



## システム管理

この章は、次の項で構成されています。



(注) このセクションに記載されている機能またはコマンドには、ルーティングの優先順位に影響を与えるものや、影響を受けるものが含まれています。詳細については、付録B「IPアドレスのインターフェイスおよびルーティング」を参照してください。

- [アプライアンスの管理 \(2 ページ\)](#)
- [Cisco E メールセキュリティ アプライアンスのライセンス \(5 ページ\)](#)
- [Cisco E メールセキュリティ仮想アプライアンスのライセンス \(15 ページ\)](#)
- [設定ファイルの管理 \(16 ページ\)](#)
- [\[設定ファイル \(Configuration File\) \] ページ \(21 ページ\)](#)
- [ディスク領域の管理 \(22 ページ\)](#)
- [セキュリティ サービスの管理 \(24 ページ\)](#)
- [サービス アップデート \(26 ページ\)](#)
- [アップグレードおよびアップデートを取得するための設定 \(27 ページ\)](#)
- [AsyncOS のアップグレード \(36 ページ\)](#)
- [リモート電源再投入の有効化 \(42 ページ\)](#)
- [AsyncOS の以前のバージョンへの復元 \(43 ページ\)](#)
- [アプライアンスに生成されるメッセージの返信アドレスの設定 \(45 ページ\)](#)
- [システム状態パラメータのしきい値の設定 \(46 ページ\)](#)
- [E メールセキュリティ アプライアンスの状況の確認 \(47 ページ\)](#)
- [アラート \(48 ページ\)](#)
- [ネットワーク設定値の変更 \(73 ページ\)](#)
- [システム タイム \(79 ページ\)](#)
- [ビューのカスタマイズ \(81 ページ\)](#)
- [Internet Explorer の互換モードの上書き \(83 ページ\)](#)
- [最大 HTTP ヘッダー サイズの構成 \(83 ページ\)](#)
- [サービス エンジンの再起動とステータスの表示 \(83 ページ\)](#)

# アプライアンスの管理

以下のタスクでは、アプライアンス内の一般的な機能を簡単に管理できます。

- [アプライアンスのシャットダウンおよび再起動](#) (2 ページ)
- [電子メールの受信と配信の一時停止](#) (2 ページ)
- [一時停止している電子メールの受信と配信の再開](#) (3 ページ)

## アプライアンスのシャットダウンおよび再起動

アプライアンスをシャットダウンまたは再起動した後は、配信キューにあるメッセージを失うことなく、アプライアンスを後で再起動できます。

CLI で shutdown または reboot コマンドを使用するか、Web インターフェイスを使用できます。

### 手順

- 
- ステップ 1** [システム管理 (System Administration) ] > [シャットダウン/サスペンド (Shutdown/Suspend) ] を選択します。
  - ステップ 2** [システム オペレーション (System Operations) ] セクションで、[操作 (Operation) ] ドロップダウンリストから [シャットダウン (Shutdown) ] または [再起動 (Reboot) ] を選択します。
  - ステップ 3** 開いている接続が、強制的に閉じられることなく完了できるまでの許容時間を秒数の単位で入力します。  
デフォルトの遅延値は 30 秒です。
  - ステップ 4** [確定する (Commit) ] をクリックします。
- 

## 電子メールの受信と配信の一時停止

AsyncOS では、電子メールの受信と配信を一時停止できます。次の動作を停止できます。

- 特定のリスナーまたは複数リスナーでの電子メールの受信。
- 特定のドメインまたは複数ドメインへの電子メールの配信。

CLI で suspend コマンドを使用するか、Web インターフェイスを使用します。

### 手順

- 
- ステップ 1** [システム管理 (System Administration) ] > [シャットダウン/サスペンド (Shutdown/Suspend) ] を選択します。
  - ステップ 2** 特定のリスナーまたは複数リスナーでの電子メールの受信を一時停止します。

[メールの操作 (Mail Operations)] セクションで、一時停止する機能またはリスナーを選択します。アプライアンスに複数のリスナーが存在する場合は、リスナー単位で電子メールの受信を停止することもできます。

- ステップ 3** 特定のドメインまたは複数ドメインへの電子メールの配信を一時停止します。要件に応じて、次のいずれかを実行します。
1. すべての電子メールの配信を停止するには、[ドメイン/サブドメインの指定 (Specify Domain(s)/Subdomain(s))] フィールドに ALL と入力し、[Enter] を押します。
  2. 特定のドメインまたはサブドメインへの電子メールの配信を停止するには、[ドメイン/サブドメインの指定 (Specify Domain(s)/Subdomain(s))] フィールドにドメインまたはサブドメインの名前または IP アドレスを入力し、[Enter] を押します。複数のエントリを追加する場合は、カンマ区切りのテキストを使用します。
- ステップ 4** 開いている接続が、強制的に閉じられることなく完了できるまでの許容時間を秒数の単位で入力します。
- 開いている接続が存在しない場合、システムはただちにオフラインになります。
- デフォルト遅延値は 30 秒です。
- ステップ 5** [確定する (Commit)] をクリックします。

---

#### 次のタスク

一時停止したサービスを再開する準備が整っている場合は、[一時停止している電子メールの受信と配信の再開 \(3 ページ\)](#) を参照してください。

## 一時停止している電子メールの受信と配信の再開

一時停止している電子メールの受信と配信を再開するには、[シャットダウン/サスペンド (Shutdown/Suspend)] ページまたは resume コマンドを使用します。

#### 手順

- 
- ステップ 1** [システム管理 (System Administration)] > [シャットダウン/サスペンド (Shutdown/Suspend)] を選択します。
- ステップ 2** [メールの操作 (Mail Operations)] セクションで、再開する機能またはリスナーを選択します。
- アプライアンスに複数のリスナーが存在する場合は、リスナー単位で電子メールの受信を再開できます。
- ステップ 3** すべての電子メール、または特定の1つ以上のドメインへの電子メールの配信を再開します。
- [ドメイン/サブドメインの指定 (Specify Domain(s)/Subdomain(s))] フィールドで、該当するエントリを閉じるアイコンをクリックします。

ステップ4 [確定する (Commit) ]をクリックします。

## 出荷時の初期状態へのリセット



**注意** シリアルインターフェイスを使用して、またはデフォルトの Admin ユーザアカウントで管理ポート上のデフォルト設定を使用して Web インターフェイスまたは CLI に再接続できない場合は、出荷時の初期状態にリセットしないでください。

アプライアンスを物理的に移動する際、出荷時の初期状態で始めなければならない場合があります。出荷時の設定にリセットすると元に戻せないため、ユニットを移動する場合や、設定の問題を解決する最後の手段としてのみ使用してください。出荷時の初期状態にリセットすると、Web インターフェイスまたは CLI から切断され、アプライアンスへの接続に使用したサービス (FTP、SSH、HTTP、HTTPS) がディセーブルにされ、作成した追加のユーザアカウントが削除されます。次の方法で、出荷時の初期状態にリセットできます。

- Web インターフェイスで、[システム管理 (System Administration) ]>[設定ファイル (Configuration File) ] ページの [リセット (Reset) ] ボタンをクリックするか、[システム管理 (System Administration) ]>[システムセットアップウィザード (System Setup Wizard) ] の [設定情報のリセット (Reset Configuration) ] ボタンをクリックします。
- CLI で、**resetconfig** コマンドを使用します。



(注) **resetconfig** コマンドは、アプライアンスがオフライン状態にあるときのみ動作します。出荷時の設定にリセットした後、アプライアンスはオンライン状態に戻ります。

## 次の手順

- システムセットアップウィザードを実行します。詳細については、[システムセットアップウィザードの使用](#)を参照してください。
- メール配信をオンにして、メール配信を再開します。

## AsyncOS のバージョン情報の表示

アプライアンスに現在インストールされている AsyncOS のバージョンを確認するには、Web インターフェイスの [モニタ (Monitor) ] メニューから [システム概要 (System Overview) ] ページを使用するか ([システムステータス](#)を参照)、CLI で **version** コマンドを使用します。

# Cisco E メール セキュリティ アプライアンスのライセンス

- [ライセンス キー \(5 ページ\)](#)
- [スマート ソフトウェア ライセンシング \(7 ページ\)](#)

## ライセンス キー

- [ライセンス キーの追加および管理 \(5 ページ\)](#)
- [ライセンス キーのダウンロードとアクティベーションの自動化 \(6 ページ\)](#)
- [期限切れ機能キー \(7 ページ\)](#)

## ライセンス キーの追加および管理

物理アプライアンスの場合、ライセンスキーはアプライアンスのシリアル番号に固有で、有効化されている機能に固有です（他のシステム上の1つのシステムでキーを再利用することはできません）。

CLI のライセンス キーを使用するには、**featurekey** コマンドを使用します。

### 手順

**ステップ 1** [システム管理 (System Administration) ] > [ライセンス キー (Feature Keys) ] を選択します。

**ステップ 2** アクションの実行：

目的	操作手順
実行中のライセンスキーのステータスを表示します	[シリアル番号 <serial number> のライセンス キー (Feature Keys for <serial number> ) ] セクションを確認します。
アプライアンスに対して発行されていて、まだアクティベーションされていないライセンス キーを表示します	[保留中のライセンス (Pending Activation) ] セクションを確認します。  自動ダウンロードおよびアクティベーションを有効にしている場合は、ライセンスキーはこのリストには表示されません。

目的	操作手順
最近発行されたライセンスキーを確認する	[保留中のライセンス (Pending Activation) ]セクションで、[新しいキーをチェック (Check for New Keys) ] ボタンをクリックします。  これはライセンスキーの自動ダウンロードおよびアクティベーションを有効にしていない場合、または次の自動チェックの前にライセンス キーをダウンロードする必要がある場合に役立ちます。
発行されたライセンスキーをアクティブ化します	[保留中のライセンス (Pending Activation) ] リストで、[選択したキーを有効化 (Activate Selected Keys) ] をクリックします。
新しいライセンス キーを追加します	[機能の有効化 (Feature Activation) ] セクションを使用します。

#### 次のタスク

#### 関連項目

- [ライセンス キーのダウンロードとアクティベーションの自動化 \(6 ページ\)](#)
- [\[設定ファイル \(Configuration File\) \] ページ \(21 ページ\)](#)

## ライセンス キーのダウンロードとアクティベーションの自動化

このアプライアンスに対して発行されたライセンスキーを自動的にチェック、ダウンロードおよびアクティブ化するようアプライアンスを設定できます。

#### 手順

- ステップ 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。
- ステップ 2** [ライセンス キー設定の編集 (Edit Feature Key Settings) ] をクリックします。
- ステップ 3** 新しいライセンス キーのチェック頻度を確認するには、 (?) ヘルプ ボタンをクリックしてください。
- ステップ 4** 設定事項を指定します。
- ステップ 5** 変更を送信し、保存します。

#### 次のタスク

#### 関連項目

- [ライセンス キーの追加および管理 \(5 ページ\)](#)

## 期限切れ機能キー

ライセンス キーの有効期限が切れる場合、キー失効の 90 日前、60 日前、30 日前、15 日前、5 日前、1 日前、およびキー失効時にアラートが送信されます。これらのアラートを受信するには、システムアラートに登録されていることを確認してください。詳細については、[アラート \(48 ページ\)](#) を参照してください。

(Web インターフェイスを使用して) アクセスしようとしている機能の機能キーの有効期限が切れている場合は、シスコの担当者またはサポート組織までご連絡ください。

## スマート ソフトウェア ライセンシング

- [概要 \(7 ページ\)](#)
- [スマート ソフトウェア ライセンシングのイネーブル化 \(9 ページ\)](#)
- [Cisco Smart Software Manager でのアプライアンスの登録 \(10 ページ\)](#)
- [ライセンスの要求 \(11 ページ\)](#)
- [Cisco Smart Software Manager からのアプライアンスの登録解除 \(12 ページ\)](#)
- [Cisco Smart Software Manager でのアプライアンスの再登録 \(12 ページ\)](#)
- [転送設定の変更 \(13 ページ\)](#)
- [認証と証明書を更新 \(13 ページ\)](#)
- [スマート エージェントの更新 \(14 ページ\)](#)
- [アラート \(13 ページ\)](#)
- [クラスタ モードでのスマート ライセンス \(15 ページ\)](#)

## 概要

スマート ソフトウェア ライセンシングを使用すると、Cisco E メール セキュリティ アプライアンスのライセンスをシームレスに管理およびモニタできます。スマート ソフトウェア ライセンスをアクティブ化するには、Cisco Smart Software Manager (CSSM) でアプライアンスを登録する必要があります。CSSM は、購入して使用するすべてのシスコ製品についてライセンスの詳細を管理する一元化されたデータベースです。スマート ライセンスを使用すると、製品認証キー (PAK) を使用して Web サイトで個別に登録するのではなく、単一のトークンで登録することができます。

アプライアンスを登録すると、アプライアンスのライセンスを追跡し、CSSM ポータル経由でライセンスの使用状況を監視できます。アプライアンスにインストールされているスマート エージェントは、アプライアンスと CSSM を接続し、ライセンスの使用状況に関する情報を CSSM を渡して、CSSM が使用状況を追跡できるようにします。

Cisco Smart Software Manager については [https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b\\_Smart\\_Licensing\\_Deployment\\_Guide.html](https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html) を参照してください。

### 始める前に

- ご利用のアプライアンスからインターネットに接続できることを確認します。
- シスコ セールス チームに問い合わせた Cisco Smart Software Manager ポータル (<https://software.cisco.com/#module/SmartLicensing>) でスマートアカウントを作成するか、Cisco Smart Software Manager サテライトをネットワークにインストールしてください。

Cisco Smart Software Manager ユーザ アカウントの作成または Cisco Smart Software Manager サテライトのインストールの詳細については、[https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b\\_Smart\\_Licensing\\_Deployment\\_Guide.html](https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html) を参照してください。

ライセンスの使用状況に関する情報を直接インターネットに送信したくないユーザの場合、CSSM 機能のサブセットを提供する Smart Software Manager サテライトをオンプレミスにインストールすることもできます。サテライトアプリケーションをダウンロードして導入した後は、インターネットを使用して CSSM にデータを送信せずに、ライセンスをローカルで安全に管理できます。CSSM サテライトは、情報をクラウドに定期的に送信します。



---

(注) Smart Software Manager サテライトを使用する場合、Smart Software Manager サテライト Enhanced Edition 6.1.0 を使用してください。

---

- (従来の) クラシック ライセンスの既存ユーザは、クラシック ライセンスをスマート ライセンスに移行する必要があります。  
<https://video.cisco.com/detail/video/5841741892001/convert-classic-licenses-to-smart-licenses?autoStart=true&q=classic> を参照してください。
- アプライアンスのシステム クロックを CSSM のシステム クロックと同期させる必要があります。アプライアンスのシステム クロックと CSSM のシステム クロックのずれは、スマート ライセンス操作の失敗の原因となります。



---

(注) インターネットに接続してプロキシ経由で CSSM に接続する場合、[セキュリティサービス (Security Services)] > [サービスのアップデート (Service updates)] を使用して、アプライアンスに設定されているプロキシと同じプロキシを使用する必要があります

---





- (注) 仮想ユーザの場合、新しい PAK ファイル（新規または更新）を受信するたびに、ライセンス ファイルを生成し、アプライアンスのファイルを読み込みます。ファイルを読み込んだ後は、PAK をスマート ライセンスに変換する必要があります。スマート ライセンス モードでは、ファイルのロード中、ライセンス ファイルの機能キー セクションは無視され、証明書情報のみを使用されます。

アプライアンスに対してスマート ソフトウェア ライセンシングを有効にするには、次の手順を実行する必要があります。

	操作内容	詳細情報
ステップ 1	スマートソフトウェア ライセンシングの有効化	<a href="#">スマートソフトウェア ライセンシングのイネーブル化 (9 ページ)</a>
ステップ 2	Cisco Smart Software Manager でのアプライアンスの登録	<a href="#">Cisco Smart Software Manager でのアプライアンスの登録 (10 ページ)</a>
ステップ 3 :	ライセンス (機能キー) の要求	<a href="#">ライセンスの要求 (11 ページ)</a>

## スマート ソフトウェア ライセンシングのイネーブル化

### 手順

- ステップ 1** [システム管理 (System Administration)] > [スマートソフトウェアライセンス (Smart Software Licensing)] を選択します。
- ステップ 2** [スマート ソフトウェア ライセンシングの有効化 (Enable Smart Software Licensing)] をクリックします。
- スマートソフトウェア ライセンシングの詳細については、スマートソフトウェア ライセンシングの詳細のリンクをクリックします。
- ステップ 3** スマートソフトウェア ライセンシングについての情報を読んだ後、**[OK]** をクリックします。
- ステップ 4** 変更を保存します。

### 次のタスク

スマートソフトウェア ライセンシングを有効すると、クラシック ライセンス モードのすべての機能がスマート ライセンス モードでも自動的に使用可能になります。クラシック ライセン

モードの既存ユーザの場合、CSSM でアプライアンスを登録せずに、スマート ソフトウェア ライセンシング機能を使用できる 90 日間の評価期間があります。

有効期限および評価期間の期限の前に、一定の間隔（90 日前、60 日前、30 日前、15 日前、5 日前、および最終日）で通知が表示されます。評価期間の間または終了後に、CSSM でアプライアンスを登録できます。



- (注) クラシック ライセンス モードにおけるアクティブなライセンスを持たない仮想アプライアンスの新規ユーザの場合、スマート ソフトウェア ライセンシング機能を有効にしても、評価期間は提供されません。クラシック ライセンス モードにおけるアクティブなライセンスを持つ仮想アプライアンスの既存ユーザのみに、評価期間が提供されます。新規仮想アプライアンスユーザがスマート ライセンス機能の評価を希望する場合には、シスコセールス チームに連絡し、スマートアカウントに評価ライセンスを追加してください。評価ライセンスは、登録後に評価目的で使用されます。



- (注) アプライアンスでスマート ライセンシング機能を有効にすると、スマート ライセンシングからクラシック ライセンシング モードにロールバックすることができなくなります。

## Cisco Smart Software Manager でのアプライアンスの登録

アプライアンスを Cisco Smart Software Manager に登録するには、[システム管理 (System Administration)] メニューでスマート ソフトウェア ライセンシング機能を有効にする必要があります。

### 手順

- ステップ 1** [システム管理 (System Administration)] > [スマートソフトウェアライセンシング (Smart Software Licensing)] を選択します。
- ステップ 2** [トランスポート設定 (Transport Settings)] を変更する場合には、[編集 (Edit)] をクリックします。次のオプションを使用できます。
- [直接 (Direct)] : アプライアンスを HTTPS 経由で Cisco Smart Software Manager に直接接続します。このオプションは、デフォルトで選択されます。
  - [トランスポートゲートウェイ (Transport Gateway)] : アプライアンスをトランスポートゲートウェイまたは Smart Software Manager サテライト経由で Cisco Smart Software Manager に接続します。このオプションを選択した場合、トランスポートゲートウェイまたは Smart Software Manager サテライトの URL を入力してから [OK] をクリックする必要があります。このオプションは HTTP および HTTPS をサポートします。FIPS モードの場合、トランスポートゲートウェイは HTTPS のみをサポートします。トランスポートゲートウェイについては、

[https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b\\_Smart\\_Licensing\\_Deployment\\_Guide.html](https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html)を参照してください。

