Websense Appliance Manager

Websense® V シリーズ アプライアンス

モデル：V10000、V10000 G2、V5000 G2

v7.7

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

R230312770

発行 2012
アメリカ合衆国およびアイルランドにて印刷

商標について

目次

1 V シリーズの概要

Websense の V シリーズ アプライアンスは、Web トラフィック、電子メール トラフィック、またはその両方をリアルタイムで解析し、セキュリティ ポリシーを適用します。

Websense Web Security Gateway モジュールをオンにすると、アプライアンスは次の動作を行います。

- 即座に新しいサイトとダイナミック コンテンツを分類し、予防的にセキュリティ上のリスクを発見し、管理者によって設定されたポリシーに従って望ましくないコンテンツやマルウェアをブロックします。
- プロキシ回避、ハッキング サイト、アダルト コンテンツ、ボットネット、キーロガー、フィッシング攻撃、スパイウェアやその他の多くのタイプの安全でないコンテンツを検出およびブロックするために、ルール、署名、ヒューリスティックス、アプリケーションの動作などの先進的な解析を提供します。
- SSL トラフィックがネットワークに入る前に復号化やスキャンをし、この一般的なセキュリティ ホールを閉じます。

V シリーズ アプライアンス上でのこれらのリアルタイム機能と業界最先端の Websense Web Security ソフトウェアを組み合わせることによって、90 以上のデフォルト URL カテゴリと 120 以上のネットワークおよびアプリケーション プロトコルによるウェブ フィルタリングを提供します。

- アプライアンス上のソフトウェアを Websense Data Security ソリューションと結合することによって、データ セキュリティ ソフトウェアに Master Database URL 分類と、Websense Web フィルタリング サービスによって収集されたユーザー情報の両方へのアクセスを提供できます。
- また、アプライアンス上のソフトウェアを、オンデマンドのクラウドベースの サービスである Websense ハイブリッド Web フィルタリングと同期化することによって、顧客の組織のポリシーをオフサイトのユーザーや支店、リモート コンピュータ等へ適用することができます。

Websense Email Security Gateway をオンにすると、アプライアンスは次の動作を行います。

- 着信電子メール メッセージをスキャンおよびフィルタリングし、管理者によって設定されたポリシーに従ってスパムやウィルス コンテンツをブロックします。

- Websense Data Security ソリューションと組み合わせることによって、電子メールを通じた機密情報や不適切な情報の転送をモニタおよび制限するのに役立ちます。

サブスクリプションが Websense Email Security Gateway Anywhere である場合、アプライアンスはまた、次の動作を行います。

- メッセージが顧客のネットワークに到達する前に多くのスパム コンテンツをフィルタリングできるハイブリッド ソリューションを提供します。

セキュリティに関する最良の方法

- アプライアンスを IT クロゼットまたはデータ センターの中でロックし、BIOS パスワードを有効にします。アプライアンスへの物理的アクセスはネットワークに対するセキュリティ リスクとなることがあります。
- シリアル コンソール (KVM) を通じてコマンド ライン インターフェースにアクセスすることによるアプライアンスへの物理的アクセスは、**firstboot** の実行後、管理者資格情報によって保護されます。
- 管理者資格情報が選択された少数の者に限定されていることを確認してください。これはシステムへの無許可のアクセスを防止するために役立ちます。
- Websense テクニカル サポートによって指示された時にのみトラブルシューティング用ポートを有効にし、リモート アクセスを許可します。Websense の専門技術者がログオフした後すぐに、これらの設定を「無効」に戻します。

管理コンソール

関連項目：

- *TRITON Unified Security Center でのアプライアンスの管理*, 3 ページ
- *Appliance Manager および他のコンソールへのアクセス*, 4 ページ
- *Appliance Manager へのログオン*, 5 ページ
- *二要素認証の設定*, 6 ページ
- *パスワード ログオンの無効化および有効化*, 6 ページ

Appliance Manager は、V シリーズ アプライアンスの管理コンソールの名前です。

Appliance Manager を使用して、以下のことを行います。

- ソフトウェア モジュールおよびアプライアンス リソースの状況をモニタする
- ネットワーク インターフェースの割り当ておよびルートを作成する

- パッチおよびホットフィックスを適用する
- パスワードを変更する
- トラブルシューティングを実行する
- その他

TRITON Unified Security Center は、TRITON Web、データ、電子メール、およびモバイル セキュリティ モジュールの管理コンソールの名前です。Appliance Manager および Content Gateway Manager (Web プロキシ コンポーネント) へのアクセスも提供します。

TRITON Unified Security Center はユーザーのセットアップ、Web および電子メールのフィルタリング ポリシーの適用などの作業を実行するためにを使用します。

この表は、TRITON セキュリティ モジュールとそれらに関連するコンソールを記載しています。

ソフトウェア モジュール	説明	コンソールの名前
TRITON Unified Security Center	すべてのモジュールに共通する構成および設定を管理します。複数コンソールへの一元的なアクセスを提供します。	TRITON Unified Security Center
Websense Web Security	ポリシーを使用して、クライアントからのインターネット要求をフィルタリングします。	TRITON – Web Security
Network Agent	インターネット トラフィック スニファー。HTTP、HTTPS、FTP 以外のプロトコルのフィルタリングを適用します。	TRITON – Web Security
Websense Content Gateway	プロキシ ソフトウェアと高度な分析を含みます。	Content Gateway Manager
Websense Email Security Gateway	インバウンドおよびアウトバウンドの電子メール メッセージをフィルタリングします。	TRITON – Email Security
Websense Data Security	データ損失防止管理を提供します。	TRITON – Data Security
Websense Mobile Security	Apple iOS モバイル デバイス対応のクラウドベースのサービスで、リモート デバイス管理機能および Web 脅威に対する保護を提供します。	TRITON – Mobile Security

TRITON Unified Security Center でのアプライアンスの管理

TRITON Unified Security Center (TRITON コンソール) は、ネットワーク内の Websense アプライアンスを管理する機能を提供します。TRITON インストールに含まれるアプライアンスは、TRITON コンソールの「**Appliances (アプラ**

イアンス)」> **「Manage Appliances （アプライアンスの管理)」**ページに自動的に登録されます。各アプライアンスについて下記の情報が含まれています。

- C インターフェース IP アドレス
- ホスト名
- セキュリティ モード (Web Security、Email Security、または Web Security と Email Security の両方)
- Web Security がオンの場合は、ポリシー ソース (Full、Limited、または Filtering Only)
- ソフトウェア バージョン (例、7.7.0)
- ハードウェア プラットフォーム (例、V5000、V10000、V10000 G2)
- アプリケーションの説明

詳細については、TRITON Unified Security Center のオンライン ヘルプを参照してください。

Appliance Manager および他のコンソールへのアクセス

Appliance Manager にアクセスする方法は、TRITON コンソールでアクセスを設定した方法によって異なります。次の 3 つのモードがあります。

- 特別な設定を行っていない場合は、TRITON コンソールの**「Manage Appliances」**ページのリンクから、または直接にアプライアンス C インターフェース IP アドレスおよびポート番号 (下記) を通じて Appliance Manager にアクセスできます。資格情報の入力を要求されます。
- TRITON コンソールにシングル サインオンが設定されている場合は、**「Manage Appliances」**ページの Single Sign-On (シングル サインオン)」ボタンを通じて Appliance Manager にアクセスできます。資格情報の入力は要求されません。または、C インターフェース IP アドレスおよびポート番号に直接にアクセスできます。この場合は資格情報の入力を要求されます。
- TRITON コンソールで二要素認証 (証明書認証) を設定している場合は、Appliance Manager にアクセスするためにシングル サインオン権限も設定する必要があります。Appliance Manager にアクセスするには、二要素認証を使って TRITON コンソールにログオンし、次に**「Manage Appliances」**ページの [Single Sign-On (シングル サインオン)] ボタンを使用します。二要素認証が設定されている場合は、C インターフェース IP アドレスを通じた直接アクセスが無効にされます。*二要素認証の設定* を参照してください。

シングル サインオンの設定の詳細については、TRITON コンソール オンライン ヘルプの *「既存のアプライアンスをシングル サインオンに設定する」* を参照してください。

直接アクセス

上記のように、二要素認証が設定されていない場合、コンソールに直接にまたは TRITON コンソールを通じてアクセスできます。

Appliance Manager、Content Gateway Manager、および TRITON Unified Security Center へのアクセスを提供する統合 Logon ポータルを起動するには、下記にアクセスしてください。

```
https://<IP-address-of-interface-C>:9447/
```

TRITON Unified Security Center を直接に起動するには、下記にアクセスしてください。

```
https://<IP-address-of-TRITON-machine>:9443/triton/
```

Content Gateway Manager を直接に起動するには、下記のサイトへアクセスしてください。

```
https://<IP-address-of-interface-C>:8081/
```

すべてのコンソールは下記のブラウザをサポートしています。

- Microsoft Internet Explorer8、9、および 10
- Mozilla Firefox バージョン 4.x、5.x、および 6.x
- Chrome 13 以上

ご注意

Internet Explorer 8 または 9 を使用している場合は、Enhanced Security Configuration がオフになっていることを確認してください。

Internet Explorer 8 を使用している場合は、Compatibility View はサポートされていません。

TRITON コンソールにログオンすると、デフォルトでは Web Security モジュール (TRITON – Web Security) が起動します。他のモジュールに切り替えるには、TRITON ツールバーから [Email Security] または [Data Security] を選択します。

Websense Web Security ソリューションを使用していない場合は、ログオン時に Email Security モジュールまたは Data Security モジュールが直接に起動します。モジュール間で切り替えるには、TRITON ツールバーのボタンを使用します。

Appliance Manager へのログオン

二要素認証が設定されていない場合は、ブラウザで Logon ポータル（上記）を参照するか、または下記のサイトに直接にアクセスすることによって Appliance Manager にログオンできます。

```
https://<IP-address-of-interface-C>:9447/appmng/
```

また、TRITON ツールバーの **[Appliances]** をクリックするか、[Single Sign-On] ボタン（設定されている場合）、もしくはハイパーリンクの IP アドレスをクリックすることによって、TRITON Unified Security Center に登録されている任意の V シリーズ アプライアンスの Appliance Manager にログオンすることもできます。

ユーザー名は **admin** です。

アプライアンスに対するパスワードは **firstboot** スクリプトを実行したとき、またはその後に管理者によって設定されています。

コンソールのパスワードを変更する方法については、*アカウント管理* を参照してください。

二要素認証の設定

二要素認証：

- TRITON コンソールへのログオン用に設定されており、ログオン時に適用されます。
- 管理者にログオン時に 2 つの形式の ID を提供する証明書認証を実行することを要求します。
- 管理者が他のコンソールにアクセスの前に TRITON コンソールにログオンするよう強制することによって、Appliance Manager および Content Gateway Manager に適用させることができます。
- Appliance Manager および Content Gateway Manager へのアクセスを許可された管理者のためにシングル サインオンを設定することを要求します。
- コマンド ライン インターフェース コマンドを使ってパスワード ログオン機能を**無効**にすることを要求します。それによって、シングル サインオンが設定されていない管理者が Appliance Manager および Content Gateway Manager にアクセスするのを防止します。

設定の詳細については、TRITON コンソール オンライン ヘルプの *「証明書認証の設定」* を参照してください。

パスワード ログオンの無効化および有効化

Appliance Manager パスワード ログオンを無効にすることによって TRITON コンソールからの二要素認証またはシングル サインオン アクセスのみを許可することができます。

アプライアンスのパスワード ログオンを無効にするには、下記の手順を実行します。

1. TRITON コンソールでシングル サインオンを設定します。
2. 二要素認証を使用する場合は、TRITON コンソールで二要素認証を設定します。
3. アプライアンス コマンド ライン インターフェースにアクセスして、管理者資格情報を使ってログオンします。

4. コマンド ラインに下記のように入力します。

   ```
   password-logon disable
   ```

5. ログオフし、ブラウザに Logon ポータルの IP アドレスを入力することによって直接のログオンが無効にされていることを確認します。Logon ポータルには Appliance Manager や Content Gateway Manager へのリンクが含まれていないことを確認してください。

すべての管理者のパスワード ログオンを再有効化するには、下記の手順を実行します。

1. アプライアンス コマンド ライン インターフェースにアクセスして、管理者資格情報を使ってログオンします。
2. コマンド ラインに下記のように入力します。

   ```
   password-logon enable
   ```

> **ご注意**
> 何らかの理由でアプライアンスの TRITON Unified Security Center への登録が無効になった場合、パスワード ログインが自動的に再有効化されます。

ログとレポート作成

V- シリーズ アプライアンスは、システム上でアクティビティーの詳細なログを保持します。これらのログは、予期しない動作や問題が起こったときにユーザーと Websense テクニカル サポートを支援するように設計されています。V- シリーズのログの詳細については、*ログ* を参照してください。

デフォルトでは V シリーズ上のモジュールは、モジュール使用状況およびアクションの詳細なレポート記録（通常はログ記録と呼ばれます）を生成します。そのためには別のコンピュータ上に Windows 専用のレポート作成コンポーネント（Web Security の場合は **Log Server**、Email Security の場合は **Email Log Server**）をインストールする必要があります。

どちらかの Log Server コンポーネントを追加するには、下記の手順を実行します。

- TRITON ソフトウェア インストーラをダウンロードします（www.mywebsense.com から入手できます）。
- 下記にアクセスできる Windows サーバー上に Log Server をインストールします。
  - ログ データベースをホストする Microsoft SQL Server のインスタンス
  - アプライアンス。それによってログ記録を作成するために Web Security コンポーネントまたは Email Security コンポーネントからフィルタリング データを取得できるようになります。

TRITON Unified Security Center の Web Security モジュールおよび Email Security モジュールに含まれるレポート作成ツールを使ってフィルタリング ログ記録に基づく管理レポートを生成できます。

どのアプライアンス モジュールがアクティブであるかによって、TRITON – Web Security、TRITON – Email Security、またはその両方が V シリーズ アプライアンスにプレインストールされていることがあります。これは、お客様がテスト環境で利用可能な Websense ソリューションを評価するのを支援することを目的としています。Websense, Inc., は製造環境でプレインストールされた TRITON モジュールを使用することを推奨しません。

重要

アプライアンスに TRITON – Web Security のみがインストールされており、ネットワークに少数のユーザーのみ含まれるという稀な場合を除いて、TRITON Unified Security Center は別の Windows Server 2008 R2 64 ビット コンピュータ上にインストールする必要があります。

Web Security レポートと Email Security レポート

- TRITON – Web Security または Email Security を起動すると、ダッシュボードに Websense ソフトウェアの動作ステータスが表示されます。
  - TRITON – Web Security では、Overview ダッシュボードにヘルス アラートおよび一般的なステータス情報が表示されます。[Additional Threat Tracking (追加的な脅威の追跡)]、[Security (セキュリティ)]、および [Web Usage (Web 使用状況)] タブには、Web Security ソリューションのセキュリティおよびフィルタリング効果を追跡するためのツールがあります。
  - TRITON – Email Security では、「Today (今日)」ページは現在の状況を表示し、また、午前 0 時以降のネットワーク内の Web または電子メール フィルタリング アクティビティのチャートを表示することができます。「History (履歴)」ページには最大 30 日間のネットワーク内の Web または電子メール フィルタリング アクティビティのチャートが表示されます。
- **プレゼンテーション レポート**は、クライアントのインターネット アクティビティまたはメッセージ フィルタリング アクティビティのグラフ形式およびテーブル形式のレポート (カスタマイズ可能) が表示されます。
- Websense Web Security **調査レポート**では、データを絞り込み、組織にとって最も関心が高い情報を見つけることができます。
- Websense Web Security の **Real-Time Monitor** では、Policy Server に関連付けられた Filtering Service インスタンスによってどのトラフィックが存在するか、およびそれぞれの要求に対してどのアクションが適用されるかを確認できます。

V シリーズ アプライアンス上で使用されるデータベース

Websense ソフトウェアは、アクティブ ポリシーとフィルタリング データベース内に保存されている情報 - 定期的に更新する必要があります - に基づいてインターネットおよび電子メール アクティビティをフィルタリングします。

- Websense Web Security の **Master Database** には、URL カテゴリ情報およびプロトコル定義が含まれています。これは、Filtering Service によって管理されます。管理者は TRITON - Web Security のデータベースを更新する頻度、および完全な更新の間に部分的更新、リアルタイム更新を実行するかどうかを制御できます。(詳細については、「Websense Master Database」を参照してください .)。

  フィルタリング データベースの限定的な開始時バージョンがアプライアンスにプレインストールされていますから、サブスクリプション キーを入力すると直ちにフィルタリングを開始できます。完全なインターネット フィルタリング機能を有効にするために、できるだけ早く完全な Master Database をダウンロードしてください。アプライアンスの最初の設定を完了した後、*『V-Series Appliance Getting Started Guide』* を参照してください。

- Websense Content Gateway のスキャンおよび分類オプションは、Websense ソフトウェアと共にインストールされているデータベースのセットに依存します。ソフトウェアは、定期的にこれらのデータベースに対する更新をチェックします。これらのデータベースに対する更新は、すべての Master Database の更新からは独立的に実行されます。

  アプライアンスまたは Content Gateway モジュールを再起動するたびに、これらの小規模のデータベースのダウンロードが開始されます。ダウンロードが失敗した場合、ダウンロードが正常に完了するまで 15 分ごとに新たなダウンロードが試行されます。

- Websense Email Security Gateway 電子メール フィルタリングでは、一連のアンチスパムおよびアンチウィルス データベース (設定可能) を使用します。ソフトウェアは、定期的にこれらのデータベースに対する更新をチェックします。更新は TRITON - Email Security 内から手動で開始できます。

- Websense Email Security Gateway が Websense Web Security と共に配備されている場合、Email Security Gateway はまた Web Security URL Master Database をクエリーして、電子メール コンテンツ内に埋め込まれている URL のカテゴリを取得することもできます。

Appliance Manager 内の移動

Appliance Manager を開いたとき、コンテンツ ペインに **「Status (ステータス)」> 「General (一般)」** ページが表示されます。ページ上部のバナーには、アプライアンス プラットフォーム、Appliance Controller のホスト名、セキュリティ モードを示すアイコン、および［Log Off］ボタンが表示されます。

- 他のページを表示するには、左ナビゲーション ペインでエントリを選択します。
- いずれかのページのオプションの詳細な説明を表示するには、**[Help (ヘルプ)] >[Explain This Page (このページを説明)]** に進みます。

Appliance Manager は、下記のページへのアクセスを提供します。

Status

- *一般的なシステム ステータス*
- *CPU とメモリのステータス*
- *モジュールごとのディスクの使用状況*
- *ネットワーク帯域幅*

設定

- *システム設定*
- *ネットワーク インタフェースの設定*
- *ルーティングの設定*
- *アラート*
- *Web Security コンポーネントの設定*

管理

- パッチ / ホットフィックス (*ホットフィックス管理*, *パッチ管理*)
- Backup utility ? (*Using the backup utility (バックアップ ユーティリティの使用)*)
- *ログ*
- *ツールボックス*
- *アカウント管理*

複数の Web Security Gateway アプライアンスのクラスタ化

Content Gateway は Web Security Gateway の Web プロキシ コンポーネントです。Content Gateway の重要な機能は、Content Gateway の複数のインスタンスを結合して 1 つの*管理クラスタ*を形成することです。それによって Web Security Gateway アプライアンスは、すばやくスケールアップして容量とシステム パフォーマンスを高めることができ、しかもシステム管理が複雑になることはなく、単一のクラスタ ノードから実行できます。管理クラスタ化の詳細は Content Gateway オンライン ヘルプ システムを参照してください。

クラスタ化を設定するには、Content Gateway Manager を開き、**[Get Help! (ヘルプを表示 !)]** をクリックし、次に **[Contents (コンテンツ)]** タブから **[Clusters (クラスタ)]** を選択します。**SSL Manager** を使用している場合は、SSL クラスタ化に関する項を必ずお読みください。また **「Adding nodes to a cluster (クラスタへのノードの追加)」** の項も必ずお読みください。クラスタ化を有効化する前に、この機能に完全に習熟しておいてください。すべてのノードが Content Gateway の同一バージョン上にあること、クラスタ化を各ノード上で個別に有効化しなければならないこと (ただし、一度有効化した後は、すべてのクラスタ化を任意のノード上で管理できます) などいくつかの必須要件があります。

V シリーズ アプライアンス上では、設定を完了するためにもう 1 つの追加的なステップがあります。専用ルートを追加する必要があります。

1. Content Gateway Manager で設定のすべてのステップを完了します。
2. Appliance Manager にログインして、**[Configuration (設定)]** > **[Routing (ルーティング)]** > **[IPv4]** に進みます。
3. インターフェース P1 を通じてマルチキャスト クラスタ トラフィックのための Static Route ルールを追加します。
   a. **[Add/Import (追加 / インポート)]** をクリックします。
   b. **[Add individual route (個別ルートを追加)]** を選択します。
   c. **[Destination network (アクセス先ネットワーク)]** にマルチキャスト IP アドレスを入力します。例 : 224.0.1.37
   d. サブネット マスクを指定します。
   e. ゲートウェイを指定します。
   f. [Interface (インターフェース)] ドロップダウンリストから「P1」を選択します。
   g. **[Add Route (ルートを追加)]** をクリックします。

クラスタ内の各 Content Gateway ノードに専用ルートを追加します。

一般的なシステム ステータス

Appliance Manager にログオンすると、最初に **「Status（ステータス）」**> **「General （一般）」**ページが表示されます。このページにはアプライアンス上の各ソフトウェア モジュールの現在のステータスが示されます。

このページで下記のことを行います。

- システム アラート（新しいパッチに関する情報を含む）をチェックします。
- 各モジュールごとに、下記を含むリソースの使用状況を測定します。
  - モジュールが専有している CPU の数。
  - 割り当てられているメモリ（RAM）の量。
  - モジュールが使用しているアプライアンス インタフェース（例、C、P1）。
  - モジュールに含まれているサービスまたはデーモン（もしあれば）。
- ソフトウェア サービスを停止および起動する、またはソフトウェア モジュール全体を再起動もしくは無効化します。
- アプライアンスそのものを再起動またはシャットダウンします。

重要

セキュリティ上の理由で、Appliance Manager セッションは 30 分間非アクティブになると終了します。

しかし、30 分間のタイムアウトに達した後でも**「Status」**ページをモニタすることを選択できます。そうするには、**「Appliance Controller（アプライアンス コントローラ）」**セクションで、**「Monitor status without timing out（タイムアウトなしにステータスをモニタする）」**というラベルの付いたボックスをオンにします。選択を確認することを要求されます。それによって「Information on all **Status**（すべてのステータスに関する情報）」ページは、ブラウザを閉じるまで通常通り継続的に更新されます。

