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。

- 電子メールゲートウェイの管理 （2 ページ）
- 電子メールゲートウェイのライセンス （5 ページ）
- 仮想電子メールゲートウェイのライセンス （10 ページ）
- 設定ファイルの管理 （11 ページ）
- [設定ファイル（Configuration File）] ページ （17 ページ）
- ディスク領域の管理 （17 ページ）
- セキュリティ サービスの管理 （19 ページ）
- サービス アップデート （21 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 （22 ページ）
- AsyncOS のアップグレード （32 ページ）
- リモート電源再投入の有効化 （38 ページ）
- AsyncOS の以前のバージョンへの復元 （39 ページ）
- 電子メールゲートウェイに生成されるメッセージの返信アドレスの設定 （41 ページ）
- システム状態パラメータのしきい値の設定 （42 ページ）
- 電子メールゲートウェイの状況の確認 （43 ページ）
- アラート （44 ページ）
- ネットワーク設定値の変更 （72 ページ）
- SAML 2.0 を使用したシングル サインオン（SSO） （79 ページ）
- AsyncOS API 向けの電子メールゲートウェイでの OpenID Connect 1.0 の設定 （90 ページ）
- システム タイム （93 ページ）
- ビューのカスタマイズ （96 ページ）
- 全般設定 （97 ページ）
- 最大 HTTP ヘッダー サイズの構成 （99 ページ）

• サービス エンジンの再起動とステータスの表示 （99 ページ）
• 国際化ドメイン名（IDN）を含むメッセージの受信と配信 （99 ページ）

電子メールゲートウェイの管理

以下のタスクでは、電子メールゲートウェイ内の一般的な機能を簡単に管理できます。

• 電子メールゲートウェイ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）

電子メールゲートウェイのシャットダウンおよび再起動

電子メールゲートウェイは、シャットダウンまたは再起動した後で、配信キュー内のメッセージを失わずに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。電子メールゲートウェイ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。

電子メールゲートウェイ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。

電子メールゲートウェイ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、 電子メールゲートウェイ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、電子メールゲートウェイがオフライン状態にあるときにのみ動作します。出荷時の設定にリセットした後、電子メールゲートウェイはオンライン状態に戻ります。

次のステップ

- 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

電子メールゲートウェイ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。

電子メールゲートウェイのライセンス

• ライセンス キー （5 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）

クラウド電子メールゲートウェイでは、ライセンスキーの設定を変更しないようにしてください。

ライセンス キーの追加および管理

物理 電子メールゲートウェイの場合、ライセンスキーは 電子メールゲートウェイのシリアル番号と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	操作内容
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。

目的	操作内容
電子メールゲートウェイ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。
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 （17 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

電子メールゲートウェイ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に、この 電子メールゲートウェイを設定できます。

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電子メールゲートウェイから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 （44 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

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、『Smart Licensing Deployment Guide for Cisco Secure Email Gateway and Cisco Secure Email and Web Manager』[英語] を参照してください。

仮想ゲートウェイのスマートライセンスでのセキュア電子メールリレー

セキュア電子メールリレー機能を使用すると、Cisco Secure Email Gateway を使用して大量の電子メールを送信できます。この機能は、仮想ゲートウェイのスマートライセンスを持つアカウントでのみ使用でき、オンプレミスまたはクラウドのセットアップでは使用できません。また、特定/永続ライセンス予約では機能しません。

リレーモードに切り替えると、Cisco Secure Email Gateway はメール転送エージェント（MTA）としてのみ機能し、スパム対策、ウイルス対策、マルウェア対策などの他の機能はオフになります。他のライセンスは使用できません。

サポートされている仮想プラットフォーム

- VMware ESXi 7.0, 8.0
- Microsoft HyperV Gen 2
- カーネルベース仮想マシン (KVM)
- Open Virtualization Format（OVF）
- Nutanix

セキュア電子メールリレーのスマートライセンスは、次の Cisco Smart Software Manager（CSSM）の状態で動作します。

- **コンプライアンスに準拠**：ライセンスとその日付は、 Cisco Smart Software Manager ポータルで確認できます。
- **コンプライアンス違反（OOC）**：ライセンスが使用できないか、期限切れです。要求された最初のライセンスが使用できないか期限切れの場合、リレー機能は動作しません。ただし、一部のライセンスがすでに発行されていて、次の要求が OOC である場合、リレー機能は中断することなく続行されます。

（注） リレー機能は、評価（EVAL）状態では許可されません。

セキュア電子メールリレーの仕組み

リレーモードを有効にした後、最初にセキュア電子メールリレーライセンスを要求する必要があります。セキュア電子メールリレー機能を要求すると、要求が Cisco Smart Software Manager（CSSM）ポータルに送信されます。電子メール ゲートウェイ インスタンスは、電子メールの送信数に応じて複数のライセンスを使用できます。通常、1 つのライセンスで最大 100 万件の電子メールを送信できます。

電子メールゲートウェイからの送信メールが 1 時間ごとにチェックされ、定義された制限の 80% に達すると管理者にアラートが送られます。100% に達すると、管理者にもう一度アラートが送られます。100% に達すると、10% の制限の猶予が与えられます。猶予バッファを使用した後に、次のライセンスが自動的に要求されます。スマートライセンスのコンプライアンスに準拠している場合は、このプロセスが繰り返されます。使用可能なライセンスがないためにコンプライアンス違反（OOC）になった場合、アラート/警告が送信され、機能は続行されます。

セキュア電子メールリレーライセンスがスマートライセンスに登録され、[コンプライアンスに準拠（In Compliance）] になると、ライセンスは各日の終わり（午前 0 時）に CSSM ポータルでリリースされ、翌日の始まりに新しいライセンスで電子メールゲートウェイが開始されます。

（注） セキュア電子メールリレーライセンスを要求すると、バウンス検証もデフォルトで有効になります。ただし、サポートされるバウンス検証機能は限定されており、アドレスタグ設定のみがサポートされます。

バウンスのタグ値を除き、保存や読み込み中に XML コンフィギュレーション ファイルに変更を加えないでください。

（注） リレーモードに切り替えた最初の日に、通常モードの最後の1時間に送信された発信メールがリレーモードの発信カウントに追加されます。こうした状況が発生するのは、時間ベースのインターバルカウンタが切り替え時間の始めに切り下げられるため、その時間内に通常モードで送信されたメールがリレーモードカウントに追加されるためです。

（注） アウトバウンド要求は毎日自動的に行われるため、猶予期間はありません。

メーラーエイリアスリストは 1 件としてカウントされます。

受信者またはドメインの問題が原因で送信に失敗した電子メールはカウントされます。

内部フィルタ処理設定が原因で送信に失敗した電子メールはカウントされません。

隔離された電子メール（ローカルと集中型の両方）は、発信カウントに含まれます。

リレーモードへの切り替え

始める前に

- 電子メールゲートウェイでスマート ソフトウェア ライセンシングを有効にし、スマートライセンス登録方法に従って電子メールゲートウェイを登録します。

手順

ステップ 1 [システム管理（System Administration）] > [ライセンス（Licenses）] に移動します。

ステップ 2 [リレーモードへの切り替え（Switch to relay mode）] をクリックします。

ステップ 3 表示されるポップアップで [送信（Submit）] をクリックします。

（注）
リレーモードに切り替えると、通常モードに戻ることはできません。

ステップ 4 [ライセンスの要求/リリース（Request/Release Licenses）] をクリックします。

ステップ 5 [セキュア電子メールリレー（Secure Email Relay）] の [ライセンス要求（License Request）] チェックボックスをオンにします。

ステップ 6 **[送信（Submit）]** をクリックします。

[ライセンス（Licenses）]ページで、[ライセンス認証ステータス（License Authorization Status）] にスマートライセンスのステータスが反映されるまで待ちます。

ログの表示

Cisco Secure Email リレーに関するログ情報はメールログに書き込まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

Cisco Secure Email リレーのログエントリの例

この例では、電子メールゲートウェイがリレーモードで設定されており、SENDERBASE レピュテーション フィルタリング ライセンスが期限切れと表示されているため、受信メールの処理に失敗したことがログに示されます。

```
Info: New SMTP ICID 42 interface Management (10.10.12.10) address 10.10.20.30 reverse
dns host unknown verified no
Info: ICID 42 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS not enabled country not enabled
Info: ICID 42 from address 10.10.20.30 rejected due to license expiry
```

この例では、電子メールゲートウェイがリレーモードで設定されているため、送信メールが配信されます。

```
Info: New SMTP DCID 49 interface 10.10.12.10 address 120.30.100.200 port 25
Info: TLS processing time client side: 0.123456789012
Info: Delivery start DCID 49 MID 19 to RID [0]
Info: Message done DCID 49 MID 19 to RID [0]
Debug: Service Logs: ESA Message data request queued for MID: 19
Info: MID 19 RID [0] Response 'ok:  Message 121032581 accepted'
Info: Message finished MID 19 done
```

仮想電子メールゲートウェイのライセンス

仮想電子メールゲートウェイ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） 仮想電子メールゲートウェイ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。

仮想電子メールゲートウェイのライセンスの有効期限

仮想電子メールゲートウェイのライセンスの有効期限が切れてから 180 日間、この電子メールゲートウェイ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 （46 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、仮想電子メールゲートウェイ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

- 仮想電子メールゲートウェイでの AsyncOS の復元がライセンスに影響を及ぼす可能性（39 ページ）

設定ファイルの管理

電子メールゲートウェイ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。電子メールゲートウェイ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、電子メールゲートウェイの設定全体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、変更を加えて同じ 電子メールゲートウェイ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電子メールゲートウェイの管理

- ある電子メールゲートウェイから既存の設定ファイルをダウンロードし、変更を行い、別の電子メールゲートウェイにアップロードできます。これにより、複数の電子メールゲートウェイ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 電子メールゲートウェイから M シリーズ Cisco Secure Manager Email and Web Gateway にロードできません。
- ある電子メールゲートウェイからダウンロードされた既存の設定ファイルを、複数のサブセクションに分割できます。（複数の電子メールゲートウェイ環境の）すべての電子メールゲートウェイ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電子メールゲートウェイにロードできます。

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電子メールゲートウェイを使用できます。グローバル配信停止リストを適切に設定した場合は、テスト電子メールゲートウェイ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電子メールゲートウェイにロードできます。

コンフィギュレーション ファイルの管理

電子メールゲートウェイ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フレーズと共に、暗号化されない PEM 形式で含められます。

