# Web セキュリティ アプライアンスの管理

この章は、次の項で構成されています。



## 中央集中型コンフィギュレーション管理について

中央集中型コンフィギュレーション管理を使用すると、Cisco コンテンツ セキュリティ管理アプライアンスから最大 150 の関連する Web セキュリティ アプライアンスに設定を公開できるようになり、次のような利点が得られます。

- Web セキュリティ ポリシーの設定や設定の更新を個々の Web セキュリティ アプライアンスではなくセキュリティ管理アプライアンスで一度行うだけで済み、管理を簡便化および迅速化できます。
- 展開されているネットワーク全体で、ポリシーを均一に適用できます。

設定を Web セキュリティ アプライアンスに公開するには、次の 2 つの方法があります。

- Configuration Master を使用する
- Web セキュリティ アプライアンスからの設定ファイルを使用する（拡張ファイル公開の使用）

# 適切な設定公開方式の決定

セキュリティ管理アプライアンスから設定を公開するには異なる2つの方法があり、それぞれ異なる設定を公開します。設定の中には中央集中型で管理できないものもあります。

| 設定の対象 | 操作手順 |
|---|---|
| Web セキュリティ アプライアンスの [Webセキュリティマネージャ（Web Security Manager）] メニューに表示される機能。ポリシーやカスタム URL のカテゴリなど。<br>例外：L4 トラフィック モニタの（L4TM）の設定は、Configuration Master の対象に含まれません。<br>サポートの対象となる機能は、Configuration Master のバージョンによって変わります。このバージョンは AsyncOS for Web Security のバージョンに対応します。 | Configuration Master を公開します。<br>設定マスターで設定できる機能の多くは、動作させるために、Web セキュリティ アプライアンスでも直接設定する必要があります。たとえば、SOCKS ポリシーは設定マスターで設定可能ですが、最初に SOCKS プロキシを Web セキュリティ アプライアンスで直接設定する必要があります。 |
| **注**：Cisco Identity Services Engine（ISE）との統合は、各 Web セキュリティ アプライアンスで個別に設定する必要があります。Cisco Identity Services Engine の設定は、Cisco コンテンツ セキュリティ管理アプライアンスから発行できません。 | 拡張ファイル公開を使用します。 |
| 連邦情報処理標準の FIPS モード、ネットワーク/インターフェイス設定、DNS、Web Cache Communication Protocol（WCCP）、アップストリーム プロキシ グループ、証明書、プロキシ モード、NTP などの時間設定、L4 トラフィック モニタ（L4TM）設定、および認証リダイレクト ホスト名。 | 管理対象 Web セキュリティ アプライアンスで直接設定します。<br>『AsyncOS for Cisco Web Security Appliances ユーザ ガイド』を参照 |

# 中央集中型で Web Security Appliances を管理する Configuration Master の設定

WSA：未使用のマシンを設定するには、コンフィギュレーション ファイルや Configuration Master を使用する前（SSW の後）に何を設定する必要がありますか? コンフィギュレーション ファイルを使用すると、IP アドレスの問題が発生しませんか? 複数のマシンの WSA から同じコンフィギュレーション ファイルを使用するのではなく、SMA からコンフィギュレーション ファイルを公開すればこの問題は発生しない可能性があります。

| 対象アプライアンス | 操作手順 | 追加情報 |
|---|---|---|
| — | 設定のための一般的な要件や注意事項を確認します。 | Configuration Master を使用するための重要な注意事項 （4 ページ）を参照してください。 |
| — | 各 Web セキュリティ アプライアンスで使用する設定マスターのバージョンを確認します。 | 使用する Configuration Master のバージョンの確認 （4 ページ）を参照してください。 |
| Web セキュリティ アプライアンス | すべてのターゲット Web セキュリティ アプライアンスで、セキュリティ管理アプライアンスの設定マスターで設定するポリシーおよびその他の設定をサポートするために必要な機能を有効にし、設定します。 | — |
| Web セキュリティ アプライアンス | （**オプション**）すべての Web セキュリティ アプライアンスの設定モデルとして機能できる実行中の Web セキュリティ アプライアンスがある場合、Web セキュリティ アプライアンスからの設定ファイルを使用して、セキュリティ管理アプライアンスの設定マスターを迅速に設定できます。 | Web セキュリティ アプライアンスから設定ファイルをダウンロードする方法については、『AsyncOS for Cisco Web Security Appliances User Guide』の「Saving and Loading the Appliance Configuration」を参照してください。 |
| セキュリティ管理アプライアンス | 集約設定管理を有効化し、設定します。 | セキュリティ管理アプライアンスでの中央集中型コンフィギュレーション管理の有効化 （5 ページ）を参照してください。 |
| セキュリティ管理アプライアンス | Configuration Master を初期化します。 | 設定マスターの初期化と設定 （5 ページ）を参照してください。 |
| セキュリティ管理アプライアンス | Web セキュリティ アプライアンスを設定マスターに関連付けます。 | Web Security Appliances と Configuration Master の関連付けについて （6 ページ）を参照してください。 |
| セキュリティ管理アプライアンス | ポリシー、カスタム URL カテゴリ、および Web プロキシ バイパス リストを Configuration Master にインポートするか、手動で設定します。 | 公開のための設定 （8 ページ）を参照してください |

| 対象アプライアンス | 操作手順 | 追加情報 |
|---|---|---|
| セキュリティ管理アプライアンス | それぞれの Web セキュリティ アプライアンスで有効にされている機能が、そのアプライアンスに割り当てられている設定マスターで有効化されている機能と一致していることを確認します。 | 機能が常に有効化されていることの確認 （12 ページ）を参照してください。 |
| セキュリティ管理アプライアンス | 必要とする設定マスターを設定し、必要な機能を有効にしたら、Web セキュリティ アプライアンスに設定を公開します。 | Configuration Master の公開 （15 ページ）を参照してください。 |
| セキュリティ管理アプライアンス | 既存の Configuration Master 設定が変更される可能性がある、URL カテゴリ セットの更新のために事前に準備します。 | URL カテゴリ セットの更新の準備および管理 （29 ページ） |

# Configuration Master を使用するための重要な注意事項

（注） 中央集中型で管理する Web セキュリティ アプライアンスのそれぞれについて、同名のレルムに対する設定が同一である場合を除いて、[ネットワーク（Network）]>[認証（Authentication）] ですべての [レルム名（Realm Names）] がアプライアンス全体で一意になっていることを確認します。

# 使用する Configuration Master のバージョンの確認

セキュリティ管理アプライアンスには複数の設定マスターがあるため、異なる機能をサポートするさまざまなバージョンの AsyncOS for Web Security を実行する Web セキュリティ アプライアンスを中央集中型で管理できます。

それぞれの Configuration Master には、AsyncOS for Web Security の特定のバージョンで使用する設定が行われています。

お使いの AsyncOS for Web Security のバージョンで使用できる設定マスターを判断するには、互換性マトリクス（http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html）を参照してください。

（注） 互換性マトリクスに示されているように、設定マスターのバージョンが、Web セキュリティ アプライアンスの AsyncOS のバージョンと一致している必要があります。古いバージョンの設定マスターから新しいバージョンの Web セキュリティ アプライアンスに対して公開を行うと、Web セキュリティ アプライアンスの設定が設定マスターの設定と一致していない場合には、処理に失敗するおそれがあります。この問題は、[Webアプライアンスステータスの詳細（Web Appliance Status Details）] ページに不一致が見られない場合でも発生することがあります。この場合は、各アプライアンスでの設定を手動で比較する必要があります。

## セキュリティ管理アプライアンスでの中央集中型コンフィギュレーション管理の有効化

**ステップ 1** セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）]>[集約管理サービス（Centralized Services）]>[集中型設定マネージャ（Centralized Configuration Manager）] を選択します。

**ステップ 2** [有効（Enable）] をクリックします。

**ステップ 3** システムセットアップ ウィザードを実行してから初めて集約設定管理を有効にする場合は、エンドユーザライセンス契約書を確認し、[承認（Accept）] をクリックします。

**ステップ 4** 変更を送信し、保存します。

# 設定マスターの初期化と設定



## Configuration Master の初期化

注：設定マスターを初期化すると、[初期化（Initialize）] オプションは使用できなくなります。その代わりに、公開のための設定 （8 ページ） で説明されている方法のいずれかを使用して設定マスターを設定します。

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ（Web）]>[ユーティリティ（Utilities）]>[設定マスター（Configuration Masters）] を選択します。

