



セットアップ、インストール、および基本設定

この章は、次の項で構成されています。

- [ソリューション導入の概要](#) (1 ページ)
- [SMA 互換性マトリクス](#) (2 ページ)
- [インストール計画](#) (2 ページ)
- [セットアップの準備](#) (4 ページ)
- [セキュリティ管理アプライアンスへのアクセス](#) (6 ページ)
- [Swagger UIを使用したセキュリティ管理アプライアンス API インターフェイスへのアクセス](#) (11 ページ)
- [システム セットアップ ウィザードの実行](#) (12 ページ)
- [管理対象アプライアンスの追加について](#) (16 ページ)
- [セキュリティ管理アプライアンスでのサービスの設定](#) (18 ページ)
- [設定変更のコミットおよび破棄](#) (18 ページ)

ソリューション導入の概要

シスコのセキュリティソリューションにサービスを提供する Cisco Content Security Management アプライアンス を設定するには、次の手順に従います。

	対象アプライアンス	操作手順	詳細情報
ステップ 1	すべてのアプライアンス	お使いのアプライアンスが、使用する機能のシステム要件を満たしていることを確認してください。必要に応じて、アプライアンスをアップグレードします。	SMA 互換性マトリクス (2 ページ) を参照してください。

	対象アプライアンス	操作手順	詳細情報
ステップ 2	Eメールセキュリティアプライアンス	中央集中型サービスを環境に取り入れる前に、必要なセキュリティ機能が提供されるようにすべてのEメールセキュリティアプライアンスを設定し、各アプライアンスですべての機能が予期したとおりに動作することを確認します。	Cisco Email Securityのご使用のリリースのマニュアルを参照してください。
ステップ 3	Webセキュリティアプライアンス	中央集中型サービスを環境に取り入れる前に、必要なセキュリティ機能が提供されるように少なくとも1つのWebセキュリティアプライアンスを設定し、すべての機能が予期したとおりに動作することを確認します。	『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。
ステップ 4	Content Security Managementアプライアンスアプライアンス	アプライアンスを設定し、システムセットアップウィザードを実行します。	インストール計画 (2 ページ)、セットアップの準備 (4 ページ)、およびシステムセットアップウィザードの実行 (12 ページ) を参照してください。
ステップ 5	すべてのアプライアンス	導入する各中央集中型サービスを設定します。	セキュリティ管理アプライアンスでのサービスの設定 (18 ページ) から開始します。

SMA 互換性マトリクス

セキュリティ管理アプライアンスのEメールセキュリティアプライアンスおよびWebセキュリティアプライアンスとの互換性、およびWebセキュリティアプライアンスの設定のインポートおよび公開時の設定ファイルの互換性については、
<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>
 の互換性マトリクスを参照してください。

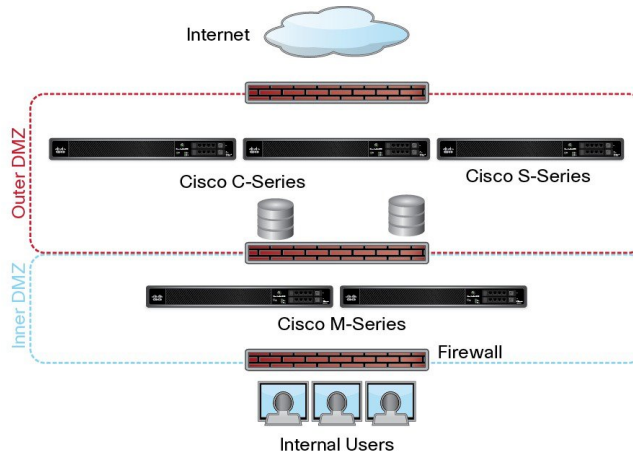
インストール計画

- ネットワーク プランニング (3 ページ)
- セキュリティ管理アプライアンスとEメールセキュリティEメールゲートウェイアプライアンスの統合について (3 ページ)
- クラスタ化されたEメールセキュリティアプライアンスを使用した展開 (4 ページ)

ネットワーク プランニング

セキュリティ管理アプライアンスの利用により、エンドユーザーのアプリケーションと、非武装地帯 (DMZ) に存在するより安全なゲートウェイシステムを切り離すことができます。2層ファイアウォールの使用によって、ネットワークプランニングの柔軟性が高まり、エンドユーザーが外部 DMZ に直接接続することを防止できます。

