに戻るために **[OK]** をクリックします。

IP アドレスの追加 / 編集が完了したら、[Network Agent 設定] のページの **[OK]** をクリックします。**[すべて保存]** 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

Websense Manager で Network Agent の設定を行った後、ネットワーク トラフィック検出ツールを使用して、ネットワーク上のコンピュータが Websense ソフトウェアによって認識されることを確認します。

1. このツールを起動するには**[スタート]>[プログラム]>[Websense]>[ユーティリティ]>[ネットワーク トラフィック検出ツール]** の順にクリックします。
2. **[ネットワーク アダプタ]** ドロップダウンリストからネットワーク カードを選択します。
3. **[モニタされたネットワークの範囲]** リストに表示されるアドレスをチェックして、該当するすべてのサブネットワークがリストされていることを確認します。
4. **[サブネットワークの追加]**および**[サブネットワークの削除]**ボタンを使用して、ネットワークの中のテストする部分を変更します。
5. **[モニタの開始]** をクリックします。

   ネットワーク トラフィック検出ツールは、ネットワーク上のコンピュータがネットワークを通じて送信する情報をモニタすることによって、そのコンピュータを検出します。**[検出されたコンピュータの数]** リストは、検出されたコンピュータの数を示します。
6. このツールによって検出されたコンピュータの詳細な情報を表示するには、[モニタされたネットワークの範囲] リストでサブネットワークを選択し、**[検出したコンピュータの表示]** をクリックします。

   そのコンピュータがリストされていない場合、そのコンピュータがネットワーク トラフィックを生成していることを確認します。そのためには、そのコンピュータからブラウザを起動し、いずれかの Web サイトを参照します。次にネットワーク トラフィック検出ツールに戻り、そのコンピュータが **[検出したコンピュータの表示]** ダイアログボックスに表示されるかどうかをチェックします。

7. ネットワーク トラフィックの状況のテストが完了したとき、[**モニタの終了**] をクリックします。

いくつかのコンピュータが表示されない場合：

- ネットワークの構成と NIC 配置要件を確認します（ハードウェア構成、344 ページ を参照）。
- お客様の Websense ソフトウェア用の『インストール ガイド』で、より詳細なネットワーク構成情報を確認します。
- 適切にモニタリング用 NIC を設定していることを確認します（NIC 設定、349 ページ）。

15 トラブルシューティング

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 の Web サイトには、膨大な技術情報があります。www.websense.com/global/en/SupportAndKB/ にアクセスしてください。キーワードまたは参照番号によってトピックを検索するか、または、もっともよく読まれている記事を参照します。

トラブルシューティングについての説明は、次のセクションに分かれています。

インストールとライセンスの問題

Websense ステータスにライセンスの問題が表示される

マスタ データベースをダウンロードし、インターネット フィルタリングを実行するには、サブスクリプション キーを入力する必要があります。ライセンス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、Websense ヘルス モニタが警告を表示します。

- 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。
- ライセンス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、359 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 ステータスを確認するには、Websense Manager の [ステータス] > [今日] ページで **[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 ダウンロードの問題のトラブルシューティングに関するヘルプ情報は、マスタ データベースをダウンロードできない、358 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、またはライセンスが期限切れになっている場合、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、Websense Manager の設定に従って、すべてのユーザにフィルタなしでインターネット 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、26 ページ を参照してください。

アップグレード後に ユーザが Websense Manager に表示されない

ディレクトリ サービスとして Active Directory を選択した場合、Websense ソフトウェアのアップグレード後にユーザ名が Websense Manager に表示されないことがあります。これは、ユーザ名に UTF-8 キャラクタ セットに含まれない文字が含まれる場合に起こります。

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キャラクタ セットを MBCS から UTF-8 に変更します。そのため、UTF-8 キャラクタ 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、次の手順によって、手動でキャラクタ セットを MBCS に変更します。

1. Websense Manager で **[設定]** > **[ディレクトリ サービス]** を選択します。
2. ページ上部の [ディレクトリ] の下で **[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. **[詳細ディレクトリ設定]** をクリックします。
4. [キャラクタ セット] の下で **[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。
   [すべて保存] 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

初期フィルタリング データベースが使用されている

Websense マスタ データベースには、インターネット コンテンツのフィルタリングの基礎となるカテゴリー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フィルタリング機能を有効にするために使用します。

完全なフィルタリングを実行するには、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、30 ページ を参照してください。

完全なデータベースのダウンロードには、インターネットの接続スピード、帯域幅、使用可能なメモリ、ディスクの空き容量に応じて、数分から場合によっては 1 時間以上かかることがあります。

マスタ データベースが 1 週間以上前のものである

Websense マスタ データベースには、インターネット コンテンツのフィルタリングの基礎となるカテゴリー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、Websense Manager で定義されたスケジュールに従ってマスタ データベースへの変更をダウンロードします。デフォルトでは、ダウンロードは毎日行われるようにスケジュールされます。

手動でデータベースのダウンロードを開始するには、以下の手順を実行します。

1. Websense Manager で **[ステータス]** > **[今日]** ページを開き、次に **[データベースのダウンロード]** を選択します。

2. 該当するFiltering Serviceインスタンスの横の[**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、[**すべて更新**]をクリックしてすべての Filtering Service がインストールされているコンピュータへのダウンロードを開始します。

   ご注意：
   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、[**閉じる**]をクリックします。

   随時、[**データベースのダウンロード**]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、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またはプロトコル関連の変更を行わないことを推奨します。

マスタ データベースをダウンロードできない

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、以下のことをチェックします。

- Websense Manager でサブスクリプション キーを正しく入力したこと、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、359 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、359 ページ）。
- ファイアウォールまたはプロキシ サーバの設定をチェックして、Filtering Service が Websense ダウンロード サーバ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 サーバの設定の確認、360 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（ディスク スペースの不足、361 ページ）およびメモリ（メモリの不足、362 ページ）があることを確認します。
- 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機器（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、362 ページ）。

サブスクリプション キー

以下の手順によって、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します。

1. Websense Manager で **[設定]** > **[アカウント]** を選択します。
2. Websense, Inc.,または再販業者から受け取ったキーと**[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。キーの大文字 / 小文字が同じでなければなりません。
3. **[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、ライセンスを更新してください。
4. [設定] ダイアログボックスでキーを変更した場合、**[OK]** をクリックしてキーを有効にし、データベース ダウンロードを可能にします。

手動でデータベース ダウンロードを開始したり、最新のデータベース ダウンロードの状況をチェックするには、[ステータス] > [今日] ページの上部の **[データベースのダウンロード]** をクリックします。

インターネット アクセス

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 サーバーへ **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 でダウンロード サーバ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、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でブラウザを開きます。
2. 次の 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、リダイレクト ページが表示され、次に、ブラウザは Websense ホーム ページを表示します。

   そうならない場合、コンピュータが次のようになっていることを確認します。

   - ポート 80、またはユーザのネットワークで HTTP トラフィック用に指定されているポートを通じて通信できる
   - DNS 検索を正しく実行できるように構成されている
   - 必要なプロキシ サーバを使用するように構成されている（ファイアウォールまたはプロキシ サーバの設定の確認、360 ページを参照）

また、ゲートウェイに Filtering Service がインストールされているコンピュータからの 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。

3. 次にいずれかの方法で、コンピュータがダウンロード サイトと通信できることを確認します。
   - コマンド プロンプトから次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、ダウンロード サーバに接続できます。

ファイアウォールまたはプロキシ サーバの設定の確認

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 サーバを通じてダウンロードされる場合、Filtering Service がインストールされているコンピュータ上のブラウザが Web ページを正しく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、Web ブラウザのプロキシ サーバの設定を調べてください。

Microsoft Internet Explorer 7 の場合

1. **[ツール]** > **[インターネット オプション]** を選択します。
2. **[接続]** タブを開きます。
3. **[LAN設定]** をクリックします。**[プロキシ サーバ]** の下にプロキシ サーバの設定情報が表示されます。

   プロキシの設定をメモしておきます。

Mozilla Firefox 2 の場合

1. **[ツール]** > **[オプション]** > **[拡張]** を選択します。
2. **[ネットワーク]** タブを選択します。
3. **[設定]** をクリックします。[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。

