CHAPTER 22

システム管理タスクの実行

システム管理の概要

S シリーズ アプライアンスは、システム管理用の各種のツールを提供します。[システム管理（System Administration）] タブの機能は、以下のタスクの管理を支援します。

- アプライアンスの設定
- 機能キー
- ユーザ アカウントの追加、編集、および削除
- ソフトウェアのアップグレードとアップデート
- システム時刻

アプライアンス設定の保存、ロード、およびリセット

Web Security Appliance のすべての設定は、1 つの XML コンフィギュレーション ファイルで管理できます。

アプライアンス設定の表示と印刷

手順 1　[システム管理（System Administration）] > [設定のサマリー（Configuration Summary）] を選択します。

手順 2　必要に応じて、[設定のサマリー（Configuration Summary）] ページを表示または印刷します。

アプライアンス設定ファイルの保存

手順 1　[システム管理（System Administration）] > [設定ファイル（Configuration File）] を選択します。

手順 2　[設定ファイル（Configuration File）] のオプションを設定します。

オプション	説明
ファイル処理オプションの指定	生成された設定ファイルの処理方法を選択します。 • [表示または保存するローカルコンピュータにファイルをダウンロード（Download file to local computer to view or save）] • [ファイルをこのアプライアンス（wsa_example.com）に保存（Save file to this appliance (example.com)）] • [ファイルをメールで送信（Email file to）]（1 つまたは複数の電子メール アドレスを指定します）。
パスフレーズ処理オプションの指定	• [設定ファイルのパスフレーズをマスク（Mask passphrases in the Configuration Files）]：エクスポートまたは保存したファイルで元のパスフレーズを「* * *」に置き換えます。パスフレーズがマスクされた設定ファイルは、アプライアンスに直接リロードできません。
ファイル命名オプションの選択	設定ファイルに名前を付ける方法を選択します。 • [システムにより生成されたファイル名を使用（Use system-generated file name）] • [ユーザ定義ファイル名を使用：（Use user-defined file name:）]

手順 3　[送信（Submit）] をクリックします。

アプライアンス設定ファイルのロード

注意　設定をロードすると、現在の設定がすべて完全に削除されます。以下の操作を実行する前に設定を保存することを強く推奨します。

（注）　互換性のあるコンフィギュレーション ファイルが、アプライアンスの現在インストールされているバージョンより URL カテゴリのセットの古いバージョンに基づいている場合、コンフィギュレーション ファイルのポリシーと ID が自動的に変更される場合があります。

手順 1　[システム管理（System Administration）] > [設定ファイル（Configuration File）] を選択します。

手順 2　[設定をロード（Load Configuration）] オプションとロードするファイルを選択します。（注）

パスフレーズがマスクされているファイルはロードできません。

ファイルには以下のヘッダーが必要です。

```
<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE config SYSTEM "config.dtd">
```

また、正しくフォーマットされた config セクションも必要です。

```
<config> ... your configuration information in valid XML </config>
```

手順 3　[ロード（Load）] をクリックします。

手順 4　表示される警告を確認します。処理の結果を確認したら、[続行（Continue）] をクリックします。

アプライアンス設定の出荷時デフォルトへのリセット

アプライアンス設定をリセットする際、既存のネットワーク設定を保持するかどうかを選択できます。

このアクションでは、コミットする必要はありません。

はじめる前に

アプライアンスから任意の場所に設定を保存します。

手順 1　[システム管理（System Administration）] > [設定ファイル（Configuration File）] を選択します。

手順 2　下方向にスクロールして、[構成のリセット（Reset Configuration）] セクションを表示します。

手順 3　ページに表示された情報を読み、オプションを選択します。

手順 4　[リセット（Reset）] をクリックします。

機能キーの使用

機能キーはシステム上で固有の機能をイネーブル化します。キーはアプライアンスのシリアル番号に固有のものです（機能キーを別のアプライアンスで再使用することはできません）。

機能キーの表示と更新

手順 1　[システム管理（System Administration）] > [機能キー（Feature Keys）] を選択します。

手順 2　保留中のキーのリストを更新するには、[新しいキーをチェック（Check for New Keys）] をクリックします。

手順 3　新しい機能キーを手動で追加するには、[ライセンス キー（Feature Keys）] フィールドにキーを貼り付けるか、入力し、[キーを送信（Submit Key）] をクリックします。機能キーが有効な場合は、そのキーが画面に追加されます。

手順 4　[保留中のライセンス（Pending Activation）] リストの新しい機能キーをアクティブ化するには、そのキーの [選択（Select）] チェックボックスをオンにして、[選択したキーを有効化（Activate Selected Keys）] をクリックします。

新しいキーが発行されたときに、キーを自動的にダウンロードおよびインストールするように、アプライアンスを設定できます。この場合、[保留中のライセンス（Pending Activation）]一覧は常に空白になります。[機能キーの設定（Feature Key Settings）] ページで自動確認を無効にした場合でも、[新しいキーをチェック（Check for New Keys）] ボタンをクリックすることにより、いつでも新しいキーの検索を指示できます。

機能キーの更新設定の変更

[ライセンス キーの設定（Feature Key Settings）] ページは、新しい機能キーを確認およびダウンロードするかどうかや、これらのキーを自動的にアクティベートするかどうかを制御するために使用します。

手順 1　[システム管理（System Administration）] > [ライセンス キーの設定（Feature Key Settings）] を選択します。

手順 2　[設定の編集（Edit Settings）] をクリックします。

手順 3　必要に応じて [ライセンス キーの設定（Feature Key Settings）] を変更します。

オプション	説明
[ライセンス キーの自動適用（Automatic Serving of Feature Keys）]	機能キーを自動的にチェックしてダウンロードし、ダウンロードした機能キーを自動的にアクティブ化します。 自動チェックは通常、月に 1 回実行されますが、機能キーが 10 日未満で期限切れになる場合は 1 日に 1 回実行されます。キーの失効後の 1 か月間は、1 日に 1 回実行されます。1 か月が経過すると、期限が切れたキーは期限切れ間近/期限切れのキーのリストに示されなくなります。

手順 4　変更を送信し、保存します。

仮想アプライアンスのライセンス

Cisco Web Security 仮想アプライアンスでは、ホスト上で仮想アプライアンスを実行する追加ライセンスが必要です。

仮想アプライアンスのライセンスの詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から入手できます。

(注)　仮想アプライアンスのライセンスをインストールする前に、テクニカル サポートのトンネルを開くことはできません。

ライセンスの期限が切れた後、アプライアンスは、180 日間セキュリティ サービスなしで、Web プロキシとして動作を継続します。この期間中、セキュリティ サービスは更新されません。

ライセンスの期限切れに関する警告を受信するように、アプライアンスを設定できます。

関連項目

- アラートの管理（22-15 ページ）

仮想アプライアンスのライセンスのインストール

『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から入手できます。

リモート電源再投入の有効化

アプライアンス シャーシの電源をリモートでリセットする機能は、80-シリーズ ハードウェアでのみ使用できます。

アプライアンスの電源をリモートでリセットする場合は、このセクションで説明されている手順を使用して、この機能を事前に有効にし、設定しておく必要があります。

はじめる前に

- 専用のリモート電源再投入（RPC）ポートをセキュア ネットワークに直接、ケーブル接続します。詳細については、お使いのアプライアンス モデルのハードウェア ガイドを参照してください。このドキュメントの場所については、ドキュメント セット（C-2 ページ）を参照してください。
- ファイアウォールを通過するために必要なポートを開くなど、アプライアンスがリモート アクセス可能であることを確認します。
- この機能では、専用のリモート電源再投入インターフェイス用に一意の IPv4 アドレスが必要です。このインターフェイスは、このセクションで説明されている手順でのみ設定可能です。`ipconfig` コマンドを使用して設定することはできません。

- アプライアンスの電源を再投入するには、Intelligent Platform Management Interface（IPMI）バージョン 2.0 をサポートするデバイスを管理できるサードパーティ製ツールが必要です。このようなツールを使用できるように準備されていることを確認します。
- コマンドライン インターフェイスの詳細については、次を参照してください。付録 B「コマンドライン インターフェイス」

手順 1　SSH またはシリアル コンソール ポートを使用して、コマンドライン インターフェイスにアクセスします。

手順 2　管理者権限を持つアカウントを使用してログインします。

手順 3　以下のコマンドを入力します。

```
remotepower
setup
```

手順 4　プロンプトに従って、以下の情報を指定します。

- この機能専用の IP アドレスと、ネットマスクおよびゲートウェイ。
- 電源の再投入コマンドを実行するために必要なユーザ名とパスフレーズ。

  これらのクレデンシャルは、アプライアンスへのアクセスに使用する他のクレデンシャルに依存しません。

手順 5　`commit` を入力して変更を保存します。

手順 6　設定をテストして、アプライアンスの電源をリモートで管理できることを確認します。

手順 7　入力したクレデンシャルが、将来、いつでも使用できることを確認します。たとえば、この情報を安全な場所に保管し、このタスクを実行する必要がある管理者が、必要なクレデンシャルにアクセスできるようにします。

関連項目

- ハードウェア アプライアンス：アプライアンスの電源のリモート リセット（A-23 ページ）

ユーザ アカウントの管理

以下のタイプのユーザは、Web Security Appliance にログインして、アプライアンスを管理できます。

- **ローカル ユーザ。**アプライアンス自体にローカルにユーザを定義できます。
- **外部システムに定義されたユーザ。**アプライアンスにログインするユーザを認証するために、外部 RADIUS サーバに接続するようにアプライアンスを設定できます。

（注）　Web インターフェイスにログインするか、SSH を使用するなどの任意の方法を使用して、アプライアンスにログインできます。

関連項目

- ローカル ユーザ アカウントの管理（22-7 ページ）
- RADIUS ユーザ認証（22-9 ページ）

ローカル ユーザ アカウントの管理

Web Security Appliance に任意の数のユーザをローカルに定義できます。

デフォルトのシステム admin アカウントは、すべての管理者権限を持っています。admin アカウント パスフレーズを変更できますが、このアカウントを編集または削除できません。

(注)　admin ユーザ パスフレーズを紛失した場合は、シスコ サポート プロバイダーに問い合わせしてください。

ローカル ユーザ アカウントの追加

はじめる前に

すべてのユーザ アカウントが従うべきパスフレーズ要件を定義します。管理ユーザのパスフレーズ要件の設定（22-11 ページ）を参照してください。

手順 1　[システム管理（System Administration）] > [ユーザ（Users）] を選択します。

手順 2　[ユーザの追加（Add User）] をクリックします。

手順 3　以下のルールに注意して、ユーザ名を入力します。

- ユーザ名に小文字、数字、およびダッシュ（-）記号を使用することはできますが、最初の文字をダッシュにすることはできません。
- ユーザ名は 16 文字以下です。
- ユーザ名としてシステムで予約されている特殊名（「operator」や「root」など）を指定することはできません。
- 外部認証も使用する場合は、ユーザ名が外部認証されたユーザ名と重複しないようにしてください。