ログインクレデンシャルを使用して、Cisco Smart Software Manager ポータル

(<https://software.cisco.com/#module/SmartLicensing>) にアクセスします。新しいトークンを作成するには、このポータルの [仮想アカウント (Virtual Account) ] ページに移動して [全般 (General) ] タブにアクセスします。アプライアンス用の製品インスタンス登録トークンをコピーします。

製品インスタンス登録トークンの作成については、[https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b\\_Smart\\_Licensing\\_Deployment\\_Guide.html](https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html)を参照してください。

- ステップ 3 アプライアンスに戻り、製品インスタンス登録トークンを貼り付けます。
- ステップ 4 [登録 (Register) ] をクリックします。
- ステップ 5 [スマートソフトウェアライセンシング (Smart Software Licensing) ] ページで、[すでに登録されている場合は、この製品インスタンスを再登録します (Reregister this product instance if it is already registered) ] チェックボックスをオンにして、アプライアンスを再登録することもできます。[Cisco Smart Software Manager でのアプライアンスの再登録 \(12 ページ\)](#) を参照してください。

---

### 次のタスク

製品登録プロセスには数分かかります。[スマートソフトウェアライセンシング (Smart Software Licensing) ] ページで登録ステータスを表示できます。

## ライセンスの要求

登録プロセスが正常に完了した後、アプライアンスの機能のライセンスを要求しなければならない場合があります。

### 手順

- 
- ステップ 1 [システム管理 (System Administration) ] > [ライセンス (Licenses) ] を選択します。
  - ステップ 2 [設定の編集 (Edit Settings) ] をクリックします。
  - ステップ 3 要求するライセンスに対応する [ライセンスの要求/リリース (License Request/Release) ] 列のチェックボックスをオンにします。
  - ステップ 4 [送信 (Submit) ] をクリックします。

(注) デフォルトでは、メール処理と E メール セキュリティ アプライアンスのバウンス検証のライセンスを利用できます。これらのライセンスは、有効化、無効化、またはリリースすることができません。

メール処理と E メール セキュリティ アプライアンスのバウンス検証のライセンスに評価期間やコンプライアンス違反はありません。これは、仮想アプライアンスには適用されません。

---

### 次のタスク

ライセンスは、期限超過また期限切れになるとコンプライアンス違反 (OOC) モードになり、各ライセンスに 30 日間の猶予期間が提供されます。有効期限および OOC 猶予期間の期限の前に、一定の間隔 (30 日前、15 日前、5 日前、および最終日) で通知が表示されます。

OOC 猶予期間の有効期限が過ぎると、ライセンスは使用できず、機能を利用できなくなります。機能にもう一度アクセスするには、CSSM ポータルでライセンスをアップデートして、認証を更新する必要があります。

## Cisco Smart Software Manager からのアプライアンスの登録解除

### 手順

- 
- ステップ 1 [システム管理 (System Administration)] > [スマートソフトウェアライセンシング (Smart Software Licensing)] を選択します。
  - ステップ 2 [アクション (Action)] ドロップダウン リストから、[登録解除 (Deregister)] を選択し、[実行 (Go)] をクリックします。
  - ステップ 3 [送信 (Submit)] をクリックします。
- 

## Cisco Smart Software Manager でのアプライアンスの再登録

### 手順

- 
- ステップ 1 [システム管理 (System Administration)] > [スマートソフトウェアライセンシング (Smart Software Licensing)] を選択します。
  - ステップ 2 [アクション (Action)] ドロップダウン リストから、[登録 (Register)] を選択し、[実行 (Go)] をクリックします。
-

### 次のタスク

登録プロセスについては、[Cisco Smart Software Manager でのアプライアンスの登録 \(10 ページ\)](#) を参照してください。

回避できないシナリオにおいては、アプライアンスの設定をリセットした後にアプライアンスを登録することができます。

## 転送設定の変更

CSSM でアプライアンスを登録する前にのみ、トランスポート設定を変更できます。



- (注) スマート ライセンス機能が有効になっている場合にのみ、トランスポート設定を変更できます。アプライアンスがすでに登録されている場合、トランスポート設定を変更するには、アプライアンスの登録を解除する必要があります。トランスポート設定を変更した後に、アプライアンスを再登録する必要があります。

トランスポート設定を変更する方法は、[Cisco Smart Software Manager でのアプライアンスの登録](#)を参照してください。

## 認証と証明書を更新

Cisco Smart Software Manager でアプライアンスを登録した後に、証明書を更新できます。



- (注) アプライアンスが正常に登録された後にのみ、認証を更新できます。

### 手順

**ステップ 1** [システム管理 (System Administration) ] > [スマートソフトウェアライセンスング (Smart Software Licensing) ] を選択します。

**ステップ 2** [アクション (Action) ] ドロップダウン リストから、適切なオプションを選択します。

- 認証を今すぐ更新
- 証明書を今すぐ更新

**ステップ 3** [移動 (Go) ] をクリックします。

## アラート

次のシナリオで通知が送信されます。

- スマート ソフトウェア ライセンスングが正常に有効化された

- スマート ソフトウェア ライセンシングの有効化に失敗した
- 評価期間が開始された
- 評価期間が終了した（評価期間中および期間終了時に一定の間隔で送信）
- 正常に登録された
- 登録に失敗した
- 正常に認証された
- 認証に失敗した
- 正常に登録解除された
- 登録解除に失敗した
- ID 証明書が正常に更新された
- ID 証明書の更新に失敗した
- 認証の有効期限が切れた
- ID 証明書の有効期限が切れた
- コンプライアンス違反猶予期間の期限が切れた（コンプライアンス違反猶予期間中および期間終了時に一定の間隔で送信）
- 機能の有効期限に関する最初のインスタンスが発生した

## スマート エージェントの更新

アプライアンスにインストールされているスマート エージェントのバージョンを更新するには、次の手順を実行します。

### 手順

---

**ステップ 1** [システム管理 (System Administration)] > [スマートソフトウェアライセンス (Smart Software Licensing)] を選択します。

**ステップ 2** [スマートエージェントの更新ステータス (Smart Agent Update Status)] セクションで、[今すぐ更新 (Update Now)] をクリックし、プロセスに従います。

(注) CLI コマンド `saveconfig` を使用して、または [システム管理 (System Administration)] > [設定サマリー (Configuration Summary)] を使用して Web インターフェイス経由で設定変更を保存しようとする、スマートライセンス関連の設定は保存されません。

---

## クラスタモードでのスマートライセンス



- (注) スマートライセンス機能のクラスタ管理は、マシンモードのみで利用できます。クラスタモードでのスマートライセンスでは、任意のアプライアンスにログインしてスマートライセンスを設定できます。アプライアンスにログインし、クラスタの他のアプライアンスに1つずつアクセスして、最初のアプライアンスからログオフすることなくスマートライセンス機能を設定できます。

詳細については、[クラスタを使用した中央集中型管理](#)を参照してください。

## Cisco Eメールセキュリティ仮想アプライアンスのライセンス

Eメールセキュリティ仮想アプライアンスのセットアップとライセンス付与については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。このマニュアルは、に記載されている場所から入手できます。



- (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、またはシステムセットアップウィザードを実行することはできません。

## 仮想アプライアンスのライセンスの有効期限

仮想アプライアンスのライセンスの有効期限が切れてから180日間、このアプライアンスはセキュリティサービスなしでメールの配信を続行します。この期間中、セキュリティサービスは更新されません。

ライセンスの有効期限が切れる時点から180日前、150日前、120日前、90日前、60日前、30日前、15日前、5日前、1日前、および0秒前にアラートが送信されます。また、猶予期間の終了についても、同じ間隔でアラートが送信されます。これらは、[システム (System)] タイプ、[重大 (Critical)] 重大度レベルのアラートです。確実にアラートが届くようにするには、[アラート受信者の追加 \(49 ページ\)](#) を参照してください。

これらのアラートはシステムログにも記録されます。

個々のライセンスキーが、仮想アプライアンスのライセンスよりも先に期限切れになることがあります。これらの有効期限が近づいてきた場合にも、アラートが送信されます。

### 関連項目

- 仮想アプライアンスでの AsyncOS の復元がライセンスに影響を及ぼす可能性 (44 ページ)

## 設定ファイルの管理

アプライアンス内のすべての設定は、1つの設定ファイルで管理できます。このファイルは Extensible Markup Language (XML) 形式で保持されます。

このファイルは次の複数の方法で使用できます。

- 設定ファイルを別のシステムに保存し、重要な設定データをバックアップおよび保持できます。アプライアンスの設定を間違えた場合、保存した最新のコンフィギュレーションファイルに「ロールバック」できます。
- 既存のコンフィギュレーションファイルをダウンロードし、アプライアンスの全体的設定を素早く確認できます（新しいブラウザの多くに、XML ファイルを直接レンダリングする機能が含まれています）。現在の設定にマイナーエラー（誤入力など）があった場合、この機能がトラブルシューティングに役立つことがあります。
- 既存のコンフィギュレーションファイルをダウンロードし、変更を行い、そのファイルを同じアプライアンスにアップロードできます。この場合は、実質的に設定の変更を行うために CLI と Web インターフェイスの両方が「バイパス」されます。
- FTP アクセスを使用して設定ファイル全体をアップロードしたり、設定ファイルの一部または全体を CLI に直接貼り付けたりできます。
- ファイルは XML 形式であるため、設定ファイルのすべての XML エンティティを定義する、関連付けられた Document Type Definition (DTD) も提供されます。XML 設定ファイルをアップロードする前にこの DTD をダウンロードして XML 設定ファイルを検証できます（XML 検証ツールはインターネットで簡単に入手できます）。

## XML 設定ファイルを使用した複数のアプライアンスの管理

- あるアプライアンスから既存の設定ファイルをダウンロードし、変更を行い、別のアプライアンスにアップロードできます。これにより、複数のアプライアンスのインストールを簡単に管理できるようになります。現時点では、設定ファイルを C/X シリーズアプライアンスから M シリーズアプライアンスにロードできません。
- あるアプライアンスからダウンロードされた既存のコンフィギュレーションファイルを、複数のサブセクションに分割できます。（複数のアプライアンス環境の）すべてのアプライアンスで共通するこれらのセクションを変更し、サブセクションの更新時にこれらのセクションを他のアプライアンスにロードできます。

たとえば、Global Unsubscribe コマンドをテストするためにテスト環境でアプライアンスを使用できます。グローバル配信停止リストを適切に設定した場合は、テストアプライアンスのグローバル配信停止設定セクションをすべての実稼働アプライアンスにロードできます。

## コンフィギュレーションファイルの管理

アプライアンスで設定ファイルを管理するには、[システム管理 (System Administration)] > [設定ファイル (Configuration File)] をクリックします。

[設定ファイル (Configuration File)] ページには、次のセクションが含まれています。



- [現在の設定 (Current Configuration)] : 現在の設定ファイルを保存およびエクスポートするために使用します。
- [設定をロード (Load Configuration)] : 設定ファイル全体または一部をロードするために使用します。
- [エンドユーザセーフリスト/ブロックリストデータベース (スパム隔離) (End-User Safelist/Blocklist Database (Spam Quarantine))] : 詳細については、[セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御](#)および[セーフリスト/ブロックリストのバックアップと復元](#)を参照してください。
- [設定情報のリセット (Reset Configuration)] : 現在の設定を出荷時デフォルト値にリセットするために使用します (リセット前に設定を保存する必要があります)。



(注) 秘密キーと証明書は設定ファイルと暗号化パスワードと共に、暗号化されない PEM 形式で含まれます。

#### 関連項目

- [現在の設定ファイルの保存およびエクスポート \(17 ページ\)](#)
- [コンフィギュレーションファイルのロード \(18 ページ\)](#)
- [設定ファイルのメール送信 \(18 ページ\)](#)
- [現在の設定のリセット \(21 ページ\)](#)

## 現在の設定ファイルの保存およびエクスポート

[システム管理 (System Administration)] > [設定ファイル (Configuration File)] ページの [現在の設定 (Current Configuration)] セクションを使用すると、現在の設定ファイルを、ローカルマシンに保存したり、アプライアンスで保存したり (FTP/SCP ルートの `configuration` ディレクトリに保存されます)、指定されたアドレスに電子メールで送信したりできます。

次の情報は、設定ファイルには保存されません。

- URL フィルタリング機能で使用されるサービスとのセキュアな通信に使用される証明書。
- [テクニカルサポートに問い合わせる (Contact Technical Support)] ページに保存されている CCO ユーザ ID と契約 ID。

[設定ファイル内のパスワードを隠す (Mask passphrases in the Configuration Files)] チェックボックスをクリックして、ユーザのパスワードをマスクできます。パスワードをマスクすると、元の暗号化されたパスワードが、エクスポートまたは保存されたファイルで「\*\*\*\*\*」に置き換えられます。ただし、パスワードがマスクされた設定ファイルを AsyncOS に再びロードすることはできないことに注意してください。

[設定ファイル内のパスワードを隠す (Encrypt passphrases in the Configuration Files)] チェックボックスをクリックして、ユーザのパスワードをマスクできます。次に、暗号化される、設定ファイル内の重要なセキュリティ パラメータを示します。

- 証明書の秘密キー
- RADIUS パスワード

- LDAP バインドのパスワード
- ローカル ユーザのパスワードのハッシュ
- SNMP パスワード
- DK/DKIM 署名キー
- 発信 SMTP 認証パスワード
- PostX 暗号化キー
- PostX 暗号化プロキシパスワード
- FTP プッシュ ログ サブスクリプションのパスワード
- IPMI LAN パスワード
- アップデータ サーバの URL

これは、saveconfig コマンドを使用してコマンドライン インターフェイスでも構成できます。

## 設定ファイルのメール送信

[システム管理 (System Administration)] > [設定ファイル (Configuration File)] の [ファイルをメールで送信 (Email file to)] フィールドを使用するか、mailconfig コマンドを使用して、現在の設定を添付ファイルとしてユーザにメール送信できます。

## コンフィギュレーション ファイルのロード

[システム管理 (System Administration)] > [設定ファイル (Configuration File)] ページの [設定をロード (Load Configuration)] セクションを使用して、新しい設定情報をアプライアンスにロードします。これは、loadconfig コマンドを使用してコマンドライン インターフェイスでも構成できます。

情報は次の 3 つのいずれかの方法でロードできます。

- configuration ディレクトリに情報を格納し、アップロードする。
- 設定ファイルをローカル マシンから直接アップロードする。
- 設定情報を直接貼り付ける。



(注) パスフレーズがマスクされた設定ファイルはロードできません。

クラスタモードでは、クラスタまたはアプライアンスのいずれの設定をロードするかを選択できます。クラスタ設定をロードする手順については、[クラスタ化されたアプライアンスの設定のロード](#)を参照してください。

どの方法の場合でも、設定の上部に次のタグを含める必要があります。

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>
```

```
... your configuration information in valid XML
```

```
</config>
```

</config>閉じタグは設定情報の後に指定する必要があります。XML構文の値は、アプライアンスの configuration ディレクトリにある DTD (Document Type Definition) を使用して解析および検証されます。DTD ファイルの名前は config.dtd です。loadconfig コマンドを使用したときにコマンドラインで検証エラーが報告された場合、変更はロードされません。設定ファイルをアップロードする前に、アプライアンスの外部で DTD をダウンロードし、設定ファイルを検証できます。

いずれの方法の場合でも、設定ファイル全体 (最上位のタグである <config></config> 間で定義された情報) または設定ファイルの *complete* および *unique* サブセクション (上記の宣言タグが含まれ、<config></config> タグ内に存在する場合) をインポートできます。

「complete (完全)」とは、DTD で定義されたサブセクションの開始タグおよび終了タグ全体が含まれることを意味します。たとえば、次の内容をアップロードまたは解析します。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<!DOCTYPE config SYSTEM "config.dtd">
```

```
<config>
```

```
<autosupport_enabled>0</autosu
```

```
</config>
```

この場合は、アップロード中に検証エラーが発生します。ただし、

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<!DOCTYPE config SYSTEM "config.dtd">
```

```
<config>
```

```
<autosupport_enabled>0</autosupport_enabled>
```

```
</config>
```

この場合は、検証エラーが発生しません。

「unique (一意)」とは、アップロードまたは貼り付けられる設定ファイルのサブセクションが、設定として多義的でないことを意味します。たとえば、システムは1つのホスト名しか持つことができないため、次の内容 (宣言と <config></config> タグを含む) をアップロードすることは可能です。

```
<hostname>mail4.example.com</hostname>
```

上記の内容は許容されます。ただし、システムでは複数のリスナーを定義できるため (リスナーごとに異なる受信者アクセステーブルが定義されます)、

```

<rat>

  <rat_entry>

    <rat_address>ALL</rat_address>

    <access>RELAY</access>

  </rat_entry>

</rat>

```

上記の内容だけをアップロードすることは多義的と見なされ、「完全」な構文であっても許可されません。



**注意** 設定ファイルまたは設定ファイルのサブセクションをアップロードまたは解析する場合は、待機中の可能性がある、保存されていない変更が破棄されることがあります。

設定ファイルのディスク領域の割り当てが、現在アプライアンスに保存されているデータの量よりも小さい場合、設定ファイルで指定されたクォータを満たすために、最も古いデータが削除されます。

## 空白タグと省略されたタグ

設定ファイルのセクションをアップロードまたは解析する場合は注意が必要です。タグを含めないと、コンフィギュレーションファイルのアップロード時に設定の値が変更されません。ただし、空白タグを含めると、設定の問題が解消されます。

たとえば、

```
<listeners></listeners>
```

上記の内容をアップロードすると、システムからすべてのリスナーが削除されます。



**注意** 設定ファイルのサブセクションをアップロードしたり、貼り付けたりした場合、Web インターフェイスまたは CLI から切断され、大量の設定データが破壊されることがあります。管理ポートで別のプロトコル、シリアルインターフェイス、またはデフォルト設定を使用してアプライアンスに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。また、DTD で定義された設定構文がよくわからない場合は、このコマンドを使用しないでください。新しい設定ファイルをアップロードする前に、必ず設定データをバックアップしてください。

## ログサブスクリプションのパスフレーズのロードについての注意事項

パスフレーズが必要なログサブスクリプションを含むコンフィギュレーションファイルをロードしようとしても（たとえば、FTP プッシュを使用）、loadconfig コマンドは不明なパスフレーズについて警告しません。FTP プッシュが失敗し、logconfig コマンドを使用して正しいパスフレーズを設定するまで警告が生成されます。

## 文字セットエンコーディングについての注意事項

XML コンフィギュレーション ファイルの「encoding」属性は、ファイルをオフラインで操作するために使用している文字セットに関係なく、「ISO-8859-1」である必要があります。showconfig コマンド、saveconfig コマンド、または mailconfig コマンドを発行するたびにエンコーディング属性がファイルで指定されることに注意してください。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

現時点では、このエンコーディングを持つ設定ファイルだけをロードできます。

### 関連項目

- [クラスタ化されたアプライアンスの設定のロード](#)

## 現在の設定のリセット

現在の設定をリセットすると、アプライアンスが元の出荷時デフォルト値に戻ります。リセットする前に設定を保存する必要があります。GUIでこのボタンを使用して設定をリセットすることは、クラスタリング環境ではサポートされていません。

[出荷時の初期状態へのリセット \(4 ページ\)](#) を参照してください。

## 設定ファイルの表示

設定ファイルの詳細は、showconfig コマンドを使用してのみ表示できます。showconfig コマンドは、現在の設定を画面に出力します。