**ステップ 2** [オプション（Options）] 列の [初期化（Initialize）] をクリックします。

**ステップ 3** [Configuration Masterの初期化（Initialize Configuration Master）] ページで、次の手順を実行します。

- 以前のリリース用の Configuration Master がすでにあり、新しい Configuration Master で同じ設定を適用したい場合は、[Configuration Masterのコピー（Copy Configuration Master）] を選択します。また、この後の作業で、既存の Configuration Master から設定をインポートすることもできます。
- 上記に該当しない場合は、[デフォルト設定を使用（Use default settings）] を選択します。

**ステップ 4** [初期化（Initialize）] をクリックします。

これで Configuration Master が使用可能な状態になります。

**ステップ 5** それぞれの Configuration Master のバージョンに対して初期化作業を繰り返します。

# Web Security Appliances と Configuration Master の関連付けについて

Web セキュリティのバージョンと Configuration Master の互換性については、使用する Configuration Master のバージョンの確認 （4 ページ）を参照してください。

Configuration Master にアプライアンスを追加する最も簡単な方法は、状況に応じて異なります。

| 条件（IF） | 参照する手順 |
|---|---|
| Web セキュリティ アプライアンスをセキュリティ管理アプライアンスにまだ追加していません。 | Web Security Appliances の追加と Configuration Master のバージョンとの関連付け （6 ページ） |
| Web セキュリティ アプライアンスを追加済みです。 | Configuration Master のバージョンと Web Security Appliance との関連付け （7 ページ） |

## Web Security Appliances の追加と Configuration Master のバージョンとの関連付け

まだ Web セキュリティ アプライアンスを中央集中管理の対象に追加していない場合は、この手順を実行してください。

### 始める前に

まだ追加していない場合は、各 Web セキュリティ アプライアンスに適した Configuration Master のバージョンを選択してください。使用する Configuration Master のバージョンの確認 （4 ページ）を参照してください。

**ステップ 1** セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）]>[集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] を選択します。

**ステップ 2** [Webアプライアンスの追加（Add Web Appliance）] をクリックします。

**ステップ 3** [アプライアンス名（Appliance Name）] および [IPアドレス（IP Address）] テキスト フィールドに、Web セキュリティ アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスまたは変換可能なホスト名を入力します。

（注） [IP アドレス（IP Address）] フィールドに DNS 名を入力した場合でも、[送信（Submit）] をクリックすると、IP アドレスに変換されます。

**ステップ 4** Centralized Configuration Manager サービスが事前に選択されています。

**ステップ 5** [接続の確立（Establish Connection）] をクリックします。

**ステップ 6** 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立（Establish Connection）] をクリックします。

（注） ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモート アプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は Security Management Appliance に保存されません。

**ステップ 7** 「Success」 メッセージがページのテーブルの上に表示されるまで待機します。

**ステップ 8** アプライアンスに関連付ける Configuration Master のバージョンを選択します。

**ステップ 9** 変更を送信し、保存します。

**ステップ 10** 中央集中型コンフィギュレーション管理をイネーブルにする Web Security Appliance ごとに、この手順を繰り返します。

## Configuration Master のバージョンと Web Security Appliance との関連付け

Web セキュリティ アプライアンスをセキュリティ管理アプライアンスにすでに追加している場合、次の手順を使用して、Web セキュリティ アプライアンスと設定マスター バージョンをすぐに関連付けることができます。

### 始める前に

まだ追加していない場合は、各 Web セキュリティ アプライアンスに適した Configuration Master のバージョンを選択してください。使用する Configuration Master のバージョンの確認 （4 ページ）を参照してください。

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ（Web）] > [ユーティリティ（Utilities）] > [設定マスター（Configuration Masters）] を選択します。

（注） Configuration Master が [無効（Disabled）] と表示されている場合にイネーブルにするには、[ウェブ（Web）]>[ユーティリティ（Utilities）]>[セキュリティサービス表示（Security Services Display）] の順にクリックし、次に [表示設定の編集（Edit Display Settings）] をクリックします。対象とする Configuration Master のチェックボックスを選択して、イネーブルにします。詳細については、公開する機能の有効化 （13 ページ）を参照してください。

**ステップ 2** [アプライアンス割り当てリストの編集（Edit Appliance Assignment List）] をクリックします。

**ステップ 3** 関連付けるアプライアンスの行でクリックし、[マスター（Masters）] 列にチェックマークを入れます。

**ステップ 4** 変更を送信し、保存します。

# 公開のための設定

公開する設定を Configuration Master に設定します。

Configuration Master の設定には、いくつかの方法があります。

| 条件（IF） | 操作手順 |
|---|---|
| AsyncOS for Security Management の以前のリリースからアップグレードする場合<br>および<br>新しい Configuration Master のバージョンを初期化（以前の既存の Configuration Master を新しいバージョンにコピー）していない場合 | 古いバージョンをインポートします。既存の Configuration Master からのインポート （8 ページ）を参照してください。 |
| Web セキュリティ アプライアンスを設定済みで、同じ設定を複数の Web セキュリティ アプライアンスで使用する場合 | その Web セキュリティ アプライアンスから保存したコンフィギュレーション ファイルを Configuration Master にインポートします<br>（中央集中型で Web Security Appliances を管理する Configuration Master の設定 （2 ページ）でコンフィギュレーション ファイルを保存した場合）。<br>インポートの手順については、Web セキュリティ アプライアンスからの設定のインポート （9 ページ）を参照してください。 |
| インポートした設定を変更する必要がある場合 | 設定マスターでの Web セキュリティ機能の直接設定 （10 ページ）を参照してください。 |
| ポリシー設定、URL カテゴリ、バイパス設定を Web セキュリティ アプライアンスでまだ設定していない場合 | これらの設定をセキュリティ管理アプライアンスの該当する Configuration Master に直接設定します。<br>設定マスターでの Web セキュリティ機能の直接設定 （10 ページ）を参照してください。 |

## 既存の Configuration Master からのインポート

既存の Configuration Master を新しい Configuration Master のバージョンにアップグレードすることができます。

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ（Web）] > [ユーティリティ（Utilities）] > [設定マスター（Configuration Masters）] を選択します。

**ステップ 2** [オプション（Options）] 列で、[設定のインポート（Import Configuration）] をクリックします。

**ステップ 3** [設定ソースの選択（Select Configuration Source）] で、リストから [設定マスター（Configuration Master）] を選択します。

**ステップ 4** この設定に、既存のカスタム ユーザ ロールを取り込むかどうかを選択します。

**ステップ 5** [インポート（Import）] をクリックします。

### 次のタスク

Custom Web User ロールについて

## Web セキュリティ アプライアンスからの設定のインポート

Webセキュリティ アプライアンスで機能している既存の設定を使用する場合は、そのコンフィギュレーションファイルをセキュリティ管理アプライアンスにインポートして、設定マスターにポリシー設定を作成できます。

### 始める前に

コンフィギュレーション ファイルと Configuration Master のバージョンの互換性を確認してください。使用する Configuration Master のバージョンの確認 （4 ページ）を参照してください。

**注意** 管理対象の Web セキュリティ アプライアンスに設定をすでに公開してある場合でも、互換性のある Web コンフィギュレーション ファイルを何回でもインポートすることができます。コンフィギュレーションファイルを設定マスターにインポートすると、選択した設定マスターに関連付けられている設定が上書きされます。また、[セキュリティサービス表示（Security Services Display）] ページのセキュリティ サービスの設定は、インポートしたファイルと一致するよう設定されます。

**（注）** セキュリティ管理アプライアンスより古い URL カテゴリ セットを使用するコンフィギュレーション ファイルをインポートしようとすると、ロードに失敗します。

**ステップ 1** Web セキュリティ アプライアンスのコンフィギュレーション ファイルを保存します。

**ステップ 2** セキュリティ管理アプライアンスで、[ウェブ（Web）] > [ユーティリティ（Utilities）] > [設定マスター（Configuration Masters）] を選択します。

**ステップ 3** [オプション（Options）] 列で、[設定のインポート（Import Configuration）] をクリックします。

**ステップ 4** [設定の選択（Select Configuration）] ドロップダウン リストから、[Web設定ファイル（Web Configuration File）] を選択します。

**ステップ 5** [新しいマスターのデフォルト（New Master Defaults）] セクションで、[参照（Browse）] をクリックし、Web セキュリティ アプライアンスから有効なコンフィギュレーション ファイルを選択します。