図 1: セキュリティ管理アプライアンスを組み込んだ一般的なネットワーク設定



次の図は、セキュリティ管理アプライアンスと複数の DMZ を組み込んだ一般的なネットワーク設定を示しています。内部ネットワークで、DMZ の外側にセキュリティ管理アプライアンスを展開します。セキュリティ管理アプライアンス (M シリーズ) によって管理対象の E メールセキュリティアプライアンス (C シリーズ) と管理対象の Web セキュリティアプライアンス (S シリーズ) へのすべての接続が開始されます。

企業データセンターはセキュリティ管理アプライアンスを共有し、複数の Web セキュリティアプライアンスおよび E メールセキュリティアプライアンスの中央集中型レポート生成とメッセージトラッキング、および複数の Web セキュリティアプライアンスの集約ポリシー設定を実行できます。また、セキュリティ管理アプライアンスは外部スパム隔離として使用されます。

E メールセキュリティアプライアンスおよび Web セキュリティアプライアンスをセキュリティ管理アプライアンスに接続してすべてのアプライアンスを適切に設定した後、AsyncOS は管理対象アプライアンスからデータを収集して集約します。集約されたデータからレポートを作成できます。また、電子メールの全体像と Web の使用状況を判断できます。

セキュリティ管理アプライアンスと E メールセキュリティ E メールゲートウェイアプライアンスの統合について

セキュリティ管理アプライアンスと E メールセキュリティアプライアンスの統合の詳細については、お使いの E メールセキュリティアプライアンスのユーザーマニュアルまたはオンラインヘルプで、「Centralizing Services on a Cisco Content Security Management Appliance」の章を参照してください。

クラスタ化されたEメールセキュリティアプライアンスを使用した展開

Eメールアプライアンスの中央集中型管理機能を使用するEメールセキュリティアプライアンスのクラスタには、セキュリティ管理アプライアンスを配置できません。ただし、クラスタ化されたEメールセキュリティアプライアンスは、中央集中型レポートイングとトラッキングのためにセキュリティ管理アプライアンスにメッセージを配信して隔離できます。

セットアップの準備

システムセットアップ ウィザードを実行する前に、次の手順を実行してください。

- ステップ1 製品の最新リリース ノートを確認します。 [ネットワーク プランニング \(3 ページ\)](#) を参照してください。
- ステップ2 セキュリティ ソリューションのコンポーネントに互換性があることを確認します。 [SMA 互換性マトリクス \(2 ページ\)](#) を参照してください。
- ステップ3 この導入に対応できるネットワークと物理的空間の準備があることを確認します。 [インストール計画 \(2 ページ\)](#) を参照してください。
- ステップ4 セキュリティ管理アプライアンスを物理的にセットアップし、接続します。 [アプライアンスの物理的なセットアップと接続 \(4 ページ\)](#) を参照してください。
- ステップ5 ネットワーク アドレスと IP アドレスの割り当てを決定します。 [ネットワーク アドレスと IP アドレスの割り当ての決定 \(5 ページ\)](#) を参照してください。
- ステップ6 システムセットアップに関する情報を収集します。 [セットアップ情報の収集 \(5 ページ\)](#) を参照してください。

アプライアンスの物理的なセットアップと接続

この章の手順を続行する前に、アプライアンスに付属するクイック スタート ガイドに記載された手順を実行してください。このガイドでは、アプライアンスを梱包箱から取り出し、物理的にラックに取り付けて電源を投入済みであることを前提としています。

GUI にログインするには、PC とセキュリティ管理アプライアンスの間にプライベート接続を設定する必要があります。たとえば、付属するクロスケーブルを使用して、アプライアンスの管理ポートからラップトップに直接接続できます。任意で、PC とネットワーク間、およびネットワークとセキュリティ管理アプライアンスの管理ポート間をイーサネット接続（イーサネット ハブなど）で接続できます。

ネットワークアドレスとIPアドレスの割り当ての決定



- (注) すでにアプライアンスをネットワークに配線済みの場合は、コンテンツセキュリティアプライアンスのデフォルトIPアドレスが、ネットワーク上の他のIPアドレスと競合していないことを確認します。各アプライアンスの管理ポートに事前に設定されているIPアドレスは、192.168.42.42です。

設定後に、メインセキュリティ管理アプライアンスの[管理アプライアンス (Management Appliance)]>[ネットワーク (Network)]>[IP インターフェイス (IP Interfaces)] ページに移動し、セキュリティ管理アプライアンスが使用するインターフェイスを変更します。