```
mail3.example.com> showconfig
```

```
Do you want to include passphrases? Please be aware that a configuration without passphrases will fail when reloaded with loadconfig.
```

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<!DOCTYPE config SYSTEM "config.dtd">
```

```
<!--
```

```
Product: IronPort model number Messaging Gateway Appliance(tm)
```

```
Model Number: model number
```

```
Version: version of AsyncOS installed
```

```
Serial Number: serial number
```

```
Current Time: current time and date
```

```
[The remainder of the configuration file is printed to the screen.]
```

## [設定ファイル (Configuration File) ] ページ

- [設定ファイルの管理 \(16 ページ\)](#)
- [出荷時の初期状態へのリセット \(4 ページ\)](#)
- [セーフリスト/ブロックリストのバックアップと復元](#)

## ディスク領域の管理

- (仮想アプライアンスのみ) 使用可能なディスク領域の拡大 (22 ページ)
- ディスク領域の使用率の表示および割り当て (22 ページ)
- その他のクォータのディスク領域の管理 (23 ページ)
- ディスク領域に関するアラートの受信の確認 (24 ページ)

### (仮想アプライアンスのみ) 使用可能なディスク領域の拡大

ESXi 5.5 および VMFS 5 を実行する仮想アプライアンスの場合、2 TB を超えるディスク領域を割り当てることができます。ESXi 5.1 を実行するアプライアンスの場合は 2 TB に制限されます。

仮想アプライアンス インスタンスにディスク領域を追加するには、次の手順を実行します。



- (注) ディスク領域の削減はサポートされていません。詳細については、VMware のマニュアルを参照してください。

#### はじめる前に

必要な追加ディスク領域を慎重に検討します。

#### 手順

**ステップ 1** E メール セキュリティ アプライアンスのインスタンスをダウンさせます。

**ステップ 2** VMware が提供するユーティリティまたは管理ツールを使用してディスク領域を増やします。

VMware のマニュアルで仮想ディスク設定の変更に関する情報を参照してください。ESXi 5.5 に関するこの情報は、リリースの時点では、<http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html> で参照可能でした。

**ステップ 3** [システム管理 (System Administration)] > [ディスク管理 (Disk Management)] に移動して、変更内容が反映されたことを確認します。

### ディスク領域の使用率の表示および割り当て

アプライアンスで、展開で使用される各機能にディスク領域を割り当てることで、ディスク使用率を最適化できます。

目的	操作手順
<ul style="list-style-type: none"> <li>各サービスのディスク領域クォータと現在の使用率を表示します</li> <li>いつでもアプライアンスでディスク領域を再割り当てします</li> </ul>	[システム管理 (System Administration)] > [ディスク管理 (Disk Management)] に移動します。
データ ボリュームの管理	<ul style="list-style-type: none"> <li>サービスの報告と追跡およびスパム隔離の場合、最も古いデータが自動的に削除されます。</li> <li>ポリシー、ウイルス、アウトブレイク隔離の場合、隔離に設定されたデフォルトアクションが実行されます。<a href="#">隔離メッセージに自動的に適用されるデフォルトアクション</a>を参照してください。</li> <li>その他のクォータの場合、まず手動でデータを削除して、設定する新しいクォータを下回るように使用量を減らします。「<a href="#">その他のクォータのディスク領域の管理 (23 ページ)</a>」を参照してください。</li> </ul>

## その他のクォータのディスク領域の管理

その他のクォータにはシステム データとユーザ データが含まれます。システム データは削除できません。管理できるユーザ データには次のファイル タイプがあります。

管理対象	手順
ログ ファイル	<p>[システム管理 (System Administration)] &gt; [ログ サブスクリプション (Log Subscriptions)] に移動して、</p> <ul style="list-style-type: none"> <li>どのログ ディレクトリが最もディスク領域を消費しているかを確認します。</li> <li>生成されるすべてのログ サブスクリプションが必要であることを確認します。</li> <li>必要以上に詳細なログ レベルになっていないかを確認します。</li> <li>可能な場合は、ロールオーバー ファイル サイズを小さくします。</li> </ul>
パケット キャプチャ	[ヘルプとサポート (Help and Support)] (画面上部の右側付近) > [パケットキャプチャ (Packet Capture)] に移動します。

管理対象	手順
コンフィギュレーションファイル  (これらのファイルが多く のディスク領域を消費する 可能性は低いと考えられま す)。	アプライアンスの /data/pub ディレクトリに FTP でアクセスしま す。  アプライアンスへの FTP アクセスを構成するには、 <a href="#">FTP</a> 、 <a href="#">SSH</a> 、 <a href="#">および SCP アクセス</a> を参照してください。
クォータ サイズ	[システム管理 (System Administration) ]>[ディスク管理 (Disk Management) ]に移動します。

## ディスク領域に関するアラートの受信の確認

その他のディスク使用量がクォータの 75% に達すると、警告レベルのシステム アラートを受信します。これらのアラートを受信した場合は、対処する必要があります。

確実にアラートが届くようにするには、[アラート \(48 ページ\)](#) を参照してください。

## ディスク領域と集中管理

ディスク領域管理はマシン モードでのみ使用可能で、グループまたはクラスタ モードでは使用できません。

## セキュリティ サービスの管理

[サービスの概要 (Services Overview) ] ページには次のエンジンの現在のサービスとルール  
のバージョンがリストされます。

- Graymail
- McAfee
- Sophos

[サービスの概要 (Services Overview) ] ページでは、次のタスクを実行できます。

- エンジンを手動で更新します。詳細については、[エンジンの手動アップデート \(25 ページ\)](#) を参照してください。
- エンジンの以前のバージョンにロールバックします。詳細については、[エンジンの以前のバージョンへのロールバック \(25 ページ\)](#) を参照してください。

[自動更新 (Automatic Updates) ] 列は特定のエンジンの自動更新の状態を示します。自動更新を有効または無効にする場合、特定のエンジンの [グローバル設定 (Global Settings) ] ページに移動します。



特定のサービスエンジンの自動更新を無効にすると、警告が定期的に表示されます。警告の間隔を変更する場合、[セキュリティサービス (Security Services)] > [サービスのアップデート (Service Updates)] ページの [無効な自動エンジン更新のアラート間隔 (Alert Interval for Disabled Automatic Engine Updates)] オプションを使用します。



(注) ロールバックが適用されているエンジンの場合、自動更新は自動的に無効になります。

#### 関連項目

- [エンジンの手動アップデート \(25 ページ\)](#)
- [エンジンの以前のバージョンへのロールバック \(25 ページ\)](#)
- [ログの表示 \(26 ページ\)](#)
- [システムアラート \(57 ページ\)](#)

## エンジンの手動アップデート

#### 手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [サービスの概要 (Services Overview)] ページに進みます。
- ステップ 2** サービスエンジンの最新サービスまたはルールバージョンを参照するには、[入手可能な更新 (Available Updates)] 列の [更新 (Update)] をクリックします。  
(注) [更新 (Update)] オプションは、特定のエンジンの新しい更新が入手可能である場合にのみ使用できます。

## エンジンの以前のバージョンへのロールバック

#### 手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [サービスの概要 (Services Overview)] ページに進みます。
- ステップ 2** [バージョンの変更 (Modify Versions)] カラムで [変更 (Change)] をクリックします。
- ステップ 3** 必要なルールおよびサービスバージョンのアップデートを選択し、[適用 (Apply)] をクリックします。  
アプライアンスにより、エンジンが以前のバージョンにロールバックされます。

(注) サービスアップデートには、サービスバージョンとルールバージョンがパッケージとして一緒に含まれています。

[適用 (Apply)] をクリックすると、そのエンジンの自動更新が自動的に無効になります。自動更新を有効にするには、そのエンジンの [グローバル設定 (Global Settings)] ページに移動します。

## ログの表示

エンジンのロールバックおよび自動更新の無効化に関する情報は、次のログに記載されます。

- アップデータ ログ：エンジンのロールバックおよびエンジンの自動更新に関する情報が含まれます。ほとんどの情報は [情報 (Info)] または [デバッグ (Debug)] レベルです。

詳細については、[アップデータ ログの例](#)を参照してください。

## サービス アップデート

次のサービスは最大の効果得るために更新する必要があります。

- ライセンス キー (Feature Keys)
- McAfee Anti-Virus の定義
- PXE エンジン
- Sophos Anti-Virus の定義
- IronPort アンチ スпам ルール
- アウトブレイク フィルタ ルール
- タイム ゾーンルール
- URL カテゴリ (URL フィルタリング機能に使用します。詳細は、[将来の URL カテゴリ セットの変更](#)を参照してください。
- 登録クライアント (URL フィルタリング機能で使用されるクラウドベース サービスとの通信に必要な証明書を更新するために使用されます。詳細については、[Cisco Web セキュリティ サービスへの接続について](#)を参照してください。)
- グレイメールルール



(注) DLP エンジンとコンテンツ照合分類子の設定は、[セキュリティサービス (Security Services)] > [データ損失防止 (Data Loss Prevention)] ページで扱われます。詳細については、[DLP エンジンおよびコンテンツ照合分類子の更新について](#)を参照してください。

サービス アップデートの設定は、DLP アップデートを除いてアップデートを受け取るすべてのサービスに使用されます。DLP アップデートを除いて、任意のサービスにそれぞれ設定を指定できません。

これらの重要なアップデートを取得するようにネットワークとアプライアンスを設定するには、[アップグレードおよびアップデートを取得するための設定](#)（27 ページ）を参照してください。

## アップグレードおよびアップデートを取得するための設定

- [アップグレードおよびアップデートの配信オプション](#)（27 ページ）
- [Cisco サーバからアップグレードおよびアップデートをダウンロードするためのネットワークの設定](#)（27 ページ）
- [厳密なファイアウォール環境でのアップグレードとアップデートのためのアプライアンスの設定](#)（28 ページ）
- [ローカルサーバからのアップグレードおよびアップデート](#)（29 ページ）
- [ローカルサーバからアップグレードおよびアップデートするためのハードウェアおよびソフトウェア要件](#)（30 ページ）
- [ローカルサーバでのアップグレードイメージのホスト](#)（30 ページ）
- [アップグレードおよびアップデートをダウンロードするためのサーバ設定](#)（31 ページ）
- [自動アップデートの設定](#)（34 ページ）
- [アップデート サーバの証明書の有効性を検証するためのアプライアンスの設定](#)（34 ページ）
- [プロキシサーバとの通信を信頼するようにアプライアンスを設定](#)（35 ページ）

### アップグレードおよびアップデートの配信オプション

アプライアンスに AsyncOS アップグレード ファイルおよびアップデート ファイルを配信する方法は複数あります。

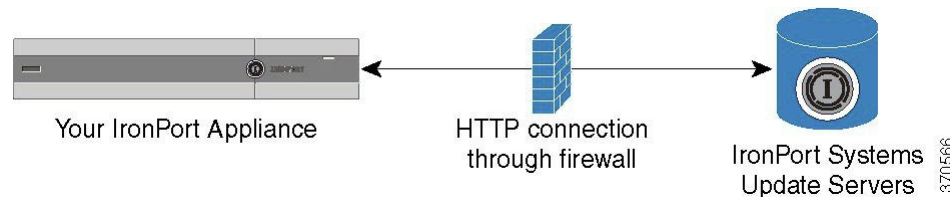
- 各アプライアンスでは Cisco アップデート サーバからファイルを直接ダウンロードできます。これがデフォルトの方法です。
- シスコからファイルを 1 回ダウンロードし、ネットワーク内のサーバからアプライアンスにファイルを配信できます。[ローカルサーバからのアップグレードおよびアップデート](#)（29 ページ）を参照してください。

方法の選択と設定については、[アップグレードおよびアップデートをダウンロードするためのサーバ設定](#)（31 ページ）を参照してください。

### Cisco サーバからアップグレードおよびアップデートをダウンロードするためのネットワークの設定

アプライアンスは、アップグレードおよびアップデートを検索してダウンロードするために、Cisco アップデート サーバに直接接続できます。

図 1: ストリーミングアップデートの方法



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。厳密なファイアウォールポリシーがある場合は、代わりに静的な場所の設定が必要になることがあります。詳細については、[厳密なファイアウォール環境でのアップグレードとアップデートのためのアプライアンスの設定 \(28 ページ\)](#) を参照してください。

ポート 80 および 443 による Cisco アップデートサーバからのアップグレードのダウンロードを許可する、ファイアウォールのルールを作成します。

## 厳密なファイアウォール環境でのアップグレードとアップデートのためのアプライアンスの設定

Cisco IronPort アップグレードおよび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、アップデートおよび AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。

### 手順

- 
- ステップ 1** シスコ カスタマー サポートに問い合わせ、スタティック URL アドレスを取得します。
  - ステップ 2** ポート 80 によるスタティック IP アドレスからのアップグレードおよびアップデートのダウンロードを許可する、ファイアウォールのルールを作成します。
  - ステップ 3** [セキュリティ サービス (Security Services) ] > [サービスのアップデート (Service Updates) ] を選択します。
  - ステップ 4** [アップデート設定を編集 (Edit Update Settings) ] をクリックします。
  - ステップ 5** [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 で受け取った AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルのスタティック URL を [ベース URL (Base URL) ] フィールドに入力します。
  - ステップ 6** IronPort アップデートサーバが [アップデートサーバ (リスト) (Update Servers (list)) ] セクションで選択されていることを確認します。
  - ステップ 7** 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およびアップデート

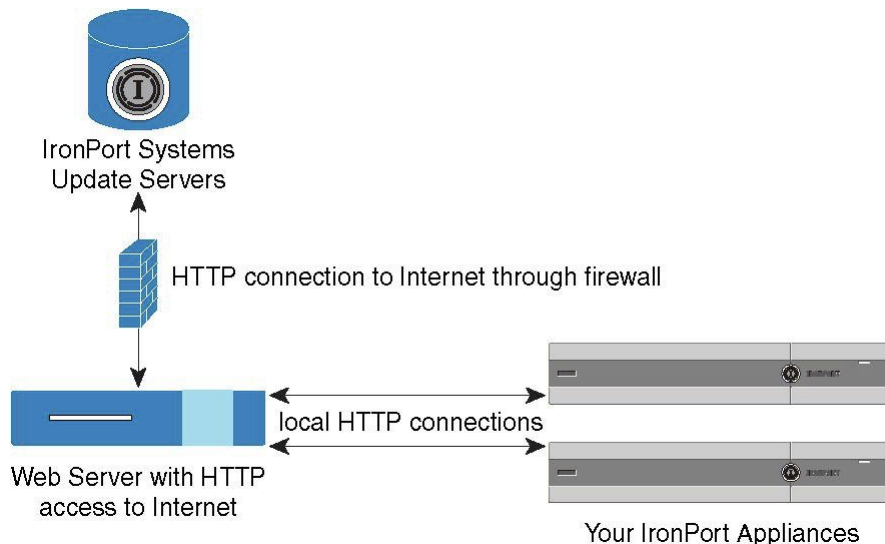
直接 Cisco アップデートサーバからアップグレードを取得するのではなく、AsyncOS アップグレードイメージをローカルサーバにダウンロードし、所有するネットワーク内からアップグレードをホスティングできます。この機能を使用して、インターネットにアクセスできるネットワーク上のすべてのサーバに HTTP でアップグレードイメージをダウンロードします。アップデートイメージをダウンロードする場合は、内部 HTTP サーバ（アップデートマネージャ）を設定し、アプライアンスで AsyncOS イメージをホスティングすることができます。

アプライアンスがインターネットにアクセスできない場合や、ダウンロードに使用するミラーサイトへのアクセスが組織で制限される場合はローカルサーバを使用します。ローカルサーバから各アプライアンスへの AsyncOS アップグレードのダウンロードは、通常 Cisco IronPort サーバからのダウンロードよりも高速です。



- (注) AsyncOS アップグレードに限りローカルサーバを使用することを推奨します。セキュリティアップデートイメージにローカルアップデートサーバを使用する場合、ローカルサーバは Cisco IronPort から自動的にセキュリティアップデートを受信しないため、ネットワーク上のアプライアンスは常に最新のセキュリティサービスであるわけではない可能性があります。

図 2: リモートアップデートの方法



### 手順

- ステップ 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。
- ステップ 2 アップグレードファイルをダウンロードします。

**ステップ3** GUIの[セキュリティ サービス (Security Services)]>[サービスのアップデート (Service Updates)]ページまたはCLIのupdateconfig コマンドのいずれかを使用して、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。

**ステップ4** [システム管理 (System Administration)]>[システム アップグレード (System Upgrade)]ページまたはCLIのupgrade コマンドのいずれかを使用して、アプライアンスをアップグレードします。

## ローカルサーバからアップグレードおよびアップデートするためのハードウェアおよびソフトウェア要件

AsyncOS アップグレード ファイルおよびアップデート ファイルのダウンロードでは、次の要件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ます。

- Cisco Systems アップデート サーバへのインターネット アクセス。
- Web ブラウザ ([ブラウザ要件](#)を参照)。



(注) 今回のリリースでアップデートサーバのアドレスへの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名を使用する必要があります。

AsyncOS アップデート ファイルのホスティングでは、次の要件を備えた内部ネットワークにサーバを構築する必要があります。

- Web サーバ：たとえば、Microsoft Internet Information Services (IIS; インターネット インフォメーション サービス) または Apache オープン ソース サーバでは、次の要件を満たしている必要があります。
  - 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 (認証不要) または基本 (「シンプル」) 認証用に設定されていること
  - 各 AsyncOS アップデート イメージ用に最低 350 MB 以上の空きディスク領域が存在すること

## ローカルサーバでのアップグレード イメージのホスト

ローカルサーバの設定が完了したら、[http://updates.ironport.com/fetch\\_manifest.html](http://updates.ironport.com/fetch_manifest.html) にアクセスして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、(物理アプライアンスの) シリアル番号または(仮想アプライアンスの) VLN 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のバージョンをクリックし、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。アップグレードイメージを使用するには、[アップデート設定を編集 (Edit Update Settings)] ページで (または CLI の `updateconfig` 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。

ローカルサーバは、ネットワーク上のアプライアンスで利用可能な AsyncOS アップグレードをダウンロード済みのアップグレードイメージに限定する XML ファイルもホスティングします。このファイルは「マニフェスト」と呼ばれます。マニフェストはアップグレードイメージの ZIP ファイルの `asynco` ディレクトリにあります。ローカルサーバのルートディレクトリにある ZIP ファイルを解凍したら、[アップデート設定を編集 (Edit Update Settings)] ページで (または CLI の `updateconfig` を使用して)、XML ファイルの完全な URL (ファイル名を含む) を入力します。

リモートアップグレードの詳細については、ナレッジベースを参照するか、シスコ サポート プロバイダーにお問い合わせください。

## プロキシサーバを経由したアップデート

アプライアンスは、(デフォルトで) Cisco アップデートサーバに直接接続して、アップデートを受け取るように設定されます。この接続は、ポート 80 の HTTP によって確立され、コンテンツは暗号化されます。ファイアウォールでこのポートを開くことを避ける場合は、アップデートされたルールをアプライアンスで受け取ることができる、プロキシサーバおよび具体的なポートを定義できます。