V シリーズ 上のモジュールは、下記を含むことがあります。

- **Appliance Controller** ソフトウェアはバックグラウンドで動作します。これはアプライアンス設定の管理、パッチのダウンロードと適用、バックアップ ユーティリティへのアクセス、モジュール再起動の要求、シャットダウンの開始、およびその他のアプライアンス管理タスクの処理を行います。
- **Websense Content Gateway** には、Websense プロキシ ソフトウェアおよび Web コンテンツのスキャンおよび分析が含まれます。複数のサービス（デーモン）がこのソフトウェアを構成しています。

- **Websense Web Security** は、Web フィルタリングを処理するソフトウェアです。複数のサービス（デーモン）がこのソフトウェアを構成しています。
- **Network Agent** は、インターネット トラフィックをモニタし、インスタント メッセージングなどの非 HTTP プロトコルをフィルタリングする Web Security コンポーネントです。
- **Websense Email Security** は、電子メール フィルタリングを処理するソフトウェアです。複数のサービス（デーモン）がこのソフトウェアを構成しています。

このページのリンクおよびボタンを使って下記のタスクを実行することができます。

ボタンまたはリンク	説明
View Patch （パッチを表示）	新しいパッチが利用可能であることを知らせるアラートが発行された時に表示されます。このボタンをクリックし、**「Administration（管理）」>「Patches （パッチ）」/「Hotfixes（ホットフィックス）」**ページに進むと、利用可能なパッチのリストが表示され、パッチ管理機能にアクセスできます。
Restart Appliance （アプライアンスを再起動）	このアプライアンスを再起動させます。すべてのモジュールが停止されます。次に、モジュールが再起動されます。「Disabled（無効）」というフラグが付けられたモジュールは再起動されません。
Shutdown Appliance（アプライアンスをシャットダウン）	このアプライアンスおよびすべてのソフトウェア モジュールを正常にシャットダウンさせます。
Restart Module （モジュールを再起動） (Websense Content Gateway)	このアプライアンス上の Websense Content Gateway モジュール（のすべてのサービス）を停止させ、次に再起動させます。
Launch （起動） (Content Gateway Manager)	Content Gateway Manager を起動します。*管理コンソール* を参照してください。
Stop Services （サービスを停止） Start Services （サービスを開始） (Websense Content Gateway)	このアプライアンス上のすべてのプロキシ サービスおよびコンテンツ分析を停止させます。 または、サービスが停止されている場合は、[Start Services（サービスを開始）] によってすべてのサービスが開始されます。
Restart Module （モジュールを再起動） (Websense Web Security)	このアプライアンス上の Websense Web Security モジュール（の使用中のサービスのサービス）を停止させ、次に再起動させます。
Launch （起動） (TRITON– Web Security)	TRITON – Web Security を起動します。*管理コンソール* を参照してください。
Stop Services （サービスを停止） Start Services （サービスを開始） (Websense Web Security)	このアプライアンス上で実行しているすべての Websense Web Security サービスを停止させます。[このアプライアンスがネットワークの完全なポリシー ソースとして指定されていない場合、一部のサービスが使用中でない場合があります。] または、サービスが停止されている場合は、[Start Services（サービスを開始）] によってすべてのサービスが開始されます。

ボタンまたはリンク	説明
Restart Module （モジュールを再起動） (Network Agent)	このアプライアンス上の Network Agent サービスを停止させ、次に再起動させます。
Disable Module （モジュールを無効化） Enable Module （モジュールを有効化） (Network Agent)	Network Agent のための [Disable Module（モジュールを無効化）] ボタンは、Network Agent が Websense Web Security Gateway (Anywhere) または Web Security Gateway Anywhere アプライアンス上でプロビジョニングされ、実行している時にのみ表示されます。Network Agent は Websense Web Security (Gateway なし) アプライアンス上では無効化できません。 [Disable Module] ボタンをクリックすると、[Disable Network Agent (Network Agent を無効にする)] ダイアログ ボックスが表示されます。このダイアログは 次の 2 つのオプションを提供します。1) モジュールを永久的に無効化する、または 2) モジュールを一時的に無効化する。 すべての配備で Network Agent が使用されているわけではなく、Network Agent を無効化するとシステム リソース -- CPU およびメモリ -- がアプライアンス上でプロビジョニングされた他のモジュールに再配分されます。 しかし、Network Agent を永久的に無効化した場合、アプライアンス上で再び Network Agent を使用できるようにするためにはアプライアンスを**再イメージング**する必要があります。*永久的に無効化した場合の Network Agent の再有効化* を参照してください。 Network Agent を一時的に無効化した場合、アプライアンス上で Network Agent をシャットダウンし、次にアプライアンスを再起動したときに再起動しないよう指示するフラグがセットされます。 **ご注意**：Network Agent を一時的に無効化した場合の重要な副次的な影響として、ポリシー ソース、C インターフェース IP アドレスを変更するか、またはパッチを適用する前に、Network Agent を再度有効化しなければなりません。Network Agent を再-有効化するためには平均で 10 分かかります。 Network Agent が一時的に無効化された状態にあるとき、[Enable Module] と [Permanently Disable] の両方のボタンが表示されます。 Network Agent の目的の概要については、*Network Agent インターフェース (N), 26 ページ* を参照してください。
Stop Services （サービスを停止） Start Services （サービスを開始） (Network Agent)	このアプライアンス上の Network Agent サービスを停止させます。 または、サービスが停止されている場合は、[Start Services（サービスを開始）] によってすべてのサービスが開始されます。

ボタンまたはリンク	説明
Restart Module （モジュールを再起動） (Websense Email Security Gateway)	このアプライアンス上の Email Security Gateway サービスを停止させ、次に再起動させます。
Stop Services （サービスを停止） Start Services （サービスを開始） (Websense Email Security Gateway)	このアプライアンス上で実行しているすべての Websense Email Security Gateway サービスを停止させます。 または、サービスが停止されている場合は、[Start Services（サービスを開始）] によってすべてのサービスが開始されます。

Network Agent の無効化

Network Agent の [Disable Module（モジュールを無効化）] オプションは、Network Agent が Web Security Gateway (Anywhere または Web Security Gateway Anywhere) アプライアンス上でプロビジョニングされ、実行している時にのみ表示されます。Network Agent は Websense Web Security (Gateway なし) アプライアンス上では無効化できません。

Network Agent が有効化されているとき、CPU およびメモリが割り当てられます。Network Agent を使用していない場合、これらのリソースはアプライアンス上の他のモジュールには利用できません。

Network Agent を使用する計画がない場合、それを無効化することによってそのリソースを他のモジュールに再割り当てすることができます。

Network Agent を無効化するとき、それを一時的または永久的に無効化できます。

Network Agent を永久的に無効化した場合、アプライアンス上で再び Network Agent を使用できるようにするためにはアプライアンスを**再イメージング**する必要があります。

Network Agent を一時的に無効化した場合、Network Agent をシャットダウンし、次にアプライアンスを再起動したときに再起動しないよう指示するフラグがセットされます。アプライアンスが再起動した時、Network Agent のリソースはアプライアンス上の他のモジュールに再割り当てされます。

重要

Network Agent を一時的に無効化した場合の重要な副次的な影響として、ポリシー ソース、C インターフェース IP アドレスを変更するか、またはパッチを適用する前に、Network Agent を再度有効化しなければなりません。Network Agent を再有効化するためには平均で 10 分かかります。

Network Agent が一時的に無効化された状態にあるとき、[Enable Module] と [Permanently Disable] の両方のボタンが表示されます。

Network Agent の概要については、*ネットワーク インタフェースの設定*, 22 ページ を参照してください。

永久的に無効化した場合の Network Agent の再有効化

Network Agent を永久的に無効化した後でそれを再有効化する場合、アプライアンスを再-イメージングする必要があります。これは現在のシステムを消去し、もとの未構成のシステム イメージを復元します。『V-Series Getting Started』ガイドの *「Restoring to factory image (出荷時のイメージに復元する)」* を参照してください。

再イメージングを行った後、パッチを割り当て、完全なバックアップまたはモジュールレベルのバックアップを復元できます。完全なバックアップを復元する場合には、バックアップは Network Agent が有効化されているときに作成されている必要があります。そうでない場合、構成されたシステムとの互換性がないため復元が失敗します。

CPU とメモリのステータス

「Status (ステータス)」>「CPU」および「Memory (メモリ)」 ページは、このアプライアンス上で実行している各ソフトウェア・モジュールの直前 60 秒間における CPU およびメモリの使用に関する情報を表示します。

- **[CPU Usage (CPU の使用状況)]** は、下記の情報を表示します。
  - 専有しているリソースとモジュールに利用可能な合計リソース量をもとにした直前 60 秒間のすべての CPU 使用量の集計
  - 利用可能な各 CPU について、直前 60 秒間にモジュールが使用した割合 (%)
- **「Memory Usage (メモリの使用状況)]** は、下記の情報を表示します。
  - 利用可能なメモリについて、直前 60 秒間にモジュールが使用した割合 (%)
  - 直前 60 秒間にモジュールが使用した実際のメモリの量 (メガバイト)
  - 直前 60 秒間にこのモジュールに使用可能だった合計メモリ量 (メガバイト)

モジュールごとのディスクの使用状況

「Status」>「Disk (ディスク)」「Usage (使用状況)」 ページは、このアプライアンス上の各モジュールについて直前 60 秒間のディスク アクティビティの集計、および全体の使用可能なディスク スペースに関する情報を表示します。

- **[Disk Activity (ディスク アクティビティ)]** ページは、1 秒あたりの平均の入 / 出力操作数 (IOPS) を表示し、直前 60 秒間のアクティビティのグラフを作成します。

- **[Usage Statistics（使用状況統計）]** ページは、モジュール内の使用されているディスク スペースと使用可能なディスク スペースを表示します。

Appliance Controller、Websense Web Security、および Network Agent モジュールの各セクションに、それぞれのモジュール内の全てのコンポーネントに関する情報の一覧を示しています。これは**システム** ディスク アクティビティ、または使用状況として表されています。

Websense Content Gateway モジュールのセクションはまた、キャッシュおよび PreciseID ディスクのアクティビティおよび使用状況に関する情報も表示できます。

- キャッシュは、**オブジェクト ストア**と呼ばれる高速オブジェクト データベースから成ります。オブジェクト ストアは、URL および関連付けられているヘッダに従ってオブジェクトのインデックスを作成し、Websense Content Gateway が Web ページおよび Web ページの一部を保存、取得、および提供できるようにし、それによって最大限の帯域幅の節約を可能にします。キャッシュ ディスクに障害が発生した場合、Websense Content Gateway はプロキシ専用モード（キャッシュ機能なし）に移行します。
- Websense Content Gateway と Websense Data Security を統合している時には、PreciseID Fingerprinting を使用して、不正操作や、再フォーマット、または他の変更がある場合でも機密情報を検出できます。

「Email Security Gateway」セクションは、システム全体の情報のほかに、MTA のディスク アクティビティおよび使用状況に関する情報、電子メール メッセージの送信、受信、および転送を担当するメール転送エージェントも表示します。

ネットワーク帯域幅

「Status」> 「Network Bandwidth（ネットワーク帯域幅）」 ページは、下にリストしているアプライアンス ネットワーク インターフェース上のスループットに関する情報を表示します。

- **Appliance Controller インターフェース** (C)
- **Websense Content Gateway インターフェース** (P1) または (P1 および E1)
- **Websense Content Gateway インターフェース** (P2) または (P2 および E2)
- **Network Agent インターフェース** (N)
- **Websense Email Security Gateway** (E1) または (E1 および P1)
- **Websense Email Security Gateway** (E2) または (E2 および P2)

インターフェース E1 および E2 は、V-10000 および V-10000 G2 モデルにだけ含まれています。P1、P2、E1、および E2 のディスポジションは、適用される構成上にインストールされているモジュールによって異なります。インターフェースの設定の詳細については、*ネットワーク インタフェースの設定* を参照してください。帯域幅の表示では、それらは有効化されている場合にのみ表示されます。

各インターフェースについて、直前 60 秒間について下記の情報が表示されます。

Inbound/Outbound（インバウンド / アウトバウンド）

- インターフェース上の現在のインバウンドおよびアウトバウンド転送速度（メガビット / 秒）
- 最大帯域幅容量（メガビット / 秒）

Bandwidth Statistics（帯域幅統計）

- 受信および送信したデータの合計のメガビット数
- 受信および送信したパケットの合計数
- 欠損パケット数（インバウンドおよびアウトバウンド）
- エラーの合計数（インバウンドおよびアウトバウンド）
- インバウンドおよびアウトバウンドの転送速度（メガビット / 秒）

システム ウォッチドッグ

V シリーズ アプライアンスは、システム ウオッチドッグ デーモンを実行して、クリティカルなシステム処理および状態を監視します。監視しているいずれかの処理が失敗するか、またはいずれかの条件が満たされない場合、ウォッチドッグ サービスはリセットまたは再起動を実行します。

監視対象には下記の処理および状態が含まれます。

- Appliance kernel -- はアクティブ カーネルです。
- Domain Agent -- は実行している Domain Agent です。これはユーザー インターフェースとアプライアンス バックエンド処理の間で通信を行うための必須の処理です。
- Journal Commit I/O -- detect a ?journal commit I/O? error.
- File table -- はファイル テーブル オーバーフロー状態を検出します。

ウォッチドッグのアクションはシステム ログ ファイルに記録されます。それを Appliance Manager の **「Administration（管理）」** > **「Logs（ログ）」** ページで閲覧することができます。

2 設定

Appliance Manager の 「Configuration (設定)」セクションを使用して、以下のことを行います。

- アプライアンスの時刻と日付、ホスト名、説明を設定します (*システム設定* を参照)。
- アプライアンスのネットワーク インターフェースを指定します (*ネットワーク インタフェースの設定* を参照)。これは使用するモジュールによって異なり、C、P1、P2、N、E1、E2 などが含まれます。
- オプションとして、Content Gateway または Email Security モジュール、もしくはアプライアンス自体の静的経路を指定することもできます (*ルーティングの設定* を参照)。
- SNMP アラート機能を設定します (*アラート* を参照)。
- どのコンピュータがネットワークのフィルタリング設定およびポリシーをホストしているかを指定します (*Web Security コンポーネントの設定* を参照)。

システム設定

「Configuration (設定)」> 「System (システム)」 ページを使って下記の手順を実行します。

- 現在のアプライアンスのホスト名、セキュリティ モード (Web セキュリティ、電子メール セキュリティ、Web および電子メール セキュリティ モード)、バージョン番号、ハードウェア プラットフォーム、システムの日付および時刻、稼働時間などの基本的なアプライアンス情報を表示します。
- アプライアンスにどのソフトウェア モジュールがインストールされているかを調べ、それらのバージョン番号を取得します。

- システムの **時刻および日付**を設定します。

> **重要**
>
> いずれかの Websense サービスが実行している場合、時刻を変更する前にすべての Websense サービスを停止します。次に、時刻をリセットし、**次に**時刻が Websense サービスを実行しているすべてのサーバーで一致していることを確認します。最後に、Websense サービスを再起動します。
>
> 最初にサービスを停止しなかった場合、時刻のリセットの後に入力されたクライアントによる更新およびポリシー変更は保存されません。

  - **[Time zone (タイム ゾーン)]** リストを使用してこのシステムで使用するタイム ゾーンを選択します。

    GMT (グリニッジ標準時)、デフォルト。UTC (協定世界時) とも言います。他のタイム ゾーンは GMT をもとに加算または減算によって計算されます。地理的に分散しているシステムに共通タイム スタンプを設定するために GMT を選択する場合があります。
  - **[Time and date (時刻と日付)]** ラジオ ボタンを使用して日付を設定する方法を指定します。

    時刻は 24 時間表記法を使って設定および表示されます。

    - Internet Network Time Protocol (NTP) サーバー (www.ntp.org.) と同期化するには、**[Automatically synchronize (自動的に同期化)]** オプションを選択し、一次 NTP サーバーのアドレスを入力します。二次および三次フィールドは任意です。

> **重要**
>
> システム クロックを NTP サーバーと同期化する場合、NTP プロトコル パケットとそれらの応答パケットがアプライアンスと NTP サーバーの間にあるどのファイアウォールまたは NAT デバイス上でも許可される必要があります。NTP サーバーへのアウトバウンド接続が可能であることを確認します。NTP サーバーの UDP ポート 123 へのアウトバンド トラフィックを許可するファイアウォール ルールを追加します。
>
> このアプライアンス上のインターフェース C がインターネットに接続されていない場合、インターフェース C が NTP サーバーにアクセスする方法を用意する必要があります。1 つの解決策は、ローカル ネットワーク上でインターフェース C からアクセスできる位置に NTP サーバーをインストールすることです。

    - 自分で時刻を設定するには、**[Manually set (手動で設定)]** オプションを選択し、[Date (日付)] と [Time (時刻)] のフィールドの値を変更します。入力フィールドの下に示されている形式を使用します。
  - **[OK]** をクリックし、変更を適用し、保存します。

- アプライアンスの**ホスト名**またはシステム名 (1 ～ 32 文字) を設定します。
  - 最初の文字は英文字でなければなりません。
  - 他の文字には英文字、数字、ダッシュ、またはピリオドを使用できます。
  - 名前の最後の文字にピリオドを使用できません。

重要
これが Web Security Gateway アプライアンスであり、Content Gateway が Integrated Windows Authentication を実行するように設定する場合、ホスト名は (ドメイン名を除き) 11 文字を超えてはなりません。詳細については、Content Gateway Manager Help の *「Integrated Windows Authentication」* のセクションを参照してください。

- システムの識別と管理に役立てるために (特にクラスタ内に複数のアプライアンスが配備されているとき)、固有の**アプライアンスの説明**を作成または編集します。

  説明は、アプライアンスが TRITON Unified Security Center に追加された時にアプライアンス リストに表示されます。

変更が可能なセクションで **[OK]** をクリックすると新しい値が保存および適用されます。**[Cancel (キャンセル)]** は、変更を破棄し、入力フィールドの値を現在の設定に戻します。

V シリーズ 7.7.0 による IPv6 のサポート

TRITON Enterprise のバージョン 7.7 (7.7 V シリーズ アプライアンスを含む) は、IP v 6 の増分サポートを提供します。

V シリーズのサポートは、Web Security および Web Security Gateway (Anywhere) との組み合せによって提供されます。

IP v 6 は Email Security Gateway ではサポートされません。

重要
IPv6 を Web Security Gateway (Anywhere) と共に使用するには、Content Gateway プロキシを**明示のプロキシ**として設定する必要があります。IPv6 は、透過的プロキシ配備では**サポートされません**。

Web Security に対する IPv6 のサポートは下記を含みます。

- インターフェース C および N 上のデュアル IP スタックの実装
- インターネットまたはインターフェース C および N 上のクライアントへの IP v 6 トラフィック (C または N 上で送信された Block ページを含む)

- IPv6 静的経路
- IPv6 データに対する SNMP トラップおよびカウンタ
- Command Line Utility および Command Line Interface 内のネットワーク診断ツール

Web Security Gateway (Anywhere) に対するサポートは上記のすべて、および下記を含みます。

- インターフェース P1 および P2 上のデュアル IP スタックの実装
- インターネットまたはインターフェース P1 および P2、およびそれらにボンディングされたインターフェース (E1/E2) (構成されている場合) へのトラフィック

制限と制約 :

- IPv6 専用の内部ネットワークはサポートされません。
- V シリーズ アプライアンス間、および TRITON コンポーネントとの通信には IP v 4 を使用する必要があります。

IPv6 設定のまとめ

IPv6 サポートはデフォルトでは無効化されています。

Appliance Manager の **「Configuration (設定)」> 「Network (ネットワーク)」 「Interfaces (インターフェース)」> 「IPv6」** ページの上部で IPv6 を有効化できます。IPv6 サポートを有効化すると、アプライアンス上のすべての関連する機能に対してすべての IPv6 サポートが有効化されます。

IPv6 アドレスを受け入れるフィールドでは、アドレスを標準に適合する任意の形式で入力できます。例 :

- 16 ビット値の中の先頭の 0 を省略できます
- 連続する 0 の 1 つのグループをダブル コロンに置換できます

IP v 6 サポートを無効化するには、アプライアンスのフル再起動が必要です。

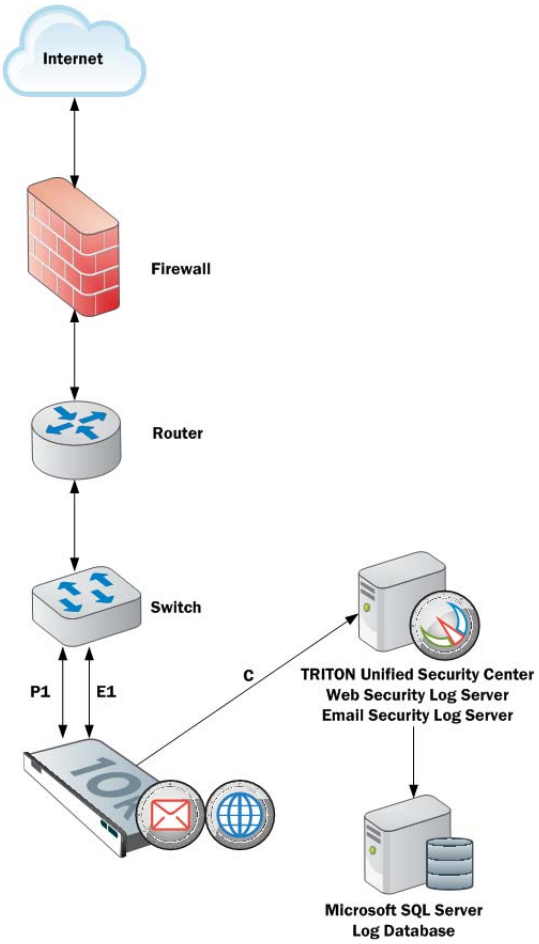
IPv6 が無効化されると、IPv6 の値は設定ファイルに残りますが、編集することはできません。

ネットワーク インタフェースの設定

「Configuration (設定)」> 「Network Interfaces IPv4 (ネットワーク インタフェース IP v 4)」 および **「IPv6」** のページを使用して、アプライアンス上の各ネットワーク インターフェースの IP アドレス、サブネット マスク、デフォルト ゲートウェイ、DNS アドレスを指定します。

- *Appliance Controller インターフェース (C)*
- *Websense Content Gateway インターフェース (P1 および P2)*
- *Network Agent インターフェース (N)*

- *Email Security Gateway インターフェース (E1 および E2)*
- *インターフェースのボンディング*



Web Security Gateway (Anywhere) を備えたアプライアンスは、C、P1、P2、および N の IPv6 アドレスをサポートします。

Appliances with Email Security Gateway を備えたアプライアンスは、E1 および E2 の IPv6 アドレスを**サポートしません**。

IPv6 サポートの詳細については、*V シリーズ 7.7.0 による IPv6 のサポート* を参照してください。

[OK] をクリックして、各セクションに新しい値を保存し、適用します。

Appliance Controller インターフェース (C)

Appliance Controller インターフェース (C) :

