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

Cisco コンテンツ セキュリティ ソリューションにサービスを提供する Cisco コンテンツ セキュリティ管理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	セキュリティ管理アプライアンス	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 （11 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 （17 ページ）から開始します。

SMA 互換性マトリクス

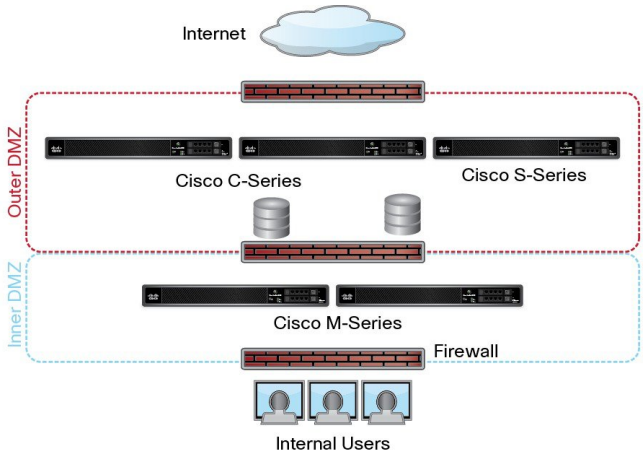
セキュリティ管理アプライアンスの E メール セキュリティ アプライアンスおよび Web セキュリティ アプライアンスとの互換性、および Web セキュリティ アプライアンスの設定のインポートおよび公開時の設定ファイルの互換性については、http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html の互換性マトリクスを参照してください。

インストール計画

ネットワーク プランニング

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導入します。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ティングとメッセージ 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 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 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、セキュリティ管理アプライアンスを配置することはできません。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、中央集中型レポーティ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 サーバを使用する場合は不要）
- NTP サーバのホスト名または 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。

Cisco 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（IP アドレスまたはホスト名）：
3	管理者パスフレーズ		「admin」アカウントの新しいパスフレーズを選択します。
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 サーバを使用
			___ これらの DNS サーバを使用

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 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）

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、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 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 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、[クラウドEメールセキュリティ（Cloud Email Security）][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 AsycnOS 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

上のコマンドライン 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。
- セキュリティ管理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ティング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）。

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

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、ユーザ名とパスフレーズ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 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 （13 ページ）

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

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 （15 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 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（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。

パスフレーズの設定

AsyncOS の admin アカウントの パスフレーズ： adminpassphrase を変更する必要があります。パスフレーズは安全な場所に保管してください。パスフレーズの変更はすぐに有効になります。

（注） パスフレーズの再設定後にシステム設定を取り消しても、パスフレーズ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 サーバを使用することもできます。独自のサーバを使用する場合は、各 DNS サーバの 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 サーバは、4 台までです。

（注） 指定した DNS サーバ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 コンテンツ セキュリティ 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ティ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 レポーティングの使用
- 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 コンテンツ セキュリティ管理アプライアンスの 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