CHAPTER 9

Web セキュリティ アプライアンスの管理

- 「中央集中型コンフィギュレーション管理について」（P.9-1）
- 「適切な設定公開方式の決定」（P.9-1）
- 「Configuration Master の設定」（P.9-2）
- 「拡張ファイル公開を使用するための設定」（P.9-14）
- 「Web セキュリティ アプライアンス への設定の公開」（P.9-14）
- 「公開ジョブのステータスと履歴の表示」（P.9-20）
- 「Web セキュリティ アプライアンスのステータスの表示」（P.9-21）
- 「URL カテゴリ セットの更新と中央集中型コンフィギュレーション管理」（P.9-24）

中央集中型コンフィギュレーション管理について

集約設定管理を使用すると、シスコのコンテンツセキュリティ管理アプライアンスから関連する 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方法は 2 つあります。

- Configuration Master を使用する
- Web セキュリティ アプライアンスからのコンフィギュレーション ファイルを使用する（拡張ファイル公開を使用する）

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。

一般的には次のようになります。

- 次の設定に対しては、Configuration Master を使用します。

  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。

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。

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 で設定できる一部の機能は、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 Configuration Master 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。

- 次の設定に対しては、コンフィギュレーション ファイル（拡張ファイル公開）を使用します。

  アプライアンスの管理に関係する機能。たとえば、ログ サブスクリプションやアラートの設定、または管理責任の分散など。

  例外：

  セキュリティ管理アプライアンスを使用して、Web セキュリティ アプライアンスの次の機能を有効にすること、または設定することはできません：連邦情報処理標準の FIPS モード、ネットワーク/インターフェイスの設定、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。

  これらの設定は、管理対象の 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。『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

Configuration Master の設定

Configuration Master を使用して中央集中型コンフィギュレーション管理を設定するには、「Configuration Master の設定の概要」（P.9-2）で説明する手順を順序に従って実行してください。

拡張ファイル公開だけを使用するように準備するには、「拡張ファイル公開を使用するための設定」（P.9-14）を参照してください。

Configuration Master の設定の概要

Web セキュリティ アプライアンスを中央集中方式で管理するようにシステムを設定するには、次の手順に従ってください。

ステップ 1　**（任意）Web セキュリティ アプライアンス。**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動作している Web セキュリティ アプライアンスがすでにある場合は、その 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 ファイルをダウンロードします。このファイルを使用すると、セキュリティ管理アプライアンスでの Configuration Master の設定を迅速に行うことができます。方法については、『*Cisco IronPort AsyncOS for Web Security User Guide* 』の「Saving and Loading the Appliance Configuration」を参照してください。

コンフィギュレーション ファイルと Configuration Master バージョンの互換性については、このリリースのリリース ノート（ http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html）を参照してください。

ステップ 2　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」（P.9-3）を参照してください。

ステップ 3　各 Web セキュリティ アプライアンスに使用する Configuration Master 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」（P.9-3）を参照してください。

ステップ 4　**セキュリティ管理アプライアンス。**集約設定管理を有効にし、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イネーブル化」（P.9-4）を参照してください。

ステップ 5　**セキュリティ管理アプライアンス。**Configuration Master を初期化します。「Configuration Master の初期化」（P.9-4）を参照してください。

ステップ 6　**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 Configuration Master に関連付けます。「Web セキュリティ アプライアンスと Configuration Master の関連付けについて」（P.9-5）を参照してください。

ステップ 7　**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」（P.9-6）を参照してください。

ステップ 8　**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 アプライアンスでイネーブル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 Configuration Master でイネーブルにされている機能と一致していることを確認します。「機能が常にイネーブルにされていることの確認」（P.9-11）を参照してください。

ステップ 9　**セキュリティ管理アプライアンス。**必要とする Configuration Master を設定し、必要な機能をイネーブルにしたら、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」（P.9-14）を参照してください。

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、複数の Web セキュリティ アプライアンスで異なる機能をサポートする異なるバージョンの AsyncOS for Web Security が実行されている異機種混在環境でも集約的に管理できます。