次に、Websense ソフトウェアがダウンロードの実行のために同じプロキシ サーバを使用するように設定されていることを確認します。

1. Websense Manager で **[設定]** > **[データベースのダウンロード]** を選択します。
2. **[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を確認します。
3. **認証** 設定が正しいことを確認します。ユーザ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。基本認証を有効にする方法については Websense Knowledge Base を参照してください。

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 Websense 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、32 ページ）。

ディスク スペースの不足

Websense マスタ データベースは Websense の **bin** ディレクトリ（デフォルトでは、/opt/Websense/bin または C:¥Program Files¥Websense¥bin）に保存されます。このディレクトリが置かれているドライブには、圧縮されたデータベースをダウンロードするための十分なスペースと、データベースを解凍するための十分なスペースがなければなりません。

コンピュータには少なくともマスタ データベースのサイズの 2 倍の空きディスク スペースがなければなりません。マスタ データベースのエントリが増えると、ダウンロードのために必要とされるサイズが大きくなります。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 3 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。

空きディスク スペースを確認するには、Windows では Windows Explorer を使用します。

1. Windows Explorer（Internet Explorer ではありません）で **[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 ドライブに置かれます。
3. 右クリックし、ポップアップメニューから **[プロパティ]** を選択します。
4. [全般] タブで、空きスペースが 3 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、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 システムの中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、次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. 3 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、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。

十分なディスク スペースがあることが確認されたけれども、まだダウンロードの問題が解決されない場合は、すべての Websense サービスを終了し (Websense サービスの停止と起動、288 ページを参照)、**Websense.xfr** および **Websense**(拡張子なし) ファイルを削除し、サービスを開始し、次に手動で新しいデータベースをダウンロードします。

メモリの不足

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。たとえば、小さなネットワークでは、すべてのプラットフォームで、2 GB のメモリを推奨します。

システム要件については、『配備ガイド』を参照してください。

Windows システムのメモリをチェックするには、以下の手順を実行します。

1. [タスク マネージャ] を開きます。
2. **[パフォーマンス]** タブを選択します。
3. 利用可能な**物理メモリ**の合計を確認します。
4. インストールされているメモリが 2 GB 未満である場合、コンピュータの RAM をアップグレードしてください。

また、**[コントロール パネル] > [管理ツール] > [パフォーマンス]** でもこの情報を取得できます。

Linux システムのメモリをチェックするには、以下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、次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。
4. インストールされているメモリが 2 GB 未満である場合、コンピュータの RAM をアップグレードしてください。

制限アプリケーション

ウィルス スキャナやサイズ制限アプリケーション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、以下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、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て、Filtering Service を実行しているコンピュータを含めます。

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

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。Websense ソフトウェアはシステム 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。

ダウンロードが全く行われない場合は、マスタ データベースをダウンロードできない、358 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

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. [データベースのダウンロード] 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 サーバに接続した場合は、ルート記録をテクニカル 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 Websense ダウンロード サーバ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** ディレクトリの中の次のファイル：**websense.ini**、**eimserver.ini**、**config.xml**。

テクニカル サポートの連絡先については、www.websense.com/SupportPortal/default.aspx を参照してください。

フィルタリングの問題

Filtering Service が実行していない

Filtering Service が実行していないとき、インターネット要求をフィルタリングおよびログ記録することはできません。

以下の場合に 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。
- 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 データベースをダウンロードできない、358 ページを参照）。
- **websense.ini** ファイルが見つからないか、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、以下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¥Websense¥bin または /opt/Websense/bin）へ移動し、**websense.ini** がテキスト エディタで開くことを確認します。このファイルが壊れている場合は、バックアップ ファイルによって置換します。
- 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ツール、401 ページを参照）。
- Websense Manager からログオフし、Websense 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、288 ページを参照）。

  1 分間待ってから、再び Websense Manager にログオンします。

User Service を使用できない

User Service が実行していない、または Policy Server が User Service と通信できない場合、Websense ソフトウェアはユーザ ベースのフィルタリング ポリシーを正しく適用できません。

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、以下の手順に従います：

1. Websense Policy Server サービスを再開します（Websense サービスの停止と起動、288 ページを参照）。
2. Websense User Service を開始、または再開します。
3. Websense Manager を閉じます。

   1 分間待ってから、再び Websense Manager にログオンします。

まだ問題が解決しない場合は、以下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ツール、401 ページを参照）。
- Websense **bin** ディレクトリ（デフォルトでは、C:¥Program Files¥Websense¥bin または /opt/Websense/bin）へ移動し、**websense.ini** がテキスト エディタで開くことを確認します。このファイルが壊れている場合は、バックアップ ファイルによって置換します。

サイトが間違って「IT」に分類されている

Internet Explorer のバージョン 4.0 以上では、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、ユーザがアドレス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、Websense ソフトウェアは、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「IT（情報技術）/ 検索エンジン & 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。Websense ソフトウェアが要求されたサイトのカテゴリを基にフィルタリングするようにするには、アドレスバーからの検索をオフにしなければなりません。

1. **[ツール]** > **[インターネット オプション]** を選択します。
2. **[詳細設定]** タブを選択します。
3. [アドレス バーからの検索] の下の、**[アドレス バーから検索しない]** を選択します。
4. **[OK]** をクリックします。

> **ご注意：**
> この手順は Internet Explorer のバージョン 5、6、7 で有効です。

キーワードがブロックされない

この問題には 2 つの理由が考えられます。**[キーワード ブロックの無効化]** が選択されているか、または、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の Web サーバへ送信したことです。

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、以下の手順を実行します。

1. Websense Manager で、**[設定]** > **[フィルタリング]** を選択します。
2. [一般的なフィルタリング] の下の **[キーワードの検索オプション]** リストをチェックします。**[キーワード ブロックの無効化]** 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、Websense フィルタリング設定の構成、56 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。
   [すべて保存] をクリックするまで、変更は適用されません。

サイトが **post** を使用してデータを Web サーバへ送信する場合、Websense ソフトウェアはその URL のキーワード フィルタリング設定を認識しません。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。

サイトが post コマンドを使用するかどうかを調べるには、ブラウザでサイト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、そのサイト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 が指定どおりにフィルタリングされない

制限付きアクセス フィルタまたはカスタム URL リストの中の HTTPS URL が指定どおりにフィルタリングされない場合、統合製品がその URL を、Filtering Service が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、**https://<ドメイン>** という URL が **https://<IP アドレス>:443** に変換されます。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 フィルタと照合できず、サイトを正しくフィルタリングしません。

この問題を回避するには、カスタム URL または制限付きアクセス フィルタを使用してフィルタリングするサイトに IP アドレスと URL の両方を追加します。

ユーザが指定通りにプロトコルまたはアプリケーションにアクセスできない

ネットワークに Microsoft ISA Server が含まれていて、特定の認証方法を設定した場合にメッセージング アプリケーションへの接続が切断される可能性があります。

匿名認証以外の認証方法がアクティブになっている場合、プロキシ サーバーはユーザがアプリケーションへの接続を要求したときに受信したデータ パケットを識別しようとします。プロキシ サーバーはデータ パケットの識別に失敗し、接続が切断されます。これによって Websense のプロトコル フィルタリング アクティビティの正確さが損なわれる場合があります。

また、アプリケーションが使用するポートがブロックされる場合にも、プロトコルまたはインターネット アプリケーションにアクセスできなくなる可能性があります。これは次の場合に起こる可能性があります。

- ポートがファイアウォールによってブロックされている。
- ポートのいずれかの ID が、ブロックされているカスタム プロトコルに含まれている (単一ポートとして、またはポート範囲の一部として)。

FTP 要求が指定通りにブロックされない

Websense ソフトウェアは、Check Point® ファイアウォールと統合されているとき、FTP 要求を認識しフィルタリングするためにはクライアントのブラウザで **[フォルダの表示]** が有効にされていることを必要とします。

