使用開始にあたって

Websense® V-Series Appliance V10000,
V10000 G2/G3 および V5000 G2

v7.7.3

Published 2012 Revision G
Printed in the United States of America and Ireland.

商標について

WinPcap

目次

第 1 章 **Websense V- シリーズ アプライアンスの紹介 5**

セキュリティ モード 6
アプライアンス上に供給されているソフトウェア 7
Web コンポーネント 7
Web Security Gateway 7
Email のコンポーネント 8
アプライアンス外で実行するソフトウェア 9
Web コンポーネント 9
Data Security のコンポーネント 9
Email のコンポーネント 10
TRITON Unified Security Center 10
TRITON Unified Security Center での
アプライアンスの管理 10
TRITON Infrastructure 11
TRITON – Web Security 11
TRITON – Data Security 12
TRITON – Email Security 12
データベース管理ソフトウェア 13
V シリーズ 7.7.x による IPv6 のサポート 14
IPv6 設定のまとめ 14

第 2 章 **Websense V- シリーズ アプライアンスの設定 17**

アプライアンス ハードウェアのセットアップ 17
V10000 および V10000 G2/G3 ハードウェアのセットアップ . 17
V10000 および V10000 G2/G3 Web モードで
Web Security Gateway を使用 18
V10000 G2/G3 Email モード 18
V10000 G2/G3:Web および Email モードで、
Web Security Gateway を使用 18
V10000 G2/G3:Web および Email モードで、
Web Security を使用
(Web gateway なし) 19
V5000 G2 ハードウェアのセットアップ 19
V5000 G2 : Web モードで、Web Security Gateway を使用 . 20
V5000 G2 : Web モードで、
Web Security を使用 (gateway なし) 20
V5000 G2 : Web および Email モードで、
Web Security を使用
(Web gateway なし) 21

V5000 G2 : Email モード 21
シリアル ポートのアクティブ化 21
コマンド ラインの初期設定の実行 22
データの収集 23
firstboot を実行する 26
アプライアンスの設定 27
システム設定 28
ネットワーク インタフェースの設定 30
Appliance Controller インターフェース (C) 31
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 31
Websense Content Gateway インターフェース (P1 および P2) 32
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 33
Network Agent インターフェース (N) 33
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 34
Email Security Gateway インターフェース (E1 および E2、または P1 および P2) 35
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 36
Email Security 仮想インターフェース 37
インターフェースのボンディング 37
Websense Web Security のみを使用する V10000/V10000 G2/G3 37
Websense Email Security Gateway のみを使用する V10000 G2/G3 38
ルーティングの設定 39
静的経路の設定 39
静的経路の追加 40
経路テーブルのエクスポート 41
モジュール経路の設定 42
モジュール経路の追加 42
アラート 42
SNMP ポーリング (モニタリング) を有効化する 43
SNMP トラップの有効化 43
特定のアラートの有効化 44
Web Security コンポーネントの設定 45
ポリシーソースとは 47
アプライアンスがポリシー ソースでない場合は？ 48
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 . . . 49
ハイブリッド設定の準備 49
冗長性 50
アプライアンス外またはオプションのコンポーネントのインストール 51

TRITON 管理サーバーの作成 52
出荷時のイメージへの復元 53
USB イメージ 53
DVD イメージ 53
バックアップ設定を復元 54

1 Websense V-シリーズ アプライアンスの紹介

Websense V シリーズ アプライアンスは、Web および電子メールのトラフィックおよびコンテンツの分析のために最適化された堅牢なオペレーティング システムを備えた高性能セキュリティ アプライアンスです。

アプライアンスは、下記の機能を提供します。

- アプライアンスの初期設定のためのコマンドライン インターフェース。この機能は USB キーボードおよびモニタまたはシリアル ポート接続を通じて入手でき、基本的なアプライアンス制御コマンドを提供します。
- Appliance Manager、これは、管理機能を提供する Web ベースの設定インターフェースです。
  - システム ダッシュボード、これはアプライアンス上のソフトウェア モジュールおよびシステム リソースの現在のステータスを表示します。
  - アプライアンス設定とネットワーク設定
  - パッチおよびホットフィックス管理、トラブルシューティグ、バックアップおよび復元、および他のアカウント設定のための一連のシステム管理ツール
- プロキシ キャッシング、Web フィルタリング、および電子メール フィルタリングなどのライセンス契約済み機能のカスタム化。この機能は Web ベースの設定インターフェースを通じて入手できます。
- アプライアンス設定および管理のためのイベント ロギング。ログ エントリを Appliance Manager で閲覧でき、またログ ファイルを後で閲覧するためにダウンロードできます。
- 最小限の初期設定の後、Web フィルタリングおよび統合プロキシ キャッシング（ライセンス登録いている場合、Web モード）
- ハイブリッド Web フィルタリングおよびアプライアンス外の Data Security の機能への設定可能なリンク（ライセンス登録している場合、Web モード）
- 電子メールの堅牢なアンチウィルスおよびアンチスパム スキャンニングおよびフィルタリング（Email モード）
- エンド ユーザーが隔離されたメッセージおよび個別の許可 / ブロック リストを管理することができる Personal Email Manager 機能（Email モード）

セキュリティ モード

Websense V シリーズ アプライアンスは、下記のいずれかのセキュリティ モードで実行できます。

Websense V10000 G2/G3 アプライアンス：

セキュリティ モード	モジュール名
Web	Web Security Gateway / Anywhere (V10000 G2 以前の V10000 でも実行します)
Email	Email Security Gateway / Anywhere
Web および Email	Web Security Gateway / Anywhere および Email Security Gateway / Anywhere Web Security および Email Security Gateway / Anywhere

Websense V5000 G2 アプライアンス：

セキュリティ モード	モジュール名
Web	Web Security Web Security Gateway / Anywhere
Email	Email Security Gateway / Anywhere
Web および Email	Web Security および Email Security Gateway / Anywhere

firstboot の初期設定時に、アプライアンスのセキュリティ モードを選択します。*firstboot* の詳細については、*コマンド ラインの初期設定の実行*, 22 ページ を参照してください。

firstboot でセキュリティ モードを選択しても、関連付けられている機能は自動的には有効化されません。これらの機能は、TRITON Unified Security Center で有効なライセンス キーを入力したときのみ完全に有効化されます。詳細は、*TRITON Unified Security Center*, 10 ページ を参照してください。

firstboot が完了した後、アプライアンスのセキュリティ モードを変更する場合は、最初にアプライアンスを出荷時のイメージに復元する必要があります。次に、再イメージングを行った後 firstboot を実行し、別のセキュリティ モードを選択します。*出荷時のイメージへの復元*, 53 ページ を参照してください。