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。

使用している AsyncOS for Web Security のバージョンで使用できる Configuration Master を判断するには、「SMA 互換性マトリクス」（P.2-2）を参照してください。

（注）　最善の結果を得るには、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 のバージョンと同じである必要があります。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イネーブル化

手順

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）] > [Web] > [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。

Configuration Master の初期化

（注）　Configuration Master 7.1 を Configuration Master 7.5 および 7.7 にコピーしたり、インポートする前に、「Configuration Master 7.5 および 7.7 を設定する前の注意事項」（P.9-25）を参照してください。

手順

ステップ 1　メイン 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）] > [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）] カラムの [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、後で既存の 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。

（注）　Configuration Master 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」（P.9-6）で説明されている方法のいずれかを使用して Configuration Master を設定します。

Web セキュリティ アプライアンスと Configuration Master の関連付けについて

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おいて、そのアプライアンスの AsyncOS バージョンと一致する Configuration Master にポリシー設定を関連付ける必要があります。たとえば、Web セキュリティ アプライアンスで AsyncOS 7.7 for Web を実行中の場合は、Configuration Master 7.7 に関連付ける必要があります。

このための最も単純な方法は、状況によって異なります。

条件	参照する手順
まだ 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 に追加していない	「Web セキュリティ アプライアンスの追加と Configuration Master のバージョンとの関連付け」（P.9-5）
すでに Web セキュリティ アプライアンスを追加済みである	「Configuration Master のバージョンと Web セキュリティ アプライアンスとの関連付け」（P.9-6）

Web セキュリティ アプライアンスの追加と 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。

手順

ステップ 1　使用している Web セキュリティ アプライアンスと、この AsyncOS for Security Management のリリースで使用できる Configuration Master のバージョンとの互換性を確認します。「SMA 互換性マトリクス」（P.2-2）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、[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 3　[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 4　[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、すぐに IP アドレスに解決されます。

ステップ 5　Centralized Configuration Manager サービスが事前に選択されています。

ステップ 6　[接続の確立（Establish Connection）] をクリックします。

ステップ 7　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、セキュリティ管理アプライアンスには保存されません。

ステップ 8　[成功（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 9　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 10　変更を送信し、保存します。

ステップ 11　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 セキュリティ アプライアンスごとに、この手順を繰り返します。

Configuration Master のバージョンと Web セキュリティ アプライアンスとの関連付け

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追加済みの場合は、次の手順を使用して、Web セキュリティ アプライアンスを Configuration Master のバージョンに素早く関連付けることができます。

手順

ステップ 1　使用している Web セキュリティ アプライアンスと、この AsyncOS for Security Management のリリースで使用できる Configuration Master のバージョンとの互換性を確認します。「SMA 互換性マトリクス」（P.2-2）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、[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、[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、「公開する機能のイネーブル化」（P.9-12）を参照してください。

ステップ 3　[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 4　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）] カラムにチェックマークを入れます。

ステップ 5　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。

- 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 : 以前の既存の Configuration Master をコピーして新しい Configuration Master のバージョンを初期化していない場合は、古いバージョンをインポートすることができます。「既存の Configuration Master からのインポート」（P.9-7）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、複数の Web セキュリティ アプライアンスで同じ設定を使用したい場合 : 保存されているコンフィギュレーション ファイルをアプライアンスから Configuration Master にインポートします （「Configuration Master の設定」（P.9-2）でコンフィギュレーション ファイルを保存した場合）。

  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」（P.9-8）を参照してください。
- インポートした設定を変更する場合は、「Configuration Master での Web セキュリティ機能の直接設定」（P.9-8）を参照してください。
- Web セキュリティ アプライアンスでポリシー、URL カテゴリ、バイパス設定をまだ設定していない場合は、セキュリティ管理アプライアンスでこれらの設定を対応する Configuration Master に設定します。

  詳細については、「Configuration Master での Web セキュリティ機能の直接設定」（P.9-8）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。たとえば、Configuration Master 7.1 の設定を、Configuration Master 7.5 および 7.7 にインポートすることができます。