[フォルダの表示] が有効にされていない場合、FireWall-1 プロキシへ送信された FTP 要求は接頭辞「http://」が付いた形式で Websense ソフトウェアへ送信されます。その結果、Websense ソフトウェアはこれらの要求を FTP 要求としてではなく、HTTP 要求としてフィルタリングします。

Websense ソフトウェアがユーザまたはグループ ポリシーを適用しない

ユーザまたはグループ ポリシーを割り当てた後でも Websense ソフトウェアがコンピュータまたはネットワーク ポリシーもしくは**デフォルト** ポリシーを適用する場合にはユーザ識別の問題、371 ページを参照してください。詳細については技術情報を参照してください。

リモート ユーザが正しいポリシーによってフィルタリングされない

リモート ユーザがキャッシュされたドメイン資格情報（ネットワーク ログイン情報）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、Websense ソフトウェアはそのユーザ、またはそのユーザのグループもしく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、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、もしくはユーザがローカル ユーザ アカウントを使ってコンピュータにログオンした場合、Websense ソフトウェアはデフォルト ポリシーを適用します。

ユーザがユーザまたはグループ ポリシー、もしくはデフォルト ポリシーによってフィルタリングされない場合があります。これはユーザがローカル ユーザ 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、ポリシーの対象となるネットワーク内 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

Network Agent がインストールされていない

プロトコルに基づいたフィルタリングを可能にするには、Network Agent がインストールされていなければなりません。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 フィルタリングまたはログ記録を必要としない場合、「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。その手順は、現在のシステム ステータスの確認、296 ページ を参照してください。

スタンドアロン 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フィルタするために Network Agent がインストールされている必要があります。そのための手順については、『インストール ガイド』を参照し、次に Network Agent の構成、345 ページを参照してください。

Network Agent が実行していない

プロトコルに基づいたフィルタリングを可能にするには、Network Agent がインストールされていなければなりません。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 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フィルタするために 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、以下の手順を実行します。

1. [Windows サービス] ダイアログボックス (Windows のサービス ダイアログ ボックス、401 ページを参照) で、**Websense Network Agent** サービスが開始しているかどうかを調べます。
2. **Websense Policy Broker** および **Websense Policy Server** サービスを再開します (Websense サービスの停止と起動、288 ページを参照)。
3. **Websense Network Agent** サービスを開始、または再開します。
4. Websense Manager を閉じます。
5. 1 分間待ってから、再び Websense Manager にログオンします。

それでも問題が解決しない場合は、以下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、401 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、402 ページを参照)。

Network Agent が NIC をモニタしていない

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、Network Agent の設定を更新しなければなりません。

1. Websense Manager で **[設定]** 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 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 の構成、345 ページ を参照してください。

Network Agent が Filtering Service と通信しない

インターネット使用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？

  「はい」なら Filtering Service の IP アドレスまたは UID 情報の更新、370 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 インタフェース カード (NIC) がありますか？

  「はい」なら、ネットワークの構成、343 ページの説明に従って Websense ソフトウェアの設定を確認します。

- Network Agent に接続しているスイッチを再構成しましたか？

  「はい」なら、『インストールガイド』に従ってハードウェア設定を確認し、Network Agent の構成、345 ページの説明に従って Websense の設定を確認します。

このいずれもあてはまらない場合は、ローカル設定、347 ページの Network Agent と Filtering Service の関連付けに関する説明をお読みください。

Filtering Service の IP アドレスまたは UID 情報の更新

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。Websense 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、以下の手順を実行します。

1. Websense Manager を開きます。

   ステータス メッセージは、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 **[設定]** 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 がインストールされているコンピュータの IP アドレスを選択します。
4. ページ上部の [Filtering Service の定義] の下の **[サーバーの IP アドレス]** リストを展開し、次に 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。**[すべて保存]** をクリックするまで、変更は適用されません。

ユーザ識別の問題

関連トピック：

- フィルタリングの問題、364 ページ
- リモート ユーザが手動認証の入力を求められない、381 ページ
- リモート ユーザが正しくフィルタリングされない、381 ページ

ユーザまたはグループ ベースのポリシーを割り当てた後でも Websense ソフトウェア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またはネットワーク ポリシーもしくは**デフォルト** ポリシーを適用する場合には、以下の手順によって問題の原因を調べます。

- Microsoft ISA Server を使用していて、その認証方法を変更した場合、Web Proxy Service が再開していることを確認します。
- 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に適用されます。ユーザ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。User Service キャッシュの更新を強制するには、Websense Manager での何かの変更をキャッシュして、[**すべて保存**] をクリックします。
- Windows XP SP2 を実行しているコンピュータ上のユーザが不適切にフィルタリングされる場合、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、デフォルトで有効にされています。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 ログオン情報を取得できるようにするには、以下の手順を実行します。

  1. クライアント コンピュータ上の Windows の [**スタート**] メニューから [**設定**] > [**コントロール パネル**] > [**セキュリティ センター**] > [**Windows ファイアウォール**] を選択します。
  2. [**例外**] タブを選択します。
  3. [**ファイルとプリンタの共有**] にチェックを付けます。
  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。

Websense 透過的識別エージェントを使用している場合、該当するトラブルシューティングのセクションを参照してください。

- DC Agent のトラブルシューティング、372 ページ .

- Logon Agent のトラブルシューティング、374 ページ .
- eDirectory Agent のトラブルシューティング、377 ページ .
- RADIUS Agent のトラブルシューティング、379 ページ .

DC Agent のトラブルシューティング

DC Agent でのユーザ識別の問題のトラブルシューティングでは、以下の手順を実行します。

1. すべてのネットワーク接続をチェックします。
2. Windowsイベントビューワでエラー メッセージをチェックします(Windows イベント ビューア、401 ページを参照)。
3. Websense ログ ファイル (Websense.log) で、詳細なエラー情報を確認します (Websense ログ ファイル、402 ページを参照)。

DC Agent でのユーザ識別の問題の一般的な原因として、次のことが考えられます。

- ネットワーク サービスまたは Windows サービスがドメイン コントローラとの間で、DC Agent からはポリシーが定義されていない新規ユーザと認識されるような方法で通信している。ユーザがデフォルト ポリシーによって不適切にフィルタリングされる、372 ページを参照してください。
- DC Agent または 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て、ドメイン コントローラには匿名ユーザと同様に扱われる。ドメインコントローラが匿名ユーザ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、DC Agent はリストをダウンロードすることを許可されません。手動での DC Agent および User Service の許可の変更、373 ページを参照してください。
- User Service キャッシュが古くなっている。User Service は、デフォルトでは、ユーザ名の 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。キャッシュはまた、Websense Manager で変更を行って、[**すべて保存**] をクリックするたびに更新されます。

ユーザがデフォルト ポリシーによって不適切にフィルタリングされる

何らかのネットワークまたは Microsoft Windows 200x がドメイン コントローラに接続したとき、接続に使用されたアカウント名から Websense ソフトウェアが、識別できないユーザがフィルタリングされているコンピュータからインターネットにアクセスしようとしていると判断することがあります。このユーザにはユーザまたはグループ ベースのポリシーが割り当てられていませんから、コンピュータまたはネットワークのポリシーまたはデフォルト ポリシーが適用されます。

- ネットワーク サービスでは、ネットワーク上のデータにアクセスするためにドメイン権限が要求されることがあり、ドメイン コントローラとの接続には、サービスの実行に使用しているドメイン ユーザ名が使用されます。

この問題を解決する方法については、特定のユーザ名を無視するエージェントの設定、238 ページを参照してください。

- Windows 200x サービスは定期的に、コンピュータ名とその後のドル記号によって設定されるユーザ名（例、jdoe-computer$）を使ってドメイン コントローラに接続します。DC Agent はサービスを、ポリシーが設定されていない新規ユーザとして解釈します。

  この問題を解決するには、以下の手順によって、DC Agent が **computer$** の形式のログオンを無視するように設定します。

  1. DC Agent がインストールされているコンピュータ上で、Websense **bin** ディレクトリに移動します（デフォルトでは、**C:¥Program Files¥Websense¥bin**）。
  2. テキストエディタで **transid.ini** ファイルを開きます。
  3. ファイルに次のエントリを追加します。