手順 4　ユーザの氏名を入力します。

手順 5　ユーザ タイプを選択します。

ユーザ タイプ（User Type）	説明
管理者（Administrator）	すべてのシステム設定に対する完全なアクセス権を許可します。ただし、`upgradecheck` および `upgradeinstall` CLI コマンドは、システム定義の「admin」アカウントからのみ発行できます。
演算子	ユーザ アカウントを作成、編集、および削除できません。オペレータ グループでは、以下の CLI コマンドの使用も制限されます。 • `resetconfig` • `upgradecheck` • `upgradeinstall` • `systemsetup` またはシステム セットアップ ウィザードの実行

ユーザ タイプ（User Type）	説明
オペレータ（読み取り専用）（Read-Only Operator）	このロールのユーザ アカウントは、 • 設定情報を表示できます。 • 機能の設定方法を確認するために変更を行って送信はできますが、コミットはできません。 • キャッシュをクリアしたり、ファイルを保存するなどのアプライアンスへの他の変更を加えることはできません。 • ファイル システム、FTP、または SCP にアクセスできません。
ゲスト	ゲスト グループのユーザは、レポートやトラッキングなど、システムのステータス情報の参照のみを実行できます。

手順 6　パスフレーズを入力するか、または作成します。

手順 7　変更を送信し、保存します。

ユーザ アカウントの削除

手順 1　[システム管理（System Administration）] > [ユーザ（Users）] を選択します。

手順 2　プロンプトが表示されたら、一覧表示されているユーザ名に対応するゴミ箱アイコンをクリックして確認します。

手順 3　変更を送信し、保存します。

ユーザ アカウントの編集

手順 1　[システム管理（System Administration）] > [ユーザ（Users）] を選択します。

手順 2　ユーザ名をクリックします。

手順 3　必要に応じて、[ユーザの編集（Edit User）] ページでユーザに変更を加えます。

手順 4　変更を送信し、保存します。

パスフレーズの変更

現在ログインしているアカウントのパスフレーズを変更するには、ウィンドウの右上で、[オプション（Options）] > [パスフレーズの変更（Change Passphrase）] を選択します。他のアカウントの場合は、[ローカル ユーザ設定（Local User Settings）] ページで、アカウントを編集してパスフレーズを変更します。

関連項目

- ユーザ アカウントの編集（22-8 ページ）
- 管理ユーザのパスフレーズ要件の設定（22-11 ページ）

ユーザ プリファレンスの定義

レポートの表示形式などの設定は、各ユーザごとに保持され、ユーザがどのクライアント マシンからアプライアンスにログインするかに関係なく同じです。

手順 1　[オプション（Options）] > [環境設定（Preferences）] を選択します。

手順 2　[ユーザ設定（User Preferences）] ページで、[設定を編集（Edit Preferences）] をクリックします。

手順 3　必要に応じて、プリファレンスを設定します。

プリファレンス設定	説明
言語の表示（Language Display）	Web インターフェイスおよび CLI で使用される Web の言語。
ランディング ページ（Landing Page）	ユーザがアプライアンスにログインするときに表示されるページ。
表示されるレポート時間範囲（Reporting Time Range Displayed）（デフォルト）	[レポート（Reporting）] タブでレポートに対して表示するデフォルトの時間範囲。
表示するレポート行の数（Number of Reporting Rows Displayed）	デフォルトで各レポートに表示されるデータの行数。

手順 4　変更を送信し、保存します。

管理ログインの認証および許可の設定

- RADIUS ユーザ認証（22-9 ページ）
- 管理ユーザのパスフレーズ要件の設定（22-11 ページ）
- アプライアンスへのアクセスに対するセキュリティ設定の追加（22-12 ページ）

RADIUS ユーザ認証

Web Security Appliance は RADIUS ディレクトリ サービスを使用して、HTTP、HTTPS、SSH、および FTP によりアプライアンスにログインするユーザを認証します。PAP または CHAP 認証を使用して、認証のために複数の外部サーバと連携するように、アプライアンスを設定できます。外部ユーザのグループを Web Security Appliance のさまざまなユーザ ロール タイプにマッピングできます。

RADIUS 認証のイベントのシーケンス

外部認証がイネーブルになっている場合にユーザが Web Security Appliance にログインすると、アプライアンスは以下を実行します。

1. ユーザがシステム定義の「admin」アカウントであるかどうかを確認します。
2. 「admin」アカウントでない場合は、まず、設定されている外部サーバをチェックし、ユーザがそのサーバで定義されているかどうかを確認します。
3. 最初の外部サーバに接続できない場合、アプライアンスはリスト内の以下の外部サーバをチェックします。
4. アプライアンスが外部サーバに接続できない場合、アプライアンスは Web Security Appliance で定義されたローカル ユーザとしてユーザを認証しようとします。
5. そのユーザが外部サーバまたはアプライアンスに存在しない場合、またはユーザが間違ったパスフレーズを入力した場合は、アプライアンスへのアクセスが拒否されます。

RADIUS を使用した外部認証のイネーブル化

手順 1　[システム管理（System Administration）] > [ユーザ（Users）] ページで、[外部認証を有効にする（Enable External Authentication）] をクリックします。

手順 2　認証タイプとして [RADIUS] を選択します。

手順 3　RADIUS サーバの IPv4 アドレス/ホスト名、ポート番号、共有シークレット パスフレーズを入力します。

手順 4　タイムアウトまでにアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。

手順 5　RADIUS サーバが使用する認証プロトコルを選択します。

手順 6　（任意）[行を追加（Add Row）] をクリックして別の RADIUS サーバを追加します。各 RADIUS ログについて、3 ～ 5 のステップを繰り返します。

（注）　最大 10 台の RADIUS サーバを追加できます。最初の行のサーバに到達できない場合、要求は次の行のサーバに渡されます。

手順 7　[外部認証キャッシュ タイムアウト（External Authentication Cache Timeout）] フィールドで、再認証のために RADIUS サーバに再接続するまで、アプライアンスが外部認証クレデンシャルを保存する秒数を入力します。

（注）　RADIUS サーバがワンタイム パスフレーズ（たとえば、トークンから作成されるパスフレーズ）を使用する場合、ゼロ（0）を入力します。値をゼロに設定すると、現行セッション中、アプライアンスは認証のために RADIUS サーバに再アクセスしません。

手順 8　グループ マッピングを設定します。すべての外部認証されたユーザ全員を管理者ロールにマッピングするか、異なるアプライアンス ユーザ ロール タイプにマッピングするかを選択します。

設定	説明
外部認証されたユーザを複数のローカル ロールにマッピング。（Map externally authenticated users to multiple local roles.）	RADIUS CLASS 属性で定義されたグループ名を入力し、アプライアンス ロール タイプを選択します。[行の追加（Add Row）] をクリックして、さらにロール マッピングを追加できます。 RADIUS CLASS 属性に基づいて、RADIUS ユーザをアプライアンス ロールに割り当てます。CLASS 属性の要件: • 最小 3 文字 • 最大 253 文字 • コロン、カンマ、または改行文字なし • 各 RADIUS ユーザの 1 つ以上の CLASS 属性をマッピング（この設定を使用すると、CLASS 属性がマッピングされていない RADIUS ユーザへのアクセスは拒否されます）。 複数の CLASS 属性がある RADIUS ユーザの場合は、最も制限されたロールを割り当てます。たとえば、RADIUS ユーザに 2 つの CLASS 属性があり、それらが Operator ロールと Read-Only Operator ロールにマッピングされている場合は、Operator ロールよりも制限が厳しい Read-Only Operator ロールに RADIUS ユーザを割り当てます。 以下のアプライアンス ロールは、最も制限が厳しいものから順番に並んでいます。 • 管理者（Administrator） • 演算子 • オペレータ（読み取り専用）（Read-Only Operator） • ゲスト
外部認証されたすべてのユーザを管理ロールにマップします。（Map all externally authenticated users to the Administrator role.）	すべての RADIUS ユーザを Administrator ロールに割り当てます。

手順 9　変更を送信し、保存します。

管理ユーザのパスフレーズ要件の設定

アプライアンスでローカル定義された管理ユーザのパスフレーズ要件を設定するには、以下の手順を実行します。

手順 1　[システム管理（System Administration）] > [ユーザ（Users）] を選択します。

手順 2　[パスフレーズの設定（Passphrase Settings）] セクションで、[設定を編集（Edit Settings）] をクリックします。

手順 3　以下のオプションから選択します。

オプション	説明
パスフレーズで許可しない単語の一覧（List of words to disallow in passphrases）	1 行ごとに各禁止単語を記入した .txt ファイルを作成し、そのファイルを選択してアップロードします。後続のアップロードによって以前のアップロードが上書きされます。
パスフレーズの強度（Passphrase Strength）	管理ユーザが新しいパスフレーズを入力するときに、パスフレーズ強度インジケータを表示できます。 この設定は強固なパスフレーズの作成を実行するわけではありません。入力されたパスフレーズがどの程度簡単に推測されるかを示すだけです。 インジケータを表示するロールを選択します。次に、選択した各ロールに対して、ゼロよりも大きい数値を入力します。数値が大きいほど、強力なパスフレーズとして登録されたパスフレーズが推測困難であることを意味します。この設定には最大値がありませんが、非常に大きな数値を指定するとパスフレーズの作成が非常に困難になります。 さまざまな値を試すことで、最も要件を満たす数値を確認してください。 パスフレーズの強度は対数目盛で測定されます。評価は、NIST SP 800-63 付則 A の定義に準拠する、米国国立標準技術研究所のエントロピー ルールに基づいています。 一般的に、強固なパスフレーズは以下のような特徴を備えています。 • 長い • 大文字、小文字、数字、特殊文字が含まれている • どのような言語であれ辞書にある単語が含まれていない これらの特徴を備えたパスフレーズを適用するには、このページの他の設定を使用します。

手順 4　変更を送信し、保存します。

アプライアンスへのアクセスに対するセキュリティ設定の追加

CLI コマンド `adminaccessconfig` を使用すると、管理者がアプライアンスにログインする際のアクセス要件をさらに厳格にするように Web Security Appliance を設定できます。