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 （12 ページ）
- コンフィギュレーション ファイルのロード （13 ページ）
- 設定ファイルのメール送信 （13 ページ）
- 現在の設定のリセット （16 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）]** の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、電子メールゲートウェイで保存したり（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 ユーザー ID と契約 ID。

[設定ファイル内のパスフレーズを隠す（Mask passphrases in the Configuration Files）] チェックボックスをクリックして、ユーザのパスフレーズをマスクできます。パスフレーズをマスクすると、元の暗号化されたパスフレーズが、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、パスフレーズ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フレーズを隠す（Encrypt passphrases in the Configuration Files）] チェックボックスをクリックして、ユーザのパスフレーズをマスクできます。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
- ローカルユーザー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、新しい設定情報を電子メールゲートウェイにロードします。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、クラスタまたは電子メールゲートウェイ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、クラスタ化された電子メールゲートウェイ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、電子メールゲートウェイの `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、電子メールゲートウェイの外部で 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、現在電子メールゲートウェイ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。別のプロトコル、シリアルインターフェイス、または管理ポートのデフォルト設定を使用して電子メールゲートウェイ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

- クラスタ化された電子メールゲートウェイの設定のロード

現在の設定のリセット

現在の設定をリセットすると、電子メールゲートウェイ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 （11 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 E メール ゲートウェイのみ）使用可能なディスク領域の増加 （17 ページ）
- ディスク領域の使用率の表示および割り当て （18 ページ）
- その他のクォータのディスク領域の管理 （18 ページ）
- ディスク領域に関するアラートの受信の確認 （19 ページ）

（仮想 E メール ゲートウェイのみ）使用可能なディスク領域の増加

ESXi 5.5 および VMFS 5 を実行する仮想 E メール ゲートウェイの場合、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 E メール ゲートウェイの場合は 2 TB に制限されます。

仮想 E メール ゲートウェイ 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 ゲートウェイ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。

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

E メール ゲートウェイで、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	操作内容
• 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 • いつでも E メールゲートウェイでディスク領域を再割り当てできます	[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	• 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。 • 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。隔離メッセージに自動的に適用されるデフォルト アクションを参照してください。 • 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。その他のクォータのディスク領域の管理 （18ページ） を参照してください。

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	[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] に移動して、 • 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。 • 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。 • 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。 • 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。
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。
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）。	E メール ゲートウェイの /data/pub ディレクトリに FTP でアクセスします。 E メール ゲートウェイへの FTP アクセスを構成するには、FTP、SSH、および SCP アクセスを参照してください。
クオータ 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 （44 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 （20 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 （21 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 （20 ページ）
- エンジンの以前のバージョンへのロールバック （21 ページ）
- ログの表示 （21 ページ）
- システム アラート （54 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）] クリックします。

電子メールゲートウェイにより、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 スパム 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、Talosインテリジェンス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電子メールゲートウェイを設定するには、「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 （22 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 （22 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 （23 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 電子メールゲートウェイの設定 （23 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 （24 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 （25 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 （26 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 （27 ページ）
- 自動アップデートの設定 （30 ページ）
- アップデータサーバ証明書の有効性を検証するための 電子メールゲートウェイの設定 （30 ページ）
- プロキシサーバとの通信を信頼するためのアプライアンスの設定 （31 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

電子メールゲートウェイに 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。

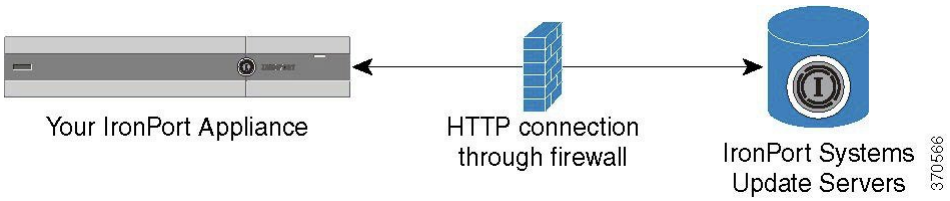
- 各電子メールゲートウェイでは、シスコのアップデートサーバからファイルを直接ダウンロードできます。これがデフォルトの方法です。
- シスコからファイルを1回ダウンロードし、ネットワーク内のサーバから電子メールゲートウェイにファイルを配信できます。ローカルサーバからのアップグレードおよびアップデート （24 ページ）を参照してください。

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 （27 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

電子メールゲートウェイは、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 電子メールゲートウェイの設定 （23 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 電子メールゲートウェイの設定

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て、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。

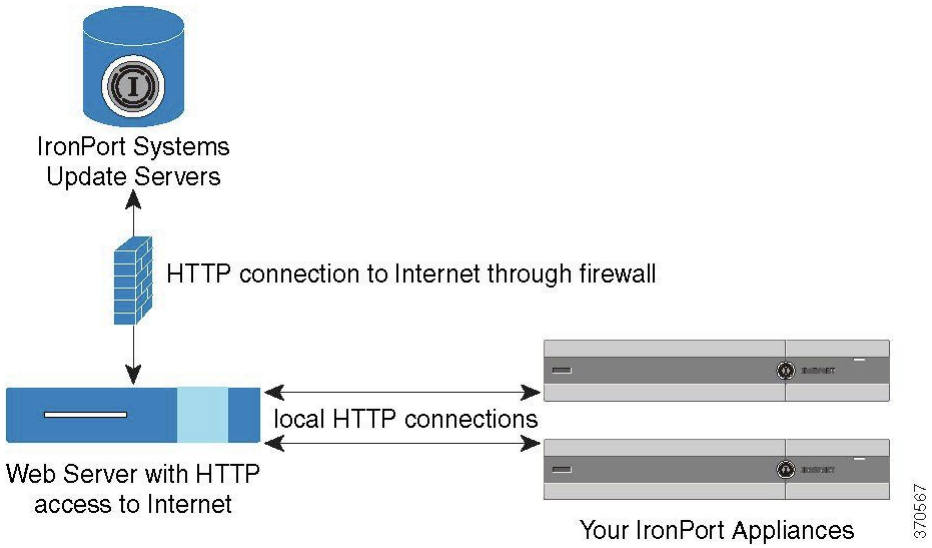
ローカル サーバからのアップグレードおよびアップデート

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。

電子メールゲートウェイ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 電子メールゲートウェイへの 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、ネットワーク上の電子メールゲートウェイは常に最新のセキュリティサービス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 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 電子メールゲートウェイの）シリアル番号または（仮想 電子メールゲートウェイの）VLN および 電子メールゲートウェイ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 電子メールゲートウェイを設定します。

ローカルサーバは、ネットワーク上の 電子メールゲートウェイで利用可能な 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 asyncos 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

電子メールゲートウェイは、（デフォルトで）シスコの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かないようにする場合は、アップデートされたルールを電子メールゲートウェイ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

電子メールゲートウェイ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

電子メールゲートウェイ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 （22 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)）	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。 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。 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フレーズも入力します。 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。 （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。
アップデートサーバ（リスト）（Update Servers (lists)）	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電子メールゲートウェイ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。 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。 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。 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フレーズを入力します。

設定	説明
自動更新	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（電子メールゲートウェイがアップデートを確認する頻度）をイネーブルにします。 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。 （注） [セキュリティ サービス（Security Services）] > [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、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。
無効な自動エンジン更新のアラート間隔	「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。 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。
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、 電子メール ゲートウェイで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。 （注） HTTP プロトコルは、HTTP プロキシサーバーを設定するときに使用できます。 （注） HTTPS プロトコルは、HTTP プロキシサーバーの設定ではサポートされていません。

設定	説明
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。 （注） HTTP プロトコルは、HTTPS プロキシサーバーを設定するときに使用できます。 （注） HTTPS プロトコルは、HTTPS プロキシサーバーの設定ではサポートされていません。

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。

アップデータサーバ証明書の有効性を検証するための電子メールゲートウェイの設定

電子メールゲートウェイでは、電子メールゲートウェイがアップデータサーバと通信するたびに、シスコのアップデータ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、詳細がアップデータ 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ためのアプライアンスの設定

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証明書を電子メールゲートウェイに追加できます。これにより、電子メールゲートウェイ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。	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 （22 ページ）
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。	使用可能なアップグレードの通知 （33 ページ）
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。	AsyncOS のアップグレードの準備 （34 ページ） クラスタ内のマシンのアップグレード
ステップ 4	アップグレードを実行します。	アップグレードのダウンロードとインストール （35 ページ）

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）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 アップグレードが電子メールゲートウェイで使用可能な場合、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す。

目的	操作内容
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、電子メールゲートウェイ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 アップグレードが電子メールゲートウェイで使用可能な場合、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す。

目的	操作内容
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。

目的	操作内容
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、電子メールゲートウェイ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 コマンドで電子メールゲートウェイ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電子メールゲートウェイを設定します。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 （22 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 （27 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（34 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。
- アップグレード後は、FIPS モードでは TLS v1.0 を使用できなくなります。ただし、必要に応じて、電子メールゲートウェイで TLS v1.0 を再び有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）] > [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 [アップグレード（Upgrade）] をクリックしてアップグレードプロセスに進みます。

ステップ 4 次のオプションを選択します。

目的	操作内容
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) 現在の設定を電子メールゲートウェイ上の 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、電子メールゲートウェイ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電子メールゲートウェイ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（11 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	操作内容
ダウンロードステータスの表示	ページの中央を確認してください。 進行中のダウンロードおよびダウンロードが完了してインストールされるのを待っているものがない場合は、ダウンロードのステータス情報は表示されません。
ダウンロードのキャンセル	ページの中央にある、[ダウンロードをキャンセル（Cancel Download）] ボタンをクリックします。 このオプションは、ダウンロード進行中にのみ表示されます。
ダウンロードされたインストーラの削除	ページの中央にある、[ファイルを削除（Delete File）] ボタンをクリックします。 このオプションは、インストーラがダウンロードされている場合にのみ表示されます。

ステップ 4 （オプション）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

電子メールゲートウェイ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。

電子メールゲートウェイ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、電子メールゲートウェイ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。
- 電子メールゲートウェイ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フレーズ。

   これらのクレデンシャルは、電子メールゲートウェイ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、電子メールゲートウェイ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

- 電子メールゲートウェイ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

電子メールゲートウェイにおける 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、復元は電子メールゲートウェイ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電子メールゲートウェイ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コンフィギュレーション ファイルが必要です。コンフィギュレーション ファイルに下位互換性はありません。