使用することを選択した各イーサネットポートに関する次のネットワーク情報が必要になります。

- IP アドレス
- ネットマスク

さらに、ネットワーク全体に関する次の情報も必要になります。

- ネットワーク上のデフォルトのルータ (ゲートウェイ) の IP アドレス
- DNS サーバーの IP アドレスおよびホスト名 (インターネットルートサーバーを使用する場合は不要)
- NTP サーバーのホスト名または IP アドレス (システム時刻を手動で設定する場合は不要)

詳細については、[ネットワークとIPアドレスの割り当て](#)を参照してください。



- (注) インターネットとコンテンツセキュリティアプライアンスの間でファイアウォールが稼働しているネットワークの場合は、アプライアンスを正常に機能させるために、特定のポートを開ける必要がある場合があります。ファイアウォールの詳細については、[ファイアウォール情報](#)を参照してください。

Eメールセキュリティアプライアンスとの電子メールメッセージの送受信には、常にセキュリティ管理アプライアンスの同じIPアドレスを使用します。説明については、使用しているEメールセキュリティアプライアンスのマニュアルにあるメールフローに関する情報を参照してください。

シスコのコンテンツセキュリティ管理アプライアンスとその管理対象アプライアンス間の通信では、IPv6はサポートされていません。

セットアップ情報の収集

次の表を使用して、システムセットアップの情報を収集してください。システムセットアップウィザードを実行するときに、この情報を手元に用意する必要があります。



(注) ネットワークおよびIPアドレスの詳細については、[ネットワークとIPアドレスの割り当て](#)を参照してください。

次の表は、システム セットアップ ワークシートを示しています

1	通知		システム アラートが送信される電子メールアドレス :
2	システム タイム		NTP サーバー (IP アドレスまたはホスト名) :
3	管理者パスワード		「admin」アカウントの新しいパスワードを選択します。
4	AutoSupport		AutoSupport を有効にする __ はい __ いいえ
5	ホストネーム		セキュリティ管理アプライアンスの完全修飾ホスト名 :
6	インターフェイス/IP アドレス		IPアドレス:
			ネットマスク :
7	ネットワーク	ゲートウェイ	デフォルト ゲートウェイ (ルータ) の IP アドレス :
		DNS	__ インターネットのルート DNS サーバーを使用
			__ これらの DNS サーバーを使用

セキュリティ管理アプライアンスへのアクセス

セキュリティ管理アプライアンスには、標準の Web ベース グラフィカル ユーザー インターフェイス、スパム隔離を管理するための別個の Web ベース インターフェイス、コマンドライン インターフェイス、および特定の機能へのアクセス権が付与された管理ユーザー用の特別な、または制限付きの Web ベース インターフェイスがあります。

- [ブラウザ要件 \(7 ページ\)](#)
- [Web インターフェイスへのアクセスについて \(8 ページ\)](#)
- [レガシー Web インターフェイスへのアクセス \(9 ページ\)](#)
- [Web インターフェイスへのアクセス \(8 ページ\)](#)
- [コマンドライン インターフェイスへのアクセス \(10 ページ\)](#)
- [サポートされる言語 \(10 ページ\)](#)

- [新しい Web インターフェイスの暗色モードでの利用 \(11 ページ\)](#)

ブラウザ要件

GUI にアクセスするには、ブラウザが JavaScript および Cookie をサポートし、受け入れるよう設定されている必要があります。さらに、Cascading Style Sheet (CSS) を含む HTML ページを描画できる必要があります。

表 1: サポートされるブラウザおよびリリース

ブラウザ	Windows 7	MacOS 10.6
Safari	—	7.0 以降
Google Chrome	最新の安定バージョン	最新の安定バージョン
Microsoft Internet Explorer	11.0	—
Mozilla Firefox	最新の安定バージョン	最新の安定バージョン

- Internet Explorer 11.0 (Windows 7 のみ)
- Safari 7 以降
- Firefox (最新の安定バージョン)
- Google Chrome (最新の安定バージョン)

ブラウザは、そのブラウザの公式なサポート対象オペレーティング システムに対してのみサポートされます。

インターフェイスの一部のボタンまたはリンクからは追加のウィンドウがオープンされるため、GUI を使用するには、ブラウザのポップアップブロックの設定が必要な場合があります。

HTML ページのシームレスなナビゲーションとレンダリングのために、次のブラウザを使用してアプライアンスの新しい Web インターフェイス (AsyncOS 12.0 以降) にアクセスすることをお勧めします。

- Google Chrome (最新の安定バージョン)
- Mozilla Firefox (最新の安定バージョン)

