CHAPTER 3

アプライアンスの設定

この章は、次の項で構成されています。

アプライアンスの設定の概要

Security Management アプライアンスでシステム セットアップ ウィザードを実行後は、Security Management アプライアンスおよびその他の Cisco IronPort アプライアンスを設定し、それらが通信できるようにする必要があります。

Cisco IronPort アプライアンスを設定するには、次の手順を実行します。

ステップ 1 **Web セキュリティ アプライアンス。**ネットワーキング、認可、およびセキュリティ サービスを設定し、ポリシーを設定してテストします。『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

ステップ 2 **Security Management アプライアンス。**管理サービスをイネーブルにします。その他の Cisco IronPort アプライアンスを管理する Security Management アプライアンスで、サービスをイネーブルにする必要があります。次のサービスを 1 つ以上イネーブルにできます。

- 電子メールおよび Web 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
- 電子メール アプライアンスの中央集中型トラッキング
- （電子メール用）Cisco IronPort スパム検疫
- （Web 用）Cisco IronPort 中央集中型コンフィギュレーション マネージャ

「Security Management アプライアンスでのサービスのイネーブル化」（P.3-3）を参照してください。

（注） アプライアンスで発生した Web イベント数をレポートするためのカウンタが、Web セキュリティ アプライアンスに追加されました。Email Security アプライアンスには、発生した電子メール イベント数をレポートするためのカウンタが追加されました。これで、[Management Appliance] > [Centralized Services] によって、Security Management アプライアンスで電子メール カウンタと Web カウンタの両方が中央集中化されます。電子メール カウンタと Web カウンタは、Security Management アプライアンスの中央集中型レポーティング ディスク領域を共有します。中央集中型レポーティングだけをオンにすると、電子メール カウンタがすべての領域を使用します。反対に、中央集中型 Web レポーティングだけをオンにすると、Web カウンタがすべてのディスク領域を使用します。両方をオンにすると、電子メールと Web レポーティングによって領域が共有されます。領域は、先着順に割り当てられます。この時点では、電子メール カテゴリと Web カテゴリで中央集中型レポーティング ディスク領域を共有する方法がありません。

ステップ 3　**Security Management アプライアンス。**管理対象の Email Security アプライアンスおよび Web セキュリティ アプライアンスを追加します。Security Management アプライアンスで [Management Appliance] > [Centralized Services] > [Security Appliances] を選択し、Cisco IronPort アプライアンスを追加します。「管理対象アプライアンスの追加」（P.3-11）を参照してください。

ステップ 4　**Email Security アプライアンス。**管理対象の Web セキュリティ アプライアンスおよび Email Security アプライアンスで、モニタリング サービスとセキュリティ サービスを設定します。第 9 章「システム ステータスのモニタリング」を参照してください。

Security Management アプライアンスでのサービスのイネーブル化

Security Management アプライアンスを使用して Email Security アプライアンスおよび Web セキュリティ アプライアンスを管理するには、Security Management アプライアンス上で適切なサービスをイネーブルにする必要があります。

中央集中型レポーティングおよび中央集中型トラッキングのため、または外部 Cisco IronPort スパム検疫として Security Management アプライアンスを使用するには、まず Email Security アプライアンス上にモニタリング サービスを設定する必要があります。

（注） Security Management アプライアンス上でサービスをイネーブルにした後、適切な Cisco IronPort アプライアンスを管理対象アプライアンスとして追加していない場合は、追加する必要があります。詳細については、「管理対象アプライアンスの追加」（P.3-11）を参照してください。

Security Management アプライアンス上で電子メール セキュリティ サービスまたは Web セキュリティ サービスのいずれかをイネーブルにする場合は、次の項を参照してください。

- 「Security Management アプライアンスでの中央集中型電子メール レポーティングのイネーブル化とディセーブル化」（P.3-3）
- 「Security Management アプライアンスでの中央集中型 Web レポーティングのイネーブル化とディセーブル化」（P.3-5）
- 「Security Management アプライアンスでの中央集中型電子メール トラッキングのイネーブル化とディセーブル化」（P.3-6）