出荷時のイメージへの復元の前に、アプライアンスおよびその各モジュールのフル バックアップを実行することをお勧めします。アプライアンスをバッ

クアップした後でアプライアンスのセキュリティ モードを変更した場合は、バックアップが新しいモードに適用される場合と適用されない場合があります。たとえば、Web Security（プロキシなし）から取り出したバックアップ ファイルから Web Security Gateway（プロキシを含む）を実行しているアプライアンスを復元することはできません。

アプライアンス上に供給されているソフトウェア

Web コンポーネント

Web モードまたは Web および Email モードで実行しているアプライアンスでは、操作を簡単にするために、下記のコア Web セキュリティ コンポーネントが事前にロードされています。

- Policy Database
- Policy Broker
- Policy Server
- Filtering Service
- User Service
- Usage Monitor
- Control Service
- Directory Agent
- State Server
- Multiplexer
- TRITON Unified Security Center (Web Security コンソースのみ)、下記のコンポーネントを含みます。
  - TRITON Web Server
  - Settings Database
  - Investigative Reports Scheduler
  - Manager Web Server
  - Reporting Web Server
  - Reports Information Service
- Network Agent

Web Security Gateway

firstboot 中に Web Security Gateway を設定する場合は、アプライアンスには下記のコンポーネントも含まれます。

- Websense Content Gateway

Web モード（のみ）のアプライアンスで、デフォルトではアプライアンスに TRITON コンソールがインストールされ、その Web セキュリティ機能のみが有効化されます。しかし、アプライアンス上での Web Security コンソールの

使用は任意であり、一般的には評価の際にのみ使用します。製造環境では、TRITON Unified Security Center をアプライアンス外で、別の Windows コンピュータ上で実行することをお勧めします。[評価の場合でも、Web Security コンソールは、アプライアンスが *Full ポリシー ソース* モードで実行している場合にのみアプライアンス上で実行できます]。ポリシー ソースの詳細については、Websense Appliance Manager ヘルプ を参照してください。

組織が大量のレポート、または少量の非常に大きなレポートを生成する場合、アプライアンス上で Web Security コンソールをホストすると他のアプライアンス モジュールのパフォーマンスに影響を与えることがあります。

重要

TRITON コンソールは、アプライアンス上で実行しているとき、Web セキュリティ機能のみが有効化されます。Web セキュリティー機能以上の機能 – 例、TRITON – Data Security を使用する場合は、TRITON Unified Security Center をアプライアンス外の Windows Server 2008 R2 コンピュータにインストールする必要があります。

Email のコンポーネント

Email モードまたは Web および Email モードで実行しているアプライアンスでは、アプライアンスに下記のサービスを含む多くの電子メール セキュリティ機能が含まれています。

- Configuration Service
- Authentication Service
- Quarantine Service
- Log Service
- Update Service
- Filtering Service
- Mail Transfer Agent

管理 (TRITON Unified Security Center を通じて) とロギング (Email Security Log Server を通じて) だけがアプライアンス外のコンポーネントによって実行されます。

アプライアンス外で実行するソフトウェア

この項に記載している Websense コンポーネントは、アプライアンス外にインストールする必要があります。また、Microsoft SQL Server はアプライアンス外にインストールする必要があります。

ここで記載しているコンポーネントをインストールするには Websense Installer を使用します。コンポーネントとインストール手順の詳細については、「Websense Deployment and Installation Center」を参照してください。

Web コンポーネント

下記の Web コンポーネントはアプライアンス上では実行しません。一部のコンポーネントは、Windows 専用コンポーネントです。

- Web Security Log Server
- Real-Time Monitor
- Remote Filtering Server
- Sync Service（ハイブリッド Web セキュリティを使用しているサイト用）
- Linking Service（統合 Data Security 機能を使用しているサイト用）
- 透過識別エージェント（ユーザーに資格情報を要求せずにユーザー、グループ、またはドメイン [OU] ポリシーを適用する）
  - DC Agent
  - Logon Agent
  - eDirectory Agent
  - RADIUS Agent

ご注意
ライセンスに Websense Web Security Gateway Anywhere が含まれる場合は、TRITON Unified Security Center をアプライアンス外の Windows Server 2008 R2 コンピュータで実行する必要があります。

Data Security のコンポーネント

下記の Data Security コンポーネントはアプライアンス外で実行します。

- TRITON – Data Security コンソール
- Protector
- Mobile Agent
- SMTP エージェント
- Microsoft ISA/TMG エージェント

- Endpoint エージェント
- プリンタ エージェント
- crawler
- 統合エージェント

Email のコンポーネント

下記の Email Security Gateway コンポーネントはアプライアンス上では実行しません。それらのコンポーネントは、Windows 専用コンポーネントです。

- TRITON – Email Security コンソール (TRITON Unified Security Center の Email Security モジュール、*TRITON Unified Security Center*, 10 ページ を参照)
- TRITON – Data Security コンソール (TRITON Unified Security Center の Data Security モジュール、*TRITON Unified Security Center*, 10 ページ を参照)Data Security モジュールは、電子メール DLP (data leakage prevention) 機能では必須です。
- Email Security Log Server

TRITON Unified Security Center

TRITON Unified Security Center (TRITON コンソール) は、配備全体に対する Web ブラウザ ベースのグラフィカル管理アプリケーションです。

グローバル設定およびロギングの管理のほかに、下記の 3 つの管理モジュールで構成されています。TRITON – Web Security、TRITON – Data Security、TRITON – Email Security 各モジュールはそれぞれの製品の機能を設定および管理するために使用します。

ライセンスによっては、これらのモジュールの一部が有効化されない場合があります。

TRITON コンソールの 2 つ以上のモジュール – 例、Web Security と Data Security の両方 – を有効化するには、TRITON コンソールを Windows Server 2008 R2 コンピュータにインストールする必要があります。TRITON Unified Security Center がアプライアンスの C インターフェース (およびアプライアンスが Email モードまたは Web および Email モードである場合は E1 インターフェース) に接続できる必要があります。