（注） Configuration Master 7.5 および 7.7 にコピーまたはインポートする前に、「Configuration Master 7.5 および 7.7 を設定する前の注意事項」（P.9-25）を参照してください。

手順

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）] > [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）] カラムで、[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。

カスタム ユーザ ロールの詳細については、「Custom Web User ロールについて」（P.13-9）を参照してください。

ステップ 5　[インポート（Import）] をクリックします。

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

使用中の 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、Configuration Master 用のデフォルトのポリシー設定を作成できます。

コンフィギュレーション ファイルと Configuration Master バージョンの互換性については、このリリースのリリース ノート（http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html）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。ただし、コンフィギュレーション ファイルを Configuration Master にインポートすると、選択した Configuration Master に関連付けられている設定が上書きされることに注意してください。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。

Configuration Master に Web コンフィギュレーション ファイルを取り込むには、次の手順を実行します。

手順

ステップ 1　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。

ステップ 2　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）] > [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）] カラムで、[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　[ファイルをインポート（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。

Configuration Master での Web セキュリティ機能の直接設定

Configuration Master では、バージョンに応じて次の機能を設定できます。

Configuration Master 7.1	Configuration Master 7.5	Configuration Master 7.7
• ID • SaaS ポリシー • 復号ポリシー • ルーティング ポリシー • アクセス ポリシー • 全体の帯域幅の制限 • Cisco IronPort データ セキュリティ • 外部データ漏洩防止 • Outbound Malware Scanning • カスタム URL カテゴリ • 定義済みの時間範囲 • バイパス設定	• ID • SaaS ポリシー • 復号ポリシー • ルーティング ポリシー • アクセス ポリシー • 全体の帯域幅の制限 • Cisco IronPort データ セキュリティ • 外部データ漏洩防止 • Outbound Malware Scanning • カスタム URL カテゴリ • 定義済みの時間範囲 • バイパス設定	• ID • SaaS ポリシー • 復号ポリシー • ルーティング ポリシー • アクセス ポリシー • 全体の帯域幅の制限 • Cisco IronPort データ セキュリティ • 外部データ漏洩防止 • Outbound Malware Scanning • SOCKS ポリシー • カスタム URL カテゴリ • 定義済みの時間範囲 • バイパス設定

Configuration Master で各機能を直接設定するには、[Web] > [Configuration Master <*version*>] > <*feature*> を選択します。

「Configuration Master で機能を設定する場合の SMA 特有の違い」（P.9-9）で説明する一部の項目を除いて、Configuration Master 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『*Cisco IronPort AsyncOS for Web Security 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」（P.9-3）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 Configuration Master 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/en/US/products/ps10164/products_user_guide_list.html ですべてのバージョンを入手できます。

Configuration Master で機能を設定する場合の SMA 特有の違い

Configuration Master 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 9-1　機能の設定：Configuration Master と Web セキュリティ アプライアンスとの違い

機能またはページ	詳細
すべての機能、特に各リリースでの新機能	Configuration Master 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）] にある機能をイネーブルにする必要があります。詳細については、「機能が常にイネーブルにされていることの確認」（P.9-11）を参照してください。
ID	• 「Configuration Master で ID を使用する場合のヒント」（P.9-10）を参照してください。 • 同じ名前で、異なるプロトコルを使用する異なる Web セキュリティ アプライアンスにレルムがある場合、Configuration Master で目的のレルムごとに適切なスキームを選択します。 • 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 の追加または編集時に [ユーザを透過的に識別する（Identify Users Transparently）] オプションを使用できます。 この機能は、Configuration Master 7.5 で導入されました。
SaaS ポリシー	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。
[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 とユーザ（Identities and Users）] オプションを設定すると、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。 [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。対象とするグループが見つからない場合は、そのグループを「Authorized Groups」に追加することができます。これを行うには、[ディレクトリ（Directory）] 検索フィールドにこのグループを入力して、[追加（Add）] ボタンをクリックします。
[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）]	このページで指定できるオプションは、関連する Configuration Master に対して Adaptive Scanning がイネーブルにされているかどうかによって変わります。[Web] > [ユーティリティ（Utilities）] > [セキュリティ サービス表示（Security Services Display）] でこの設定を確認してください。 この機能は、Configuration Master 7.5 で導入されました。