     ```
     IgnoreDollarSign=true
     ```

  4. ファイルを保存して閉じます。
  5. DC Agent を再開します（Websense サービスの停止と起動、288 ページを参照してください）。

手動での DC Agent および User Service の許可の変更

ドメイン コントローラが実行しているコンピュータで、以下の手順を実行します。

1. ユーザ アカウントを作成します。例、**Websense**。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［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ステップ 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. Websense DC Agent がインストールされている各コンピュータで［Windows サービス］ダイアログボックスを開きます（**［開始］>［プログラム］>［管理ツール］>［サービス］**を選択します）。
3. **[Websense DC Agent]** をクリックし、**［停止］**をクリックします。
4. **[Websense DC Agent]** をダブルクリックします。
5. **［ログオン］**タブで、**［このアカウント］**オプションを選択します。
6. ステップ 1 で作成した Websense DC Agent アカウントのユーザ名を入力します。例、**DomainName¥websense**
7. このアカウントの Windows パスワードを入力および確認してください。
8. **[OK]** をクリックしてダイアログボックスを閉じます。
9. ［サービス］ダイアログボックスで**[Websense DC Agent]**を選択し、**[開始]**をクリックします。

10. Websense User Service の各インスタンスに対してこの手順を繰り返します。

Logon Agent のトラブルシューティング

ネットワーク内のいずれかのユーザが Logon Agent によって識別されないために**デフォルト** ポリシーによってフィルタリングされる場合、以下のことを調べてください。

- Windows グループ ポリシー オブジェクト (GPO) がこれらのユーザのコンピュータに正しく適用されていることを確認します (グループ ポリシー オブジェクト、374 ページを参照)。
- User Service が Linux コンピュータ上にインストールされていて、ユーザが Windows Active Directory (ネイティブ モード) を使用している場合、ディレクトリ サービスの設定をチェックします (Linux 上の User Service の実行、375 ページを参照)。
- クライアント コンピュータが、ログオン スクリプトを実行しているドメイン コントローラと通信できることを確認します。(ドメイン コントローラの状況、375 ページを参照)。
- クライアント コンピュータ上で NetBIOS が有効になっていることを確認します (NetBIOS、375 ページを参照)。
- クライアント コンピュータ上のユーザ プロファイルが壊れていないことを確認します (ユーザ プロファイルの問題、376 ページを参照)。

グループ ポリシー オブジェクト

ユーザの環境が Websense ソフトウェアの『インストール ガイド』で示している前提条件を満たしていることを確認した後、そのグループ ポリシー オブジェクトが正しく適用されていることを確認します。

1. Active Directory がインストールされているコンピュータで、Windows の [コントロール パネル] を開き、**[管理ツール] > [Active Directory ユーザとコンピュータ]** を選択します。
2. ドメイン エントリを右クリックし、次に、**[プロパティ]** を選択します。
3. **[グループ ポリシー]** タブをクリックし、[グループ ドメイン ポリシー オブジェクト リンク] リストからドメイン ポリシーを選択します。
4. **[編集]** をクリックし、ディレクトリ ツリーの [ユーザ構成] ノードを展開します。
5. [Windows 設定] ノードを展開し、**[スクリプト]** を選択します。
6. 右側のペインで、**[ログオン]** をダブルクリックし、次に、**logon.bat** が [ログオン プロパティ] ダイアログボックスにリストされていることを確認します。

   このスクリプトはクライアントのログオン アプリケーションによって要求されます。

   - スクリプトの中に **logon.bat** がない場合、Websense ソフトウェアの『インストール ガイド』の「初期設定」の章を参照してください。

- スクリプトの中に**logon.bat**があるにもかかわらずLogon Agentが動作していない場合、このセクションの中の別のトラブルシューティング手順を使って、ネットワーク接続の問題がないことを確認するか、または Websense Knowledge Base を参照してください。

Linux 上の User Service の実行

ユーザの透過的識別のために Logon Agent を使用していて、User Service が Linux コンピュータにインストールされているとき、Websense を一時的に、混在モードの Active Directory と通信するように設定する必要があります。

1. Websense Manager で **[設定]** >**[ディレクトリ サービス]** を選択します。
2. 現在のディレクトリ設定をメモしておきます。
3. [ディレクトリ] の下で **[Windows NT Directory / Active Directory (混在モード)]** を選択します。
4. **[OK]** をクリックして変更をキャッシュし、**[すべて保存]** をクリックします。
5. [ディレクトリ] の下で、**[Active Directory (ネイティブ モード)]** を選択します。元の設定が表示されない場合、手順 2 で記録したメモを使ってディレクトリ設定を再作成します。その方法の詳細については、Windows Active Directory (ネイティブ モード)、64 ページ を参照してください。
6. 設定の変更を完了したら、**[OK]** をクリックし、次に **[すべて保存]** をクリックします。

ドメイン コントローラの状況

クライアント コンピュータがドメイン コントローラと通信できることを確認するには、以下の手順を実行します。

1. クライアント コンピュータ上のドライブをドメイン コントローラのルート共有ドライブへマッピングします。これはログオン スクリプトが通常実行しているドライブで、**LogonApp.exe** はここに常駐します。
2. クライアント コンピュータで、Windows コマンド プロンプトを開き、次のコマンドを実行します。

   ```
   net view /domain:<domain name>
   ```

これらのテストのいずれかが失敗した場合、Windows オペレーティング システムのマニュアルでその解決方法を調べてください。Websense ソフトウェアに関係しないネットワーク接続の問題があります。

NetBIOS

Websense ログオン スクリプトをユーザのコンピュータ上で実行するには、NetBIOS for TCP/IP が有効にされていて、TCP/IP NetBIOS ヘルパー サービスが実行している必要があります。

クライアント コンピュータで NetBIOS for TCP/IP が有効にされていることを確認するには、以下の手順を実行します。

1. **[マイ ネットワークプレース]**を右クリックし、**[プロパティ]**を選択します。
2. **[ローカル エリア接続]**を右クリックし、**[プロパティ]**を選択します。
3. **[インターネット プロトコル (TCP/IP)]**を選択し、**[プロパティ]**をクリックします。
4. **[詳細]**をクリックします。
5. **[WINS]**タブを選択し、次に、正しい NetBIOS オプションが設定されていることを確認します。
6. 変更を行った場合、**[OK]**をクリックし、次に、他の [プロパティ]ダイアログボックスを閉じて変更を保存するために **[OK]**を 2 回クリックします。

   変更が必要でない場合、**[キャンセル]**をクリックして変更を行わずに各ダイアログボックスを閉じます。

Windows の [サービス] ダイアログボックスを使用して、クライアント コンピュータ上で **TCP/IP NetBIOS ヘルパー** サービスが実行していることを確認します (Windows のサービス ダイアログボックス、401 ページを参照)。TCP/IP NetBIOS ヘルパー サービスは、Windows 2000、Windows XP、Windows Server 2003、および Windows NT 上で動作します。

ユーザ プロファイルの問題

クライアント コンピュータ上のユーザ プロファイルが壊れている場合、Websense ログオン スクリプト (および Windows GPO 設定) を実行できません。この問題は、ユーザ プロファイルを再作成することによって解決できます。

ユーザ プロファイルを再作成するとき、ユーザの既存の「マイ ドキュメント」フォルダ、「使用頻度の高いレポート」、およびその他のカスタム データおよび設定は、自動的には新しいプロファイルに転送されません。新しいプロファイルによって問題が解決されたことを確認して、ユーザの既存のデータを新しいプロファイルにコピーするまで、既存の壊れたプロファイルを削除してはいけません。

ユーザ プロファイルを再作成するには、以下の手順を実行します。

1. ローカル管理者権限でクライアント コンピュータにログオンします。
2. ユーザ プロファイルを含むディレクトリの名前を次のように変更します。

   ```
   C:\Documents and Settings\<user name>
   ```

3. コンピュータを再起動します。
4. フィルタリングされたユーザとして、コンピュータにログオンします。新しいユーザ プロファイルが自動的に作成されます。
5. ユーザが指定通りにフィルタリングされていることを確認します。
6. カスタム データ (「マイ ドキュメント フォルダ」の内容など) を古いプロファイルから新しいプロファイルにコピーします。[ファイルおよび設定の転送] ウィザードを使用してはいけません。これを使用すると、破損した部分が新しいプロファイルに転送される可能性があります。

eDirectory Agent のトラブルシューティング

関連トピック：

- eDirectory Agent 診断を有効にする、378 ページ
- eDirectory Agent が eDirectory Server の接続をミスカウントする、378 ページ
- eDirectory Agent をコンソール モードで実行する、379 ページ