プロキシサーバを使用する場合は、任意で認証およびポートを指定できます。



- (注) プロキシサーバを定義すると、プロキシサーバを使用するように設定されているすべてのサービスアップデートで、そのプロキシサーバが自動的に使用されます。任意のサービスのアップデートのために、プロキシサーバをオフにはできません。

## アップグレードおよびアップデートをダウンロードするためのサーバ設定

アプライアンスにアップグレードおよびアップデートをダウンロードするために必要なサーバ情報および接続情報を指定します。

AsyncOS のアップグレードとサービスのアップデートに同じまたは異なる設定を使用できます。

### はじめる前に

アプライアンスがシスコから直接アップグレードおよびアップデートをダウンロードするか、または代わりにネットワーク上のローカルサーバでこれらのイメージをホスティングするかを設定します。次に、選択した方式をサポートするようにネットワークをセットアップします。

アップグレードおよびアップデートを取得するための設定 (27 ページ) のすべての内容を参照してください。

### 手順

- ステップ 1** [セキュリティ サービス (Security Services) ] > [サービスのアップデート (Service Updates) ] を選択します。
- ステップ 2** [更新設定を編集 (Edit Update Settings) ] をクリックします。
- ステップ 3** オプションを入力します。

設定	説明
アップデート サーバ (イメージ) (Update Servers (images))	<p>Cisco IronPort AsyncOS アップグレードイメージを、Cisco IronPort アップデート サーバまたはネットワーク上のローカル サーバのどちらからダウンロードするかを選択します。デフォルトは、アップグレードおよびアップデートの両方で Cisco IronPort アップデート サーバです。</p> <p>アップグレードとアップデートに同じ設定を使用するには、表示されるフィールドに情報を入力します。</p> <p>ローカルアップデート サーバを選択した場合は、アップグレードおよびアップデートのダウンロードに使用するサーバのベース URL とポート番号を入力します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。</p> <p>AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルにそれぞれ別の設定を入力するには、[クリックして AsyncOS の異なる設定を使用する (Click to use different settings for AsyncOS) ] リンクをクリックします。</p> <p>(注) Cisco Intelligent Multi-Scan でサードパーティのアンチスパム ルールのアップデートをダウンロードするには、別のローカル サーバが必要です。</p>



設定	説明
アップデートサーバ (リスト) (Update Servers (lists))	<p>導入に適したアップグレードおよびアップデートのみ各アプライアンスで利用できることを確認するために、Cisco IronPort は関連するファイルのマニフェストリストを生成します。</p> <p>利用可能なアップグレードおよびサービス アップデートのリスト (マニフェスト XML ファイル) を、Cisco IronPort アップデートサーバまたはネットワーク上のローカルサーバのどちらからダウンロードするかを選択します。</p> <p>アップデートおよび AsyncOS アップグレードのためのサーバの指定は、別のセクションに分かれています。デフォルトのアップグレードおよびアップデートは Cisco IronPort アップデートサーバです。</p> <p>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 HTTP ポート番号を含む、各リストのマニフェスト XML ファイルのフルパスを入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合、有効なユーザ名とパスワードを入力します。</p>
自動更新	<p>Sophos および McAfee Anti-Virus 定義ファイル、Cisco Anti-Spam ルール、Cisco Intelligent Multi-Scan ルール、PXE Engine アップデート、アウトブレイク フィルタ ルール、時間帯ルールに対する自動アップデートとアップデート間隔 (アプライアンスがアップデートを確認する頻度) をイネーブルにします。</p> <p>数字の後に秒、分、時間を表す s (秒)、m (分) および h (時) を含めます。自動更新をディセーブルにするには、0 (ゼロ) を入力します。</p> <p>(注) [セキュリティ サービス (Security Services)] &gt; [データ消失防止 (Data Loss Prevention)] ページからのみ、DLP の自動アップデートを有効にできます。ただし、最初にすべてのサービスの自動アップデートをイネーブルにする必要があります。詳細については、<a href="#">DLP エンジンおよびコンテンツ照合分類子の更新について</a>を参照してください。</p>
無効な自動エンジン更新のアラート間隔	<p>「自動更新」機能が特定のエンジンで無効になっている場合、送信されるアラートの特定の頻度を入力します。</p> <p>末尾に m、h、または d が含まれ、月、時間、または日を示します。デフォルト値は 30 日です。</p>

設定	説明
インターフェイス (Interface)	表示されているセキュリティ コンポーネントのアップデートをアップデート サーバに問い合わせる際に使用するネットワーク インターフェイスを選択します。利用可能なプロキシデータ インターフェイスが表示されます。デフォルトでは、アプライアンスは使用するインターフェイスを選択します。
HTTP プロキシ サーバ (HTTP Proxy Server)	GUI に表示されているサービスで使用されるオプションのプロキシ サーバ。  プロキシ サーバを指定すると、すべてのサービスのアップデートのために使用できます。
HTTPS プロキシ サーバ (HTTPS Proxy Server)	HTTPS を使用したオプションのプロキシサーバ。HTTPS プロキシサーバを定義すると、GUI に表示されているサービスのアップデートで使用されます。

ステップ4 変更を送信し、保存します。

## 自動アップデートの設定

### 手順

- ステップ1 [セキュリティ サービス (Security Services) ] > [サービスのアップデート (Service Updates) ] ページに移動して、[更新設定を編集 (Edit Update Settings) ] をクリックします。
- ステップ2 チェックボックスをオンにして、自動アップデートをイネーブルにします。
- ステップ3 アップデート間隔 (次のアップデートの確認までに待機する時間) を入力します。数字の後に **m** (分) および **h** (時) を追加します。最大アップデート間隔は 1 時間です。

## アップデートサーバの証明書の有効性を検証するためのアプライアンスの設定

E メールセキュリティ アプライアンスでは、アプライアンスがアップデート サーバと通信するたびに、シスコのアップデートサーバの証明書の有効性を確認できます。このオプションが設定されている場合、検証に失敗すると、更新はダウンロードされず、詳細がアップデート ログに記録されます。

このオプションを構成するには、`updateconfig` コマンドを使用します。次の例は、このオプションを構成する方法を示しています。

```

mail.example.com> updateconfig
Service (images):                               Update URL:
-----
Feature Key updates                             http://downloads.ironport.com/asyncos
Timezone rules                                  Cisco IronPort Servers
Enrollment Client Updates                      Cisco IronPort Servers
Support Request updates                        Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades               Cisco IronPort Servers
Service (list):                                Update URL:
-----
Timezone rules                                  Cisco IronPort Servers
Enrollment Client Updates                      Cisco IronPort Servers
Support Request updates                        Cisco IronPort Servers
Service (list):                                Update URL:
-----
Cisco IronPort AsyncOS upgrades                Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> validate_certificates
Should server certificates from Cisco update servers be validated?
[Yes]>
Service (images):                               Update URL:
-----
Feature Key updates                             http://downloads.ironport.com/asyncos
Timezone rules                                  Cisco IronPort Servers
Enrollment Client Updates                      Cisco IronPort Servers
Support Request updates                        Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades               Cisco IronPort Servers
Service (list):                                Update URL:
-----
Timezone rules                                  Cisco IronPort Servers
Enrollment Client Updates                      Cisco IronPort Servers
Support Request updates                        Cisco IronPort Servers
Service (list):                                Update URL:
-----
Cisco IronPort AsyncOS upgrades                Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>

```

## プロキシサーバとの通信を信頼するようにアプライアンスを設定

透過的でないプロキシサーバを使用している場合、プロキシ証明書の署名に使用するCA証明書をアプライアンスに追加できます。これにより、アプライアンスはプロキシサーバ通信を信頼します。

このオプションを構成するには、`updateconfig` コマンドを使用します。次の例は、このオプションを構成する方法を示しています。

```

mail.example.com> updateconfig
...
...
...
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> trusted_certificates
Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
[]> add
Paste certificates to be trusted for secure updater connections, blank to quit
Trusted Certificate for Updater:
Paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MMIICiDCCAfGgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhmCSU4x
DDAKBgNVBAGTA0tBUjENM.....
-----END CERTIFICATE-----
.
Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
- LIST - List trusted certificates for updates.
- DELETE - Delete a trusted certificate for updates.
[]>

```

## AsyncOS のアップグレード

### 手順

	コマンドまたはアクション	目的
ステップ 1	まだ実行していない場合は、すべてのアップデートとアップグレードのダウンロードに適用される設定を行い、これらのダウンロードをサポートして任意で配信できるようにネットワークをセットアップします。	<a href="#">アップグレードおよびアップデートを取得するための設定 (27 ページ)</a>
ステップ 2	アップグレードが使用可能になる時期を確認し、インストールするかどうかを決定します。	<a href="#">使用可能なアップグレードの通知 (37 ページ)</a>
ステップ 3	各アップグレードの実行前に、必須タスクと推奨タスクを実行します。	<a href="#">AsyncOS のアップグレードの準備 (38 ページ)</a> <a href="#">クラスタ内のマシンのアップグレード</a>
ステップ 4	アップグレードを実行します。	<a href="#">アップグレードのダウンロードとインストール (39 ページ)</a>

## クラスタ化されたシステムのアップグレードについて

クラスタ化されたマシンをアップグレードする場合は、[クラスタ内のマシンのアップグレード](#)を参照してください。

## アップグレード手順用のバッチ コマンドについて

アップグレード手順用のバッチコマンドの詳細については、『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』

([http://www.cisco.com/en/US/products/ps10154/prod\\_command\\_reference\\_list.html](http://www.cisco.com/en/US/products/ps10154/prod_command_reference_list.html)) を参照してください。

## 使用可能なアップグレードの通知

デフォルトでは、AsyncOS アップグレードがアプライアンスで使用可能な場合、管理者および技術者の権限を持つユーザには、Web インターフェイスの上部に通知が表示されます。

クラスタ マシンでは、現在ユーザがログインしているマシンだけにアクションが適用されません。

目的	操作手順
最新のアップグレードの詳細情報を表示する	アップグレード通知にカーソルを合わせます。
使用できるすべてのアップグレードのリストを表示する	通知の下向き矢印をクリックします。
現在の通知を閉じる 新しいアップグレードが入手可能になるまで、アプライアンスは別の通知を表示しません。	下向き矢印をクリックして[通知を消去 (Clear the notification)]を選択してから、[閉じる (Close)]をクリックします。
今後の通知を中止する (管理者権限を持つユーザのみ)	[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [システムアップグレード (System Upgrade)] に移動します。

## 使用可能なアップグレードの通知

デフォルトでは、AsyncOS アップグレードがアプライアンスで使用可能な場合、管理者および技術者の権限を持つユーザには、Web インターフェイスの上部に通知が表示されます。

クラスタ マシンでは、現在ユーザがログインしているマシンだけにアクションが適用されません。

目的	操作手順
最新のアップグレードの詳細情報を表示する	アップグレード通知にカーソルを合わせます。
使用できるすべてのアップグレードのリストを表示する	通知の下向き矢印をクリックします。
現在の通知を閉じる 新しいアップグレードが入手可能になるまで、アプライアンスは別の通知を表示しません。	下向き矢印をクリックして[通知を消去 (Clear the notification) ]を選択してから、[閉じる (Close) ]をクリックします。
今後の通知を中止する (管理者権限を持つユーザのみ)	[管理アプライアンス (Management Appliance) ] > [システム管理 (System Administration) ] > [システムアップグレード (System Upgrade) ] に移動します。

## AsyncOS のアップグレードの準備

ベストプラクティスとして、次の手順を実行したアップグレードの準備を推奨します。

### 始める前に

ワークキュー内のすべてのメッセージをクリアします。ワークキューをクリアせずにアップグレードを実行することはできません。

### 手順

- 
- ステップ 1** XML 設定ファイルのオフボックスを保存します。何らかの理由でアップグレード前のリリースに戻す場合は、このファイルが必要です。
  - ステップ 2** セーフリスト/ブロックリスト機能を使用している場合、リストのオフボックスをエクスポートします。
  - ステップ 3** すべてのリスナーを一時停止します。CLI からのアップグレードを実行する場合は、`suspendlistener` コマンドを使用します。GUI からのアップグレードを実行する場合は、リスナーの停止が自動的に実行されます。
  - ステップ 4** キューが空になるまで待ちます。CLI の `workqueue` コマンドでワークキュー内のメッセージ数を表示するか、`rate` コマンドでアプライアンスのメッセージスループットをモニタすることができます。

(注) アップグレード後、再びリスナーをイネーブルにします。

---

## アップグレードのダウンロードとインストール

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。



(注) AsyncOS を Cisco IronPort 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する場合は、アップグレードはダウンロード中に即座に実行されます。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、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。

### はじめる前に

- Cisco から直接アップグレードをダウンロードするか、またはネットワーク上のサーバからアップグレードイメージをホストするかを選択します。次に、選択した方式をサポートするようにネットワークをセットアップします。そして、選択した入手先からアップグレードを入手するためにアプライアンスを設定します。アップグレードおよびアップデートを取得するための設定 (27 ページ) およびアップグレードおよびアップデートをダウンロードするためのサーバ設定 (31 ページ) を参照してください。
- ここで、アップグレードをインストールする場合は、AsyncOS のアップグレードの準備 (38 ページ) の手順を実行します。
- クラスタ化されたシステムのアップグレードをインストールする場合は、クラスタ内のマシンのアップグレードを参照してください。
- アップグレードをダウンロードするだけの場合、インストールの準備が完了するまでの前提条件はありません。

### 手順

**ステップ 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。

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

システムではステータスログの履歴データ (最大3カ月) を分析して、アプライアンスの状態を判断し、アプライアンスがアップグレード可能かどうかの推奨を提供します。

(注) システムでこの分析を実行するには、ステータスログに1カ月以上のログデータが含まれている必要があります。

**ステップ 3** 分析結果に応じて、次のいずれかを実行します。

- 分析で、過去数カ月にシステムで次のいずれかの問題が発生したことが検出された場合は、表示された内容に従います。
  - リソース節約モード
  - メール処理の遅延

- High CPU usage
  - 高いメモリ使用量
  - 高いメモリ ページ スワッピング
- システムで分析を実行できない場合（ステータスログのデータが不十分なため）、推奨は提供されません。この場合、アプライアンスで最近問題が発生していない場合にのみ、アプライアンスのアップグレードを検討してください。
- 分析で問題が検出されなかった場合は、ステップ 4 に進みます。

**ステップ 4** 次のオプションを選択します。

目的	操作手順
1 回の操作でアップグレードのダウンロードとインストールを実行する	[ダウンロードしてインストール (Download and Install) ] をクリックします。  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。
アップグレードインストーラをダウンロードする	[ダウンロードのみ (Download only) ] をクリックします。  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。  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。
ダウンロードしたアップグレードインストーラをインストールする	[Install (インストール) ] 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。  インストールする AsyncOS のバージョンは、[インストール (Install) ] オプションの下に表示されます。

**ステップ 5** 以前にダウンロードしたインストーラでインストールする場合を除き、利用可能なアップグレードのリストから AsyncOS のバージョンを選択します。

**ステップ 6** インストール中の場合、次に従います。

- a) 現在の設定をアプライアンス上の `configuration` ディレクトリに保存するかどうかを選択します。
- b) コンフィギュレーションファイルでパスフレーズをマスクするかどうかを選択します。  
  
(注) マスクされたパスフレーズが記載されたコンフィギュレーションファイルは、GUI の [設定ファイル (Configuration File) ] ページや CLI の `loadconfig` コマンドからロードできません。
- c) コンフィギュレーションファイルのコピーを電子メールで送信する場合は、ファイルを送信する電子メールアドレスを入力します。複数の電子メールアドレスを指定する場合は、カンマで区切ります。

**ステップ 7** [続行 (Proceed) ] をクリックします。



**ステップ 8** 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。

応答するまでプロセスは中断されます。

ページの上部の近くに、経過表示バーが表示されます。

- b) 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。

### 次のタスク

- プロセスが中断された場合、プロセスを再開する必要があります。
- アップグレードをダウンロードしてインストールしなかった場合は次のとおりです。  
アップグレードをインストールする準備ができたなら、「始める前に」の項の前提条件も含め次の手順を最初から実行しますが、[インストール (Install)] オプションを選択します。
- アップグレードをインストールした場合、次のとおりです。
  - リスナーを再びイネーブル (再開) にします。
  - 新しいシステムの設定ファイルを保存します。詳細については、[設定ファイルの管理 \(16 ページ\)](#) を参照してください。
- アップグレードが完了したら、再びリスナーをイネーブルにします。

## バックグラウンド ダウンロードのキャンセルまたは削除ステータスの表示

### 手順

**ステップ 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。

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

**ステップ 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。

目的	操作手順
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。

**ステップ4** (任意) アップグレードログを確認します。

## 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および90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、ハードウェアインストレーションガイド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。
- この機能を使用するには、専用のリモート電源再投入インターフェイスの一意の 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へのアクセスに関する詳細については、CLIのリファレンスガイドを参照してください。

### 手順

**ステップ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。

**ステップ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。

**ステップ3** 以下のコマンドを入力します。

**remotepower**

**setup**

**ステップ 4** プロンプトに従って、以下の情報を指定します。

1. 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。
2. 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ワード。

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。

**ステップ 5** `commit` を入力して変更を保存します。

**ステップ 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。

**ステップ 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。

---

次のタスク

関連項目

- [アプライアンスの電源のリモートリセット](#)

## AsyncOS の以前のバージョンへの復元

AsyncOS には、緊急時に AsyncOS オペレーティング システムを以前の認定済みのビルドに戻す機能があります。

### 復元の影響

アプライアンスにおける `revert` コマンドの使用は、非常に破壊的な操作になります。このコマンドはすべての設定ログおよびデータベースを破壊します。管理インターフェイスのネットワーク情報のみが保存されます。他のすべてのネットワーク設定は削除されます。さらに、復元はアプライアンスが再設定されるまでメール処理を中断します。このコマンドはネットワーク設定を破壊するため、`revert` コマンドを発行する場合は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。



---

**注意** 戻し先のバージョンの設定ファイルが必要です。設定ファイルに下位互換性はありません。

---

## 仮想アプライアンスでの AsyncOS の復元がライセンスに影響を及ぼす可能性

AsyncOS 9.0 for Email から AsyncOS 8.5 for Email に復元した場合、ライセンスは変更されません。

AsyncOS 9.0 for Email から AsyncOS 8.0 for Email 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メールを配信する 180 日間の猶予期間はなくなります。

どちらの場合も、ライセンス キーの有効期限は変更されません。

### 関連項目

- [仮想アプライアンスのライセンスの有効期限 \(15 ページ\)](#)