- すべての Websense 管理インターフェースと通信する
- Websense Data Security サーバーと通信する
- アプライアンス間通信を提供する
- 非 HTTP および非 HTTPS プロトコルの強制を転送する (オプション)

- インターネットを通じて Websense Master Database ダウンロードを処理する（ユーザーのサイトがデータベース ダウンロード用に PI を使用していない場合）。

C インターフェースの初期設定は、アプライアンスに最初に電源を投入したときに完了します。**firstboot** というスクリプトがインタフェース C を構成するために必要な値を要求します。

重要

C インターフェースの IP アドレスの変更は配備に大きな影響を与え、一部のコンポーネントの再インストールが必要になる場合があります。

アプライアンスが製造環境にあり、C インターフェースの IP アドレスを変更する必要がある場合は、*C インターフェース IP アドレスの変更*, 31 ページ を参照してください。

C インターフェースの IP アドレスの入力フィールドを有効にするには、マウス ポインタを iHelp アイコンの上に置き、ポップアップの [Enable IP (IP を有効化する)] フィールドをクリックします。

ネットワーク インターフェース C の設定のガイドライン

IP アドレス (C インターフェース)	必須。 このインターフェースは一般的にインターネットへの継続的なアクセスを必要としますが、一部のサイトはインターネットとのすべての通信に P1 を使用します。 C インターフェースの IP アドレスを変更する場合、更新プロセスに約 10 分かかります。 IP アドレスを変更した後、ログオン ページに戻ります。ユーザー名とパスワードを入力します。 **「Status (ステータス)」> 「General (一般)」**ページはサービスが起動中であることを示します。すべてのサービスが起動するまで待ちます。
サブネット マスク (C)	必須。
デフォルト ゲートウェイ (C)	オプション。 トラフィックをサブネットの外へ経路指定できるルータの IP アドレス。
一次 DNS (C)	必須。 ドメイン名サーバーの IP アドレス。
二次 DNS (C)	オプション。 一次 DNS が利用できない場合にバックアップとして使用します。
三次 DNS (C)	オプション。 一次 DNS と二次 DNS が利用できない場合にバックアップとして使用します。

Websense Content Gateway インターフェース (P1 および P2)

Websense Content Gateway インターフェース (P1 および P2) は、Websense Content Gateway モジュールとの間で転送されるトラフィックを処理します。

- P1 および P2 プロキシ インターフェースはどちらも、ユーザーのインターネット要求を受け入れ (インバウンド トラフィック)、Web サービスと通信する (アウトバウンド トラフィック) ために使用できます。つまり、どちらのインターフェースも、プロキシ モジュールとの間のトラフィックを処理するように構成できます。
- 一般的な構成では、インバウンドとアウトバウンドの両方のトラフィックに対して P1 を使用し、P2 は使用しません。
- もう 1 つのオプションは、P1 がユーザーのインターネット要求を受け入れる (インバウンドのみ) ように構成することです。この場合、P2 が Web サーバーと通信する (アウトバウンド) ように構成します。

重要

P2 インターフェースを使用する場合、P1 インターフェースは eth0 にバインドされ、P2 インターフェースは eth1 にバインドされます。Websense Content Gateway を設定するとき、このことに留意してください。

たとえば、透過的プロキシ配備を使用しており、P1 インターフェースが WCCP ルータに接続されていると想定します。この場合、Websense Content Gateway が WCCP 通信に対して eth0 を使用するように設定する必要があります (Content Gateway Manager で、**「Configure (設定)」> 「Networking (ネットワーク)」> 「WCCP」** ページの [General (一般)] タブを参照してください)。

ネットワーク インタフェース P1 および P2 の設定のガイドライン

一般的なガイドライン	P1 と P2 の両方を使用する場合、それらを同じサブネットに配置する必要があります。デフォルト ゲートウェイは自動的に P2 に割り当てられます（これは eth1 にバインドされます）。アウトバウンド パケットがインターネットにアクセスできることを確認してください。
IP アドレス（P1 または P2 インターフェース）	必須。
Subnet mask（サブネット マスク）	必須。
デフォルト ゲートウェイ	必須。 ゲートウェイは、インターネットとの通信（アウトバウンド トラフィック）に使用するインターフェース（P1 または P2）の IP アドレスと同じサブネットの中に配置する必要があります 。 P1 と P2 の両方を使用する場合、それらを同じサブネットに配置する必要があります。デフォルト ゲートウェイは自動的に P2 に割り当てられます（これは eth1 にバインドされます）。アウトバウンド パケットがインターネットにアクセスできることを確認してください。
一次 DNS	必須。 ドメイン名サーバーの IP アドレス。
二次 DNS	オプション。 一次 DNS が利用できない場合にバックアップとして使用します。
三次 DNS	オプション。 一次 DNS と二次 DNS が利用できない場合にバックアップとして使用します。

Network Agent インターフェース（N）

Network Agent は、HTTP および HTTPS 以外のプロトコルをフィルタリングするために使用する ソフトウェア コンポーネントです。これは帯域幅最適化データと拡張ロギング詳細情報を提供します。

Network Agent はネットワーク・ポートでの送信バイト数を含め、全体的なネットワーク利用状況を、継続的にモニタリングします。このエージェントは、事前指定されている間隔で他の Websense ソフトウェアに利用状況のサマリを送信します。

Network Agent は、通常、ネットワーク内のインバウンドとアウトバウンドの両方のトラフィックをモニタリングするように設定します。エージェントは、下記を区別します。

- 社内コンピュータ間で送信される要求（例、イントラネット サーバーへのヒット）
- 社内コンピュータからウェブ サーバーなどの外部コンピュータに送信される要求（例、ユーザー インターネット要求）

非 HTTP プロトコルのブロック情報をインターフェース C かインターフェース N のどちらに経路指定するかを選択します。

ネットワーク インターフェース N の設定のガイドライン

非 HTTP および 非 HTTPS トラフィックのブロック情報を送信するために使用するインターフェースを選択します。	• インターフェース C を使ってブロック情報を送信する場合は、**インターフェース C** のみを選択します。 • ネットワーク インターフェース N を双方向スパン ポートに接続し、N を使用してブロック情報を転送する場合は、**インターフェース N** を選択します。 TRITON – Web Security で設定されているブロック用 NIC の設定は、このペインで入力する設定を無効にしません。Appliance Manager での設定が優先します。
N インターフェースの IP アドレス	必須。 Network Agent はネットワーク内のインバウンドとアウトバウンドの両方のトラフィックをモニタリングできる必要があります。Network Agent はポート 80 および 443 を無視します。
Subnet mask（サブネット マスク）	インターフェース N が選択されている場合は必須。そうでない場合は、サブネット マスクには固定値 255.255.255.255 が設定されます。
デフォルト ゲートウェイ	インターフェース N がチェックされている場合は必須。そうでない場合は、このフィールドは無効化されます。
一次 DNS	必須。 ドメイン名サーバーの IP アドレス。
二次 DNS	オプション。 一次 DNS が利用できない場合にバックアップとして使用します。
三次 DNS	オプション。 一次 DNS と二次 DNS が利用できない場合にバックアップとして使用します。

代わりに Network Agent をネットワーク内の別のサーバーにインストールすることができます。要件については、*『V- Series Appliance Getting Started Guide』* を参照してください。

Email Security Gateway インターフェース (E1 および E2)

Websense Email Security Gateway インターフェースは、Websense Email Security Gateway モジュールとの間のインバウンドおよびアウトバウンド トラフィックを処理します。

ご注意
インターフェースの名前は、V シリーズ アプライアンスのモジュールによって異なります。V10000 G2 では E1 と E2 が使用されます。V5000 G2 では P1 と P2 が使用されます。

- E1 および E2 インターフェースはどちらも、インバウンド トラフィックを受け入れ、アウトバウンド トラフィックを送信するために使用できます。V5000 G2 では P1 と P2 を使用します。
- 一般的な構成では、インバウンドとアウトバウンドの両方のトラフィックに対して E1 を使用し、E2 は使用しません。
- もう 1 つのオプションは、E1 がインバウンドを受け入れ、E2 がアウトバンド トラフィックを送信するように構成することです。
- 大量のアウトバウンド トラフィックをサポートする必要があるとき、E1 または E2 上に仮想インターフェースを構成することができます。*Email Security 仮想インターフェース*, 29 ページ を参照してください。

重要

V10000 G2 では、E2 インターフェースを使用する場合、E1 インターフェースは eth0 にバインドされ、E2 インターフェースは eth1 にバインドされます。Websense Email Security Gateway を設定するとき、このことに留意してください。

V5000 G2 では、P2 インターフェースを使用する場合、P1 インターフェースは eth0 にバインドされ、P2 インターフェースは eth1 にバインドされます。Websense Email Security Gateway を設定するとき、このことに留意してください。

ネットワーク インタフェース E1 および E2 の設定のガイドライン

ご注意

v5000 G2 では E1 を P1 に、E2 を P2 に置き換えます。

E1 と E2 の両方を使用し、それらを同じサブネットに配置する場合、デフォルト ゲートウェイは自動的に E2 に割り当てられます（これは eth1 にバインドされます）。アウトバウンド パケットがインターネットにアクセスできることを確認してください。

IP アドレス（E1 または E2 インターフェース）	必須。
Subnet mask（サブネット マスク）	必須。

デフォルト ゲートウェイ	必須。 ゲートウェイは、インターネットとの通信（アウトバウンド トラフィック）に使用するインターフェース（E1 または E2）の IP アドレスと同じサブネットの中に配置する必要があります 。 E1 と E2 の両方を使用し、それらを同じサブネットに配置する場合、デフォルト ゲートウェイは自動的に E2 に割り当てられます（これは eth1 にバインドされます）。アウトバウンド パケットがインターネットにアクセスできることを確認してください。
一次 DNS	必須。 ドメイン名サーバーの IP アドレス。
二次 DNS	オプション。 一次 DNS が利用できない場合にバックアップとして使用します。
三次 DNS	オプション。 一次 DNS と二次 DNS が利用できない場合にバックアップとして使用します。

Email Security 仮想インターフェース

E1 または E2 上に複数の仮想 IP アドレスを設定できます。

- 仮想 IP アドレスは、アウトバウンド トラフィックにのみ使用します。
- 仮想 IP アドレスは、指定した物理インターフェースにバインドされます。
- 仮想 IP アドレスは、指定した物理インターフェースと同じサブネットに配置する必要があります。
- それぞれの物理インターフェース（E1 と E2）に対して最大 10 個の仮想 IP アドレスを指定できます。

複数の仮想インターフェースは、複数のドメインおよび（または）大量のアウトバウンド トラフィックをサポートする場合に便利です。

E1 または E2 に仮想 IP アドレスを追加するには、下記の手順を実行します。

1. **「Configure（設定）」>「Network Interfaces（ネットワーク インターフェース）」>「Virtual Interfaces（仮想インターフェース）」**に進み、**[Add（追加）]** をクリックします。
2. E1 または E2 を選択します。E2 を構成していない場合は、選択できません。
3. [Virtual IP address（仮想 IP アドレス）] 入力フィールドの各行に 1 つの IPv4 アドレスを入力します。
4. **[Add Interfaces（インターフェースを追加）]** をクリックします。

仮想 IP インターフェースを削除するには、下記の手順を実行します。

1. **「Configure」>「Network Interfaces」>「Virtual Interfaces」**ページで、削除するエントリの左側のチェック ボックスを選択し、**[Delete（削除）]** をクリックします。
2. 削除することを確認します。

インターフェースのボンディング

V10000 アプライアンス (Websense Web Security のみ) および 1 つのモジュール – Websense Web Security または Websense Email Security Gateway – だけを実行する V10000 G2 アプライアンスは、フェイルオーバー またはバランシング用にインターフェースをボンディングできます。構成の詳細は下記の通りです。

V5000 G2 アプライアンス上ではインターフェースのボンディングはサポートされていません。

Websense Web Security のみを使用する V10000/V10000 G2

インターフェース E1 および E2 をネットワークに接続し、次にソフトウェア設定を通じて Websense Content Gateway インターフェースにボンディングします (オプションで E 1 を P1 に、E2 を P2 にボンディングします)。他のペアリングはできません。

インターフェースのボンディングは、下記の方法で利用できます。

- アクティブ / スタンバイ モード : P1 (または P2) がアクティブ モードで、E1 (または E2) がスタンバイ モード。プライマリ インターフェースに障害が発生した場合にのみ、それにボンディングされているインターフェース (E1 または E2) がアクティブになります。
- ロード バランシング : V10000/V10000 G2 に直接に接続されているスイッチまたはルータがロード バランシングをサポートする場合 (etherchannel、トランク グループまたは同様の構成)、プライマリ インターフェースとの間のトラフィックをプライマリ インターフェースとそれにボンディングされているインターフェース (E1 または E2) との間で分散することができます。

それぞれの Websense Content Gateway インターフェース (P1 および P2) について、ボンディングするかどうかを個別に選択できます。ボンディングを全く行わなくてもかまいません。

インターフェース (P1 または P2) をボンディングする場合、そのボンディングについていずれかのモード (アクティブ / スタンバイ またはロード バランシング) を選択します。両方のインターフェースに対して同じボンディング モードを選択する必要はありません。

ボンディングの前にすべてのインターフェースが適切に接続されていることを確認してください。

Websense Email Security Gateway のみを使用する V10000 G2

インターフェース P1 および P2 をネットワークに接続し、次にソフトウェア設定を通じて Websense Email Security Gateway インターフェースにボンディングします (オプションで P1 を E1 に、P2 を E2 にボンディングします)。他のペアリングはできません。

インターフェースのボンディングは、下記の方法で利用できます。

- アクティブ / スタンバイ モード : E1 (または E2) がアクティブ モードで、P1 (または P2) がスタンバイ モード。プライマリ インターフェースに障害が発生した場合にのみ、それにボンディングされているインターフェース (P1 または P2) がアクティブになります。
- ロード バランシング : V10000/V10000 G2 に直接に接続されているスイッチまたはルータがロード バランシングをサポートする場合 (etherchannel、トランク グループまたは同様の構成)、プライマリ インターフェースとの間のトラフィックをプライマリ インターフェースとそれにボンディングされているインターフェース (P1 または P2) との間で分散することができます。

それぞれの Websense Email Security Gateway インターフェース (E1 および E2) について、ボンディングするかどうかを個別に選択できます。ボンディングを全く行わなくてもかまいません。

インターフェース (E1 または E2) をボンディングする場合、そのボンディングについていずれかのモード (アクティブ / スタンバイ またはロード バランシング) を選択します。両方のインターフェースに対して同じボンディング モードを選択する必要はありません。

ボンディングの前にすべてのインターフェースが適切に接続されていることを確認してください。

C インターフェース IP アドレスの変更

C インターフェース IP アドレスを変更しなければならない場合があります。それによる影響とその対処方法はアプライアンスの設定および配備の詳細によって異なります。**実行するべきアクティビティの数やサービス中断が重大な問題になる場合があります。可能な限り、現在の C インターフェース IP アドレスを変更しないでください。**

多くの場合、アプライアンスに依存する、またはアプライアンスに直接にサービスを提供するオフボックス コンポーネントは、C インターフェース IP アドレスを変更する前にアンインストールし、IP アドレスの変更が完了してから再インストールする必要があります。これには、下記のコンポーネントが含まれます。

- オフボックス TRITON Unified Security Center
- Filtering Service
- Network Agent
- Real Time Monitor
- DC Agent
- Logon Agent
- eDirectory Agent
- Radius Agent
- Remote Filtering Service
- Sync Service

- Linking Service

重要
何らかの変更を行う前に、アプライアンスおよび影響を受けるオフボックス コンポーネントのバックアップを作成することを強く推奨します。

下記のうち、ユーザーの配備と一致するシナリオのステップに従ってください。

シナリオ 1：1 つのアプライアンス、Web Security のみ、オンボックス TRITON Unified Security Center およびオフボックス Log Server を使用

シナリオ 2：1 つのアプライアンス、Web Security のみ、オフボックス TRITON Unified Security Center およびオフボックス Log Server を使用

シナリオ 3：1 つまたは複数のアプライアンス、Email Security Gateway のみ、オフボックス TRITON Unified Security Center およびオフボックス Log Server を使用

シナリオ 4：1 つのアプライアンス、Web Security および Email Security、オフボックス TRITON Unified Security Center およびオフボックス Log Server を使用

シナリオ 5：1 つのクラスタ内の複数のアプライアンス、Web Security のみ、オフボックス TRITON Unified Security Center、およびオフボックス Log Server を使用

シナリオ 6：1 つクラスタ内の複数のアプライアンス、Web Security のみ、オフボックス Policy Broker、オフボックス TRITON Unified Security Center、およびオフボックス Log Server を使用

シナリオ 1：1 つのアプライアンス、Web Security のみ、オンボックス TRITON Unified Security Center およびオフボックス Log Server を使用

この構成は、小規模な配備および Proof of Concept（コンセプトの証明）プロジェクト用です。

ステップの概要は以下の通りです。

1. Web DLP を構成する場合、Data Security Management Server で Content Gateway の登録を削除します。
2. Log Server ホストで Log Server サービスを停止します。
3. アプライアンス上で、C インターフェース IP アドレスを変更します。
4. Log Server ホストで、websense.ini の 「IP address of the Policy Server (Policy Server の IP アドレス)」のエントリを新しい C インターフェース IP アドレスに変更し、Log Server を再起動します。

5. Web DLP を使用する場合、Content Gateway モジュールを起動すると自動的にそれが Data Security Management Server に再登録されます。

詳細なステップごとの手順については、「Websense」「Technical Library（テクニカル ライブラリ）」に進み、*「C インターフェース IP アドレスの変更：ステップごとの手順」というタイトルの文書を参照してください。*

シナリオ 2：1 つのアプライアンス、Web Security のみ、オフボックス TRITON Unified Security Center およびオフボックス Log Server を使用

ステップの概要は以下の通りです。

1. Web DLP を構成する場合、Data Security Management Server で Content Gateway の登録を削除します。
2. Log Server ホストで Log Server サービスを停止します。
3. TRITON Unified Security Center ホスト上で、TRITON Unified Security Center および関連するコンポーネント（上記のコンポーネント リストを参照）をアンインストールします。アンインストールしたコンポーネントのリストを作成します。
4. アプライアンス上で、C インターフェース IP アドレスを変更します。
5. TRITON Unified Security Center および関連するコンポーネントを再インストールします。
6. Log Server ホストで、websense.ini の 「IP address of the Policy Server (Policy Server の IP アドレス)」のエントリを新しい C インターフェース IP アドレスに変更し、Log Server を再起動します。
7. Web DLP を使用する場合、Content Gateway モジュールを起動すると自動的にそれが Data Security Management Server に再登録されます。

詳細なステップごとの手順については、「Websense」「Technical Library（テクニカル ライブラリ）」に進み、*「C インターフェース IP アドレスの変更：ステップごとの手順」というタイトルの文書を参照してください。*

シナリオ 3：1 つまたは複数のアプライアンス、Email Security Gateway のみ、オフボックス TRITON Unified Security Center およびオフボックス Log Server を使用

ステップの概要は以下の通りです。

1. Email DLP を使用している場合、Email DLP の登録を削除します。
2. アプライアンス上で、C インターフェース IP アドレスを変更します。
3. TRITON – Email Security でアプライアンス IP アドレスを新しい値に変更します。
4. Email DLP を使用している場合、Email DLP を再登録します。

詳細なステップごとの手順については、「Websense」「Technical Library（テクニカル ライブラリ）」に進み、*「C インターフェース IP アドレスの変更：ステップごとの手順」というタイトルの文書を参照してください。*

シナリオ 4：1 つのアプライアンス、Web Security および Email Security、オフボックス TRITON Unified Security Center およびオフボックス Log Server を使用

ステップの概要は以下の通りです。

1. Web DLP を使用している場合、Data Security Management Server で Content Gateway の登録を削除します。
2. Email DLP を使用している場合、Data Security Management Server で Email DLP の登録を削除します。
3. Log Server ホストで Log Server サービスを停止します。
4. TRITON Unified Security Center ホスト上で、TRITON Unified Security Center および関連するコンポーネント（上記のコンポーネント リストを参照）をアンインストールします。アンインストールしたコンポーネントのリストを作成します。
5. アプライアンス上で、C インターフェース IP アドレスを変更します。
6. TRITON Unified Security Center および関連するコンポーネントを再インストールします。
7. Log Server ホストで、websense.ini の 「IP address of the Policy Server (Policy Server の IP アドレス)」のエントリを新しい C インターフェース IP アドレスに変更し、Log Server を再起動します。
8. TRITON – Email Security でアプライアンス IP アドレスを新しい値に変更します。
9. Email DLP を使用している場合、Data Security Management Server に再登録します。
10. Web DLP を使用する場合、Content Gateway モジュールを起動すると自動的にそれが Data Security Management Server に再登録されます。

詳細なステップごとの手順については、「Websense」「Technical Library（テクニカル ライブラリ）」に進み、*「C インターフェース IP アドレスの変更：ステップごとの手順」というタイトルの文書を参照してください。*

シナリオ 5：1 つのクラスタ内の複数のアプライアンス、Web Security のみ、オフボックス TRITON Unified Security Center、およびオフボックス Log Server を使用

このシナリオで扱う操作

1. ポリシー ソース アプライアンス全体の C インターフェースの変更
2. ユーザー ディレクトリおよびフィルタリング アプライアンスの C インターフェースの変更

3. Filtering のみのアプライアンスの C インターフェースの変更

ポリシー ソース アプライアンス全体の C インターフェースの変更のステップの概要：

1. Web DLP を構成する場合、Data Security Management Server で Content Gateway の登録を削除します。
2. Log Server ホストで Log Server サービスを停止します。
3. TRITON Unified Security Center ホスト上で、TRITON Unified Security Center および関連するコンポーネント（上記のコンポーネント リストを参照）をアンインストールします。アンインストールしたコンポーネントのリストを作成します。
4. クラスタ内のすべてのアプライアンスのポリシー ソース設定のドキュメントを作成し、次に「ユーザー ディレクトリおよびフィルタリング」と「フィルタリングのみ」のアプライアンス上でポリシー ソースの設定を「Full」ポリシー ソースに変更します。
5. 元の「Full」ポリシー ソース アプライアンス上で、C インターフェース IP アドレスを変更します。
6. 「ユーザー ディレクトリおよびフィルタリング」と「フィルタリングのみ」のそれぞれのアプライアンス上で、ポリシー ソース設定を「Full」ポリシー ソースから元の設定に変更し、アプライアンスを新しい「Full」ポリシー ソース C インターフェース IP アドレスに関連付けます。
7. TRITON Unified Security Center および関連するコンポーネントを再インストールします。
8. Log Server ホストで、websense.ini の 「IP address of the Policy Server (Policy Server の IP アドレス)」のエントリを新しい C インターフェース IP アドレスに変更し、Log Server を再起動します。
9. Web DLP を使用する場合、Content Gateway モジュールを起動すると自動的にそれが Data Security Management Server に再登録されます。