**ステップ 6** [ファイルのインポート（Import File）] をクリックします。

**ステップ 7** [インポート（Import）] をクリックします。

## 設定マスターでの Web セキュリティ機能の直接設定

設定マスターでは、バージョンに応じて次の機能を設定できます。

| | | |
|---|---|---|
| • ID/識別プロファイル<br>• SaaS ポリシー<br>• 復号ポリシー（Decryption Policies）<br>• ルーティング ポリシー<br>• アクセス ポリシー<br>• 全体の帯域幅の制限（Overall Bandwidth Limits） | • Cisco データ セキュリティ<br>• 発信マルウェアスキャン（Outbound Malware Scanning）<br>• 外部データ消失防止 | • SOCKS ポリシー（SOCKS Policies）<br>• カスタム URL カテゴリ<br>• 定義されている時間範囲とクォータ<br>• バイパス設定<br>• L4 トラフィック モニタ（L4 Traffic Monitor） |

設定マスターで各機能を直接設定するには、[Web] > [設定マスター（Configuration Master）] <version> > <feature> を選択します。

設定マスターで機能を設定する場合の SMA 特有の違い （10 ページ）で説明する一部の項目を除いて、設定マスターで機能を設定する方法は、Web セキュリティ アプライアンスで同じ機能を設定する場合と同じです。各説明については、ご使用の Web セキュリティ アプライアンスのオンライン ヘルプ、または設定マスターのバージョンに対応する AsyncOS バージョンの『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。必要な場合は、使用する Configuration Master のバージョンの確認 （4 ページ）を参照して、使用している Web セキュリティ アプライアンスに対応する正しい設定マスターを判別してください。

Web セキュリティ ユーザ ガイドは、http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html ですべてのバージョンを入手できます。

### 設定マスターで機能を設定する場合の SMA 特有の違い

設定マスターで機能を設定するときには、以下で説明する Web セキュリティ アプライアンスで同じ機能を直接設定する場合との違いに注意してください。

**表 1 : 機能の設定 : *Configuration Master* と *Web Security Appliance* との違い**

| 機能またはページ | 詳細（Details） |
|---|---|
| すべての機能、特に各リリースでの新機能 | 設定マスターで設定する各機能について、セキュリティ管理アプライアンス で [Web]>[ユーティリティ（Utilities）]>[セキュリティサービス表示（Security Services Display）] にある機能を有効にする必要があります。詳細については、機能が常に有効化されていることの確認 （12 ページ）を参照してください。 |

| 機能またはページ | 詳細（Details） |
|---|---|
| ID（Identities）/識別プロファイル（Identification Profiles） | • Configuration Master で ID/識別プロファイルを使用する場合のヒント （12 ページ）を参照してください。<br>• トランスペアレント ユーザ ID をサポートする認証レルムがある Web セキュリティ アプライアンスが管理対象アプライアンスとして追加されている場合、ID/識別プロファイルの追加または編集時に [ユーザを透過的に識別（Identify Users Transparently）] オプションを使用できます。 |
| Cisco Identity Services Engine（ISE）を使用してユーザを識別するポリシー | セキュリティ グループ タグ（SGT）情報は、Web セキュリティ アプライアンスから約 5 分ごとに更新されます。管理アプライアンスは、ISE サーバと直接通信することはありません。<br>SGT のリストをオンデマンドで更新するには、[Web] > [ユーティリティ（Utilities）] > [Webアプライアンスステータス（Web Appliance Status）] を選択し、ISE サーバに接続されている Web セキュリティ アプライアンスをクリックして、[データの更新（Refresh Data）] をクリックします。他のアプライアンスについて必要に応じて繰り返します。<br>一般的な導入シナリオでは、会社には、すべての WSA が接続する ISE サーバは 1 台だけあります（これが ISE の本質です）。異なるデータを持つ複数の ISE サーバはサポートされません。 |
| [アクセスポリシー（Access Policies）] > [グループの編集（Edit Group）] | [ポリシーメンバの定義（Policy Member Definition）] セクションで [ID（Identities）]/[識別プロファイルおよびユーザ（Identification Profiles and Users）] オプションを設定する際、外部ディレクトリ サーバを使用している場合には以下が適用されます。<br>[グループの編集（Edit Group）] ページでグループを検索した場合、検索結果の最初の 500 項目しか表示されません。目的のグループが見つからない場合は、そのグループを [ディレクトリ（Directory）] 検索フィールドに入力して、[追加（Add）] ボタンをクリックすると、[承認済みグループ（Authorized Groups）] リストに追加することができます。 |
| [アクセスポリシー（Access Policies）] > [Webレピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）] | |
| SaaS ポリシー（SaaS Policies） | 認証オプションの [透過的なユーザ識別によって検出されたSaaSユーザにプロンプトを出力する（Prompt SaaS users who have been discovered by transparent user identification）] は、トランスペアレント ユーザ ID をサポートする認証レルムが設定された Web セキュリティ アプライアンスが管理対象アプライアンスとして追加されている場合のみ有効になります。 |

### Configuration Master で ID/識別プロファイルを使用する場合のヒント

セキュリティ管理アプライアンスで ID/識別プロファイルを作成する際には、特定のアプライアンスのみに適用されるオプションがあります。たとえば、セキュリティ管理アプライアンスを購入し、Web セキュリティ アプライアンスごとに作成された既存の Web セキュリティ アプライアンスのコンフィギュレーションとポリシーを保持する場合は、1 つのファイルをマシンにロードし、次に他のマシンから手動でポリシーを追加する必要があります。

これを実行するための方法の 1 つとして、各アプライアンスに ID/識別プロファイルのセットを作成し、これらの ID/識別プロファイルを参照するポリシーを設定する方法があります。セキュリティ管理アプライアンスが設定を公開すると、これらの ID/識別プロファイルと、ID/識別プロファイルを参照するポリシーは自動的に削除され、無効になります。この方法を使用すると、手動で何も設定する必要がありません。これは基本的に「アプライアンスごと」の ID/識別プロファイルです。

この方法の唯一の問題は、デフォルトのポリシーまたは ID/識別プロファイルが、サイト間で異なる場合です。たとえば、あるサイトではポリシーを「default allow with auth」に設定し、別のサイトでは「default deny」に設定している場合です。この場合、アプライアンスごとの ID/識別プロファイルとポリシーをデフォルトのすぐ上に作成する必要があります。基本的には独自の「デフォルト」ポリシーを作成します。

# 機能が常に有効化されていることの確認

Configuration Master を公開する前に、それが公開されることと、公開後に目的の機能がイネーブルになり、意図するように設定されていることを確認します。

このためには、次の両方を実行してください。

- イネーブルにされている機能の比較 （12 ページ）
- 公開する機能の有効化 （13 ページ）

（注） 異なる機能を持つ複数の Web セキュリティ アプライアンスが同じ設定マスターに割り当てられている場合は、各アプライアンスを別個に公開するようにし、公開前にこれらの手順を実行する必要があります。

## イネーブルにされている機能の比較

それぞれの Web セキュリティ アプライアンスで有効にされている機能が、そのアプライアンスに関連付けられている設定マスターで有効化されている機能と一致していることを確認します。

（注） 異なる機能を持つ複数の Web セキュリティ アプライアンスが同じ設定マスターに割り当てられている場合は、各アプライアンスを別個に公開するようにし、公開前にこのチェックを実行する必要があります。

**ステップ 1** セキュリティ管理アプライアンスで、[Web] > [ユーティリティ（Utilities）] > [Webアプライアンスステータス（Web Appliance Status）] を選択します。

**ステップ 2** 設定マスターを公開する Web セキュリティ アプライアンスの名前をクリックします。

**ステップ 3** [セキュリティサービス（Security Services）] テーブルまでスクロールします。

**ステップ 4** イネーブルにされているすべての機能の機能キーがアクティブで、期限切れでないことを確認します。

**ステップ 5** [サービス（Services）] 列の設定を比較します。

[Webアプライアンスサービス（Web Appliance Service）] 列と、[管理アプライアンス上でサービスを表示しますか?（Is Service Displayed on Management Appliance?）] 列が一致している必要があります。

- [有効化（Enable）] = [はい（Yes）]
- [無効（Disabled）] および [未設定（Not Configured）] = [いいえ（No）] または [無効（Disabled）]
- N/A = 適用されません。たとえば、そのオプションは Configuration Master で設定できませんが、一覧には表示されて、機能キーのステータスを確認することができます。