サポートされているブラウザのいずれかで、アプライアンスのレガシー Web インターフェイスにアクセスできます。

アプライアンスの新しい Web インターフェイス (AsyncOS 12.0 以降) でサポートされている解像度は、1280 X 800 ~ 1680 X 1050 です。すべてのブラウザに対して最適に表示される解像度は 1440x900 です。



(注) シスコでは、より高い解像度でアプライアンスの新しい Web インターフェイスを表示することは推奨していません。

Web インターフェイスへのアクセスについて

セキュリティ管理 アプライアンスには、デフォルトではポート 80 で使用可能な標準管理者インターフェイスと、デフォルトではポート 82 で使用可能なスパム隔離エンドユーザーインターフェイスの、2 つの Web インターフェイスがあります。スパム隔離 HTTPS インターフェイスを有効にすると、デフォルトでポート 83 に設定されます。

各 Web インターフェイスを設定する際に HTTP または HTTPS を指定できるため（セキュリティ管理 アプライアンス上で [管理アプライアンス (Management Appliance)] > [ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] に移動）、セッション中にそれらを切り替える場合は、再認証を要求される場合があります。たとえば、ポート 80 の HTTP を介して管理者 Web インターフェイスにアクセスし、次に同じブラウザでポート 83 の HTTPS を介してスパム隔離エンドユーザー Web インターフェイスにアクセスした場合、管理者 Web インターフェイスに戻るときに再認証を要求されます。



(注) 次のものを同時に使用して設定変更を実行しないでください。

- 同じブラウザ上の複数のタブ。
- 同じシステムまたは 2 つの異なるシステム上の複数のブラウザ。

また、予期しない動作が発生する可能性があるため、Web インターフェイスと CLI セッションを同時に使用しないでください。

Web インターフェイスへのアクセス

ステップ 1 ブラウザを開き、アプライアンスの IP アドレスまたはホスト名を入力します。

ステップ 2 (新しい Web インターフェイスのみ) 新しい Web インターフェイスには次のいずれかの方法でアクセスできます。

(注) アプライアンスの新しい Web インターフェイスは、AsyncOS API HTTP/HTTPS ポート (6080/6443) および trailblazer HTTPS ポート (4431) を使用します。CLI で `trailblazerconfig` コマンドを使用して、trailblazer HTTPS ポートを設定できます。trailblazer HTTPS ポートがファイアウォールで開かれていることを確認します。

- `trailblazerconfig` CLI コマンドが有効になっているときは、URL (`https://example.com:<trailblazer-https-port>/ng-login`) を使用します

ここで、example.com はアプライアンスのホスト名で、<trailblazer-https-port> はアプライアンスで設定されている trailblazer の HTTPS ポートです。

trailblazerconfig CLI コマンドの詳細については、[trailblazerconfig コマンド](#)を参照してください。

- trailblazerconfig CLI コマンドが無効になっているときは、URL (https://example.com:<https-port>/ng-login) を使用します
ここで example.com はアプライアンスのホスト名で、<https-port> はアプライアンスで設定されている HTTPS ポートです。
- レガシー Web インターフェイスにログインし、**[セキュリティ管理アプライアンス (Security Management appliance)]** をクリックして新しい外観を取得します。お試しください! リンクで新しい Web インターフェイスにアクセスできます。

重要

- アプライアンスで AsyncOS API が有効になっていることを確認してください。
- アプライアンスのレガシー Web インターフェイスにログインする必要があります。
- trailblazerconfig が有効になっている場合は、設定済み HTTPS ポートがファイアウォールで開いている必要があります。デフォルトの HTTPS ポートは 4431 です。
また、アプライアンスにアクセスするために指定したホスト名を DNS サーバが解決できることを確認します。
- trailblazerconfig が無効になっている場合は、**[管理アプライアンス (Management Appliance)] > [ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)]** で設定された AsyncOS API ポートがファイアウォールで開きます。デフォルトの AsyncOS API HTTP/HTTPS ポートは 6080/6443 です。

ステップ 3 次のデフォルト値を入力します。

- ユーザー名 : **admin**
- パスフレーズ : **ironport**

(注) Web インターフェイスまたはコマンドラインインターフェイスのいずれを使用した場合も、システム セットアップ ウィザードの完了後は、このパスフレーズが無効になります。

レガシー Web インターフェイスへのアクセス



- (注) レガシー Web インターフェイスにアクセスするには、セキュリティ管理アプライアンスにログインする必要があります。詳細については、[Web インターフェイスへのアクセス \(8 ページ\)](#) を参照してください。

レポート、メッセージトラッキング、隔離、ネットワーク アクセス、およびシステム ステータスのモニターを有効にして設定するには、レガシー Web インターフェイスにアクセスする必要があります。