ユーザ名が eDirectory Agent に渡されない場合、ユーザが適切にフィルタリングされない場合があります。ユーザが Novell eDirectory サーバにログオンしなかった場合、eDirectory Agent はそのログオンを検出できません。これは以下の原因で起こります。

- ユーザが eDirectory ユーザ ログオン セッションのデフォルト ルート コンテクストに含まれていないドメインにログオンした。このルート コンテクストはインストール時に指定され、[**設定**] > [**ディレクトリ サービス**] ページで Novell eDirectory のために指定されたルート コンテクストと一致している必要があります。
- ユーザが Websense フィルタリングを回避するためにログオン プロンプトをバイパスしようとした。
- ユーザが eDirectory サーバでアカウントをセットアップしていない。

ユーザが eDirectory サーバにログオンしない場合、ユーザ固有のポリシーをそのユーザに適用することができません。代わりに、**デフォルト**ポリシーが有効になります。ネットワーク内にユーザが匿名でログオンする共有ワークステーションがある場合、これらのコンピュータに対するフィルタリング ポリシーをセットアップします。

eDirectory Agent がユーザ名を受け取り、そのユーザを識別するか否かを判断するには、以下の手順を実行します。

1. eDirectory Agent 診断を有効にする、378 ページに示す方法で eDirectory Agent のログ記録をアクティブにします。
2. 指定したログ ファイルをテキスト エディタで開きます。
3. 適切にフィルタリングされていないユーザに対応するエントリを検索します。
4. 次のようなエントリによって、eDirectory Agent がユーザを識別したことが示されます。

   ```
   WsUserData::WsUserData()
   User: cn=Admin,o=novell (10.202.4.78)
   WsUserData::~WsUserData()
   ```

   上の例では、ユーザ **Admin** が eDirectory サーバにログオンし、正常に識別されました。

5. ユーザが識別されているにもかかわらず、指定通りフィルタリングされない場合、ポリシー設定をチェックして、そのユーザに適切なポリシーが適用されていること、および Websense Manager 内のユーザ名が Novell eDirectory 内のユーザ名と対応することを確認します。

   ユーザが識別されない場合、以下のことを確認します。

   - ユーザが Novell eDirectory アカウントを持っている。
   - ユーザが eDirectory ユーザ ログオンのデフォルト ルート コンテクストに含まれているドメインにログオンしている。
   - ユーザがログオン プロンプトをバイパスしていない。

eDirectory Agent 診断を有効にする

eDirectory Agent には診断機能が組み込まれていますが、デフォルトではこれらの機能は有効にされていません。インストール時または他の任意の時点で、ログ記録およびデバッグを有効にできます。

1. eDirectory Agent を停止します (Websense サービスの停止と起動、288 ページを参照してください)。
2. eDirectory Agent をインストールしているコンピュータ上で eDirectory Agent のインストール ディレクトリを選択します。
3. テキスト エディタでファイル **wsedir.ini** を開きます。
4. **[eDirAgent]** セクションを見つけます。
5. ログ記録およびデバッグ機能を有効にするには、次のように **[DebugMode]** の値を **[On]** に変更します。

   ```
   DebugMode=On
   ```

6. ログの詳細レベルを指定するには、次の行を変更します。

   ```
   DebugLevel=<N>
   ```

   N を 0 ～ 3 の値に設定できます。ここで、3 は最も詳細なレベルを示します。
7. ログ 出力ファイルの名前を指定するために、**LogFile** の行を変更します。

   ```
   LogFile=filename.txt
   ```

   デフォルトでは、ログ出力は eDirectory Agent コンソールに送信されます。エージェントをコンソール モード (eDirectory Agent をコンソール モードで実行する、379 ページを参照) で実行している場合、デフォルト値を保持することができます。
8. **wsedir.ini** ファイルを保存して閉じます。
9. eDirectory Agent サービスを開始します (Websense サービスの停止と起動、288 ページを参照)。

eDirectory Agent が eDirectory Server の接続をミスカウントする

eDirectory Agent がネットワーク内で 1000 以上のユーザを監視しているにもかかわらず、Novell eDirectory サーバーには 1000 の接続だけが表示される場合、eDirectory サーバーから Websense eDirectory Agent に情報を伝達する

Windows API の制限が原因である可能性があります。これが起こるのは非常にまれです。

この制限を回避するには、**wsedir.ini** ファイルにサーバー接続を正確にカウントするパラメータを追加します (Windows のみ)。

1. Websense eDirectory Agent サービスを停止します (Websense サービスの停止と起動、288 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¥Websense¥bin**) を選択します。
3. テキスト エディタで **wsedir.ini** ファイルを開きます。
4. 空白の行を挿入し、次のように入力します。

   ```
   MaxConnNumber = <NNNN>
   ```

   ここで、<NNNN> は Novell eDirectory サーバへの接続の最大数です。たとえば、ネットワークのユーザ数が 1,950 であれば、最大数として 2000 を入力するとよいでしょう。
5. ファイルを保存します。
6. eDirectory Agent を再起動します。

eDirectory Agent をコンソール モードで実行する

1. 次のどちらかを実行します。
   - Windows コマンド プロンプト (**[スタート] > [ファイル名を指定して実行] > [cmd]**) で、次のコマンドを入力します。

     ```
     eDirectoryAgent.exe -c
     ```
   - Linux コマンド シェルで、次のコマンドを入力します。

     ```
     eDirectoryAgent -c
     ```
2. エージェントを停止する準備ができたとき、**[Enter]** を押します。エージェントの実行を停止するために数秒かかることがあります。

RADIUS Agent のトラブルシューティング

RADIUS Agent には診断機能が組み込まれていますが、これらの機能はデフォルトではアクティブ化されません。RADIUS Agent のログ記録およびデバッグ機能をアクティブにするには、以下の手順を実行します。

1. RADIUS Agent を停止します (Websense サービスの停止と起動、288 ページを参照)。
2. RADIUS Agent がインストールされているコンピュータで、エージェントのインストール ディレクトリ (デフォルトでは、**Websense¥bin¥**) に進みます。
3. テキストエディタで **wsradius.ini** ファイルを開きます。
4. **[RADIUSAgent]** セクションを見つけてください。
5. ログ記録およびデバッグ機能を有効にするには、次のように **[DebugMode]** の値を **[On]** に変更します。

```
DebugMode=On
```

6. ログの詳細レベルを指定するには、次の行を変更します。

   ```
   DebugLevel=<N>
   ```

   N を 0 ～ 3 の値に設定できます。ここで、3 は最も詳細なレベルを示します。
7. **LogFile** 行を出力ファイルの名前に対応するように変更します。

   ```
   LogFile=filename.txt
   ```

   デフォルトでは、ログ出力は RADIUS Agent コンソールに送信されます。エージェントをコンソール モードで実行している場合 (RADIUS Agent をコンソール モードで実行する、380 ページを参照)、オプションとして、デフォルト値のままにしておくことができます。
8. **wsradius.ini** ファイルを保存して、閉じます。
9. RADIUS Agent サービスを開始します (Websense サービスの停止と起動、288 ページを参照)。

リモート ユーザが設定通りに識別およびフィルタリングされていない場合、考えられる原因は RADIUS Agent と RADIUS サーバー間の通信の問題です。原因を判断するために、RADIUS Agent ログでエラーをチェックします。

RADIUS Agent をコンソール モードで実行する

RADIUS 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、以下のどちらかのコマンドを入力します。

- Windows コマンド プロンプトで

  ```
  RadiusAgent.exe -c
  ```
- Linux シェル プロンプトで

  ```
  ./RadiusAgent -c
  ```