コマンド（Command）	説明
adminaccessconfig > banner	管理者がログインを試みるときに指定したテキストが表示されるようにアプライアンスを設定します。Web UI、CLI、FTP などの任意のインターフェイスを使用して管理者がアプライアンスにアクセスすると、カスタムのログイン バナーが表示されます。 CLI プロンプトに貼り付けるか、Web Security Appliance 上のテキスト ファイルからコピーすることによって、カスタム テキストをロードできます。ファイルからテキストをアップロードするには、まず FTP を使用してアプライアンスの configuration ディレクトリにファイルを転送します。
adminaccessconfig > welcome	これは、管理者がログインに成功したときに表示されるポストログイン バナーです。このテキストは、ログインの adminaccessconfig > banner テキストと同じ方法でアプライアンスの設定に追加されます。
adminaccessconfig > ipaccess	管理者が Web Security Appliance にアクセスするときの接続元の IP アドレスを制御します。管理者は、任意のマシンまたは指定した一覧内の IP アドレスを持つマシンからアプライアンスにアクセスできます。 アクセスを許可リストに制限する場合は、IP アドレス、サブネット、または CIDR アドレスを指定できます。デフォルトでは、アプライアンスにアクセスできるアドレスを一覧表示すると、現在のマシンの IP アドレスが許可リストの最初のアドレスとして一覧表示されます。許可リストから現在のマシンの IP アドレスは削除できません。この情報は、Web UI を使用して表示することもできます。ユーザ ネットワーク アクセス（22-14 ページ）を参照してください。
adminaccessconfig > csrf	悪意のある要求、またはなりすました要求を識別して、これから保護するために使用される、Web UI のクロスサイト要求偽造保護機能を有効/無効にします。最大のセキュリティを確保するには、CSRF 保護をイネーブルにすることを推奨します。
adminaccessconfig > hostheader	HTTP 要求でホスト ヘッダーを使用するよう設定します。 デフォルトでは、Web UI は、HTTP 要求内で Web クライアントから送信されたホスト ヘッダーを使用して応答します。セキュリティを高めるために、アプライアンス固有のホスト名、つまりアプライアンスに設定された名前（wsa_04.local など）のみを使用して応答するように Web UI を設定することができます。
adminaccessconfig > timeout	非アクティビティのタイムアウト間隔、つまりユーザがログアウトするまでに非アクティブでいられる期間（分数）を指定します。5 ～ 1440 分（24 時間）の値を指定できます。デフォルト値は 30 分です。この情報は、Web UI を使用して表示することもできます。ユーザ ネットワーク アクセス（22-14 ページ）を参照してください。
adminaccessconfig > strictssl	管理者がより強力な SSL 暗号（56 ビット暗号化以上）を使用してポート 8443 で Web インターフェイスにログインできるように、アプライアンスを設定します。 より強力な SSL 暗号を必要とするようにアプライアンスを設定すると、その変更は HTTPS を使用して管理の目的でアプライアンスにアクセスする管理者にのみ適用されます。HTTPS を使用して Web プロキシに接続されている他のネットワーク トラフィックには適用されません。

ユーザ ネットワーク アクセス

非アクティブなユーザをアプライアンスからログアウトするまでの時間を指定できます。また、許可するユーザ接続のタイプを指定することもできます。

セッション タイムアウトは、管理者を含め、Web UI または CLI にログインしているすべてのユーザに適用されます。ユーザをログアウトすると、そのユーザはアプライアンスのログイン ページにリダイレクトされます。

手順 1　[システム管理（System Administration）] > [ネットワーク アクセス（Network Access）] を選択します。

手順 2　[設定の編集（Edit Settings）] をクリックします。

手順 3　[セッション非アクティブ タイムアウト（Session Inactivity Timeout）] フィールドに、ログアウトするまでに許容するユーザの非アクティブ時間を分数で入力します。

5 ～ 1440 分（24 時間）の範囲でタイムアウト間隔を定義できます。デフォルト値は 30 分です。

手順 4　[ユーザ アクセス（User Access）] セクションで、ユーザのシステム アクセスを制御します。[任意の接続を許可（Allow Any Connection）] または [特定の接続のみを許可（Only Allow Specific Connections）] のいずれかをオンにします。

[特定の接続のみを許可（Only Allow Specific Connections）] をオンにする場合、特定の接続を IP アドレス、IP 範囲、または CIDR 範囲として定義します。

（注）　アプライアンスの管理 IP アドレスは自動的に許可されます。

手順 5　変更を送信し、保存します。

このタイムアウトの値を設定するには、CLI `adminaccessconfig` > `timeout` を使用することもできます。

管理者パスフレーズのリセット

すべての管理者レベルのユーザは、「admin」ユーザのパスフレーズを変更できます。

はじめる前に

- admin アカウントのパスフレーズが不明な場合は、カスタマー サポート プロバイダーに連絡してパスフレーズをリセットしてください。
- パスフレーズの変更は即座に有効になり、変更を送信する必要はありません。

手順 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] を選択します。

手順 2　[User（ユーザ）] リストで [admin] リンクをクリックします。

手順 3　[パスフレーズの変更（Change Passphrase）] を選択します。

手順 4　新しいパスフレーズを作成するか、または入力します。

生成されたメッセージの返信アドレスの設定

レポート用に生成されるメールの返信アドレスを設定できます。

手順 1　[システム管理(System Administration)] > [返信先アドレス(Return Addresses)] を選択します。

手順 2　[設定の編集(Edit Settings)] をクリックします。

手順 3　表示名、ユーザ名、およびドメイン名を入力します。

手順 4　変更を送信し、保存します。

アラートの管理

アラートとは、Cisco Web セキュリティ アプライアンス アプライアンスで発生しているイベントに関する情報が記載されている、電子メールによる通知のことです。これらのイベントにはマイナー(情報)からメジャー(クリティカル)までの重要度(または重大度)レベルがあり、一般的にアプライアンスの特定のコンポーネントまたは機能に関連しています。

(注)　アラートと通知メール通知を受信するには、アプライアンスが電子メール メッセージへの送信に使用する SMTP リレー ホストを設定する必要があります。

アラートの分類とコンポーネント

アラートに含まれる情報は、アラートの分類と重大度によって決まります。アラート受信者に送信するアラート分類と重大度を指定できます。

アラートの分類

以下のタイプのアラートが送信されます。

- システム(System)
- ハードウェア(Hardware)
- アップデータ(Updater)
- Web プロキシ(Web Proxy)
- マルウェア対策(Anti-Malware)
- L4 トラフィック モニタ(L4 Traffic Monitor)

アラートの重大度

アラートは、以下の重大度に従って送信されます。

- クリティカル:ただちに対処する必要があります。
- 警告:今後モニタリングが必要な問題またはエラー。すぐに対処が必要な場合もあります。
- 情報:デバイスのルーティン機能で生成される情報。

アラート受信者の管理

（注）　システムのセットアップ時に AutoSupport をイネーブルにした場合、指定した電子メール アドレスにすべての重大度およびクラスのアラートを受信します（デフォルト）。この設定はいつでも変更できます。

アラート受信者の追加および編集

手順 1　[システム管理（System Administration）] > [アラート（Alerts）] を選択します。

手順 2　[アラート受信者（Alert Recipients）] リストで受信者をクリックして編集するか、[受信者の追加（Add Recipient）] をクリックして新しい受信者を追加します。

手順 3　受信者の電子メール アドレスを追加または編集します。複数のアドレスをカンマで区切って入力することもできます。

手順 4　各アラート タイプごとに、受信するアラートの重大度を選択します。

手順 5　変更を送信し、保存します。

アラート受信者の削除

手順 1　[システム管理（System Administration）] > [アラート（Alerts）] を選択します。

手順 2　[アラート受信者（Alert Recipient）] のリストで、アラート受信者に対応するゴミ箱アイコンをクリックして確定します。

手順 3　変更を保存します。

アラート設定値の設定

アラート設定はグローバルな設定であるため、すべてのアラートの動作に影響します。

手順 1　[システム管理（System Administration）] > [アラート（Alerts）] を選択します。

手順 2　[設定の編集（Edit Settings）] をクリックします。

手順 3　必要に応じて、アラートの設定値を設定します。

オプション	説明
アラートの送信元アドレス（From Address to Use When Sending Alerts）	アラートを送信するときに使用する RFC 2822 準拠の「Header From:」アドレス。システムのホスト名（「alert@<hostname>」）に基づいてアドレスを自動生成するオプションが用意されています。
重複アラート送信時の待ち時間（Wait Before Sending a Duplicate Alert）	重複アラートの時間間隔を指定します。2 つの設定があります。 [重複アラート初回送信時の待ち時間（秒）（Initial Number of Seconds to Wait Before Sending a Duplicate Alert）]。この値を 0 に設定した場合、重複するアラート サマリーは送信されず、すべての重複アラートがただちに送信されます（これにより、短時間に大量の電子メールを受信する可能性があります）。重複したアラートを送信するまでに待機する秒数は、アラートを送信するたびに増加します。この増加は、待機する秒数に、直前の間隔の 2 倍を加えたものになります。つまり、この値を 5 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、75 秒後、155 秒後、315 秒後などの間隔で送信されます。 [重複アラート送信時の最大待ち時間（秒）（Maximum Number of Seconds to Wait Before Sending a Duplicate Alert）]。[重複するアラート メッセージを送信する前に待機する最大の秒数（Maximum Number of Seconds to Wait Before Sending a Duplicate Alert）] フィールドを使用して、待機間隔の秒数に制限を設けることができます。たとえば、初期値を 5 秒に設定し、最大値を 60 秒に設定すると、アラートは 5 秒、15 秒、35 秒、60 秒、120 秒などの間隔で送信されます。
Cisco AutoSupport	シスコに以下の情報を送信するかどうかを指定します。 • システムで生成されたすべてのアラート メッセージのコピー • システムの稼働時間、`status` コマンドの出力、および使用されているバージョンを通知する週報 また、シスコに送信したあらゆるメッセージのコピーを内部のアラート受信者に送信するかどうかを指定します。これは、重大度が「情報（Information）」のシステム アラートを受信するよう設定されている受信者にのみ適用されます。

手順 4　変更を送信し、保存します。

アラート リスト

以下の項では、分類別にアラートを一覧表示します。各項の表には、アラート名（内部で使用される descriptor）、アラートの実際のテキスト、説明、重大度（クリティカル、情報、または警告）およびメッセージのテキストに含まれるパラメータ（存在する場合）が含まれています。

機能キー アラート

以下の表は、生成されるさまざまな機能キー アラートの一覧です。アラートの説明と重大度が記載されています。

メッセージ(Message)	アラートの重大度	パラメータ
A “$feature” key was downloaded from the key server and placed into the pending area. EULA acceptance required.	情報(Information)。	**$feature**:機能の名前。
Your “$feature” evaluation key has expired. Please contact your authorized sales representative.	警告(Warning)。	**$feature**:機能の名前。
Your “$feature” evaluation key will expire in under $days day(s). Please contact your authorized sales representative.	警告(Warning)。	**$feature**:機能の名前。 **$days**:機能キーの期限が切れるまでの日数。

ハードウェア アラート

以下の表は、生成されるさまざまなハードウェア アラートの一覧です。アラートの説明と重大度が記載されています。

メッセージ(Message)	アラートの重大度	パラメータ
A RAID-event has occurred: $error	警告	**$error**:RAID エラーのテキスト。

ロギング アラート

以下の表は、生成されるさまざまなロギング アラートの一覧です。アラートの説明と重大度が記載されています。

メッセージ(Message)	アラートの重大度	パラメータ
$error.	情報(Information)。	**$error**:エラーのトレースバック文字列。
Log Error: Subscription $name: Log partition is full.	クリティカル(Critical)。	**$name**:ログ サブスクリプション名。
Log Error: Push error for subscription $name: Failed to connect to $ip: $reason.	クリティカル(Critical)。	**$name**:ログ サブスクリプション名。 **$ip**:リモート ホストの IP アドレス。 **$reason**:接続エラーについて説明するテキスト。
Log Error: Push error for subscription $name: An FTP command failed to $ip: $reason.	クリティカル(Critical)。	**$name**:ログ サブスクリプション名。 **$ip**:リモート ホストの IP アドレス。 **$reason**:問題点について説明するテキスト。
Log Error: Push error for subscription $name: SCP failed to transfer to $ip:$port: $reason',	クリティカル(Critical)。	**$name**:ログ サブスクリプション名。 **$ip**:リモート ホストの IP アドレス。 **$port**:リモート ホストのポート番号。 **$reason**:問題点について説明するテキスト。