Security Management アプライアンスでの中央集中型電子メール レポーティングのイネーブル化とディセーブル化

（注） 中央集中型電子メール レポーティングをイネーブルにする前に、十分なディスク領域がサービスに割り当てられていることを確認します。「ディスク使用量の管理」（P.12-123）を参照してください。Security Management アプライアンス

上で電子メール レポーティングをイネーブルにすると、モニタリング サービスを使用して、電子メール トラフィックのレポートを作成し、メッセージ ルーティングを追跡し、また疑わしいメッセージとスパム メッセージを外部 Cisco IronPort スパム検疫に配信することができます。Email Security アプライアンスのモニタリング サービスを設定する方法の詳細については、『*Cisco IronPort AsyncOS for Email User Guide*』を参照してください。Security Management アプライアンスでのモニタリング サービスの詳細については、第 9 章「システム ステータスのモニタリング」を参照してください。

Security Management アプライアンスで中央集中型電子メール レポーティングをイネーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Reporting] を選択します。

ステップ 2　[Email Reporting Service] セクションで [Enable] をクリックします。

ステップ 3　システム セットアップ ウィザードを実行してから初めて中央集中型電子メール レポーティングをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[Accept] をクリックします。

[Centralized Reporting] ページが表示されます。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

中央集中型電子メール レポーティングをイネーブルにすると、管理対象の Email Security アプライアンスの電子メール レポーティング グループを作成できます。「電子メール レポーティング グループの作成」（P.4-4）を参照してください。中央集中型電子メール レポーティングの使用方法の詳細については、第 4 章「中央集中型電子メール レポーティングの使用」を参照してください。

中央集中型電子メール レポーティングのディセーブル化

Security Management アプライアンスで中央集中型電子メール レポーティングをディセーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Reporting] を選択します。

ステップ 2　[Reporting Services] セクションで [Edit Settings] をクリックします。

ステップ 3　[Enable Centralized Reporting Service] チェックボックスをオフにします。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Security Management アプライアンスでの中央集中型 Web レポーティングのイネーブル化とディセーブル化

（注）　中央集中型 Web レポーティングをイネーブルにする前に、十分なディスク領域がサービスに割り当てられていることを確認します。「ディスク使用量の管理」（P.12-123）を参照してください。

Security Management アプライアンス上で Web レポーティングをイネーブルにすると、サービスの表示とモニタ、および Web トラフィックのレポートを実行できます。Email Security アプライアンスでモニタリング サービスを設定する方法の詳細については、『*Cisco IronPort AsyncOS for Security Management ユーザ ガイド*』を参照してください。Security Management アプライアンスでモニタリング サービスを設定する方法の詳細については、第 9 章「システム ステータスのモニタリング」を参照してください。

Security Management アプライアンスで中央集中型 Web レポーティングをイネーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] を選択します。

ステップ 2　[Web Reporting Service] セクションで [Enable] をクリックします。

ステップ 3　システム セットアップ ウィザードを実行してから初めて中央集中型 Web レポーティングをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[Accept] をクリックします。

[Centralized Web Reporting] ページが表示されます。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Web の中央集中型レポーティングをイネーブルにすると、Security Management アプライアンスのページから Web アプライアンスを追加するか、または [Disk Management] ページからディスク領域を適切に割り当てることができます。さらに、Web レポーティングを設定し、Web レポートのユーザ名とロールを表示するか、または匿名表示することができます。Web レポートの設定の詳細については、「中央集中型 Web レポーティングの設定」（P.5-3）を参照してください。

これらの項目の詳細については、「管理対象アプライアンスの追加」（P.3-11）または「ディスク使用量の管理」（P.12-123）を参照してください。

中央集中型 Web レポーティングのディセーブル化

Security Management アプライアンスで中央集中型 Web レポーティングをディセーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] を選択します。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　[Web Reporting Service] セクションで [Enable Centralized Reporting Service] チェックボックスをオフにします。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Security Management アプライアンスでの中央集中型電子メール トラッキングのイネーブル化とディセーブル化

Security Management アプライアンス上で電子メール メッセージ トラッキングをイネーブルにすると、モニタリング サービスを使用して、電子メール トラフィックのレポートを作成し、メッセージ ルーティングを追跡し、また疑わしいメッセージとスパム メッセージを外部 Cisco IronPort スパム検疫に配信することができます。Email Security アプライアンスのモニタリング サービスを設定する方法の詳細については、『*Cisco IronPort AsyncOS for Email User Guide*』を