コンフィギュレーションの不一致は、赤色のテキストで表示されます。

### 次のタスク

ある機能についてのイネーブルおよびディセーブルの設定が一致していない場合は、次のいずれかを実行します。

- Configuration Master の対応する設定を変更します。公開する機能の有効化 （13 ページ）を参照してください。
- Web Security Appliance の当該の機能をイネーブルまたはディセーブルにします。変更内容によっては、複数の機能に影響が生じる場合があります。関連する機能については、『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。

## 公開する機能の有効化

Configuration Master を使用して設定を公開する機能をイネーブルにします。

### 始める前に

イネーブルにする機能とディセーブルにする機能を確認します。イネーブルにされている機能の比較 （12 ページ）を参照してください。

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ（Web）]>[ユーティリティ（Utilities）]>[セキュリティ サービス表示（Security Services Display）] を選択します。

**ステップ 2** [設定の編集（Edit Settings）] をクリックします。

[セキュリティサービス表示の編集（Edit Security Services Display）] ページに、各 Configuration Master に表示される機能が一覧されます。

横に [なし（N/A）] と表示されている機能は、その Configuration Master のバージョンで使用できないことを意味します。

（注） Web プロキシは機能として一覧されていません。これは、Web プロキシは Web セキュリティ アプライアンスで管理されているプロキシタイプのいずれかを実行するために有効になっていると見なされているためです。Web プロキシを無効にすると、Web セキュリティ アプライアンスに公開されたすべてのポリシーが無視されます。

**ステップ 3** （任意）使用しない Configuration Master は非表示にします。手順および注意については、使用しない Configuration Master のディセーブル化 （14 ページ）を参照してください。

**ステップ 4** 使用する各設定マスターについて、有効にする各機能に対する [はい（Yes）] チェックボックスを選択または選択解除します。

次の特定機能には特に注意してください（使用可能なオプションは、Configuration Master のバージョンによって異なります）。

- トランスペアレント モード。フォワード モードを使用した場合、プロキシ バイパス機能は使用できなくなります。
- HTTPS プロキシ。HTTPS プロキシは、復号ポリシーを実行するためにイネーブルにする必要があります。
- アップストリーム プロキシ グループ。ルーティング ポリシーを使用する場合は、Web セキュリティ アプライアンスでアップストリーム プロキシ グループが使用できるようになっている必要があります。

**ステップ 5** [送信（Submit）] をクリックします。セキュリティ サービスの設定に加えた変更が、Web セキュリティ アプライアンスで設定されたポリシーに影響する場合、GUI に特定の警告メッセージが表示されます。変更を送信することが確実な場合は、[続行（Continue）] をクリックします。

**ステップ 6** [セキュリティサービス表示（Security Services Display）] ページで、選択した各オプションの横に [はい（Yes）] と表示されることを確認します。

**ステップ 7** 変更を保存します。

---

### 次のタスク

- 公開先のアプライアンスに対して、すべての機能が正しく有効または無効になっていることを確認します。イネーブルにされている機能の比較 （12 ページ）を参照してください。
- 公開先の各 Web セキュリティ アプライアンスで、設定マスターに対して有効にした機能と一致する機能が有効になっていることを確認します。

# 使用しない Configuration Master のディセーブル化

使用しない Configuration Master を表示しないようにすることができます。

ただし、少なくとも 1 つの Configuration Master は有効にする必要があります。

（注） Configuration Master をディセーブルにすると、それに対するすべての参照が、対応する [設定マスター（Configuration Master）] タブを含めて GUI から削除されます。その Configuration Master を使用する保留中の公開ジョブは削除され、非表示の Configuration Master に割り当てられていたすべての Web セキュリティ アプライアンスが、割り当てられていないものとして再分類されます。

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ（Web）]>[ユーティリティ（Utilities）]>[セキュリティ サービス表示（Security Services Display）] を選択します。

**ステップ 2** [設定の編集（Edit Settings）] をクリックします。

**ステップ 3** 使用しない Configuration Master に対するチェックボックスを選択解除します。

**ステップ 4** 変更を送信し、保存します。

# 拡張ファイル公開を使用するための設定

システムで Configuration Master を使用するよう設定されている場合は、拡張ファイル公開に対する設定も行われています。

そうでない場合は、次の項で説明する手順を実行してください。これらは、拡張ファイル公開だけでなく、Configuration Master の公開にも適用されます。



# Web セキュリティ アプライアンスへの設定の公開



## Configuration Master の公開

Configuration Master で設定を編集またはインポートした後、その設定を、Configuration Master に関連付けられている Web セキュリティ アプライアンスへ公開できます。

## Configuration Master を公開する前に

Configuration Master を公開すると、その Configuration Master に関連付けられている Web セキュリティ アプライアンスの既存のポリシー情報が上書きされます。

Configuration Master を使用して設定できる設定の詳細については、適切な設定公開方式の決定（2 ページ）を参照してください。

すべての公開ジョブ

- 対象とする Web セキュリティ アプライアンスの AsyncOS バージョンは、Configuration Master のバージョンと同じであるか、または次で互換性が確認されているバージョンである必要があります。 SMA 互換性マトリクス
- （初回のみ）中央集中型で Web Security Appliances を管理する Configuration Master の設定（2 ページ）で説明する手順に従います。
- Configuration Master を公開し、公開後に意図する機能がイネーブルになるようにするには、各 Web セキュリティ アプライアンスと、これに対応する Configuration Master の機能を確認し、必要に応じて変更を加えます。イネーブルにされている機能の比較 （12 ページ）、および必要に応じて公開する機能の有効化 （13 ページ）を参照してください。ターゲットアプライアンスで有効にされていない機能の設定を公開しても、これらの設定は適用されません。

同じ Configuration Master に割り当てられている複数の Web セキュリティ アプライアンスで異なる機能が有効になっている場合は、各アプライアンスに個別に公開する必要があります。それぞれの公開前に機能が有効になっていることを確認してください。

公開中に検出された設定の不一致を特定するには、公開履歴の表示 （22 ページ）を参照してください。

- 公開前に、対象とする各 Web セキュリティ アプライアンスからコンフィギュレーションファイルを保存して、公開された設定によって問題が生じた場合に既存の設定を復元できるようにしておきます。詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。
- Web セキュリティ アプライアンスでコミットしたときに Web プロキシの再起動が必要になる変更内容は、それをセキュリティ管理アプライアンスから公開したときにもプロキシの再起動が必要になります。この場合は、警告が発生します。

Web プロキシの再起動により、Web セキュリティ サービスは一時的に中断されます。Web プロキシの再起動による影響の詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』の「Checking for Web Proxy Restart on Commit」を参照してください。

- ID/識別プロファイルに対する変更を公開すると、すべてのエンドユーザが再認証を受ける必要が生じます。

特殊な状況

- 対象の Web セキュリティ アプライアンスで AsyncOS を復元した場合は、そのアプライアンスを異なる Configuration Master と関連付けなければならない場合があります。
- Configuration Master を、トランスペアレント ユーザ ID が有効化されたレルムを持たない Web セキュリティ アプライアンスに公開したものの、[ID（Identity）]/[識別プロファイル

（Identification Profile）] または [SaaSポリシー（SaaS Policy）] でトランスペアレント ユーザ ID を選択していると、次のようになります。

- [ID（Identity）]/[識別プロファイル（Identification Profiles）] の場合、トランスペアレント ユーザ ID は無効になり、代わりに [認証が必要（Require Authentication）] オプションが選択されます。
- [SaaSポリシー（SaaS Policies）] の場合、トランスペアレント ユーザ ID のオプションは無効になり、代わりにデフォルトのオプション（SaaS ユーザに対して常にプロキシ認証を要求）が選択されます。

- RSA サーバ用に設定されていない複数の Web セキュリティ アプライアンスにセキュリティ管理アプライアンスから外部 DLP ポリシーを公開すると、セキュリティ管理アプライアンスによって次の公開ステータス警告が送信されます。

「**The Security Services display settings configured for Configuration Master** <*version*> **do not currently reflect the state of one or more Security Services on Web Appliances associated with this publish request. The affected appliances are: "<***WSA Appliance Names***>". This may indicate a misconfiguration of the Security Services display settings for this particular Configuration Master. Go to the Web Appliance Status page for each appliance provides a detailed view to troubleshooting this issue. Do you want to continue publishing the configuration now?**」