Configuration Master で ID 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 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 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一連の ID を作成し、これらの ID 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 と、ID を参照するポリシーは自動的に削除され、ディセーブルになります。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 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 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 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。

機能が常にイネーブルに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」（P.9-11）
- 「公開する機能のイネーブル化」（P.9-12）

（注）　異なる機能がイネーブルになっている複数の Web セキュリティ アプライアンスが同じ Configuration Master 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 アプライアンスでイネーブル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 Configuration Master でイネーブルに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 Configuration Master 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。

Web セキュリティ アプライアンスでイネーブルにされている機能を確認するには、次の手順を実行します。

手順

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 Appliances Status）] を選択します。

ステップ 2　Configuration Master 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ライセンス 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）] カラムの設定を比較します。

[Web アプライアンス サービス（Web Appliance Service）] カラムと、[管理アプライアンスに表示されているサービス（Is Service Displayed on Management Appliance?）] カラムが同じである必要があります。

- [有効（Enabled）] = [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、ライセンス 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が不一致の場合は、文字が赤色で表示されます。

ステップ 6　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。「公開する機能のイネーブル化」（P.9-12）を参照してください。
- Web セキュリティ アプライアンス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、複数の機能に影響する場合があります。関連する機能については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

公開する機能のイネーブル化

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。

（注）　Configuration Master に対して機能をイネーブルにしても、その機能が Web セキュリティ アプライアンスでイネーブルになるわけではありません。

各 Configuration Master に対してイネーブルにした機能は、[セキュリティ サービス表示（Security Services Display）] ページに要約されます。「N/A」と表示されている場合は、その機能がその Configuration Master のバージョンで使用できないことを表します。

公開する機能をイネーブルにするには、次の手順を実行してください。

手順

ステップ 1　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」（P.9-11）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、[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 3　[設定を編集（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。

（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イネーブルになっていると見なされているためです。Web プロキシをディセーブルにすると、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 4　（任意）使用しない Configuration Master は非表示にします。意図しない影響が生じるのを避けるため、「使用しない Configuration Master のディセーブル化」（P.9-13）の「注」を参照してください。

ステップ 5　使用する各 Configuration Master について、イネーブル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 6　使用する各 Configuration Master に対して変更を加えます。

ステップ 7　[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 8　[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 9　変更を保存します。

ステップ 10　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イネーブルまたはディセーブル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」（P.9-11）を参照してください。

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。

たとえば、一部の Configuration Master をディセーブルにしたとき、[設定マスター（Configuration Master）] タブと [セキュリティ サービス表示（Security Services Display）] ページは次のように表示されます。

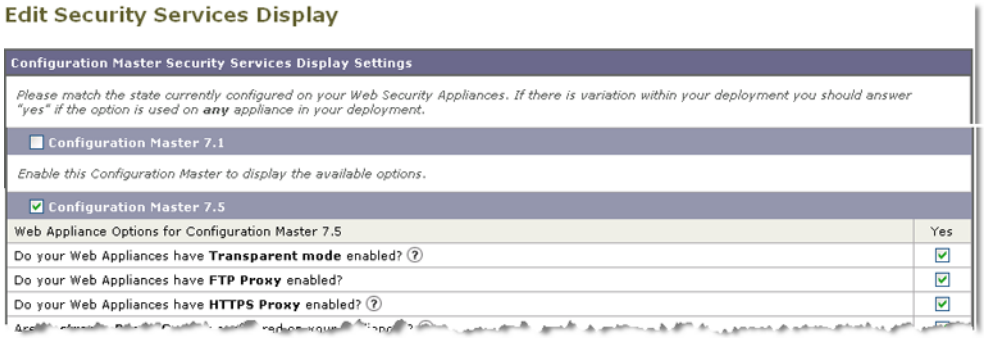
（注）　Configuration Master をディセーブルにすると、それに対するすべての参照が、対応する [設定マスター（Configuration Master）] タブを含めて GUI から削除されます。その Configuration Master を使用する保留中の公開ジョブは削除され、非表示の Configuration Master に割り当てられていたすべての Web セキュリティ アプライアンスが、割り当てられていないものとして再分類されます。少なくとも 1 つの Configuration Master をイネーブルにする必要があります。

