CHAPTER 2

セットアップ、インストール、および基本設定

この章では、セキュリティ管理アプライアンスの設定について始めます。

この章は、次の内容で構成されています。

ソリューション導入の概要

集中管理型の Cisco IronPort ソリューションを設定するには、次の手順に従ってください。

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。「SMA 互換性マトリクス」（P.2-2）を参照してください。

ステップ 2 **すべてのアプライアンス。**必要に応じて、アプライアンスをアップグレードします。

ステップ 3 **電子メール 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電子メール 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 IronPort AsyncOS for Email Security*』マニュアルを参照してください。

ステップ 4 **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すべての 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。『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 5 **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。「設置計画」（P.2-4）、「セットアップの準備」（P.2-6）、および「システム セットアップ ウィザードの実行」（P.2-10）を参照してください。

ステップ 6　**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」（P.2-17）から開始します。

SMA 互換性マトリクス

ここでは、今回リリースの AsyncOS for Security Management と、電子メール セキュリティ アプライアンスおよび Web セキュリティ アプライアンスに対応する各 AsyncOS リリースとの互換性について説明します。さらに、サポートされるコンフィギュレーション ファイルの表も示してあります。

（注）　（Web セキュリティ アプライアンスのある導入環境の場合）Web セキュリティ アプライアンスは、前の 2 つのメジャー バージョンまで、そのコンフィギュレーション データの後方互換性を維持します。ソースおよびターゲット アプライアンスでのソフトウェアのバージョンによっては、アップグレードが セキュリティ管理アプライアンスの機能に影響を与える可能性があることに注意してください。

表 2-1　セキュリティ管理アプライアンスと電子メール セキュリティ アプライアンスの互換性

バージョン	レポート	トラッキング	セーフリスト/ブロックリスト	ISQ
ESA 6.3	サポートなし	サポートなし	サポートなし	サポート
ESA 6.4	サポート	サポート	サポート	サポート
ESA 6.5	サポート	サポート	サポート	サポート
ESA 7.0	サポート	サポート	サポート	サポート
ESA 7.1	サポート	サポート	サポート	サポート
ESA 7.5	サポート	サポート	サポート	サポート

表 2-2　セキュリティ管理アプライアンスと Web セキュリティ アプライアンスの互換性

バージョン	中央集中レポーティングおよびトラッキング	ICCM 公開[a]	Web セキュリティ アプライアンス への拡張ファイル公開
WSA 5.6	機能は使用不可	サポートなし	サポートなし
WSA 5.7	機能は使用不可	サポートなし	コンフィギュレーション ファイルのバージョンは、ターゲットの WSA バージョンと一致している必要があります。
WSA 6.0	機能は使用不可	サポートなし	サポートなし
WSA 6.3	機能は使用不可	6.3 の Configuration Master でサポート	コンフィギュレーション ファイルのバージョンは、ターゲットの WSA バージョンと一致している必要があります。
WSA 7.0	機能は使用不可	6.3 の Configuration Master でサポート	コンフィギュレーション ファイルのバージョンは、ターゲットの WSA バージョンと一致している必要があります。
WSA 7.1	サポート	6.3 と 7.1 の Configuration Master でサポート	コンフィギュレーション ファイルのバージョンは、ターゲットの WSA バージョンと一致している必要があります。
WSA 7.5	サポート	6.3、7.1、および 7.5 の Configuration Master でサポート Configuration Master 7.5 を強く推奨します。	コンフィギュレーション ファイルのバージョンは、ターゲットの WSA バージョンと一致している必要があります。

a. 表内の ICCM 公開行と拡張ファイル公開行の公開先は Web セキュリティ アプライアンスです。

表 2-3　（WSA のある導入のみ）Configuration Master の互換性

ターゲット Configuration Master のバージョン：	ソース Configuration Master のバージョン：	ソース コンフィギュレーション ファイルが存在する Web セキュリティ アプライアンスのバージョン：
6.3	N/A	Web セキュリティ アプライアンス 6.3
7.1	Configuration Master 6.3	Web セキュリティ アプライアンス 7.1
7.5	Configuration Master 6.3 または 7.1	Web セキュリティ アプライアンス 7.5

設置計画

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 2-1 を参照）。

図 2-1　セキュリティ管理アプライアンスを含む一般的なネットワーク設定

図 2-1 に、セキュリティ管理アプライアンスと複数の DMZ を含む一般的なネットワーク設定を示します。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。管理対象電子メール セキュリティ アプライアンス（Cisco IronPort C-Series）および管理対象 Web セキュリティ アプライアンス（Cisco IronPort S-Series）へのすべての接続は、セキュリティ管理アプライアンス（Cisco IronPort M-Series）によって開始されます。

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 電子メール 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およびメッセージ トラッキング、および複数の Web セキュリティ アプライアンスの中央集中型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 Cisco IronPort スパム隔離としても使用できます。