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）」** 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、7.7.3)
- ハードウェア プラットフォーム (例、V5000、V10000、V10000 G2/G3)
- 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。

TRITON Infrastructure

TRITON Infrastructure は、TRITON モジュールが必要とする共通ユーザー インターフェース、ロギング、およびレポート作成コンポーネントで構成されています。

TRITON Infrastructure はまた (オプションで)、Websense ロギング データに使用できる SQL Server 2008 R2 Express を含みます。最良の方法として、SQL Server 2008 R2 Express を非製造または評価環境でのみ使用するようにしてください。製造環境では、Full SQL Server を使用する必要があります。

TRITON Infrastructure サービスは、下記を含みます。

- Websense TRITON Unified Security Center
- Websense TRITON Central Access
- Websense TRITON Settings Database
- Websense TRITON Reporting Database (SQL Server 2008 R2 Express を使用している場合)

TRITON – Web Security

TRITON – Web Security は、一般的な設定タスクの実行、フィルタリング ポリシーの設定、ユーザーおよびグループへのポリシーの割り当て、レポートの実行および他の管理タスクのために使用します。

TRITON – Web Security サービスは、下記を含みます。

- Websense TRITON – Web Security (旧 ApacheTomcatWebsense)
- Websense Web Reporting Tools (旧 Apache2Websense)
- Investigative Reports Scheduler
- Reports Information Service
- Websense RTM Client (Real-Time Monitor を使用している場合)
- Websense RTM Database (Real-Time Monitor を使用している場合)
- Websense RTM Server (Real-Time Monitor を使用している場合)

Web モードのアプライアンスでは、評価や小規模なインストールのために便利なように、Web Security モジュールのみを備えた TRITON Unified Security

Center（TRITON – Web Security）が事前にインストールされています。このコンポーネントは、Web および Email モードのアプライアンスではインストールされていません。

TRITON – Web Security コンソールにアクセスするには、サポートされているブラウザで以下のアドレスを入力します。

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

- オフボックスの TRITON マネージャを使用している場合、<IP address> を TRITON マネージャがインストールされているサーバーの IP アドレスに置換します。
- オンボックスの TRITON マネージャを使用している場合、アプライアンスのインターフェース C の IP アドレスを指定します。
- TRITON – Web Security マネージャへのアクセスは Websense, Inc によって発行される SSL セキュリティ証明書によってセキュリティが保護されます。ブラウザは Websense, Inc を既知の認証機関（CA）として認識しませんから、セキュリティ関連の警告が表示されます。

ご注意
上記のサービス名は、TRITON – Web Security のアプライアンス外のインストールの場合の名前です。アプライアンス上の場合、Websense TRITON – Web Security のサービス名は下記のようになります。*Manager Web Server*、また Websense Web Reporting Tools のサービス名は次の通りです。*Reporting Web Server*。

TRITON – Data Security

TRITON – Data Security は、Websense Data Security のセットアップおよび設定、インシデント管理、システム ステータス レポート、およびロールベースの管理のすべての側面を一元管理します。

TRITON – Data Security サービスは下記を含みます。

- Websense Data Security Management Server
- Websense TRITON – Data Security
- Websense Data Policy Engine
- Websense Data Fingerprint Database
- Websense Data Discovery and Fingerprint Crawler
- Websense PreciseID and Data Endpoint Server

TRITON – Email Security

TRITON – Email Security は、一般的なシステム プロパティ、管理者ロール、ユーザー ディレクトリ、電子メール フィルタリング、電子メール ポリシー、および Personal Email Manager エンドユーザー 機能オプションを設定および管理するために使用します。また、電子メール アクティビティ レポートを

作成および表示するためにも使用します。

アプライアンス外の Websense Email Security 管理コンソールは、下記の 1 つのサービスで構成されています。

- Websense TRITON – Email Security

データベース管理ソフトウェア

Websense Web セキュリティおよび Email セキュリティ製品には、それぞれのレポート作成データベース（どちらも Log Database と呼びます）をホストするために Microsoft SQL Server が必要です。Web Security Log Database と Email Security Log Database の両方を同じデータベース エンジン インスタンスによってホストできます。これらの Log Databases に格納されている情報がレポートの作成のために使用されます。

Web Security Log Server または Email Security Log Server をインストールする前に、SQL Server 2005 または 2008 をインストールして、ネットワーク内のコンピュータ上で実行する必要があります。SQL Server のサポートされているバージョンの詳細については、「Deployment and Installation Center」を参照してください。SQL Server は Websense ライセンスには含まれていませんから、別途に入手する必要があります。インストールと設定の手順については、Microsoft のマニュアルを参照してください。

SQL Server がない場合、評価のために、Websense Installer を使用して SQL Server 2008 R2 Express をインストールできます。SQL Server 2008 R2 Express は、TRITON Unified Security Center と同じコンピュータ上または別のコンピュータ上にインストールできます。インストールの手順については、Deployment and Installation Center を参照してください。

ご注意
製造環境では、フル SQL Server を使用するのが最良の方法です。SQL Server 2008 R2 Express は、非製造環境と評価環境に適しています。

V シリーズ 7.7.x による IPv6 のサポート

TRITON Enterprise のバージョン 7.7.x (7.7.x V シリーズ アプライアンスを含む) は、いくつかの IP v 6 機能の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。

詳細については、「TRITON – Web Security Help and Content Gateway Manager Help」を参照してください。

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。

2 Websense V- シリーズ アプライアンスの設定

Websense V シリーズ アプライアンスの設定は、下記のタスクを含みます。

1. *アプライアンス ハードウェアのセットアップ*, 17 ページ
2. *コマンド ラインの初期設定の実行*, 22 ページ
3. *アプライアンスの設定*, 27 ページ
4. *アプライアンス外またはオプションのコンポーネントのインストール*, 51 ページ

個別の配備では、それ以外の初期設定手順も必要になる場合があります。詳細については、「Deployment and Installation Center」を参照してください。

アプライアンス ハードウェアのセットアップ

アプライアンスの梱包に入っているクイック スタート ポスターに、各 Websense アプライアンスの梱包に含まれるすべての品目が示されています。2 ページから成っているクイック スタート ポスターは、ハードウェアを設定する方法を説明し、ケーブルをアプライアンスおよびネットワークに接続する方法を示しています。