メッセージ(Message)	アラートの重大度	パラメータ
Log Error: 'Subscription $name: Failed to connect to $hostname ($ip): $error.	クリティカル(Critical)。	**$name**:ログ サブスクリプション名。 **$hostname**:Syslog サーバのホスト名。 **$ip**:Syslog サーバの IP アドレス。 **$error**:エラー メッセージのテキスト。
Log Error: Subscription $name: Network error while sending log data to syslog server $hostname ($ip): $error	クリティカル(Critical)。	**$name**:ログ サブスクリプション名。 **$hostname**:Syslog サーバのホスト名。 **$ip**:Syslog サーバの IP アドレス。 **$error**:エラー メッセージのテキスト。
Subscription $name: Timed out after $timeout seconds sending data to syslog server $hostname ($ip).	クリティカル(Critical)。	**$name**:ログ サブスクリプション名。 **$timeout**:秒単位のタイムアウト。 **$hostname**:Syslog サーバのホスト名。 **$ip**:Syslog サーバの IP アドレス。
Subscription $name: Syslog server $hostname ($ip) is not accepting data fast enough.	クリティカル(Critical)。	**$name**:ログ サブスクリプション名。 **$hostname**:Syslog サーバのホスト名。 **$ip**:Syslog サーバの IP アドレス。
Subscription $name: Oldest log file(s) were removed because log files reached the maximum number of $max_num_files. Files removed include: $files_removed.	情報(Information)。	**$name**:ログ サブスクリプション名。 **$max_num_files**:ログ サブスクリプションごとに許可されるファイルの最大数。 **$files_removed**:削除されたファイルのリスト。

レポート アラート

以下の表は、生成されるさまざまなレポート アラートの一覧です。アラートの説明と重大度が記載されています。

メッセージ(Message)	アラートの重大度	パラメータ
The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.	クリティカル(Critical)。	適用なし
The reporting system is now able to handle new data.	情報(Information)。	適用なし
A failure occurred while building periodic report ‘$report_title’. This subscription should be examined and deleted if its configuration details are no longer valid.	クリティカル(Critical)。	**$report_title**:レポートのタイトル。
A failure occurred while emailing periodic report ‘$report_title’. This subscription has been removed from the scheduler.	クリティカル(Critical)。	**$report_title**:レポートのタイトル。

メッセージ(Message)	アラートの重大度	パラメータ
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc). Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.	警告(Warning.)。	**$threshold:**: しきい値。
PERIODIC REPORTS: While building periodic report $report_title' the expected domain specification file could not be found at '$file_name'. No reports were sent.	クリティカル(Critical)。	**$report_title**: レポートのタイトル。 **$file_name**: ファイルの名前。
Counter group "$counter_group" does not exist.	クリティカル(Critical)。	**$counter_group**: counter_group の名前。
PERIODIC REPORTS: While building periodic report $report_title' the domain specification file '$file_name' was empty. No reports were sent.	クリティカル(Critical)。	**$report_title**: レポートのタイトル。 **$file_name**: ファイルの名前。
PERIODIC REPORTS: Errors were encountered while processing the domain specification file '$file_name' for the periodic report '$report_title'. Any line which has any reported problem had no report sent. $error_text	クリティカル(Critical)。	**$report_title**: レポートのタイトル。 **$file_name**: ファイルの名前。 **$error_text**: 発生したエラーのリスト。
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc). Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.	警告(Warning.)。	**$threshold**: しきい値。
The reporting system has encountered a critical error while opening the database. In order to prevent disruption of other services, reporting has been disabled on this machine. Please contact customer support to have reporting enabled. The error message is: $err_msg	クリティカル(Critical)。	**$err_msg**: エラー メッセージ テキスト。

システム アラート

以下の表は、生成されるさまざまなシステム アラートの一覧です。アラートの説明と重大度が記載されています。

メッセージ（Message）	アラートの重大度	パラメータ
Startup script $name exited with error: $message	クリティカル（Critical）。	**$name**：スクリプトの名前。 **$message**：エラー メッセージ テキスト。
System halt failed: $exit_status: $output',	クリティカル（Critical）。	**$exit_status**：コマンドの終了コード。 **$output**：コマンドからの出力。
System reboot failed: $exit_status: $output	クリティカル（Critical）。	**$exit_status**：コマンドの終了コード。 **$output**：コマンドからの出力。
Process $name listed $dependency as a dependency, but it does not exist.	クリティカル（Critical）。	**$name**：プロセスの名前。 **$dependency**：一覧表示されている依存性の名前。
Process $name listed $dependency as a dependency, but $dependency is not a wait_init process.	クリティカル（Critical）。	**$name**：プロセスの名前。 **$dependency**：一覧表示されている依存性の名前。
Process $name listed itself as a dependency.	クリティカル（Critical）。	**$name**：プロセスの名前。
Process $name listed $dependency as a dependency multiple times.	クリティカル（Critical）。	**$name**：プロセスの名前。 **$dependency**：一覧表示されている依存性の名前。
Dependency cycle detected: $cycle.	クリティカル（Critical）。	**$cycle**：サイクルに関係するプロセス名のリスト。
An error occurred while attempting to share statistical data through the Network Participation feature. Please forward this tracking information to your support provider: Error: $error.	警告（Warning）。	**$error**：例外に関連付けられたエラー メッセージ。
There is an error with “$name”.	クリティカル（Critical）。	**$name**：コア ファイルを生成したプロセスの名前。
An application fault occurred: “$error”	クリティカル（Critical）。	**$error**：エラーのテキスト（通常はトレースバック）。
Appliance: $appliance, User: $username, Source IP: $ip, Event: Account locked due to X failed login attempts. User $username is locked after X consecutive login failures. Last login attempt was from $ip.	情報（Information）。	**$appliance**：特定の WSA の ID。 **$username**：特定のユーザ アカウントの ID。 **$ip**：ログインが試行された IP アドレス。
Tech support: Service tunnel has been enabled, port $port	情報（Information）。	**$port**：サービス トンネルに使用されるポート番号。

メッセージ(Message)	アラートの重大度	パラメータ
Tech support: Service tunnel has been disabled.	情報(Information)。	適用なし
• The host at $ip has been added to the blacklist because of an SSH DOS attack. • The host at $ip has been permanently added to the ssh whitelist. • The host at $ip has been removed from the blacklist	警告(Warning)。	**$ip**:ログインが試行された IP アドレス。 [説明(Description)]: SSH を介してアプライアンスへの接続を試みているが、有効なクレデンシャルを提示しない IP アドレスは、2 分以内に 10 回以上試行に失敗した場合、SSH のブラックリストに追加されます。 同じ IP アドレスからのユーザ ログインが成功した場合、その IP アドレスはホワイトリストに追加されます。 ホワイトリストに含まれているアドレスは、ブラックリストにも含まれている場合でもアクセスが許可されます。 1 日が経過すると、エントリはブラックリストから自動的に削除されます。

アップデータ アラート

以下の表は、生成されるさまざまなアップデータ アラートの一覧です。アラートの説明と重大度が記載されています。

メッセージ(Message)	アラートの重大度	パラメータ
The $app application tried and failed $attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage.	警告。	**$app**:Web Security Applianceセキュリティ サービス名。 **$attempts**:試行回数。
The updater has been unable to communicate with the update server for at least $threshold.	警告(Warning)。	**$threshold:**:しきい値の時間。
Unknown error occurred: $traceback.	クリティカル(Critical)。	**$traceback**:トレースバック情報。

マルウェア対策アラート

高度なマルウェア対策に関連するアラートについては、高度なマルウェア防御の問題に関連するアラートの受信の確認(14-16 ページ) を参照してください。

FIPS の準拠性

Federal Information Processing Standard(FIPS)は、機密情報であるが機密扱いされていない情報を保護するために、すべての政府機関で使用される暗号化モジュールの要件を規定しています。FIPS は、連邦政府のセキュリティとデータ プライバシー要件の遵守を確実にするために役立ちます。国立標準技術研究所(NIST)によって開発された FIPS は、連邦政府の要件を満たす任意の規格がない場合に使用されます。

WSA は Cisco Common Cryptographic Module (C3M)を使用して FIPS モードの FIPS 140-2 準拠を実現します。デフォルトでは、FIPS モードはディセーブルです。

- FIPS 証明書の要件（22-23 ページ）
- FIPS モードの有効化/無効化（22-23 ページ）

FIPS 証明書の要件

FIPS モードでは、Web Security Appliance でイネーブルになっているすべての暗号化サービスについて FIPS 準拠の証明書を使用する必要があります。これは、以下の暗号化サービスに適用されます。

- HTTPS プロキシ
- 認証
- SaaS のアイデンティティ プロバイダー
- アプライアンス管理 HTTPS サービス

（注）　FIPS モードをイネーブルにする前に、FIPS 準拠証明書を使用してアプライアンス管理 HTTPS サービスを設定する必要があります。他の暗号化サービスはイネーブルにする必要はありません。

FIPS 準拠の証明書は以下の要件を満たす必要があります。

証明書	アルゴリズム（SNMP (v3) Auth. Alrorithm）	署名アルゴリズム	注記（Notes）
X509	RSA	sha1WithRSAEncryption sha256WithRSAEncryption	最適な復号化パフォーマンスと十分なセキュリティを実現するために、1024 ビットのキー サイズを推奨します。ビットサイズをさらに大きくすると、セキュリティは向上しますが、復号化のパフォーマンスに影響します。

FIPS モードの有効化/無効化

はじめる前に

- FIPS モードで使用される証明書で、FIPS 140-2 認定の公開キー アルゴリズムが使用されていることを確認します（FIPS 証明書の要件（22-23 ページ）を参照）。

（注）　FIPS モードを変更すると、アプライアンスが再起動されます。

手順 1　[システム管理（System Administration）] > [FIPS モード（FIPS Mode）] を選択します。

手順 2　[設定の編集（Edit Settings）] をクリックします。

手順 3　[FIPS コンプライアンスの有効化（Enable FIPS Compliance）] をオンにして、FIPS コンプライアンスを有効にします。

手順 4　[送信（Submit）] をクリックします。

手順 5　[続行（Continue）] をクリックして、アプライアンスの再起動を許可します。

システムの日時の管理

時間帯の設定

手順 1　[システム管理（System Administration）] > [タイム ゾーン（Time Zone）] を選択します。

手順 2　[設定の編集（Edit Settings）] をクリックします。

手順 3　地域、国、およびタイム ゾーンを選択するか、GMT オフセットを選択します。

手順 4　変更を送信し、保存します。

NTP サーバによるシステム クロックの同期

アプライアンスで手動で時間を設定するのではなく、ネットワーク タイム プロトコル（NTP）サーバをクエリーして現在の日時を追跡できるように、Web セキュリティ アプライアンスを設定することを推奨します。これは、特にアプライアンスが他のデバイスと統合している場合に有効です。統合されたすべてのデバイスが同じ NTP サーバを使用する必要があります。