「ユーザー ディレクトリおよびフィルタリング」アプライアンスの C インターフェースの変更のステップの概要：

1. C インターフェース IP アドレスを変更する「ユーザー ディレクトリおよびフィルタリング」アプライアンスに登録されているオフボックス コンポーネント（例、Network Agent）をアンインストールします。
2. C インターフェース IP アドレスを変更する「ユーザー ディレクトリおよびフィルタリング」アプライアンスに依存する「フィルタリングのみ」アプライアンスを一時的に「Full」ポリシー アプライアンスに設定します。
3. 「ユーザー ディレクトリおよびフィルタリング」アプライアンスの C インターフェース IP アドレスを変更します。
4. 「フィルタリングのみ」アプライアンスのポリシー ソース設定を元に戻し、それを新しい「ユーザー ディレクトリおよびフィルタリング」C インターフェース IP アドレスに関連付けます。

5. 「ユーザー ディレクトリおよびフィルタリング」アプライアンスに登録されているオフボックス コンポーネントを再インストールします。

「フィルタリングのみ」アプライアンスの C インターフェースの変更のステップの概要：

1. C インターフェース IP アドレスを変更する「フィルタリングのみ」アプライアンスに登録されているオフボックス コンポーネント（例、Network Agent）をアンインストールします。
2. C インターフェース IP アドレスを変更します。
3. 「フィルタリングのみ」アプライアンスに登録されているオフボックス コンポーネントを再インストールします。

詳細なステップごとの手順については、「Websense」「Technical Library（テクニカル ライブラリ）」に進み、*「C インターフェース IP アドレスの変更：ステップごとの手順」というタイトルの文書を参照してください。*

シナリオ 6：1 つクラスタ内の複数のアプライアンス、Web Security のみ、オフボックス Policy Broker、オフボックス TRITON Unified Security Center、およびオフボックス Log Server を使用

ご注意
どのアプライアンスも「Full」ポリシー ソースに設定されません。

ステップの概要は以下の通りです。

1. Web DLP を構成する場合、Data Security Management Server で Content Gateway の登録を削除します。
2. C インターフェース IP アドレスを変更するアプライアンスに登録されているオフボックス コンポーネント（例、Network Agent）をアンインストールします。
3. クラスタ内のすべてのアプライアンスのポリシー ソース設定のドキュメントを作成し、次に各アプライアンスのポリシー ソース設定を「Full」ポリシー ソースに変更します。
4. C インターフェース IP アドレス（複数のアプライアンスを変更する場合は複数）を変更します。
5. アプライアンスのポリシー ソース設定を元のモードに戻し、必要に応じてそれらのアプライアンスを変更したアプライアンスの新しい C インターフェース IP アドレスに関連付けます（アプライアンスが「フィルタリングのみ」アプライアンスで、C インターフェースの変更先がそれに関連付けられている「ユーザー ディレクトリおよびフィルタリング」アプライアンスである場合）。

6. クラスタ内のアプライアンスに登録されているオフボックス コンポーネントを再インストールします。
7. Web DLP を使用する場合、Content Gateway モジュールを起動すると自動的にそれが Data Security Management Server に再登録されます。

詳細なステップごとの手順については、「Websense」「Technical Library（テクニカル ライブラリ）」に進み、*「C インターフェース IP アドレスの変更：ステップごとの手順」というタイトルの文書を参照してください。*

ルーティングの設定

「Configuration」>「Routing（ルーティング）」ページを使用して、下記の経路を指定します。

- サブネットおよびクライアント コンピュータから任意のアクティブ アプライアンス インターフェース（N を除く）を経由する静的経路。IP v 6 が有効化されている場合、静的 IPv6 経路も追加およびインポートできます。
- アプライアンス モジュールからアプライアンス インターフェース C を経由してサブネットに至るモジュール経路 IPv6 モジュール経路は**サポートされません**。

静的経路の設定

- アプライアンス上の N 以外の任意のアクティブ インターフェースに対して静的経路を指定できます。N は Network Agent 専用で、ルーティングできません。
- 同じモジュール上の 2 つの異なるインターフェースに同じ経路を追加することはできません。それを試みた場合、アプライアンスにエラーが表示されます。
- インターフェースに対して静的経路が指定され、その後にインターフェースが非アクティブになった場合でもその静的経路はルーティング テーブルから消去されず、非アクティブであることを示すグレイで表示されます。
- インターフェースの IP アドレスの変更によって無効になった静的経路は無効化され、赤で表示されます。
- 静的経路を追加および削除できますが、変更はできません。経路を変更するには、それを削除し、新しい値を指定して新しい経路を追加します。
- 静的経路を追加、インポート、または削除したときは、指定されたインターフェースを管理するモジュールに関連するサービスを再起動する必要があります。たとえば、インターフェース P1 に静的経路を追加する場合、追加を完了したときにすべての Content Gateway サービスを再起動する必要があります。
- 静的経路テーブルは、最大 5000 個のエントリを含みます。

静的経路の追加

静的経路は一度に 1 つ、またはインポート ファイルを使用すれば複数を追加できます。

静的経路を追加したとき、各フィールドに入力されたデータがアプライアンスによって検証され、経路が不適切である場合はエラー メッセージが表示されます。

静的経路を追加するには、下記の手順を実行します。

1. **「Configuration」>「Routing（ルーティング）」**ページに進み、[IPv4] または [IPv6] タブを選択し、**[Static Routes（静的経路）]** タブで **[Add/Import（追加 / インポート）]** をクリックします。
2. **手動で 1 つの経路を追加するには、[Add individual route（個別の経路を追加）]** ラジオ ボタンを選択し、すべてのフィールドに値を入力し、**[経路を追加]** をクリックします。

Destination Network （宛先ネットワーク）	必須。トラフィックの宛先のサブネット IP アドレスを指定します。
Subnet Mask （サブネット マスク）(IPv4) または Subnet prefix length （サブネット プレフィクスの長さ）(IPv6)	必須。 クライアントが常駐するネットワークのサブネット マスク またはプレフィックス (255.255.0.0、64 など）
Gateway （ゲートウェイ）	必須。 プロキシ サブネットからクライアント サブネットへのアクセスを提供する IP アドレス。このアドレスはアプライアンスと同じサブネット上である必要があります。
Interface （インターフェース）	必須。 静的経路に使用するアプライアンス インターフェース。アクティブ インターフェースだけがドロップ ダウン リストに表示されます。

3. **インポート リスト ファイルを使って複数の経路を追加するには、**下記の手順を実行します。
   a. インポート ファイルを準備します。下記の**「インポート ファイル仕様」**を参照してください。
   b. **[Import route file（経路ファイルをインポート）]** ラジオ ボタンを選択します。
   c. 完全パスとファイル名を指定するか、または **[Browse（参照）]** を使ってファイルを指定します。**[Import Route（経路をインポート）]** をクリックして、ファイル内で指定されている経路をインポートします。

      アプライアンスはファイルを読み込み、各経路を検証し、無効の経路についてエラーを報告します。

重複する経路エントリは無視されます。重複するエントリは作成されません。

ファイル内の経路の数と既存の経路の数の合計が経路テーブルの制限(5000)を超える場合は、インポートは失敗します。経路は追加されず、エラー メッセージが表示されます。

インポートファイルの仕様:

1. ファイルはプレーン テキスト ファイルでなければなりません。(大部分のルーターは経路テーブルをプレーン テキスト ファイルにエクスポートします)。
2. ファイルに注釈行を含めることができます。Comment lines begin with ?#?.
3. 経路を指定する行は、下記の 4 つのフィールドをこの順序で含んでいる必要があります。各フィールドをスペースで区切る必要があります。

   IPv4 の場合:

   ```
   destination netmask default-gateway interface
   ```

   Destination はサブネット アドレスまたはホスト IP アドレスです。

   Netmask は、*宛先*の適切な値を決定します。

   Default-gateway は、次のホップです。

   Interface は、トラフィックのルーティングに使用するアプライアンス インターフェースです。指定したインタフェースは有効化されている必要があります。無効化されている場合、アプライアンスはエラーを報告し、経路を追加しません。

   IPv6 の場合:

   ```
   destination prefix-length default-gateway interface
   ```

   Destination はサブネット アドレスまたはホスト IP アドレスです。

   Prefix-length は、*宛先*の適切な値を決定します。

   Default-gateway は、次のホップです。

   Interface は、トラフィックのルーティングに使用するアプライアンス インターフェースです。指定したインタフェースは有効化されている必要があります。無効化されている場合、アプライアンスはエラーを報告し、経路を追加しません。

静的経路の削除

1. [静的経路]テーブルで削除する経路を選択します。
   - 1 つの経路を選択するには、削除するエントリの左側のボックスをクリックします。
   - 複数のエントリを選択するには、削除する各エントリの左側のボックスをクリックします。
   - すべての経路を削除するには、**「Destination Network(宛先ネットワーク)」**のラベルの左側のボックスをクリックします。
2. **[削除]**をクリックします。

経路テーブルのエクスポート

経路テーブルをテキスト ファイルにエクスポートするには、**[Export Table (テーブルをエクスポート)]** をクリックします。[Browse (参照)] ダイアログを使ってファイルの場所と名前を指定します。

テーブル内の経路が、有効化されているかどうかに関わりなくすべてエクスポートされます。

ファイルは、上記でインポート ファイルについて示した形式で作成されます。

モジュール経路の設定

配備先によっては、一部の Web Security または Email Security トラフィックをアプライアンス C インターフェース経由でルーティングする必要がある、またはそうすることが望ましい場合があります (一般的には Web および 電子メール トラフィックのルーティングのために別の、専用インターフェース (P1/P2、E1/E2) が使用され、C は管理トラフィック用に予約されます)。しかし、一部のサイトでは C インターフェースを通じて認証 (または他の) トラフィックをルーティングすることもできます。そのためには **「Configuration」> 「Routing」** ページでモジュール経路を定義します。

モジュール経路テーブルは、最大 5000 個のエントリを含みます。

モジュール経路の追加

1. **「Configuration」> 「Routing」** ページの 「Module Route (モジュール 経路)」セクションで **[Add (追加)]** をクリックします。
2. 各フィールドの値を指定し、**[Add Route (経路を追加)]** をクリックします。

Module	必須。ドロップダウン リストからモジュールを選択します。リストにはアプライアンス上にインストールされているモジュールだけ表示されます。Network Agent モジュールはインストールできますが、このリストには表示されません。
Destination subnet (宛先サブネット)	必須。トラフィックの宛先のサブネット IP アドレスを指定します。
Subnet mask (サブネット マスク)	必須。宛先サブネットのサブネット マスク。

ご注意
サブネット上にエンドポイントがあることを確認するのは管理者の責任です。

モジュール経路の削除

1. 「静的経路」セクションで削除する経路を選択します。

- 1 つの経路を選択するには、削除するエントリの左側のボックスをクリックします。
- 複数のエントリを選択するには、削除する各エントリの左側のボックスをクリックします。
- すべての経路を削除するには、**「Module（モジュール）」**のラベルの左側のボックスをクリックします。

2. **[削除]** をクリックします。

アラート

「Configuration」>「Alerting（アラート）」ページを使用して、SNMP アラートを有効化および設定します。

SNMP アラートには 2 つの方法があり、**「Setup（設定）」**タブでそれを有効化できます。

- SNMP マネージャがアプライアンスの標準 SNMP カウンタをポーリングできるようにする（*SNMP ポーリング（モニタリング）を有効化する* を参照）。
- アプライアンスが選択したイベントに関する SNMP トラップを SNMP マネージャに送信するように設定する（*SNMP トラップの有効化* を参照）。

  アプライアンス上で SNMP トラップ サーバーを有効化した後、**[Alerts（アラート）]** タブを使用して、どちらのイベントでトラップを送信するかを設定します。*特定のアラートの有効化*, 43 ページ を参照してください。

SNMP ポーリング（モニタリング）を有効化する

1. Monitoring Server で **[On（オン）]** をクリックします。
2. ネットワークで使用する **SNMP バージョン**（v1、v2c、または v3）を選択します。
   - SNMP v1 および v2c では、コミュニティー名のあとにカウンタの生成元モジュールを示す接尾辞（-wcg、-wws、-na、または -esg）が付けられます。
   - SNMP v3 では、各モジュールのカウンタをポーリングするためにコンテクスト名（WCG、WWS、NA、または ESG）を指定できます。
3. v1 または v2c を選択した場合、アプライアンスの**コミュニティー名**を指定し、次に **[OK]** をクリックします。

   これで SNMP モニタリングの設定を完了しました。
4. v3 を選択した場合、ネットワークで使用する**セキュリティ レベル**（「None（なし）」、「Authentication only（認証のみ）」、または「Authentication and Encryption（認証と暗号化）」）を選択し、SNMP 通信に関連付ける**ユーザー名**を選択します。

5. 認証を含むセキュリティ レベルを選択した場合、選択したユーザー名に対応する**パスワード**も入力および確認し、次に**認証プロトコル** (MD5 または SHA) を選択します。
6. 認証と暗号化を選択した場合、**暗号プロトコル** (DES または AES) を選択し、次に暗号化に使用する**プライバシー パスワード**を入力および確認します。
7. **[OK]** をクリックし、変更を適用します。

SNMP トラップの有効化

アプライアンスが SNMP トラップを送信できるようにする前に、**「Configuration」> 「Alerting (アラート)」**ページの「Trap Server (トラップ サーバー)」セクションのリンクを使って、**アプライアンスの MIB ファイル**をダウンロードします。SNMP マネージャがアプライアンスによって送信されたトラップを解釈できるためには、SNMP マネージャに MIB ファイルがインストールされている必要があります。

アプライアンスが SNMP トラップの送信を開始する準備が完了したあと、以下の手順を実行します。

1. 「Trap Server」で **[On]** をクリックし、ネットワークで使用する SNMP のバージョン (v1、v2c、または v3) を選択します。
2. SNMP v1 または v2c では、下記の情報を入力します。
   - アプライアンスによって送信されるトラップに関連付ける**コミュニティー名**
   - SNMP マネージャが使用する IP アドレスとポート。
3. 設定を確認するには、**[Send Test Trap (テスト トラップを送信する)]** をクリックします。テスト トラップの送信が成功した場合、**[OK]** をクリックして変更を適用し、保存します。どちらのイベントでトラップを送信するかを設定する方法については、*特定のアラートの有効化*, page 43, を参照してください。

   テスト トラップの送信に問題がある場合は、コミュニティー名、IP アドレス、およびポートを確認し、ネットワークがアプライアンス C インターフェースと SNMP マネージャの間の通信を許可していることを確認してください。
4. SNMP v3 では、SNMP マネージャの**エンジン ID** と **IP アドレス**、および SNMP 通信に使用する**ポート**を入力します。
5. ネットワークで使用する**セキュリティ レベル** (「None」、「Authentication only」、または「Authentication and Encryption」) を選択し、SNMP 通信に関連付ける**ユーザー名**を選択します。
6. 認証を含むセキュリティ レベルを選択した場合、選択したユーザー名に対応する**パスワード**も入力および確認し、次に**認証プロトコル** (MD5 または SHA) を選択します。
7. 認証と暗号化を選択した場合、**暗号プロトコル** (DES または AES) を選択し、次に暗号化に使用する**プライバシー パスワード**を入力します。

8. 設定を確認するには、**[Send Test Trap（テスト トラップを送信する）]** をクリックします。テスト トラップの送信が成功した場合、**[OK]** をクリックして変更を適用します。どちらのイベントでトラップを送信するかを設定する方法については、*特定のアラートの有効化*, page 43, を参照してください。

   テスト トラップの送信に問題がある場合は、コミュニティー名、IP アドレス、およびポートを確認し、ネットワークがアプライアンスと SNMP マネージャの間の通信を許可していることを確認してください。

特定のアラートの有効化

アプライアンスは次の各モジュールについてトラップを送信できます：Appliance Controller、Websense Content、Gateway、Websense Web Security、Network Agent、Email Security Gateway。**「Configuration」> 「Alerting」** ページの [Alerts（アラート）] タブは、有効化したモジュールにのみ関連するアラートをリストします。

各モジュールのテーブルは、下記の項目をリストします。

- アラートをトリガーするハードウェアまたはソフトウェア **イベント**（例、ネットワーク インターフェース リンクの停止または起動、Websense サービスの停止）。
- これはアラート条件を定義する **しきい値**（もしあれば）（例、CPU 使用率が 90% を超える、空きディスク スペースがディスク サイズ全体の 10% 未満になる）。
- アラートの**タイプ**（システム リソースか稼働中のイベントか）。
- イベントが発生したとき、またはしきい値に達したときに SNMP トラップを送信するかどうか。

モジュールのすべてのアラートを有効化するには、テーブル ヘッダーの **SNMP** の隣のチェック ボックスを選択します。カラム内のすべてのチェック ボックスが選択されます。

そうでない場合は、イベント名の隣のチェックボックスをオンにして、そのイベントに対する SNMP アラートを有効にします。イベントのアラートを無効化するには、対応するチェック ボックスをクリアします。

時間ベースのしきい値：設定可能なしきい値があるイベントの大部分には、設定可能な時間（分単位で指定）を基準とするしきい値もあります。時間を基準とするしきい値が設定されていて、両方のしきい値を超えたときにアラートが送信されます。時間を基準にしたしきい値を有効化するには、ページ上部の **[Enable time-based thresholds（時間を基準とするしきい値を有効にする）]** チェック ボックスを選択します。時間を基準とするしきい値は、設定可能なすべてのイベントに対して有効化されます。

イベントによってクリアされるアラート：イベント条件によるアラートを生成するほかに、条件がしきい値以下に戻ったときに送信するアラートを構成することもできます。これらのアラートを**イベントによってクリアされるアラート**と言います。イベントによってクリアされるアラートを有効化するに

は、ページ上部の [Generate event- cleared alerts (**イベントによってクリアにされるアラートを生成する**)] チェック ボックスを選択します。

下記のイベントは、イベントによってクリアされるアラートを生成しません。

- ホスト名の変更
- IP アドレスの変更
- スケジュール設定したバックアップの失敗
- SNMP 認証の失敗

アラートの設定を完了したとき、[OK] をクリックして、変更を適用します。

Web Security コンポーネントの設定

「Configuration」> 「Web Security Components (Web Security のコンポーネント)」 ページを使って、アプライアンス上でどの Web Security コンポーネントがアクティブであるか、および、アプライアンスが Web Security グローバル設定およびフィルタリング ポリシー情報をどこから取得するかを指定します。また TRITON – Web Security の場所も指定します。

1. [Policy Source] の下で、このアプライアンスにどの Web Security 設定を使用するかを選択します。**「Full」 ポリシー ソース** (デフォルト。*ポリシーソースとは*を参照)、**「ユーザー ディレクトリおよびフィルタリング」**、または **「フィルタリングのみ」** (*アプライアンスがポリシー ソースでない場合は？*を参照)。
   - このアプライアンスが「Full」ポリシー ソース アプライアンスである場合、Policy Broker および Policy Server の両方の機能を実行します。「Full」ポリシー ソース アプライアンスはネットワーク内に 1 つだけ存在できます。
   - このアプライアンスが「ユーザー ディレクトリおよびフィルタリング」アプライアンスである場合、Policy Server の機能も実行します。Policy Broker アプライアンスまたはサーバーの IP アドレスを入力します。「Full」ポリシー ソース以外のモードを選択した場合、**ポリシー ソース IP アドレス**を入力します。これには、他のアプライアンスの IP アドレス、または Websense Policy Broker がインストールされているサーバーの IP アドレスを使用できます。
   - このアプライアンスが「フィルタリングのみ」アプライアンスである場合、Policy Server の IP アドレスを入力します。Policy Broker コンピュータの IP アドレスである必要はありません。
2. [OK] をクリックし、変更を保存して適用します。

3. これが 「Full」ポリシー サーバーとして実行している Websense Web Security または Websense Web Security Gateway 専用アプライアンスである場合、**[TRITON – Web Security]** で、アプライアンス**上**にインストールされている TRITON インスタンスを使用するか、またはアプライアンス**外**のインスタンスを使用するかを指定します。

   ご注意
   アプライアンスの以前のバージョンからアップグレードするとき、以前の設定は保存されます。アプライアンス外の管理コンソールの場所が確定していない場合、システムは、デフォルトで、ポリシー ソース アプライアンス上の TRITON – Web Security を使用します。

   - Websense Data Security または Email Security Gateway を Websense Web Security Gateway と共に使用している場合、TRITON Unified Security Center を Windows Server 2008 R2 64 ビット コンピュータ上にインストールする必要があります。
   - 一般的に、TRITON – Web Security のアプライアンス上へのインストールは、評価用および小規模な配備を想定しています。ほとんどの製造サイトでは、mywebsense.com から TRITON インストーラをダウンロードし、別の Windows サーバーに TRITON コンソールをインストールすることを推奨します。

4. アプライアンス外の TRITON – Web Security インスタンスの使用からアプライアンス上のインスタンスの使用に移行する場合、元の TRITON コンソールのバックアップを作成していることを確認してください。次に、**[Import Configuration (設定をインポート)]** を展開し、バックアップ ファイルの場所を参照します。

   これによって多くの既存の設定およびポリシー情報をアプライアンスに移動することができ、設定を再作成する必要がなくなります。

   移行の際に一部の設定が保存されないことがありますから、必ず新しい TRITON コンソール内の設定を確認してください。

5. **[OK]** をクリックし、変更を保存して適用します。

ポリシーソースとは

すべての Websense Web Security の配備には、1 つの**ポリシー ソース**を含める必要があります。これは、次の 2 つのコンポーネントをホストするアプライアンスまたは他のサーバーです : Websense Policy Broker および Websense Policy Database。他のすべての Websense アプライアンスまたは他のサーバーは、このコンピュータにアクセスし、そこから定期的アップデートを受け取ります。このアプライアンス (または他のサーバー) を**ポリシー ソース**と言います。

- Websense Web Security Gateway 専用アプライアンスをポリシー ソースとして設定すると、すべての利用可能な Websense Web Security のコンポーネント（下記を含む）がそのアプライアンスで実行します。
  - Filtering Service
  - Policy Database
  - Policy Broker
  - Policy Server
  - User Service
  - Directory Agent（ハイブリッド サービスに必須）
  - State Server（オプション）
  - Mux Service（アプライアンスが「フィルタリングのみ」のときは使用できません）
  - 使用状況モニタ［しようじょうきょうもにた］
  - Control Service
  - TRITON – Web Security（オプション）
    - Reports Information Service
    - Investigative Reports Scheduler
    - Manager Web Server
    - Reporting Web Server
    - Central Access
    - Unified Security Center
    - Settings Database
  - Websense Content Gateway モジュール
  - Network Agent モジュール（オプション）

  Log Server のような Windows 専用サービスや透過的識別エージェントのようなオプション サービスは、依然として他のコンピュータ上で実行します。
- ポリシー ソース アプライアンスが **Web および Email Security** モードで実行するとき（Websense Web Security Gateway および Email Security Gateway をホストする）、TRITON サービスはデフォルトでは無効化されます。
- アプライアンス以外のポリシー ソースは、**Policy Broker** をホストするサーバーです。Policy Database は、自動的に作成され、Policy Broker コンピュータで実行します。このコンピュータは、一般的には、Policy Server インスタンスも含み、またその他の Websense ソフトウェア コンポーネントを含むことがあります。