参照してください。Security Management アプライアンスでのモニタリング サービスの詳細については、第 9 章「システム ステータスのモニタリング」を参照してください。

Security Management アプライアンスで中央集中型電子メール トラッキングをイネーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスの場合：

a. [Management Appliance] > [Centralized Services] > [Email] > [Centralized Message Tracking] を選択します。

b. [Message Tracking Service] セクションで [Enable] をクリックします。

c. システム セットアップ ウィザードを実行してから初めて中央集中型電子メッセージ トラッキングをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[Accept] をクリックします。

[Centralized Message Tracking] ページが表示されます。中央集中型電子メール トラッキングをイネーブルにすると、[Message Tracking Service] ボックスの右側のカラムに「Enable」と表示されます。

d. Security Management アプライアンスでの変更を**送信**し、確定します。

ステップ 2　Email Security アプライアンスの場合：

a. 電子メール メッセージへの添付ファイル名を検索および記録できるようにする場合は、次の点に注意してください。

少なくとも 1 つの受信コンテンツ フィルタまたは本文スキャン機能が Email Security アプライアンスで設定され、イネーブルになっていることを確認します。コンテンツ フィルタおよび本文スキャンの詳細については、『*Cisco IronPort AsyncOS for Email Security Advanced Configuration Guide*』を参照してください。（この機能は AsyncOS Release 7.5 で導入されました）。

b. [Security Services] > [Message Tracking] で、[Edit Settings] をクリックして [Centralized Tracking] を選択します。

c. Email Security アプライアンスでの変更を送信し、確定します。

中央集中型トラッキングの使用に関する詳細については、第 6 章「電子メール メッセージのトラッキング」を参照してください。

中央集中型電子メール トラッキングのディセーブル化

Security Management アプライアンスで中央集中型電子メール トラッキングをディセーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Message Tracking] を選択します。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　[Enable Centralized Message Tracking Service] チェックボックスをオフにします。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Security Management アプライアンスでの Cisco IronPort スパム検疫のイネーブル化とディセーブル化

（注）　Security Management アプライアンス上で Cisco IronPort スパム検疫をイネーブルにすると、モニタリング サービスを使用して、電子メール トラフィックのレポートを作成し、メッセージ ルーティングを追跡し、また疑わしいメッセージとスパム メッセージを外部 Cisco IronPort スパム検疫に配信することができます。Email Security アプライアンスのモニタリング サービスを設定する方法の詳細については、『*Cisco IronPort AsyncOS for Email User Guide*』を参照してください。Security Management アプライアンスでのモニタリング サービスの詳細については、第 9 章「システム ステータスのモニタリング」を参照してください。

Security Management アプライアンスで Cisco IronPort スパム検疫をイネーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Email] > [Spam Quarantine] を選択します。

[Spam Quarantine] ページが表示されます。

ステップ 2　[Enable] をクリックします。

ステップ 3　システム セットアップ ウィザードを実行してから初めて Cisco IronPort スパム検疫をイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[Accept] をクリックします。

[Edit Cisco IronPort Spam Quarantine] ページが表示されます。

ステップ 4　（任意）スパム検疫設定を編集し、検疫へのアクセスを設定します。詳細については、「IronPort スパム検疫の設定」（P.7-3）を参照してください。

ステップ 5　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Cisco IronPort スパム検疫のディセーブル化

Security Management アプライアンスで Cisco IronPort スパム検疫をディセーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Email] > [Spam Quarantine] を選択します。

[Spam Quarantine] ページが表示されます。

ステップ 2　[Cisco IronPort Spam Quarantine Settings] セクションで [Edit Settings] をクリックします。

ステップ 3　[Enable Cisco IronPort Spam Quarantine] チェックボックスをオフにします。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Security Management アプライアンスでの中央集中型コンフィギュレーション マネージャのイネーブル化とディセーブル化

Security Management アプライアンスで Cisco IronPort 中央集中型コンフィギュレーション マネージャをイネーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Configuration Manager] を選択します。