仮想電子メールゲートウェイでの 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、電子メールゲートウェイ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

- 仮想電子メールゲートウェイのライセンスの有効期限 （10 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 （13 ページ）を参照してください。

ステップ 2 電子メールゲートウェイ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 バージョンを戻す電子メールゲートウェイの 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てください。

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、電子メールゲートウェイ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 電子メールゲートウェイが 2 回リブートするまで待ちます。

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。

復元が完了した電子メールゲートウェイは、選択された AsyncOS バージョンを使用して稼働します。

電子メールゲートウェイに生成されるメッセージの返信アドレスの設定

クラウド電子メールゲートウェイの返信アドレスは変更しないことを推奨します。

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す。

- 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

（注） バウンスメッセージの場合、電子メールの標準規格に従って、エンベロープ送信者は常に空（<>）になります。返信アドレスの設定は、エンベロープ送信者ではなく、ヘッダー送信元にのみ影響します。

返信アドレスの表示、ユーザー、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、電子メールゲートウェイ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、電子メールゲートウェイ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、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、または15分のアラート間隔の後、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 （46 ページ） を参照してください。

電子メールゲートウェイの状況の確認

ヘルスチェック機能を使用して、電子メールゲートウェイ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、電子メールゲートウェイ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、コマンド **healthcheck** 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が示されます。

- 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

ヘルスチェックにおいて、電子メールゲートウェイで上記の問題が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、電子メールゲートウェイ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 E メール ゲートウェイ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、 E メール ゲートウェイで生成されます。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電子メールゲートウェイを設定できます。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（47ページ）を参照してください。

アラートの配信

電子メールゲートウェイから [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電子メールゲートウェイ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。

（注） （オプション - TLS サポートが `alertconfig` CLI コマンドを使用して有効化され、FQDN 検証が [SSL 構成（SSL Configuration）] の設定ページで有効な場合のみ）：サーバー証明書にある [共通名（Common Name）]、[SAN：DNS名（SAN: DNS Name）] フィールド、またはその両方が FQDN 形式かどうかを確認します

（注） （オプション - TLS サポートが `alertconfig` CLI コマンドを使用して有効化され、X 509 検証が [SSL 構成（SSL Configuration）] の設定ページで有効な場合のみ）：サーバ証明書の署名アルゴリズムを確認します。

（注） （オプション - TLS サポートが `alertconfig` CLI コマンドを使用して有効化され、 [SSL構成時の設定（SSL Configuration Settings）] ページで X 509 検証が有効になっている場合のみ）：サーバー証明書にある [共通名（Common Name）] または [SAN: DNS名（SAN: DNS Name）] フィールドにサーバー名が存在するかどうかを確認します。

（注） （オプション - TLS サポートが `alertconfig` CLI コマンドを使用して有効化され、 [SSL構成時の設定（SSL Configuration Settings）] ページで X 509 検証が有効になっている場合のみ）：サーバー証明書のバージョンを確認します。

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

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 （オプション）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電子メールゲートウェイ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 （48 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 （44 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 コマンドを使用して、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

電子メールゲートウェイ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、電子メールゲートウェイ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、電子メールゲートウェイは **[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電子メールゲートウェイ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 （49 ページ）
- アンチウイルス アラート （49 ページ）

- ディレクトリ獲得攻撃（DHAP）アラート （50 ページ）
- ハードウェア アラート （51 ページ）
- スパム隔離アラート （52 ページ）
- セーフリスト/ブロックリスト アラート （53 ページ）
- システム アラート （54 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 （69 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	メッセージと説明	パラメータ
AS.SERVER.ALERT	$engine anti-spam - $message $tb 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。	「**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。
AS.TOOL.INFO_ALERT	Update - $engine - $message 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。	「**engine**」：アンチスパム エンジンの名前 「**message**」：メッセージ。
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	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）。
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	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	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.	「**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パケット衝突数。
	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。	
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。	

アラート名	メッセージと説明	パラメータ
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	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。	
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 「**rcpt**」：受信者または「all」 「**reason**」：メッセージが削除されない理由
	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。	
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。	

アラート名	メッセージと説明	パラメータ
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 警告。メッセージの開放に失敗した場合に送信されます。	「**mid**」：MID 「**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 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。	「**mid**」：MID 「**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 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。	「**user**」：エンドユーザ名
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	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'. 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。	「**error**」：エラーの原因
SLBL.DB.SPACE_LIMIT	SLBL: End-User Safelist/Blocklist database exceeded allowed disk space: $current of $limit. 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。	「**current**」：データベース使用量（MB） 「**limit**」：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	Secure Endpoint の問題に関するアラートの確実な受信を参照してください	-
AMP.ENGINE.ALERT.WARN	アラートテキスト：ファイル分析グループ名を Cisco Threat Grid サーバーに登録できませんでした。Cisco TAC に連絡して、サポートを受けてください。 アラートレベル：警告（WARNING）。 説明：電子メールゲートウェイが、スマートアカウント ID を使用したアプライアンスグループ名を Cisco Secure Malware Analytics（Thread Grid）サーバーに登録できなかった場合、アラートが送信されます。	パラメータ：失敗の理由
AsyncOS API アラート	『AsyncOS API for Cisco Secure Email Gateway - 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。 メールボックスでのメッセージの修復	-
COMMON.APP_FAILURE	An application fault occurred: $error 警告。不明なアプリケーション障害が発生した場合に送信されます。	「**error**」：エラーのテキスト（通常はトレースバック）
COMMON.ENGINE_AUTO_UPDATE_ENABLED	<$level>: <$class> 情報：自動更新が特定のエンジン <$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。	'**$engine**'：サービス エンジンの名前。値は次のとおりです。 • Sophos • McAfee • グレイメール

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> 情報：自動更新が特定のエンジン <$engine> に対して無効になっています。特定のエンジンのグローバル設定ページで自動更新を有効にしない限り、このエンジンの自動更新を受け取ることはありません。	'**$engine**'：サービス エンジンの名前。値は次のとおりです。 • Sophos • McAfee • グレイメール
COMMON.KEY_EXPIRED_ALERT	Your "$feature" key has expired. Please contact your authorized Cisco sales representative. 警告。ライセンス キーの有効期限が切れた場合に送信されます。	「**feature**」：有効期限が切れる機能の名前。
COMMON.KEY_EXPIRING_ALERT	Your "$feature" key will expire in under $days day(s). Please contact your authorized Cisco sales representative. 警告。ライセンス キーの有効期限が切れる場合に送信されます。	「**feature**」：有効期限が切れる機能の名前。 「**days**」：有効期限が切れるまでの日数。
COMMON.KEY_FINAL_EXPIRING_ALERT	This is a final notice. Your "$feature" key will expire in under $days day(s). Please contact your authorized Cisco sales representative. 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。	「**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。
KEYS.GRACE_EXPIRING_ALERT	この電子メールゲートウェイのすべてのセキュリティ サービス ライセンスが期限切れになりました。The email gateway will continue to deliver mail without security services for $days days. To renew security services licenses, Please contact your authorized Cisco sales representative. クリティカル。仮想電子メールゲートウェイ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。	「**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、仮想電子メールゲートウェイのライセンスの有効期限 （10 ページ）を参照してください。

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	This is the final notice. All security services licenses for this email gateway have expired. The email gateway will continue to deliver mail without security services for 1 day. To renew security services licenses, Please contact your authorized Cisco sales representative. クリティカル。仮想電子メールゲートウェイライセンスの有効期限の1日前に送信されます。	猶予期間の詳細については、仮想電子メールゲートウェイのライセンスの有効期限 （10 ページ）を参照してください。
KEYS.GRACE_EXPIRED_ALERT	Your grace period has expired. All security sevice have expired, and your email gateway is non-functional. The email gateway will no longer deliver mail until a new license is applied. To renew security services licenses, Please contact your authorized Cisco sales representative. クリティカル。仮想電子メールゲートウェイの猶予期間を過ぎると送信されます。	猶予期間の詳細については、仮想電子メールゲートウェイのライセンスの有効期限 （10 ページ）を参照してください。
DNS.BOOTSTRAP_FAILED	Failed to bootstrap the DNS resolver. Unable to contact root servers. 警告。電子メールゲートウェイがルート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。	
COMMON.INVALID_FILTER	Invalid $class: $error 警告。無効なフィルタが存在する場合に送信されます。	「**class**」：「Filter」、「SimpleFilter」などのいずれか。 「**error**」：フィルタが無効な理由に関する追加の情報。

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_ALLOWED_LIST IPBLOCKD.HOST_ADDED_TO_BLOCKED_LIST IPBLOCKD.HOST_REMOVED_FROM_BLOCKED_LIST	The host at $ip has been added to the blocked list because of an SSH DOS attack. The host at $ip has been permanently added to the ssh allowed list. The host at $ip has been removed from the blocked list.	「**ip**」：ログインを試行したIPアドレス。
	警告。 SSHを介して電子メールゲートウェイ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のブロックリストに追加されます。 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アドレスは許可リストに追加されます。 許可リスト上のアドレスは、それらがブロックリストに含まれていてもアクセスが許可されます。 エントリは約1日後にブロックリストから自動的に削除されます。	
LDAP.GROUP_QUERY_FAILED_ALERT	LDAP: Failed group query $name, comparison in filter will evaluate as false	「**name**」：クエリーの名前。
	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。	
LDAP.HARD_ERROR	LDAP: work queue processing error in $name reason $why	「**name**」：クエリーの名前。 「**why**」：エラーが発生した理由。
	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。	
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	MID $mid matched the $rule_name rule. \n Details: $details	「**mid**」：メッセージの一意の識別番号。 「**rule_name**」：一致したルールの名前。 「**details**」：メッセージまたはルールに関する詳細情報。
	情報。Header Repeatsルールがtrueと評価されるたびに送信されます。	

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.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	Subject - '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.電子メールゲートウェイはメッセージの配信を再度試行するか、メッセージをバウンスします。	' 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%. 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。	「**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。
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. 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。	「**hostname**」：ホストの名前。