手順

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）] > [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　[設定を編集（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。

- 「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イネーブル化」（P.9-4）
- 「Configuration Master の初期化」（P.9-4）
- 「Web セキュリティ アプライアンスと Configuration Master の関連付けについて」（P.9-5）

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」（P.9-14）
- 「拡張ファイル公開による設定の公開」（P.9-18）

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」（P.9-15）
- 「Configuration Master の公開」（P.9-16）
- 「Configuration Master を後日公開」（P.9-17）
- 「コマンドライン インターフェイスによる Configuration Master の公開」（P.9-17）

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」（P.9-1）を参照してください。

Configuration Master を公開する前に、次のことを確認します。

- 対象となる Web セキュリティ アプライアンスの AsyncOS のバージョンが、Configuration Master のバージョンと同じかそれより新しいものである必要があります。具体的な要件については、「SMA 互換性マトリクス」（P.2-2）を参照してください。AsyncOS 7.5 を実行している Web セキュリティ アプライアンスに対して公開するには、Configuration Master 7.5 を使用することを強く推奨します。
- （初回のみ）「Configuration Master の設定」（P.9-2）で説明する手順に従います。
- 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ます。詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。
- Configuration Master が公開を実施し、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」（P.9-11）、および必要に応じて「公開する機能のイネーブル化」（P.9-12）を参照してください。

  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イネーブルになっている場合は、各アプライアンスを別個に公開するようにし、それぞれの公開前に機能がイネーブルになっていることを確認する必要があります。
- 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 がイネーブルになっ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）] または [SaaS ポリシー（SaaS Policy）] で [透過的なユーザ識別（Transparent User Identification）] を選択していると、次のようになります。
  - [ID（Identity）] の場合、[透過的なユーザ識別（Transparent User Identification）] はディセーブルになり、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 Policy）] の場合、[透過的なユーザ識別（Transparent User Identification）] オプションはディセーブルになり、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。
- 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。

  プロキシの再起動が必要な変更を Web セキュリティ アプライアンスで行うと、公開時にもプロキシの再起動が発生することがあります。たとえば、Web セキュリティ アプライアンスで新しいグループをアクセス ポリシーのグループ認証設定に追加すると、次に Configuration Master が公開されるときに Web プロキシが再起動します。このような場合は、プロキシの再起動に関する警告は発生しません。

  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、『*Cisco IronPort for Web Security User Guide*』の「Checking for Web Proxy Restart on Commit」を参照してください。
- ID 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。

（注） セキュリティ管理アプライアンスから、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、外部 DLP ポリシーを公開しても問題ありません。公開しようとすると、セキュリティ管理アプライアンスから、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 Name***>".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 の公開

手順

ステップ 1　「Configuration Master を公開する前に」（P.9-15）の重要な要件と情報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、[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、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 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　[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、[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。

ステップ 8　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」（P.9-20）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

手順

ステップ 1　「Configuration Master を公開する前に」（P.9-15）の重要な要件と情報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、[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、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 5　Configuration Master を公開する日時を入力します。

ステップ 6　公開する Configuration Master を選択します。

ステップ 7　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 8　[送信（Submit）] をクリックします。

ステップ 9　スケジュールされているジョブのリストは、[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 10　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。「公開履歴の表示」（P.9-20）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。

（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。

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」（P.9-15）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*]