電子メール 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の物理的寸法

Cisco IronPort M1000/1050 および M600/650 セキュリティ管理アプライアンスには、次の物理的寸法が適用されます。

- 高さ：8.656 cm（3.40 インチ）
- 幅：レールを取り付けて 48.26 cm（19.0 インチ）（レールを取り付けない場合は 17.5 インチ）
- 奥行：75.68 cm（29.79 インチ）
- 重量：最大 26.76 kg（59 ポンド）

Cisco IronPort M1070 および 670 セキュリティ管理アプライアンスには、次の物理的寸法が適用されます。

- 高さ：8.64 cm（3.40 インチ）
- 幅：レールの取り付け有無によらず 48.24 cm（18.99 インチ）
- 奥行：72.06 cm（28.40 インチ）
- 重量：最大 26.76 kg（59 ポンド）

Cisco IronPort M160 セキュリティ管理アプライアンスには、次の物理的寸法が適用されます。

- 高さ：4.20 cm（1.68 インチ）
- 幅：レールを取り付けて 48.26 cm（19.00 インチ）（レールを取り付けない場合は 17.5 インチ）
- 奥行：57.60 cm（22.70 インチ）
- 重量：最大 7.80 kg（21.6 ポンド）

セキュリティ管理アプライアンスと電子メール 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電子メール セキュリティ アプライアンスの統合の詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』の「Cisco IronPort M-Series Security Management Appliance」の章を参照してください。（「M シリーズ アプライアンス」はセキュリティ管理アプライアンスの別の表現です）。

中央集中型管理とセキュリティ管理アプライアンス

セキュリティ管理アプライアンスをクラスタに配置することはできません。ただし、クラスタ化された電子メール 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、外部スパム隔離にメッセージを保存できます。

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　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」（P.2-2）を参照してください。

ステップ 2　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。「設置計画」（P.2-4）を参照してください。

ステップ 3　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」（P.2-6）を参照してください。

ステップ 4　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」（P.2-6）を参照してください。

ステップ 5　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」（P.2-7）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

この章の手順を実行する前に、アプライアンスに付属の『*Cisco IronPort M-Series Quickstart Guide*』に記載された手順を実行してください。

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

出荷時に割り当てられた管理ポートの 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 [Management Appliance] > [Network] > [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。

- ネットワークのデフォルト 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、付録 B「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 Cisco IronPort アプライアンスの間でファイアウォールを稼働しているネットワークの場合は、Cisco IronPort 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、付録 C「ファイアウォール情報」を参照してください。

（注）　電子メール セキュリティ アプライアンスとの間で電子メール メッセージを送受信するには、常にセキュリティ管理アプライアンスで同じ IP アドレスを使用してください。詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』の「Mail Flow and the IronPort M-Series Appliance」を参照してください。

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、付録 B「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。

表 2-4　システム セットアップ ワークシート

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	システム時刻		NTP サーバ（IP アドレスまたはホスト名）：
3	admin パスワード		「admin」アカウントの新しいパスワードを選択：
4	AutoSupport		Cisco IronPort AutoSupport をイネーブルにするかどうか。 ___ はい ___ いいえ
5	ホスト名		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

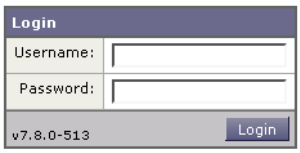
セキュリティ管理アプライアンスへのアクセス

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。

グラフィカル ユーザ インターフェイスへのアクセス

ステップ 1　セキュリティ管理アプライアンス上のグラフィカル ユーザ インターフェイスにアクセスするには、Web ブラウザを開き、IP アドレス テキスト フィールドに **192.168.42.42** と入力します。

ログイン画面が表示されます。



ステップ 2　出荷時に割り当てられた次のユーザ名とパスワードを、対応するテキスト フィールドに入力し、セキュリティ管理アプライアンスにログインします。

- ユーザ名：**admin**

- パスワード：**ironport**

（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」（P.12-24）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 Web インターフェイスへのアクセス

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 Cisco IronPort 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。イネーブルにすると、Cisco IronPort スパム隔離 HTTPS インターフェイスは、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 [Management Appliance] > [Network] > [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 admin Web インターフェイスにアクセスし、同じブラウザでポート 83 の HTTPS を介して Cisco IronPort Spam Quarantine エンド ユーザ Web インターフェイスにアクセスした場合、admin 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。

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。サポートされるブラウザには、次のものが含まれます。

- Internet Explorer 8.0 および 7.0
- Safari 4.0
- Firefox 3.5x および 3.0x

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。

（注）　GUI へのアクセス時には、複数のブラウザ ウィンドウまたはタブを同時に使用して、セキュリティ管理アプライアンスに変更を行わないように注意してください。GUI セッションと CLI セッションを同時に使用しないてください。同時に使用すると、予期しない動作が発生し、サポート対象外になります。