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	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%.	「**hostname**」：ホストの名前。 「**queue_threshold_start**」：キューのターピットを開始するパーセントしきい値。 「**queue_threshold_halt**」：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。
	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。	
MAIL.RES_CON_START_ ALERT. WORKQ	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.	「**hostname**」：ホストの名前。 「**suspend_threshold**」：リスナーが一時停止されるワーク キューの下限サイズ。 「**resume_threshold**」：リスナーが再開されるワーク キューの上限サイズ。
	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。	
MAIL.RES_CON_START_ ALERT	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources.	「**hostname**」：ホストの名前。
	クリティカル。電子メールゲートウェイが「リソース節約」モードになった場合に送信されます。	
MAIL.RES_CON_STOP_ALERT	This system (hostname: $hostname) has exited 'resource conservation' mode as resource utilization has dropped below the conservation threshold.	「**hostname**」：ホストの名前。
	情報。電子メールゲートウェイの「リソース節約」モードが解除された場合に送信されます。	

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.URL_REP_CLIENT.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.BEAKER_CONNECTOR.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.BEAKER_CONNECTOR.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。	「**num**」：ワーク キューに存在するメッセージ数。 「**reason**」：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。	「**num**」：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電子メールゲートウェイ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。	「**mid**」：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。	「**version**」：検出されたスキーマ バージョン。 「**target_version**」：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 $file_system partition. クリティカル。隔離用のディスク領域がフルになった場合に送信されます。	「**file_system**」：ファイルシステムの名前
QUARANTINE.THRESHOLD_ALERT	Quarantine "$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。	「**quarantine**」：隔離の名前。 「**full**」：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 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。	「**quarantine**」：隔離の名前。 「**full**」：隔離エリアの容量使用率。
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 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。	「**err_msg**」：発生したエラー メッセージ
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 $threshold percent, full processing of reporting data will be restarted automatically. 警告。システムのディスク領域が不足している場合に送信されます。ログ エントリに関するディスク使用率がログ使用率のしきい値を超過すると、reportd は集約をディセーブルにし、アラートを送信します。	「**threshold**」：しきい値
REPORTING.CLIENT.UPDATE_FAILED_ALERT	Reporting Client: The reporting system has not responded for an extended period of time ($duration). 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。	「**duration**」：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」）。
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。
SYSTEM.LOGIN_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
SYSTEM.RCPTVALIDATION.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_ALLOWED_LIST IPBLOCKD.HOST_ADDED_TO_BLOCKED_LIST IPBLOCKD.HOST_REMOVED_FROM_BLOCKED_LIST	The host at $ip has been added to the blocked list because of an SSH DOS attack. The host at $ip has been permanently added to the ssh allowed list. The host at $ip has been removed from the blocked list.	「**ip**」：ログインを試行したIPアドレス。
	警告。 SSHを介して電子メールゲートウェイへの接続を試みているが、有効なクレデンシャルを提示しないIPアドレスは、2分以内に11回以上試行に失敗した場合、SSHのブロックリストに追加されます。 同じIPアドレスからユーザが正常にログインすると、そのIPアドレスは許可リストに追加されます。 許可リスト上のアドレスは、それらがブロックリストに含まれていてもアクセスが許可されます。 エントリは約1日後にブロックリストから自動的に削除されます。	
WATCHDOG_RESTART_ALERT_MSG	<$level>: <$class>, <$hostname>: $subject $text 警告。 電子メールゲートウェイは、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。 • スパム対策 • ウイルス対策 • アンチ マルウェア防御 • グレイメール 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。	[「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 [「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

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'	警告。[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。 追加された国：<$added> 削除された国：<$deleted> 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。	'added'：次の国が追加されます。<iso_code1>:<country_name1>,<iso_code2>:<country_name2>, 'deleted'：次の国が削除されます。<iso_code1>:<country_name1>:<iso_code2>:<country_name2>,
MAIL.UPDATED_SHORT_URL_DOMAIN_LIST	情報（Info）。短縮URLドメインのリストが更新されています。 追加されたドメイン：<$added_domains> 削除されたドメイン：<$deleted_domains>	'added_domains'：次のドメインが追加されます。<domains_1>, <domain_2> 'deleted_domains'：次のドメインが削除されます。<domain_3>, <domain_4>
MAIL.DOMAINS_NOT_REACHABLE	警告。以下のドメインは短縮されたURLサポートの電子メールゲートウェイではアクセスできません。<$domains> 電子メールゲートウェイがこれらのドメインに接続できるようにするために、ファイアウォールのルールを確認します。	<$domains>：ドメインのカンマ区切りリスト。
MAIL.UPGRADE_CONFIG_CHANGE.ALERT	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。	**'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。
CERTIFICATE.CERT_EXPIRING_ALERT	証明書「$certificate」は $days 日後に期限切れになります。 アラートレベル：警告（WARNING）	「**certificate**」：期限が近づいている証明書の名前。 「**days**」：有効期限が切れるまでの日数。
CERTIFICATE.CERT_CRITICAL_EXPIRING_ALERT	証明書「$certificate」は $days 時間後に期限切れになります。 アラートレベル：クリティカル（CRITICAL） 「クリティカル」証明書の有効期間は、5日未満です。	「**certificate**」：期限が近づいている証明書の名前。 「**days**」：日数と残り時間（HH：MM：SS）。たとえば、4日 10:12:20 時間（4 days 10:12:20 hour(s)）です。

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
CERTIFICATE.CERT_EXPIRED_ALER	証明書「$certificate」の有効期限が切れています。 アラートレベル：クリティカル（CRITICAL）	「**certificate**」：期限が切れている証明書の名前。
CERTIFICATE.UPDATER_ CERT_EXPIRING_ALERT	証明書「$certificate」は $days 日後に期限切れになります。アップデータの信頼できる証明書リストから未使用の証明書を削除するには、CLI で `updateconfig -> trusted_certificates -> delete` サブコマンドを使用します。 アラートレベル：警告（WARNING）	「**certificate**」：期限が近づいている証明書の名前。 「**days**」：有効期限が切れるまでの日数。
CERTIFICATE.UPDATER_CERT_ CRITICAL_EXPIRING_ALERT	証明書「$certificate」は $days 時間後に期限切れになります。アップデータの信頼できる証明書リストから未使用の証明書を削除するには、CLI で `updateconfig -> trusted_certificates -> delete` サブコマンドを使用します。 アラートレベル：クリティカル（CRITICAL）	「**certificate**」：期限が近づいている証明書の名前。 「**days**」：有効期限が切れるまでの日数。
MAIL.APP.NO_ACCESS_KEY	アラートテキスト：「Cisco Advanced Phishing Protection クラウドサービスの有効期限のポーリングに失敗しました。API AccessUID と API アクセス秘密鍵を追加してください。（Failed to poll for the Cisco Advanced Phishing Protection Cloud Service expiry date, add API AccessUID and API Access secret key.）」 説明：API アクセスキーと秘密鍵が入力されなかったため、APP の有効期限についてのクエリに失敗して、アラートが送信されました。	該当なし

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.APP.INVALID_KEY	アラートテキスト：APIアクセスキーが無効なため、Cisco Advanced Phishing Protection クラウドサービスの有効期限についてのポーリングに失敗しました。（Failed to poll for the Cisco Advanced Phishing Protection Cloud Service expiry date because the API Access Key is invalid.）APIアクセスUIDと秘密鍵を再設定する必要があります。（You need to re-configure the API Access UID and secret key.） 説明：APIアクセスキーと秘密鍵が入力されなかったため、APPの有効期限についてのクエリに失敗して、アラートが送信されました。	該当なし
MAIL.APP.EXPIRED	アラートテキスト：Cisco Advanced Phishing Protection クラウドサービスの有効期限が切れ、無効になっています。（The Cisco Advanced Phishing Protection Cloud Service has expired and is disabled.）シスコアカウントマネージャに連絡して、サービスを更新および有効化してください。（Contact your Cisco Account Manager to renew the service and enable it.） 説明：Cisco Advanced Phishing Protection クラウドサービスの有効期限が切れて無効になっています。APPライセンスを更新して、APPサービスを有効にする必要があります。	該当なし
MAIL.APP.EXPIRY_REMINDER	アラートテキスト：Cisco Advanced Phishing Protection クラウドサービスは $eaas_expiry_date に期限切れになります。（Cisco Advanced Phishing Protection Cloud Service expires on $eaas_expiry_date.）シスコアカウントマネージャに連絡して、サービスを更新してください。（You need to contact your Cisco Account Manager to renew the service.） 説明：有効期限の3日前からアラートが毎日送信されます。	パラメータ：eaas_expiry_date eaas_expiry_date（Cisco Advanced Phishing Protection クラウドサービスの有効期限）

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.APP.SERVICE_ UNAVAILABLE	アラートテキスト：Cisco Advanced Phishing Protection クラウドサービスの更新。（Cisco Advanced Phishing Protection Cloud Service update.）クラウドサービスとの通信を確立できません。（Unable to establish communication with the cloud service.） 説明：10 回連続してメールを APP に転送できなかったため、APP クラウドサービスを利用できません。	該当なし
MAIL.APP.SERVICE_ AVAILABLE	アラートテキスト：Cisco Advanced Phishing Protection クラウドサービスの更新。（Cisco Advanced Phishing Protection Cloud Service update.）クラウドサービスとの通信が確立されました。（Communication with the cloud service has been established.） 説明：APP クラウドサービスは利用可能です。	該当なし

アップデータ 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タ 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タ アラートのリスト

アラート名	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	「**app**」：アプリケーション名。 「**attempts**」：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. MANIFEST_FAILED_ALERT	The updater has been unable to communicate with the update server for at least $threshold.	「**threshold**」：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。	

アラート名	メッセージと説明	パラメータ
UPDATER.UPDATERD. RELEASE_NOTIFICATION	$mail_text 警告。リリースの通知です。	「**mail_text**」：通知するテキスト。 「**notification_subject**」：通知するテキスト。
UPDATER.UPDATERD. UPDATE_FAILED	Unknown error occured: $traceback クリティカル。アップデートの実行に失敗しました。	「**traceback**」：トレースバック。

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	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. 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。	「**text**」：アップデート アラートのテキスト。 「**time**」：最終アップデートの時刻。 「**date**」：最終アップデートの日付。
AS.UPDATE_FAILURE	$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 email gateway for this failure is: $error 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。	「**engine**」：アップデートに失敗したエンジン。 「**error**」：発生したエラー。