いつでも、再度 **[Enter]** を押すとエージェントが停止します。エージェントの実行を停止するために数秒かかることがあります。

RADIUS Agent は、以下のコマンドライン パラメータを受け入れます。

> **ご注意 :**
> Linux では、–r および –s パラメータの代わりに、Websense RADIUS Agent を開始または停止するためのスクリプト (**WsRADIUSAgent start|stop**) を使用することを推奨します。

パラメータ	説明
–i	RADIUS Agent サービス / デーモンをインストールします。
–r	RADIUS Agent サービス / デーモンを実行します。
–s	RADIUS Agent サービス / デーモンを停止します。

パラメータ	説明
-c	RADIUS Agent をサービスまたはデーモンとしてではなくアプリケーション プロセスとして実行します。コンソール モードでは、RADIUS Agent がログ出力をコンソールまたはテキスト ファイルに送信するように設定できます。
-v	RADIUS Agent のバージョン番号を表示します。
-? -h -help <no option>	使用状況の情報をコマンドラインに表示します。可能なすべてのコマンドライン パラメータをリストし、説明します。

リモート ユーザが手動認証の入力を求められない

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求めら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 ユーザが正しくフィルタリングされない

リモート ユーザがフィルタリングされない場合、または割り当てられたポリシーによってフィルタリングされない場合、RADIUS Agent ログをチェックして、**Error receiving from server: 10060** (Windows の場合) または **Error receiving from server: 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 サーバが適切に設定されていることを確認します (RADIUS 環境の設定、224 ページを参照)。

RADIUS Agent に組み込まれている診断ツールを使用して、フィルタリングの問題をトラブルシューティングできます (RADIUS Agent のトラブルシューティング、379 ページを参照)。

Remote Filtering 機能 (リモート クライアントのフィルタ、159 ページを参照) を実装している場合、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、リモート ユーザをフィルタリングできません。

Remote Filtering のセットアップの方法は、Remote Filtering 技術資料を参照してください。

ブロック メッセージの問題

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

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、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

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、288 ページを参照)。
2. Websense **bin** ディレクトリに移動します (デフォルトでは、C¥Program Files¥Websense¥bin または /opt/websense/bin)。

3. テキストエディタで **eimserver.ini** ファイルを開きます。
4. [WebsenseServer] の下に空白の行を追加し、次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、次のように入力します。

   ```
   BlockMsgServerName = 10.201.72.15
   ```

5. ファイルを保存して閉じます。
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、**BlockMsgServerName** パラメータで他の NIC の IP アドレスの入力してみます。

それでもブロック ページが表示されない場合、ユーザが以下の 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ます。

- 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、Websense Knowledge Base でその他のトラブルシューティングのヒントを参照してください。

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

広告がブロックされたとき、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とき、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。これは以下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とき、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ときの通常の方法です)。要求された URL が .gif または同様の拡張子で終わる場合、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。
- 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 UTF-8、日本語の場合 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。

プロトコル ブロック メッセージが設定通り表示されない

以下のいずれかの理由によってプロトコル ブロック メッセージが表示されないか、または遅れて表示されることがあります。

- プロトコル ブロック メッセージを適切に表示するためには、Windows コンピュータ上に User Service がインストールされている必要があります。詳細は、『インストールガイド』を参照してください。
- Network Agent が複数のネットワーク インタフェース カード (NIC) をもつコンピュータ上にインストールされており、NIC が Filtering Service 以外のネットワーク セグメントをモニタリングしている場合、プロトコル ブロック メッセージがクライアント コンピュータに到達しない場合があります。Filtering Service コンピュータに NetBIOS があり、Server Message Block プロトコルがクライアント コンピュータにアクセスし、そのポート 15871 がブロックされていないことを確認します。
- Network Agent が内部コンピュータ**に送信された**要求をモニタするように設定されているとき、プロトコル ブロック メッセージが少し遅れるか、または、要求されたプロトコル データの発信元の内部コンピュータに表示される (クライアント コンピュータにではなく) ことがあります。
- フィルタリングされたクライアントまたは Websense フィルタリングがインストールされているコンピュータが Windows 200x を実行している場合、プロトコル ブロック メッセージを表示するには、Windows **Messenger** サービスが実行している必要があります。クライアントまたはサーバ コンピュータ上の Windows Services ダイアログボックスを使用して、Messenger サービスが実行しているかどうかを調べます (Windows のサービス ダイアログボックス、401 ページを参照)。ブロック メッセージが表示されない場合でも、プロトコルはブロックされています。

ブロック ページの代わりにプロトコル ブロック メッセージが表示される

統合製品が Websense ソフトウェアに HTTPS 情報を送信しない場合、または Websense ソフトウェアがスタンドアロン モードで実行している場合、Network Agent は、カテゴリ設定のためにブロックされている HTTPS サイト要求をプロトコル要求として解釈することがあります。その結果、プロトコル ブロック メッセージが表示されます。また、HTTPS 要求はプロトコル要求としてログ記録されます。

ログ、ステータス メッセージ、およびアラートの問題

Websense コンポーネントのエラー メッセージを探す方法

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、Websense Manager の [**ステータス**] > [**今日**] ページの上部の [**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、385 ページを参照)。

- アラート メッセージをクリックすると、[**ステータス**] > [**アラート**] ページに詳細な情報が表示されます。
- [ステータス] > [アラート] ページのメッセージの隣の [**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を支援する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 (デフォルトでは C:¥Program Files¥Websense¥bin または /opt/Websense/bin) の **websense.log** ファイルに記録されます。Websense ログ ファイル、402 ページを参照してください。

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、401 ページを参照してください。

Websense のヘルス アラート

Websense の [ヘルス アラートの要約] は、Websense ソフトウェアのコンポーネントのモニタリングで検出された潜在的な問題をリストします。これには次のような問題が含まれます。

- Filtering Service が実行していない
- User Service を使用できない
- Log Server が実行していない
- Policy Server のための Log Server が設定されていない
- ログ データベースを使用できない
- Network Agent が実行していない
- Policy Server のための Network Agent が設定されていない
- モニタリング用の NIC が Network Agent 用に設定されていない
- Network Agent 用の NIC が Network Agent 用に設定されていない
- 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 データベースの更新中
- マスタ データベースが 1 週間以上前のものである
- マスタ データベースのダウンロードが失敗した
- WebCatcher が無効にされている
- ライセンスの問題がある
- サブスクリプション キーの有効期限切れが近づいている
- サブスクリプション キーが入力されていない

[アラート]ページには、エラーまたは警告状態に関する基本情報が表示されます。問題の解決方法を調べるには、**[ソリューション]**をクリックします。

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ときに、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、296 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

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、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 を無効にします。

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。詳細は、NIC 設定、349 ページ を参照してください。

Policy Server と Policy Database の問題

- パスワードを忘れた、386 ページ
- Policy Server にログオンできない、387 ページ
- Websense Policy Database サービスが開始しない、387 ページ

パスワードを忘れた

ユーザが優先管理者または指定済み管理者であり、Websense Manager から Websense ユーザ アカウントを使用して Policy Server にログオンしている場合、任意の無条件優先管理者がパスワードをリセットできます。

- WebsenseAdministrator パスワードは、**[設定]** > **[アカウント]** ページで設定されます。
- 他の管理者アカウント パスワードは、**[指定済み管理]** > **[Websense ユーザ アカウントの管理]** ページで設定されます。

ユーザが指定済み管理を使用せず、WebsenseAdministrator パスワードを忘れた場合、MyWebsense にログオンし、パスワードをリセットします。

- MyWebsense アカウントに関連付けられたサブスクリプション キーが、現在の Websense Web Security または Websense Web Filter サブスクリプション キーと一致している必要があります。
- 複数のサブスクリプション キーがある場合、パスワード リセット処理を正常に完了するためには、該当する Websense Web Security または Websense Web Filter キーを選択する必要があります。
- リセット処理を完了するためには、Websense Manager コンピュータへのアクセス権限が必要です。

Policy Server にログオンできない

選択した Policy Server IP アドレスが正しいことを確認します。Websense Manager に Policy Server を追加した後で Policy Server コンピュータのアドレスが変更された場合、別の Policy Server にログオンし、Websense Manager から古い IP アドレスを削除し、新しい Policy Server IP アドレスを追加する必要があります。Policy Server インスタンスの追加と編集、280 ページを参照してください。