公開を続行した場合、RSA サーバ用に設定されていない Web セキュリティ アプライアンスは、外部 DLP ポリシーを受信しますが、これらのポリシーはディセーブルにされます。外部 DLP サーバが設定されていない場合、Web セキュリティ アプライアンスの [外部DLP（External DLP）] ページには公開されたポリシーが表示されません。

| Configuration Master の ID/識別プロファイルのスキーム | Web Security Appliance の ID/識別プロファイル |
|---|---|
| Kerberos 認証を使用 | NTLMSSP 認証または Basic 認証を使用 |
| Kerberos 認証または NTLMSSP 認証を使用 | NTLMSSP 認証を使用 |
| Kerberos 認証、NTLMSSP 認証、または Basic 認証を使用 | NTLMSSP 認証または Basic 認証を使用 |

## Configuration Master の公開

**始める前に**

Configuration Master を公開する前に （16 ページ）の重要な要件と情報を参照してください。

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ（Web）] > [ユーティリティ（Utilities）] > [Webアプライアンスへの公開（Publish to Web Appliances）] を選択します。

**ステップ 2** [今すぐ設定を公開する（Publish Configuration Now）] をクリックします。

**ステップ 3** デフォルトでは [システム生成のジョブ名（System-generated job name）] が選択されています。あるいは、ユーザ定義のジョブ名（80 文字以下）を入力します。

**ステップ 4** 公開する Configuration Master を選択します。

**ステップ 5** Configuration Master の公開先となる Web セキュリティ アプライアンスを選択します。Configuration Master に割り当てられているすべてのアプライアンスに設定を公開するには、[割り当てられたすべてのアプライアンス（All assigned appliances）] を選択します。

または

[リスト内のアプライアンスを選択してください（Select appliances in list）] を選択して、Configuration Master に割り当てられているアプライアンスの一覧を表示します。設定の公開先となるアプライアンスを選択します。

**ステップ 6** [公開（Publish）] をクリックします。

[公開中（Publish in Progress）] ページに表示される赤色の経過表示バーとテキストは、公開中にエラーが発生したことを表します。別のジョブが現在公開中の場合、要求は前のジョブが完了すると実行されます。

（注） 進行中のジョブの詳細は、[ウェブ（Web）] > [ユーティリティ（Utilities）] > [Webアプライアンスへの公開（Publish to Web Appliances）] ページにも表示されます。[公開中（Publish in Progress）] にアクセスするには、[進捗ステータスの確認（Check Progress）] をクリックします。

---

**次のタスク**

公開が正しく完了したことを確認します。公開履歴の表示（22ページ）を参照してください。完全に公開されなかった項目が表示されます。

## Configuration Master を後日公開

**始める前に**

Configuration Master を公開する前に （16 ページ）の重要な要件と情報を参照してください。

---

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ（Web）] > [ユーティリティ（Utilities）] > [Webアプライアンスへの公開（Publish to Web Appliances）] を選択します。

**ステップ 2** [ジョブをスケジュールする（Schedule a Job）] をクリックします。

**ステップ 3** デフォルトでは [システム生成のジョブ名（System-generated job name）] が選択されています。あるいは、ユーザ定義のジョブ名（80 文字以下）を入力します。

**ステップ 4** Configuration Master を公開する日時を入力します。

**ステップ 5** 公開する Configuration Master を選択します。

**ステップ 6** Configuration Master の公開先となる Web セキュリティ アプライアンスを選択します。Configuration Master に割り当てられているすべてのアプライアンスに設定を公開するには、[割り当てられたすべてのアプライアンス（All assigned appliances）] を選択します。

または

[リスト内のアプライアンスを選択してください（Select appliances in list）] を選択して、Configuration Master に割り当てられているアプライアンスの一覧を表示します。設定の公開先となるアプライアンスを選択します。

**ステップ 7** [送信（Submit）] をクリックします。

**ステップ 8** スケジュールされているジョブのリストは、[ウェブ（Web）] > [ユーティリティ（Utilities）] > [Webアプライアンスへの公開（Publish to Web Appliances）] ページに表示されます。スケジュールされているジョブを編集するには、そのジョブの名前をクリックします。保留中のジョブをキャンセルするには、対応するごみ箱アイコンをクリックして、ジョブの削除を確認します。

**ステップ 9** スケジュールされた公開時刻の後に公開が正しく完了したことを確認するために、自分自身に対する覚え書きを（カレンダーなどに）作成することもできます。

（注） スケジュールされた公開ジョブが発生する前に、アプライアンスをリブートまたはアップグレードした場合は、ジョブを再度スケジュールする必要があります。

---

**次のタスク**

公開が正しく完了したことを確認します。公開履歴の表示 （22ページ）を参照してください。完全に公開されなかった項目が表示されます。

## コマンドライン インターフェイスによる Configuration Master の公開

（注） Configuration Master を公開する前に （16 ページ）の重要な要件と情報を参照してください。

セキュリティ管理アプライアンスでは、次の CLI コマンドを使用して Configuration Master から変更を公開できます。

**publishconfig config_master** [--*job_name*] [--*host_list* | *host_ip*]

**config_master** は、サポートされている Configuration Master のバージョンです。このキーワードは必須です。*job_name* オプションは省略可能で、指定しなかった場合は生成されます。

オプション *host_list* は、公開される Web セキュリティ アプライアンスのホスト名または IP アドレスのリストで、指定しなかった場合は、Configuration Master に割り当てられているすべてのホストに公開されます。*host_ip* オプションには、カンマで区切って複数のホスト IP アドレスを指定できます。

**publishconfig** コマンドが成功したことを確認するには、**smad_logs** ファイルを調べます。[ウェブ（Web）] > [ユーティリティ（Utilities）] > [Webアプライアンスステータス（Web Appliance Status）] を選択することで、セキュリティ管理アプライアンスの GUI から公開履歴が成功だったことを確認することもできます。このページから、公開履歴の詳細を調べる Web アプライアンスを選択します。また、[ウェブ（Web）]>[ユーティリティ（Utilities）]>[公開（Publish）] > [公開履歴（Publish History）] により、[公開履歴（Publish History）] ページに進むことができます。

# 拡張ファイル公開による設定の公開

拡張ファイル公開を使用して、互換性のある XML コンフィギュレーション ファイルを、ローカル ファイル システムから管理対象の Web セキュリティ アプライアンスにプッシュします。

拡張ファイル公開を使用して設定できる設定の詳細については、適切な設定公開方式の決定（2 ページ）を参照してください。

拡張ファイル公開を実行するには、次を参照してください。


- 拡張ファイル公開：[今すぐ設定を公開する（Publish Configuration Now）] （20 ページ）
- 拡張ファイル公開：[後日公開（Publish Later）] （21 ページ）


## 拡張ファイル公開：[今すぐ設定を公開する（Publish Configuration Now）]

### 始める前に

- 公開するコンフィギュレーション バージョンが、公開先アプライアンスの AsyncOS バージョンと互換性があることを確認します。互換性マトリクス（http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html）を参照してください。
- 各宛先の Web セキュリティ アプライアンスで、Web セキュリティ アプライアンスの既存の設定をコンフィギュレーション ファイルにバックアップします。詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。

**ステップ 1** 元となる Web セキュリティ アプライアンスから、コンフィギュレーション ファイルを保存します。

Web セキュリティ アプライアンスからコンフィギュレーション ファイルを保存する方法については、『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。

**ステップ 2** セキュリティ管理アプライアンスのウィンドウで、[ウェブ（Web）]>[ユーティリティ（Utilities）]>[Web アプライアンスへの公開（Publish to Web Appliances）] を選択します。

**ステップ 3** [今すぐ設定を公開する（Publish Configuration Now）] をクリックします。

**ステップ 4** デフォルトでは [システム生成のジョブ名（System-generated job name）] が選択されています。あるいはジョブ名（80 文字まで）を入力します。

**ステップ 5** [公開する設定マスター（Configuration Master to Publish）] で、[拡張ファイルオプション（Advanced file options）] を選択します。

**ステップ 6** [参照（Browse）] をクリックして、手順 1 で保存したファイルを選択します。

**ステップ 7** [Webアプライアンス（Web Appliances）] ドロップダウン リストから、[リスト内のアプライアンスを選択してください（Select appliances in list）] または [マスターに割り当てられたすべて（All assigned to Master）] を選択して、コンフィギュレーション ファイルの公開先となるアプライアンスを選択します。