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	メッセージと説明	パラメータ
CLUSTER.CC_ERROR. AUTH_ERROR	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Machine does not appear to be in the cluster 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でない場合に起きる可能性があります。	「**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）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR.DROPPED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Existing connection dropped 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。	「**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）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR.FAILED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Connection failure 警告。クラスタへの接続に失敗した場合に送信されます。	「**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）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR. FORWARD_FAILED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Message forward failed, no upstream connection クリティカル。電子メールゲートウェイ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。	「**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）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR.NOROUTE	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=No route found 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。	「**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）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR.SSH_KEY	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Invalid host key 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。	「**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）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR.TIMEOUT	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Operation timed out 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。	「**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）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP	Error connecting to cluster machine $name - $error - $why クリティカル。電子メールゲートウェイ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。	「**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）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.AUTH_ERROR	Error connecting to cluster machine $name - $error - whyerror:=Machine does not appear to be in the cluster 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。	「**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）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.DROPPED	Error connecting to cluster machine $name - $error - whyerror:=Existing connection dropped 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。	「**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）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.FAILED	Error connecting to cluster machine $name - $error - whyerror:=Connection failure 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。	「**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）。 「**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 - whyerror:=Message forward failed, no upstream connection 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、電子メールゲートウェイ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。	「**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）。 「**why**」：エラーに関する詳細なテキスト。

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR_NOIP.NOROUTE	Error connecting to cluster machine $name - $error - whyerror:=No route found 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。	「**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）。 「**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 - whyerror:=Invalid host key 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。	「**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）。 「**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 - whyerror:=Operation timed out 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。	「**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）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.SYNC.PUSH_ALERT	Overwriting $sections on machine $name 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。	「**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）。 「**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、電子メールゲートウェイ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、 電子メールゲートウェイの 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	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

電子メールゲートウェイ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）内のエントリと一致する 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 x 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電子メールゲートウェイがメールを送信するのを防止します。

DNS アラート

電子メールゲートウェイの再起動時に、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 Secure Email Gateway』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 ユーザー 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 （73 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。

電子メールゲートウェイはインターネット 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。

（注） 接続先が単一の IP アドレスではなくサブネットである場合は、エントリがCIDR（クラスレスドメイン間ルーティング）表記（192.168.90.0/24 など）に準拠していることを確認します。

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、電子メールゲートウェイの 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。

重要

下位の AsyncOS バージョン（14.0 や 14.3 など）からアップグレードした場合、デフォルトの SSL 暗号は AsyncOS 15.x 以降で次のように変更されます。

- **GUI HTTPS の場合**：

```
AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:
!aNULL:!kRSA:@STRENGTH:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:
!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM
```

- **インバウンド SMTP の場合**：

```
AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:
!aNULL:!kRSA:@STRENGTH:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:
!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM
```

- **アウトバウンド SMTP の場合**：

```
ECDH+aRSA:ECDH+ECDSA:DHE+DSS+AES:AES128:AES256:
!3DES:!IDEA:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL:!eNULL:
!kRSA:@STRENGTH:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:
!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM:
!ECDHE-ECDSA-CAMELLIA128-SHA256:!ECDHE-RSA-CAMELLIA128-SHA256:
!ECDHE-ECDSA-CAMELLIA256-SHA384:!ECDHE-RSA-CAMELLIA256-SHA384:
!ECDHE-ECDSA-AES128-CCM:!ECDHE-ECDSA-AES256-CCM
```

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。
- その他の TLS クライアントサービスを設定します。電子メールゲートウェイが非 FIPS モードの場合、[その他のTLSクライアントサービス（Other TLS Client Services）] では、TLS v1.0 方式がデフォルトで無効になります。「LDAP」および「Updater」の TLS クライアントサービスに対しては、電子メールゲートウェイで TLS v1.0 方式を有効にできます。

次の点を考慮してください。

- （非 FIPS モードの場合）TLS v1.0 方式と v1.1 方式を同時には有効にできません。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。
- 非 FIPS モードで TLS v1.0 が有効になっている下位の AsyncOS バージョン（例：12.x または 13.0）から AsyncOS 13.5.1 以降にアップグレードすると、TLS v1.0 がデフォルトで無効になります。アップグレード後に電子メールゲートウェイで TLS v1.0 方式を有効にする必要があります。
- AsyncOS 13.5.1 以降では、SSLv2 および SSLv3 方式はサポートされません。
- 電子メールゲートウェイが FIPS モードの場合、TLS v1.0 方式はサポートされません。

- 電子メールゲートウェイが非 FIPS モードの場合、TLS v1.0 方式はデフォルトで無効になります。
- 「GUI HTTPS」、「インバウンド SMTP」、および「アウトバウンド SMTP」の TLS サービスに TLS 1.3 を設定する場合、電子メールゲートウェイは次の TLS 暗号のみをサポートします。
  - `TLS_AES_128_GCM_SHA256`
  - `TLS_AES_256_GCM_SHA384`
  - `TLS_CHACHA20_POLY1305_SHA256`

（注）
電子メールゲートウェイでは、TLS 1.3 に使用される暗号を変更できません。

TLS 1.3 を設定すると、電子メールゲートウェイと API サービスのレガシーまたは新しい Web インターフェイス全体で TLS 通信に使用できます。

ステップ 4 （オプション）[TLSを介したアラート（Alerts over TLS）]、[アウトバウンドSMTP（Outbound SMTP）]、[アップデータ（Updater）]、および [LDAP] サーバサービスについて、電子メールゲートウェイがピア証明書でFQDN検証を実行できるようにするには、[有効にする（Enable）] チェックボックスをオンにします。

ステップ 5 （オプション）[TLSを介したアラート（Alerts over TLS）]、[アウトバウンドSMTP（Outbound SMTP）]、[アップデータ（Updater）]、および [LDAP] サーバサービスについて、電子メールゲートウェイがピア証明書でX.509検証を実行できるようにするには、[有効にする（Enable）] チェックボックスをオンにします。

ステップ 6 **[送信（Submit）]** をクリックします。

ステップ 7 [変更を確定（Commit Changes）] をクリックします。

SAML 2.0 を使用したシングル サインオン（SSO）

- シングル サインオン（SSO）と SAML 2.0 について （79 ページ）
- SAML 2.0 SSO のワークフロー （80 ページ）
- SAML 2.0 に関する注意事項と制約事項 （80 ページ）
- 電子メールゲートウェイでの SSO の設定方法 （81 ページ）

シングル サインオン（SSO）と SAML 2.0 について

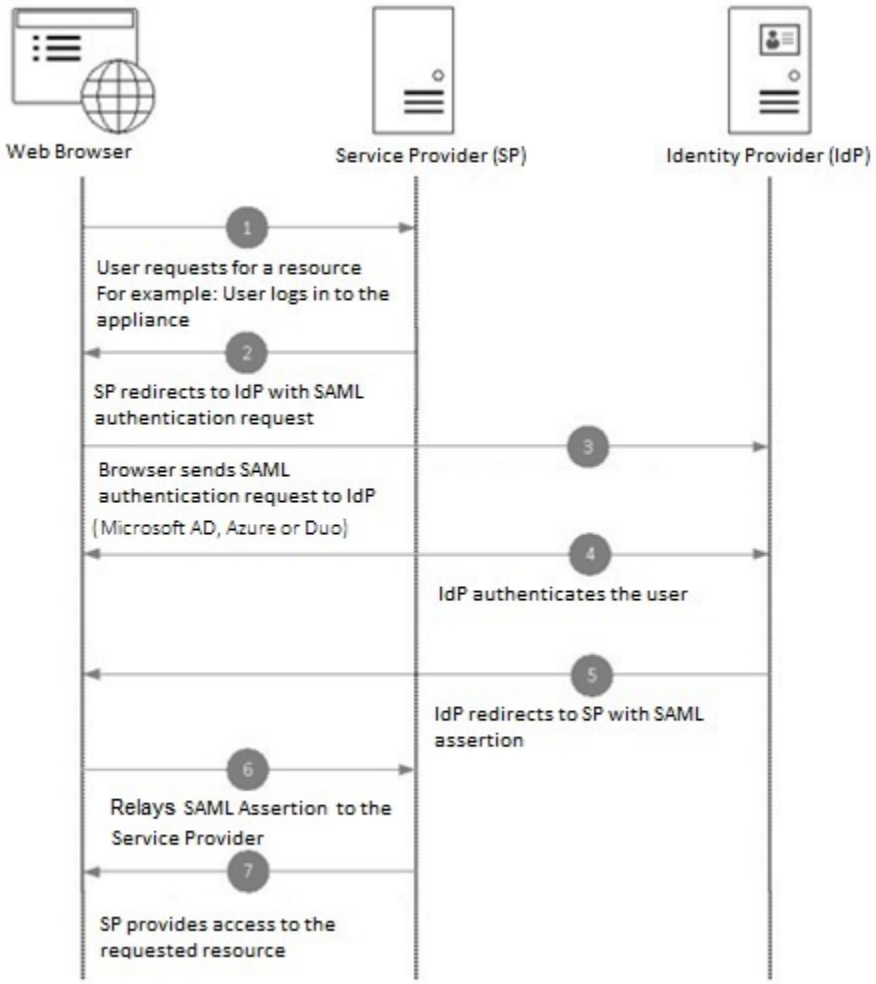
電子メールゲートウェイは SAML 2.0 SSO をサポートするようになりました。これにより、管理ユーザは組織内で他の SAML 2.0 SSO 対応サービスへのアクセスに使用している同じクレデンシャルで電子メールゲートウェイの Web インターフェイスにログインできます。たとえば、SAML ID プロバイダー（IdP）として Duo、Microsoft AD FS、または Azure を有効にした場合、

SAML 2.0 SSO をサポートするサービスプロバイダー（SP）として電子メールゲートウェイを設定できます。ユーザは一度サインインすれば、すべての SAML 2.0 SSO 対応サービスにアクセスできます。

SAML 2.0 SSO のワークフロー

SAML 2.0 SSO ワークフローを、次の図に表示します。

図 *3 : SAML* のワークフロー



SAML 2.0 に関する注意事項と制約事項

- 一般 （81 ページ）
- ログアウト （81 ページ）

- 制限事項 （81 ページ）

一般

SAML によるシングルサインオンは、グラフィカル ユーザー インターフェイス（GUI）でのみ使用できます。SAML プロファイルの設定には、GUI とコマンド ライン インターフェイス（CLI）を使用できます。