ステップ 2　[Centralized Configuration Manager] ページで [Enable] をクリックします。

ステップ 3　システム セットアップ ウィザードを実行してから初めて Cisco IronPort 中央集中型コンフィギュレーション マネージャをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[Accept] をクリックします。

[Centralized Configuration Manager] ページが表示され、サービスがイネーブルになっているのが示されます。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Cisco IronPort 中央集中型コンフィギュレーション マネージャのディセーブル化

Security Management アプライアンスで Cisco IronPort 中央集中型コンフィギュレーション マネージャをディセーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Configuration Manager] を選択します。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　[Enable Centralized Configuration Manager Service] チェックボックスをオフにします。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

管理対象アプライアンスの追加

Security Management アプライアンスでモニタリング サービスをイネーブルにした後、管理対象のアプライアンスの接続情報を追加する必要があります。「SMA 互換性マトリクス」（P.2-33）の定義に従って、サポートされる電子メールおよび Web セキュリティ アプライアンスに接続できます。

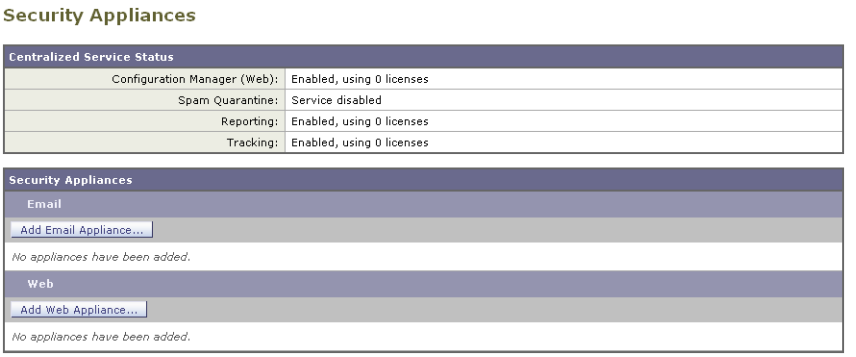
リモート アプライアンスを追加すると、Security Management アプライアンスによって、リモート アプライアンスの製品名と追加するアプライアンスのタイプが比較されます。たとえば、[Add Web Security Appliance] ページを使用してアプライアンスを追加すると、そのアプライアンスは Web セキュリティ アプライアンスであって Email Security アプライアンスではないことを確認するために、Security Management アプライアンスによってリモート アプライアンスの製品名がチェックされます。また、Security Management アプライアンスは、リモート アプライアンスのモニタリング サービスもチェックして、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。

管理対象アプライアンスを Security Management アプライアンスに追加するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択します。

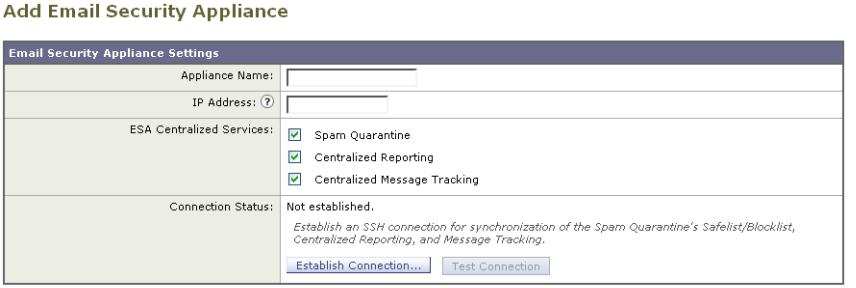
[Security Appliances] ページが表示されます。

図 3-1　[Security Appliances] ページ



ステップ 2　[Add Email Appliance] ボタンをクリックして、[Add Email Security Appliance] ページを表示します。