## AsyncOS の復元

### 手順

- ステップ 1** 戻し先のバージョンの設定ファイルがあることを確認してください。設定ファイルに下位互換性はありません。設定ファイルを取得するには、ファイルを電子メールでユーザ自身に送信するか、ファイルを FTP で取得します。詳細については、[設定ファイルのメール送信 \(18 ページ\)](#) を参照してください。
- ステップ 2** アプライアンスの現在の設定のバックアップ コピーを、（パスフレーズをマスクしない状態で）別のマシンに保存します。  
(注) このコピーは、バージョンを戻した後にロードする設定ファイルではありません。
- ステップ 3** セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリスト データベースを別のマシンにエクスポートします。
- ステップ 4** メール キューが空になるまで待ちます。
- ステップ 5** 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。  
  
revert コマンドの実行時には、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でください。
- ステップ 6** CLI から **revert** コマンドを発行します。  
(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。
- ステップ 7** アプライアンスが 2 回再起動するまで待ちます。
- ステップ 8** マシンが 2 回再起動したら、シリアルコンソールで **interfaceconfig** コマンドを使用して、アクセス可能な IP アドレスをインターフェイスに設定します。
- ステップ 9** 設定したインターフェイスの 1 つで FTP または HTTP をイネーブルにします。

- ステップ 10** 作成した XML 設定ファイルを FTP で取得するか、または GUI インターフェイスに貼り付けます。
- ステップ 11** 戻し先のバージョンの XML 設定ファイルをロードします。
- ステップ 12** セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリストデータベースをインポートして復元します。
- ステップ 13** 変更を保存します。
- 復元が完了したアプライアンスは、選択された AsyncOS バージョンを使用して稼働します。

## アプライアンスに生成されるメッセージの返信アドレスの設定

AsyncOS によって、次のタイミングで生成されるメールのエンベロープ送信者を設定できません。

- Anti-Virus 通知
- バウンス
- DMARC フィードバック
- 通知 (notify() および notify-copy() フィルタの動作)
- 隔離通知 (および隔離管理機能における「コピー送信」)
- レポート
- その他のすべてのメッセージ

返信アドレスの表示、ユーザ、およびドメイン名を指定できます。ドメイン名に仮想ゲートウェイ ドメインの使用を選択することもできます。

システムで生成された電子メール メッセージの返信アドレスを GUI または `addressconfig` コマンドを使用して CLI で変更できます。

### 手順

- ステップ 1** [システム管理 (System Administration) ] > [返信先アドレス (Return Addresses) ] ページの順に進みます。
- ステップ 2** [設定の編集 (Edit Settings) ] をクリックします。
- ステップ 3** 1 つまたは複数のアドレスへの変更
- ステップ 4** 変更を送信し、保存します。

## システム状態パラメータのしきい値の設定

組織の要件に応じて、CPU使用率や作業キューの最大メッセージ数など、アプライアンスのさまざまな状態パラメータのしきい値を設定できます。指定されたしきい値を超えた場合にアラートを送信するように、アプライアンスを設定することもできます。



- (注) CLIを使用してシステムのヘルス パラメータのしきい値を設定するには、`healthconfig` コマンドを使用します。詳細については、CLIのインラインヘルプ、または『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

### はじめる前に

しきい値を注意深く決定します。

### 手順

**ステップ 1** [システム管理 (System Administration)] > [システムの状態 (System Health)] をクリックします。

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

**ステップ 3** 次のオプションを設定します。

- CPU 使用率のしきい値レベルを指定します (パーセント)。

現在の CPU 使用率が設定済みのしきい値を超えた場合に、アラートを受信するかどうかを指定します。最初のアラートが送信された後、最初のアラートがトリガーされてから 15 分以内に、CPU 使用率が移動平均を 5% 超えた場合、追加のアラートが送信されます。

- (注) メール処理プロセスの CPU 使用率だけに基づいて、これらのアラートがトリガーされます。

- メモリ ページスワッピングのしきい値レベルを指定します (割合)。

全体的なメモリスワップ使用率が設定済みのしきい値を超えた場合に、アラートを受信するかどうかを指定します。最初のアラートが送信された後、15 分以内にメモリ ページスワッピングが最初のアラートをトリガーした値を 150% 超えた場合、追加のアラートが送信されます。例えば、しきい値が 10 に設定されている場合、

- メモリ スワップ使用率が 10.1% に達すると、最初のアラートが送信されます。
- メモリ スワップ使用率が 15.1% に達すると、もう一度アラートが送信されます。

- 作業キューの最大メッセージ数のしきい値レベルを指定します (メッセージ数)。

また、作業キューのメッセージ数が設定済みのしきい値を超えた場合に、アラートを受信するかどうかを指定します。最初のアラートが送信された後、15 分以内に作業キューの最大メッセージ数が最初のアラートをトリガーした値を 150% 超えた場合、追加のアラートが送信されます。たとえば、しきい値が 1000 に設定されている場合、

- 作業キューの最大メッセージ数が 1002 に達したときに、最初のアラートが送信されました。
- 15 分以内に作業キューの最大メッセージ数が 1510 に達すると、アラートがもう 1 つ送信されます。

(注) この機能のアラートはすべて、システムアラートカテゴリに属します。

ステップ 4 変更を送信し、保存します。

#### 次のタスク

この機能のアラートを設定した場合は、システムアラートに登録されていることを確認してください。この説明については、[アラート受信者の追加 \(49 ページ\)](#) を参照してください。

## Eメールセキュリティアプライアンスの状況の確認

ヘルスチェック機能を使用して、Eメールセキュリティアプライアンスの状態を確認できます。ヘルスチェックを実行すると、現在のステータスログの履歴データ（最大3カ月）が分析され、アプライアンスの状態が判断されます。



(注) システムでこの分析を実行するには、ステータスログに1カ月以上のログデータが含まれている必要があります。

ヘルスチェックを実行するには、

- Web インターフェイスで、[システム管理 (System Administration)] > [システムの状態 (System Health)] ページに移動して、[ヘルスチェックを実行 (Run Health Check)] をクリックします。
- CLI で **healthconfig** コマンドを実行します。

分析結果により、過去数カ月にシステムで次の問題が1つ以上発生したかどうかを示されません。

- リソース節約モード
- メール処理の遅延
- High CPU usage
- 高いメモリ使用量
- 高いメモリ ページスワッピング

ヘルスチェックにおいて、アプライアンスで上記の問題が1つ以上発生していることが示された場合、システム設定を確認して最適化することを検討してください。詳細については、<http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118881-technote-esa-00.html> を参照してください。

# アラート

アラートメッセージは自動生成される標準電子メールメッセージであり、アプライアンスで発生するイベントに関する情報が含まれています。これらのイベントにはマイナーからメジャーまでの重要度（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。アラートは、アプライアンスで生成されます。送信するアラートメッセージの種類、重大度、および送信するユーザを非常に詳細なレベルで指定できます。アラートは、GUIの[システム管理 (System Administration)] > [アラート (Alerts)] ページ（またはCLIの `alertconfig` コマンド）で管理します。

## アラートの重大度

アラートは、次の重大度に従って送信されます。

- クリティカル：すぐに対処が必要です。
- 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可能性もあります。
- 情報：デバイスのルーティン機能で生成される情報。

## AutoSupport

十分なサポートと今後のシステム変更の設計を可能にするため、システムで生成されたすべてのアラートメッセージをシスコに送信するようにアプライアンスを設定できます。この機能は **AutoSupport** と呼ばれ、シスコによるお客様のニーズへのプロアクティブな対応に役立ちます。また、**AutoSupport** は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 **AsyncOS** バージョンを通知するレポートを毎週送信します。

デフォルトでは、アラートタイプが **System** で重大度レベルが **Information** のアラートを受信するように設定されているアラート受信者は、シスコに送信される各メッセージのコピーを受信します。内部にアラートメッセージを毎週送信しない場合は、この設定をディセーブルにできます。この機能をイネーブルまたはディセーブルにするには、[アラート設定値の設定 \(50ページ\)](#) を参照してください。

## アラートの配信

アプライアンスから [アラート受信者 (Alert Recipient)] で指定されたアドレスに送信されるアラートは、該当の送信先に対して定義された **SMTP** ルートに従います。

アラートメッセージはアプライアンス内の問題の通知に使用されるため、送信に **AsyncOS** の標準メール配信システムを使用しません。代わりに、アラートメッセージは **AsyncOS** で重大なシステム故障が発生しても動作するように設計された、個別に並行動作する電子メールシステムで処理されます。

アラートメールシステムは、**AsyncOS** と同一の設定を共有しません。このため、アラートメッセージは、次のように他のメール配信とは若干異なる動作をする可能性があります。



- アラートメッセージは、標準の DNS MX レコードおよび A レコードのルックアップを使用して配信されます。
  - アラートメッセージは DNS エントリを 30 分間キャッシュし、そのキャッシュは 30 分ごとにリフレッシュされます。このため、DNS 障害時にもアラートが出力されます。
- アラートメッセージはワーク キューを通過しないため、ウイルスまたはスパムのスキャン対象外です。メッセージフィルタまたはコンテンツフィルタの処理対象にも含まれません。
- アラートメッセージは配信キューを通過しないため、バウンスのプロファイルまたは送信先制御の制限には影響を受けません。

## アラートメッセージの例

```
Date: 23 Mar 2005 21:10:19 +0000

To: joe@example.com

From: IronPort C60 Alert [alert@example.com]

Subject: Critical-example.com: (Anti-Virus) update via http://newproxy.example.com
failed

The Critical message is:

update via http://newproxy.example.com failed

Version: 4.5.0-419

Serial Number: XXXXXXXXXXXX-XXXXXXX

Timestamp: Tue May 10 09:39:24 2005

For more information about this error, please see
http://support.ironport.com

If you desire further information, please contact your support provider.
```

## アラート受信者の追加

アラートエンジンでは、送信するアラートの種類とアラート受信者を詳細に制御できます。たとえば、アラート受信者が **System**（アラートの種類）に関する **Critical**（重大度）の情報が送信されたときのみ通知を受信するように設定することで、アラート受信者に特定のアラートのみを送信するように設定できます。



---

(注) システムのセットアップ時に **AutoSupport** をイネーブ爾にした場合、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。

---

## 手順

- ステップ1 [システム管理 (System Administration)] > [アラート (Alerts)] を選択します。
- ステップ2 [受信者を追加 (Add Recipient)] をクリックします。
- ステップ3 受信者の電子メールアドレスを入力します。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。
- ステップ4 (任意) シスコ サポートからソフトウェア リリースおよび重大なサポート通知のアラートを受信するには、[リリースおよびサポート通知 (Release and Support Notifications)] をオンにします。
- ステップ5 この受信者が受信するアラートのタイプと重大度を選択します。
- ステップ6 変更を送信し、保存します。

## アラート設定値の設定

次の設定は、すべてのアラートに適用されます。



- (注) 後から確認するためにアプライアンスに保存するアラートの数を定義するには `alertconfig CLI` コマンドを使用します。

## 手順

- ステップ1 [アラート (Alerts)] ページで [設定を編集 (Edit Settings)] をクリックします。
- ステップ2 アラートの送信に使用する Header From: アドレスを入力するか、[自動生成 (Automatically Generated)] (「alert@<hostname>」を自動生成) を選択します。
- ステップ3 重複したアラートを送信するまでに待機する秒数を指定する場合は、チェックボックスをオンにします。詳細については、[重複したアラートの送信 \(51 ページ\)](#) を参照してください。
  - 重複したアラートを送信するまでに待機する秒数の初期値を指定します。
  - 重複したアラートを送信するまでに待機する秒数の最大値を指定します。
- ステップ4 [IronPort AutoSupport] オプションをオンにすることで、AutoSupport をイネーブルにできます。AutoSupport の詳細については、[AutoSupport \(48 ページ\)](#) を参照してください。
  - AutoSupport がイネーブルの場合、Information レベルの System アラートを受信するように設定されたアラート受信者に、毎週 AutoSupport レポートが送信されます。チェックボックスを外すことでディセーブルにできます。

ステップ5 変更を送信し、保存します。

## アラート設定

アラート設定では、アラートの全般的な動作と設定を制御します。設定には次のような項目があります。

- RFC 2822 Header From : アラートを送信するタイミング（アドレスを入力するか、デフォルトの「alert@<hostname>」を使用します）。また、`alertconfig -> from` コマンドを使用し、この値を CLI で設定することもできます。
- 重複したアラートを送信するまでに待機する秒数の初期値。
- 重複したアラートを送信するまでに待機する秒数の最大値。
- AutoSupport のステータス（イネーブルまたはディセーブル）。
- Information レベルの System アラートを受信するように設定されたアラート受信者への、AutoSupport の毎週のステータス レポートの送信。

### 重複したアラートの送信

AsyncOS が重複したアラートを送信するまでに待機する秒数の初期値を指定できます。この値を 0 に設定した場合、重複したアラートのサマリーは送信されず、代わりにすべての重複したアラートがリアルタイムに送信されます（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。増加する秒数は、前回の待機間隔の 2 倍の値を足した秒数です。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 秒後といった間隔で送信されます。

最終的に、送信間隔は非常に大きな秒数になります。[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 秒後、15 秒後、35 秒後、60 秒後、120 秒後といった間隔で送信されます。

## 最新アラートの表示

E メールセキュリティ アプライアンスは最新のアラートを保存するので、アラートメッセージを消失または削除した場合に GUI および CLI の両方で表示できます。これらのアラートは、アプライアンスからダウンロードできません。

最新のアラートのリストを表示するには、[アラート (Alerts)] ページにある [トップアラートを表示 (View Top Alerts)] ボタンをクリックするか、CLI で `displayalerts` コマンドを使用します。GUI でアラートを、日付、レベル、クラス、テキスト、受信者によって調整します。

デフォルトでは、アプライアンスは [トップアラート (Top Alerts)] ウィンドウに表示するために最大 50 個のアラートを保存します。アプライアンスが保存するアラートの数を編集するには、CLI で `alertconfig -> setup` コマンドを使用します。この機能を無効にするにはアラートの数を 0 に変更します。

## アラートの説明

次の表に、分類したアラートのリストを示します。表には、アラート名（Cisco で使用される内部記述子）、アラートの実際のテキスト、説明、重大度（critical、information、または warning）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。アラートの実際のテキストでは、パラメータ値は置き換えられます。たとえば、次のアラートメッセージではメッセージのテキストに「\$ip」が記述されています。アラート生成時に「\$ip」は実際の IP アドレスに置き換えられます。

- アンチスパムアラート (52 ページ)
- アンチウイルスアラート (53 ページ)
- ディレクトリ獲得攻撃 (DHAP) アラート (54 ページ)
- ハードウェアアラート (54 ページ)
- スпам隔離アラート (55 ページ)
- セーフリスト/ブロックリストアラート (56 ページ)
- システムアラート (57 ページ)
- アップデータアラート (68 ページ)
- アウトブレイクフィルタアラート (69 ページ)
- クラスタリングアラート (70 ページ)

## アンチスパムアラート

次の表は、AsyncOS で生成されるさまざまなアンチスパムアラートのリストです。アラートの説明と重大度が記載されています。

表 1: 発生する可能性があるアンチスパムアラートのリスト

アラート名 (Alert Name)	メッセージと説明	パラメータ
AS.SERVER.ALERT	\$engine anti-spam - \$message \$tb	「engine」：アンチスパムエンジンのタイプ。 「message」：ログメッセージ。 「tb」：イベントのトレースバック。
	クリティカル。アンチスパムエンジンに障害が発生した場合に送信されます。	
AS.TOOL.INFO_ALERT	Update - \$engine - \$message	「engine」：アンチスパムエンジンの名前 「message」：メッセージ。
	情報。アンチスパムエンジンに問題が発生した場合に送信されます。	

アラート名 (Alert Name)	メッセージと説明	パラメータ
AS.TOOL.ALERT	Update - \$engine - \$message クリティカル。アンチスパムエンジンの管理に使用されるツールの1つに問題があり、アップデートが中止される場合に送信されます。	「engine」：アンチスパムエンジンの名前 「message」：メッセージ。

## アンチウイルス アラート

次の表は、AsyncOS で生成されるさまざまなアンチウイルス アラートのリストです。アラートの説明と重大度が記載されています。

表 2: 発生する可能性があるアンチウイルス アラートのリスト

アラート名 (Alert Name)	メッセージと説明	パラメータ
AV.SERVER.ALERT /AV.SERVER.CRITICAL	\$engine antivirus - \$message \$tb クリティカル。アンチウイルス スキャンエンジンに重大な問題が発生した場合に送信されます。	「engine」：アンチウイルス エンジンのタイプ。 「message」：ログ メッセージ。 「tb」：イベントのトレースバック。
AV.SERVER.ALERT.INFO	\$engine antivirus - \$message \$tb 情報。アンチウイルス スキャンエンジンに情報イベントが発生した場合に送信されます。	「engine」：アンチウイルス エンジンのタイプ。 「message」：ログ メッセージ。 「tb」：イベントのトレースバック。
AV.SERVER.ALERT.WARN	\$engine antivirus - \$message \$tb 警告。アンチウイルス スキャンエンジンに問題が発生した場合に送信されます。	「engine」：アンチウイルス エンジンのタイプ。 「message」：ログ メッセージ。 「tb」：イベントのトレースバック。
MAIL.ANTIVIRUS.ERROR_MESSAGE	MID \$mid antivirus \$what error \$tag クリティカル。メッセージのスキャン中に、アンチウイルス スキャンがエラーを生成した場合に送信されます。	「mid」：MID 「what」：発生したエラー。 「tag」：ウイルス アウトブレイク名 (設定されている場合)。

## ディレクトリ獲得攻撃 (DHAP) アラート

アラート名 (Alert Name)	メッセージと説明	パラメータ
MAIL.SCANNER. PROTOCOL_MAX_RETRY	MID \$mid is malformed and cannot be scanned by \$engine.  クリティカル。メッセージが不正なため、スキャン エンジン はメッセージのスキャンに失敗しました。再試行の最大回数を超過したため、メッセージはエンジンにスキャンされずに処理されます。	「mid」 : MID 「engine」 : 使用されているエンジン。

## ディレクトリ獲得攻撃 (DHAP) アラート

以下の表は、AsyncOS で生成されるさまざまな DHAP アラートのリストです。アラートの説明と重大度が記載されています。

表 3: 発生する可能性があるディレクトリ獲得攻撃アラートのリスト

アラート名 (Alert Name)	メッセージと説明	パラメータ
LDAP.DHAP_ALERT	LDAP: Potential Directory Harvest Attack detected. See the system mail logs for more information about this attack.  警告。ディレクトリ獲得攻撃の可能性を検出した場合に送信されます。	

## ハードウェア アラート

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

表 4: 発生する可能性があるハードウェア アラートのリスト

アラート名 (Alert Name)	メッセージと説明	パラメータ
INTERFACE.ERRORS	Port \$port: has detected \$in_err input errors, \$out_err output errors, \$col collisions please check your media settings.  警告。インターフェイス エラーを検出した場合に送信されます。	「port」 : インターフェイス名。 「in_err」 : 最後のメッセージ以降の入力エラー数。 「out_err」 : 最後のメッセージ以降の出力エラー数。 「col」 : 最後のメッセージ以降の packets 衝突数。

アラート名 (Alert Name)	メッセージと説明	パラメータ
MAIL.MEASUREMENTS_FILESYSTEM	The \$file_system partition is at \$capacity% capacity	「file_system」 : ファイルシステムの名前 「capacity」 : ファイルシステムの使用率 (%)。
	警告。ディスクパーティションが75%の使用率に近づいた場合に送信されます。	
MAIL.MEASUREMENTS_FILESYSTEM.CRITICAL	The \$file_system partition is at \$capacity% capacity	「file_system」 : ファイルシステムの名前 「capacity」 : ファイルシステムの使用率 (%)。
	クリティカル。ディスクパーティションが90%の使用率に達した場合 (95%、96%、97%など) に送信されます。	
SYSTEM.RAID_EVENT_ALERT	A RAID-event has occurred: \$error	「error」 : RAID エラーのテキスト。
	警告。重大な RAID-event が発生した場合に送信されます。	
SYSTEM.RAID_EVENT_ALERT_INFO	A RAID-event has occurred: \$error	「error」 : RAID エラーのテキスト。
	情報。RAID-event が発生した場合に送信されます。	