- V5000 G2 のポスターへのアクセス
- V10000 G2 のポスターへのアクセス
- V10000 G3 のポスターへのアクセス

ご使用の Websense アプライアンス モデルに対応する項をお読みください。

- *V10000 および V10000 G2/G3 ハードウェアのセットアップ*
- *V5000 G2 ハードウェアのセットアップ*
- *シリアル ポートのアクティブ化*

V10000 および V10000 G2/G3 ハードウェアのセットアップ

下記のように、アプライアンスのネットワーク インターフェースが DNS サーバーおよびインターネットにアクセスできる必要があります。この情報は、アプライアンスに対して選択するセキュリティ モードによって少し異なります。

- *V10000 および V10000 G2/G3 Web モードで Web Security Gateway を使用*
- *V10000 G2/G3 Email モード*
- *V10000 G2/G3:Web および Email モードで、Web Security Gateway を使用*
- *V10000 G2/G3:Web および Email モードで、Web Security を使用 (Web gateway なし)*

V10000 および V10000 G2/G3 Web モードで Web Security Gateway を使用

ネットワーク インターフェース C が DNS サーバーにアクセスできる必要があります。このインターフェースは通常、インターネットに継続的にアクセスしています。基本のデータベースは、インターフェース C を通じて (またはオプションで P1 を通じて) Websense サーバーからダウンロードされます。

- インターフェーズ C が **download.websense.com** でダウンロード サーバーにアクセスできることを確認してください (別の方法として、一部のサイトでは、Websense Master Database および他のセキュリティ更新をダウンロードするために P1 プロキシ インターフェースを設定しています。この変更は、TRITON – Web Security コンソールで行う必要があります。その場合、インターフェース C はインターネット アクセスを必要としません)。
- 上記のアドレスが、C インターフェースがアクセスできる URL を管理するすべてのファイアウォール、プロキシ サーバ、ルータまたはホスト ファイルによって許可されていることを確認してください。

V10000 G2/G3 Email モード

ネットワーク インターフェース E1 および E2 (使用している場合) が DNS サーバーにアクセスできる必要があります。これらのインターフェースは通常、アプライアンスが稼働状態になった後は、インターネットに継続的にアクセスしています。基本のデータベースは、これらのインターフェースを通じて Websense サーバーからダウンロードされます。

- E1 および E2 (使用している場合) が **download.websense.com** でダウンロード サーバーにアクセスできることを確認してください。
- 上記のアドレスが、E1 (および E2) インターフェースがアクセスできる URL を管理するすべてのファイアウォール、プロキシ サーバ、ルータまたはホスト ファイルによって許可されていることを確認してください。
- ネットワーク インターフェース E1 および E2 (使用している場合) がメール サーバーにアクセスできる必要があります。

V10000 G2/G3:Web および Email モードで、Web Security Gateway を使用

ネットワーク インターフェース C および E1 ならびに EU (使用している場合) が DNS サーバーにアクセスできる必要があります。これらのインターフェースは通常、インターネットに継続的にアクセスしています。基本の

データベースは、これらのインターフェースを通じて Websense サーバーからダウンロードされます。

- インターフェース C および E1 ならびに E2（使用している場合）が **download.websense.com** でダウンロード サーバーにアクセスできることを確認してください。（一部のサイトでは、Websense Master Database および他のセキュリティ更新をダウンロードするために、(C インターフェースの代わりに）P1 プロキシ インターフェースを設定しています。この変更は、TRITON – Web Security コンソールで行う必要があります。その場合、インターフェース C はインターネット アクセスを必要としません）。
- 上記のアドレスが、C、E1 および E2（使用している場合）インターフェースがアクセスできる URL を管理するすべてのファイアウォール、プロキシ サーバ、ルータまたはホスト ファイルによって許可されていることを確認してください。
- ネットワーク インターフェース E1 および E2（使用している場合）がメール サーバーにアクセスできる必要があります。

V10000 G2/G3:Web および Email モードで、Web Security を使用 (Web gateway なし)

ネットワーク インターフェース C および E1 ならびに EU（使用している場合）が DNS サーバーにアクセスできる必要があります。これらのインターフェースは通常、インターネットに継続的にアクセスしています。基本のデータベースは、これらのインターフェースを通じて Websense サーバーからダウンロードされます。

- インターフェース C および E1 ならびに E2（使用している場合）が **download.websense.com** でダウンロード サーバーにアクセスできることを確認してください。
- 上記のアドレスが、C、E1 および E2 インターフェースがアクセスできる URL を管理するすべてのファイアウォール、プロキシ サーバ、ルータまたはホスト ファイルによって許可されていることを確認してください。
- ネットワーク インターフェース E1 および E2 （使用している場合）がメール サーバーにアクセスできる必要があります。
- ネットワーク インターフェース N をルータまたはスイッチ上のミラー ポートに接続する必要があります。
- インターフェース N を使ってブロック情報を送信する場合、インターフェース N を*双方向*ミラー ポートに接続する必要があります。インターフェース N は、双方向ミラー ポートを通じて、すべてのクライアント トラフィックをモニタするだけでなく、必要に応じてブロック情報を送信します。

V5000 G2 ハードウェアのセットアップ

下記のように、アプライアンスのネットワーク インターフェースが DNS サーバーおよびインターネットにアクセスできる必要があります。この情報は、アプライアンスに対して選択するセキュリティ モードによって少し異なります。

- *V5000 G2 : Web モードで、Web Security Gateway を使用*
- *V5000 G2 : Web モードで、Web Security を使用 (gateway なし)*
- *V5000 G2 : Web および Email モードで、Web Security を使用 (Web gateway なし)*
- *V5000 G2 : Email モード*

V5000 G2 : Web モードで、Web Security Gateway を使用

ネットワーク インターフェース C が DNS サーバーにアクセスできる必要があります。このインターフェースは通常、インターネットに継続的にアクセスしています。基本のデータベースは、インターフェース C を通じて Websense サーバーからダウンロードされます。