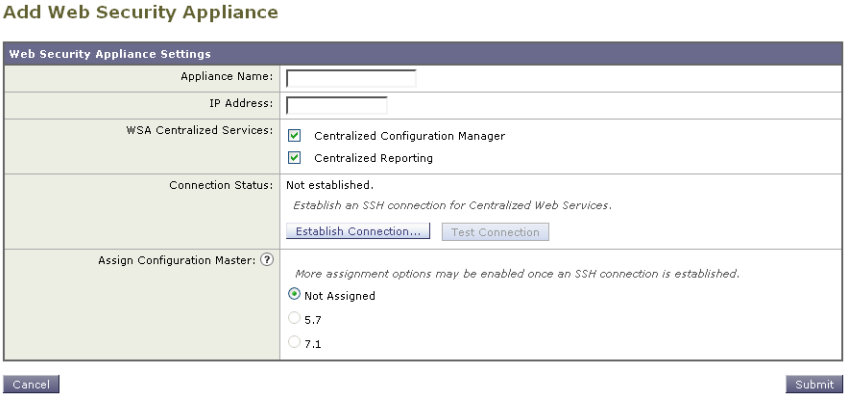
図 3-2　[Add Email Security Appliance] ページ



または

[Add Web Appliance] ボタンをクリックして、[Add Web Security Appliance] ページを表示します。

図 3-3　[Add Web Security Appliance] ページ



ステップ 3　[Appliance Name] テキスト フィールドおよび [IP Address] テキスト フィールドに、Cisco IronPort アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注）　[IP Address] テキスト フィールドに DNS 名を入力した場合でも、[Submit] をクリックすると、すぐに IP アドレスに解決されます。

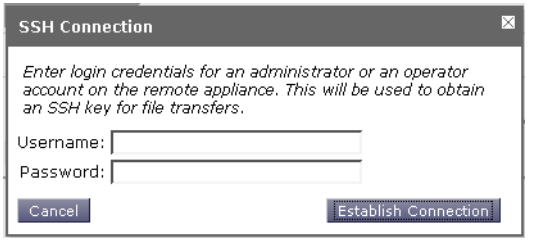
ステップ 4　Cisco IronPort アプライアンスを管理する際に使用するサービスを選択します。

（注）　Security Management アプライアンスでイネーブルにしたサービスのみ選択できます。詳細については、「Security Management アプライアンスでのサービスのイネーブル化」（P.3-3）を参照してください。

ステップ 5　[Establish Connection] をクリックします。

[SSH Connection] ダイアログボックスが表示されます。

図 3-4　[SSH Connection] ダイアログボックス



ステップ 6　[Username] および [Password] テキスト フィールドに、Cisco IronPort アプライアンス上の管理者アカウントのログイン資格情報を入力します。

（注）　ログイン資格情報を入力すると、Security Management アプライアンスからリモート アプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は、Security Management アプライアンスには保存されません。

ステップ 7　[Establish Connection] をクリックして、モニタリング サービス用の接続を確立します。

ステップ 8　[Test Connection] をクリックして、リモート アプライアンスのモニタリング サービスが正しく設定され、互換性があることを確認します。

ステップ 9　Web セキュリティ アプライアンスを追加する場合は、アプライアンスを割り当てる Configuration Master を選択します。

各 Configuration Master には、Web セキュリティ アプライアンスのバージョンごとの設定が含まれています。Security Management アプライアンスは、互換性のある AsyncOS のバージョンを実行する Web セキュリティ アプライアンスにのみ Configuration Master を公開できます（たとえば、Web セキュリティ アプ

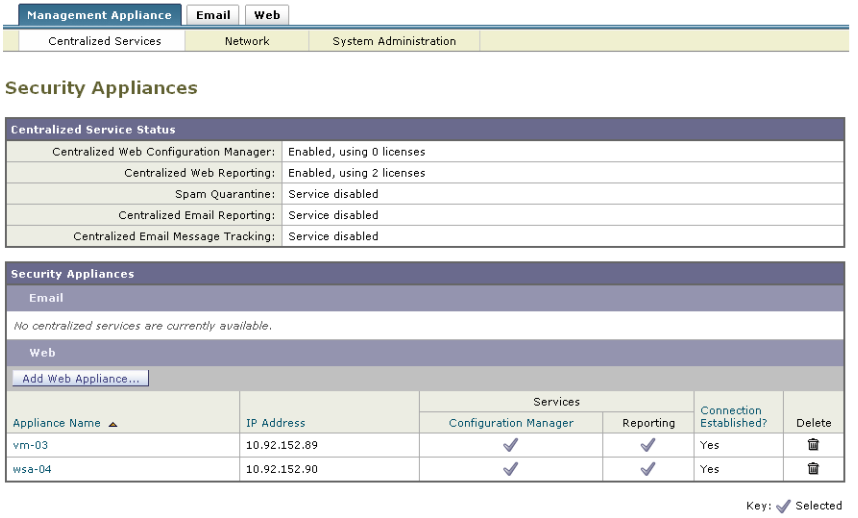
ライアンスが AsyncOS 6.3 を実行している場合、Configuration Master として 6.3.0 を選択します）。[Web] > [Utilities] > [Configuration Masters] を選択して、後で Web セキュリティ アプライアンスを割り当てることもできます（「Web セキュリティ アプライアンスと Configuration Master の関連付け」（P.8-8）を参照）。