新しい Web インターフェイスからレガシー Web インターフェイスにアクセスするには、次の図に示すように、歯車アイコン (⚙️) をクリックします。

図 2: レガシー Web インターフェイスへのアクセス



レガシー Web インターフェイスが新しいブラウザ ウィンドウで開きます。アクセスするには再度ログインする必要があります。

アプライアンスから完全にログアウトする場合は、アプライアンスの新しい Web インターフェイスとレガシー Web インターフェイスの両方からログアウトする必要があります。

コマンドラインインターフェイスへのアクセス

コマンドライン インターフェイス (CLI) には、セキュリティ管理 アプライアンスで、すべての Cisco コンテンツ セキュリティ アプライアンス上での CLI アクセスと同じ方法でアクセスします。ただし、次のような違いがあります。

- システム セットアップは、GUI を使用して実行する必要があります。
- アプライアンスでは、一部の CLI コマンドを使用できません。サポートされていないコマンドのリストについては、『IronPort AsyncOS CLI Reference Guide for Cisco Content Security Appliances』を参照してください。

実動環境では、CLI にアクセスするために、SSH を使用する必要があります。ポート 22 でアプライアンスにアクセスするために、標準 SSH クライアントを使用します。ラボ展開の場合、Telnet も使用できますが、このプロトコルは暗号化されません。

サポートされる言語

該当するライセンス キーを使用すると、AsyncOS では、次の言語で GUI および CLI を表示できます。

- 英語
- フランス語
- スペイン語
- ドイツ語
- イタリア語
- 韓国語
- 日本語
- ポルトガル語 (ブラジル)
- 中国語 (繁体字および簡体字)

- ロシア語

GUIとデフォルトのレポート言語を選択するには、次のいずれかを実行してください。

- 言語を設定します。[プリファレンスの設定](#)を参照してください。
- GUI ウィンドウの右上にある [オプション (Options)] メニューを使用して、セッションの言語を選択します。

(有効な方法は、ログイン資格情報の認証に使用する方法によって異なります。)

新しい Web インターフェイスの暗色モードでの利用

暗色モードは反転カラスキームであり、暗い色の背景上で明るい色のタイポグラフィ、UI 要素、アイコンが使用されます。アプライアンスの新しい Web インターフェイスで暗色モードを利用できるようになりました。

アプライアンスでダークモードの Web インターフェイスに切り替えるには、新しい Web インターフェイスの右上隅にあるユーザー情報セクションをクリックし、[ダークモード (Dark Mode)] を選択します。

Swagger UI を使用したセキュリティ管理アプライアンス API インターフェイスへのアクセス

Swagger UI を使用すると、アプライアンスの API リソースを視覚化して操作できます。これは API 仕様から自動的に生成されます。詳細については、<https://swagger.io/tools/swagger-ui/> を参照してください。

セキュリティ管理 アプライアンスの新しい Web インターフェイスで Swagger UI にログインする場合、次のいずれかの方法を使用します。

- URL (<https://example.com:<trailblazer-https-port>/swagger>) を使用します

ここで、example.com はアプライアンスのホスト名で、<trailblazer-https-port> はアプライアンスで設定されている先駆者の HTTPS ポートです。



(注) Swagger UI にアクセスするには、アプライアンスで trailblazer の HTTPS ポートを有効にする必要があります。trailblazerconfig CLI コマンドの詳細については、[trailblazerconfig コマンド](#) を参照してください。

- アプライアンスの新しい Web インターフェイスにログインします。右上隅の [?] ボタンをクリックして、ドロップダウンから [APIヘルプ: Swagger (API Help: Swagger)] を選択します。Swagger UI が新しいブラウザ ウィンドウに開きます。

システムセットアップウィザードの実行

AsyncOSには、システム設定を実行するための、ブラウザベースのシステムセットアップウィザードが用意されています。後で、ウィザードでは使用できないカスタム設定オプションを利用する場合があります。ただし、初期セットアップではウィザードを使用して、設定に漏れがないようにする必要があります。

セキュリティ管理アプライアンスでは、GUIを使用する場合のみ、このウィザードがサポートされます。コマンドラインインターフェイス（CLI）によるシステムセットアップはサポートされません。

- [はじめる前に](#)（12 ページ）
- [システムセットアップウィザードの概要](#)（13 ページ）

はじめる前に

[セットアップの準備](#)（4 ページ）のすべてのタスクを実行します。



注意 システムセットアップウィザードを使用すると、アプライアンスが完全に再設定されます。アプライアンスを最初にインストールする場合、または既存の設定を完全に上書きする場合にのみ、このウィザードを使用してください。