## スパム隔離アラート

以下の表は、AsyncOS で生成されるさまざまなスパム隔離アラートのリストです。アラートの説明と重大度が記載されています。

表 5: 発生する可能性があるスパム隔離アラートのリスト

アラート名 (Alert Name)	メッセージと説明	パラメータ
ISQ.CANNOT_CONNECT_OFF_BOX	ISQ: Could not connect to off-box quarantine at \$host:\$port	「host」 : オフボックス隔離のアドレス。 「port」 : オフボックス隔離に接続するポート。
	情報。AsyncOS が (オフボックス) IP アドレスに接続できない場合に送信されます。	
ISQ.CRITICAL	ISQ: \$msg	「msg」 : 表示されるメッセージ
	クリティカル。スパム隔離に重大なエラーが発生した場合に送信されます。	
ISQ.DB_APPROACHING_FULL	ISQ: Database over \$threshold% full	「threshold」 : アラートを開始する使用率のしきい値
	警告。スパム隔離データベースがフルに近い場合に送信されます。	

アラート名 (Alert Name)	メッセージと説明	パラメータ
ISQ.DB_FULL	ISQ: database is full	
	クリティカル。スパム隔離データベースがフルになった場合に送信されます。	
ISQ.MSG_DEL_FAILED	ISQ: Failed to delete MID \$mid for \$rcpt: \$reason	「mid」 : MID
	警告。スパム隔離からの電子メールの削除に失敗した場合に送信されます。	「rcpt」 : 受信者または「all」 「reason」 : メッセージが削除されない理由
ISQ.MSG_NOTIFICATION_FAILED	ISQ: Failed to send notification message: \$reason	「reason」 : 通知が送信されない理由
	警告。通知メッセージの送信に失敗した場合に送信されます。	
ISQ.MSG_QUAR_FAILED	警告。メッセージの隔離に失敗した場合に送信されます。	
ISQ.MSG_RLS_FAILED	ISQ: Failed to release MID \$mid to \$rcpt: \$reason	「mid」 : MID
	警告。メッセージの開放に失敗した場合に送信されます。	「rcpt」 : 受信者または「all」 「reason」 : メッセージが解放されない理由
ISQ.MSG_RLS_FAILED_UNK_RCPTS	ISQ: Failed to release MID \$mid: \$reason	「mid」 : MID
	警告。受信者が不明のため、メッセージの開放に失敗した場合に送信されます。	「reason」 : メッセージが解放されない理由
ISQ.NO_EU_PROPS	ISQ: Could not retrieve \$user's properties. Setting defaults	「user」 : エンドユーザ名
	情報。AsyncOS がユーザの情報を取得できない場合に送信されます。	
ISQ.NO_OFF_BOX_HOST_SET	ISQ: Setting up off-box ISQ without setting host	
	情報。AsyncOS が外部隔離を参照するように設定されているものの、外部隔離が定義されていない場合に送信されます。	

## セーフリスト/ブロックリストアラート

次の表は、AsyncOS で生成されるさまざまなセーフリスト/ブロックリストアラートのリストです。アラートの説明と重大度が記載されています。



表 6: 発生する可能性があるセーフリスト/ブロックリストアラートのリスト

アラート名 (Alert Name)	メッセージと説明	パラメータ
SLBL.DB.RECOVERY_FAILED	SLBL: Failed to recover End-User Safelist/Blocklist database: '\$error'.	「 <b>error</b> 」 : エラーの原因
	クリティカル。セーフリスト/ブロックリストデータベースの復旧に失敗しました。	
SLBL.DB.SPACE_LIMIT	SLBL: End-User Safelist/Blocklist database exceeded allowed disk space: \$current of \$limit.	「 <b>current</b> 」 : データベース使用量 (MB)
	クリティカル。セーフリスト/ブロックリストデータベースが許容されたディスク領域を超過しました。	「 <b>limit</b> 」 : 設定された制限使用量 (MB)

## システムアラート

次の表は、AsyncOS で生成されるさまざまなシステムアラートのリストです。アラートの説明と重大度が記載されています。

表 7: 発生する可能性があるシステムアラートのリスト

コンポーネント/アラート名	メッセージと説明	パラメータ
AMP.ENGINE.ALERT	<a href="#">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</a> を参照してください	-
AsyncOS API アラート	『AsyncOS API for Cisco Email Security Appliances - Getting Started Guide』の「Alerts」セクションを参照してください。	-
メールボックス自動修復アラート	の「アラート」セクションを参照してください。 <a href="#">メールボックスのメッセージの自動修復</a>	-
COMMON.APP_FAILURE	An application fault occurred: \$error	「 <b>error</b> 」 : エラーのテキスト (通常はトレースバック)
	警告。不明なアプリケーション障害が発生した場合に送信されます。	
COMMON.ENGINE_AUTO_UPDATE_ENABLED	<\$level>: <\$class>	<b>'\$engine'</b> : サービス エンジンの名前。値は次のとおりです。 <ul style="list-style-type: none"> <li>• Sophos</li> <li>• McAfee</li> <li>• グレイメール</li> </ul>
	情報 : 自動更新が特定のエンジン <\$engine> に対して有効になっています。これでこのエンジンの自動エンジン更新を受け取ることになります。	

コンポーネント/アラート名	メッセージと説明	パラメータ
COMMON.ENGINE_AUTO_UPDATE_DISABLED	<\$level>: <\$class>	'Engine': サービス エンジンの名前。 値は次のとおりです。  <ul style="list-style-type: none"> <li>• Sophos</li> <li>• McAfee</li> <li>• グレイメール</li> </ul>
	情報：自動更新が特定のエンジン <Engine> に対して無効になっています。特定のエンジンのグローバル設定ページで自動更新を有効にしない限り、このエンジンの自動更新を受け取ることはありません。	
COMMON.KEY_EXPIRED_ALERT	Your "\$feature" key has expired. Please contact your authorized Cisco sales representative.	「feature」：有効期限が切れる機能の名前。
	警告。ライセンス キーの有効期限が切れた場合に送信されます。	
COMMON.KEY_EXPIRING_ALERT	Your "\$feature" key will expire in under \$days day(s). Please contact your authorized Cisco sales representative.	「feature」：有効期限が切れる機能の名前。  「days」：有効期限が切れるまでの日数。
	警告。ライセンス キーの有効期限が切れる場合に送信されます。	
COMMON.KEY_FINAL_EXPIRING_ALERT	This is a final notice. Your "\$feature" key will expire in under \$days day(s). Please contact your authorized Cisco sales representative.	「feature」：有効期限が切れる機能の名前。  「days」：有効期限が切れるまでの日数。
	警告。ライセンス キーの有効期限が切れる場合の最後の通知として送信されます。	
KEYS.GRACE_EXPIRING_ALERT	All security services licenses for this Cisco Email Security Appliance have expired. The appliance will continue to deliver mail without security services for \$days days.	「days」：アラート送信時点での猶予期間の残り日数。  猶予期間の詳細については、 <a href="#">仮想アプライアンスのライセンスの有効期限 (15 ページ)</a> を参照してください。
	To renew security services licenses, Please contact your authorized Cisco sales representative.	
	クリティカル。仮想アプライアンスのライセンス有効期限について、猶予期間の開始時点から定期的に送信されます。	

コンポーネント/アラート名	メッセージと説明	パラメータ
KEYS.GRACE_FINAL_EXPIRING_ALERT	<p>This is the final notice. All security services licenses for this Cisco Email Security Appliance have expired. The appliance will continue to deliver mail without security services for 1 day.</p> <p>To renew security services licenses, Please contact your authorized Cisco sales representative.</p>	<p>猶予期間の詳細については、<a href="#">仮想アプライアンスのライセンスの有効期限 (15 ページ)</a> を参照してください。</p>
KEYS.GRACE_EXPIRED_ALERT	<p>Your grace period has expired. All security service have expired, and your appliance is non-functional. The appliance will no longer deliver mail until a new license is applied.</p> <p>To renew security services licenses, Please contact your authorized Cisco sales representative.</p>	<p>猶予期間の詳細については、<a href="#">仮想アプライアンスのライセンスの有効期限 (15 ページ)</a> を参照してください。</p>
DNS.BOOTSTRAP_FAILED	<p>Failed to bootstrap the DNS resolver. Unable to contact root servers.</p> <p>警告。アプライアンスがルート DNS サーバに問い合わせることができない場合に送信されます。</p>	
COMMON.INVALID_FILTER	<p>Invalid \$class: \$error</p> <p>警告。無効なフィルタが存在する場合に送信されます。</p>	<p>「<b>class</b>」 : 「Filter」、「SimpleFilter」などのいずれか。</p> <p>「<b>error</b>」 : フィルタが無効な理由に関する追加の情報。</p>

コンポーネント/アラート名	メッセージと説明	パラメータ
IPBLOCKD.HOST_ADDED_TO_WHITELIST IPBLOCKD.HOST_ADDED_TO_BLACKLIST IPBLOCKD.HOST_REMOVED_FROM_BLACKLIST	<p>The host at \$ip has been added to the blacklist because of an SSH DOS attack.</p> <p>The host at \$ip has been permanently added to the ssh whitelist.</p> <p>The host at \$ip has been removed from the blacklist</p> <p>Warning。</p> <p>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11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。</p> <p>同じIPアドレスからユーザが正常にログインすると、そのIPアドレスはホワイトリストに追加されます。</p> <p>ホワイトリストのアドレスは、ブラックリストにも登録されていてもアクセスが許可されます。</p> <p>約1日経過後にそのエントリはブラックリストから自動的に削除されます。</p>	「ip」：ログインを試行したIPアドレス。
LDAP.GROUP_QUERY_FAILED_ALERT	<p>LDAP: Failed group query \$name, comparison in filter will evaluate as false</p> <p>クリティカル。LDAPグループクエリーに失敗した場合に送信されます。</p>	「name」：クエリーの名前。
LDAP.HARD_ERROR	<p>LDAP: work queue processing error in \$name reason \$why</p> <p>クリティカル。LDAPクエリーが（すべてのサーバで試行した後）完全に失敗した場合に送信されます。</p>	<p>「name」：クエリーの名前。</p> <p>「why」：エラーが発生した理由。</p>
LOG.ERROR.*	クリティカル。さまざまなロギングエラー。	
MAIL.FILTER.RULE_MATCH_ALERT	<p>MID \$mid matched the \$rule_name rule. \n Details: \$details</p> <p>情報。Header Repeats ルールが true と評価されるたびに送信されます。</p>	<p>「mid」：メッセージの一意の識別番号。</p> <p>「rule_name」：一致したルールの名前。</p> <p>「details」：メッセージまたはルールに関する詳細情報。</p>

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	LDAP group query failure during per-recipient scanning, possible LDAP misconfiguration or unreachable server.	
	クリティカル。各受信者のスキャン時にLDAPグループクエリーに失敗した場合に送信されます。	
MAIL.QUEUE.ERROR.*	クリティカル。メールキューのさまざまなハードエラー。	
MAIL.OMH.DELIVERY_RETRY	件名 - 'Alert: Message Delivery failed for \$hostname. DANE verification failed for one or more Domain(s).'  メッセージ - The message delivery failed due to DANE verification failure for all mail exchange (MX) hosts in \$hostname. The appliance will attempt message delivery again or bounce the message.	'host' - DANE 検証が失敗したホスト。
MAIL.RES_CON_START_ALERT.MEMORY	This system (hostname: \$hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. RAM utilization for this system has exceeded the resource conservation threshold of \$memory_threshold_start%. The allowed receiving rate for this system will be gradually decreased as RAM utilization approaches \$memory_threshold_halt%.	「hostname」 : ホストの名前。  「memory_threshold_start」 : メモリのターピットを開始するパーセントしきい値。  「memory_threshold_halt」 : メモリがフルのためにシステムが停止するパーセントしきい値。
	クリティカル。メモリ使用率がシステムリソース節約しきい値を超過した場合に送信されます。	
MAIL.RES_CON_START_ALERT.QUEUE_SLOW	This system (hostname: \$hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. The queue is overloaded and is unable to maintain the current throughput.	「hostname」 : ホストの名前。
	クリティカル。メールキューが過負荷となり、システムリソース節約がイネーブルになった場合に送信されます。	

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.RES_CON_START_ALERT.QUEUE	<p>This system (hostname: \$hostname) has entered a ‘resource conservation’ mode in order to prevent the rapid depletion of critical system resources. Queue utilization for this system has exceeded the resource conservation threshold of \$queue_threshold_start%. The allowed receiving rate for this system will be gradually decreased as queue utilization approaches \$queue_threshold_halt%.</p> <p>クリティカル。キュー使用率がシステム リソース節約しきい値を超過した場合に送信されます。</p>	<p>「<b>hostname</b>」：ホストの名前。</p> <p>「<b>queue_threshold_start</b>」：キューのターピットを開始するパーセントしきい値。</p> <p>「<b>queue_threshold_halt</b>」：キューがフルのためにシステムが停止するパーセントしきい値。</p>
MAIL.RES_CON_START_ALERT.WORKQ	<p>This system (hostname: \$hostname) has entered a ‘resource conservation’ mode in order to prevent the rapid depletion of critical system resources. Listeners have been suspended because the current work queue size has exceeded the threshold of \$suspend_threshold. Listeners will be resumed once the work queue size has dropped to \$resume_threshold. These thresholds may be altered via use of the ‘tarpit’ command on the system CLI.</p> <p>情報。ワーク キューのサイズが大きすぎるため、リスナーが一時停止された場合に送信されます。</p>	<p>「<b>hostname</b>」：ホストの名前。</p> <p>「<b>suspend_threshold</b>」：リスナーが一時停止されるワーク キューの下限サイズ。</p> <p>「<b>resume_threshold</b>」：リスナーが再開されるワーク キューの上限サイズ。</p>
MAIL.RES_CON_START_ALERT	<p>This system (hostname: \$hostname) has entered a ‘resource conservation’ mode in order to prevent the rapid depletion of critical system resources.</p> <p>クリティカル。アプライアンスが「リソース節約」モードになった場合に送信されます。</p>	<p>「<b>hostname</b>」：ホストの名前。</p>
MAIL.RES_CON_STOP_ALERT	<p>This system (hostname: \$hostname) has exited ‘resource conservation’ mode as resource utilization has dropped below the conservation threshold.</p> <p>情報。アプライアンスの「リソース節約」モードが解除された場合に送信されます。</p>	<p>「<b>hostname</b>」：ホストの名前。</p>

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.SDS.CATEGORY_CHANGE	将来の URL カテゴリ セットの変更を参照してください。	—
MAIL.SDS.CERTIFICATE_INVALID	URL フィルタリングのトラブルシューティングを参照してください。	
MAIL.SDS.ERROR_FETCHING_CERTIFICATE		
MAIL.WORK_QUEUE_PAUSED_NATURAL	work queue paused, \$num msgs, \$reason クリティカル。ワーク キューが中断された場合に送信されます。	「 <b>num</b> 」 : ワーク キューに存在するメッセージ数。 「 <b>reason</b> 」 : ワーク キューが中断された理由。
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	work queue resumed, \$num msgs クリティカル。ワーク キューが再開された場合に送信されます。	「 <b>num</b> 」 : ワーク キューに存在するメッセージ数。
NTP.NOT_ROOT	Not running as root, unable to adjust system time 警告。root として NTP が実行されていないためにアプライアンスが時刻を調整できない場合に送信されます。	
QUARANTINE.ADD_DB_ERROR	Unable to quarantine MID \$mid - quarantine system unavailable クリティカル。メッセージを隔離エリアに送ることができない場合に送信されます。	「 <b>mid</b> 」 : MID
QUARANTINE.DB_UPDATE_FAILED	Unable to update quarantine database (current version: \$version; target \$target_version) クリティカル。隔離データベースがアップデートできない場合に送信されます。	「 <b>version</b> 」 : 検出されたスキーマバージョン。 「 <b>target_version</b> 」 : 対象のスキーマバージョン。
QUARANTINE.DISK_SPACE_LOW	The quarantine system is unavailable due to a lack of space on the \$file_system partition. クリティカル。隔離用のディスク領域がフルになった場合に送信されます。	「 <b>file_system</b> 」 : ファイルシステムの名前
QUARANTINE.THRESHOLD_ALERT	Quarantine "\$quarantine" is \$full% full 警告。隔離エリアの容量使用率が 5 %、50 %、または 75 % に達した場合に送信されます。	「 <b>quarantine</b> 」 : 隔離の名前。 「 <b>full</b> 」 : 隔離エリアの容量使用率。

コンポーネント/アラート名	メッセージと説明	パラメータ
QUARANTINE.THRESHOLD_ALERT.SERIOUS	Quarantine "\$quarantine" is \$full% full	「 <b>quarantine</b> 」：隔離の名前。 「 <b>full</b> 」：隔離エリアの容量使用率。
	クリティカル。隔離エリアの容量使用率が95%に達した場合に送信されます。	
REPORTD.DATABASE_OPEN_FAILED_ALERT	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	「 <b>err_msg</b> 」：発生したエラーメッセージ
	クリティカル。レポートエンジンがデータベースを開けない場合に送信されます。	
REPORTD.AGGREGATION_DISABLED_ALERT	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.	「 <b>threshold</b> 」：しきい値
	警告。システムのディスク領域が不足している場合に送信されます。ログエントリに関するディスク使用率がログ使用率のしきい値を超過すると、reportdは集約をディセーブルにし、アラートを送信します。	
REPORTING.CLIENT.UPDATE_FAILED_ALERT	Reporting Client: The reporting system has not responded for an extended period of time (\$duration).	「 <b>duration</b> 」：クライアントがレポートデーモンへの問い合わせを試行する時間。この値は、人間が読み取れる形式の文字列です（「1h 3m 27s」）。
	警告。レポートエンジンがレポートデータを保存できなかった場合に送信されます。	
REPORTING.CLIENT.JOURNAL_FULL	Reporting Client: 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。レポートエンジンが新規データを保存できない場合に送信されます。	