Websense Manager が突然停止した場合、または kill (Linux の場合) もしくは End Task (Windows の場合) コマンドによって停止された場合、数分待ってから再度ログオンします。Websense ソフトウェアは 3 分以内に、終了したセッションを検出し、閉じます。

Websense Policy Database サービスが開始しない

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 コンピュータにログオンします。
2. **[スタート]** > **[プログラム]** > **[管理ツール]** > **[コンピュータの管理]** の順に選択します。
3. ナビゲーションペインの [システム ツール] の下の **[ローカル ユーザとグループ]** を展開し、**[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、**[パスワードの設定]** 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. [コンピュータ管理] ダイアログボックスを閉じます。
7. **[スタート]** > **[プログラム]** > **[管理ツール]** > **[サービス]** の順に選択します。
8. **[Websense Policy Database]** を右クリックし、**[プロパティ]** を選択します。

9. [プロパティ] ダイアログボックスの [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、[**開始**] を選択します。

サービスが開始したとき、[サービス] ダイアログボックスを閉じます。

指定済み管理の問題

管理されたクライアントをロールから削除できない

以下の場合に、[指定済み管理] > [ロールの編集] ページの [管理されたクライアント] 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、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。

Websense Manager にログオンするときに、優先管理者が削除するクライアントを含むディレクトリ サービスと通信する Policy Server と異なった Policy Server を選択した場合、問題が発生する場合があります。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。

管理された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、267 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

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 < ロール名 > はコンピュータ 127.0.0.1 上で < 日付、時刻 > 以降 < ユーザ名 > によって使用されています。」というエラー メッセージが表示されることがあります。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、あなたが要求しているのと同じロールで Websense Manager がインストールされているコンピュータ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。

一部のユーザが フィルタなし URL リスト内のサイトにアクセスできない

フィルタなし 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、優先管理者がフィルタなし URL を追加した場合、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これらのサイトへのアクセス権限を付与されません。

そのサイトを他のロールのクライアントがアクセスできるようにするために、優先管理者は各ロールに切り替え、当該サイトをそのロールのフィルタなし URL リストに追加することができます。

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

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

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 プロトコルのフィルタリング動作を設定できます。

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。

レポートの問題

- Log Server が実行していない、390 ページ
- Policy Server に Log Server がインストールされていない、391 ページ
- ログ データベースが作成されていない、392 ページ
- ログ データベースを使用できない、392 ページ
- ログ データベースのサイズ、393 ページ

Log Server が実行していない

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、インターネット使用状況の情報が保存されず、インターネット使用状況レポートを生成できません。

以下の場合に Log Server を使用できません。

- 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 スペースが足りない。
- Microsoft SQL Server または MSDE パスワードを変更したが、ODBC または Log Server 設定を更新していない。
- 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。
- logserver.ini ファイルが見つからないか壊れている。
- 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。

問題を解決するには、以下のいずれかの手順を実行します。

- ディスクの空き容量を確認し、必要に応じて、不要なファイルを削除します。
- パスワードの変更が問題の原因であると考える場合は、Log Server 接続パスワードの更新、394 ページを参照してください。
- Websense **bin** ディレクトリ（デフォルトでは C:¥Program Files¥Websense¥bin）に移動し、テキスト エディタで **logserver.ini** が開くことを確認します。このファイルが壊れている場合は、バックアップ ファイルによって置換します。

- Windows の [サービス] ダイアログボックスで 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、288 ページを参照)。
- 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 メッセージをチェックします (トラブルシューティングのツール、401 ページを参照)。

Policy Server に Log Server がインストールされていない

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 レポートや、Websense Manager の [今日] および [履歴] 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。

このメッセージは以下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 Websense Manager のローカルホストに設定されている。
- Log Server が Linux コンピュータにインストールされている。
- Websense レポーティング ツールを使用していない。

Websense 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、以下の手順を実行します。

1. 左側のナビゲーションペインの **[設定]** タブを選択し、**[一般] > [ログ記録]** を選択します。
2. **[Log Server の IP アドレスまたは名前]** フィールドに、Log Server 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、**[すべて保存]** をクリックします。

Log Server が Linux コンピュータにインストールされている場合、または Websense レポーティング ツールを使用しない場合、Websense Manager でこのアラート メッセージを非表示にすることができます。

1. 左側のナビゲーションペインの [メイン] タブで **[ステータス] > [アラート]** を選択します。
2. [アクティブなアラート] の下の **[詳細]** をクリックします。
3. 「Log Server がインストールされていません」メッセージの **[このアラートを非表示にする]** をオンにします。
4. **[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。

ログ データベースが作成されていない

インストーラがログ データベースを作成できない場合があります。下のリストは、最も一般的な原因と解決方法を示しています。

問題:	Websense ソフトウェアがログ データベースに使用する名前 (wslogdb70 および wslogdb70_1) を使用する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。
解決方法:	既存のファイルを削除するか、名前を変更し、インストーラを再度実行します。
問題:	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。
解決方法:	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、インストーラを再実行します。
問題:	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容量がない。
解決方法:	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、インストーラを再実行します。代わりに、他の場所を選択します。
問題:	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 許可を割り当てられていない。
解決方法:	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ます。次に、インストーラを再実行します。 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 2000 または MSDE: **dbo**(データベース所有者) 許可を必要とします。 ■ SQL Server 2005: **dbo** および **SQLServerAgentReader** 許可を必要とします。

ログ データベースを使用できない

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、Websense Manager の [今日] および [履歴] 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、最初に、データベース エンジン (Microsoft SQL Server または Microsoft SQL Server

Desktop Engine [MSDE]) がログ データベース コンピュータで実行していることを確認します。

1. Windowsの[サービス]ダイアログボックス(Windowsのサービス ダイアログボックス、401 ページを参照) を開き、以下のサービスが実行していることを確認します。
   - Microsoft SQL Server
     - MSSQLSERVER
     - SQLSERVERAGENT
   - Microsoft SQL Desktop Engine (MSDE):
     - MSSQL$WEBSENSE (Websense, Inc. から MSDE を取得した場合)
     - SQLAgent$WEBSENSE
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、**[開始]** をクリックします。

   サービスが再開しない場合、Windows イベント ビューア (Windows イベント ビューア、401 ページを参照) で Microsoft SQL Server または MSDE のエラーおよび警告をチェックします。

データベース エンジンが実行している場合、次のことを確認します。

- SQL Server Agent がデータベース エンジンを実行しているコンピュータ上で実行していることを確認します。
- Windows の [サービス] ダイアログボックスを使って、**Websense Log Server** サービスが実行していることを確認します。
- Log Server とログ データベース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。
- ログ データベース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 がログ データベースにデータを記録しない、394 ページを参照)。
- Microsoft SQL ServerまたはMSDE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、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 接続パスワードの更新、394 ページを参照してください。

ログ データベースのサイズ

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ていても、レポートの表示に時間がかかるようになったり、Web ブラウザからタイムアウト メッセージが表示されるようになった場合は、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. Websense Managerで、**[設定] > [レポート] > [ログ データベース]** へ進みます。
2. このページの **[使用可能なパーティション]** のセクションを見つけます。

3. 現在のレポート操作に必要でないパーティションの**[有効にする]**チェックボックスをオフにします。
4. 変更を適用するために **[すぐに保存]** をクリックします。

Log Server がログ データベースにデータを記録しない

Log Server がログ データベースにデータを書き込めない場合、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、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。

ログ データベース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、**[設定] > [レポート] > [ログ データベース]** の順に選択して、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。ロールオーバー オプションの設定、327 ページを参照してください。

情報技術担当部門が 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、情報技術部に支援を求めてください。

Log Server 接続パスワードの更新

Websense ソフトウェアがログ データベースに接続するために使用するアカウントのパスワードを変更した場合、新しいパスワードを使用するためには Log Server も更新する必要があります。