手順 1　[システム管理（System Administration）] > [時間の設定（Time Settings）] を選択します。

手順 2　[設定の編集（Edit Settings）] をクリックします。

手順 3　[時刻の設定方法（Time Keeping Method）] として [NTP（Network Time Protocol）を使用（Use Network Time Protocol）] を選択します。

手順 4　サーバの追加が必要な場合は、[行の追加（Add Row）] をクリックして、NTP サーバの完全修飾ホスト名または IP アドレスを入力します。

手順 5　（任意）NTP クエリーに使用するアプライアンスのネットワーク インターフェイス タイプ（管理またはデータのいずれか）に関連付けられている、ルーティング テーブルを選択します。これは、NTP クエリーが発信される IP アドレスになります。

（注）　このオプションは、アプライアンスがデータ トラフィック用と管理トラフィック用に分割ルーティングを使用している場合にのみ変更できます。

手順 6　変更を送信し、保存します。

SSL の設定

セキュリティ拡張のため、いくつかのサービスで SSL v3 およびさまざまなバージョンの TLS をイネーブルまたはディセーブルにできます。最善のセキュリティを実現するには、すべてのサービスで SSL v3 をディセーブルにすることが推奨されます。デフォルトでは、すべてのバージョンの TLS がイネーブルに、SSL はディセーブルに設定されています。

(注)　これらの機能は、`sslconfig` CLI コマンドを使用してイネーブルまたはディセーブルにすることもできます。Web セキュリティ アプライアンスの CLI コマンド(B-6 ページ)を参照してください。

手順 1　[システム管理(System Administration)] > [SSL 設定(SSL Configuration)] を選択します。

手順 2　[設定の編集(Edit Settings)] をクリックします。

手順 3　これらのサービスで SSL v3、TLS v1.x をイネーブルにするには、対応するチェックボックスをオンにします。

- [アプライアンス管理 Web ユーザ インターフェイス(Appliance Management Web User Interface)]: この設定を変更すると、すべてのアクティブ ユーザの接続が切断されます。
- [プロキシ サービス(Proxy Services)]: セキュア クライアント用の HTTPS プロキシとクレデンシャル暗号化が含まれます。このセクションには、以下も含まれます。
  - [使用する暗号(Cipher(s) to Use)]: プロキシ サービスとの通信に使用する追加の暗号スイートを入力できます。スイートの区切りにはコロン(:)を使用します。特定の暗号の使用を防止するには、その文字列の先頭に感嘆符(!)を追加します。たとえば `!EXP-DHE-RSA-DES-CBC-SHA` と入力します。

    確認済みの TLS/SSL バージョンに適切なスイートのみを入力するようにしてください。詳細および暗号リストについては、https://www.openssl.org/docs/manmaster/man1/ciphers.html を参照してください。

    AsyncOS バージョン 9.0 以前のデフォルトの暗号は、`DEFAULT:+kEDH` です。AsyncOS バージョン 9.1 以降では、デフォルトの暗号は `EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA` になります。いずれの場合も、ECDHE 暗号の選択によって変わる可能性があります。

    (注)　ただし、バージョンに関係なく、新しい AsyncOS バージョンにアップグレードする際にデフォルトの暗号は変わりません。たとえば、以前のバージョンから AsyncOS 9.1 にアップグレードする場合、デフォルトの暗号は `DEFAULT:+kEDH` です。つまり、アップグレード後に、現在の暗号スイートを自分で更新する必要があります。シスコでは、`EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA` への更新を推奨します。
  - [TLS 圧縮の無効化(推奨)(Disable TLS Compression (Recommended))]: TLS 圧縮を無効にするには、このチェックボックスをオンにします。最善のセキュリティを実現するには、この設定が推奨されます。
- [セキュア LDAP サービス(Secure LDAP Services)]: 認証、外部認証、セキュア モビリティが含まれます。

- [セキュア ICAP サービス（外部 DLP）（Secure ICAP Services (External DLP)）]：アプライアンスと外部 DLP（データ漏洩防止）サーバ間の ICAP の通信を保護するのに使用されるプロトコルを選択します。詳細については、外部 DLP サーバの設定（16-10 ページ）を参照してください。
- [サービスの更新（Update Service）]：アプライアンスと利用可能なアップデート サーバ間の通信に使用するプロトコルを選択します。サービスの更新の詳細については、Web のアップグレードとアップデート（22-30 ページ）を参照してください。

（注）　Cisco アップデート サーバは SSL v3 をサポートしていません。したがって、TLS 1.0 以上を Cisco アップデート サービスでイネーブルにしておく必要があります。ただし、ローカル アップデート サーバでは現在も SSL v3 を使用することができます（そのように設定されている場合）。このサーバでサポートされている SSL/TLS のバージョンを確認する必要があります。

手順 4　[送信（Submit）] をクリックします。

証明書の管理

アプライアンスでは、デジタル証明書を使用してさまざまな接続を確立、確認、保護します。[証明書の管理（Certificate Management）] ページでは、現在の証明書リストの表示や更新、信頼できるルート証明書の管理、およびブロックされた証明書の表示を行うことができます。

関連項目

- 証明書およびキーについて（22-26 ページ）
- 証明書の更新（22-27 ページ）
- 信頼できるルート証明書の管理（22-27 ページ）
- ブロックされた証明書の表示（22-28 ページ）
  - アプライアンスで、適切な CA ルート証明書がカスタム信頼できるルート証明書リストに含まれていることを確認します（[ネットワーク（Network）] > [証明書管理（Certificate Management）] > [信頼できるルート証明書の管理（Manage Trusted Root Certificates）]）。

証明書およびキーについて

ユーザに認証を要求するときに、ブラウザはセキュア HTTPS 接続を使用して Web プロキシに認証クレデンシャルを送信します。Web Security Appliance は、デフォルトで付属の「Cisco Web セキュリティ アプライアンス デモ証明書（Cisco Web Security Appliance Demo Certificate）」を使用して、クライアントとの HTTPS 接続を確立します。多くのブラウザでは、証明書が無効であるという内容の警告が表示されます。無効な証明書に関するメッセージをユーザに表示しないようにするには、アプリケーションで自動的に認識される証明書とキーのペアをアップロードします。

関連項目

- 証明書とキーのアップロードまたは生成（22-28 ページ）
- 証明書署名要求（22-29 ページ）
- 中間証明書（22-30 ページ）

手順 5　署名証明書を受け取ったら、それをアップロードします。(任意)中間証明書をアップロードします。参照先:

- アプライアンスで、適切な CA ルート証明書がカスタム信頼できるルート証明書リストに含まれていることを確認します([ネットワーク(Network)] > [証明書管理(Certificate Management)] > [信頼できるルート証明書の管理(Manage Trusted Root Certificates)])。

信頼できるルート証明書の管理

Web セキュリティ アプライアンスには、信頼できるルート証明書のリストが付属しており、これが維持されます。信頼できる証明書を持つ Web サイトでは、復号化は必要ありません。

信頼できる証明書のリストに証明書を追加し、機能的に証明書を削除すると、信頼できる証明書のリストを管理できます。Web セキュリティ アプライアンスは、マスター リストからは証明書を削除しませんが、証明書の信頼を無効にすることができます。これで、信頼できるリストから機能的に証明書が削除されます。

信頼できるルート証明書を追加、上書き、ダウンロードするには、以下の手順を実行します。

手順 1　[ネットワーク(Network)] > [証明書の管理(Certificate Management)] の順に選択します。

手順 2　[証明書の管理(Certificate Management)] ページの [信頼できるルート証明書の管理(Manage Trusted Root Certificates)] をクリックします。

手順 3　シスコ認識済みリストに記載されていない認証局の署名が付いたカスタムの信頼できるルート証明書を追加するには、以下の手順を実行します。

[インポート(Import)] をクリックし、証明書ファイルを参照して選択し、[送信(Submit)] します。

手順 4　1 つ以上のシスコ認識済み証明書の信頼を上書きするには、以下の手順を実行します。

a.　上書きする各エントリの [信頼を上書き(Override Trust)] チェックボックスをオンにします。

b.　[送信(Submit)] をクリックします。

手順 5　特定の証明書のコピーをダウンロードするには、以下の手順を実行します。

a.　シスコの信頼できるルート証明書リストで証明書の名前をクリックし、エントリを展開します。

b.　[証明書をダウンロード(Download Certificate)] をクリックします。

証明書の更新

[更新(Updates)] セクションには、アプライアンス上のシスコの信頼できるルート証明書とブラックリストのバンドルについて、バージョン情報と最終更新情報が一覧表示されます。これらのバンドルは定期的に更新されます。

手順 1　[証明書の管理(Certificate Management)] ページで [今すぐ更新(Update Now)] をクリックし、アップデート可能なすべてのバンドルを更新します。

ブロックされた証明書の表示

シスコにより無効であると判定されてブロックされた証明書のリストを表示するには、以下の手順を実行します。

手順 1　[ブロック済み証明書を表示（View Blocked Certificates）] をクリックします。

証明書とキーのアップロードまたは生成

機能によっては、接続を確立、確認、保護するために証明書とキーが必要です。既存の証明書とキーをアップロードしたり、機能を設定するときに新しい証明書とキーを生成したりできます。

証明書およびキーのアップロード

アプライアンスにアップロードする証明書は、以下の要件を満たしている必要があります。

- X.509 標準を使用していること。
- 一致する秘密キーが PEM 形式で含まれていること。DER 形式はサポートされていません。

手順 1　[アップロードされた証明書とキーを使用（Use Uploaded Certificate and Key）] を選択します。

手順 2　[証明書（Certificate] フィールドで [参照（Browse）]をクリックし、アップロードするファイルを検索します。

（注）　Web プロキシは、ファイル内の最初の証明書またはキーを使用します。証明書ファイルは PEM 形式にする必要があります。DER 形式はサポートされていません。

手順 3　[キー（Key）] フィールドで [参照（Browse）] をクリックし、アップロードするファイルを指定します。

（注）　キーの長さは 512、1024、または 2048 ビットである必要があります。秘密キー ファイルは PEM 形式でなければなりません。DER 形式はサポートされていません。

手順 4　キーが暗号化されている場合は、[キーは暗号化されています（Key is Encrypted）] を選択します。

手順 5　[ファイルのアップロード（Upload File）] をクリックします。

証明書およびキーの生成

手順 1　[生成された証明書とキーを使用（Use Generated Certificate and Key）] を選択します。

手順 2　[新しい証明書とキーを生成（Generate New Certificate and Key）] をクリックします。

a.　[証明書とキーを生成（Generate Certificate and Key）] ダイアログボックスで、必要な生成情報を入力します。

(注)　[共通名(Common Name)] フィールドには、スラッシュ(/)を除く任意の ASCII 文字を入力できます。

b. [証明書とキーを生成(Generate Certificate and Key)] ダイアログボックスで、[生成(Generate)] をクリックします。

生成が完了すると、[証明書(Certificate)] セクションに、証明書の情報と 2 つのリンク([証明書をダウンロード Download Certificate] と [証明書署名要求のダウンロード(Download Certificate Signing Request)])が表示されます。また、認証局(CA)から署名付き証明書を受信したときに、それをアップロードするために使用する [署名付き証明書(Signed Certificate)] オプションも表示されます。