**ステップ 8** [公開（Publish）] をクリックします。

## 拡張ファイル公開：[後日公開（Publish Later）]

**始める前に**

- 公開するコンフィギュレーション バージョンが、公開先アプライアンスの AsyncOS バージョンと互換性があることを確認します。互換性マトリクス（http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html）を参照してください。
- 各宛先の Web セキュリティ アプライアンスで、Web セキュリティ アプライアンスの既存の設定をコンフィギュレーション ファイルにバックアップします。詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。

**ステップ 1** 元となる Web セキュリティ アプライアンスから、コンフィギュレーション ファイルを保存します。

Web セキュリティ アプライアンスからコンフィギュレーション ファイルを保存する方法については、『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。

**ステップ 2** セキュリティ管理アプライアンスで、[ウェブ（Web）] > [ユーティリティ（Utilities）] > [Web アプライアンスへの公開（Publish to Web Appliances）] を選択します。

**ステップ 3** [ジョブをスケジュールする（Schedule a Job）] をクリックします。

**ステップ 4** デフォルトでは [システム生成のジョブ名（System-generated job name）] が選択されています。あるいはジョブ名（80 文字まで）を入力します。

**ステップ 5** 設定を公開する日時を入力します。

**ステップ 6** [公開する設定マスター（Configuration Master to Publish）] で、[拡張ファイル オプション（Advanced file options）] を選択し、次に [参照（Browse）] をクリックして、手順 1 で保存したコンフィギュレーション ファイルを選択します。

**ステップ 7** [Webアプライアンス（Web Appliances）] ドロップダウン リストから、[リスト内のアプライアンスを選択してください（Select appliances in list）] または [マスターに割り当てられたすべて（All assigned to Master）] を選択して、コンフィギュレーション ファイルの公開先となるアプライアンスを選択します。

**ステップ 8** [公開（Publish）] をクリックします。

# 公開ジョブのステータスと履歴の表示

| 目的 | 操作手順 |
|---|---|
| スケジュール済みで実行されていない公開ジョブのリスト | [ウェブ（Web）] > [ユーティリティ（Utilities）] > [Web アプライアンスへの公開（Publish to Web Appliances）] を選択し、[保留中のジョブ（Pending Jobs）] セクションを確認してください。 |

| 目的 | 操作手順 |
|---|---|
| 各アプライアンスで最後に公開された設定のリスト | [ウェブ（Web）] > [ユーティリティ（Utilities）] > [Web アプライアンスステータス（Web Appliance Status）] を選択し、[最新公開設定（Last Published Configuration）] の情報を参照してください。 |
| 現在進行中の公開ジョブのステータス | [ウェブ（Web）] > [ユーティリティ（Utilities）] > [Web アプライアンスへの公開（Publish to Web Appliances）] を選択し、[公開の進歩ステータス（Publishing Progress）] セクションを確認してください。 |
| すべてまたは一部のアプライアンスに対するすべてまたは一部の公開ジョブの履歴 | 公開履歴の表示 を参照してください。 |

## 公開履歴の表示

公開履歴を表示すると、公開中に発生した可能性があるエラーをチェックしたり、設定されている機能とターゲットアプライアンスで有効になっている機能の不一致を特定したりするのに役立ちます。

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ（Web）]>[ユーティリティ（Utilities）]>[公開履歴（Publish History）] を選択します。

**ステップ 2** 特定のジョブに関してさらに詳細を表示するには、[ジョブ名（Job Name）] 列で特定のジョブ名をクリックします。

**ステップ 3** 詳細を確認します。

- ジョブの特定のアプライアンスに関するステータスの詳細を表示するには、[詳細（Details）] リンクをクリックします。

[Webアプライアンス公開の詳細（Web Appliance Publish Details）] ページが表示されます。

- ジョブの特定のアプライアンスに関する詳細を表示するには、アプライアンス名をクリックします。

[ウェブ（Web）]>[ユーティリティ（Utilities）]>[Webアプライアンスステータス（Web Appliance Status）] ページが表示されます。

# 中央管理型アップグレード管理

単一のセキュリティ管理アプライアンス（SMA）を使用して、複数の Web セキュリティ アプライアンス（WSA）を同時にアップグレードすることができます。各 WSA に異なるソフトウェア アップグレードを適用することもできます。

# Webセキュリティアプライアンスのアップグレードの一元管理を設定

このセキュリティ管理アプライアンスの一元化されたアップグレード サービスを構成するには、次の手順を実行します。



## 一元管理アップグレード マネージャの有効化

### 始める前に

- アップグレードの一元管理を有効にする前に、すべての Web セキュリティ アプライアンスが設定され、想定どおりに動作している必要があります。
- 一元管理アップグレードを受信する Web セキュリティ アプライアンスごとに、個別に一元管理アップグレードを有効にする必要があります。

（注） CLI での一元管理アップグレードを有効にするには、次を使用します。

```
applianceconfig > services > [...] > Enable Centralized Upgrade
> Y
```

- 適切な機能キーがセキュリティ管理アプライアンスにインストールされていることを確認します。

**ステップ 1** セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] ページを選択し、さらに、[集約管理サービス（Centralized Services）]>[一元管理アップグレード マネージャ（Centralized Upgrade Manager）] を選択します。

**ステップ 2** [設定の編集（Edit Settings）] をクリックします。

**ステップ 3** [有効（Enable）] をオンにします。

**ステップ 4** 変更を送信し、保存します。

# 管理対象の各 Web セキュリティ アプライアンスへの一元管理アップグレード サービスの追加

セキュリティ管理アプライアンスで一元管理アップグレードマネージャを有効にした後、個々の管理対象 WSA で一元管理アップグレードを有効にして、アップグレード マネージャ名簿に必要な Web セキュリティ アプライアンスを追加する必要があります。

**ステップ 1** セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] ページを選択し、その後、[集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] を選択します。

**ステップ 2** Web セキュリティ アプライアンスをまだ追加していない場合、またはアップグレードの一元管理のためアプライアンスを追加する必要がある場合：

a) [Webアプライアンスの追加（Add Web Appliance）] をクリックします。

b) [アプライアンス名（Appliance Name）] および [IP アドレス（IP Address）] テキスト フィールドに、Web セキュリティ アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注） [IP アドレス（IP Address）] テキスト フィールドに DNS 名を入力した場合でも、[送信（Submit）] をクリックすると、IP アドレスに変換されます。

c) [一元管理アップグレード（Centralized Upgrades）] を確認してください。

d) [接続の確立（Establish Connection）] をクリックします。

e) 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立（Establish Connection）] をクリックします。

（注） ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモート アプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は Security Management Appliance に保存されません。

「Success」 メッセージがページのテーブルの上に表示されるまで待機します。

f) [Test Connection] をクリックします。

テーブルの上のテスト結果を確認します。

g) [送信（Submit）] をクリックします。

同時にアップグレードの一元管理を有効にしながら、管理対象の Web セキュリティ アプライアンスのリストに追加する WSA ごとに、この手順を繰り返します。

**ステップ 3** この管理対象アプライアンスのリストに既存の WSA でアップグレードの一元管理を有効にするには、次の手順を実行します。

a) Web セキュリティ アプライアンスの名前をクリックして、[Web セキュリティ アプライアンス設定の編集（Edit Web Security Appliance Settings）] ページを開きます。

b) [WSA 集約管理サービス（WSA Centralized Services）] セクションで、[一元管理アップグレード（Centralized Upgrades）] を選択します。

c) [送信（Submit）] をクリックします。

アップグレードの一元管理を有効にする WSA ごとに、この手順を繰り返します。

**ステップ 4** 変更を保存します。

### 次のタスク

管理対象アプライアンスのリストへの追加方法およびリストの編集方法の詳細については、管理対象アプライアンスの追加についてを参照してください。

## WSA アップグレードの選択とダウンロード

**ステップ 1** セキュリティ管理アプライアンスで、[Web] ページを選択し、[ユーティリティ（Utilities）]>[一元管理アップグレード（Centralized Upgrade）] を選択します。

アップグレード用に最近選択されたアプライアンスと、アップグレード ステータスがリストされます。

**ステップ 2** [一元管理アップグレード（Centralized Upgrade）] ページで [アプライアンスのアップグレード（Upgrade Appliances）] ボタンをクリックします。

アップグレードが可能なすべての管理対象 WSA がリストされます。

**ステップ 3** リストで名前の前にあるボックスをチェックして、アップグレードする各 Web セキュリティ アプライアンスを選択します。

**ステップ 4** [ダウンロード ウィザード（Download Wizard）] または [ダウンロードおよびインストール ウィザード（Download and Install Wizard）] のいずれかをクリックします。

ダウンロード ウィザードでは、選択した WSA にダウンロードするアップグレード パッケージを選択できます。この操作はダウンロード専用です。後から、各システムにダウンロードしたパッケージをインストールし、再起動できます。