コンポーネント/アラート名	メッセージと説明	パラメータ
REPORTING.CLIENT.JOURNAL.FREE	Reporting Client: The reporting system is now able to handle new data.  情報。レポート エンジンが再び新規データを保存できるようになった場合に送信されます。	
PERIODIC_REPORTS.REPORT_TASK.BUILD_FAILURE	A failure occurred while building periodic report '\$report_title'. This subscription has been removed from the scheduler.  クリティカル。レポート エンジンがレポートを作成できない場合に送信されます。	「report_title」 : レポートのタイトル
PERIODIC_REPORTS.REPORT_TASK.EMAIL_FAILURE	A failure occurred while emailing periodic report '\$report_title'. This subscription has been removed from the scheduler.  クリティカル。レポートを電子メールで送信できなかった場合に送信されます。	「report_title」 : レポートのタイトル
PERIODIC_REPORTS.REPORT_TASK.ARCHIVE_FAILURE	A failure occurred while archiving periodic report '\$report_title'. This subscription has been removed from the scheduler.  クリティカル。レポートをアーカイブできなかった場合に送信されます。	「report_title」 : レポートのタイトル
SENDERBASE.ERROR	Error processing response to query \$query: response was \$response  情報。SenderBase からの応答を処理中にエラーが発生した場合に送信されます。	「query」 : クエリーするアドレス。 「response」 : 受信した応答の raw データ。
SMTPAUTH.FWD_SERVER_FAILED_ALERT	SMTP Auth: could not reach forwarding server \$ip with reason: \$why  警告。SMTP 認証転送サーバが到達不能である場合に送信されます。	「ip」 : リモート サーバの IP。 「why」 : エラーが発生した理由。
SMTPAUTH.LDAP_QUERY_FAILED	SMTP Auth: LDAP query failed, see LDAP debug logs for details.  警告。LDAP クエリーが失敗した場合に送信されます。	

コンポーネント/アラート名	メッセージと説明	パラメータ
SYSTEM.HERMES_SHUTDOWN_FAILURE. REBOOT	While preparing to \${what}, failed to stop mail server gracefully: \${error}\${what}=reboot  警告。再起動中のシステムをシャットダウンしている際に問題が発生した場合に送信されます。	「error」：発生したエラー。
SYSTEM.HERMES_SHUTDOWN_FAILURE. SHUTDOWN	While preparing to \${what}, failed to stop mail server gracefully: \${error}\${what}=shut down  警告。システムをシャットダウンしている際に問題が発生した場合に送信されます。	「error」：発生したエラー。
SYSTEMLOGIN_FAILURES_LOCK_ALERT	User "\$user" is locked after \$numlogins consecutive login failures. Last login attempt was from \$rhost  情報：失敗したログイン試行が最大数になったためにユーザアカウントがロックされると送信されます。	'user'：ユーザの名前 'numlogins'：構成済みのアラートしきい値 'rhost'：リモートホストのアドレス
SYSTEMRCPTVALIDATION.UPDATE_FAILED	Error updating recipient validation data: \$why  クリティカル。受信者検証のアップデートに失敗した場合に送信されます。	「why」：エラーメッセージ。
SYSTEM.SERVICE_TUNNEL.DISABLED	Tech support: Service tunnel has been disabled  情報。シスコサポートサービス用に作成されたトンネルが無効の場合に送信されます。	
SYSTEM.SERVICE_TUNNEL.ENABLED	Tech support: Service tunnel has been enabled, port \$port  情報。シスコサポートサービス用に作成されたトンネルが有効の場合に送信されます。	「port」：サービストンネルに使用されるポート。

コンポーネント/アラート名	メッセージと説明	パラメータ
IPBLOCKD.HOST_ADDED_TO_WHITELIST IPBLOCKD.HOST_ADDED_TO_BLACKLIST IPBLOCKD.HOST_REMOVED_FROM_BLACKLIST	<p>The host at \$ip has been added to the blacklist because of an SSH DOS attack.</p> <p>The host at \$ip has been permanently added to the ssh whitelist.</p> <p>The host at \$ip has been removed from the blacklist</p> <p>Warning。</p> <p>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 11 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。</p> <p>同じ IP アドレスからユーザが正常にログインすると、その IP アドレスはホワイトリストに追加されます。</p> <p>ホワイトリストのアドレスは、ブラックリストにも登録されていてもアクセスが許可されます。</p> <p>約 1 日経過後にそのエントリはブラックリストから自動的に削除されます。</p>	<p>「ip」：ログインを試行した IP アドレス。</p>
WATCHDOG_RESTART_ALERT_MSG	<p>&lt;\$level&gt;: &lt;\$class&gt;, &lt;\$hostname&gt;: \$subject \$text 警告 (Warning)。</p> <p>Cisco E メールセキュリティアプライアンスは、次のエンジンのヘルス条件をモニタするウォッチドッグサービスを使用します。</p> <ul style="list-style-type: none"> <li>• スпам対策</li> <li>• ウイルス対策</li> <li>• アンチマルウェア防御</li> <li>• グレイメール</li> </ul> <p>上記のエンジンのいずれかが特定期間のウォッチドッグサービスに応答しない場合、ウォッチドッグサービスはエンジンを再起動し、管理者にアラートを送信します。</p>	<p>[「件名」 ('subject')]：エンジンに固有のウォッチドッグアラートの件名</p> <p>[「テキスト」 ('text')]：エンジンに固有のウォッチドッグアラートのテキスト</p>

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.IMH.GEODB_UPDATE_COUNTRIES'	<p>警告 (Warning)。[位置情報の更新 (Geolocation Update)] : サポート対象の国のリストが変更されています。</p> <p>追加された国 : &lt;\$added&gt;</p> <p>削除された国 : &lt;\$deleted&gt;</p> <p>これに応じて HAT 送信者グループ、メッセージフィルタ、およびコンテンツ フィルタの設定を確認します。</p>	<p>'added' : 次の国が追加されます。 &lt;iso_code1&gt;:&lt;country_name1&gt;,&lt;iso_code2&gt;:&lt;country_name2&gt;,</p> <p>'deleted' : 次の国が削除されます。 &lt;iso_code1&gt;:&lt;country_name1&gt;,&lt;iso_code2&gt;:&lt;country_name2&gt;,</p>
MAILUPDATED_SHORT_URL_DOMAIN_LIST	<p>情報 (Info)。短縮 URL ドメインのリストが更新されています。</p> <p>追加されたドメイン : &lt;\$added_domains&gt;</p> <p>削除されたドメイン : &lt;\$deleted_domains&gt;</p>	<p>'added_domains' : 次のドメインが追加されます。 &lt;domains_1&gt;, &lt;domain_2&gt;</p> <p>'deleted_domains' : 次のドメインが削除されます。 &lt;domain_3&gt;, &lt;domain_4&gt;</p>
MAILDOMAINS_NOT_REACHABLE	<p>警告 (Warning)。以下のドメインは短縮された URL サポートのアプライアンスではアクセスできません。 &lt;\$domains&gt;</p> <p>アプライアンスがこれらのドメインに接続できるようにするために、ファイアウォールのルールを確認します。</p>	<p>&lt;\$domains&gt; : ドメインのカンマ区切りリスト。</p>
MAILUPGRADE_CONFIG_CHANGEALERT	<p>情報 (Info)。アップグレード中にユーザ設定値がシステムによって変更された場合に送信されます。</p>	<p>'text' : インテリジェントマルチスキャンおよびグレイメールグローバル設定がアップグレード中に変更されました。インテリジェントマルチスキャンおよびグレイメール設定のグローバル設定を確認してください。</p>

## アップデート アラート

次の表に、AsyncOS で生成される可能性があるさまざまなアップデート アラートのリストを示します。

表 8: 発生する可能性があるアップデート アラートのリスト

アラート名 (Alert Name)	メッセージと説明	パラメータ
UPDATER.APP.UPDATE_ABANDONED	\$app abandoning updates until a new version is published. 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	「 <b>app</b> 」 : アプリケーション名。 「 <b>attempts</b> 」 : 試行した回数。
	警告。アプリケーションはアップデートを中止しています。	
UPDATER.UPDATERD.ANIFEST_FAILED_ALERT	The updater has been unable to communicate with the update server for at least \$threshold.	「 <b>threshold</b> 」 : 人間が読み取れるしきい値の文字列。
	警告。サーバのマニフェストの取得に失敗しました。	
UPDATER.UPDATERD.RELEASE_NOTIFICATION	\$mail_text	「 <b>mail_text</b> 」 : 通知するテキスト。 「 <b>notification_subject</b> 」 : 通知するテキスト。
	警告。リリースの通知です。	
UPDATER.UPDATERD.UPDATE_FAILED	Unknown error ocured: \$traceback	「 <b>traceback</b> 」 : トレースバック。
	クリティカル。アップデートの実行に失敗しました。	

## アウトブレイク フィルタ アラート

次の表は、AsyncOS で生成されるさまざまなアウトブレイクフィルタアラートのリストです。アラートの説明と重大度が記載されています。アウトブレイクフィルタは、隔離（具体的にはアウトブレイク隔離）で使用されるシステムアラートでも参照される場合があることに注意してください。

表 9: 発生する可能性があるアウトブレイク フィルタ アラートのリスト

アラート名 (Alert Name)	メッセージと説明	パラメータ
VOF.GTL_THRESHOLD_ALERT	Outbreak Filters Rule Update Alert:\$text All rules last updated at: \$time on \$date.	「 <b>text</b> 」 : アップデートアラートのテキスト。 「 <b>time</b> 」 : 最終アップデートの時刻。 「 <b>date</b> 」 : 最終アップデートの日付。
	情報。アウトブレイクフィルタのしきい値が変更された場合に送信されます。	

アラート名 (Alert Name)	メッセージと説明	パラメータ
AS.UPDATE_FAILURE	<p>\$engine update unsuccessful. This may be due to transient network or DNS issues, HTTP proxy configuration causing update transmission errors or unavailability of downloads.ironport.com. The specific error on the appliance for this failure is: \$error</p> <p>警告。アンチスパム エンジンまたはCASE ルールのアップデートに失敗した場合に送信されます。</p>	<p>「<b>engine</b>」：アップデートに失敗したエンジン。</p> <p>「<b>error</b>」：発生したエラー。</p>

## クラスタリングアラート

次の表は、AsyncOS で生成されるさまざまなクラスタリングアラートのリストです。アラートの説明と重大度が記載されています。

表 10: 発生する可能性があるクラスタリングアラートのリスト

アラート名 (Alert Name)	メッセージと説明	パラメータ
CLUSTER.CC_ERROR.AUTH_ERROR	<p>Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Machine does not appear to be in the cluster</p> <p>クリティカル。認証エラーが発生した場合に送信されます。マシンがクラスタのメンバーでない場合に起きる可能性があります。</p>	<p>「<b>name</b>」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「<b>ip</b>」：リモートホストの IP。</p> <p>「<b>why</b>」：エラーに関する詳細なテキスト。</p>
CLUSTER.CC_ERROR.DROPPED	<p>Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Existing connection dropped</p> <p>警告。クラスタへの接続がドロップされた場合に送信されます。</p>	<p>「<b>name</b>」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「<b>ip</b>」：リモートホストの IP。</p> <p>「<b>why</b>」：エラーに関する詳細なテキスト。</p>
CLUSTER.CC_ERROR.FAILED	<p>Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Connection failure</p> <p>警告。クラスタへの接続に失敗した場合に送信されます。</p>	<p>「<b>name</b>」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「<b>ip</b>」：リモートホストの IP。</p> <p>「<b>why</b>」：エラーに関する詳細なテキスト。</p>
CLUSTER.CC_ERROR.FORWARD_FAILED	<p>Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Message forward failed, no upstream connection</p> <p>クリティカル。アプライアンスがクラスタのマシンにデータを転送できなかった場合に送信されます。</p>	<p>「<b>name</b>」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「<b>ip</b>」：リモートホストの IP。</p> <p>「<b>why</b>」：エラーに関する詳細なテキスト。</p>

アラート名 (Alert Name)	メッセージと説明	パラメータ
CLUSTER.CC_ERROR.NOROUTE	Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=No route found	<p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「ip」：リモートホストのIP。</p> <p>「why」：エラーに関する詳細なテキスト。</p>
	クリティカル。マシンがクラスタの別のマシンへのルートを取得できなかった場合に送信されます。	
CLUSTER.CC_ERROR.SSH_KEY	Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Invalid host key	<p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「ip」：リモートホストのIP。</p> <p>「why」：エラーに関する詳細なテキスト。</p>
	クリティカル。無効なSSHホストキーがあった場合に送信されます。	
CLUSTER.CC_ERROR.TIMEOUT	Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Operation timed out	<p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「ip」：リモートホストのIP。</p> <p>「why」：エラーに関する詳細なテキスト。</p>
	警告。指定された操作がタイムアウトした場合に送信されます。	
CLUSTER.CC_ERROR_NOIP	Error connecting to cluster machine \$name - \$error - \$why	<p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「why」：エラーに関する詳細なテキスト。</p>
	クリティカル。アプライアンスがクラスタの別のマシンの有効なIPアドレスを取得できなかった場合に送信されます。	
CLUSTER.CC_ERROR_NOIP.AUTH_ERROR	Error connecting to cluster machine \$name - \$error - \$why\$error:=Machine does not appear to be in the cluster	<p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「why」：エラーに関する詳細なテキスト。</p>
	クリティカル。クラスタのマシンに接続する際に認証エラーが発生した場合に送信されます。マシンがクラスタのメンバでない場合に起きる可能性があります。	
CLUSTER.CC_ERROR_NOIP.DROPPED	Error connecting to cluster machine \$name - \$error - \$why\$error:=Existing connection dropped	<p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「why」：エラーに関する詳細なテキスト。</p>
	警告。マシンがクラスタの別のマシンの有効なIPアドレスを取得できず、クラスタへの接続がドロップした場合に送信されます。	

アラート名 (Alert Name)	メッセージと説明	パラメータ
CLUSTER.CC_ERROR_NOIP.FAILED	Error connecting to cluster machine \$name - \$Error - \$why\$error:=Connection failure	「name」：マシンのホスト名およびシリアル番号（またはいずれか）。
	警告。不明な接続エラーが発生し、マシンがクラスタの別のマシンの有効なIPアドレスを取得できなかった場合に送信されます。	「why」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.FORWARD_FAILED	Error connecting to cluster machine \$name - \$Error - \$why\$error:=Message forward failed, no upstream connection	「name」：マシンのホスト名およびシリアル番号（またはいずれか）。
	クリティカル。マシンがクラスタの別のマシンの有効なIPアドレスを取得できず、アプリケーションがマシンにデータを転送できなかった場合に送信されます。	「why」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.NOROUTE	Error connecting to cluster machine \$name - \$Error - \$why\$error:=No route found	「name」：マシンのホスト名およびシリアル番号（またはいずれか）。
	クリティカル。マシンがクラスタの別のマシンの有効なIPアドレスを取得できず、別のマシンへのルートを取得できなかった場合に送信されます。	「why」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.SSH_KEY	Error connecting to cluster machine \$name - \$Error - \$why\$error:=Invalid host key	「name」：マシンのホスト名およびシリアル番号（またはいずれか）。
	クリティカル。マシンがクラスタの別のマシンの有効なIPアドレスを取得できず、有効なSSHホストキーを取得できなかった場合に送信されます。	「why」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.TIMEOUT	Error connecting to cluster machine \$name - \$Error - \$why\$error:=Operation timed out	「name」：マシンのホスト名およびシリアル番号（またはいずれか）。
	警告。マシンがクラスタの別のマシンの有効なIPアドレスを取得できず、指定された操作がタイムアウトした場合に送信されます。	「why」：エラーに関する詳細なテキスト。
CLUSTER.SYNC.PUSH_ALERT	Overwriting \$sections on machine \$name	「name」：マシンのホスト名およびシリアル番号（またはいずれか）。
	クリティカル。設定データが同期から外れ、リモートホストに送信された場合に送信されます。	「sections」：送信中のクラスタセクションのリスト。



## ネットワーク設定値の変更

このセクションでは、アプライアンスのネットワーク操作の設定に使用する機能について説明します。これらの機能では、[システムセットアップウィザードの使用](#)でシステムセットアップウィザード（または `systemsetup` コマンド）を利用して設定したホスト名、DNS、およびルーティングの設定値に直接アクセスできます。

ここでは、次の機能について説明します。

- `sethostname`
- DNS 設定（GUI および `dnsconfig` コマンドを利用）
- ルーティング設定（GUI、`routeconfig` コマンドおよび `setgateway` コマンドを利用）
- `dnsflush`
- パスフレーズ（Passphrase）
- ネットワーク アクセス
- ログインバナー

## システム ホスト名の変更

システムの識別には、ホスト名が使用されます。完全修飾ホスト名を入力する必要があります。ホスト名を変更するには：

- Web インターフェイスで、[ネットワーク（Network）]>[IP インターフェイス（IP Interfaces）]をクリックし、[管理（Management）]をクリックして[ホスト名（Hostname）]でホスト名を変更します。
- CLI で `sethostname` コマンドを使用します。



---

(注) 変更を確定するまで、新しいホスト名は有効になりません。

---

## ドメイン ネーム システム（DNS）設定値の構成

GUI の [ネットワーク（Network）] メニューの [DNS] ページまたは `dnsconfig` コマンドで、アプライアンスの DNS 設定値を設定できます。

次の設定値を設定できます。

- インターネットの DNS サーバまたはユーザ独自の DNS サーバを利用するか、および使用する具体的なサーバ
- DNS トラフィックに使用するインターフェイス
- 逆引き DNS ルックアップがタイムアウトするまで待機する秒数
- DNS キャッシュのクリア

## DNS サーバの指定

AsyncOS では、インターネットのルート DNS サーバ、ユーザ独自の DNS サーバ、またはインターネットのルート DNS サーバおよび指定した権威 DNS サーバを使用できます。インターネットのルートサーバを使用するときは、特定のドメインに使用する代替サーバを指定することもできます。代替 DNS サーバは単一のドメインに適用されるため、当該ドメインに対する権威サーバ（最終的な DNS レコードを提供）である必要があります。

AsyncOS では、インターネットの DNS サーバを使用しない場合に「スプリット」DNS サーバをサポートしています。ユーザ独自の内部サーバを使用している場合は、例外のドメインおよび関連する DNS サーバを指定することもできます。

「スプリット DNS」を設定する場合は、in-addr.arpa (PTR) エントリも同様に設定する必要があります。このため、たとえば「.eng」クエリーをネームサーバ 1.2.3.4 にリダイレクトする際に、すべての .eng エントリが 172.16 ネットワークにある場合、スプリット DNS 設定に「eng.16.172.in-addr.arpa」を指定する必要があります。

## 複数エントリとプライオリティ

入力する各 DNS サーバに、数値でプライオリティを指定できます。AsyncOS では、プライオリティが 0 に最も近い DNS サーバの使用を試みます。DNS サーバが応答しない場合、AsyncOS は次のプライオリティを持つサーバの使用を試みます。同じプライオリティを持つ DNS サーバに複数のエントリを指定する場合、システムはクエリーを実行するたびに同じプライオリティを持つ DNS サーバをリストからランダムに選びます。システムは最初のクエリーの有効期限が切れるか「タイムアウト」するまで短時間待機し、その後次のクエリーに対しては前回よりも少し長い時間待機します。その後も同様です。待機時間は、DNS サーバの正確な合計数と設定されているプライオリティに依存します。タイムアウトの長さはプライオリティに関係なく、すべての IP アドレスで同じです。最初のプライオリティには最も短いタイムアウトが設定されており、次のプライオリティにはより長いタイムアウトが設定されています。最終的なタイムアウト時間は約 60 秒です。1 つのプライオリティを設定している場合、該当のプライオリティに対する各サーバのタイムアウトは 60 秒になります。2 つのプライオリティを設定している場合、最初のプライオリティに対する各サーバのタイムアウトは 15 秒になり、次のプライオリティに対する各サーバのタイムアウトは 45 秒になります。プライオリティが 3 つの場合、タイムアウトは 5 秒、10 秒、45 秒になります。

たとえば、4 つの DNS サーバを設定し、2 つにプライオリティ 0 を、1 つにプライオリティ 1 を、もう 1 つにプライオリティ 2 を設定したとします。