電子メールゲートウェイでは、サービスプロバイダーと ID プロバイダーのインスタンスを 1 つのみ設定できます。

ログアウト

ユーザは電子メールゲートウェイからログアウトしても、他の SAML 2.0 SSO 対応アプリケーションからログアウトされることはありません。

制限事項

クラスタ レベルで SAML プロファイルを設定することはできません。すべての SAML 設定は、マシン レベルに制限されます。

電子メールゲートウェイでの SSO の設定方法

手順

	コマンドまたはアクション	目的
ステップ 1	前提条件を確認します。	前提条件 （81 ページ）
ステップ 2	電子メールゲートウェイをサービスプロバイダーとして設定します。	電子メールゲートウェイをサービスプロバイダーとして設定する （83 ページ）
ステップ 3	（IDP で） 電子メールゲートウェイを操作するように ID プロバイダーを設定します。	電子メールゲートウェイと通信するように ID プロバイダーを設定する （85 ページ）
ステップ 4	電子メールゲートウェイで ID プロバイダーを設定します。	電子メールゲートウェイでの ID プロバイダーの設定 （89 ページ）
ステップ 5	電子メールゲートウェイで SAML を使用した外部認証を有効にします。	SAML 認証の有効化

前提条件

- サポートされるアイデンティティ プロバイダー （82 ページ）
- セキュアな通信の証明書 （82 ページ）

サポートされるアイデンティティ プロバイダー

組織で使用する ID プロバイダーが 電子メールゲートウェイでサポートされているかどうかを確認します。事前認定済みの ID プロバイダーは次のとおりです。

- Microsoft Active Directory Federation Services（AD FS）2.0 以降
- Duo Access Gateway
- Azure AD

（注） 任意の標準 SAML 2.0 ID プロバイダーを使用して、E メールゲートウェイで SAML を使用して SSO を設定できます。

セキュアな通信の証明書

電子メールゲートウェイと ID プロバイダーの間の通信をセキュリティで保護するために必要な次の証明書を取得します。

- 電子メールゲートウェイで SAML 認証要求に署名する、または ID プロバイダーで SAML アサーションを暗号化する場合、自己署名証明書または信頼できる CA の証明書、および関連付けられている秘密キーを取得します。
- ID プロバイダーで SAML アサーションに署名する場合は、ID プロバイダーの証明書を取得して 電子メールゲートウェイにインポートします。 電子メールゲートウェイはこの証明書を使用して、署名済み SAML アサーションを確認します。

証明書の変換

電子メールゲートウェイから証明書を作成およびエクスポートするには、証明書の使用を参照してください。通常、 電子メールゲートウェイから取得した証明書は .pfx 形式であり、 電子メールゲートウェイをサービスプロバイダーとして設定するときには .pem 形式に変換する必要があります。

証明書を .pfx 形式から .pem 形式に変換するには、次の操作を行います。

- OpenSSL ツールをダウンロードしてインストールし、 電子メールゲートウェイから取得した証明書ファイル（.pfx）をインポートします。
- 次のコマンドを実行して、証明書を .pem 形式でエクスポートします。`openssl pkcs12 -in <certname>.pfx -nokeys -out cert.pem`
- 次のコマンドを実行して、秘密キーを .pem 形式でエクスポートします。`openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes`
- 次のコマンドを実行して、秘密キーからパスフレーズを削除します。`openssl rsa -in key.pem -out server.key`

電子メールゲートウェイをサービスプロバイダーとして設定する

（注） ID プロバイダーでのサービスプロバイダーの設定値は、 電子メールゲートウェイでのサービスプロバイダー設定に基づいて設定されます。

始める前に

前提条件 （81 ページ）を確認してください。

手順

ステップ 1 Web インターフェイスを使用して 電子メールゲートウェイにログインします。

ステップ 2 [システム管理（System Administration）] > [SAML] に移動します。

ステップ 3 [サービスプロバイダーの追加（Add Service Provider）] をクリックします。

ステップ 4 次の詳細を入力します。

フィールド	説明
プロファイル名（Profile Name）	サービス プロバイダー プロファイルの名前を入力します。
コンフィギュレーション設定	
エンティティ ID	サービスプロバイダー（この場合、ご使用の電子メールゲートウェイ）のグローバルな固有の名前を入力します。通常、サービス プロバイダー エンティティ ID の形式は URI です。
名前 ID の形式	ID プロバイダーが SAML アサーションでユーザを指定するのに使用する形式。 このフィールドは設定できません。IDプロバイダーでサービスプロバイダーを設定するときに、この値が必要になります。
アサーション コンシューマ URL	認証が正常に完了した後で、ID プロバイダーが SAML アサーションを送信する URL を入力します。 アサーションコンシューマ URL は、 電子メールゲートウェイへのアクセスに使用される URL です。ID プロバイダーでサービス プロバイダーを設定するときに、この値が必要になります。

フィールド	説明
SP 証明書	サービスプロバイダーの証明書は、次のいずれかの方法でインポートできます。 • 電子メールゲートウェイで使用可能な署名付き証明書をドロップダウンリストから選択します。 • 証明書をインポートして秘密キーと関連付けます。証明書は（.cert）形式にし、秘密キーは（.key）形式にする必要があります。 • PKCS #12 ファイル形式で証明書をインポートします。PKCS # 12 形式の証明書ではパスワードが必須です。 （オプション）認証要求の署名（Signing Authentication Requests） アプライアンスで SAML 認証要求に署名する場合、 1. 電子メールゲートウェイから取得された証明書と、関連付けられている秘密キーをアップロードします。 証明書は**.cert**形式でアップロードする必要があります。詳細については、セキュアな通信の証明書 （82 ページ）を参照してください。 2. 秘密キーのパスフレーズを入力します。 3. [署名要求（Sign Requests）] を選択します。 （オプション）**暗号化されたアサーションの復号（Decrypt Encrypted Assertions）** SAML アサーションを暗号化するように ID プロバイダーを設定する場合、 1. 電子メールゲートウェイから取得された証明書と、関連付けられている秘密キーをアップロードします。 2. 秘密キーのパスフレーズを入力します。 **（注）** 秘密キーは **.key** 形式である必要があります。証明書の使用方法については、セキュアな通信の証明書 （82 ページ） を参照してください。

フィールド	説明
署名アサーション	SAML アサーションに署名するように ID プロバイダーを設定する場合、[署名アサーション（Sign Assertions）] を選択します。 このオプションを選択すると、 電子メールゲートウェイに ID プロバイダーの証明書を追加する必要があります。 電子メールゲートウェイでの ID プロバイダーの設定 （89 ページ）を参照してください。
組織詳細	組織の詳細を入力します。ID プロバイダーは、エラー ログでこの情報を使用します。
技術的な問い合わせ先	技術的な問い合わせ先の電子メール アドレスを入力します。ID プロバイダーは、エラー ログでこの情報を使用します。

ステップ 5 [送信（Submit）] をクリックし、変更をコミットします。

ステップ 6 [SSOの設定（SSO Settings）] ページに表示されるサービス プロバイダーのメタデータ（エンティティ ID とアサーション顧客 URL）と、[サービスプロバイダー設定（Service Provider Settings）] ページに表示される名前 ID の形式を書き留めます。ID プロバイダーでサービス プロバイダーを設定するときに、これらの詳細が必要になります。

必要に応じて、メタデータをファイルとしてエクスポートできます。設定が完了したら、[メタデータのエクスポート（Export Metadata）] をクリックしてメタデータ ファイルを保存します。一部の ID プロバイダーでは、メタデータ ファイルからサービス プロバイダーの詳細をロードできます。

次のタスク

電子メールゲートウェイと通信するように ID プロバイダーを設定します。 電子メールゲートウェイと通信するように ID プロバイダーを設定する （85 ページ） を参照してください。

電子メールゲートウェイと通信するように ID プロバイダーを設定する

始める前に

次の内容について確認してください。

- 電子メールゲートウェイをサービスプロバイダーとして設定します。 電子メールゲートウェイをサービスプロバイダーとして設定する （83 ページ）を参照してください。
- サービスプロバイダーのメタデータの詳細がコピーされているか、またはメタデータ ファイルがエクスポートされている。 電子メールゲートウェイをサービスプロバイダーとして設定する （83 ページ）を参照してください。

手順

ステップ 1 ID プロバイダーで、次のいずれかを実行します。

- サービスプロバイダー（お使いの電子メールゲートウェイ）の詳細を手動で構成します。
- ID プロバイダーがメタデータ ファイルからサービス プロバイダーの詳細をロードすることを許可している場合は、メタデータ ファイルをインポートします。

電子メールゲートウェイが SAML 認証要求に署名するように構成済みの場合、または SAML アサーションを暗号化する予定の場合は、必ず関連する証明書を ID プロバイダーに追加します。

ID プロバイダー固有の手順については、以下を参照してください。

- 電子メールゲートウェイと通信するように AD FS を設定する （86 ページ）。
- 電子メールゲートウェイと通信するように Duo Access Gateway を設定する （87 ページ）。
- 電子メールゲートウェイと通信するように Azure AD を設定する （88 ページ）。

ステップ 2 ID プロバイダーのメタデータを書き留めるかまたはメタデータをファイルとしてエクスポートします。

次のタスク

電子メールゲートウェイ上で ID プロバイダーの設定を構成します。 電子メールゲートウェイでの ID プロバイダーの設定 （89 ページ） を参照してください。

電子メールゲートウェイと通信するように AD FS を設定する

以下は、お使いの 電子メールゲートウェイと通信するように AD FS（2.0 以降）を設定するために実行する必要があるタスクの概要です。完全かつ詳細な手順については、Microsoft のマニュアルを参照してください。

- リレーパーティとしてサービスプロバイダー（電子メールゲートウェイ）のアサーションコンシューマ URL を追加します。
- [リレーパーティトラスト（Relaying Party Trusts）] > [プロパティ（Properties）] > [ID（Identifiers）] > [リレーパーティID（Relaying Party Identifier）] で、サービスプロバイダー（電子メールゲートウェイ）のエンティティ ID を入力します。この値が、電子メールゲートウェイのサービスプロバイダー設定のエンティティ ID 値と同じかどうかを確認します。
- 署名入りの SAML 認証要求を送信するようにサービス プロバイダー（アプライアンス）を構成済みの場合は、サービス プロバイダーの証明書（認証要求を署名するために使用される）を [リレー パーティ トラスト（Relaying Party Trusts）] > [プロパティ（Properties）] > [署名（Signature）] の下で .cer 形式でアップロードします。