ダウンロードおよびインストール ウィザードでは、ダウンロードするアップグレードパッケージと選択した WSA への即時インストールを選択できます。インストール後、各システムは自動的に再起動されます。

**ステップ 5** 起動したウィザードの [アップグレードの取得（Fetch Upgrades）] ページが表示されます。選択した WSA で利用可能なすべてのアップグレードが取得された場合は（WSA マトリックスの [ステータス（Status）] 列に「利用可能なアップグレードの取得が完了しました（Completed Fetching Available Upgrades）」と表示される）、[次へ（Next）] をクリックして続行します。

**ステップ 6** [利用可能なアップグレード（Available Upgrades）] ページでは、選択した WSA ごとに利用可能なアップグレード ビルドがすべてリストされます。比較用に最大 5 つまでを選択し、[次へ（Next）] をクリックします。

**ステップ 7** ウィザードの [アップグレードの選択（Upgrade Selection）] ページでは、WSA ごとに選択したアップグレードの互換性マトリックスが示されます。WSA ごとに目的のアップグレード ビルドをチェックし、[次へ（Next）] をクリックします。

**ステップ 8** [サマリ（Summary）] ページに、選択した WSA とアップグレード ビルドごとの概要情報がリストされます。[次へ（Next）] をクリックして、ウィザードを続行します。

**ステップ 9** WSA 接続ステータスなどの一連のダウンロード チェックに続き、[レビュー（Review）] ページで各 WSA のダウンロード ステータスのリストが提供されます。[ダウンロードの開始（Begin Download）] をクリックして、選択した各 WSA へアップグレード パッケージをダウンロードします。

[一元管理アップグレード（Centralized Upgrade）] ページには、プロセス全体を通じてダウンロード ステータス情報が表示されます。

---

**次のタスク**

- [ダウンロード ウィザード（Download Wizard）] - この手順の初めにこのボタンをクリックした場合は、ダウンロードの完了時に、[Web] > [ユーティリティ（Utilities）] > [一元管理アップグレード（Centralized Upgrade）] を選択するか、またはブラウザ ウィンドウのページ更新ボタンをクリックすることで、[一元管理アップグレード（Centralized Upgrade）] ページを更新します。

  アップグレード可能なすべての管理対象 WSA のリストに加え、[一元管理アップグレード（Centralized Upgrade）] ページの別のセクションではアップグレード パッケージがダウンロードされているすべての WSA がリストされます（エントリごとに表示されているゴミ箱ボタンをクリックすると、その WSA からダウンロードされたアップグレード パッケージを削除できます）。

  いつでも、このリストで 1 つまたは複数の WSA を選択し、その後、[インストール ウィザード（Install Wizard）] をクリックして、ダウンロードされたアップグレード パッケージの選択した各 WSA へのインストールを開始できます。WSA でインストールが完了すると、それが再起動されます。このウィザードの使用方法の詳細についてはインストール ウィザードの使用 （26 ページ）を参照してください。

- [ダウンロードおよびインストール ウィザード（Download and Install Wizard）] - この手順の初めにこのボタンをクリックした場合は、ダウンロードの完了時に、アップグレードのインストールが自動的に始まります。このプロセスの詳細については、インストール ウィザードの使用 （26 ページ）のステップ 2 以降を参照してください。インストールが完了すると、WSA が再起動します。

# インストール ウィザードの使用

ダウンロードおよびインストールプロセスの一部として自動的に行うかどうかに関係なくインストール ウィザードを開始する場合、またはアップグレード パッケージがダウンロードされたが、まだインストールされていない 1 つ以上の WSA を選択後 [一元管理アップグレード（Centralized Upgrade）] ページで [インストール ウィザード（Install Wizard）] ボタンをクリックした場合は、次の手順に従ってインストールを設定します。

---

**ステップ 1** 以前にダウンロードしたアップグレード パッケージをインストールする場合：

a) [一元管理アップグレード（Centralized Upgrade）] ページの [ダウンロードした AsyncOS バージョンの Web アプライアンス（Web Appliances with Downloaded AsyncOS Versions）] セクションで目的の WSA

を選択します（[Web] > [ユーティリティ（Utilities）] > [一元管理アップグレード（Centralized Upgrade）]）。

b) [インストール ウィザード（Install Wizard）] をクリックします。

**ステップ 2** ウィザードの [アップグレードの準備（Upgrade Preparation）] ページで、選択した WSA ごとに次を実行します。

- WSA の現在の設定のバックアップ コピーをそのシステムの `configuration` ディレクトリに保存する場合は、[アップグレードする前に現在の設定を configuration ディレクトリに保存する（Save the current configuration to the configuration directory before upgrading）] をオンにします。
- [現在の設定を保存（Save current configuration）] オプションがオンになっている場合、[設定ファイル内のパスワードを隠す（Mask **passwords** in the configuration file）] をオンにしてバックアップ コピー内の現在のすべての構成パスワードをマスクすることができます。[設定のロード（Load Configuration）] コマンドは、マスク付きパスワードを使用したバックアップ ファイルの再ロードには使用できない点に注意してください。
- [現在の設定を保存（Save current configuration）] オプションがオンになっている場合、[ファイルをメールで送信（Email file to）] フィールドに 1 つ以上の電子メール アドレスを入力できます。入力した各アドレスに、バックアップ設定ファイルのコピーが電子メールで送信されます。カンマで複数のアドレスを区切ります。

**ステップ 3** [Next] をクリックします。

**ステップ 4** [アップグレードの概要（Upgrade Summary）] ページには、選択した各 WSA のアップグレードの準備情報がリストされます。[次へ（Next）] をクリックして、ウィザードを続行します。

**ステップ 5** 接続ステータスなどの一連のデバイス チェックに続き、[レビュー（Review）] ページで各 WSA のインストール ステータスのリストが提供されます。エラーが表示されているデバイスを選択解除できます。[インストールの開始（Begin Install）] をクリックして、選択した各 WSA へのアップグレード パッケージのインストールを開始します。

インストール ステータス情報が表示された [一元管理アップグレード（Centralized Upgrade）] ページに戻ります。

（注） 各 WSA は、インストールの完了時に再起動されます。

---

### 次のタスク

（注） また、WSA 自体から以前にダウンロードしたパッケージのインストーラを実行することもできます。つまり、ダウンロードされたアップグレード パッケージは、WSA 上の [システム管理（System Administration）] > [システム アップグレード（System Upgrade）] ページに [インストール（Install）] ボタンとともにリストされます。詳細については、『Cisco Web Security Appliances ユーザ ガイド』の AsyncOS とセキュリティ サービス コンポーネントのアップグレードおよび更新に関する説明を参照してください。

# Web セキュリティ アプライアンスのステータスの表示



## Web アプライアンス ステータスの概要の表示

[ウェブ（Web）] > [ユーティリティ（Utilities）] > [Web アプライアンス ステータス（Web Appliance Status）] ページは、セキュリティ管理アプライアンスに接続されている Web セキュリティ アプライアンスの概要を提供します。

[Web アプライアンス ステータス（Web Appliance Status）] ページには、接続されている Web セキュリティアプライアンスのリストが、アプライアンス名、IP アドレス、AsyncOS バージョン、最後に公開された設定情報（ユーザ、ジョブ名、コンフィギュレーションバージョン）、使用可能または使用不可にされているセキュリティサービスの数、および接続しているアプライアンスの総数（最大 150）とともに表示されます。警告アイコンは、接続されたアプライアンスの 1 つに注意が必要なことを示しています。

## 個々の Web セキュリティ アプライアンスのステータスの表示

[アプライアンスステータス（Appliance Status）] ページには、接続されている各アプライアンスの状態が詳細に表示されます。

[Web アプライアンスステータス（Web Appliance Status）] ページで管理対象 Web セキュリティアプライアンスの詳細を表示するには、アプライアンスの名前をクリックします。

ステータス情報としては、接続されている Web セキュリティ アプライアンスに関する一般情報、それらの公開された設定、公開履歴、機能キーのステータスなどがあります。