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」（P.13-59）を参照してください。
- GUI ウィンドウの右上にある [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）。

セキュリティ管理アプライアンスのコマンドライン インターフェイスへのアクセス

セキュリティ管理アプライアンス上のコマンドライン インターフェイス（CLI）には、すべての Cisco IronPort 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一覧については、『*Cisco IronPort AsyncOS CLI Reference Guide*』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」（P.2-6）のすべてのタスクを実行します。

警告　**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。

警告　**セキュリティ管理アプライアンスは、管理ポートにデフォルトの IP アドレス 192.168.42.42 が設定された状態で出荷されます。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。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。

セッション 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」（P.12-24）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

システム セットアップ ウィザードでは、次の設定作業が順に示されます。

ステップ 1　エンド ユーザ ライセンス契約書の確認

ステップ 2　次に示すシステム設定の実行：

- 通知設定と AutoSupport
- システム時刻設定
- admin パスワード

ステップ 3　次に示すネットワーク設定の実行：

- 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 4　設定の確認

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。[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。

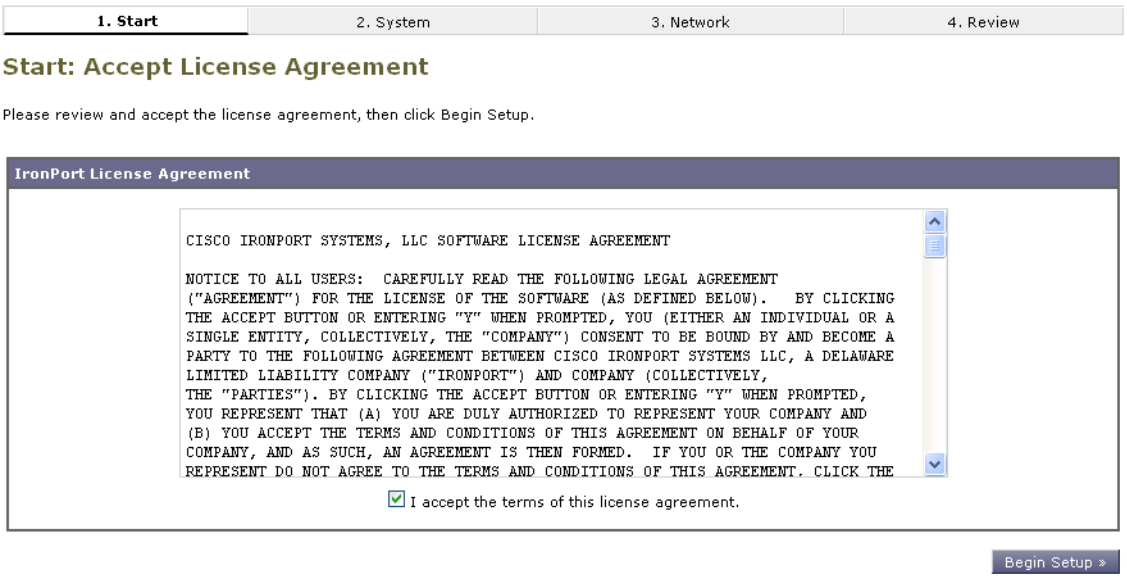
システム セットアップ ウィザードの起動

ウィザードを起動するには、「グラフィカル ユーザ インターフェイスへのアクセス」（P.2-8）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、[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（[Management Appliance] > [System Administration] > [System Setup Wizard]）。

エンド ユーザ ライセンス契約書を確認します。

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、[Begin Setup] をクリックして続行します。

図 2-2　　ライセンス契約書の確認



システムの設定

システム セットアップ ウィザードの設定を開始すると、[System Configuration] ページが表示されます。このページでは、システム設定を実行できます。

図 2-3　　[System Configuration] ページでのシステム設定の実行

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」（P.13-30）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時間帯を設定して、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、手動で設定するか、ネットワーク タイム プロトコル（NTP）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もできます。デフォルトでは、Cisco IronPort Systems のタイム サーバ（time.IronPort.com）が、セキュリティ管理アプライアンス上で時刻を同期するエントリとして追加されます。NTP サーバのホスト名を入力し、[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」（P.13-46）を参照してください。

（注） レポートのデータを収集すると、セキュリティ管理アプライアンスによってデータにタイム スタンプが適用されます。タイム スタンプは、「システム時刻の設定」（P.13-46）の手順で実装された設定を使用して適用されます。
セキュリティ管理アプライアンスがデータを収集する方法の詳細については、「セキュリティ アプライアンスによるレポート用データの収集方法」（P.3-2）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を変更する必要があります。新しいパスワードは 6 文字以上の長さである必要があります。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