- 暗号化された SAML アサーションを送信するように AD FS を構成する場合は、サービスプロバイダー（電子メールゲートウェイ）の証明書を[リレーパーティトラスト（Relaying Party Trusts）]>[プロパティ（Properties）]>[暗号化（Encryption）]の下で .cer 形式でアップロードします。
- [リレー パーティ トラスト（Relaying Party Trusts）]>[プロパティ（Properties）]>[詳細（Advanced）]の下で、セキュアハッシュ アルゴリズムを SHA-1 に設定します。
- 応答に SPNameQualifier を含めるためのカスタム ルールを追加します。次のファイルは、サンプルのカスタム ルールです。

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>

issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
 Issuer=
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
 =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
 =
"urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified");
```

- 要求ルールを編集し、電子メール アドレスの LDAP 属性を発信要求タイプ（電子メールアドレス）として送信する発行変換規則を追加します。また、発行変換規則を追加して、グループ属性の LDAP 属性を送信要求タイプ（未指定のグループ）として送信するようにします。

電子メールゲートウェイと通信するように Duo Access Gateway を設定する

以下は、お使いの 電子メールゲートウェイと通信するように Duo Access Gateway を設定するために実行する必要があるタスクの概要です。完全かつ詳細な手順については、Duo Security のマニュアルを参照してください。

- SAMLアサーションを受信および処理するサービスプロバイダーエンドポイントとして、サービスプロバイダーの（ 電子メールゲートウェイの）アサーションコンシューマ URL を追加します。
- [Duo管理パネル（Duo Admin Panel）]>[アプリケーション（Applications）]>[アプリケーションの保護（Protect an Application）]>[SAMLサービスプロバイダー（SAML Service Provider）]で、サービスプロバイダー（ 電子メールゲートウェイ）のエンティティ ID を入力します。この値が、電子メールゲートウェイのサービスプロバイダー設定のエンティティ ID 値と同じかどうかを確認します。
- 署名入りの SAML 認証要求を送信するようにサービスプロバイダー（ 電子メールゲートウェイ）を構成済みの場合は、Duo Access Gateway に認証ソースを設定する際に、サービスプロバイダーの証明書（認証要求を署名するために使用される）を .cer 形式でアップロードします。
- 暗号化された SAML アサーションを送信するように Duo を構成する計画の場合は、Duo Access Gateway に認証ソースを設定する際に、サービスプロバイダーの（電子メールゲートウェイの）証明書を .cer 形式でアップロードします。

- [Duo管理パネル（Duo Admin Panel）] > [アプリケーション（Applications）] > [アプリケーションの保護（Protect an Application）] > [SAMLサービスプロバイダー（SAML Service Provider）] で、NameID 形式として [未指定（unspecified）] を選択します。
- [Duo管理パネル（Duo Admin Panel）] > [アプリケーション（Applications）] > [アプリケーションの保護（Protect an Application）] > [SAMLサービスプロバイダー（SAML Service Provider）] で、セキュア ハッシュ アルゴリズムを SHA-256 に設定します。
- [Duo管理パネル（Duo Admin Panel）] で [SAML-サービスプロバイダー設定（SAML - Service Provider Setting）] を設定ファイルとして保存し、Duo Access Gateway でその設定ファイルを SAML アプリケーションとしてインポートします。

電子メールゲートウェイと通信するように Azure AD を設定する

以下は、お使いの 電子メールゲートウェイと通信するように Azure AD を実行する必要があるタスクの概要です。完全かつ詳細な手順については、Microsoft Azure AD のマニュアルを参照してください。

- SAML アサーションを受信および処理するサービスプロバイダー識別子として、サービスプロバイダーの（ 電子メールゲートウェイの）アサーションコンシューマ URL を追加します。
- [エンタープライズアプリケーション（Enterprise Application）] > [新しいアプリケーション（New Application）] > [ギャラリー以外のアプリケーション（Non-gallery application）] > [シングルサインオン（Single Sign-On）] > [基本SAML設定（Basic SAML Configuration）] にある Azure ポータルにサービスプロバイダーの（電子メールゲートウェイの）エンティティ ID を入力します。この値が、 電子メールゲートウェイのサービスプロバイダー設定のエンティティ ID 値と同じかどうかを確認します。
- 署名入りの SAML 認証要求を送信するようにサービスプロバイダー（ 電子メールゲートウェイ）を構成済みの場合は、[SAML署名証明書（SAML Signing Certificate section）] セクション（[エンタープライズアプリケーション（Enterprise Application）] > [新しいアプリケーション（New Application）] > [ギャラリー以外のアプリケーション（Non-gallery application）] > [シングルサインオン（Single Sign-On）] > [SAML署名証明書（SAML Signing Certificate）]）で、サービスプロバイダーの証明書（認証要求を署名するために使用される）をアップロードします。
- [ユーザ属性とクレーム（User Attributes and Claims）] セクション（[エンタープライズアプリケーション（Enterprise Application）] > [新しいアプリケーション（New Application）] > [ギャラリー以外のアプリケーション（Non-gallery application）] > [シングルサインオン（Single Sign-On）] > [ユーザ属性とクレーム（User Attributes and Claims）]）でグループクレームを設定し、グループ属性を追加します。
- [SAML] > [ユーザとグループ（Users & Groups）] のために作成された Azure アプリケーションでユーザまたはグループを追加して、この Azure SAML アプリケーションにログインできるユーザを制御します。

電子メールゲートウェイでの ID プロバイダーの設定

始める前に

次の内容について確認してください。

- 電子メールゲートウェイとの通信のための ID プロバイダーが構成されている。 電子メールゲートウェイと通信するように ID プロバイダーを設定する （85 ページ）を参照してください。
- ID プロバイダーのメタデータの詳細がコピーされている、または ID プロバイダーのメタデータがファイルとしてエクスポートされている。

手順

ステップ 1 Web インターフェイスで 電子メールゲートウェイにログインします。

ステップ 2 [システム管理（System Administration）] > [SAML] に移動します。

ステップ 3 [IDプロバイダーの追加（Add Identity Provider）] をクリックします

ステップ 4 次の詳細を入力します。

フィールド	説明
プロファイル名（Profile Name）	ID プロバイダー プロファイルの名前を入力します。
構成設定（ID プロバイダー設定の手動構成）	
エンティティ ID	ID プロバイダーのグローバルに一意の名前を入力します。通常、ID プロバイダーエンティティ ID の形式は URI です。
SSO URL	サービス プロバイダーが SAML 認証要求を送信する必要がある URL を指定します。
証明書	ID プロバイダーが SAML アサーションに署名する場合、ID プロバイダーの署名証明書をアップロードする必要があります。
構成設定（ID プロバイダー メタデータのインポート）	
IDP メタデータのインポート	[メタデータのインポート（Import Metadata）] をクリックして、メタデータ ファイルを選択します。

ステップ 5 変更を送信し、保存します。

次のタスク

SAML 認証の有効化。

AsyncOS API 向けの電子メールゲートウェイでの OpenID Connect 1.0 の設定

- 概要 （90 ページ）
- ワークフロー （90 ページ）
- サンプルアクセストークン （91 ページ）
- 前提条件 （91 ページ）
- 電子メールゲートウェイでの OpenID Connect の設定 （92 ページ）

概要

Cisco Secure Email Gateway は、OpenID Connect 1.0 認証で ID プロバイダー（IDP）を使用するアプリケーションまたはクライアントとの統合をサポートし、電子メールゲートウェイで使用可能な AsyncOS API とシームレスに接続します。現在、お使いの E メールゲートウェイは、Microsoft AD FS のみを使用して OpenID Connectで認定されています。

ワークフロー

次のワークフローでは、AD FS を ID プロバイダー、外部アプリケーションをクライアント、電子メールゲートウェイをリソースプロバイダーとして使用しています。

手順：

1. （1 回限りのアクティビティ）アクセストークンを検証するように電子メールゲートウェイを設定します。詳細については、電子メールゲートウェイでの OpenID Connect の設定（92 ページ）を参照してください。
2. （1 回限りのアクティビティ）電子メールゲートウェイは、OpenID Connect の設定メタデータと必要なキーを取得して、ステップ 1 で行った設定に基づいてアクセストークンを検証します。
3. AD FS で外部アプリケーションを認証した後、アクセストークンを取得します。アクセストークンを認証および受信する方法の詳細については、認証プロバイダーまたは ID プロバイダーのマニュアルを参照してください。
4. API 要求をアクセストークンとともに電子メールゲートウェイに送信します。
5. 電子メールゲートウェイは、ステップ 2 で取得したキーセットを使用して API 要求のアクセストークンを検証します。

6. 電子メールゲートウェイは、アクセストークン内の必要な要求（発行者、対象者）を検証します。
7. 電子メールゲートウェイは、ロール要求値を使用して、AsyncOS API にアクセスするためのユーザロール権限を許可し、割り当てます。
8. 電子メールゲートウェイは、AsyncOS API 要求に適切な応答を提供します。

サンプルアクセストークン

次に、サンプルアクセストークンの形式を示します。