Configuration Master および Web セキュリティ アプライアンスの管理の詳細については、第 8 章「Web セキュリティ アプライアンスの管理」を参照してください。

ステップ 10　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

[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。チェック マークは、イネーブルになっているサービスを示し、[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。

図 3-5　[Security Appliances] ページの管理対象アプライアンス



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 Security Management 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　Security Management 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）。Email Security 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での変更を送信し、[Commit Changes] をクリックして変更を確定します。

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　Security Management 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確定します。

レポートの概要

すべての Cisco IronPort アプライアンスには、Email Security アプライアンス、Web セキュリティ アプライアンス、および Security Management アプライアンスに共通する基本概念、設定、およびページがあります。レポート情報には、次の内容があります。

- 「レポーティング オプション」（P.3-16）
- 「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.3-17）
- 「[Interactive Report] ページ」（P.3-18）
- 「インタラクティブ レポートの時間範囲の選択」（P.3-18）
- 「Security Management アプライアンスのレポート フィルタ」（P.3-19）
- 「レポート データの印刷とエクスポート」（P.3-21）

レポーティング オプション

データを表示および保存するための多くのオプションが用意されています。

- インタラクティブ レポート ページを表示およびカスタマイズし、表示しているレポートの PDF を生成する

- いくつかの事前定義されたレポート タイプの PDF または CSV ファイルを随時オンデマンドで生成する
- 事前定義された PDF または CSV レポートの自動作成を指定した時間にスケジュールする
- スケジュールされたレポートまたはオンデマンド レポートを、選択した受信者に電子メールで送る
- スケジュールされたレポートまたはオンデマンド レポートのアーカイブ済みのコピーを、システムから削除されるまで表示する

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

Security Management アプライアンスは、約 15 分ごとにすべての管理対象アプライアンスからすべてのレポートのデータを取得し、これらのアプライアンスからのデータを集約します。アプライアンスによっては、Security Management アプライアンスのレポート データに含める一部のメッセージで、多少の時間がかかることがあります。データの詳細については、[System Status] ページを確認してください。

（注）　Security Management アプライアンスは、レポートのデータを収集する際に、Security Management アプライアンス上で時間設定を行った際に設定した情報からタイム スタンプを適用します。Security Management アプライアンス上の時間設定の詳細については、「システム時刻の設定」（P.12-105）を参照してください。

レポート データを保存する方法

すべてのアプライアンスには、レポート データが保存されています。表 3-1 は、各アプライアンスがデータを保存する時間間隔を示しています。

表 3-1　Email Security アプライアンスおよび Web セキュリティ アプライアンスのレポート データ ストレージ

	毎分	毎時	毎日	毎週	毎月	毎年
C-Series または S-Series 上でのローカル レポート	•	•	•	•	•	

表 3-1　Email Security アプライアンスおよび Web セキュリティ アプライアンスのレポート データ ストレージ （続き）

C-Series または S-Series 上での中央集中型レポート	•	•	•	•		
M-Series		•	•	•	•	•

[Interactive Report] ページ

アプライアンスのすべてのレポート ページは、インタラクティブ レポート ページです。このため、システム内の 1 つまたはすべての管理対象 Email Security アプライアンスおよび Web セキュリティ アプライアンスの情報をモニタできます。インタラクティブ レポート ページでは、異なる時間範囲の中央集中型トラッキングおよびレポート データを表示でき、ページごとに表示するカラムのタイプを指定できます。