ここで、**config_master** は 7.1、7.5、または 7.7 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。

host_list オプションは、公開する 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。[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、[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」（P.9-1）を参照してください。

（注）　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。拡張ファイル公開を使用するときには、プロキシの再起動に関する警告が発生します。

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、『*Cisco IronPort for Web Security User Guide*』の「Checking for Web Proxy Restart on Commit」を参照してください。

拡張ファイル公開を実行するには、次のいずれかを選択します。

- 「拡張ファイル公開：[今すぐ設定を公開する（Publish Configuration Now）]」（P.9-18）
- 「拡張ファイル公開：[後で公開（Publish Later）]」（P.9-19）

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

手順

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。

ファイルの互換性については、「SMA 互換性マトリクス」（P.2-2）を参照してください。

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、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 2　各宛先の Web セキュリティ アプライアンスにおいて、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 ファイルに保存します。詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 3　セキュリティ管理アプライアンスのメイン ウィンドウで、[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 4　[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 5　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 6　[公開する設定マスター（Configuration Master to Publish）] で、[詳細ファイル オプション（Advanced file options）] を選択します。

ステップ 7　[参照（Browse）] をクリックして、ステップ 1 で保存したファイルを選択します。

ステップ 8　[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 [すべてがマスターに割り当てられました（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 9　[公開（Publish）] をクリックします。

拡張ファイル公開：[後で公開（Publish Later）]

手順

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。

ファイルの互換性については、「SMA 互換性マトリクス」（P.2-2）を参照してください。

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、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 2　各宛先の Web セキュリティ アプライアンスにおいて、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 ファイルに保存します。詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 3　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 アプライアンスへの公開（Publish to Web Appliances）] を選択します。

ステップ 4　[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 5　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 6　設定を公開する日時を入力します。

ステップ 7　[公開する設定マスター（Configuration Master to Publish）] で、[詳細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、ステップ 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 8　[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 [すべてがマスターに割り当てられました（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 9　[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

- 「スケジュール設定された公開ジョブの表示」（P.9-20）
- 「現在の公開ジョブのステータスの表示」（P.9-20）
- 「公開履歴の表示」（P.9-20）

スケジュール設定された公開ジョブの表示

スケジュール設定されているものの、まだ実行されていない公開ジョブの一覧を確認するには、[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）] を選択して、[保留中のジョブ（Pending Jobs）] セクションを確認します。

現在の公開ジョブのステータスの表示

現在進行中の公開ジョブのステータスを確認するには、[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）] を選択して、[公開の進歩ステータス（Publishing Progress）] セクションを確認します。

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のあるエラーのチェックに役立ちます。

手順

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）] > [公開履歴（Publish History）] を選択します。

[公開履歴（Publish History）] ページには、試行された最近のすべての公開ジョブがリストされます。カラム情報には、ジョブ名、ジョブ完了時刻、使用された Configuration Master（または、拡張ファイル公開を実行した場合は XML コンフィギュレーション ファイルの名前）、ジョブの公開先にしたアプライアンスの数、およびステータス（[成功（Success）] または [失敗（Failure）]）があります。

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）] カラムで特定のジョブ名のハイパーテキスト リンクをクリックします。

ステップ 3　[公開履歴：ジョブの詳細（Publish History: Job Details）] ページでは、アプライアンス名をクリックすることにより、[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）] ページを表示して、ジョブの特定のアプライアンスに関する追加の詳細を表示できます。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こともでき、対応する [詳細（Details）] リンクをクリックして [Web アプライアンス公開の詳細（Web Appliance Publish Details）] ページに詳細を表示します。

[Web アプライアンス ステータス（Web Appliance Status）] ページの [Web アプライアンス サービス（Web Appliance Service）] カラムのステータスと、[管理アプライアンスに表示されているサービス（Is Service Displayed on Management Appliance?）] カラムのステータスに不一致があると、公開処理が失敗します。両方のカラムで、機能がイネーブルになっているものの、対応するライセンス キーがアクティブになっていない場合（期限切れなど）にも、公開処理が失敗します。