1. Log Server コンピュータ上で **[スタート] > [プログラム] > [Websense] > [ユーティリティ] > [Log Server の構成]** の順に選択します。Log Server の構成ユーティリティが開きます。
2. **[データベース]** タブをクリックし、[ODBC データ ソース名 (DSN)] フィールドに正しいデータベース (デフォルトでは **wslogdb70**) が表示されることを確認します。
3. **[接続]** をクリックします。[データソースを選択] ダイアログボックスが開きます。
4. **[コンピュータ データソース]** タブをクリックし、**[wslogdb70]**(または使用しているログ データベースの名前) をダブルクリックします。[SQL Server ログイン] ダイアログボックスが開きます。
5. [ログインID] フィールドに正しいアカウント名 (通常は **sa**) が表示されることを確認し、次に、新しいパスワードを入力します。

6. [OK] をクリックし、次に [Log Server の構成] ダイアログボックスで [**適用**] をクリックします。
7. [**接続**] タブをクリックし、Log Server を停止してから再起動します。
8. Log Server が再起動したとき、[OK] をクリックしてこのユーティリティを閉じます。

Microsoft SQL Server 2005 のユーザ許可の設定

Microsoft SQL Server 2005 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 2005 の SQL Server Agent ジョブは SQL Server の msdb データベースに保存されます。

Websense Log Server を正しく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、msdb データベース内の以下のいずれかのロールのメンバーシップを割り当てられている必要があります。

- SQLAgentUser ロール
- SQLAgentReader ロール
- SQLAgentOperator ロール

> **ご注意：**
> SQL ユーザ アカウントはまた、DBCreator 固定サーバ ロールのメンバーである必要があります。

Microsoft SQL Server 2005 で、SQL Server ユーザ アカウントに、Websense レポート コンポーネントを正常にインストールするために必要な許可を与えます。

1. SQL Server コンピュータで、[**スタート**] > [**プログラム**] > [**Microsoft SQL Server 2005**] > [**Microsoft SQL Server 管理スタジオ**] の順に選択します。
2. [**オブジェクト エクスプローラ**] ツリーを選択します。
3. [**セキュリティ**] > [**ログイン**] を選択します。
4. 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。
5. ログイン アカウントを右クリックし、このユーザの [**プロパティ**] を選択します。
6. [**ユーザ マッピング**] を選択し、以下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. メンバーシップに以下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. [OK] をクリックして保存します。

7. [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。
8. [OK] をクリックして保存します。

Log Server がディレクトリ サービスに接続できない

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、401 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、Websense Log Server と Websense 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、ファイアウォールがこれらのコンポーネント間の通信のために使用するポート上でのアクセスを許可するように設定します。

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である

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がインターネット アクセスで消費した時間を示し、各サイトで消費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

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。

一部のプロトコル要求がログ記録されない

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、クライアントへのメッセージ用に、サーバへのログインに使用した IP アドレスとは別の識別用 IP アドレスと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が不明であるからです。

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 ツールによって作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

すべてのレポートにデータがない場合、以下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。データベースのパーティション、397 ページを参照してください。
- Microsoft SQL Server または MSDE で SQL Server Agent ジョブがアクティブである。SQL Server Agent のジョブ、398 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。Log Server の構成、398 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

Websense ログ レコードは、データベース内でパーティションに保存されます。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。

Websense 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、以下の手順を実行します。

1. **[設定]** > **[レポート]** > **[ログ データベース]** を順に選択します。
2. **[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**[有効にする]**チェックボックスをオンにします。
4. 変更を適用するために **[すぐに保存]** をクリックします。

SQL Server Agent のジョブ

SQL Server Agent データベース ジョブが無効に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。

MSDE を実行している場合、以下の手順を実行します。

1. **[スタート]** > **[プログラム]** > **[管理ツール]** > **[サービス]**の順に選択します。
2. SQL Server と SQL Server Agent サービスの両方が起動していることを確認してください。Websense, Inc. から MSDE を取得した場合、これらのサービスの名前は MSSQL$WEBSENSE および SQLAgent$WEBSENSE です。

完全な Microsoft SQL Server を実行している場合、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を確認するよう依頼してください。

Log Server の構成

Log Server が Filtering Service サービスからログ情報を受信するには、Websense 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、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、Websense Manager が Log Server に正常に接続されていることを確認します。

1. 無条件の統括管理者許可を使って Websense Manager にログオンします。
2. **[設定]** > **[一般]** > **[ログ記録]** を順に選択します。
3. Log Server がインストールされている**コンピュータ名**または**IPアドレス**を入力します。
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. Websense Manager が指定された Log Server と通信可能かを判断するためには、**[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 アドレスまたはコンピュータ名とポートを更新します。
6. 作業が終了したら、**[OK]** をクリックして、変更をキャッシュします。**[すべて保存]** をクリックするまで、変更は適用されません。

次に、Log Server 構成ユーティリティの設定を確認します。

1. Log Server が実行しているコンピュータ上で、**[スタート]** > **[プログラム]** > **[Websense]** > **[ユーティリティ]** > **[Log Server の構成]** の順に選択します。
2. **[接続]** タブで、ポートが Websense Manager に入力した値と一致していることを確認します。
3. **[OK]** をクリックし、変更を保存します。
4. **[接続]** タブ上のボタンを使用して、Log Server を停止し、次に起動します。

5. **[終了]** をクリックして、Log Server の構成ユーティリティを閉じます。

今日 または 履歴 ページに図が表示されない

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。**[今日および履歴ページでのレポートの参照]** が選択されていない場合、そのロールの指定済み管理者の画面にはこれらの図は表示されません。

複数の Policy Server を使用する環境では、Log Server は 1 つの Policy Server との通信のためにのみインストールされます。[今日] および [履歴] ページの図を表示するか、または他のレポート作成機能にアクセスするには、その Policy Server にログオンする必要があります。

特定のレポート作成機能にアクセスできない

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にする必要があります。

Microsoft Excel 出力に一部のレポート データがない

Microsoft Excel ワークシートで開くことができる最大の行数は 65,536 です。レコード数が 65,536 を超えるレポートを Microsoft Excel 形式にエクスポートした場合、65,537 番目以降のすべて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、以下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

[レポート] > [プレゼンテーション レポート] 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 Websense Manager ウィンドウに表示できます。

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 Websense Manager 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、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、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。

調査レポートの検索の問題

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 文字を入力できない
- 検索パターンが見つからない

拡張 ASCII 文字

[調査レポート] のメイン ページの棒グラフの上の [検索] フィールドを使用して、選択した図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。

Linux サーバ上で Mozilla Firefox を使用して Websense Manager にアクセスしている場合、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、サポートされているブラウザを使って Windows サーバーから Websense Manager にアクセスしてください。

検索パターンが見つからない

調査レポートでは、[調査レポート] のメイン ページの [検索] 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。そのような場合に、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

- 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、以下の原因が考えられます。
  - Web サーバのタイムアウト
  - MSDE または 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 **[ヒット件数]** です。

トラブルシューティングのツール

- Windows のサービス ダイアログボックス、401 ページ
- Windows イベント ビューア、401 ページ
- Websense ログ ファイル、402 ページ

Windows のサービス ダイアログボックス

Microsoft Windows コンピュータでは、Filtering Service、Network Agent、Policy Server、User Service、およびすべての Websense の透過的識別エージェントはサービスとして実行します。Windows の [サービス] ダイアログボックスを使って、これらのサービスのステータスを確認できます。

1. Windows の [コントロール パネル] で **[管理ツール]** フォルダを開きます。
2. **[サービス]** をダブルクリックします。
3. 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。
4. 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 [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

Windows イベントビューアは、Windows イベントに関するエラー メッセージとサービス アクティビティを記録します。これらのメッセージは、インターネット フィルタリングやユーザ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. Windows の [コントロール パネル] で **[管理ツール]** フォルダを開きます。
2. **[イベント ビューア]** をダブルクリックします。
3. イベント ビューアで **[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。
4. 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

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¥Websense¥bin または /opt/Websense/bin）に格納されている **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ために支援が必要なとき、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

M

N

O

P

R

き

く

け

こ

さ

し

す

せ

た

ち

つ

て

と

な

に

ね

は

よ

り

れ

ろ

わ