- インターフェーズ C が **download.websense.com** でダウンロード サーバーにアクセスできることを確認してください (別の方法として、一部のサイトでは、Websense Master Database および他のセキュリティ更新をダウンロードするために P1 プロキシ インターフェースを設定しています。この変更は、TRITON – Web Security コンソールで行う必要があります。その場合、インターフェース C はインターネット アクセスを必要としません)。
- 上記のアドレスが、C インターフェースがアクセスできる URL を管理するすべてのファイアウォール、プロキシ サーバ、ルータまたはホスト ファイルによって許可されていることを確認してください。

V5000 G2 : Web モードで、Web Security を使用 (gateway なし)

ネットワーク インターフェース C が DNS サーバーにアクセスできる必要があります。インターフェース C はインターネットに継続的にアクセスしている必要があります。基本のデータベースは、このインターフェースを通じて Websense サーバーからダウンロードされます。

- インターフェーズ C が **download.websense.com** でダウンロード サーバーにアクセスできることを確認してください
- 上記のアドレスが、C インターフェースがアクセスできる URL を管理するすべてのファイアウォール、プロキシ サーバ、ルータまたはホスト ファイルによって許可されていることを確認してください。
- ネットワーク インターフェース N をルータまたはスイッチ上のミラー ポートに接続する必要があります。
- インターフェース N を使ってブロック情報を送信する場合、インターフェース N を *双方向*ミラー ポートに接続する必要があります。インターフェース N は、双方向ミラー ポートを通じて、すべてのクライアント トラフィックをモニタするだけでなく、必要に応じてブロック情報を送信します。

V5000 G2 : Web および Email モードで、Web Security を使用

(Web gateway なし)

インターフェース C、P1 および P2 (使用している場合) が DNS サーバーにアクセスできる必要があります。これらのインターフェースは通常、アプライアンスが稼働状態になった後は、インターネットに継続的にアクセスしています。基本のデータベースは、これらのインターフェースを通じて Websense サーバーからダウンロードされます。

- C、P1 および P2 (使用している場合) が **download.websense.com** でダウンロード サーバーにアクセスできることを確認してください。
- 上記のアドレスが、C、P1 および P2 インターフェースがアクセスできる URL を管理するすべてのファイアウォール、プロキシ サーバ、ルータまたはホスト ファイルによって許可されていることを確認してください。
- ネットワーク インターフェース P1 および P2 (使用している場合) がメール サーバーにアクセスできる必要があります。

V5000 G2 : Email モード

インターフェース P1 および P2 (使用している場合) が DNS サーバーにアクセスできる必要があります。これらのインターフェースは通常、アプライアンスが稼働状態になった後は、インターネットに継続的にアクセスしています。基本のデータベースは、これらのインターフェースを通じて Websense サーバーからダウンロードされます。

- P1 および P2 (使用している場合) が **download.websense.com** でダウンロード サーバーにアクセスできることを確認してください。
- 上記のアドレスが、P1 および P2 インターフェースがアクセスできる URL を管理するすべてのファイアウォール、プロキシ サーバ、ルータまたはホスト ファイルによって許可されていることを確認してください。
- ネットワーク インターフェース P1 および P2 (使用している場合) がメール サーバーにアクセスできる必要があります。

シリアル ポートのアクティブ化

ハードウェアをセットアップした後、シリアル ポートまたはモニタおよびキーボード ポートを通じてアプライアンスに直接に接続します。シリアル ポートの有効化には、下記の設定値を使用します。

- 9600 ボーレート
- 8 データ ビット
- パリティなし

アプライアンスを起動したとき、firstboot という名前のアクティブ化スクリプトが実行します。

コマンド ラインの初期設定の実行 を参照してください。

firstboot が実行し、コマンド ライン シェルを終了した後、アプライアンスのコマンド ライン シェルへのアクセスには管理者資格情報 (firstboot で設定した「admin」と パスワード) が必要です。

コマンド ラインの初期設定の実行

Websense V シリーズ アプライアンスの設定は、下記のタスクを含みます。このトピックは、**ステップ 2** を扱います。

1. *アプライアンス ハードウェアのセットアップ*, 17 ページ
2. *コマンド ラインの初期設定の実行*, 22 ページ
   - *データの収集*
   - *firstboot を実行する*
3. *アプライアンスの設定*, 27 ページ
   - *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*
4. *アプライアンス外またはオプションのコンポーネントのインストール*, 51 ページ

個別の配備では、それ以外の初期設定手順も必要になる場合があります。詳細については、「Deployment and Installation Center」を参照してください。

Websense アプライアンスを初めて起動したとき、短いスクリプト (**firstboot**) で下記の操作を要求されます。

- アプライアンスのセキュリティ モードを選択する
- C というラベルのネットワーク インターフェースを設定する
- そのほかに、ホスト名、パスワードなどのいくつかの一般的な項目を入力する

firstbootfirstboot スクリプトを終了する前に、これらの設定を検討し変更することができます。設定を承認した後、アプライアンス モードが設定されます。

後で、セキュリティ モード以外の設定は、Appliance Manager のユーザー インターフェースを通じて変更できます。

セキュリティ モードを変更するには、Websense Downloads サイトからのイメージを使ってアプライアンスを再イメージングし、**firstboot** スクリプトを再度実行します。

データの収集

スクリプトを実行する前に、下記の情報を収集します。この情報の一部は、ハードウェアのセットアップ中にクイック スタート ポスターに書き出しているかも知れません。

セキュリティ モード	下記のいずれかを選択します。 Web Email Web および Email
持っている Web セキュリティ ライセンス (Web モードで要求された場合)	下記のいずれかを選択します。 Websense Web Security Web Security Gateway Web Security Gateway Anywhere
ホスト名 (例 : appliance.domain.com) 1 ～ 60 文字。 最初の文字は英文字でなければなりません。 使用できる文字 : 英文字、数字、ダッシュ、またはピリオド。 名前の最後の文字にピリオドを使用できません。 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。	
ネットワーク インターフェース C の IP アドレス	
ネットワーク インターフェース C のサブネット マスク	