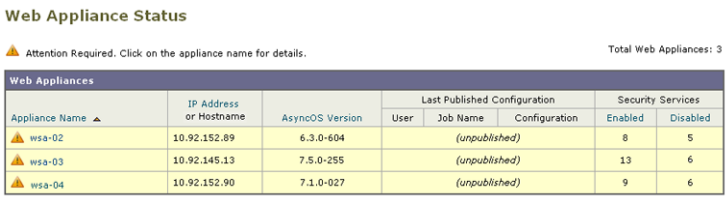
Web セキュリティ アプライアンスのステータスの表示

[Web アプライアンス ステータス（Web Appliances Status）] ページ

[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）] ページには、ご使用の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 アプライアンスの高レベルな概要が表示されます。

（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。

図 9-1　[Web アプライアンス ステータス（Web Appliances Status）] ページ



（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 アプライアンスでディセーブルになっているか、そこに存在しない場合は、[N/A] と表示されます。

[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。

（注）　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。

[アプライアンス ステータス（Appliance Status）] ページ

[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、ライセンス キーのステータスなどがあります。

[アプライアンス ステータス（Appliance Status）] ページには、複数のセクションがあります。

- 「[Web アプライアンス ステータスの詳細（Web Appliance Status Details）] ページ：システム ステータス、設定の公開履歴、および中央集中型レポーティングのステータス」
- 「[Web アプライアンス ステータスの詳細（Web Appliance Status Details）] ページ：セキュリティ サービス セクション」
- 「[Web アプライアンス ステータスの詳細（Web Appliance Status Details）] ページ：AnyConnect セキュア モビリティ、プロキシ、および認証の設定」

図 9-2　[Web アプライアンス ステータスの詳細（Web Appliance Status Details）] ページ：システム ステータス、設定の公開履歴、および中央集中型レポーティングのステータス

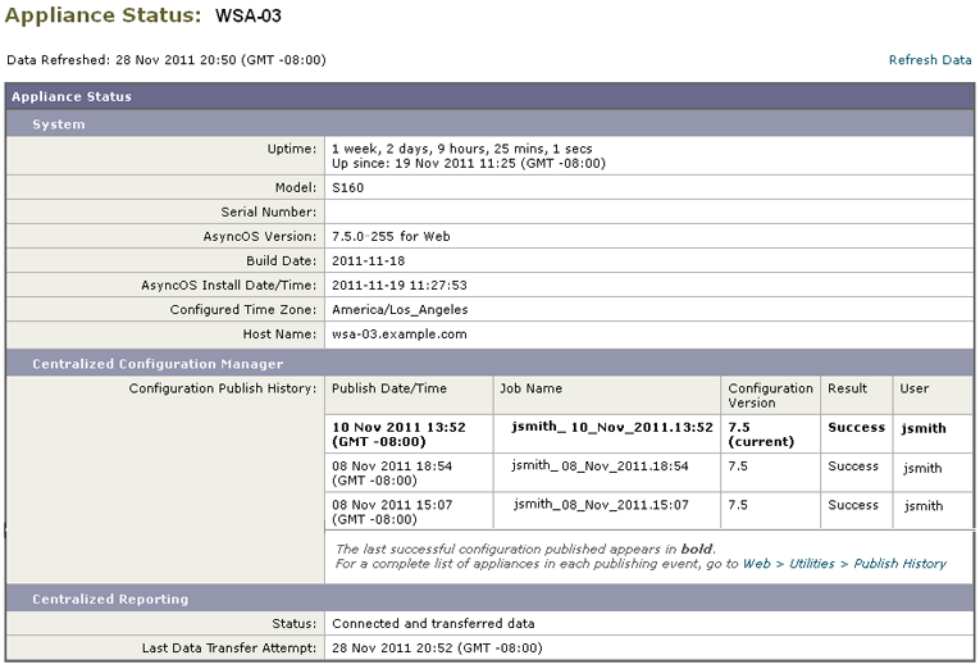


図 9-3　[Web アプライアンス ステータスの詳細（Web Appliance Status Details）] ページ：セキュリティ サービス セクション

図 9-4　[Web アプライアンス ステータスの詳細（Web Appliance Status Details）] ページ：AnyConnect セキュア モビリティ、プロキシ、および認証の設定