各アプライアンスのインタラクティブ レポート ページの詳細については、次の項を参照してください。

- 「[Email Reporting] タブの使用」（P.4-6）
- 「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）

インタラクティブ レポートの時間範囲の選択

ほとんどのインタラクティブ レポート ページでは、含まれるデータの時間範囲を選択できます。選択した時間範囲は、[Time Range] メニューで異なる値を選択するまで、すべてのレポート ページを通して使用されます。

使用可能な時間範囲オプションは、アプライアンスごとに異なり、また Security Management アプライアンス上の電子メール レポートおよび Web レポートによって異なります。

表 3-2　レポートの時間範囲オプション

オプション	説明	SMA 電子メール レポート	ESA	SMA Web レポート	WSA
Hour	過去 60 分間と最大 5 分間の延長時間		•		•
Day	過去 24 時間	•	•	•	•
Week	当日の経過時間を含む、過去 7 日間	•	•	•	•
30 days	当日の経過時間を含む、過去 30 日間	•	•	•	•
90 days	当日の経過時間を含む、過去 90 日間	•	•	•	
Year	過去 12 ヵ月間と当月の経過した日数	•			
Yesterday	アプライアンスで定義された時間帯を使用した、前日の 24 時間（00:00 ～ 23:59）	•	•	•	•
Previous Calendar Month	月の最初の日の 00:00 から月の最後の日の 23:59 まで	•	•	•	
Custom Range	ユーザ指定の時間範囲。 開始日時と終了日時を選択する場合は、このオプションを選択します。	•	•	•	•

（注）　インタラクティブ レポート ページの時間範囲は、グリニッジ標準時（GMT）オフセットで表示されます。たとえば、太平洋標準時は、GMT + 7 時間（GMT + 07:00）です。

Security Management アプライアンスのレポート フィルタ

AsyncOS には、前年をカバーするレポート（[Last Year] レポート）のデータの集約を制限できるレポート フィルタがあります。1 ヵ月分に大量の一意のエントリが存在することで、集約されたレポートのパフォーマンスが低下する場合に

は、これらのフィルタを使用できます。これらのフィルタにより、レポート内の詳細、個々の IP、ドメイン、またはユーザ データを制限できます。概要レポートおよびサマリー情報は、引き続きすべてのレポートで利用できます。

CLI で **reportingconfig -> filters** メニューを使用すると、1 つ以上のレポート フィルタをイネーブルにできます。変更を有効にするには、変更を確定する必要があります。

- [IP Connection Level Detail]。このフィルタをイネーブルにすると、Security Management アプライアンスは、個々の IP アドレスに関する情報を記録しません。このフィルタは、攻撃による大量の受信 IP アドレスを処理するシステムに適しています。

  このフィルタは、次の [Last Year] レポートに影響を与えます。

  - Sender Profile for Incoming Mail
  - IP Addresses for Incoming Mail
  - IP Addresses for Outgoing Senders

- [User Detail]。このフィルタをイネーブルにすると、Security Management アプライアンスは、電子メールを送受信する個々のユーザ、およびユーザの電子メールに適用されるコンテンツ フィルタに関する情報を記録しません。このフィルタは、何百万もの内部ユーザの電子メールを処理するアプライアンス、またはシステムが受信者のアドレスを検証しない場合に適しています。

  このフィルタは、次の [Last Year] レポートに影響を与えます。

  - Internal Users
  - Internal User Details
  - IP Addresses for Outgoing Senders
  - Content Filters

- [Mail Traffic Detail]。このフィルタをイネーブルにすると、Security Management アプライアンスは、アプライアンスがモニタする個々のドメインおよびネットワークに関する情報を記録しません。このフィルタは、有効な着信または発信ドメインの数が数千万の単位で測定される場合に適しています。