ネットワーク インターフェース C のデフォルト ゲートウェイ (IP アドレス) *オプション* 注意：インターフェース C にインターネットへのアクセスを提供していない場合、TRITON – Web Security コンソールを使用して、PI を Websense から Master URL Database の更新をダウンロードするように設定します (Web モード)。 Websense からアンチスパンおよびアンチウィルス データベースの更新をダウンロードするには E1 または P1* を設定します (Email モード)。 これらのインターフェースをデータベース ダウンロードのためにインターネットにアクセスするように設定する作業は、Appliance Manager および TRITON Unified Security Center を通じて行います。インターフェースの設定の詳細については、Appliance Manager ヘルプを参照してください。データベース ダウンロードの設定の詳細については、TRITON – Web Security and – Email Security ヘルプを参照してください。 * V5000 G2 では、P1 を使用します。E1 インタフェースはありません。	
ネットワーク インターフェース C の一次 DNS サーバー (IP アドレス)	
ネットワーク インターフェース C の二次 DNS サーバー (IP アドレス) *オプション*	
ネットワーク インターフェース C の三次 DNS サーバー (IP アドレス) *オプション*	

統合パスワード (8 ～ 15 文字、少なくとも 1 つの文字と 1 つの数字) このパスワードは、下記のコンポーネントに対するパスワードです (アプライアンスのセキュリティ モードによって異なります)。 Web モード • Appliance Manager • TRITON – Web Security • Content Gateway Manager (Web Security Gateway / Anywhere を使用しているサイトの場合) Email モード • Appliance Manager Web および Email モード • Appliance Manager • Content Gateway Manager (Web Security Gateway / Anywhere を使用しているサイトの場合)	
このアプライアンスの統合方法 (Web Security を使用しているサイトの場合。下記のいずれかを選択します)。 • スタンドアロン (Network Agent のみ) • Microsoft TMG • Cisco PIX • Cisco ASA • Citrix	サードパーティの統合製品 (もしあれば) を選択します。
使用状況統計を送信しますか？	オプションとして、フィルタリングおよび分類の精度の向上に役立てるために、アプライアンス モジュールからの使用状況統計を Websense に送信することができます。

firstboot を実行する

コマンド ライン初期設定スクリプト (**firstboot**) を下記の手順で実行します。

1. USB キーボードおよびモニタ、またはシリアル ポート接続を通じてアプライアンスにアクセスします。

> **ご注意**
> アプライアンスを設定するには、シリアル ポートを通じて、またはキーボード / ビデオ ポートを通じて接続し、firstboot スクリプトを完了します。シリアル ポートの有効化には、下記の設定値を使用します。
>
> - 9600 ボーレート
> - 8 データ ビット
> - パリティなし

2. プロンプトが表示された時に、ライセンス契約を承諾します。
3. 開始するかどうかを尋ねられたとき、「**yes**」と入力し、アクティブ化スクリプト **firstboot** を開始します。

   手動でスクリプトを再実行するには、下記のコマンドを入力します。

   ```
   firstboot
   ```

4. 最初のプロンプトで、下記のいずれかのセキュリティ モードを選択します。
   - **Web**：モデル V10000 G2/G3 では、このモードを選択したとき Web Security Gateway が提供されます。モデル V10000 および V5000 G2 では、Web モードを選択したとき、Web Security または Web Security Gateway（どちらを使用するかを選択できます）が提供されます。
   - **Email**：Email Security Gateway の機能が提供されます。
   - **Web および Email**：Email Security Gateway の機能と、Web Security Gateway（V10000 G2/G3 の場合）または Web Security（V10000 G2/G3 または V5000 G2 の場合）が提供されます。
5. 画面の手順に従って、上記で収集した情報を入力してください。

アクティブ化スクリプトが正常に完了した後、サポートされているブラウザを開き、アドレス バーに下記の URL を 入力することによって Appliance Manager にアクセスします。

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

これで次のステップに移る準備ができました。*アプライアンスの設定*

すべての Websense コンソールは、下記のブラウザをサポートします。

- Microsoft Internet Explorer 8 および 9
- Mozilla Firefox バージョン 5 以上

- Google Chrome 13 以上

> **ご注意**
> Internet Explorer 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。

アプライアンスの設定

Websense V シリーズ アプライアンスの設定は、下記のタスクを含みます。このトピックは、**ステップ 3** を扱います。

1. *アプライアンス ハードウェアのセットアップ*
2. *コマンド ラインの初期設定の実行*
3. *アプライアンスの設定*
   - *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*
   - *Web Security コンポーネントの設定*
4. *アプライアンス外またはオプションのコンポーネントのインストール*

Appliance Manager は、アプライアンスのための Web ベースのインターフェースです。これはシステム ステータスの表示、ネットワークおよび通信設定の構成、および一般的なアプライアンス管理のために使用します。

firstboot スクリプトによって要求された初期設定を完了した後、Appliance Manager を使用してネットワーク インターフェース P1、P2、N、E1、および E2 の重要な構成します（一部のモードでは一部のインターフェースは任意です）。V5000 G2 では、E1 および E2 インターフェースはありません。

システム設定

サポートされているブラウザを通じて Appliance Manager にアクセスします。

> **重要**
>
> ネットワーク内でいずれかの 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。

いずれかのフィールドに関する詳細な手順、または他の利用可能な設定の詳細については、本文で参照されている Appliance Manager ヘルプをお読みください。

1. サポートされているブラウザを開き、アドレス バーに下記の URL を入力します。

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

   （*コマンド ラインの初期設定の実行*を参照）。
2. ユーザー名 **admin** およびアプライアンスの初期設定時に設定したパスワード設定を使ってログオンします。
3. 左側のナビゲーション ペインで、**[Configuration（設定）]** >**[System（システム）]** をクリックします。
4. **[Time and Date（時刻と日付）]** で下記の手順を実行します。
   - **[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。

5. システムの識別と管理に役立てるために (特に複数のアプライアンスが配備されるとき)、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。