手順 3　[証明書をダウンロード Download Certificate] をクリックして、アプライアンスにアップロードする新しい証明書をダウンロードします。

手順 4　[証明書署名要求のダウンロード(Download Certificate Signing Request)] をクリックして、署名のために認証局(CA)に送信する新しい証明書ファイルをダウンロードします。この処理の詳細については、証明書署名要求(22-29 ページ)を参照してください。

a. CA から署名付き証明書が返送されたら、[証明書(Certificate)] フィールドの [署名付き証明書(Signed Certificate)] で [参照(Browse)] をクリックして、署名付き証明書ファイルを指定し、[ファイルのアップロード(Upload File)] をクリックしてアプライアンスにアップロードします。

b. CA のルート証明書がアプライアンスの信頼できるルート証明書リストに含まれていることを確認します。リストにない場合は追加します。詳細については、信頼できるルート証明書の管理(22-27 ページ)を参照してください。

証明書署名要求

Web Security Appliance は、アプライアンスにアップロードされた証明書の証明書署名要求(CSR)を生成することはできません。そのため、アプライアンス用に作成された証明書を使用するには、別のシステムから署名要求を発行する必要があります。後でアプライアンスにインストールする必要があるため、このシステムから PEM 形式のキーを保存します。

最新バージョンの OpenSSL がインストールされた、任意の UNIX マシンを使用できます。CSR にアプライアンスのホスト名があることを確認してください。OpenSSL を使用した CSR の生成の詳細については、以下の場所にあるガイドラインを参照してください。

`http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28`

CSR が生成されたら、認証局(CA)に送信します。CA は、証明書を PEM 形式で返します。

初めて証明書を取得する場合は、インターネットで「certificate authority services SSL server certificates(SSL サーバ証明書を提供している認証局)」を検索して、環境のニーズに最も適したサービスを選択します。サービスの手順に従って、SSL 証明書を取得します。

(注)　独自の証明書を生成して署名することもできます。そのためのツールは `http://www.openssl.org` の無料のソフトウェア OpenSSL に含まれています。

中間証明書

ルート認証局（CA）証明書の検証に加えて、中間証明書の検証の使用もサポートされています。中間証明書とは信頼できるルート認証局によって発行された証明書であり、追加の証明書を作成するために使用されます。これは、信頼の連鎖を作成します。たとえば、信頼できるルート認証局によって証明書を発行する権利が与えられた example.com によって証明書が発行されたとします。example.com によって発行された証明書は、example.com の秘密キーおよび信頼できるルート認証局の秘密キーと照合して検証する必要があります。

サーバは、SSL ハンドシェイクで「証明書チェーン」を送信してクライアント（ブラウザなど、この場合は HTTPS プロキシである WSA）がサーバを認証できるようにします。通常、サーバ証明書は中間証明書により署名され、中間証明書は信頼できるルート証明書により署名され、ハンドシェイク中にサーバ証明書と全体の証明書チェーンがクライアントに表示されます。通常、ルート証明書は WSA の信頼できる証明書ストアに存在するため、証明書チェーンの検証は成功します。

ただし、サーバでエンドポイント エンティティ証明書が変更された場合、新しいチェーンに必要な更新が実行されません。その結果、サーバは SSL ハンドシェイク中にサーバ証明書のみを表示し、WSA プロキシは中間証明書が存在しないため証明書チェーンを検証できません。

以前のソリューションでは、WSA 管理者が手動で介入し、信頼できる証明書ストアに必要な中間証明書をアップロードしていました。CLI コマンド `advancedproxyconfig > HTTPS > Do you want to enable automatic discovery and download of missing Intermediate Certificates?` を使用して、「中間証明書の検出」を有効にできるようなりました。WSA は、前述のような状況での手動による手順を省くために、この検出プロセスを使用します。

中間証明書の検出では、「AIA 追跡」という方法を使用します。この方法では、信頼できない証明書が存在する場合、WSA はその証明書に「Authority Information Access」という拡張情報があるか検証します。この拡張情報には、オプションの CA 発行者の URI フィールドが含まれています。このフィールドには、問題のサーバ証明書の署名に使用される発行者証明書を照会することができます。これが使用可能になると、WSA はルートの CA 証明書が取得されるまで発行者の証明書を再帰的に取得し、チェーンを再度検証しようとします。

Web のアップグレードとアップデート

シスコでは、Web とそのコンポーネント向けに、アップグレード（新しいソフトウェア バージョン）とアップデート（現在のソフトウェア バージョンの変更）を定期的にリリースしています。

Web をアップグレードするためのベスト プラクティス

- アップグレードを開始する前に、[システム管理（System Administration）] > [設定ファイル（Configuration File）] ページまたは `saveconfig` コマンドを使用して、Web Security Appliance から XML コンフィギュレーション ファイルを保存します。
- PAC ファイルやカスタマイズしたエンドユーザ通知ページなど、アプライアンスに格納されている他のファイルを保存します。

- アップグレード時には、さまざまなプロンプトで長い時間作業を中断しないでください。TCP セッションがダウンロード中にタイムアウトしてしまった場合、アップグレードが失敗する可能性があります。
- アップグレードが完了したら、XML ファイルに設定情報を保存します。

関連項目

- アプライアンス設定の保存、ロード、およびリセット（22-2 ページ）

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とアップデート

- AsyncOS for Web のアップグレード（22-31 ページ）

AsyncOS for Web のアップグレード

はじめる前に

- 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（アプライアンス設定の保存、ロード、およびリセット（22-2 ページ）を参照）。

手順 1　[システム管理（System Administration）] > [システム アップグレード（System Upgrade）] を選択します。

手順 2　[使用可能なアップグレード（Available Upgrades）] をクリックします。

手順 3　入手可能なアップグレードのリストからアップグレードを選択して、[アップグレード開始（Begin Upgrade）] をクリックし、アップグレード プロセスを開始します。表示される質問に答えます。

更新プロセス中、CLI および Web アプリケーション インターフェイスは、応答が遅くなったり、使用できなくなったりする場合があります。

手順 4　アップグレードが完了したら、[今すぐ再起動（Reboot Now）] をクリックして Web セキュリティ アプライアンスを再起動します。

- アップグレードのダウンロードとインストール（22-31 ページ）
- バックグラウンド ダウンロードのステータスの表示、キャンセル、または削除（22-33 ページ）

アップグレードのダウンロードとインストール

はじめる前に

- 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（アプライアンス設定の保存、ロード、およびリセット（22-2 ページ）を参照）。

（注）　Cisco サーバからではなくローカル サーバから 1 回の操作でダウンロードとアップグレードを実行する場合は、*ダウンロード中に*即座にアップグレードがインストールされます。アップグレード プロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間は、Ctrl を押した状態で C を押すと、ダウンロードの開始前にアップグレード プロセスを終了できます。

1 回の操作でダウンロードとインストールを行うか、またはバックグラウンドでダウンロードし後でインストールできます。

手順 1　[システム管理（System Administration）] > [システム アップグレード（System Upgrade）] を選択します。

手順 2　[アップグレード オプション（Upgrade Options）] をクリックします。

アップグレード オプションとアップグレード イメージを選択します。

設定	説明
アップグレード オプションの選択	• [ダウンロードとインストール（Download and install）]：1 回の操作でアップグレードをダウンロードしてインストールします。 すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするよう求められます。 • [ダウンロードのみ（Download only）]：アップグレード インストーラをダウンロードしますが、インストールは行いません。 すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするよう求められます。インストーラはサービスを中断することなく、バックグラウンドでダウンロードします。 ダウンロードが完了すると、[インストール（Install）] ボタンが表示されます。このボタンをクリックして、ダウンロードしたアップグレードをインストールします。
	[アップグレード サーバで使用可能なアップグレード イメージファイルのリスト（List of available upgrade images files at upgrade server）] から、ダウンロードするアップグレード イメージを選択するか、ダウンロードしてインストールしたアップグレード イメージを選択します。
アップグレードの準備	• 現在の設定のバックアップ コピーをアプライアンス上の `configuration` ディレクトリに保存するには、[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（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は、[設定ファイルでパスワードをマスクする（Mask passwords in the configuration file）] を選択して、バックアップ コピー内の現在の設定パフワードをすべてマスクすることができます。ただし、パスワードがマスクされている設定ファイルは、[設定をロード（Load Configuration）] コマンドや `loadconfig` CLI コマンドを使用してロードできません。 • [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は、[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。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。

手順 3　[続行(Proceed)] をクリックします。

インストール中の場合、次に従います。

a. プロセス中のプロンプトに応答できるようにしてください。

b. 完了を求めるプロンプトで、[今すぐ再起動(Reboot Now)] をクリックします。

c. 約 10 分後、アプライアンスにアクセスしてログインします。

アップグレードの問題を修正するためにアプライアンスの電源を再投入する必要があると思われる場合は、再起動後 20 分以上が経過してから再投入してください。

バックグラウンド ダウンロードのステータスの表示、キャンセル、または削除

手順 1　[システム管理(System Administration)] > [システム アップグレード(System Upgrade)] を選択します。

手順 2　[アップグレードオプション(Upgrade Options)] をクリックします。

手順 3　次のオプションを選択します。

目的	操作手順
ダウンロード ステータスの表示	ページの中央を確認してください。 進行中のダウンロードおよびダウンロードが完了してインストールされるのを待っているものがない場合は、ダウンロードのステータス情報は表示されません。
ダウンロードのキャンセル	ページの中央にある、[ダウンロードをキャンセル(Cancel Download)] ボタンをクリックします。 このオプションは、ダウンロード進行中にのみ表示されます。
ダウンロードされたインストーラの削除	ページの中央にある、[ファイルを削除(Delete File)] ボタンをクリックします。 このオプションは、インストーラがダウンロードされている場合にのみ表示されます。

手順 4　(任意)アップグレード ログを確認します。

関連項目

- ローカルおよびリモート アップデート サーバ(22-35 ページ)

自動および手動によるアップデート/アップグレードのクエリー

アプライアンスは、すべてのセキュリティ サービス コンポーネントの新しいアップデートについて定期的にアップデート サーバに照会します。新しいアップグレードについては照会しません。アップグレードするには、使用可能なアップグレードについて照会するように、手動でアプライアンスに指示する必要があります。また、手動でアプライアンスに指示して、使用可能なセキュリティ サービスのアップデートについて照会することもできます。詳細については、以前のバージョンの AsyncOS for Web への復元(22-39 ページ)を参照してください。

アップデートまたはアップグレードについてアップデート サーバに照会する場合、アプライアンスは以下の手順を実行します。

1. アップデート サーバに問い合わせます。

   シスコでは、アップデート サーバに以下のソースを使用できます。

   - **Cisco アップデート サーバ。**詳細については、Cisco アップデート サーバからのアップデートとアップグレード（22-35 ページ）を参照してください。
   - **ローカル サーバ。**詳細については、ローカル サーバからのアップグレード（22-36 ページ）を参照してください。
2. 使用可能なアップデートまたはアップグレードのバージョンを一覧表示する XML ファイルを受信します。この XML ファイルは「マニフェスト」と呼ばれます。
3. アップデートまたはアップグレード イメージ ファイルをダウンロードします。