Policy Database は、ネットワーク内のすべてのアプライアンスおよびすべてのドメインのすべてのフィルタリング ポリシー（クライアント定義、フィルター、フィルター コンポーネントを含む）を保持します。また、配備全体に適用するグローバル設定情報も保持します。

「Full」ポリシー ソース コンピュータでないアプライアンスを構成する場合、それをポリシー ソースに関連付ける必要があります。

アプライアンスがポリシー ソースでない場合は？

ポリシー ソースとして使用していない Websense V シリーズ アプライアンスは、**「ユーザー ディレクトリーおよびフィルタリング」**または **「フィルタリングのみ」**のどちらかを実行するように指定できます。

- **「ユーザー ディレクトリおよびフィルタリング」**アプライアンスは、ポリシー ソース コンピュータの軽量バージョンです。このアプライアンスは下記のコンポーネントを実行します。
  - Policy Server
  - User Service
  - 使用状況モニタ [しようじょうきょうもにた]
  - Filtering Service
  - Control Service
  - Directory Agent
  - Websense Content Gateway モジュール
  - Network Agent モジュール (オプション)

  リモート アプライアンス上に User Service および Policy Server があれば、ローカル ネットワーク ユーザー名を取得できます。User Service と Policy Server の両方のコンポーネントが同じアプライアンス上で実行しますから、その間の遅延がなくなります。

  ポリシーを変更すると、その変更が即座にポリシー ソース アプライアンスに反映されます。変更は 30 秒以内に「ユーザー ディレクトリおよびフィルタリング」アプライアンスにプッシュされます。

  これらのアプライアンスとポリシー ソース コンピュータとの接続が中断された場合でも、これらのアプリケーションは最大 14 日間、フィルタリングを継続できます。したがってネットワーク接続が不良である、または失われた場合でも、フィルタリングは想定通りに続行します。

  「ユーザー ディレクトリおよびフィルタリング」アプライアンスは、更新について「Full」ポリシー ソースに照会するように設定されます。
- **「フィルタリングのみ」**アプライアンスは、Policy Server を実行しません。このアプライアンスは下記のコンポーネントのみ実行します。
  - Filtering Service
  - Control Service
  - Websense Content Gateway モジュール
  - Network Agent モジュール (オプション)

  「フィルタリングのみ」アプライアンスは、Policy Server に照会するように設定されます。アプライアンスがポリシー ソースの近くにあり、同じネットワーク上にあるときに最も適切に機能します 。

  これらのアプライアンスは、常に最新情報を反映するため、およびフィルタリングを継続するために、中央管理されたポリシーに継続的に接続していることを必要とします。ポリシー サーバーへの接続が何らかの理由で利用できなくなった場合、「フィルタリングのみ」アプライアンスは最大 3 時間までフィルタリングを継続できます。

ポリシー サーバー コンピュータが WAN 接続されているリモートネットワーク上にある場合、ローカル ユーザーのユーザー名と IP アドレスのマッピングを取得するのが困難である場合があります。

V シリーズ アプライアンス対応のユーザー ディレクトリ

組織がユーザー ID または認証に依存している場合、Websense User Service を実行している各アプライアンスをユーザー ディレクトリと通信するように設定する必要があります。複数のアプライアンスが同じユーザー ディレクトリと通信するか、または異なるユーザー ディレクトリと通信するように設定できます。

ハイブリッド設定の準備

Web Security Gateway Anywhere 環境では、一部のユーザーがハイブリッド (SaaS) サービスによってフィルタリングされることがあります。そのような場合、ユーザー、グループ、およびドメイン (OU) ベースのフィルタリングを有効化するためには、アプライアンス上に **Directory Agent** という相互運用性コンポーネントが必要です。

Directory Agent は、下記のコンポーネントと通信できる必要があります。

- サポートされている LDAP ベースのディレクトリ サービス :
  - Windows Active Directory (Mixed Mode)
  - Windows ActiveDirectory (Native Mode ョ)
  - Oracle (Sun Java) System Directory
  - Novell eDirectory
- Websense **Sync Service**

配備後に、TRITON – Web Security を使用して User Service および Directory Agent を設定します。

- User Service の設定は、「Settings (設定)」 > 「General (一般)」 > 「Directory Services (ディレクトリ サービス)」 ページで行います。
- Directory Agent の設定は、「Settings」 > 「Hybrid Configuration (ハイブリッド設定)」 > 「Shared User Data (共有ユーザー データ)」 ページで行います。
  - Directory Agent の複数のインスタンスを実行することができます。
  - 各 Directory Agent は、一意な、重複しない root コンテクストを使用する必要があります。
  - 各 Directory Agent インスタンスを異なる Policy Server に関連付ける必要があります。
  - すべての Directory Agent インスタンスは 1 つの Sync Service に接続する必要があります (1 つの配備には 1 つの Sync Service インスタンスのみを含めることができます)。

- すべての追加的な Directory Agent インスタンス（「ユーザー ディレクトリおよびフィルタリング」および「フィルタリングのみ」アプライアンス上で実行している Directory Agent）に対して Sync Service 接続を手動で設定する必要があります。Directory Agent インスタンスに対して Sync Service と同じ Policy Server に接続する通信が自動的に設定されます。詳細については、TRITON – Web Security Help を参照してください。

Directory Agent が User Service とは異なる root コンテクストを使用し、そのディレクトリ データを User Service とは異なる方法で処理するように設定できます。また、Windows Active Directory では User Service が複数のグローバル カタログ サーバーと通信するように設定されている場合、Directory Agent はそれらのすべてと通信できます。

冗長性

インターネット使用状況フィルタリングは、複数の Websense ソフトウェア コンポーネント間のやりとりを必要とします。

- ユーザーによるインターネット アクセスの要求は、Content Gateway によってプロキシ処理されます。
- また、ユーザーによるインターネット アクセスの要求は、Network Agent によってモニタされます。
- 要求は Websense Filtering Service に送信され、そこで処理されます。
- Filtering Service は、Policy Server および Policy Broker と通信し、要求に応じて適切なポリシーを適用します。

一部のネットワークでは、追加のコンピュータを使用して Content Gateway、Filtering Service、Network Agent、または他のコンポーネントの追加のインスタンスを配備できます。たとえば、大規模な、セグメント化されたネットワークでは、各セグメントについて別々の Network Agent が必要になる場合があります。また、組織のネットワークの外側にあるラップトップおよび他のコンピュータのフィルタリングを可能にするために、Remote Filtering Server を別のコンピュータに配備することができます。

コンポーネントの分散オプションについては、Websense Deployment and Installation Center にお問い合わせください。より複雑な配備を計画する場合は、最寄りの Websense セールス エンジニアまたは許可された Websense 再販売業者にお問い合わせください。

3 管理

Websense, Inc. では、製品の更新のダウンロード、パッチおよびホットフックスの取得、カスタマ フォーラムへのアクセス、製品ニュースの閲覧、および Websense ソフトウェアおよびアプライアンスに関する他のテクニカル サポート リソースへのアクセスのためにご利用いただけるカスタマ ポータルを提供しており、mywebsense.com からアクセスできます。

最良の方法として、最初にアプライアンスをセットアップするときに MyWebsense アカウントを作成しておくと、次のことが可能になります。

- アプライアンスが製造されて以降に発表されたすべてのパッチを即座に適用する
- サポートまたは更新が必要なときにいつでもアクセスできる。

管理のオプション

管理ページから下記の作業を実行できます。

- ソフトウェア パッチをインストールする（*パッチ管理* を参照）。
- ソフトウェア ホットフィックスをインストールする（*ホットフィックス管理* を参照）。
- アプライアンスの設定、Web Security モジュール、および Email Security モジュールのバックアップを作成および復元する（*Using the backup utility（バックアップ ユーティリティの使用）* を参照）。
- すべてのアクティブ モジュールのシステム ログにアクセスする（*ログ* を参照）。
- ブロック ページをカスタマイズし、アプライアンスのコマンドライン インターフェースへのリモート アクセスを有効化し、コマンドライン ユーティリティを起動する（*ツールボックス* を参照）。
- Appliance Manager または Content Gateway Manager の **admin** パスワードを変更する（*アカウント管理* を参照）。

パッチ管理

V シリーズ アプライアンスは、使いやすいパッチ管理機能によって常に最新状態に維持されます。

「Administration (管理)」> 「Patches / Hotfixes (パッチ / ホットフィックス)」> 「Patches (パッチ)」ページに進み、パッチをチェックし、ダウンロードし、インストールします。

- アプライアンスは、1 日に 1 回、自動的に新しいパッチをチェックします。チェックの時刻はランダムに設定されており、変更できず、アプライアンスによって異なります。
- 手動で新しいパッチをチェックするには、**[Check for Patches (パッチをチェック)]** ボタンを使用します。
- 新しいパッチがあるときは、**[Available patches (利用可能なパッチ)]** テーブルにパッチのバージョン番号、説明、ステータスが 表示され、**「Status (ステータス)」> 「General (一般)」**ページにアラートが表示されます。
- パッチをダウンロードした後、それをネットワーク上の他の場所にコピーでき、そこからパッチを複数のアプライアンスに簡単にアップロードできます。
- アプライアンス管理インターフェース (C) がインターネットに直接に接続していない場合、プロキシ サーバーを設定し、それを通じてアプライアンスのパッチをチェックすることができます。
- [Patch History (パッチの履歴)] テーブルは、アプライアンスに適用されてきたパッチの履歴を表示します。

参照：

パッチ更新のオプション, 53 ページ

パッチの履歴, 55 ページ

アプライアンスのパッチに関する最良の方法

- サイトの新しいアプライアンスを最新バージョンに更新するために即座にパッチを適用する。
- ネットワーク上のすべての V シリーズ アプライアンスを同じバージョンに保つ。
- ソフトウェア パッチが利用可能になったとき、即座にそれらをインストールする。

アプライアンスのパッチ プロセス

パッチの検出は、24 時間ごとに自動的に実行される（時刻はランダムに設定されています）か、または **[Check for Patches (パッチをチェック)]** ボタンを使って手動で実行されます。

パッチのダウンロードおよびインストールは、アプライアンス管理者によって手動で開始されます。

- ネットワークのアクティビティが低レベルである時間帯に、**「Administration」>「Patches / Hotfixes」**ページを使用して各パッチをアプライアンスにダウンロードおよびインストールします。
- パッチを順番にインストールします。
- **「Patches（パッチ）」**ページに表示されるアプライアンスの現在のバージョン番号は、現在のアプライアンスのバージョンです（インストールされた最新のパッチを反映します）。
- アプライアンスにパッチを適用したときは必ず、アプライアンスの外で実行しているすべての Websense モジュール（Log Server など）が対応するレベルにアップグレードされていることを確認してください。詳細については、パッチ リリース ノートを参照してください。
- オンラインの「V-Series Compatibility Matrix （V シリーズ互換性マトリックス）」は、各アプライアンス バージョンに対応する Websense ソフトウェア モジュールの表を示しています。
- ネットワークに複数のアプライアンスをインストールできます。ただし、すべてのアプライアンスは同じバージョンの Websense ソフトウェア モジュールを実行している必要があります。Websense, Inc. は、1 つのネットワーク上の異なるアプライアンスで異なるバージョンのソフトウェアを実行することを推奨しません。そのようなシナリオではフィルタリングの結果に一貫性が保たれません。

パッチ更新のオプション

- 利用可能なパッチは、**[Available patches（利用可能なパッチ）]** テーブルにリストされます。
- 利用可能な各パッチについて、バージョン番号、説明、およびステータスが示されます。パッチのリリース ノートへのリンクも示されます。

重要
リリース ノートを読んでおくことは非常に重要です。
パッチに含まれる変更の概要のほかに、他のモジュールへの影響に関する情報やパッチを適用するために要する時間（推定値）が示されています。

下記のオプションを利用できます。

Download **（ダウンロード）**	利用可能なパッチのダウンロードを開始するには、**[ダウンロード]** をクリックします。[Status（ステータス）] フィールドの進捗バーがダウンロードの進捗を示します。 最初のダウンロードの進行中に他のパッチを選択し、ダウンロードを開始することもできます。この場合、連続的ダウンロード キューが生成されます。 パッチのダウンロードが完了すると、下記のようになります。 • **[Download（ダウンロード）]** ボタンが **[Install（インストール）]** ボタンと **[Delete（削除）]** ボタンに置き換わります（下記を参照）。 • パッチの説明の後に **[Save to network location（ネットワークの場所へ保存）]** リンクが表示されます。パッチ ファイルをネットワーク上の他の場所にコピーするとき、このリンクをクリックします。これは、複数のアプライアンスがあり、各アプライアンスに対して個別に Websense からパッチをダウンロードするのが面倒な場合に便利です。代わりに、各アプライアンスでは、単に **[Upload Patch Manually（手動でパッチをアップロード）]** 機能を使って、そのネットワーク上の場所からパッチをアップロードします。 パッチのダウンロードおよび適用を番号順に実行することを推奨します。多くの場合、これは必須条件です。
Pause **（一時停止）**	ダウンロードの進行中に、**[Pause（一時停止）]** ボタンが表示されます。ダウンロードを一時的に停止するには、**[Pause]** をクリックします。
Cancel **（キャンセル）**	ダウンロードの進行中に、**[Cancel（キャンセル）]** ボタンが表示されます。ダウンロード プロセスを終了するには、**[Cancel]** ボタンをクリックします。
Resume **（再開）**	パッチのダウンロードを一時停止したとき、**[Resume（再開）]** ボタンが表示されます。一時停止したダウンロードを続行するには、**[Resume]** をクリックします。

Install **（インストール）**	パッチのダウンロードと検証（ダウンロード プロセスの中でチェックサムが実行されます）が完了し、インストールの準備ができたとき、**[Install（インストール）]** ボタンが有効化されます。 **重要**：パッチをインストールする前に、必ずパッチのリリース ノートをお読みください。 **重要**：Network Agent が一時的に無効化されていて、それを永久的に無効化**しない**場合（そのためにはアプライアンスが再びそれを使用できるようにするための再イメージングが必要です）、パッチをインストールする前に Network Agent を再度有効化する必要があります。*パッチをインストールする前の Network Agent 再有効化*, 56 ページ を参照してください。 パッチをインストールするには、**[Install]** をクリックします。 確認を要求し、ステータスを表示する一連のページが表示されます。インストール後に再起動が必要な場合は、そのことが通知されます。再起動の後、パッチはパッチ キューから削除され、[Patch History（パッチの履歴）] テーブルにログ記録されます。 アプライアンスの新しいバージョン番号が **[Appliance version（アプライアンス バージョン）]** フィールドに反映されます。 以前のパッチがインストールされておらず、必要とされる場合、**[Status（ステータス）]** カラムに以前のパッチが必要であることを示すメッセージが表示され、それに依存するパッチの **[Install]** ボタンが無効化されます。最初に以前のパッチをインストールします。 パッチのインストールが失敗した場合、そのパッチからインストールされたファイルはすべて即座にアンインストールされ、パッチのインストールが失敗したことを示すメッセージが表示されます。インストールを再試行することができます。インストールが失敗した場合は、パッチを削除し、それを再びダウンロードし、インストールを再試行してください。
Delete **（削除）**	パッチを削除するには、**[Delete（削除）]** をクリックします。
Check for Patches **（パッチをチェック）**	手動で新しいパッチをチェックするには、**[Check for Patches（パッチをチェック）]** をクリックします。
Upload Patch Manually **（手動でパッチをアップロード）**	ネットワーク上の他の場所からパッチをアップロードするとき、**[Upload Patch Manually（手動でパッチをアップロード）]** をクリックします。これは、クラスタ内で、または複数のアプライアンスがローカル ネットワークへのアクセス権をもっている場合に、パッチを複数のアプライアンスに分配する便利で効率的な方法です。 パッチをアプライアンスからネットワーク内の他の場所にコピーする方法については、上の「**Download**」の項目を参照してください。

パッチの履歴

「**Administration**」>「**Patches / Hotfixes**」>「**Patches**」ページの **[Patch History（パッチの履歴）]** テーブルは、アプライアンスにインストールされているす

べてのパッチのリストを表示します。各パッチについて、下記の情報が表示されます。

- バージョン番号
- パッチのインストールの日付と時刻
- パッチのインストールの成功または失敗を確認するコメント
- パッチの詳細を示すパッチ ログ ファイルへのリンク

パッチをインストールする前の Network Agent 再有効化

Network Agent が一時的に無効化されていて、それを永久的に無効化せず、パッチをインストールする場合、下記の手順を実行します。(Network Agent を一時的および永久的に無効化する方法については、*Network Agent の無効化*, 15 ページ を参照してください。

1. 「**Patches**」ページでインストールを開始し、[**Network Agent Disable (Network Agent を無効化)**] ダイアログ ボックスが表示されており、Network Agent を永久的に無効化**しない**場合は、[**Cancel**] を選択し、ダイアログ ボックスを閉じて、「**Status**」> 「**General**」ページに進みます。[**Network Agent**] 領域で、[**Enable Module (モジュールの有効化)**] をクリックし、[**OK**] をクリックして操作を続行します。アプライアンスが自動的に再起動します。
2. 「**Patches**」ページでインストールを開始して**いない**場合、「**Status**」> 「**General**」ページに進み、[**Network Agent**] 領域で [**Enable Module**] をクリックし、[**OK**] をクリックして操作を続行します。アプライアンスが自動的に再起動します。
3. アプライアンスが再起動した後、ログオンして、「**Administration**」> 「**Patch / Hotfixes**」> 「**Patches**」ページに進み、パッチのインストールを実行します。
4. パッチのインストールが完了したとき、Network Agent を再び一時的に無効化する場合は、「**Status**」> 「**General**」ページに戻り、Network Agent を無効化します。

パッチのインストールの前に Network Agent を再有効化する (永久的に無効化しない場合) 理由は、もし Network Agent が停止していて、パッチに Network Agent への更新が含まれる場合、停止しているモジュールへの更新が行われず、その結果、将来にモジュールを再有効化したとき、システム上の他のモジュールとの互換性が失われていることがあることです。

ホットフィックス管理

関連項目：

- *ホットフィックス アプリケーション プロセス*, 58 ページ
- *ホットフィックスのインストール*, 58 ページ
- *ホットフィックスの履歴*, 60 ページ

Websense, Inc. は、必要に応じて、アプライアンス モジュールの個別の問題に対処するために、限定的な*ホットフィックス*を公開します。多くの場合、ホットフィックスについては Websense Technical Alert 電子メールで通知され、また、ユーザーが報告した具体的な問題への回答として Websense Technical Agent が特定のホットフィックスを推奨します。

Appliance Manager の **「Hotfixes」** ページでは、ホットフィックス アプリケーションの検索、インストール、アンインストール、および履歴の保持を行います。

ホットフィックスを管理するには、**「Administration」** > **「Patches / Hotfixes」** > **「Hotfixes」** ページに進みます。

- ほとんどの場合、ホットフィックスは下記のどちらかによって通知されます。
  - A Websense Technical Alert 電子メール
  - Websense Technical Support AgentAgent は、ユーザーが報告した問題に対応するために特定のホットフィックスの名前を提供します。
- ホットフィックスは、アプライアンス上で実行しているどのモジュールに関する問題にでも対応できます。
- アプライアンス上で設定されていない、または実行していないモジュールに関してはホットフィックスは推奨されません。
- 最良の方法として、Websense Technical Support Agent から指示されない限り、まだ遭遇していない問題についてのホットフィックスをインストールしないほうが賢明です。
- ホットフィックスの名前は、以下のように構成されています。*XXX*-#.#.#-###:

  例：WCG-7.7.4-001
- Hotfix 機能は、アプライアンス上のモジュールのバージョンに対応していないホットフィックスをインストールしません。
- ホットフィックスに他のホットフィックス（1 つまたは複数）との依存関係がある場合、ホットフィックス機能は、依存対象がインストールされるまでそのホットフィックスのインストールを許可しません。

ホットフィックス アプリケーション プロセス

下記はです。詳細については、*ホットフィックスのインストール* を参照してください。

1. **[Hotfix Installation (ホットフィックス インストール)]** 領域で、ホットフィックスの名前を入力し、**[Find (検索)]** をクリックします。ホットフィックスが見つからない場合、Websense からの通知をもう一度読んで、名前が正しく入力されているか調べます。繰り返し試みても名前が見つからない場合、Websense テクニカル サポートにお問い合わせください。
2. ホットフィックスが見つかると、ホットフィックスの説明と他の関連情報を含むポップアップが表示されます。説明を読んで、求めていたホットフィックスであると思われる場合、**[Download]** をクリックして、ホットフィックスをアプライアンスにダウンロードします。そうでない場合は、**[Cancel]** をクリックします。
3. ホットフィックスをダウンロードした後、**[Downloaded hotfixes (ダウンロード済みのホットフィックス)]** テーブルに説明とステータスが表示されます。ホットフィックスに依存関係がなく、すぐにインストールできることを確認してください。ホットフィックスが他のホットフィックスに従属する場合、従属対象のホットフィックスを最初にダウンロードおよびインストールする必要があります。
4. **[Install]** をクリックし、ホットフィックスをインストールします。

複数のアプライアンスがあり、何度も Websense.com からホットフィックスをダウンロードするのが面倒な場合、**[Save to network location]** リンクを使用して、ダウンロード済みのホットフィックスをネットワーク上の都合の良い場所にコピーし、各アプライアンスで **[Upload Hotfix Manually]** ボタンを使用してファイルをアプライアンスにアップロードすることができます。

詳細については、下記を参照してください。

ホットフィックスのインストール, 58 ページ

ホットフィックスの履歴, 60 ページ

ホットフィックスのインストール

関連項目：

- *ホットフィックス管理*, 57 ページ
- *ホットフィックス アプリケーション プロセス*, 58 ページ
- *ホットフィックスの履歴*, 60 ページ

[Hotfix Installation (ホットフィックスのインストール)] 領域では、下記の操作を実行します。

- ホットフィックスを検索し、ダウンロードする

- ホットフィックスをインストールする
- インストールしていないホットフィックスを削除する
- ホットフィックスをネットワーク上の場所にコピーする
- ネットワーク上の場所からホットフィックスをアップロードする