```
Header
alg:RSA256
typ:JWT
[...]
Payload
claim: aud: CiscoEmailAPICaller
claim: iss: http://adfsserver/adfs/services/trust
claim: iat: 1594712147
claim: exp: 1594712807
claim: CustomOrgIdentifier: MyCustomOrgId
claim: LastName: Fernandes
claim: FirstName: Erik
claim: Email: erik.fernandes@customorg.com
claim: Role: LogCollector
claim: Role: ReadOnly
[...]
```

電子メールゲートウェイは、次のアルゴリズムによってのみ署名されたアクセストークンの検証をサポートします。

- RSA256
- RSA384
- RSA512

前提条件

OpenID Connect で電子メールゲートウェイを設定する前に、次の前提条件を満たしていることを確認します。

- 組織で使用される認証プロバイダーは電子メールゲートウェイでサポートされている。
- アプリケーションは認証プロバイダーで認証し、アクセストークンを取得できる。
- 電子メールゲートウェイは、HTTP 経由で認証プロバイダーに接続して、OpenID Connect メタデータ設定を取得できる。

電子メールゲートウェイでの OpenID Connect の設定

始める前に

次の情報について確認してください。

- （認証プロバイダーの設定に基づいて）認証プロバイダーによって発行された有効なアクセストークン。
- アクセストークンには、電子メールゲートウェイが必要な許可チェックを実行できるようにするためのロール情報が含まれている必要があります。

手順

ステップ 1 [システム管理（System Administration）] > [OpenID Connect] 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 以下の表に記載される必須パラメータを入力して、OpenID Connect を設定します。

OpenID Connect パラメータ	説明
[IDプロバイダーのメタデータのURL（Identity Provider Metadata URL）]	Open ID Connect の設定メタデータを取得するために使用する ID プロバイダーの URL を入力します。メタデータは、アクセストークンの検証に使用されます。 ID プロバイダーの URL は、https://example.com/adfs/.well-known/openid-configuration のようになります。
発行元（Issuer）	アクセストークンの発行者の値を入力します。 （注） この値は、アクセストークンの検証時にアクセストークンの発行者要求値と一致する必要があります。 発行者は http://example.com/adfs/services/trust のようになります。
対象読者	アクセストークンの対象者要求値と一致する必要がある対象者の値を入力します。 （注） 複数の対象者値を追加する場合は、[行を追加（Add Row）] をクリックします。

OpenID Connect パラメータ	説明
[要求名（Claim Name）]	ユーザロール情報を含むアクセストークンの要求の名前を入力します。要求名は、アクセストークンからロール情報を取得するために使用されます。
ID プロバイダーとアプライアンスロールのマッピング	ID プロバイダーサーバで定義されたユーザグループロールを入力し、電子メールゲートウェイで設定された対応するローカルユーザロールを選択して、両方のロールをマッピングします。 （注） 複数のロールマッピングレコードを追加する場合は、[行を追加（Add Row）] をクリックします。

ステップ 4 変更を送信し、保存します。

次のタスク

AsyncOS API コールの Authorization Bearer ヘッダーにアクセストークンを含め、API 要求を送信します。

次に、API の Authorization Bearer ヘッダーにアクセストークンを含めた AsyncOS API を呼び出す例を示します。

```
curl --location --request
GET 'https://esa.com/esa/api/v2.0/config/logs/subscriptions?retrievalMethod=manual'

--header 'Authorization: Bearer <add access_token here>’
```

システム タイム

電子メールゲートウェイの時間設定は変更しないことを推奨します。

電子メールゲートウェイ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 settz 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 ゾーンの選択

[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、電子メールゲートウェイ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、電子メールゲートウェイの時間設定を編集できます。

- （推奨）Network Time Protocol（NTP）を使用した電子メールゲートウェイのシステム時刻の設定 （95 ページ）
- 電子メールゲートウェイのシステム時刻の手動設定 （95 ページ）

（推奨）Network Time Protocol（NTP）を使用した電子メールゲートウェイのシステム時刻の設定

これは、特に電子メールゲートウェイ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 サーバーを追加できます。

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。

電子メールゲートウェイの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 （96 ページ）
• ユーザ設定値の設定 （96 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	操作内容
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	[マイ ダッシュボード（My Dashboard）] 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、ユーザが電子メールゲートウェイ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、ユーザが電子メールゲートウェイ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）	ユーザが電子メールゲートウェイ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。

全般設定

電子メールゲートウェイの次の一般設定を編集できます。

- Internet Explorer の互換モードの上書き （98 ページ）
- 新しい Web インターフェイスを使用した電子メールゲートウェイの使用状況統計の収集（98 ページ）

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。

新しいWebインターフェイスを使用した電子メールゲートウェイの使用状況統計の収集

[使用状況分析（Usage Analytics）] は、分析統計情報のためにサイトアクティビティデータへのインサイトを得るために使用します。[使用状況分析（Usage Analytics）] が有効になっている場合、電子メールゲートウェイは新しい Web インターフェイスで電子メールゲートウェイの機能の使用状況データを収集します。使用状況の統計情報は、分析して、電子メールゲートウェイのユーザエクスペリエンスを向上させるためのインサイトを得るために使用します。

新規インストールの場合、使用状況の分析機能は電子メールゲートウェイにおいて、デフォルトで無効になっています。使用状況の分析機能を有効にするには、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）] > [一般設定（General 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 [使用状況分析（Usage Analytics）] チェックボックスをオンにします。
ステップ 4 変更を送信し、保存します。

最大 HTTP ヘッダー サイズの構成

電子メールゲートウェイに送信される 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。

- 電子メールゲートウェイで有効になっているサービスエンジンを再起動します。電子メールゲートウェイを再起動する必要はありません。
- 電子メールゲートウェイ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。

詳細については、Cisco Secure Email Gateway の『CLI リファレンスガイド』を参照してください。

国際化ドメイン名（IDN）を含むメッセージの受信と配信

電子メールゲートウェイは、IDN ドメインを含む電子メールアドレスを持つメッセージを受信および配信できます。

現在、電子メールゲートウェイは次の言語の IDN ドメインのみをサポートしています。

インドの地域言語：ヒンディー語、タミル語、テルグ語、カンナダ語、マラーティ語、パンジャブ語、マラヤラム語、ベンガル語、グジャラート語、ウルドゥー語、アッサム語、ネパール語、バングラ語、ボド語、ドグリ語、カシミール語、コンカニ語、マイティリ語、マニプリ語、オリヤ語、サンスクリット語、サンタル語、シンド語、トゥル語。

ヨーロッパおよびアジアの言語：フランス語、ロシア語、日本語、ドイツ語、ウクライナ語、韓国語、スペイン語、イタリア語、中国語、オランダ語、タイ語、アラビア語、カザフ語。

関連トピック：

- 前提条件 （100 ページ）
- 電子メールゲートウェイで IDN ドメインを使用して設定可能な機能 （100 ページ）

前提条件

国際化ドメイン名（IDN）機能を使用する前に、次の前提条件を満たしていることを確認してください。

- すべての着信メッセージには UTF-8 でエンコードされた IDN が必要です。

  たとえば、電子メールゲートウェイにメッセージを送信する MTA は IDN をサポートし、メッセージ内のドメインが UTF-8 形式であることを確認する必要があります。

- すべての発信メッセージには UTF-8 でエンコードされた IDN が必要であり、宛先サーバーはそれに応じて IDN を受け入れ、サポートする必要があります。

  たとえば、電子メールゲートウェイからのメッセージを受け入れる MTA は UTF-8 形式でエンコードされた IDN とドメインをサポートする必要があります。

- 該当するすべての DNS レコードで、Punycode 形式を使用して IDN を設定する必要があります。

  たとえば、IDN に MX レコードを設定する場合、DNS レコードのドメインは Punycode 形式である必要があります。

電子メールゲートウェイで IDN ドメインを使用して設定可能な機能

このリリースでは、電子メールゲートウェイ内で IDN ドメインを使用して設定できるのは次の機能**のみ**です。

- **SMTP ルートの設定**：
  - IDN ドメインを追加または編集します。
  - IDN ドメインを使用して SMTP ルートをエクスポートまたはインポートします。
- **DNS の設定**：IDN ドメインを使用して DNS サーバーを追加または編集します。
- **リスナーの設定**：
  - インバウンドリスナーまたはアウトバウンドリスナーのデフォルトドメインの IDN ドメインを追加または編集します。
  - HAT テーブルまたは RAT テーブルで IDN ドメインを追加または編集します。
  - IDN ドメインを使用して HAT テーブルまたは RAT テーブルをエクスポートまたはインポートします。
- **メールポリシーの設定**
  - [着信メールポリシー（Incoming Mail Policies）] の送信者（[送信者を追跡する（Following Senders）] オプションまたは [送信者を追跡しない（Following Senders are not）] オプション）と受信者（[受信者を追跡する（Following Recipients）]または[受

信者を受信しない（Recipients are not）]オプション）の IDN ドメインを使用してドメインを追加または編集します。

- [発信メールポリシー（Outgoing Mail Policies）] の送信者（[送信者を追跡する（Following Senders）] オプションまたは [送信者を追跡しない（Following Senders are not）] オプション）と受信者（[受信者を追跡する（Following Recipients）]または[受信者を受信しない（Recipients are not）]オプション）の IDN ドメインを使用してドメインを追加または編集します。
- [着信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] で IDN ドメインを使用した送信者または受信者を検索します。
- IDN ドメインを使用して送信者判定の例外を定義します。
- IDN ドメインを使用してアドレスリストを作成します。
- 宛先の制御に IDN ドメインを使用して宛先ドメインを追加または編集します。

- **バウンスプロファイルの設定**：IDN ドメインを使用して代替電子メールアドレスを追加または編集します。
- **送信者ドメインレピュテーションの設定**：IDN ドメインの送信者ドメイン レピュテーション スコアを定義します。
- **IP レピュテーションの設定**：IDN ドメインの IP レピュテーションスコアを定義します。
- **LDAP の設定**：IDN ドメインを使用して、LDAP グループクエリを作成し、クエリを受け入れ、クエリをルーティングし、クエリをマスカレードします。
- **レポートの設定**：IDNデータ（ユーザ名、電子メールアドレス、ドメイン）をレポートに表示します。
- **メッセージトラッキングの設定**：メッセージトラッキングに IDN データ（ユーザー名、電子メールアドレス、およびドメイン）を表示します。
- **ポリシー、ウイルス、およびアウトブレイク隔離の設定**：
  - ウイルス対策エンジンによる判定に従って、マルウェアを送信する可能性のある IDN ドメインを含むメッセージを表示します。
  - スパムまたはマルウェアの可能性があるとアウトブレイクフィルタによって検出された IDN ドメインを含むメッセージを表示します。
  - メッセージフィルタ、コンテンツフィルタ、およびDLPメッセージアクションによって検出された IDN ドメインを含むメッセージを表示します。
- **スパムの隔離の設定**：
  - スパム、または疑いのあるスパムとして検出されたIDNドメインを含むメッセージを表示します。
  - IDNドメインを含む電子メールアドレスをセーフリストとブロックリストのカテゴリに追加します。

（注） 現在、IDN ドメインを持つ受信者は、[スパムの隔離（Spam Quarantine）] 設定ページの [エンドユーザーの隔離アクセス（End-User Quarantine Access）] セクションでエンドユーザー認証方式が [なし（None）] に設定されている場合にのみ、エンドユーザーの隔離にアクセスできます。

- [SPF構成設定（SPF Configuration Settings）]：IDN ドメインを使用してメッセージの SPF 検証を実行します。
- [DKIM構成設定（DKIM Configuration Settings）]：IDN ドメインを使用して DKIM 署名とメッセージの検証を実行します
- [DMARC構成設定（DMARC Configuration Settings）]：IDNドメインを使用してメッセージの DMARC 検証を実行します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。