（注） 表示可能なデータがあるのは、集中管理をサポートするマシンのみです。

（注） Web セキュリティアプライアンスの Acceptable Use Control Engine の各種バージョンが、セキュリティ管理アプライアンスのバージョンと一致しない場合は、警告メッセージが表示されます。そのサービスが Web セキュリティ アプライアンスで無効になっているか、そこに存在しない場合は、[なし（N/A）] と表示されます。

# Web アプライアンス ステータスの詳細

このページの情報のほとんどは、Web セキュリティ アプライアンスから取得されます。

- セキュリティ ステータス情報（稼働時間、アプライアンスモデル、シリアル番号、AsyncOS のバージョン、ビルド日、AsyncOS のインストール日時、ホスト名）
- 設定公開履歴（公開日時、ジョブ名、コンフィギュレーションバージョン、公開の結果、ユーザ）
- 直近に試行されたデータ転送の時刻など、中央集中型レポーティングのステータス
- Web セキュリティ アプライアンスの各機能のステータス（各機能が有効になっているかどうか、機能キーのステータス）
- 管理対象および管理側のアプライアンスの Acceptable Use Controls Engine のバージョン
- Web セキュリティ アプライアンスの AnyConnect セキュア モビリティ設定
- この Web セキュリティ アプライアンスが接続された Cisco Identity Services Engine（ISE）サーバ
- Web セキュリティ アプライアンスのプロキシ設定（アップストリーム プロキシとプロキシの HTTP ポート）
- 認証サービス情報（サーバ、スキーム、レルム、シーケンス、トランスペアレントユーザ ID のサポートの有無、認証に失敗した場合のトラフィックのブロックまたは許可）

ヒント　Web セキュリティ アプライアンスで発生した最新の設定変更が [Web アプライアンス ステータス（Web Appliance Status）] ページに反映されるまでに、数分かかることがあります。データをすぐに更新するには、[データの更新（Refresh Data）] リンクをクリックします。ページのタイム スタンプは、データが最後にリフレッシュされた時刻を示しています。

# URL カテゴリ セットの更新の準備および管理

システムで Web の使用率を管理するために事前定義されている URL カテゴリを最新の状態に維持するためには、Web Usage Controls（WUC）の URL カテゴリ セットを時折更新します。デフォルトでは、Web セキュリティ アプライアンスが URL カテゴリ セットの更新を Cisco から自動的にダウンロードし、セキュリティ管理アプライアンスがこれらの更新を管理対象の Web セキュリティ アプライアンスから数分以内に自動的に受信します。

これらの更新は既存の設定およびアプライアンスの動作に影響を与える可能性があるので、事前に準備して更新後に対処する必要があります。

以下のことを実施してください。

- URL カテゴリ セットの更新による影響の理解　（30 ページ）
- URL カテゴリ セットの更新に関する通知およびアラートの受信　（30 ページ）
- 新規または変更されたカテゴリのデフォルト設定の指定　（30 ページ）
- URL カテゴリ セットの更新時にポリシーと ID/識別プロファイルの設定を確認　（30 ページ）

# URL カテゴリ セットの更新による影響の理解

URL カテゴリ セットが更新されると、Configuration Master の既存のポリシーの動作が変化する可能性があります。

URL カテゴリ セットの更新前後に必要となる処理の重要情報については、資料に掲載されているリンクで、『AsyncOS for Cisco Web Security Appliances User Guide』の「URL Filters」の章の「Managing Updates to the Set of URL Categories」セクションを参照してください。カテゴリについては、同じ章の「URL Category Descriptions」で説明されています。

# URL カテゴリ セットの更新に関する通知およびアラートの受信

| 受信対象 | 操作手順 |
|---|---|
| URL カテゴリ セットの更新の事前通知 | Cisco コンテンツ セキュリティ アプライアンスに関する通知（URL カテゴリ セットの更新に関する通知を含む）を受け取るには今すぐサインアップしてください。Cisco 通知サービスを参照してください。 |
| URL カテゴリ セットの更新が既存のポリシー設定に影響する場合のアラート | [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[アラート（Alerts）] に移動し、[システム（System）] カテゴリで警告レベルのアラートを受信するように設定されていることを確認します。アラートについての詳細は、アラートの管理を参照してください。 |

# 新規または変更されたカテゴリのデフォルト設定の指定

URL カテゴリ セットを更新する前に、URL フィルタリングを行うポリシーの新規カテゴリやマージされたカテゴリにデフォルトの動作を指定するか、これらがすでに設定されている Web セキュリティ アプライアンスから設定をインポートする必要があります。

詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』の「URL Filters」の章の「Choosing Default Settings for New and Changed Categories」セクションまたは Web セキュリティ アプライアンスのオンライン ヘルプを参照してください。

# URL カテゴリ セットの更新時にポリシーと ID/識別プロファイルの設定を確認

URL カテゴリ セットの更新によって、次の 2 種類のアラートがトリガーされます。

- カテゴリの変更についてのアラート
- カテゴリの変更によって変更された、またはディセーブルにされたポリシーについてのアラート

URL カテゴリ セットの変更に関するアラートを受信した場合は、既存の URL カテゴリに基づくポリシーと ID/識別プロファイルが引き続きポリシーの目的を満たしていることを確認してください。

注意が必要な変更の詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』の「Responding to Alerts about URL Category Set Updates」を参照してください。

# Application Visibility and Control（AVC）の更新

SMA は管理対象の Web セキュリティ アプライアンスの多くに存在する AVC エンジンのバージョンを自動的に使用します。

# コンフィギュレーション管理上の問題のトラブルシューティング



## [設定マスター（Configuration Master）] > [ID（Identities）]/[識別プロファイル（Identification Profiles）] に [グループ（Groups）] が表示されない

### 問題

[ウェブ（Web）] > [設定マスター（Configuration Master）] > [ID（Identities）]/[識別プロファイル（Identification Profiles）] のポリシー メンバーシップの定義ページで、[選択されたグループとユーザ（Selected groups and Users）] に [グループ（Groups）] オプションが表示されません。

### 解決方法

複数の Web セキュリティ アプライアンスがある場合、[ネットワーク（Network）] > [認証（Authentication）] の各 WSA で、同じ名前のレルムに対してすべての設定が同一でない限り、すべての WSA でレルム名が一意であることを確認します。

ヒント 各 WSA についてレルム名を確認するには、[ウェブ（Web）] > [ユーティリティ（Utilities）] > [Web アプライアンス ステータス（Web Appliance Status）] に移動して、各アプライアンス名をクリックし、詳細ページの下部までスクロールします。

# [設定マスター（Configuration Master）] > [アクセス ポリシー（Access Policies）] > [Web レピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）] ページの設定が想定とは異なる

### 問題

Configuration Master の [アクセス ポリシー（Access Policies）] > [Web レピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）] ページに、Web レピュテーション スコアのしきい値設定やマルウェア対策スキャン エンジンを選択する機能など、想定される設定が表示されません。または、Web セキュリティ アプライアンスで 適応型セキュリティを使用している場合にこれらの設定が含まれます。

### 解決方法

使用可能なオプションは、[ウェブ（Web）] > [ユーティリティ（Utilities）] > [セキュリティ サービス表示（Security Services Display）] で、Adaptive Security がその Configuration Master に対して選択されているかどうかによって異なります。

# 設定公開失敗のトラブルシューティング

### 問題

設定を公開できません。

### 解決方法

[ウェブ（Web）] > [ユーティリティ（Utilities）] > [Web アプライアンスステータス（Web Appliance Status）] ページを確認します。公開が失敗する理由は次のとおりです。

- [Webアプライアンスサービス（Web Appliance Service）] 列のステータスと、[管理アプライアンス上でサービスを表示しますか?（Is Service Displayed on Management Appliance?）] 列のステータスとの間に不一致があります。
- 両方の列で、機能が有効になっているものの、対応する機能キーがアクティブになっていません（期限切れなど）。
- Configuration Master のバージョンが、Web セキュリティ アプライアンスの AsyncOS のバージョンと一致している必要があります。古いバージョンの Configuration Master から新しいバージョンの Web セキュリティ アプライアンスに対して公開を行うと、Web セキュリティ アプライアンスの設定が Configuration Master の設定と一致していない場合には、処理に失敗するおそれがあります。この問題は、[Webアプライアンスステータス（Web Appliance Status Details）] ページに不一致が見られない場合でも発生することがあります。

### 次の作業

- 公開履歴の表示 （22 ページ）
- イネーブルにされている機能の比較 （12 ページ）
- 公開する機能の有効化 （13 ページ）