下記のオプションを利用できます。

Hotfix ID（ホットフィックス ID）入力フィールド	Websense.com ホットフィックス リポジトリ内の検索対象のホットフィックスの名前を正確に指定します。先行する 0 および末尾の 0 も入力する必要があります。 形式は下記の通りです。XXX-#.#.#-### 例：WCG-7.7.0-001
[Find（検索）] ボタン	ホットフィックスの名前を入力した後、**[Find]** をクリックして、Appliance Manager に Websense.com からホットフィックスを検索するよう指示します。ホットフィックスが見つかった場合、**[Hotfix Details（ホットフィックスの詳細）]** ポップアップ ダイアログ ボックスにホットフィックスの説明と、[Download] および [Cancel] ボタンが表示されます。
Downloaded hotfixes テーブル	このテーブルは、アプライアンスにダウンロードされていて、まだインストールされていないホットフィックスの完全なリストを保持します。インストール済みホットフィックスの記録は、「Hotfix History（ホットフィックスの履歴）」セクションに保持されます。
Hotfix ID	ホットフィックス の ID。
説明	ホットフィックスの詳細な説明。通常、以下の情報が含まれます。 • 名前 • ホットフィックスが対処する問題の簡単な説明 • ホットフィックスを適用できるモジュール • 相対的重大度（高、中、低） • リリース日付 • 公式**リリース ノート**（Websense.com にホストされています）へのリンク • ホットフィックスをネットワーク上の場所に保存するためのダイアログを開く **[Save to network location]** リンク
Status	ホットフィックスがすぐにインストールできるか、または最初に依存関係にある他のホットフィックスをインストールする必要があるかを示します。
Action（アクション）	インストールを開始するための **[Install（インストール）]** ボタンと、インストールの前にアプライアンスからホットフィックスを削除するための **[Delete（削除）]** ボタンが含まれます。ホットフィックスをアンインストールおよび削除するには、[Hotfix History] 領域からアクセスできるアンインストール機能を使用します。
Upload Hotfix Manually	このボタンを使用して、ホットフィックスをアプライアンスからネットワーク上の場所にアップロードします。

ホットフィックスの履歴

関連項目：

- *ホットフィックス管理*, 57 ページ
- *ホットフィックス アプリケーション プロセス*, 58 ページ
- *ホットフィックスのインストール*, 58 ページ

「Hotfix History」セクションでは、下記の操作を実行します。

- アプライアンスの現在のバージョンを表示する
- インストール済みのホットフィックスの記録を表示する
- ホットフィックスをアンインストールする
- アンインストールされたホットフィックスの記録を表示する

下記のオプションを利用できます。

[View] ドロップダウン リスト	このドロップ ダウンリストから、**[Installed hotfixes]** を選択すると、インストール済みホットフィックスと、インストールを試みたが失敗したホットフィックスのリストを含むテーブルが表示されます。**[Uninstalled hotfixes]** を選択すると、アンインストールされた、またはアンインストールを試みたが失敗したホットフィックスのリストを含むテーブルが表示されます。
[View] ドロップダウンリストから **[Installed hotfixes]** を選択したとき	
[Hotfix ID] の横の**ラジオ ボタン**	**[Uninstall]** ボタンをオンにするにはこのラジオ ボタンを選択します。ホットフィックスに依存関係があるためにアンインストールできない場合、テーブルの下にメッセージが表示されます。
Hotfix ID	ホットフィックス の ID。
Name	ホットフィックスの名前とリリース ノートへのリンク
Module	影響を受けるアプライアンス モジュールの名前。
Date Installed（インストールした日付）	ホットフィックスをインストールした日付。
Status	インストールが成功したか失敗したかを示します。インストールが失敗した場合、インストール ログ ファイルへのリンクが表示されます。
Uninstall ボタン	選択したホットフィックスのアンインストールを開始するときこのボタンを使用します。
[View] ドロップダウンリストから **[Uninstalled hotfixes]** を選択したとき	
Hotfix ID	ホットフィックスの名前

Reason（理由）	ホットフィックスをアンインストールする理由。ホットフィックスをアンインストールした理由を忘れることがよくあります。ここで明確な説明を記録しておくことによって、将来にエラーを繰り返したり、時間を無駄にすることが少なくなります。
Date Uninstalled（アンインストールした日付）	ホットフィックスをアンインストールした日付。
Status	アンインストール操作の成功または失敗を示します。ホットフィックスのアンインストールが失敗することがあります。その 1 つの理由として、アンインストールするためには他のホットフィックス（1 つまたは複数）をアンインストールしなければならない場合があります。

パッチおよびホットフィックス プロキシの設定

アプライアンス管理インターフェース（C）がインターネットに直接に接続していない場合、プロキシ サーバーを設定し、それを通じてアプライアンスのパッチおよびホットフィックスをチェックすることができます。

Use proxy server（プロキシ サーバーを使用）	このオプションを有効化または無効化するにはチェック ボックスを選択します。
Proxy IP address and port（プロキシ IP アドレスとポート）	使用するプロキシの IP アドレスとポート番号を指定します。
User name/ password（ユーザー名 / パスワード）（オプション）	オプションとして、ユーザー名とパスワードによってプロキシ接続を認証します。
Test Connection（テスト接続）	指定したプロキシへの接続をテストするには、**[Test Connection（テスト接続）]** をクリックします。

Using the backup utility（バックアップ ユーティリティの使用）

関連項目：

- *バックアップのスケジュール設定*, 63 ページ
- *アプライアンス設定の完全バックアップ*, 65 ページ
- *モジュール設定のバックアップ*, 66 ページ
- *バックアップ ファイルの復元*, 66 ページ

「Administration」>「Backup Utility (バックアップ ユーティリティ)」ページの [Backup (バックアップ)] タブでは、設定のバックアップを開始するか、バックアップの自動更新スケジュールを設定するか、または既存のバックアップ ファイルを管理します。既存のバックアップ ファイルからアプライアンスまたはモジュール構成を復元するには、[Restore (復元)] タブをクリックし、*バックアップ ファイルの復元*, 66 ページ の説明に従ってください。

V シリーズ アプライアンス上で、下記の 2 つのタイプのバックアップを利用できます。

- **「完全なアプライアンス設定」**のバックアップでは、すべてのアプライアンス設定と、すべてのアクティブ モジュール (例、Web Security Gateway、Email Security) の設定およびポリシー情報を保存します。Websense, Inc. は、ネットワーク内の各アプライアンスの完全バックアップを定期的に実行することを推奨します。

  完全バックアップ ファイルはモジュール バックアップ ファイルよりも小さいことがあります。なぜならファイルが圧縮されるからです。

- **「モジュール設定」**のバックアップ (Web Security Configuration または Email Security Configuration) は、選択したモジュールのすべての設定情報を保存します。この情報は、選択したアプライアンスに保存されているクライアントおよびポリシーデータを含みます。

  Content Gateway のバックアップは Content Gateway Manager で実行されます。バックアップは手動で実行する必要があります。スケジュール設定機能はありません。

バックアップのタイプおよびバックアップ ステータス情報は、[Perform Backup (バックアップ実行)] リストに表示されます。バックアップを開始またはスケジュール設定するには、最初にバックアップのタイプを選択し、次に **[Run Backup Now (バックアップを直ちに実行)]** または **[Configure Backup Schedule (バックアップ スケジュールを設定)]** をクリックします (バックアップのスケジュール設定の詳細については、*バックアップのスケジュール設定*, 63 ページ を参照してください)。

最初にバックアップ機能を設定する必要があります。これは自動的には行われません。しかし、一度バックアップをスケジュール設定すれば、そのバックアップは自動的に定期的に実行され、手動での作業の必要はありません。スケジュール設定したバックアップの自動的反復を停止するには、**[Cancel Scheduled Backup (スケジュール設定したバックアップをキャンセル)]** をクリックします。

[Local Backup Files (ローカル バックアップ ファイル)] リストは、現在のアプライアンスに保存されているすべてのバックアップ ファイルのリストを表示します。表示されるバックアップ ファイルのタイプを変更するには、**[View backups for (表示するバックアップ)]** リストからバックアップのタイプを選択します。

リストの各エントリは、以下の情報を含みます。

- バックアップの日付と時刻
- バックアップ ファイルの名前

「完全なアプライアンス設定」バックアップ ファイルには、以下の情報も含まれます。

- バックアップを実行したアプライアンスのパッチ バージョン。バックアップから復元するとき、バックアップ ファイルは復元するアプライアンスと同じバージョンである必要があります。
- バックアップ ソースのホスト名。
- 各バックアップ ファイルに含まれるポリシー情報に関するコメント。
  - **Email Security モード**は、Email Security Gateway アプライアンスの完全バックアップを指定します。
  - **「Full」ポリシー ソース** (Web Security Gateway モード) または **「Web (ポリシー ソース)、および Email Security」** (Web および Email Security モード) は、バックアップがポリシー ソース アプライアンス上に生成された場合のデフォルトのコメントです。
  - **「ユーザー ディレクトリおよびフィルタリング」** (Web Security Gateway モード) または **「Web (ユーザー / フィルタリング) および Email Security」** (Web および Email Security モード) は、バックアップが Filtering Service および User Service のコンポーネントを実行するように設定されているアプライアンス上に生成された場合のデフォルトのコメントです。
  - **「フィルタリングのみ」** (Web Security Gateway モード) または **「Web (フィルタリングのみ)、および Email Security」** (Web および Email Security モード) は、バックアップが「フィルタリングのみ」アプライアンス上に生成された場合のデフォルトのコメントです。

アプライアンス上に各モジュールについて最大 20 個のアプライアンス バックアップ ファイルと 20 個のバックアップ ファイルを保存できます。21 個目のバックアップ ファイルが作成されると、最も古いファイルが自動的に削除されます。

バックアップ ファイルを他のコンピュータにダウンロードするには、ファイル名をクリックし、ファイルを保存するパスを参照します。

ローカル バックアップを手動で削除するには、[Local Backup Files (ローカル バックアップ ファイル)] リストのバックアップ ファイル名の隣のチェック ボックスをオンにして、**[Delete]** をクリックします。

バックアップのスケジュール設定

関連項目：

- *Using the backup utility (バックアップ ユーティリティの使用)*, 61 ページ
- *アプライアンス設定の完全バックアップ*, 65 ページ
- *モジュール設定のバックアップ*, 66 ページ
- *バックアップ ファイルの復元*, 66 ページ

「Backup Utility」> 「Configure Backup Schedule (バックアップ スケジュールの設定)」ページを使用して、選択したバックアップのタイプが実行される頻度および時間帯を指定し、バックアップ ファイルを保存する場所を選択します。各アプライアンスのバックアップ タイプ (「full」アプライアンス、「Web Security」または「Email Security」) ごとに別々にスケジュール設定します。

バックアップをスケジュール設定するには、下記の手順を実行します。

1. **[Backup frequency (バックアップの頻度)]** を、次の頻度から選択します : 毎日、毎週、または毎月。
   - 毎週のバックアップでは、バックアップを実行する曜日を選択します。
   - 毎月のバックアップでは、バックアップを実行する日を選択します。月の 29 日、30 日、31 日はバックアップをスケジュールできません。これらの日を含まない月があるからです。
2. バックアップ プロセスの **[Start time (開始時刻)]** を指定します。アプライアンスの負荷が大きくないと考えられる時間帯を選択するのが理想的です。

   時刻を 24 時間形式で入力します (ここで 00:00 は真夜中を指し、12:00 は正午を指します)。
3. バックアップ ファイルの **[Storage location (保管場所)]** を設定します。各バックアップ タイプについて 1 つのリモート バックアップ場所のみを設定できます。
   - ファイルをローカルに保存するには、**[Appliance (アプライアンス)]** を選択します。最大 20 個のバックアップ ファイルを保存できます。バックアップ ファイル ディレクトリの名前の変更、移動、削除はできません。

     アプライアンスに保存したバックアップ ファイルは 「Backup Utility」ページの [Local Backup files] リストに表示されます。
   - バックアップ ファイルをネットワーク内の他のコンピュータに保存するには、**[Remote machine (リモート コンピュータ)]** を選択し、次に、**[Samba file share (Samba ファイル共有)]** または **[FTP server (FTP サーバー)]** を使用するかどうかを指定し、下記の接続情報を入力します。
     a. リモート コンピュータの **IP アドレス / ホスト名**および使用する接続**ポート**。
     b. バックアップ ファイルを作成する**デフォルト ディレクトリ**。各バックアップ ファイル タイプについて異なるサブディレクトリが自動的に作成されます。

重要

複数のアプライアンスのバックアップ ファイルを同じリモート コンピュータ上に作成する場合、必ずそれぞれのアプライアンス バックアップ ファイルに別々のディレクトリを使用してください。

それによって、名前の競合のためにファイルが誤って上書きされたり削除されてしまうのを防止できます。

c. リモート コンピュータに接続するときに使用する**ユーザー名**と**パスワード**。ネットワーク ログオンを使用する場合、アカウントが常駐する **ドメイン**も指定します。

d. **[Test Connection]** をクリックして、アプライアンスがリモート コンピュータと通信し、指定した場所に書き込むことができることを確認します。

e. 指定した時間を過ぎたリモート バックアップ ファイルを自動的に削除する場合、**[Delete backup files that are older than (バックアップ ファイルの保存期間)]** チェックボックスをオンにし、リストから時間を選択します。

4. **[OK]** をクリックして変更を保存し、「Backup Utility」ページに戻ります。新しいバックアップ スケジュールが [Perform Backup (バックアップを実行)] リストに表示されます。

アプライアンス設定の完全バックアップ

「完全なアプライアンス設定」のバックアップでは、すべてのアプライアンス設定と、アプライアンス上のすべてのアクティブ モジュール (Web Security、Email Security、またはその両方) の設定およびポリシー データを保存します。複数のアプライアンスがある場合は、それぞれのアプライアンスでバックアップを実行します。バックアップ ファイルは、それを作成したアプライアンスに関するデータのみを含みます。

ご注意
ソフトウェア コンポーネントがアプライアンスの外にインストールされている場合 (Log Server、TRITON Unified Security Center など)、Websense, Inc., は、アプライアンスのバックアップを行うのとほぼ同時にこれらのコンピュータで Backup Utility を実行することを推奨します。それによってシステムを復元するとき、すべてのコンピュータ上の時刻互換性があるバックアップのセットから復元できます。

Web Security アプライアンスの完全アプライアンス設定バックアップ ファイルは、下記のバックアップを含みます。

- バックアップを実行するアプライアンスのすべての設定ファイル (Appliance Manager の設定ファイルを含む)
- Websense Content Gateway のスナップショット (すべての設定データを含む)
- Websense Web Security の下記を含むすべての構成設定：
  - Policy Database に保存されているグローバル設定情報 (選択したアプライアンス上で Policy Broker が実行している場合)
  - **config.xml** ファイルに保存されている Filtering Service や Log Server の設定などのローカル設定情報 (選択したアプライアンス上で Policy Broker が実行している場合)

- Websense コンポーネント初期化 (.ini) ファイルおよび設定 (.cfg) ファイル

Email Security アプライアンスの完全アプライアンス設定バックアップ ファイルは、下記のバックアップを含みます。

- バックアップを実行するアプライアンスのすべての設定ファイル (Appliance Manager の設定ファイルを含む)
- Websense Email Security のポリシーおよび設定データ

Web および Email Security モードで実行しているアプライアンスでは、両方の情報のセットがバックアップ ファイルに含まれます。

モジュール設定のバックアップ

モジュール設定のバックアップは、選択したモジュールのポリシー データを含むすべての設定情報を保存します。

- *「Full」ポリシー ソース* アプライアンスで実行した Web Security 設定のバックアップは、Policy Database に保存されているすべての情報を含みます。
- Email Security 設定のバックアップは、Email Security モジュールが選択したアプライアンスで有効化されている場合のみ実行できます。
- Content Gateway のバックアップ動作は、Content Gateway Manager を通じて管理されます。コンソールを開き、バックアップを開始するには、「Backup Utility」 ページの上部の [Content Gateway Manager] リンクをクリックします。

バックアップ ファイルの復元

関連項目 :

- *Using the backup utility (バックアップ ユーティリティの使用)*, 61 ページ
- *バックアップのスケジュール設定*, 63 ページ
- *アプライアンス設定の完全バックアップ*, 65 ページ
- *モジュール設定のバックアップ*, 66 ページ

復元プロセスを開始すると、アプライアンスまたはモジュールの現在の設定がすべて消去されます。アプライアンスに保存されているバックアップ ファイルは影響を受けません。完全アプライアンス設定を復元すると、復元プロセスの終了時にアプライアンスが再起動します。モジュールを復元した後、アプライアンスは再起動しません。

アプライアンスまたはモジュールを保存されている設定に復元するには、以下の手順を実行します。

1. アプライアンスの外で実行しているすべての Websense ソフトウェア コンポーネントを停止します。

   たとえば、Log Server、Sync Service、Linking Service、透過的識別エージェント、TRITON Unified Security Center に関連付けられているすべてのコンポーネント、および統合 Data Security Management Server を停止します。
2. 設定を復元するアプライアンス上で Appliance Manager を開き、**「Administration」> 「Backup Utility」** ページに進みます。
3. **[Restore (復元)]** タブをクリックし、**[Select restore mode (復元モードを選択)]** リストから復元する設定のタイプを選択します。完全アプライアンス設定を復元するとき、下記の点について注意してください。
   - 現在のアプライアンスのバージョンが、バックアップ ファイルに関連付けられているバージョンと一致している必要があります。(アプライアンスのバージョンは、**[Restore]** に表示されます)。したがって、バージョン 7..5 バックアップは、バージョン 7.5 のアプライアンスにのみ復元できます。
   - 現在のアプライアンスのポリシー ソース モード (「Full」 ポリシー ソース、「ユーザー ディレクトリおよびフィルタリング」、または「フィルタリングのみ」) が、バックアップ ファイルの作成時に設定されていたポリシー ソース モードと一致している必要があります。
   - ほとんどの場合、現在のアプライアンスのモード (「Email Security」、「Web Security」、「Web および Email Security」) がバックアップ ファイルのモードと一致している必要があります。(たとえば、「Email Security のみ」 アプライアンスを復元するためには「Email Security のみ」 アプライアンスからのバックアップを使用する必要があります)。

     1 つの例外があります。V10000 G2 アプライアンス上で「Web および Email Security」 モードで実行している場合、Web Security Gateway の完全バックアップを復元できます。
   - 現在のアプライアンスのハードウェア モデルが、バックアップされているモデルと同じである必要があります。(たとえば、モデル V10000 G2 アプライアンスの復元にはモデル V10000 G2 からのバックアップを使用する必要があります)。
   - また、バックアップを作成した元のアプライアンスをネットワーク内の他の場所で同時に実行することはできません。完全設定を復元すると、元のアプライアンスが再作成され、そのアプライアンスからの一意な ID 番号を使用します。
4. **[Run Restore Wizard (復元ウィザードを実行)]** をクリックします。復元ウィザードが開きます。
5. バックアップ ファイルが保存されている場所を指定するラジオ ボタンを選択し、**[Next]** をクリックします。
   - **This remote machine (このリモート コンピュータ):** *< ホスト名または IP アドレス >* : 指定したコンピュータ上のデフォルトの場所からファイルを取得します。デフォルトの場所は、選択したバックアップ タイプのバックアップ スケジュールで指定したパスです。

- **This appliance（このアプライアンス）**：ローカルで保存されているバックアップ ファイルを使用します。
- **Another location (browse for file)（他の場所（ファイルを参照））**：ネットワーク内のアクセス可能ないずれかのコンピュータに保存されているファイルを使用します。

6. 使用するファイルを選択または指定します。
   - デフォルトのローカルまたはリモート バックアップ ファイル保存場所を選択した場合、使用できるバックアップ ファイルのリストが表示されます。リストからエントリを選択し、**[Next]** をクリックします。
   - 他の場所を選択した場合、リモート コンピュータ上のバックアップ ファイルが保存されているパスを参照し、**[Next]** をクリックします。
7. 「Confirm（確認）」ページで詳細を確認し、**[Restore Now（直ちに復元）]** をクリックします。アプライアンスが選択した設定で復元されます。

   完全アプライアンス設定の復元を開始した場合、アプライアンスは復元プロセス中に再起動されます。
8. オフボックス コンポーネントを起動する前に、すべての TRITON コンポーネント ホストのシステム時刻が同期化されていることを確認してください。アプライアンス上で、時刻を手動で設定するか、または NTP サーバーが設定されている場合は [OK] をクリックして NTP サーバーによる更新をトリガします。
9. アプライアンスの外で実行している Websense コンポーネントを起動します。

   復元プロセスによってアプライアンス IP アドレスが変更された場合、オンボックス コンポーネントとオフボックス コンポーネントの間の通信を再確立するために、オフボックス コンポーネントを再設定または再インストールしなければならない場合があります。

ログ

Websense テクニカル サポートは、トラブルシューティングを支援するためにログ ファイルを要求することがあります。このページは、表示またはダウンロードするためにこれらのログ ファイルにアクセスできるようにします。

ご注意

Network Agent は、TRITON – Web Security でロギングを有効化している場合のみログ ファイルを生成します。.