セキュリティ管理アプライアンスが、管理ポートからネットワークに接続されていることを確認します。



注意 セキュリティ管理アプライアンスには、管理ポートに IP アドレス 192.168.42.42 がデフォルトで設定済みです。セキュリティ管理アプライアンスをネットワークに接続する前に、他の装置の IP アドレスが、この工場出荷時のデフォルト設定と競合していないことを確認してください。



(注) デフォルトでは、30 分以上アイドル状態になっている場合、またはログアウトせずにブラウザを閉じた場合は、セッションがタイムアウトします。この場合、ユーザー名とパスワードを再入力する必要があります。システムセットアップウィザードを実行中にセッションがタイムアウトした場合は、最初からやり直す必要があります。タイムアウト制限を変更するには、[Web UI セッションタイムアウトの設定](#)を参照してください。

システムセットアップウィザードの概要

ステップ1 システムセットアップウィザードの起動 (13 ページ)

ステップ2 エンドユーザー ライセンス契約書の確認 (13 ページ)

ステップ3 システムの設定 (14 ページ)

- 通知設定と AutoSupport
- システム時刻設定
- 管理者パズフレーズ

ステップ4 ネットワークの設定 (14 ページ)

- アプライアンスのホスト名
- アプライアンスの IP アドレス、ネットワーク マスク、およびゲートウェイ
- デフォルト ルータと DNS 設定

ステップ5 設定の確認 (15 ページ)

ウィザードの各ページを実行し、ステップ4で設定を慎重に確認します。[前へ (Previous)] をクリックすると、前の手順に戻ることができます。プロセスの最後に、変更を確定するようウィザードのプロンプトが表示されます。確定するまで、大部分の変更は有効になりません。

ステップ6 次の手順 (16 ページ)

システムセットアップウィザードの起動

ウィザードを起動するには、[Web インターフェイスへのアクセス \(8 ページ\)](#) の説明に従って GUI にログインします。GUI に初めてログインすると、デフォルトでは、システムセットアップウィザードの最初のページが表示されます。また、[システム管理 (System Administration)] メニューからシステムセットアップウィザードにアクセスすることもできます ([管理アプライアンス (Management Appliance)] > [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)])。

エンドユーザー ライセンス契約書の確認

ライセンス契約書の参照から開始します。ライセンス契約書を参照し、同意する場合は、同意することを示すチェックボックスをオンにし、[セットアップの開始 (Begin Setup)] をクリックして続行します。

システムの設定

システムアラート用の電子メールアドレスの入力

ユーザーの介入を必要とするシステムエラーが発生した場合、AsyncOS では、電子メールでアラートメッセージが送信されます。アラートの送信先となる電子メールアドレス（複数可）を入力します。

システムアラート用の電子メールアドレスを1つ以上追加する必要があります。複数のアドレスを指定する場合は、カンマで区切ります。入力した電子メールアドレスでは、当初、すべてのレベルのすべてのタイプのアラートが受信されます。アラート設定は、後からカスタマイズできます。詳細については、[アラートの管理](#)を参照してください。

時間の設定

セキュリティ管理アプライアンス上のタイムゾーンを設定して、レポート、メッセージヘッダーおよびログファイルのタイムスタンプが正確になるようにします。ドロップダウンメニューを使用して時間帯を見つけるか、GMT オフセットによって時間帯を定義します。

システムクロック時刻は手動で設定することができますが、ネットワークタイムプロトコル（NTP）サーバーを使用してネットワーク上またはインターネット上の他のサーバーと時刻を同期することを推奨します。デフォルトでは、Cisco NTP サーバー（time.sco.cisco.com）がコンテンツセキュリティアプライアンスで時刻を同期するためにエントリとして追加されました。NTPサーバーのホスト名を入力し、[エントリの追加（Add Entry）]をクリックして追加のNTPサーバーを設定します。詳細については、[システム時刻の設定](#)を参照してください。

パスワードの設定

AsyncOS の admin アカウントのパスワード：adminpassphrase を変更する必要があります。パスワードは安全な場所に保管してください。パスワードの変更はすぐに有効になります。



(注) パスワードの再設定後にシステム設定を取り消しても、パスワードの変更は元に戻りません。

AutoSupport のイネーブル化

AutoSupport 機能（デフォルトで有効）で、セキュリティ管理アプライアンスに関する問題をカスタマーサポートに通知することにより、最適なサポートを提供できます。詳細については、[Cisco AutoSupport](#)を参照してください。