  このフィルタは、次の [Last Year] レポートに影響を与えます。

  - Domains for Incoming Mail
  - Sender Profile for Incoming Mail

- Internal User Details
- Domains for Outgoing Senders

（注）　過去 1 時間の最新のレポート データを表示するには、個々のアプライアンスにログインして、そこでデータを表示する必要があります。

レポート データの印刷とエクスポート

ページ右上の [Printable PDF] リンクをクリックすると、すべてのレポート ページを読みやすい印刷形式の PDF 版で生成できます。

さらに、[Export] リンクをクリックすると、グラフと他の raw データをカンマ区切り（CSV）形式でエクスポートできます。大部分のレポートでは、CSV 形式のスケジューリングを行うことができます。ただし、CSV 形式で拡張レポートをスケジュールすることはできません。

PDF レポートまたは CSV レポートを、その個々のレポートの特定のロケールでスケジュールすることができます。[Scheduled Reports] ページの言語ドロップダウン メニューでは、現在選択されているロケールおよび言語で PDF レポートを表示またはスケジュールすることができます。

（注）　Windows コンピュータ上で中国語、日本語、または韓国語で PDF を生成するには、該当するフォント パックを Adobe.com からダウンロードして、ローカル コンピュータにインストールする必要があります。

場合によっては、いくつかのレポート ページに、トップレベルのページからアクセスできる独自のサブレポートが複数含まれることがあります。たとえば、Email Security アプライアンスの [Incoming Mail] レポート ページでは、個々の IP アドレス、ドメイン、およびネットワーク オーナーの情報を表示できます。これらの各サブページには、[Incoming Mail] レポート ページからアクセスできます。

トップレベル ページ（この場合には [Incoming Mail] レポート ページ）の右上にある [Printable PDF] リンクをクリックすると、これらの各サブレポート ページの結果を、1 つの統合レポートに生成できます。

（注）　PDF への印刷の唯一の例外は、[Web Tracking] ページを使用している場合です。[Web Tracking] ページからは、[Printable Download] リンクを使用しないと印刷できません。このリンクでは、現在のページ、または最大 10,000 のトランザクションの PDF への出力、あるいは CSV ファイルへのすべてのデータの出力を選択できます。

レポート データのエクスポート

Security Management アプライアンスの大部分のレポート ページには、エクスポート リンクが表示されています。このリンクから、raw データをカンマ区切り（CSV）ファイルにエクスポートし、Microsoft Excel などのデータベース アプリケーションを使用してアクセスおよび処理できます。

エクスポートされた CSV データは、Security Management アプライアンスでの設定にかかわらず、すべてのメッセージ トラッキングおよびレポーティング データを GMT で示します。GMT 時間変換の目的は、アプライアンスとは独立してデータを使用できるようにすること、または複数の時間帯でアプライアンスからのデータを参照することです。

次の例は、Anti-Malware カテゴリ レポートの raw データ エクスポートのエントリであり、太平洋夏時間（PDT）が GMT - 7 時間で表示されています。

```
Begin Timestamp, End Timestamp, Begin Date, End Date, Name,
Transactions Monitored, Transactions Blocked, Transactions Detected

1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59
GMT, Adware, 525, 2100, 2625
```

表 3-3　raw データ エントリの表示

カテゴリ ヘッダー	値	説明
Begin Timestamp	1159772400.0	エポックから秒数によるクエリー開始時刻。
End Timestamp	1159858799.0	エポックから秒数によるクエリー終了時刻。
Begin Date	2006-10-02 07:00 GMT	クエリーの開始日。
End Date	2006-10-03 06:59 GMT	クエリーの終了日。
Name	Adware	マルウェア カテゴリの名前。

表 3-3　raw データ エントリの表示 （続き）

カテゴリ ヘッダー	値	説明
Transactions Monitored	525	モニタリングされたトランザクション数。
Transactions Blocked	2100	ブロックされたトランザクション数。
Transactions Detected	2625	トランザクションの合計数： 検出されたトランザクション数＋ブロックされたトランザクション数。

（注）　カテゴリ ヘッダーは、レポートのタイプごとに異なります。

ローカライズされた CSV データをエクスポートすると、ブラウザによっては見出しが正しく表示されない場合があります。これは、ブラウザによっては、ローカライズされたテキストに対して適切な文字セットが使用されない場合があることから発生します。この問題の回避策としては、ローカル マシンにファイルを保存し、[File] > [Open] を使用して任意の Web ブラウザでファイルを開きます。ファイルを開いたら、ローカライズされたテキストを表示するための文字セットを選択します。