6. **[OK]** をクリックします。

   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。

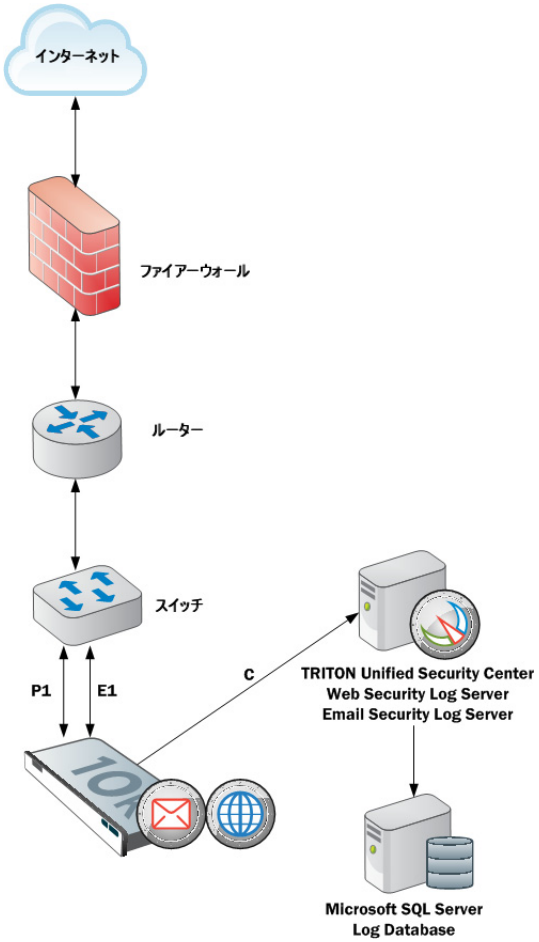
7. *ネットワーク インタフェースの設定* に進みます。

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、または P1 および P2)*
- *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.x 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)、**firstboot** 中に割り当て済み :

- 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）。

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、本文中で参照されている Appliance Manager のヘルプをお読みください。

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。すべての必要なサービスが起動するのを待ちます（次のオプションのサービスがあります：Directory Agent、State Server、Multiplexer、TRITON – Web Security manager）。
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。
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、443、8070、および 8080 を無視します。
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。

Email Security Gateway インターフェース（E1 および E2、または P1 および P2）

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。アプライアンス外のコンポーネントを配備する前に、インターフェース E1、E2、および C を正しく設定します。

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/G3 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 (P1) を使用し、E2 (P2) は使用しません。
- もう 1 つのオプションは、E1 (P1) がインバウンドを受け入れ、E2 (P2) 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 (P1 または P2) 上に仮想インターフェースを構成することができます。

重要

V10000 G2/G3 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。 デフォルトでは E1 が レポート作成用に SQL Server に接続されます。E1 に有効な IP アドレスがないか、または DNS アドレスがない場合、Email Security Gateway は SQL Server ホスト名を解決できず、SQL Server との接続を作成できません。この場合、管理コンソールのオフボックス インストールがブロックされます。 V5000 G2 では E1 を P1 に置き換えます。
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。

この時点でインターフェースのボンディングを設定しない場合、*ルーティングの設定*に進みます。

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/G3 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。

重要 : 速度またはデュプレックス モードが異なるインターフェースをボンディングしていはいけません。パフォーマンス上の問題が生じることがあるからです。

Websense Web Security のみを使用する V10000/V10000 G2/G3

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。速度またはデュプレックス モードが異なるインターフェースをボンディングしていはいけません。パフォーマンス上の問題が生じることがあるからです。

Websense Email Security Gateway のみを使用する V10000 G2/G3

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 G2/G3 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。速度またはデュプレックス モードが異なるインターフェースをボンディングしていはいけません。パフォーマンス上の問題が生じることがあるからです。

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。
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。注釈行は「#」から始めます。
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。

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。
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。

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*, 44 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**暗号化 キー**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*, 44 ページ 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*, 44 ページ 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 に進みます。

Web Security コンポーネントの設定

1. **「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。
   - **[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。
- 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 Web Security 専用（または 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。

- 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 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 サービスにのみ必須）
  - State Server（オプション）
  - Multiplexer（オプション）
  - Usage Monitor
  - 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 (Web Security Gateway を使用している場合のみ）
  - Network Agent モジュール (Web Security では必須、Web Security Gateway ではオプション）

  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。

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
  - Usage Monitor
  - Filtering Service
  - Control Service
  - Directory Agent
  - Websense Content Gateway モジュール (Web Security Gateway を使用している場合）
  - Network Agent モジュール (Web Security では必須、Web Security Gateway ではオプション）

  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 (Web Security Gateway を使用している場合)
- Network Agent モジュール (Web Security では必須、Web Security Gateway ではオプション)

「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。これはアプライアンスが Policy サーバーに近接し、同じネットワーク上にあるとき、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 Policy Server に継続的に接続していることを必要とします。Policy Server 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。

Policy Server 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 Active Directory (Native Mode®)
  - 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。

アプライアンス外またはオプションのコンポーネントのインストール

Websense V シリーズ アプライアンスの設定は、下記のタスクを含みます。このトピックは、**ステップ 4** を扱います。

1. *アプライアンス ハードウェアのセットアップ*
2. *コマンド ラインの初期設定の実行*
3. *アプライアンスの設定*
   - *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*
4. *アプライアンス外またはオプションのコンポーネントのインストール*

アプライアンスを設定した後、アプライアンス外のコンポーネントをインストールします。

注意：アプライアンス外のコンポーネントを配備する前に、必ず Appliance Manager を使って使用するアプライアンス インターフェース [C、P1、P2(オプション)、E1、および E2 (オプション)] を設定してください。Email Security Gateway を使用しているサイトでは、デフォルトでは E1 がレポート作成用に SQL Server に接続されます。E1 に有効な IP アドレスがないか、または DNS アドレスがない場合、Email Security Gateway は SQL Server ホスト名を解決できず、SQL Server との接続を作成できません。この場合、管理コンソールのオフボックス インストールがブロックされます [V5000 G2 では E1 を P1 に置き換えます]。

これらのコンポートの詳細については、*アプライアンス外で実行するソフトウェア, 9 ページ* を参照してください。コンポーネントをインストールするコンピュータで Websense Installer を (カスタム インストール モードで) 実

行します。その方法については、Websense Technical Library を参照してください。

ご注意
アプライアンス上で Policy Broker を実行する場合、Policy Server のアプライアンス上のインスタンスだけが Policy Broker と通信できます。この場合、Policy Server をアプライアンス外にインストールできません。ただし、Policy Broker がアプライアンス外にインストールされている場合、Policy Server のアプライアンス上およびアプライアンス外のインスタンスがどちらも Policy Broker と通信できます。

追加の機能を提供するため、または処理負荷を分散するために、ネットワーク内のコンピュータに Web セキュリティ フィルタリングのコンポーネントの追加のインスタンスをインストールできます。たとえば、ネットワーク内のコンピュータに Websense Network Agent の追加のインスタンスをインストールできます。