ネットワークの設定

マシンのホスト名を定義し、ゲートウェイと DNS 設定値を設定します。



- (注) セキュリティ管理アプライアンスが、管理ポートを通してネットワークに接続されていることを確認します。

ネットワーク設定

セキュリティ管理アプライアンスの完全修飾ホスト名を入力します。この名前は、ネットワーク管理者が割り当てる必要があります。

セキュリティ管理アプライアンスの IP アドレスを入力します。

ネットワーク上のデフォルトルータ（ゲートウェイ）のネットワーク マスクと IP アドレスを入力します。

次に、Domain Name Service（DNS）設定値を設定します。AsyncOS には、インターネットのルートサーバーに直接問い合わせできる、高性能な内部 DNS リゾルバ/キャッシュが組み込まれていますが、指定した DNS サーバーを使用することもできます。独自のサーバーを使用する場合は、各 DNS サーバーの IP アドレスを指定する必要があります。システムセットアップウィザードを使用して入力できる DNS サーバーは、4 台までです。



- (注) 指定した DNS サーバーの初期プライオリティは 0 です。詳細については、[ドメインネームシステムの設定](#)を参照してください。



- (注) アプライアンスでは、着信接続に対して DNS ルックアップを実行するために、稼働中の DNS サーバーへのアクセスが必要です。アプライアンスをセットアップするときに、アプライアンスからアクセス可能な稼働中の DNS サーバーを指定できない場合は、[インターネットのルートDNSサーバーを使用（Use Internet Root DNS Servers）]を選択するか、管理インターフェイスの IP アドレスを一時的に指定することによってシステムセットアップウィザードを完了できます。

設定の確認

これで、入力した設定情報の要約がシステムセットアップウィザードに表示されます。変更する必要がある場合は、ページの下部にある **[前へ (Previous)]** をクリックし、情報を編集します。

情報を確認した後、**[この設定をインストール (Install This Configuration)]** をクリックします。次に、表示される確認ダイアログボックスで **[インストール (Install)]** をクリックします。

[この設定をインストール (Install This Configuration)] をクリックしてもページが反応しないように見える場合、その原因はウィザードで指定した新しい IP アドレスをアプライアンスが使用していることにあります。引き続きこのアプライアンスを使用するには、新しい IP アド

レスを使用します。『Quick Start Guide』の手順に従い、新しいハードウェア アプライアンスにアクセスするために使用したコンピュータの IP アドレスを一時的に変更した場合は、まずコンピュータの IP アドレスを元の設定に戻します。

次の手順

セキュリティ管理アプライアンスをインストールし、システム セットアップ ウィザードを実行した後、アプライアンス上の他の設定を修正して、モニターリング サービスを設定できます。

システム セットアップ ウィザードを実行するためにアプライアンスにアクセスするときに使用したプロセスに基づき、[システムセットアップの次のステップ (System Setup Next Steps)] ページが表示されます。このページが自動的に表示されない場合、このページを表示するには [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [次のステップ (Next Steps)] を選択します。

[システムセットアップの次のステップ (System Setup Next Steps)] ページのいずれかのリンクをクリックして、Cisco Content Security アプライアンス の設定を続行します。

管理対象アプライアンスの追加について

各アプライアンスに対して最初の中央集中型サービスを設定するときに、管理対象の電子メールおよび Web セキュリティアプライアンスをセキュリティ管理アプライアンスに追加します。

サポートされている電子メールおよび Web セキュリティアプライアンスは、[SMA 互換性マトリクス \(2 ページ\)](#) に記載されています。

リモートアプライアンスを追加すると、セキュリティ管理アプライアンスによって、リモートアプライアンスの製品名と追加するアプライアンスのタイプが比較されます。たとえば、[Web セキュリティアプライアンスの追加 (Add Web Security appliance)] ページを使用してアプライアンスを追加すると、そのアプライアンスは Web セキュリティアプライアンスであって E メールセキュリティアプライアンスではないことを確認するために、セキュリティ管理アプライアンスによってリモートアプライアンスの製品名がチェックされます。また、セキュリティ管理アプライアンスは、リモートアプライアンス上のモニターリングサービスをチェックして、それらが正しく設定され、互換性があることを確認します。


[セキュリティアプライアンス (Security Appliances)] ページには、追加した管理対象アプライアンスが表示されます。[接続が確立されていますか? (Connection Established?)] 列は、モニターリングサービスの接続が適切に設定されているかどうかを示します。