Appliance Manager で Network Agent ログ ファイルを調べる場合、最初に TRITON – Web Security にログオンし、**「Settings」> 「Network Agent」> 「Global（グローバル）」** に進みます。次に、**[Additional Settings（追加設定）]** にスクロール ダウンし、プロトコル トラフィックのロギングを有効化して、ロギングの間隔を指定します。

ログを表示するモジュールを選択します。

- Appliance Controller
- Websense Content Gateway
- Websense Web Security
- Network Agent
- Websense Email Security Gateway

Appliance Controller のログを調べる場合、次に日付範囲を選択します。

- ドロップダウン リストを使って日付範囲を選択します。
- ログファイルの日付範囲は 1 週間単位で設定し、最大は 5 週間です。

次に、表示オプションを選択します。下記のどちらかを選択します。

- View last _ lines （最後の__行を読む）
  ポップアップ ウィンドウに表示するログ行の数を指定します。
  - 最後の 50 行
  - 最後の 100 行
  - 最後の 500 行
- Download entire log file（ログ ファイル全体をダウンロード）

[Submit（送信）] をクリックして要求したログ ファイルの収集のプロセスを開始します。

ログ ファイル全体をダウンロードする場合、**[File Download（ファイルのダウンロード）]** ダイアログ ボックスを使って保存場所に移動します。

ツールボックス

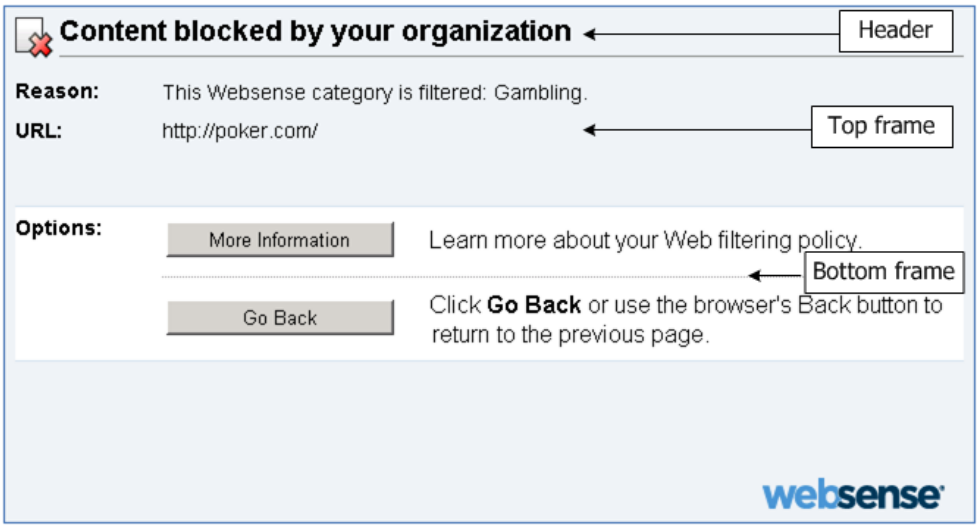
「Adminisration」>「Toolbox（ツールボックス）」 ページを使用して、カスタマイズされたブロック ページをセットアップし、基本 Linux コマンドにアクセスし、トラブルシューティングに役立てます。

- *Web Security ブロック ページ*
- *アプライアンス コマンド ライン*
- *コマンド ライン ユーティリティ*
- *テクニカル サポート ツール*

Web Security ブロック ページ

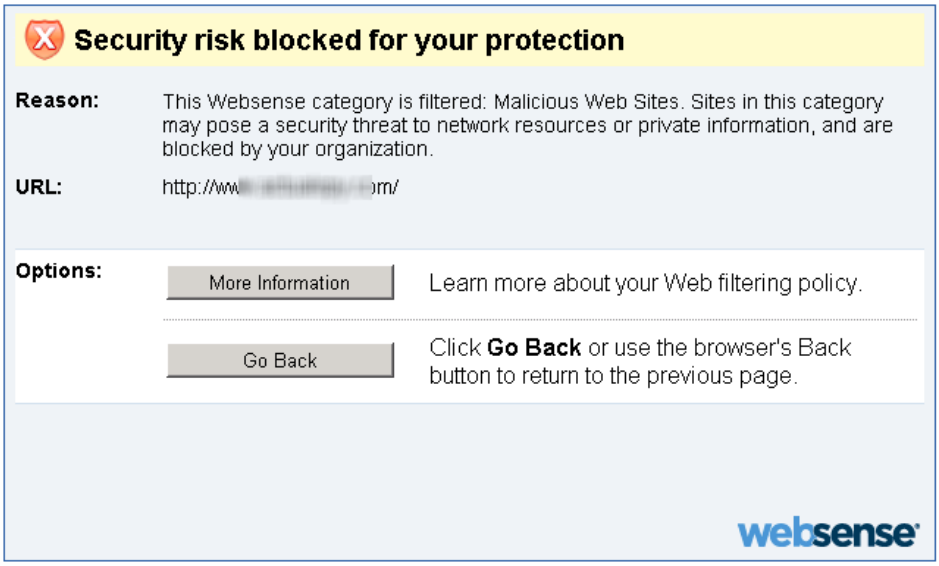
アプライアンスは、一連のデフォルト Web Security ブロック ページをホストします。これらのページは、Web 要求がブロックされたときにエンド ユーザーに表示されます。

ブロック ページは、HTML および JavaScript ファイルによって構成されています。デフォルトでは、ブロック ページには下の 3 つの主なセクションがあります。



- サイトがブロックされていることを示すヘッダー。
- トップ フレームには、要求された URL と URL のカテゴリを示すブロック メッセージが含まれます。
- ボトム フレームには、ユーザーが利用できるオプションが示されます（「前のページに戻る」、「サイトを続行する」、「割り当て時間を使ってサイトにアクセスする」、「種々の資格情報を使ってサイトへのアクセスを試みる」）。

サイトが「セキュリティ リスク」クラスのカテゴリに属しているためブロックされた場合、ブロック ページの特別なバージョンが表示されます。



Web Security ブロック ページの動作および外観を確認するには、testdatabase.websense.com のリンクを使用して、ユーザーの組織がブロックするカテゴリに含まれるテスト サイトへのアクセスを試みます。

「Administration」> 「Toolbox」 ページを使用して、次のどちらの操作を行うかを指定します。

- Websense Web Security ソフトウェアで提供されるブロック ページ（標準およびセキュリティー）を使用する（**デフォルト ブロック ページ**）。
- ブロック ページ ファイルを組織のニーズに適合するように編集する（**カスタム ブロック ページ**）。

ブロック ページのカスタマイズ

[Custom block page（カスタム ブロック ページ）] を選択したとき、デフォルト ブロック ページ ファイルのコピーがアプライアンス上の編集可能なディレクトリの中に作成されます。デフォルト ブロック ページ ファイルを移動または削除することはできません。したがって、いつでもデフォルトに戻ることができます。

カスタム ブロック ページのオプションを選択した後、下記の手順を実行します。

1. 変更するファイルを選択し、**[Download File(s)（ファイルをダウンロード）]** をクリックします。下記のファイルが利用可能です。

ファイル名	内容
block.html	ブロック メッセージのトップ フレームのテキストを含みます。このテキストは、アクセスが制限されていることを説明し、要求されたサイトをリストし、サイトが制限されている理由を示します。
blockFrame.html	ブロックされているカテゴリに含まれるサイトのテキストとボタン（[Go Back（戻る）] オプション）。
blockStyle.css	ほとんどのブロック ページのスタイルが含まれているカスケード表示形式のスタイル シート
continueFrame.html	**[Confirm（確認）]** アクションが適用されるカテゴリに含まれるサイトのテキストとボタン。
master.html	ブロック ページの情報フレームを作成し、下記のいずれかのファイルを使ってボトム フレームに適切なオプションを表示します。
messagefile.txt	ブロック ページで使用するテキスト文字列を含みます。
moreInfo.html	ユーザーがブロック・ページの **[More information（詳細情報）]** リンクをクリックしたときに表示されるページのコンテンツ。

ファイル名	内容
webDLPPolicyViolation.html	Websense Data Security コンポーネントがコンテンツの Web への送信または Web からのダウンロードをブロックするときのブロック ページ コンテンツを提供します。
quotaFrame.html	**[Quota（割り当て）]** アクションが適用されるカテゴリに含まれるサイトのテキストとボタン。
security.js	セキュリティ ブロック ページの作成に使用する JavaScript ファイル。

- 1 つのファイルを選択した場合は、そのファイルのデフォルトの使用目的、最後の変更日付、およびサイズなどの詳細情報が表示されます。
- 複数のファイルをダウンロードする場合は、ファイルは 1 つの ZIP ファイルに入れられます。

2. ローカルで変更を行います。

> **重要**
> デフォルト ファイル名を変更しては**いけません**。

- Websense ロゴを他のイメージに置換する方法については、*ブロック ページ ロゴの変更* を参照してください。
- ブロック メッセージに表示する情報が与えられているスペースより長い場合は *メッセージ フレームのサイズの変更* を参照してください。
- 元のデフォルトのブロック ページ ファイルのセットからやり直す場合は、*最初からやり直す* を参照してください。
- ブロック ページのカスタマイズに関するその他の情報については、TRITON – Web Security Help の「Block Pages」の項を参照してください。

3. **[Upload File(s)（ファイルをアップロード）]** をクリックして変更済みのファイルおよびそれをサポートするグラフィック ファイルをアプライアンス上に配置します。
   - 編集済みのファイルは、カスタム グラフィック ファイル（ロゴなど）を参照できます。カスタム グラフィックを使用する場合、必ずこれらの追加のグラフィック ファイルを編集可能なディレクトリにアップロードしてください。
   - 6 個以上のファイルをアップロードする場合、アップロードする最初の 5 つのファイルを選択したあと、**[Add More Files（さらにファイルを追加）]** をクリックます。一度に最大 10 個のファイルをアップロードできます。
4. **[Apply Changes（変更を適用）]** をクリックします。それによって Filtering Service が再起動します。
5. カスタマイズしたブロック ページをテストするには、testdatabase.websense.com に進み、組織のポリシーによってブロックされているカテゴリに含まれるテスト サイトへのアクセスを試みます。

6. 調整が必要な場合は ステップ 2 に戻ります。

ブロック ページ ロゴの変更

master.html ファイルは、ブロック ページ上に Websense ロゴを表示するために使用する HTML コードを含みます。御社の組織ロゴを代わりに表示するには、次の手順に従います :

1. **master.html** ファイルを一時ディレクトリにダウンロードします。
2. 御社の組織ロゴを入手を実行して、このファイルを同じ場所にコピーしてください。
3. メモ帳や vi などのテキスト エディタ (HTML エディタでない) で **master.html** を開き、下記の行を編集して、Websense ロゴを組織のロゴのイメージ名に置換します。

   ```
   <img title="Websense" src="/Images/wslogo_block_page.png"
   ...>
   ```

   - **title** パラメータの値を組織の名前を反映するように置換します。
   - イメージ ファイルが **Custom** フォルダ (Images フォルダではない) に置かれるようにパスを変更します。
   - **wslogo_block_page.png** を御社の組織ロゴのファイル名に置き換えてください。

     変更後の行は下記のようになります。

     ```
     <img title="ABC_Corporation" src="/en/Custom/
     myimage.png" ...>
     ```

     パラメータおよびフォルダ名は大文字と小文字を区別します。
4. ファイルを保存して、閉じます。
5. イメージ ファイル (組織のロゴを含む) と **master.html** の編集済みのコピーの両方を V シリーズ アプライアンスにコピーして、**[Apply Changes (変更を適用)]** をクリックします。

メッセージ フレームのサイズの変更

ブロック メッセージに表示する情報の内容によっては、ブロック メッセージのデフォルトの長さおよびトップ フレームの高さが適当でない場合があります。これらのサイズ パラメータを変更するには、下記の手順を実行します。

1. **master.html** ファイルをダウンロードします。
2. メモ帳や vi などのテキストエディタ (TML エディタではない) でこのファイルを開きます。
3. メッセージ フレームの幅を変更するには、下記の行を編集します。

   ```
   <div style="border:1px solid #285EA6;width:600px...">
   ```

   必要に応じて、**width** パラメータの値を変更します。
4. 追加的情報を表示するためにメッセージのトップ フレームをスクロールさせるには、下記の行を編集します。

   ```
   <iframe src="$*WS_BLOCKMESSAGE_PAGE*$*WS_SESSIONID*$" ...
   ```

```
scrolling="no" style="width:100%; height: 6em;">
```

メッセージ テキストがフレームの高さを超えるときにスクロール バーを表示するようにするには、**scrolling** パメータの値を **auto** に変更します。

また、**height** パラメータの値を変更して、フレームの高さを変えることもできます。

5. ファイルを保存して、閉じます。
6. ファイルを V シリーズ アプライアンスにアップロードして、**[Apply Changes]** をクリックします。

最初からやり直す

デフォルト ブロック ページ ファイルを使って最初からやり直す必要がある場合はいつでも、[Upload] および [Download] ボタンの下の **default files** リンクをクリックします。これによってデフォルト ブロック ページ ファイルのコピーをローカル コンピュータにダウンロードできるようになります。

変更するファイルを編集し、次に編集済みファイルをアプライアンスにアップロードします。

アプライアンス コマンド ライン

アプライアンスの**「Toolbox」**ページの**「アプライアンス コマンド ライン」**セクションは、下記の機能を提供します。

- アプライアンスの**コマンド ライン インターフェース**への SSH リモート アクセスをオンおよびオフにする（同じシェルを使って **firstboot** スクリプトを実行）。SSH アクセスによって、管理者はネットワーク上でアプライアンスへの経路をもつコンピュータからアプライアンスのコマンド ライン シェルにログオンできます。
- Appliance Manager に組み込まれている **コマンド ライン ユーティリティー** へのアクセス。コマンド ライン ユーティリティは、一般的なトラブルシューティング コマンドへの便利なアクセス方法を提供します。

SSH リモート アクセス

[Remote Access（リモート アクセス）] オプションを使用して、アプライアンスのコマンド ライン インターフェースへの SSH アクセスを有効化および無効化します。

SSH アクセスが有効化されているとき、アプライアンスのコマンド ライン シェルに接続するためには下記の方法があります。

- SSH をサポートするターミナル エミュレータを使用する。
- SSH で C インターフェースの IP アドレスに接続する
- プロンプトに応じて、Appliance Manager 管理者ログオン資格情報を使用する。
- ヘルプ コマンドを実行し、利用可能なコマンドを確認する。

コマンド ライン コマンドのリストを下に示しています。Appliance Manager では *コマンド ライン ユーティリティ* に記載されている debug-util サブコマンドも利用できます。詳細は当該の項を参照してください。

admin email
debug-util controller
debug-util esg
debug-util na
debug-util view
debug-util wcg
debug-util wse
firstboot
help
history
ip address
ip dns
ip gateway
local-access
module disable
module enable
module restart
module start
module stop
password-logon disable
password-logon enable
patch delete
patch list
policy-source
quit
reload
remote-access disable
remote-access enable
reset password
show cpu
show disk-io
show disk-space
show interface c
show memory
show module

show module service
show password-logon
show patch
show patch history
show platform
show policy-source
show remote-access
show remote-access history
show security-mode
show smtp server
show ssh
shutdown
smtp server
ssh disable
ssh enable

コマンド ライン ユーティリティ

[Command Line Utility (コマンド ライン ユーティリティ)] は、トラブルシューティング、デバッグ、およびユーティリティ コマンドを実行するために使用します。実行の結果は、そのページの **「Console output (コンソール アウトプット)」** セクションに表示されます。最後に実行したコマンドの出力ファイルをダウンロードできます。

[Launch Utility (ユーティリティを起動)] をクリックし、コマンド ユーティリティを開きます。

[Module (モジュール)] ドロップ ダウン リストには、アプライアンスにインストールされている各モジュールのエントリがあります。使用するモジュールを選択します。

- Appliance Controller
- Websense Content Gateway
- Websense Web Security
- Network Agent
- Websense Email Security Gateway

[Command] ドロップダウン リストから実行するコマンドを選択し、下記のように適切なパラメータを入力し、必要に応じて [Run] および [Stop] ボタンを使用します。

コマンド	説明	パラメータ
arp	選択したモジュールのカーネル ARP テーブルを表示します。	なし。
cache-user-names	Websense Web Security モジュールにのみ適用します。 Content Gateway によって IP アドレスから解決されたユーザー名のキャッシングをオンにする、オフにする、またはそのステータスをクエリーするために使用します。キャッシングされたエントリは 10 分間有効です。	[Action]: ユーザー名のキャッシングをオンにするには **enable** と入力します。 ユーザー名のキャッシングをオフにするには **disable** と入力します。 ユーザー名のキャッシングのステータスを表示するには、**status** と入力します。
content-line -r	Websense Content Gateway モジュールにのみ適用します。 Content Gateway の records.config ファイルの設定変数の現在の値を表示するために使用します。	[Variable Name] : 値を取得する設定変数の名前を入力します。 **例** : `proxy.config.vmap.enabled` この変数は、0 または 1 を返します。 0 は、仮想 IP マネージャが無効化されていることを示します。1 は、それが有効化されていることを示します。 有効な設定変数の完全なリストを参照するには、**Websense Content Gateway variables** リンクをクリックし、records.config トピックに移動します [このセッションの前の部分でプロキシ コンソールにログオンしていなかった場合、資格情報を求められることがあります]
content-line -s	Websense Content Gateway モジュールにのみ適用します。 Use it to set the value of a configuration variable in Content Gateway?s records.config file. このコマンドを使用すると、プロキシを再起動することなしに Content Gateway 変数への変更を行うことができます。変更を有効にするには、`content_line -x`（下記）を実行します。	[Variable Name] : 変更する変数の名前を入力します。 [Value]: 変数に供給する値を入力します。 **例**: 変数名 **proxy.config.arm.enabled** と値 "1" または "0" を入力します。 これは透過的プロキシ キャッシングのために使用する ARM、IP スプーフィング、および ARM セキュリティを有効または無効にします。 有効な設定変数の完全なリストを参照するには、**records.config** リンクをクリックします [このセッションの前の部分でプロキシ コンソールにログ オンしていなかった場合、資格情報を求められることがあります]

コマンド	説明	パラメータ
content-line -x	Websense Content Gateway モジュールにのみ適用します。 Content Gateway の records.config ファイルのすべての設定変数の値を読み出し、適用するために使用します。 content_line -s を使用してファイル records.config のいずれかの変数の設定を変更した場合、このコマンドを使用して直ちに（プロキシを再起動せずに）変更を有効にできます。	なし。
copy-MasterCA	Websense Web Security モジュールにのみ適用します。 TRITON コンソールがアプライアンス上にあり、証明書認証の root 証明書への変更の後に新しいマスター証明書が作成されたとき、このコマンドを使用して新しい Master CA を Websense Web Security モジュールにコピーします。 **ご注意**:TRITON コンソールにログ オンしている場合、ログ オフされます。	なし
directory-agent-service	Websense Web Security モジュールにのみ適用します。 このコマンドは、ディレクトリ エージェント サービスを無効化および有効化します。	[Action]: ディレクトリ エージェント サービスを有効化するには enable と入力します。 ディレクトリ エージェント サービスを無効化するには disable と入力します。
esg-license-reset	Email Security Gateway モジュールにのみ適用します。 このコマンドは、Email Security Gateway のすべてのライセンス情報を消去します。このコマンドを実行した後で Email Security Gateway を使用するためにはライセンス キーを再度入力する必要があります。 **ご注意**：ネットワークにアクセスできない場合、コマンドは 30 分待って中止されます。	なし

コマンド	説明	パラメータ
ethtool	指定したネットワーク インターフェース(NIC)デバイスの現在のイーサネット カード設定を表示します。下記の設定が含まれます。 • サポートされているポート • サポートされているリンク モード • オートネゴシエーション サポート • 公告されているリンク モード • 公告されているオートネゴシエーション • 速度 • デュプレックス • ポート • PHYAD • トランシーバ • オートネゴシエーション設定 • Wake-on のサポート • Wake-on のステータス • リンクの検出 **ethtool** を使用してローカル ネットワーク接続性を確認します。たとえば、ping コマンドが失敗した場合、このコマンドを使用して、正しい IP アドレスを使用しているかどうかを判断します。	なし。
ethtool -k	選択したネットワーク インターフェース(NIC)デバイスのオフロード パラメータ(チェックサムを含む)を表示します。 これは種々の問題を調査するために使用できます。たとえば、NIC の設定は正しいが、デュプレックスの問題がある場合、デュプレックス設定を変更する必要があることがわかります。 **-k** 指定したイーサネット デバイスのチェックサム パラメータを変更します。	なし。

コマンド	説明	パラメータ
ifconfig	ネットワーク インターフェースの問題のトラブルシューティングに使用します。IP の問題を特定し、サブネットおよびネットワーク インタフェースをチェックするのに役立ちます。 指定した NIC に関する下記のようなステータス情報を表示します (下記以外のステータス情報も表示されます)。 • IP およびブロードキャスト アドレス • サブネットマスク • 受信および送信パケット数 • 受信および送信バイト数	[Interface]: 設定する NIC を入力します。有効な NIC 値の情報アイコンをクリックします。 all (すべて) を入力すると、すべてのインターフェース ステータスが表示されます。 例 : eth0 または eth1
mux-service	SIEM 統合をサポートする Multiplexer サービスを有効化または無効化します。See TRITON ? Web Security Help. 「フィルタリングのみ」アプライアンスでは Multiplexer サービスは実行しません。代わりに、ポリシー ソース コンピュータ上で実行している Multiplexer サービスを使用します。	[Action]:Multiplexer サービスを有効化するには enable と入力します。 Multiplexer サービスを無効化するには disable と入力します。
nc -uvz	指定したサーバーに User Datagram Protocol (UDP) を使ってアクセスし、ネットワーク上でのデータ読み込みおよび書き込みを試みます。 これを使ってコンポーネントの機能テストと接続性の確認を行います。 これを使って UDP ネットワークを通過するデータをチェックします。 Web ページのロードで問題が発生する場合、またはロードがブロックされる場合、このコマンドは問題の原因を判断するのに役立ちます。 リセットがプロキシによるものである場合、それがどの DOM/ モジュールによるものかを判断できます。 **-u** netcat を UDP モードで実行します。 **-v** netcat を冗長モードで実行します。 **-z** netcat をゼロ I/O モードで実行します (スキャン用)。	[Destination]: 通信相手のサーバーの IP アドレスを入力します。 [Port]: そのサーバーのポート番号を入力します。

コマンド	説明	パラメータ
nc –vz	netcat (nc) ユーティリティ。 指定したサーバーに Transmission Control Protocol これを使ってコンポーネントの機能テストと接続性の確認を行います。 **–v** netcat を冗長モードで実行します。 **–z** netcat をゼロ I/O モードで実行します（スキャン用）	[Destination]: 通信相手のサーバーの IP アドレスを入力します。 [Port]: そのサーバーのポート番号を入力します。
netstat –neatup	選択したモジュール上のオープン ソケットのリストを、「プロセス」列と共に表示します。 **–n** アクティブ TCP 接続を表示します。ただし、アドレスとポート番号は数字で表され、名前を特定する試みは行いません。 **–e** 送受信したバイトおよびパケットの数などのイーサネット統計情報を表示します。 **–a** すべてのアクティブ TCP 接続、およびコンピュータがリスンしている TCP および UDP ポートを表示します。 **–t** どのオープン ポートが TCP を使用しているかを示します。 **–u** どのオープン ポートが UDP を使用しているかを示します。 **–p** すべてのソケットの統計または状態の表示を、プロトコルに関係するものに限定します。	なし。
netstat –ng	選択したモジュールに関するマルチキャスト グループ メンバーシップ情報を表示します。 **–n** アクティブ TCP 接続を表示します。ただし、アドレスとポート番号は数字で表され、名前を特定する試みは行いません。 **–g** すべてのインターフェースのマルチキャスト グループ メンバーシップを表示します。	なし。

コマンド	説明	パラメータ
netstat – nltup	ネットワーク接続およびルーティングの問題がある場合、下記のいずれかの netstat コマンドを使用します。 **netstat –nltup** は、下記の情報を表示します。 • ネットワーク内のトラフィックの量。 • すべてのアクティブ TCP 接続、およびコンピュータがリスンしている TCP および UDP ポート。アドレスとポート番号は数字で表され、名前を特定する試みは行いません。 • 送受信したバイトおよびパケットの数などのイーサネット統計情報。 **–n** アクティブ TCP 接続および接続時に使用するポートを表示します。 (これは Filtering Service がフィルタリングを行っていない場合などに便利です。ここでモジュールが使用している接続を調べることができます。それが Filtering Service コンピュータの IP およびポートでない場合、それが問題の原因であることがわかります)。 **–l** 特定のインターフェース (eth0、eth1 など) の状態を表示します。 **–t** どのオープン ポートが TCP を使用しているかを示します。 **–u** どのオープン ポートが UDP を使用しているかを示します。 **–p** すべてのソケットの統計または状態の表示を、プロトコルに関係するものに限定します。	なし。