Cisco IronPort AutoSupport 機能（デフォルトでイネーブル）で、セキュリティ管理アプライアンスに関する問題を Cisco IronPort 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 IronPort AutoSupport」（P.13-32）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。

図 2-4　　ネットワーク設定の実行

（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 システム設定値の設定」（P.13-41）を参照してください。

（注）　アプライアンスでは、着信接続にのための 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、[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 [Previous] をクリックし、情報を編集します。

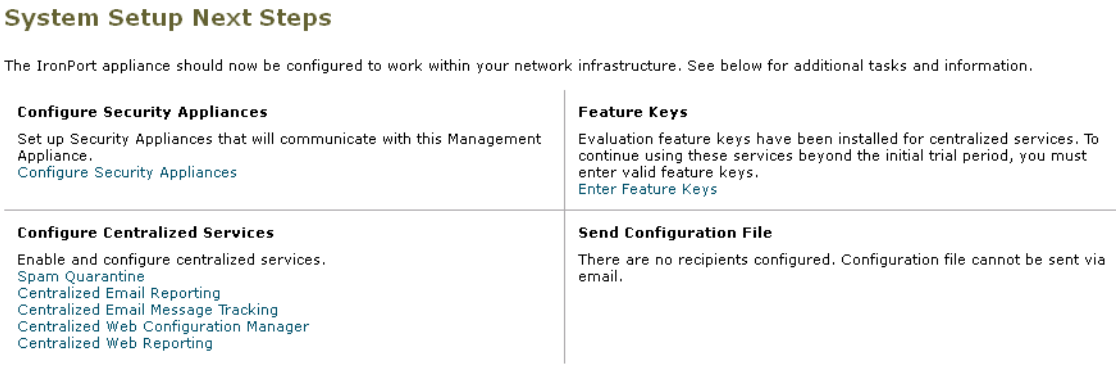
図 2-5　　設定の確認

情報を確認した後、[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 [Install] をクリックします。

次の手順

システム セットアップ ウィザードによって セキュリティ管理アプライアンスに設定が正しくインストールされると、[System Setup Next Steps] ページが表示されます。

図 2-6　　システム セットアップ：次の手順



[System Setup Next Steps] ページのいずれかのリンクをクリックして、Cisco IronPort アプライアンスの設定を続行します。

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。

設定およびトラブルシューティングを容易にするために、「ソリューション導入の概要」（P.2-1）で説明するプロセスに従うことを推奨します。

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」（P.2-2）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、[Add Web セキュリティ アプライアンス] 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 電子メール 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。

[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。[Connection Established?] カラムは、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。

- 「管理対象の各電子メール 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」（P.4-3）
- 「管理対象の各電子メール 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」（P.6-3）
- 「管理対象の各電子メール 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」（P.7-7）
- 「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」（P.5-4）
- 「Web セキュリティ アプライアンスの追加と Configuration Master のバージョンとの関連付け」（P.8-5）

管理対象アプライアンスの編集と削除

管理対象アプライアンスを セキュリティ管理アプライアンスに追加後、設定の編集または削除が必要になることがあります。

管理対象アプライアンスの編集

管理対象アプライアンスの設定を編集するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択します。

ステップ 2　[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 3　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）。電子メール 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 4　[Submit] をクリックして、ページ上の変更を送信し、[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削除

管理対象アプライアンスのリストから Cisco IronPort アプライアンスを削除するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択します。

ステップ 2　[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 3　確認のダイアログボックスで [Delete] をクリックします。

ステップ 4　[Submit] をクリックし、[Commit Changes] をクリックして変更を保存します。

セキュリティ管理アプライアンスでのサービスの設定

セキュリティ管理アプライアンスで 1 つまたは複数のセキュリティ サービスを設定し、使用するには、次の情報を参照してください。

電子メール セキュリティ サービス：

- 第 4 章「中央集中型電子メール セキュリティ レポーティングの使用」
- 第 6 章「電子メール メッセージのトラッキング」
- 第 7 章「Cisco IronPort スパム隔離の管理」

Web セキュリティ サービス：

- 第 5 章「中央集中型 Web レポーティングの使用方法」
- 第 8 章「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

セキュリティ管理アプライアンス GUI で設定を変更する場合、[Commit Changes] ボタンをクリックして、その変更を明示的に確定する必要があります。変更を行わなかった場合、[Commit Changes] の代わりに [No Changes] が表示されます。

図 2-7　　[Commit Changes] ボタン

[Commit Changes] をクリックすると、コメントの追加と変更の確定、最新の確定以降に行ったすべての変更の破棄、またはキャンセルを行うことができるページが表示されます。変更が送信されると、[Commit Changes] の色がオレンジに変化します。

変更の破棄

変更をコミットせずにキャンセルするには、[Commit Changes] ボタンをクリックしてから、[Abandon Changes] をクリックします。