表 11: DNS サーバ、プライオリティ、およびタイムアウト間隔の例

[プライオリティ (Priority)]	サーバ	タイムアウト (秒)
0	1.2.3.4、 1.2.3.5	5、5
1	1.2.3.6	10
2	1.2.3.7	45

AsyncOS は、プライオリティ 0 に設定された 2 つのサーバをランダムに選択します。プライオリティ 0 のサーバが 1 つダウンしている場合、もう 1 つのサーバが使用されます。プライオリティ 0 のサーバが両方ダウンしている場合、プライオリティ 1 のサーバ (1.2.3.6) が使用され、最終的にプライオリティ 2 (1.2.3.7) のサーバが使用されます。

タイムアウト時間はプライオリティ 0 のサーバは両方とも同じであり、プライオリティ 1 のサーバにはより長い時間が設定され、プライオリティ 2 のサーバにはさらに長い時間が設定されます。

## インターネット ルート サーバの使用

AsyncOS DNS リゾルバは、高性能な電子メール配信に必要な大量の同時 DNS 接続を収容できるように設計されています。



- (注) デフォルト DNS サーバにインターネット ルート サーバ以外を設定することを選択した場合、設定されたサーバは権威サーバとなっていないドメインのクエリを再帰的に解決できる必要があります。

## 逆引き DNS ルックアップのタイムアウト

アプライアンスは電子メールの送受信の際、リスナーに接続しているすべてのリモートホストに対して「二重 DNS ルックアップ」の実行を試みます (二重 DNS ルックアップを実行することで、システムはリモート ホストの IP アドレスの正当性を確保および検証します。これは、接続元ホストの IP アドレスに対する逆引き DNS (PTR) ルックアップと、それに続く PTR ルックアップ結果に対する正引き DNS (A) ルックアップからなります。その後、システムは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。結果が一致しないか、A レコードが存在しない場合ログファイルには、一致する受信者がドロ、システムはホストアクセス テーブル (HAT) 内のエン트리と一致する IP アドレスのみを使用します)。この特別なタイムアウト時間はこのルックアップにのみ適用され、[複数エントリとプライオリティ \(74 ページ\)](#) で説明されている一般的な DNS タイムアウトには適用されません。

各 DNS サーバのデフォルト値は 20 秒です。DNS サーバに複数のエントリが存在する場合、合計タイムアウト値は (DNS サーバの数 x 逆引き DNS ルックアップのタイムアウトの値) 秒です。たとえば、DNS サーバの数が 8 で、逆引き DNS ルックアップのタイムアウトの値が 20 秒の場合、合計タイムアウト値は  $(8 \times 20) = 160$  秒です。

秒数に「0」を入力することで、すべてのリスナーに対してグローバルに逆引き DNS ルックアップのタイムアウトを無効にできます。値を 0 秒に設定した場合、逆引き DNS ルックアップは試行されず、代わりに標準のタイムアウト応答がすぐに返されます。また、受信ホストの証明書にホストの IP ルックアップにマッピングされた一般名 (CN) がある場合、TLS 認証接続を求めるドメインにアプライアンスがメールを送信するのを防止します。

## DNS アラート

アプライアンスの再起動時に、まれにメッセージ「DNSキャッシュのブートストラップに失敗しました (Failed to bootstrap the DNS cache)」が付与されたアラートが生成される場合があります。メッセージは、システムによるプライマリ DNS サーバへの問い合わせができなかったことを示しています。この事象は、ネットワーク接続が確立される前に DNS サブシステムがオンラインになった場合、ブートのタイミングで発生します。このメッセージが別のタイミングで表示された場合、ネットワーク問題が発生しているか、または DNS 設定で有効なサーバが指定されていないことを示しています。

## DNS キャッシュのクリア

GUI の [キャッシュを消去 (Clear Cache)] ボタン、または `dnsflush` コマンドを使用して、DNS キャッシュのすべての情報をクリアします (`dnsflush` コマンドの詳細については、『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』を参照してください)。ローカル DNS システムが変更された際に、この機能を使用できます。コマンドはすぐに実行され、キャッシュの再投入中に一時的に性能が低下する可能性があります。

## グラフィカル ユーザ インターフェイスを使用した DNS 設定値の設定

### 手順

- ステップ 1 [ネットワーク (Network)] > [DNS] を選択します。
- ステップ 2 [設定の編集 (Edit Settings)] をクリックします。
- ステップ 3 インターネットのルート DNS サーバまたはユーザ独自の DNS サーバを使用するか、またはインターネットのルート DNS サーバを使用して代替 DNS サーバを指定するかを選択します。
- ステップ 4 ユーザ独自の DNS サーバを使用する場合は、サーバ ID を入力し [行を追加 (Add Row)] をクリックします。各サーバでこの作業を繰り返します。ユーザ独自の DNS サーバを入力する場合は、プライオリティも同時に指定します。詳細については、[DNS サーバの指定 \(74 ページ\)](#) を参照してください。
- ステップ 5 あるドメインに対して代替 DNS サーバを指定する場合は、ドメインと代替 DNS サーバの IP アドレスを入力します。[行を追加 (Add Row)] をクリックし、ドメインを追加します。

(注) ドメイン名をカンマで区切ることで、1つの DNS サーバに対して複数のドメインを入力できます。IP アドレスをカンマで区切ることで、複数の DNS サーバを入力することもできます。
- ステップ 6 DNS トラフィック用のインターフェイスを選択します。
- ステップ 7 逆引き DNS ルックアップを中止するまでに待機する秒数を入力します。
- ステップ 8 [キャッシュをクリア (Clear Cache)] をクリックして、DNS キャッシュをクリアすることもできます。
- ステップ 9 変更を送信し、保存します。

## TCP/IP トラフィック ルートの設定

一部のネットワーク環境では、標準のデフォルト ゲートウェイ以外のトラフィック ルートを使用する必要があります。

E メールセキュリティ アプライアンスはインターネット プロトコルバージョン 4 (IPv4) およびインターネット プロトコルバージョン 6 (IPv6) の両方のスタティック ルートを使用します。

スタティック ルートは CLI で `routeconfig` コマンドを使用して管理するか、または次の手順に従います。

### 手順

- 
- ステップ 1** [ネットワーク (Network) ]>[ルーティング (Routing) ] を選択します。
  - ステップ 2** 作成するスタティック ルートのタイプ (IPv4 または IPv6) のために、[ルートを追加 (Add Route) ] をクリックします。
  - ステップ 3** ルートの名前を入力します。
  - ステップ 4** 宛先 IP アドレスを入力します。
  - ステップ 5** ゲートウェイの IP アドレスを入力します。
  - ステップ 6** 変更を送信し、保存します。
- 

## デフォルト ゲートウェイの設定

デフォルト ゲートウェイを設定するには、CLI で `setgateway` コマンドを使用するか、または次の手順に従います。

### 手順

- 
- ステップ 1** [ネットワーク (Network) ]>[ルーティング (Routing) ] を選択します。
  - ステップ 2** 変更するインターネット プロトコルバージョンのために、ルート リストで [デフォルトルート (Default Route) ] をクリックします。
  - ステップ 3** ゲートウェイの IP アドレスを変更します。
  - ステップ 4** 変更を送信し、保存します。
- 

## SSL 設定の指定

[SSL 構成時の設定 (SSL Configuration Settings) ] ページまたは `sslconfig` コマンドを使用して、アプライアンスの SSL 設定を構成できます。

## 手順

**ステップ 1** [システム管理 (System Administration) ] > [SSL 構成時の設定 (SSL Configuration Settings) ] をクリックします。

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

**ステップ 3** 要件に応じて、次を実行します。

- GUI HTTPS SSL を設定します。[GUI HTTPS] で、使用する SSL 方式と暗号方式を指定します。
- 受信 SMTP SSL を設定します。[受信SMTP (Inbound SMTP) ] で、使用する SSL 方式と暗号化方式を指定します。
- 送信 SMTP SSL を設定します。[送信SMTP (Outbound SMTP) ] で、使用する SSL 方式と暗号化方式を指定します。

次の点を考慮してください。

- SSL v2 方式と TLS v1 方式を同時にイネーブルにはできません。ただし、これらの方式は SSL v3 方式と共にイネーブルにできます。
- TLS v1.0 方式と v1.1 方式を同時に有効にはできません。ただし、これらの方式は TLS v1.2 方式と共に有効にできます。

**ステップ 4** [送信 (Submit) ] をクリックします。

**ステップ 5** [変更を確定 (Commit Changes) ] をクリックします。

## 強化されたセキュリティのための SSLv3 の無効化

セキュリティを強化するために、次のサービスに対して SSLv3 を無効にできます。

- アップデータ
- URL フィルタリング
- エンドユーザ隔離
- LDAP

上記のサービスの SSLv3 をイネーブルまたはディセーブルにするには、CLI で `sslv3config` コマンドを使用します。次の例は、エンドユーザ隔離に対して SSLv3 を無効にする方法を示しています。

```
mail.example.com> sslv3config
Current SSLv3 Settings:
-----
          UPDATER      :      Enabled
    WEBSECURITY      :      Enabled
             EUQ       :      Enabled
             LDAP      :      Enabled
-----
```

```
Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.
[]> setup
Choose the service to toggle SSLv3 settings:
1. EUQ Service
2. LDAP Service
3. Updater Service
4. Web Security Service
[1]>
Do you want to enable SSLv3 for EUQ Service ? [Y]>n
Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.
[]>
```

## システムタイム

アプライアンスのシステム時刻の設定、使用する時間帯の設定、またはNTPサーバとクエリーインターフェイスの選択を行うには、GUIの[システム管理 (System Administration)]メニューから[タイムゾーン (Time Zone)]ページまたは[時刻設定 (Time Settings)]ページを使用するか、CLIのntpconfig コマンド、settime コマンドおよび setz コマンドを使用します。

AsyncOS で使用される時間帯ファイルは、[システム管理 (System Administration)]>[時刻設定 (Time Settings)]ページ、または tzupdate CLI コマンドで確認することもできます。

## タイムゾーンを選択

[タイムゾーン (Time Zone)]ページ (GUIの[システム管理 (System Administration)]メニューから利用可能) では、アプライアンスの時間帯を表示します。特定の時間帯または GMT オフセットを選択できます。

### 手順

- ステップ 1** [システム管理 (System Administration)]>[タイムゾーン (Time Zone)]ページで、[設定を編集 (Edit Settings)]をクリックします。
- ステップ 2** 地域、国、および時間帯をプルダウンメニューから選択します。
- ステップ 3** 変更を送信し、保存します。

## GMT オフセットの選択

### 手順

- ステップ 1** [システム管理 (System Administration)]>[タイムゾーン (Time Zone)]ページで、[設定を編集 (Edit Settings)]をクリックします。
- ステップ 2** 地域のリストから [GMT オフセット (GMT Offset)]を選択します。

**ステップ3** [タイムゾーン (Time Zone)] リストでオフセットを選択します。オフセットとは、GMT (グリニッジ子午線) に達するために足し引きする必要がある時間のことです。時間の前にマイナス記号 (「-」) が付いている場合、グリニッジ子午線の東側にあたります。プラス記号 (「+」) の場合、グリニッジ子午線の西側にあたります。

**ステップ4** 変更を送信し、保存します。

## 時刻設定の編集

次の方法の1つを使用して、アプライアンスの時間設定を編集できます。

- (推奨) ネットワーク タイム プロトコル (NTP) を使用したアプライアンスのシステム時刻の設定 (80 ページ)
- アプライアンス システム時刻の手動設定 (80 ページ)

### (推奨) ネットワークタイムプロトコル (NTP) を使用したアプライアンスのシステム時刻の設定

これは、特にアプライアンスが他のデバイスに統合されている場合に推奨される、時刻の設定方法です。統合されたデバイスはすべて、同じの NTP サーバを使用する必要があります。

#### 手順

**ステップ1** [システム管理 (System Administration)] > [時刻設定 (Time Settings)] ページに移動します。

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

**ステップ3** [時刻の設定方法 (Time Keeping Method)] セクションで、[NTP (Network Time Protocol) を使用 (Use Network Time Protocol)] を選択します。

**ステップ4** NTP サーバのアドレスを入力し、[行を追加 (Add Row)] をクリックします。複数の NTP サーバを追加できます。

**ステップ5** NTP サーバをリストから削除するには、サーバのゴミ箱アイコンをクリックします。

**ステップ6** NTP クエリー用のインターフェイスを選択します。これは、NTP クエリーが発信される IP アドレスになります。

**ステップ7** 変更を送信し、保存します。

### アプライアンス システム時刻の手動設定

通常、この時刻の設定方法は推奨されません。代わりにネットワーク タイム プロトコル サーバを使用します。



## 手順

- ステップ1 [システム管理 (System Administration)] > [時刻設定 (Time Settings)] ページに移動します。
- ステップ2 [設定の編集 (Edit Settings)] をクリックします。
- ステップ3 [時刻の設定方法 (Time Keeping Method)] セクションで、[時刻を手動で設定 (Set Time Manually)] を選択します。
- ステップ4 月、日、年、時、分、および秒を入力します。
- ステップ5 [A.M.] または [P.M.] を選択します。
- ステップ6 変更を送信し、保存します。

## ビューのカスタマイズ

- [お気に入りページの使用 \(81 ページ\)](#)
- [ユーザ設定値の設定 \(82 ページ\)](#)

### お気に入りページの使用

(ローカル認証された管理ユーザ限定) よく利用するページのクイック アクセス リストを作成できます。

目的	操作手順
お気に入りリストにページを追加する	追加するページに移動し、ウィンドウの右上隅付近にある [お気に入り (My Favorites)] メニューから [このページをお気に入りに追加 (Add This Page To My Favorites)] を選択します。 お気に入りへの変更では確定操作は必要ありません。
お気に入りの順序を変更する	[お気に入り (My Favorites)] > [お気に入りをすべて表示 (View All My Favorites)] を選択し、適切な順序にお気に入りをドラッグします。
お気に入りを削除する	[お気に入り (My Favorites)] > [お気に入りをすべて表示 (View All My Favorites)] を選択し、お気に入りを削除します。
お気に入りページに移動する	ウィンドウの右上隅付近にある [お気に入り (My Favorites)] からページを選択します。
カスタム レポート ページを表示または作成する	[ <a href="#">マイ ダッシュボード (My Dashboard)</a> ] ページを参照してください。

## ユーザ設定値の設定

ローカルユーザは、各アカウントに固有な言語などのプリファレンス設定を定義できます。これらの設定は、ユーザがアプライアンスに最初にログインするときにデフォルトで適用されます。各ユーザにプリファレンス設定が保存され、ユーザがアプライアンスにログインするクライアントマシンに関係なく同じです。

ユーザがこれらの設定を変更し、変更をコミットしないと、再びログインするときに設定がデフォルト値に戻ります。



(注) この機能は、外部認証されたユーザは使用できません。これらのユーザは、[オプション (Options)] メニューから直接言語を選択できます。

### 手順

- ステップ 1** プリファレンス設定を定義するユーザアカウントでアプライアンスにログインします。
- ステップ 2** [オプション (Options)] > [環境設定 (Preferences)] を選択します。[オプション (Options)] メニューは、ウィンドウの上部右側にあります。
- ステップ 3** [設定を編集 (Edit Preferences)] をクリックします。
- ステップ 4** 設定を行います。

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 で使用する言語の Web 用 AsyncOS。
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。

- ステップ 5** 変更を送信し、保存します。
- ステップ 6** ページ下部の [前のページに戻る (Return to previous page)] リンクをクリックします。

## Internet Explorer の互換モードの上書き

優れた Web インターフェイスのレンダリングのために、Internet Explorer 互換モードのオーバーライドを有効にすることを推奨します。



(注) この機能を有効にすることが組織のポリシーに違反する場合は、この機能を無効にすることができます。

### 手順

- ステップ 1 [システム管理 (System Administration)] > [一般設定 (General Settings)] をクリックします。
- ステップ 2 [IE 互換モードの上書き (Override IE Compatibility Mode)] チェックボックスをオンにします。
- ステップ 3 変更を送信し、保存します。

## 最大 HTTP ヘッダー サイズの構成

アプライアンスに送信される HTTP 要求の HTTP ヘッダーの最大サイズを設定するため、CLI で `adminaccessconfig > maxhttpheaderfieldsize` コマンドを使用できるようになりました。

HTTP ヘッダー フィールドのサイズの既定値は 4096 (4 KB)、最大値は 33554432 (32 MB) です。

## サービス エンジンの再起動とステータスの表示

CLI で `diagnostic > services` サブコマンドを使用して、以下を実行できます。

- アプライアンスで有効になっているサービスエンジンを再起動します。アプライアンスを再起動する必要はありません。
- アプライアンスで有効になっているサービス エンジンのステータスを表示します。

### 例：DLP エンジンのステータスの表示

次の例では、`services` コマンドを使用して、アプライアンスで有効になっている DLP エンジンのステータスを表示します。

```
mail.example.com> diagnostic
```

```
Choose the operation you want to perform:  
- RAID - Disk Verify Utility.  
- DISK_USAGE - Check Disk Usage.  
- NETWORK - Network Utilities.
```

```
- REPORTING - Reporting Utilities.  
- TRACKING - Tracking Utilities.  
- RELOAD - Reset configuration to the initial manufacturer values.  
- SERVICES - Service Utilities.  
[]> services
```

```
Choose one of the following services:  
- ANTISPAM - Anti-Spam services  
- ANTIVIRUS - Anti-Virus services  
- DLP - Cisco Data Loss Prevention services  
- ENCRYPTION - Encryption services  
- GRAYMAIL - Graymail services  
- REPORTING - Reporting associated services  
- SBRS - Reputation Engine services  
- TRACKING - Tracking associated services  
- URLFILTERING - URL Filtering  
- EUQWEB - End User Quarantine GUI  
- WEBUI - Web GUI  
[]> dlp
```

```
Choose the operation you want to perform:  
- RESTART - Restart the service  
- STATUS - View status of the service  
[]> status
```

Cisco Data Loss Prevention has been up for 3s.

### 例：Graymail エンジンの再起動

次の例では、`services` コマンドを使用して、アプライアンスの Graymail エンジンを再起動します。

```
mail.example.com> diagnostic
```

```
Choose the operation you want to perform:  
- RAID - Disk Verify Utility.  
- DISK_USAGE - Check Disk Usage.  
- NETWORK - Network Utilities.  
- REPORTING - Reporting Utilities.  
- TRACKING - Tracking Utilities.  
- RELOAD - Reset configuration to the initial manufacturer values.  
- SERVICES - Service Utilities.  
[]> services
```

```
Choose one of the following services:  
- ANTISPAM - Anti-Spam services  
- ANTIVIRUS - Anti-Virus services  
- DLP - Cisco Data Loss Prevention services  
- ENCRYPTION - Encryption services  
- GRAYMAIL - Graymail services  
- REPORTING - Reporting associated services  
- SBRS - Reputation Engine services  
- TRACKING - Tracking associated services  
- URLFILTERING - URL Filtering  
- EUQWEB - End User Quarantine GUI  
- WEBUI - Web GUI  
[]> graymail
```

```
Choose the operation you want to perform:  
- RESTART - Restart the service  
- STATUS - View status of the service
```

```
[ ]> restart
```