セキュリティ サービスのコンポーネントの手動による更新

デフォルトでは、各セキュリティ サービス コンポーネントは、Cisco アップデート サーバからデータベース テーブルに定期的にアップデートを受信します。ただし、手動でデータベース テーブルを更新できます。

（注） 一部のアップデートは、機能に関連した GUI ページからオンデマンドで利用できます。

ヒント アップデータ ログ ファイルのアップデート アクティビティの記録を表示してください。[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] ページのアップデータ ログ ファイルに登録します。

（注） 処理中のアップデートは中断できません。すべての処理中のアップデートは、新しい変更が適用される前に完了する必要があります。

手順 1 [システム管理（System Administration）] > [アップグレードとアップデートの設定（Upgrade and Update Settings）] を選択します。

手順 2 [更新設定を編集（Edit Update Settings）] をクリックします。

手順 3 アップデート ファイルの場所を指定します。

手順 4 [セキュリティ サービス（Security Services）] タブにあるコンポーネント ページの [今すぐ更新（Update Now）] 機能キーを使用してアップデートを開始します。たとえば、[セキュリティ サービス（Security Services）] > [Web レピュテーション フィルタ（Web Reputation Filters）] ページです。

更新プロセス中、CLI および Web アプリケーション インターフェイスは、応答が遅くなったり、使用できなくなったりする場合があります。

ローカルおよびリモート アップデート サーバ

デフォルトでは、アプライアンスはアップデートとアップグレードのイメージおよびマニフェスト XML ファイルについて、Cisco アップデート サーバに照会します。ただし、ユーザはアップグレードとアップデートのイメージおよびマニフェスト ファイルのダウンロード元を選択できます。以下の理由から、イメージ ファイルまたはマニフェスト ファイルにローカル アップデート サーバを使用します。

- **同時にアップグレードするアプライアンスが複数あります。**ネットワーク内の Web サーバにアップグレード イメージをダウンロードして、ネットワーク内のすべてのアプライアンスに使用できます。
- **ファイアウォールの設定には、Cisco アップデート サーバのスタティック IP アドレスが必要です。**Cisco アップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合は、アップデートとアップグレードの静的な参照先の設定が必要になることがあります。詳細については、Cisco アップデート サーバのスタティック アドレスの設定（22-35 ページ）を参照してください。

（注）　ローカル アップデート サーバは、セキュリティ サービスのアップデートを自動的に受信せず、アップグレードのみを受信します。アップグレードにローカル アップデート サーバを使用した場合は、その後、アップデートとアップグレードの設定を元に戻して、また Cisco アップデート サーバを使用するようにします。これにより、セキュリティ サービスが再び自動的にアップデートされるようになります。

Cisco アップデート サーバからのアップデートとアップグレード

Web Security Appliance は、Cisco アップデート サーバに直接接続して、アップグレード イメージとセキュリティ サービス アップデートをダウンロードできます。各アプライアンスは、個別にアップデートとアップグレードをダウンロードします。

Cisco アップデート サーバのスタティック アドレスの設定

Cisco アップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合は、アップデートとアップグレードの静的な参照先の設定が必要になることがあります。

手順 1　シスコ カスタマー サポートに問い合わせて、スタティック URL アドレスを取得します。

手順 2　[システム管理（System Administration）] > [アップグレードとアップデートの設定（Upgrade and Update Settings）] ページの順に進み、[更新設定を編集（Edit Update Settings）] をクリックします。

手順 3　[アップデート設定を編集（Edit Update Settings）] ページの [アップデート サーバ（イメージ）（Update Servers (images)）] セクションで、[ローカル アップデート サーバ（Local Update Servers）] を選択し、ステップ 1 で取得したスタティック URL アドレスを入力します。

手順 4　[アップデート サーバ（リスト）（Update Servers (list)）] セクションで Cisco アップデート サーバが選択されていることを確認します。

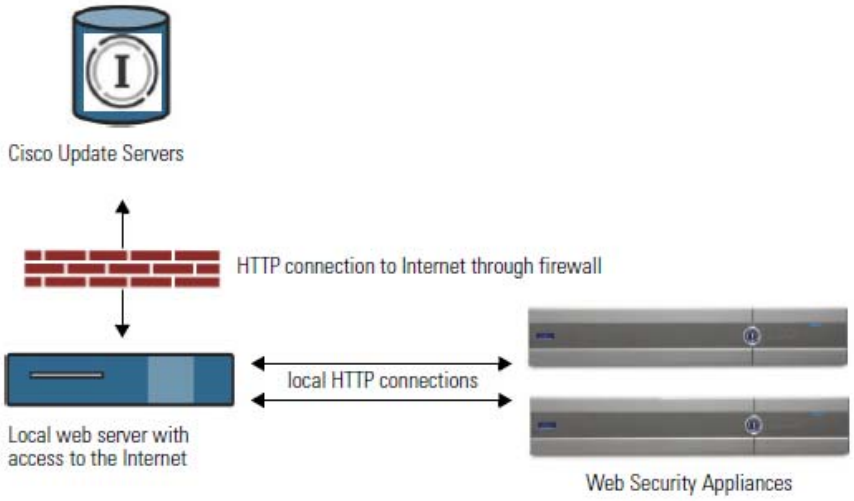
手順 5　変更を送信し、保存します。

ローカル サーバからのアップグレード

Web Security Appliance は、Cisco アップデート サーバからアップグレードを直接取得する代わりに、ネットワーク内のサーバからアップグレードをダウンロードできます。この機能を使用すると、シスコから 1 回だけアップグレード イメージをダウンロードして、ネットワーク内のすべての Web Security Appliance でそれを使用することができます。

図 22-1 は、Web Security Appliance がローカル サーバからアップグレード イメージをダウンロードする方法を示します。

図 22-1　　ローカル サーバからのアップグレード



ローカル アップグレード サーバのハードウェアおよびソフトウェア要件

アップグレード ファイルを*ダウンロード*するには、Web ブラウザを備えた内部ネットワークにシステムを構築する必要があり、Cisco アップデート サーバへのインターネット アクセスが必要です。

(注)　このアドレスへの HTTP アクセスを許可するファイアウォール設定値を設定する必要がある場合、特定の IP アドレスではなく DNS 名を使用して設定する必要があります。

アップグレード ファイルを*ホスティング*するには、内部ネットワーク上のサーバに以下の機能を持つ Web サーバ（Microsoft IIS（Internet Information Services）や Apache オープン ソース サーバなど）が必要です。

- 24 文字を超えるディレクトリまたはファイル名の表示をサポートしていること
- ディレクトリの参照ができること
- 匿名（認証なし）または基本（「簡易」）認証用に設定されている
- 各アップグレード イメージ用に少なくとも 350 MB の空きディスク領域が存在すること

ローカル サーバからのアップグレードの設定

（注）　アップグレードの完了後にセキュリティ サービス コンポーネントが引き続き自動更新されるように、アップデートとアップグレードの設定を変更して、Cisco アップデート サーバ（ダイナミックまたはスタティック アドレスを使用）を使用することを推奨します。

手順 1　アップグレード ファイルを取得および供給するようにローカル サーバを設定します。

手順 2　アップグレード zip ファイルをダウンロードします。

ローカル サーバのブラウザを使用して、`http://updates.ironport.com/fetch_manifest.html` に進み、アップグレード イメージの zip ファイルをダウンロードします。イメージをダウンロードするには、シリアル番号（物理アプライアンス用）または VLN（仮想アプライアンス用）およびアプライアンスのバージョン番号を入力します。利用可能なアップグレードのリストが表示されます。ダウンロードするアップグレード バージョンをクリックします。

手順 3　ディレクトリ構造を変更せずにローカル サーバのルート ディレクトリにある ZIP ファイルを解凍します。

手順 4　[システム管理（System Administration）] > [アップグレードとアップデートの設定（Upgrade and Update Settings）] ページまたは `updateconfig` コマンドを使用して、ローカル サーバを使用するようにアプライアンスを設定します。

手順 5　[システム管理（System Administration）] > [システム アップグレード（System Upgrade）] ページで、[使用可能なアップグレード（Available Upgrades）] をクリックするか、`upgrade` コマンドを実行します。

ローカルとリモートにおけるアップグレード方法の相違

以下の相違点は、Cisco アップデート サーバからではなく、ローカル サーバからアップグレードする場合に該当します。

- *ダウンロード中に*、アップグレードによるインストールがすぐに実行されます。
- アップグレード プロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間は、Control を押した状態で C を押すと、ダウンロードの開始前にアップグレード プロセスを終了できます。

アップグレードおよびサービス アップデートの設定の変更

Web Security Appliance がセキュリティ サービスのアップデートや Web のアップグレードをダウンロードする方法を設定できます。たとえば、ファイルをダウンロードするときに使用するネットワーク インターフェイスを選択したり、アップデート間隔を設定したり、自動アップデートをディセーブルにしたりできます。

手順 1　[システム管理（System Administration）] > [アップグレードとアップデートの設定（Upgrade and Update Settings）] を選択します。

手順 2　[更新設定を編集（Edit Update Settings）] をクリックします。

手順 3　以下の情報を参考にして、設定値を設定します。

設定	説明
自動更新（Automatic Updates）	セキュリティ コンポーネントの自動アップデートをイネーブルにするかどうかを選択します。自動更新を選択する場合、時間間隔を入力します。デフォルトはイネーブルで、更新間隔は 5 分です。
アップグレードの通知（Upgrade Notifications）	新規のアップグレードが使用可能な場合に、Web インターフェイスの上部に通知を表示するかどうかを選択します。アプライアンスは、管理者に対してのみこの通知を表示します。 詳細については、Web のアップグレードとアップデート（22-30 ページ）を参照してください。
アップデート サーバ（リスト）（Update Servers (list)）	利用可能なアップグレードとアップデートのリスト（マニフェスト XML ファイル）を、Cisco アップデート サーバまたはローカル Web サーバのどちらからダウンロードするかを選択します。 ローカル アップデート サーバを選択した場合、サーバのファイル名およびポート番号を含む、リストのマニフェスト XML ファイルの完全なパスを入力します。ポート フィールドを空欄にした場合は、ポート 80 が使用されます。サーバが認証を必要とする場合、有効なユーザ名とパスフレーズも入力します。 • ハードウェア アプライアンスのマニフェストを取得するための URL は以下のとおりです。 https://update-manifests.ironport.com • 仮想アプライアンスのマニフェストを取得するための URL は以下のとおりです。 https://update-manifests.sco.cisco.com
アップデート サーバ（イメージ）（Update Servers (images)）	アップグレード イメージやアップデート イメージを、Cisco アップデート サーバまたはローカル Web サーバのどちらからダウンロードするかを選択します。 ローカル アップデート サーバを選択した場合は、サーバのベース URL とポート番号を入力します。ポート フィールドを空欄にした場合は、ポート 80 が使用されます。サーバが認証を必要とする場合、有効なユーザ名とパスフレーズも入力します。
着信サービス一覧（Routing Table）	アップデート サーバに接続するときに、どのネットワーク インターフェイスのルーティング テーブルを使用するかを選択します。
プロキシ サーバ（Proxy Server）（オプション）	アップストリームのプロキシ サーバが存在し、認証が必要な場合は、サーバ情報、ユーザ名、およびパスフレーズをここに入力します。