管理対象アプライアンスの追加方法は、次の手順に含まれています。

- [管理対象の各 E メールセキュリティアプライアンスへの中央集中型電子メール レポート サービスの追加](#)
- [管理対象の各 E メールセキュリティアプライアンスへの中央集中型メッセージ トラッキング サービスの追加](#)

- 管理対象の各 E メールセキュリティアプライアンスへの中央集中型スパム隔離サービスの追加
- 管理対象の各 E メールセキュリティアプライアンスへの集約ポリシー、ウイルス、アウトブレイク隔離サービスの追加
- 管理対象の各 Web セキュリティアプライアンスへの中央集中型 Web レポーティングサービスの追加
- Web Security Appliances の追加と Configuration Master のバージョンとの関連付け

管理対象アプライアンス設定の編集

ステップ 1 (新しい Web インターフェイスのみ) セキュリティ管理アプライアンスで  をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] を選択します。

ステップ 3 [セキュリティアプライアンス (Security Appliance)] セクションで、編集するアプライアンスの名前をクリックします。

ステップ 4 アプライアンスの設定に必要な変更を行います。

たとえば、モニターリングサービスのチェックボックスをオンまたはオフにする、ファイル転送アクセスを再設定する、または IP アドレスを変更する、などの変更を行います。

(注) 管理対象アプライアンスの IP アドレスを変更すると、さまざまな問題が発生する可能性があります。Web セキュリティアプライアンスの IP アドレスを変更すると、アプライアンスの公開履歴が失われ、スケジュールされた公開ジョブに対して Web セキュリティアプライアンスが現在選択されていると、公開エラーが発生します。(割り当てられたすべてのアプライアンスを使用するように設定されたスケジュール済み公開ジョブは、影響を受けません)。E メールセキュリティアプライアンスの IP アドレスを変更すると、アプライアンスのトラッキングアベイラビリティデータが失われます。


ステップ 5 [送信 (Submit)] をクリックして、ページ上の変更を送信し、[変更を確定 (Commit Changes)] をクリックして変更を保存します。

管理対象アプライアンスのリストからのアプライアンスの削除

始める前に

リモートアプライアンスをセキュリティ管理アプライアンスから削除する前にそのアプライアンスで有効なすべての集約管理サービスを無効にする必要があります。たとえば、集約されたポリシー、ウイルス、アウトブレイク隔離サービスが有効な場合、E メールセキュリティア

プライアンスでまずそのサービスを無効にする必要があります。電子メールまたはネットワークのセキュリティアプライアンスのマニュアルを参照してください。

-
- ステップ 1** (新しい Web インターフェイスのみ) セキュリティ管理アプライアンスで  をクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] を選択します。
- ステップ 3** [セキュリティアプライアンス (Security Appliances)] セクションで、削除する管理対象アプライアンスの行にあるゴミ箱アイコンをクリックします。
- ステップ 4** 確認のダイアログボックスで [削除 (Delete)] をクリックします。
- ステップ 5** 変更を送信し、保存します。
-

セキュリティ管理アプライアンスでのサービスの設定

電子メール セキュリティ サービス :

- [中央集中型の電子メールセキュリティ レポートニングの使用](#)
- [メッセージのトラッキング](#)
- [スパム隔離](#)
- [集約されたポリシー、ウイルス、およびアウトブレイク隔離](#)


Web セキュリティ サービス :

- [集約されたポリシー、ウイルス、およびアウトブレイク隔離](#)
- [Web セキュリティアプライアンスの管理](#)

設定変更のコミットおよび破棄

Cisco Content Security Management GUI で設定を変更した後、ほとんどの場合、変更を明示的にコミットする必要があります。

図 3: [変更を確定 (Commit Changes)] ボタン



目的	操作手順
すべての保留中の変更をコミットする	ウィンドウの右上にあるオレンジ色の [変更を確定 (Commit Changes)] ボタンをクリックします。変更内容の説明を追加し、[確定する (Commit)] をクリックします。コミットが必要な変更を実行していない場合、[変更を確定 (Commit Changes)] の代わりにグレーの [保留中の変更なし (No Changes Pending)] ボタンが表示されます。
すべての保留中の変更を破棄する	ウィンドウの右上にあるオレンジ色の [変更を確定 (Commit Changes)] ボタンをクリックし、[変更を破棄 (Abandon Changes)] をクリックします。



- (注) 古い Web インターフェイスでの構成変更は、ログアウトし、新しい Cisco コンテンツ セキュリティ管理 Web インターフェイスにログインした後に、新しい Web インターフェイスで更新されます。

関連項目

- [以前コミットしたコンフィギュレーションへのロールバック](#)

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。