TRITON 管理サーバーの作成

重要
TRITON 管理サーバーを作成する前に、アプライアンスをセットアップし構成する必要があります。それがまだ完了していない場合は、TRITON 管理サーバーを作成する前に下記の手順を実行します。

- *アプライアンス ハードウェアのセットアップ*, 17 ページ
- *コマンド ラインの初期設定の実行*, 22 ページ
- *アプライアンスの設定*, 27 ページ

TRITON Unified Security Center がインストールされているコンピュータを *TRITON 管理サーバー*と言います。TRITON 管理サーバーの作成の手順については、Websense Technical Library を参照してください。

TRITON – Web Security コンソールにアクセスするには、サポートされているブラウザで以下のアドレスを入力します。

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

- オフボックスの TRITON マネージャを使用している場合、<IP address> を TRITON マネージャがインストールされているサーバーの IP アドレスに置換します。
- オンボックスの TRITON – Web Security マネージャを使用している場合、アプライアンスのインターフェース C の IP アドレスを指定します。
- TRITON – Web Security マネージャへのアクセスは Websense, Inc によって発行される SSL セキュリティ証明書によってセキュリティが保護されま

す。ブラウザは Websense, Inc. を既知の認証機関 (CA) として認識しませんから、セキュリティ関連の警告が表示されます。

出荷時のイメージへの復元

USB イメージ

v7.7.3 以降の V シリーズ アプライアンスにはリカバリ DVD が添付されていません。リカバリ イメージは USB フラッシュ ドライブからダウンロードしてインストールできます。リカバリ イメージは MyWebsense からダウンロードできます。イメージをダウンロードした後、USB フラッシュ ドライブに焼き付けなければなりません。USB ドライブのイメージを作成する方法については、Websense Technical Library の中の記事を参照してください。

DVD イメージ

リリース v7.7.3 以前の V10000、V10000 G2 および V5000 G2 には、アプライアンスを出荷時のイメージに復元するために使用するリカバリー用 DVD が添付されています。この復元手順は、インストール環境を以前のバージョンにロールバックする必要がある場合にのみ使用します。(設定の完全バックアップを保存した後) この DVD を使用して、アプライアンスを再イメージングし、カスタム アプライアンスおよびモジュールの設定を復元できます。

重要
アプライアンスに添付されているオリジナルのリカバリー用 DVD を使用します。DVD をなくした場合、DVD イメージを My Websense からダウンロードできます。アプライアンスの製造日付に関連付けられているイメージを使用することが重要です。MyWebsense Downloads ページに、各イメージに対応するアプライアンス製造日付が示されます。

出荷時のイメージにリセットする前に、アプライアンス外で実行中のすべての Websense コンポーネントを停止する必要があります。

1. アプライアンスの外で実行しているすべての Websense コンポーネントを停止します。たとえば、Web Security または Email Security Log Servers、Sync Service、Linking Service、透過的 ID エージェント、および TRITON Unified Security Center を停止します。
2. 可能な場合は、保存した情報をバックアップします。
   a. Web ブラウザを使用して、下記の Appliance Manager にログオンします。

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

b. 「**Administration (管理)**」> 「**Backup Utility (バックアップ ユーティリティ)**」に進み、設定の完全バックアップを作成します。詳細については、オンライン ヘルプを参照してください。このバックアップ ファイルを別のコンピュータに保存します。

3. コンピュータ ラックに移動し、アプライアンス DVD ドライブにリカバリー用ディスクを挿入します。
4. アプライアンスを再起動します (代わりの方法として、電源をオフにし、再びオンにします)。
5. 再起動が開始した後、端末画面をよく見てください。再起動中にファンクション キーのリストが画面右上に表示されたとき、**F11 を押します。** 次に下記のいずれかを選択します。
   - **Boot from SATA Optical** drive (V10000 G2) (SATA Optical ドライブから起動する)
   - **Boot from Embedded SATA 1 TEAC DVD-ROM DV-28SW** drive (V5000 G2) (組み込みの SATA 1 TEAC DVD-ROM DV-28SW ドライブから起動する)
   - **Boot from Primary CDROM:TEAC DVD-ROM DV-28SW** drive (V5000 G2R2) (一次 CDROM:TEAC DVD-ROM DV-28SW ドライブから起動する)
6. 続行するかどうかを尋ねられたとき、「**yes**」と入力します。

   イメージの復元には 20 分以上かかることがあります。DVD を取り出すとき、必ずそれをドライブから削除してください。
7. いずれかのキーを押して、ライセンス契約を表示します。
8. 「**yes**」と入力してライセンス契約を承諾し、次に「**yes**」と入力して firstboot を開始します。

   firstboot スクリプトが開始します。
9. 画面の手順に従って、必要な情報を入力してください。

   要求される情報の詳細については、*コマンド ラインの初期設定の実行* を参照してください。

バックアップ設定を復元

1. バックアップ設定を Appliance Manager を通じて復元します。
   a. Web ブラウザを使用して、下記の Appliance Manager にログオンします。

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

   b. 「**Administration**」> 「**Backup Utility**」に進みます。
   c. **[Restore (復元)]** を選択します。
2. **[(Full Appliance Configuration (完全なアプライアンス設定)]** 復元モードを選択し、**[Run Restore Wizard (復元ウィザードを実行)]** をクリックします。
3. 復元ウィザードには下記の項目が表示されます。

a. File Location (ファイルの場所): **[Another location (browse for file) (他の場所 (ファイルを参照))]** を選択します。**[次]** をクリックします。

b. Select File (ファイルを選択): バックアップ ファイル (*.bak ファイル) を**参照**し、ファイルを選択します。**[次]** をクリックします。

c. Confirm (確認) : バックアップ ファイルの詳細情報を確認して、**[Restore Now (直ちに復元)]** をクリックします。

復元が完了した後、アプライアンスは自動的に再起動します。アプライアンスおよびソフトウェア モジュールの設定が復元されます。

4. アプライアンスの日付と時刻が他のサーバーと同期化していることを確認してください。
5. アプライアンス外で実行するコンポーネントを再起動します。
6. 場合によっては、復元の後、Websense Web Security Master Database の手動のダウンロードを開始する必要があります。Master Database に関する警告メッセージを受け取った場合に、TRITON Unified Security Center (Web Security モジュール) でその作業を行います。