手順 4　変更を送信し、保存します。

関連項目

- ローカルおよびリモート アップデート サーバ（22-35 ページ）。
- 自動および手動によるアップデート/アップグレードのクエリー（22-33 ページ）
- 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とアップデート（22-31 ページ）

以前のバージョンの AsyncOS for Web への復元

緊急時に、オペレーティング システムを以前の認定済みビルドに戻すことができます。

(注)　バージョン 7.5 よりも前の Web 用 AsyncOS のバージョンには戻せません。

仮想アプライアンスの AsyncOS を復元した場合のライセンスへの影響

AsyncOS 8.0 に復元した場合、アプライアンスがセキュリティ機能なしで Web トランザクションを処理する 180 日の猶予期間はありません。ライセンスの有効期限は影響を受けません。

復元プロセスでのコンフィギュレーション ファイルの使用

バージョン 7.5 で有効であり、それ以降のバージョンにアップグレードする場合、アップグレードプロセスは Web Security Appliance のファイルに現在のシステム設定を自動的に保存します(ただし、バックアップとして、コンフィギュレーション ファイルをローカル マシンに手動で保存することを推奨します)。これにより、以前のバージョンに復元した後、Web で以前のリリースに関連するコンフィギュレーション ファイルをロードできます。ただし、復元を実行すると、管理インターフェイスに現在のネットワーク設定を使用します。

SMA によって管理されるアプライアンスの AsyncOS の復元

Web Security Appliance から Web 用 AsyncOS に復元することができます。ただし Web Security Appliance がセキュリティ管理アプライアンスで管理されている場合は、以下のルールとガイドラインを考慮してください。

- 中央集中型レポーティングをWeb Security Appliance でイネーブルにすると、Web 用 AsyncOS は復帰を開始する前にセキュリティ管理アプライアンスへのレポート データの転送を終了します。セキュリティ管理アプライアンスへのファイル転送に 40 秒以上かかる場合、Web はメッセージを表示して、ファイルが転送されるまで待つか、またはすべてのファイルを転送せずに復元を続行するかを尋ねます。
- 復元後、適切な設定マスターに Web Security Appliance を関連付ける必要があります。それ以外の場合、セキュリティ管理アプライアンスから Web Security Appliance に設定をプッシュすると失敗する可能性があります。

以前のバージョンへの Web 用の AsyncOS の復元

注意　Web Security Appliance のオペレーティング システムの復元は非常に破壊的な操作であり、すべての設定ログとデータベースが削除されます。さらに、アプライアンスが再設定されるまで、復元によって Web トラフィック処理が中断されます。初期の Web Security Appliance 設定に応じて、この操作がネットワークの設定を破壊する場合があります。このような場合、復元の実行後にアプライアンスへの物理的なローカル アクセスが必要になります。

（注）　URL カテゴリ セットのアップデートが利用可能な場合は、AsyncOS の復元後に適用されます。

はじめる前に

- Cisco Quality Assurance に問い合わせて、目的とする復元が実行可能かどうかを確認してください。
- Web Security Appliance から別のマシンに以下の情報をバックアップします。
  - システム コンフィギュレーション ファイル（パスフレーズをマスクしない状態）。
  - 保持するログ ファイル。
  - 保持するレポート。
  - アプライアンスに保存されるカスタマイズされたエンド ユーザ通知ページ。
  - アプライアンス上に格納されている PAC ファイル。

手順 1　バージョンを戻すアプライアンスの CLI にログインします。

（注）　次のステップで `revert` コマンドの実行するときに、いくつかの警告プロンプトが発行されます。これらの警告プロンプトに同意すると、すぐにバージョンを戻す動作が開始します。このため、復元に向けた準備手順が完了するまで、復元プロセスを開始しないてください。

手順 2　`revert` コマンドを入力します。

手順 3　復元で続行するアプライアンスを 2 回確認します。

手順 4　戻る利用可能なバージョンの 1 つを選択します。

アプライアンスが 2 回リブートします。

（注）　復元プロセスは時間のかかる処理です。復元が完了して、アプライアンスへのコンソール アクセスが再び利用可能になるまでには、15 ～ 20 分かかります。

アプライアンスは、選択された Web バージョンを使用して稼働します。Web ブラウザから Web インターフェイスにアクセスできます。

SNMP の使用によるシステムのヘルスおよびステータスのモニタリング

オペレーティング システムは、SNMP（シンプル ネットワーク管理プロトコル）によるシステム ステータスのモニタリングをサポートしています。（SNMP の詳細については、RFC 1065、1066、および 1067 を参照してください）。

以下の点に注意してください。

- SNMP は、デフォルトで**オフ**になります。
- SNMP SET 動作（コンフィギュレーション）は実装されません。

- SNMPv1、v2、および v3 をサポートしています。SNMPv3 の詳細については、RFC 2571-2575 を参照してください。
- SNMPv3 をイネーブルにする場合、メッセージ認証と暗号化は必須です。認証のパスフレーズと暗号は異なっている必要があります。暗号化アルゴリズムは AES（推奨）または DES を指定できます。認証アルゴリズムは SHA-1（推奨）または MD5 を指定できます。次に `snmpconfig` コマンドを実行するときは、コマンドにこのパスフレーズが「記憶」されています。
- SNMPv3 ユーザ名は v3get です。

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 serv.example.com
```

- SNMPv1 または SNMPv2 のみを使用する場合は、コミュニティ ストリングを設定する必要があります。コミュニティ ストリングは、`public` にデフォルト設定されません。
- SNMPv1 および SNMPv2 の場合、どのネットワークからの SNMP GET 要求を受け入れるかを指定する必要があります。
- トラップを使用するには、SNMP マネージャ（組み込まれていません）が稼動しており、その IP アドレスがトラップ ターゲットとして入力されている必要があります（ホスト名を使用できますが、その場合、トラップは DNS が動作しているときに限り機能します）。

MIB ファイル

MIB ファイルは http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html. から入手できます。各 MIB ファイルの最新バージョンを使用します。

以下の複数の MIB ファイルがあります。

- websecurityappliance-mib.txt：Web Security Appliance 用のエンタープライズ MIB の SNMPv2 互換の説明。
- -MAIL-MIB.txt：電子メール セキュリティ アプライアンス用のエンタープライズ MIB の SNMPv2 互換の説明。
- IRONPORT-SMI.txt：この「管理情報構造」ファイルによって、websecurityappliance-mib の役割を定義します。

このリリースには、RFC 1213 および 1907 で規定されている MIB-II の読み取り専用のサブセットが実装されています。

SNMP モニタリングのイネーブル化と設定

SNMP をアプライアンスのシステム ステータス情報を収集するように設定するには、コマンドライン インターフェイス（CLI）で `snmpconfig` コマンドを使用します。インターフェイスの値を選択し、設定し終えると、アプライアンスは SNMPv3 GET 要求に応答します。

SNMP モニタリングを使用する場合、以下の点に注意してください。

- これらのバージョン 3 要求には、一致するパスフレーズが含まれている必要があります。
- デフォルトでは、バージョン 1 および 2 要求は拒否されます。
- イネーブルにする場合は、バージョン 1 および 2 要求に一致するコミュニティ ストリングが含まれている必要があります。

ハードウェア オブジェクト

Intelligent Platform Management Interface Specification（IPMI）準拠のハードウェア センサーによって、温度、ファン スピード、および電源モジュール ステータスなどの情報が報告されます。

モニタリング可能なハードウェア関連オブジェクト（たとえば、ファンの数や動作温度範囲）を確認するには、アプライアンス モデルのハードウェア ガイドを参照してください。

関連項目

- ドキュメント セット（C-2 ページ）

SNMP トラップ

SNMP には、1 つまたは複数の条件が合致したときにトラップ（または通知）を送信して管理アプリケーションに知らせる機能が備わっています。トラップとは、トラップを送信するシステムのコンポーネントに関するデータを含むネットワーク パケットです。トラップは、SNMP エージェント（この場合は Cisco Web セキュリティ アプライアンス アプライアンス）で条件が満たされた場合に生成されます。条件が満たされると、SNMP エージェントは SNMP パケットを形成し、SNMP 管理コンソール ソフトウェアを実行中のホストに送信します。

インターフェイスに対して SNMP をイネーブルにするときに、SNMP トラップを設定（特定のトラップをイネーブルまたはディセーブルに）できます。

複数のトラップ ターゲットの指定方法: トラップ ターゲットの入力を求められたときに、カンマで区切った IP アドレスを 10 個まで入力できます。

関連項目

- SNMP の connectivityFailure トラップについて（22-42 ページ）

SNMP の connectivityFailure トラップについて

connectivityFailure トラップは、インターネットへのアプライアンスの接続をモニタするために使用されます。これは、5～7 秒ごとに 1 つの外部サーバに接続して HTTP GET 要求を送信する試みにより実行されます。デフォルトでは、モニタされる URL はポート 80 上の `downloads.ironport.com` です。

モニタする URL またはポートを変更するには、`snmpconfig` コマンドを実行し、connecivityFailure トラップをイネーブルにします（すでにイネーブルになっている場合も実行します）。URL を変更するプロンプトが表示されます。

ヒント　connectivityFailure トラップをシミュレートするために、`dnsconfig` CLI コマンドを使用して、未使用の DNS サーバを入力することができます。downloads.ironport.com の検索は失敗し、5 ～ 7 秒ごとにトラップが送信されます。テストが完了したら、DNS サーバを使用中のサーバーに戻してください。

CLI の例：snmpconfig

```
wsa.example.com> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP

Do you want to enable SNMP?
[Y]>

Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: wsa.example.com)
[1]>

Which port shall the SNMP daemon listen on interface "Management"?
[161]>

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2

Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2

Enter the SNMPv3 authentication passphrase.
[]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[]>
Enter the SNMPv3 privacy passphrase.
[]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[]>

Service SNMP V1/V2c requests?
[N]> Y

Enter the SNMP V1/V2c community string.
[cisco]> public

Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>

From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>

Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred).Enter "None" to disable traps.
[127.0.0.1]> 203.0.113.1

Enter the Trap Community string.
[cisco] > tcomm

Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
```

```
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
[N]> Y

Do you want to disable any of these traps?
[Y]> n

Do you want to enable any of these traps?
[Y]> y

Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 1,7,12

What threshold would you like to set for CPU utilization?
[95]>

What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>

What threshold would you like to set for memory utilization?
[95]>

Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3

Enter the System Contact string.
[snmp@localhost]> wsa-admin@example.com

Current SNMP settings:
Listening on interface "Management" 198.51.100.1  port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: wsa-admin@example.com

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>

wsa.example.com> commit

Please enter some comments describing your changes:
[]> Enable and configure SNMP

Changes committed: Fri Nov 06 18:13:16 2015 GMT
wsa.example.com>
```