コマンド	説明	パラメータ
netstat –s	選択したモジュール上の各プロトコルのサマリー統計を表示します。デフォルトでは、IP、ICMP、TCP、UDP、および TCPEXT プロトコルの統計を表示します。これは下記の項目を含みます。 • IP – 各プロトコルの受信、転送、および破棄されたパケットの数。 • ICPM – 受信した、失敗した、および送信したメッセージの数。 • TCP – アクティブおよび非アクティブな接続開始の数と失敗した接続試行の数。 • UDP – 受信および送信したパケットの数。 • TCPEXT – SYN クッキー、ACK、受信した / キューに入れられたパケット、再送信、および DSACK に関する統計。 これは単なる例です。ほかにも多くの統計が表示されます。	なし。
nslookup	これは DNS 解決の問題に対して使用します。たとえば、特定の Web サイトがロードしていない場合、そのサイトに対して nslookup を実行し、その IP アドレスを表示します。 **nslookup** によって DNS サーバーに対して問い合わせを行い、特定のコンピュータの IP アドレス、ドメインの MX レコード、ドメインの DNS サーバーなどの DNS の詳細情報を見つけることができます。	[Host]:DNS 情報を調べるホストのホスト名（例、myintranet.com）または IP アドレスを入力します。 [DNS server]: アプライアンスの DNS サーバーのホスト名または IP アドレスを入力します。
ping、ping6	ホスト名または IP アドレスが存在し、選択したモジュールからの要求を受け入れること、および DNS が名前解決を実行していることを確認します。 このコマンドを使用して、他のホスト（例、Data Security Management Server、TRITON – Web Security コンピュータ）への接続性をテストし、応答時間を判定します。 IPv4 アドレスに対して **ping** を使用し、IPv6 アドレスに対して **ping6** を使用します。 **ご注意** :ping6 は Websense Web Security モジュールではサポートされていません。	[Destination]: テストするホストのホスト名（例、myintranet.com）または IP アドレスを入力します。

コマンド	説明	パラメータ
ping –I、ping6 –I	ネットワーク インターフェースがホスト名または IP アドレスと通信できること、および DNS が名前解決を実行していることを確認します。 このコマンドを使用して、アプライアンスの NIC の 1 つから他のホスト（例、Data Security Management Server、TRITON – Web Security コンピュータ）への接続性をテストします。 IPv4 アドレスに対して **ping** を使用し、IPv6 アドレスに対して **ping6** を使用します。 **ご注意** :ping6 –I は、Websense Web Security モジュールではサポートされていません。	[Interface]: テストする NIC の名前を入力します。有効な NIC 値の情報アイコンをクリックします。 **例** : eth0 [Destination]: テストするホストのホスト名または IP アドレスを入力します。
policy–broker–token	Web Security モジュールにのみ適用します。 このコマンドを使用して、このアプライアンスの Policy Broker トークンを取得します。これはリモート フィルタリングのサポートを構成するために必要です。詳細については、Websense Technical Library を参照してください。	なし。
print–bypass	このコマンドは、Websense Content Gateway モジュールにのみ適用します。 Content Gateway が透過的プロキシ キャッシング モードのとき、このコマンドを使用して、プロキシがバイパスしているソースおよび宛先 IP を確認します。 サイトが正しくロードしていない場合、このコマンドは、サイトがキャッシュからロードしているのか、サイトから直接にダウンロードしようとしているのかを調べるのに役立ちます。 プロキシのソースおよび宛先バイパス テーブル内のすべてのエントリは、出力コンソールに出力されます。 ソースおよび宛先バイパスの詳細については、Content Gateway Manager Help システムの **「Configuration Files」 > 「bypass.config」** セクションを参照してください。	なし。

コマンド	説明	パラメータ
route -A inet6 -n	選択したモジュールのカーネル IP ルーティング テーブルの IPv6 エントリの内容を数値形式で表示します。 これは複雑なネットワーク環境、たとえばプロキシ チェイニングが行われている環境で、環境が適切に設定されているかどうかを確認するのに役立ちます。	なし。
route -n	選択したモジュールのカーネル IP ルーティング テーブルの内容を数値形式で表示します。 これは複雑なネットワーク環境、たとえばプロキシ チェイニングが行われている環境で、環境が適切に設定されているかどうかを確認するのに役立ちます。	なし。
show-triton-admin-email	Web Security モジュールにのみ適用します。 アラート、パスワード リセット、および他の TRITON 管理者メッセージの送信先の電子メール アドレスを表示します。	なし。
show-triton-smtp-settings	Web Security モジュールにのみ適用します。 TRITON から通知が送信されるときに使用される SMTP サーバー情報および送信者の電子メール設定を表示します。	なし
state-server	アプライアンスが「Full」ポリシー ソース、または「ユーザー ディレクトリおよびフィルタリング」システムとして設定されているとき、Websense Web Security モジュールに適用します。 複数の Filtering Service が配備されている場合、時刻ベースのフィルタリング アクション (Quota、Confirm、Password Override、Account Override) を適切に実行するために Websense State Server が必要です。TRITON - Web Security Help の 「**Policy Server, Filtering Service, and State Server**」を参照してください。	[Action]: ステート サーバー サービスを有効化するには **enable** と入力します。 ステート サーバー サービスを無効化にするには **disable と入力します。**

コマンド	説明	パラメータ
sysctl-tcp-timestamps	Websense Content Gateway モジュールにのみ適用します。 TCP タイム スタンプの設定を表示または変更します。 TCP タイム スタンプを適切にサポートしていない特定の Web サイトでパフォーマンス上の問題が発生している場合、この設定を編集します。 オペレーティング システムは、インストール時にこのカーネル設定を設定します。 設定が変更されて、他のサイトとの間でサイト遅延が発生している場合、TCP タイム スタンプに最もよく適合しているサイトの設定をデフォルト値に戻し、問題があるサイトへのトラフィックをプロキシ経由でルーティングすることを検討します。 必ずユーザーにとって最も重要なサイトに最もよく適合している設定を選択してください。 この設定は、すべての TCP 接続に対するカーネルによるタイム スタンプの使用に影響を与えます。	[Value]: 現在のタイム スタンプの設定を無効化するには 0 を入力し、それをデフォルトに戻します。 カスタム設定を再び有効化するには、1 を入力します。 現在の設定を表示するには、view と入力します。
sysctl-tcp-window-scaling	Websense Content Gateway モジュールにのみ適用します。 TCP ウィンドウの拡大 / 縮小の設定を表示または変更します。 TCP ウインドウの拡大 / 縮小を適切にサポートしていない特定の Web サイトでパフォーマンス上の問題がある場合は、この設定を編集します。 オペレーティング システムは、インストール時にこのカーネル設定を設定します。 設定が変更されて、他のサイトとの間でサイト遅延が発生している場合、TCP ウィンドウの拡大 / 縮小設定に最もよく適合しているサイトの設定をデフォルト値に戻し、問題があるサイトへのトラフィックをプロキシ経由でルーティングすることを検討します。 必ずユーザーにとって最も重要なサイトに最もよく適合している設定を選択してください。 この設定は、すべての TCP 接続に対するカーネルによるウィンドウの拡大 / 縮小の使用に影響を与えます。	[Value]: 現在のウィンドウの拡大 / 縮小の設定を無効化するには 0 を入力し、それをデフォルトに戻します。 カスタム設定を再び有効化するには、1 を入力します。 現在の設定を表示するには、view と入力します。

コマンド	説明	パラメータ

tcpdump	Web トラフィックに問題がある場合、たとえばサイトがロードしない場合や認証の問題がある場合などに、パケット キャプチャを取得するために使用します。
	tcpdump は、指定したネットワーク インターフェースによるパケットの送 / 受信を中止し、表示します。[Expression (式)] フィールドを使用して表示するパケットを選択します。
	tcpdump からの出力は、インターフェースとの間のすべてのルーティングが適切に行われているかどうかを判断するのに役立ちます。出力は冗長形式です。各パッケージのデータを 16 進法と ASCII の両方の形式で表示し、各行にリンク レベル ヘッダーを含みます。
	ご注意 : tcpdump コマンドを手動で停止しない場合、許容されている最大の数、すなわち 10,000 個のパケットがキャプチャされます。
		[Interface]: デバッグしている NIC の名前を入力します。有効な NIC 値の情報アイコンをクリックします。
		例 : eth0
		[Expression]: 問題の NIC へ転送されるパケットをフィルタリングするブール式を入力します。たとえば、情報アイコンをクリックします。
		例 1 : ポート 8080 上のプロキシとの間のすべての TCP トラフィックをキャプチャするには、下記の式を入力します。
		`tcp port 8080`
		例 2 : サイト google.com へのすべての TCP トラフィックをキャプチャするには、下記の式を入力します。
		`tcp and dst host google.com`
		例 3 : 特定のエンドユーザー コンピュータからのすべての TCP トラフィックをキャプチャするには、下記の式を入力します。
		`tcp and src host user.websense.com`
		ご注意 :DNS サーバーによって解決できる場合はホスト名を入力できますが、どちらの場合でも出力では IP アドレスを使用します。

tcpdump –w	指定した NIC からファイルにトラフィック (ロー パケット) をダンプするために使用します。 ファイルをダウンロードするには、このコマンドを実行した後、**Download output file for last command** リンクをクリックします。このリンクは、コンソール出力ウィンドウの下にあります。 場合によっては Websense テクニカル サポートがこのファイルを要求することがあります。	[Interface]: デバッグしているアプライアンス NIC の名前を入力します。有効な NIC 値の情報アイコンをクリックします。 [Expression]: 問題の NIC へ転送されるパケットをフィルタリングするブール式を入力します。たとえば、情報アイコンをクリックします。 all を入力すると、すべてのパケットがキャプチャされます。 **ご注意 :**DNS サーバーによって解決できる場合はホスト名を入力できますが、どちらの場合でも出力では IP アドレスを使用します。

コマンド	説明	パラメータ
top -bn1	選択したモジュールで現在実行しているすべてのオペレーティング システム タスクを表示します。これは CPU およびメモリの問題のトラブルシューティングに役立ちます。 **-b** バッチ モードで実行する。 **-n** 繰り返し回数の表示を更新し、終了する。 **-1** アイドル プロセスを表示しない。	なし。
traceroute、traceroute6	これはパケットがネットワーク上で特定のホストに到達するために使用した経路を判断するために使用します。 一部のコンピュータがフィルタリングまたはブロックされない場合、またはトラフィックがアプライアンスに到達しない場合、このコマンドは、コンピューター間にあり、ホストへのアクセスをブロックしている可能性があるにデバイス（またはホップ）を表示します。**tcpdump** を使用して各デバイスからのパケット キャプチャを取得します。 また、遅延の問題がある場合、**traceroute** は原因を突き止めるのに役立ちます。 IPv4 アドレスに対して **traceroute** を使用し、また IPv6 アドレスに対して **traceroute6** を使用します。 **ご注意** :traceroute は、IP アドレスがスプーフィングされている場合には、限定されたユーティリティーになります。 **ご注意** :traceroute6 は、Websense Web Security モジュールではサポートされていません。	[Destination]: 調べている宛先ホストのホスト名または IP アドレスを入力します。
triton-admin-email	Websense Web Security モジュールにのみ、また、TRITON - Web Security がアプライアンス上で実行しているときにのみ適用します。 これはアラート、パスワード リセット通知、および他の管理者からの通信の送信先電子メール アドレスを設定するために使用します。	[Email address]: 管理者の電子メール アドレス

コマンド	説明	パラメータ
triton-smtp-settings	Websense Web Security モジュールにのみ、また、TRITON - Web Security がアプライアンス上で実行しているときにのみ適用します。 これは SMTP サーバーおよび送信者設定を設定するために使用します。 **注意**：通常、これらの設定は、**「Settings（設定）」**>**「Notifications（通知）」**ページの TRITON Unified Security Center で行われます。	[SMTP server IP]: 電子メール アラートの経路上に配置する SMTP サーバーの IP アドレスまたはホスト名。 [Port]:SMTP ポート。 [From email address]: 電子メール アラートの送信者が使用する電子メール アドレス。 [Sender name]: アラートの送信者の名前。
triton-websecurity-services	Websense Web Security モジュールにのみ適用します。 これは TRITON - Web Security サービスのステータスを開始、停止、再開、および照会するために使用します。	[Action]:TRITON - Web Security サービスを開始するには、「start」と入力します。. TRITON - Web Security サービスを停止するには、「**stop**」と入力します。. TRITON - Web Security サービスを再開するには、「**restart**」と入力します。. TRITON - Web Security サービスのステータスを表示するには、「*status*」と入力します。.
user-group-ip-precedence	Web Security モジュールにのみ適用します。 これは次の項目に適用される識別属性の優先順位を変更するために使用します。フィルタリング ポリシー、指定済み管理者 (DA) ロール、プロトコル ポリシー、および利用可能な割り当て時間。 デフォルトでは、属性の優先順位は次の順序（降順）です。 ユーザー > コンピュータ > ネットワーク > グループ > ドメイン user-group-ip-precedence が有効化されると、優先順位は、下記の通りになります。 ユーザー > グループ > ドメイン > コンピュータ > ネットワーク	[Action]: 優先順位を下記に変更するには 「**enable**」と入力します。ユーザー > グループ > ドメイン > コンピュータ > ネットワーク 優先順位を下記に設定するには「**disable**」と入力します。ユーザー > コンピュータ > ネットワーク > グループ > ドメイン 現在の設定を表示するには、「**status**」と入力します。 **警告**：user-group-ip-precedence のステータスを変更すると Filtering Service が停止し、再起動します。

コマンド	説明	パラメータ
wcg-net-check	このコマンドは、Websense Content Gateway モジュールにのみ適用します。 これは Websense Content Gateway についての下記のような診断を表示します。 • インターフェースのステータス • DNS ネーム サーバーへの接続 • Policy Server への接続 • ゲートウェイのパケット損失 • 種々のモジュールの ping 統計 • インターネット接続性 • フィルタリング ステータス このコマンドは、特に遅延の問題、停止、フィルタリングの問題を調べるのに役立ちます。	なし。
wget	これは接続性の問題を診断できるように、Web からファイルを非対話形式でダウンロードするために使用します。 **wget** は、たとえばプロキシを設定しているが Web にアクセスできないような場合に使用します。**wget** は、Web サイトにアクセスし、データを取得しているプロキシをシミュレートします。 このコマンドは、HTTP、HTTPS、および FTP プロトコルをサポートします。	[URL] : ファイルをダウンロードする Web サイトの URL を入力します。
wget-proxy	これは指定した URL とプロキシとの間の接続性をテストするために使用します（ファイルのダウンロードはサポートされていません）。 wget は、たとえばプロキシを設定しているが Web にアクセスできないような場合に使用します。wget は、Web サイトにアクセスし、データを取得しているプロキシをシミュレートします。 このコマンドは、HTTP、HTTPS、および FTP プロトコルをサポートします。	[URL] : 接続性をテストする Web サイトの URL を入力します。 [Proxy IP]: プロキシ IP アドレスを入力します。ほとんどのアプライアンスの設定では、これは P1 インターフェースの IP アドレスです。 [Port]: プロキシがこのトラフィックに使用されると想定するポートを入力します。HTTP に対しては、デフォルトは 8080 に設定されます。HTTPS に対しては、デフォルトは 8070 に設定されます。 [User name]: 認証が必要な場合に、クライアントのユーザー名を入力します。 [Password]: 認証が必要な場合に、クライアントのパスワードを入力します。 Enter ?none? in both fields if user name and password are not applicable.

テクニカル サポート ツール

Websense テクニカル サポートまたは Websense パートナーと協力してネットワークの問題の考えられる原因を調べるとき、下記の組み込みツールがトラブルシューティングに役立つことがあります。

- *トラブルシューティング用ポート*
- *アプライアンス設定のサマリー*
- *リモート アクセス*

トラブルシューティング用ポート

Websense Web Security には、トラブルシューティング用ポートを一時的に開くオプションがあり、それによって種々のトラブルシューティング テストを実行できます (この機能は、Websense Email Security Gateway では利用できません)。

このツールは Websense テクニカル サポートから指示された場合にのみ使用してください。

[Enable troubleshooting ports (トラブルシューティング用ポートの有効化)] をオンにし、**[Save]** をクリックして、この特別のポートを有効化します。

重要
テクニカル サポートがそれらのポートの使用を完了したとき、必ずチェック ボックスを**オフ**にし、**[Save]** をクリックしてポートを無効化してください。これらのポートを開いたまま席を離れてはいけません。

アプライアンス設定のサマリー

設定サマリー ツールは、アプライアンスからデータを収集し、アーカイブ ファイルを生成します。これを Websense テクニカル サポートによる分析とデバッグのために送信することができます。このプロセスには 1 ～ 2 分を要します。

Websense テクニカル サポートがこのファイルを要求したとき、下記の手順を実行します。

- **[Generate File (ファイルを生成)]** をクリックします。
- ファイルが準備できたとき、ページの上部に下記のメッセージが表示されます。Configuration summary has been successfully collected. (設定のサマリーの収集が正常に完了しました) メッセージ内のリンクをクリックして、このアーカイブ ファイルをデスクトップにダウンロードします。
- 次に、このファイルを開くか、保存することができます。
- ユーザーの技術者は、Websense テクニカル サポートへのソース ファイルの転送のために FTP サイトを用意します。

リモート アクセス

リモート アクセスは Websense テクニカル サポートによって要求されたときにのみ有効化します。

- [On] をクリックし、次に [Save] をクリックしたとき、パスコードが収集され、画面に表示されます。
- そのパスコードを Websense テクニカル サポートの技術者に提供します。それによって SSH が有効化され、技術者はアプライアンスにログオンできるようになります。
- アプライアンスへのリモート アクセスを許可し、Websense 技術者がログオンすると「Toolbox（ツールボックス）」ページの下部の [Remote access logon history（リモート アクセス ログオン履歴）] に記録が追加されます。
- 技術者が作業を完了したとき、必ず [Off] をクリックし、[Save] をクリックしてアクセスを無効化してください。

アカウント管理

「Administration（管理）」>「Account Management（アカウント管理）」ページでは下記の操作を行います。

- Appliance Manager にアクセスするためのパスワードを変更する（*Appliance Manager のパスワードの変更*）
- Content Gateway Manager にアクセスするためのパスワードを変更する（*Content Gateway Manager のパスワードのリセット*）
- TRITON – Web Security がアプライアンス上で実行しているとき、TRITON –Web Security パスワードをリセットできます（*TRITON – Web Security パスワードのリセット*）
- パスワード回復の電子メール メッセージを受信するための admin 通知電子メール アドレスと SMTP サーバーを指定する（*admin 通知電子メール アドレスの設定*）
- 利用可能な言語のリストから、Help システムで表示される言語を選択する（*ヘルプ システムの言語*）.

Appliance Manager のパスワードの変更

1. 現在のパスワードを入力してください。
2. 新しいパスワードを入力します。
3. 新しいパスワードを確認します。

[OK] をクリックして新しいパスワードを保存します。

[Cancel] をクリックすると、最後に [OK] をクリックした後に入力したすべての値が破棄され、入力フィールドが最後に保存した値に戻ります。

admin 通知電子メール アドレスの設定

これらの設定を使用して、Appliance Manager のパスワード回復を実行するときに使用する電子メール アドレスと SMTP サーバーを指定し、検証します。パスワードの回復のメカニズムの詳細については、*Appliance Manager のパスワードのリセット* を参照してください。

1. パスワード回復のための電子メール メッセージの送信先の電子メール アドレスを指定します。
2. SMTP サーバーの IP アドレスとポートを指定します。
3. SMTP 接続が認証を必要とする場合、アカウント名とパスワードを提供します。
4. [Test Connection (テスト接続)] ボタンをクリックして SMPT 接続を検証します。

[OK] をクリックして新しい値を保存します。

[Cancel] をクリックすると、最後に **[OK]** をクリックした後に入力したすべての値が破棄され、入力フィールドが最後に保存した値に戻ります。

TRITON – Web Security パスワードのリセット

管理者はいつでも「TRITON Settings (TRITON の設定)」>「My Account (マイアカウント)」ページから管理者の TRITON コンソール パスワードを変更できます。

管理者が TRITON – Web Security パスワードを忘れた場合のために、TRITON – Web Security がアプライアンスで実行しているとき、**「Administration」> 「Account Management」** ページに管理者パスワードを簡単にリセットするためのセクションが含まれています。

[logon page (ログオン ページ)] リンクをクリックし、**[Forgot my password (パスワードを忘れた)]** をクリックします。

ご注意

ほとんどの配備先では、TRITON – Web Security を含む TRITON Unified Security Center は、別のコンピュータにインストールされます。そのような場合、

- **「TRITON – Web Security Password Reset (TRITON – Web Security パスワード リセット)」** セクションは表示されません。
- パスワードをリセットするには、TRITON コンソールを起動し、ログオン ページで **[Forgot my password]** をクリックします。

パスワード リセットのプロセスでは、管理者アカウントに関連付けられた電子メール アドレスに一時パスワードを送信します。一時パスワードは、30 分間だけ有効です。一時パスワードでログオンする前に 30 分以上が経過した場合は、もう一度新しいパスワードを要求する必要があります。

一時パスワードを使ってログオンしたとき、新しいパスワードを入力するように求められます。

電子メール SMTP の設定および管理者電子メール アドレスが TRITON – Web Security 用に設定されていない場合、**「Toolbox」** > **「Command Line Utility」** の **「Websense Web Security」** カテゴリ内の **triton-smtp-settings** コマンドと **triton-admin-email** コマンドを使用してこの設定を行う必要があります。*コマンド ライン ユーティリティ* を参照してください。

Content Gateway Manager のパスワードのリセット

このオプションは、Content Gateway がアプライアンス上で実行しているときにのみ利用できます。

1. プロキシ パスワードをリセットするには、**[Reset Password]** をクリックします。
2. 画面の下部に新しいパスワードが表示されます。そのパスワードをメモしておきます。
3. Appliance Manager の **「Account Management」** ページから移動すると、リセットしたパスワードは表示されなくなります。
4. 新しいパスワードを使って Content Gateway Manager にログオンします。
5. **「Configure」** > **「My Proxy (マイ プロキシ)」** > **「UI Setup (UI の設定)」** > **「Login (ログイン)」** に進み、このパスワードを希望する文字列に変更します。

Appliance Manager のパスワードのリセット

Appliance Manager のログオン パスワードを忘れたか、なくした場合、新しいパスワードを作成するために 2 通りの方法があり、どちらもログオン ポータルで開始されます。

- **[Forgot my password]** をクリックします。
  - 通知用の電子メール アドレスと SMTP サーバーが設定されている場合、その電子メール アドレスに一時パスワードが送信されます。1 時間以内に一時パスワードを使ってログオンし、パスワードをリセットします。*admin 通知電子メール アドレスの設定* を参照してください。
  - 通知用の電子メールを送信できない場合、エラー メッセージが表示され、Websense テクニカル サポートに連絡するように通知されます。セキュリティ コードも提供されます。セキュリティ コードをメモしておいてください。新しいパスワードを生成するとき、Websense Technical Support はそのコードを要求します。

ヘルプ システムの言語

[Language] ドロップ ダウン リストからヘルプ システム情報の表示言語を選択し、[OK] をクリックして適用します。