AnyConnect Secure Mobility Settings

Cisco ASA:	[IP address and port go here]

Proxy Settings

Upstream Proxies:	*No upstream proxies configured.*
HTTP Ports to Proxy:	[Port goes here]

Authentication Service

Authentication Realms:	Name	Protocol	Servers	Support Transparent User Identification
	NTLM AUTH	NTLM	ad.example.com	No
	LDAP AUTH	LDAP	ad.example.com	No
Authentication Sequences:	Name		Order of Realms	
	All Realms		NTLMSSP: NTLM AUTH Basic: NTLM AUTH, LDAP AUTH	
Unreachable Authentication Service Action:	Block all traffic if authentication fails			

詳細には次の情報が含まれます。

- 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 セキュリティ機能のステータス（機能説明、設定のサマリー、セキュリティ サービスの設定、ライセンス キーのステータス）
- この情報は、使用するアプライアンスに中央集中型管理を設定する場合に使用します。
- 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
- AnyConnect セキュア モビリティの設定
- 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（名前、プロトコル、認証レルムのサーバ、認証手順におけるレルムの名前と順序、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 アプライアンスに変更を加えたときや、アプライアンスに対する情報を表示できないというメッセージが表示された場合に詳細をリフレッシュするには、[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 セットの更新と中央集中型コンフィギュレーション管理

URL カテゴリ セットの更新は、Configuration Master 7.5 以降に対してのみ適用されます。

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、Cisco IronPort 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 アプライアンスセキュリティ管理アプライアンスが URL カテゴリ セットをシスコから自動的にダウンロードし、Web セキュリティ アプライアンスがこれらの更新を管理対象のから数分以内に自動的に受信します。更新された URL カテゴリ セットは、Configuration Master 7.5 以降の ID とアプライアンス ポリシーにただちに表示されます。

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」（P.9-24）
- 「URL カテゴリ セットの更新に関するアラートを受信」（P.9-25）
- 「Configuration Master 7.5 および 7.7 を設定する前の注意事項」（P.9-25）
- 「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」（P.9-25）
- 「URL カテゴリ セットの更新時にポリシーと ID の設定を確認」（P.9-25）

URL カテゴリ セットの更新による影響の理解

URL カテゴリ セットの更新の前後に実行する手順の重要な説明については、「マニュアル」（P.1-4）のリンクに掲載されている、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Managing Updates to the Set of URL Categories」の章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アラートを受信

Configuration Master のポリシー設定に影響を及ぼす URL カテゴリ セットの更新について、アラートを受信するようにするには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アラート（Alerts）] を選択し、[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設定します。アラートについての詳細は、「アラートの管理」（P.14-33）を参照してください。

Configuration Master 7.5 および 7.7 を設定する前の注意事項

Configuration Master 7.1 の設定を Configuration Master 7.5 または 7.7 にコピーまたはインポートすると、URL カテゴリを参照するすべての ID およびポリシーが Configuration Master 7.5 および 7.7 で変更されます。この代わりとして、正しく設定された 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 ファイルをインポートすることができます。また、コピーまたはインポートする前に Configuration Master 7.1 の各ポリシーについて未分類の URL 設定を評価することもできます。

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

将来、URL カテゴリ セットが更新されると、既存の Configuration Master 7.5 以降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、『*User Guide for Cisco IronPort AsyncOS for Web Security*』の「URL Filters」の章にある「Choosing Default Settings for New and Changed Categories」項、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 の設定を確認

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、Configuration Master 7.5 以降で既存の URL カテゴリに基づくポリシーと ID を確認して、それら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、「マニュアル」（P.1-4）のリンクに掲載されている、『*Cisco IronPort for Web Security User Guide*』の「Responding to Alerts about URL Category Set Updates」を参照してください。