CHAPTER 13

一般的な管理タスク

システム管理タスクのほとんどは、グラフィカル ユーザ インターフェイス（GUI）の [System Administration] メニューを使用して実行できます。ただし、一部のシステム管理機能は、コマンドライン インターフェイス（CLI）からのみ実行できます。

また、第 9 章「システム ステータスのモニタリング」で説明されているように、[Monitor] メニューでアプライアンスのステータス モニタリング機能を使用することができます。

（注） この章で説明する機能やコマンドの中には、ルーティングの優先順位に影響を及ぼすものがあります。詳細については、「IP アドレス、インターフェイス、およびルーティング」（P.B-3）を参照してください。

この章は、次の内容で構成されています。

機能キーでの作業

メイン セキュリティ管理アプライアンスで、GUI を使用して [Management Appliance] > [System Administration] > [Feature Keys] を選択して（またはコマンド ライン プロンプトから **featurekey** コマンドで）キーを入力し、関連する機能をイネーブルにします。

キーは、アプライアンスのシリアル番号に固有のものであり、またイネーブルする機能にも固有です。1 つのシステムのキーを、別のシステムで再利用することはできません。キーを間違って入力した場合は、エラー メッセージが生成されます。

Cisco IronPort カスタマー サポートは、システム上で特定の機能をイネーブルにするキーを提供する場合があります。

[Feature Keys] ページと [Feature Key Settings] ページの 2 つのページで、機能キーの機能が提供されます。

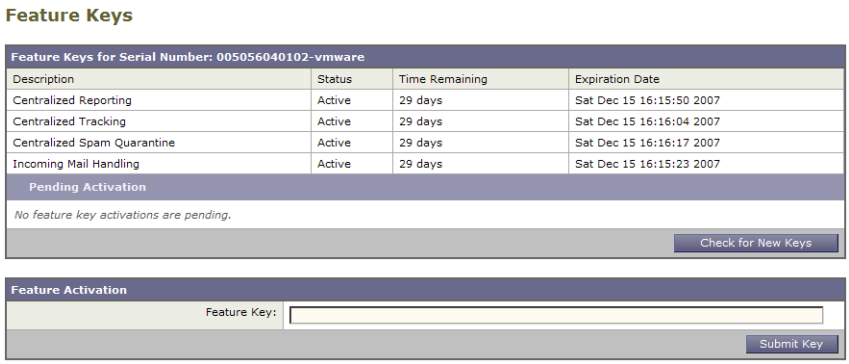
[Feature Keys] ページ

セキュリティ管理アプライアンスにログインし、[Management Appliance] > [System Administration] > [Feature Keys] を選択します。[Feature Keys] ページでは、次の作業を実行します。

- アプライアンスのアクティブな機能キーをすべて表示する。
- アクティベーションを保留中のすべての機能キーを表示する。
- 発行された新しいキーを検索する。
- 機能キーをインストールする。

[Feature Keys for Serial Number: <*Serial Number*>] セクションには、アプライアンスに対してイネーブルとなっている機能の一覧が表示されます。[Pending Activation] セクションには、アプライアンスに対して発行され、まだアクティベートされていない機能キーの一覧が表示されます。デフォルトでは、アプライアンスは、新しいキーを定期的に確認します。アプライアンス設定を変更すると、この動作を変更できます。さらに、[Check for New Keys] ボタンをクリックして、保留中のキーの一覧をリフレッシュできます。

図 13-1　[Feature Keys] ページ



新しい機能キーを手動で追加するには、[Feature Key] フィールドにキーを貼り付けるか、または入力し、[Submit Key] をクリックします。機能が追加されない場合は、エラー メッセージが表示されます（たとえば、キーが正しくない場合など）。それ以外の場合は、機能キーがリストに追加されます。

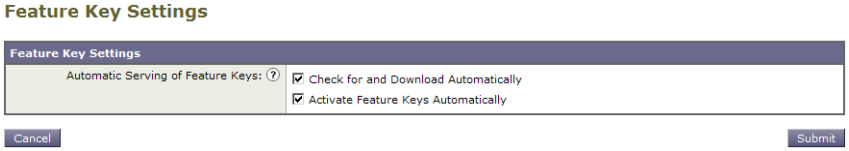
[Pending Activation] リストの新しい機能キーをアクティベートするには、そのキーを選択し（[Select] チェックボックスを選択）、[Activate Selected Keys] をクリックします。

新しいキーが発行されたときに、キーを自動的にダウンロードおよびインストールするように、アプライアンスを設定できます。この場合、[Pending Activation] リストは常に空白になります。

[Feature Key Settings] ページ

[Management Appliance] > [System Administration] > [Feature Key Settings] ページを使用して、アプライアンスが新しい機能キーがあるか確認し、ダウンロードするかどうか、またキーが自動的にアクティベートされるかどうかを制御します。

図 13-2　[Feature Key Settings] ページ



期限切れ機能キー

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、シスコ担当者または他のカスタマー サポート組織までご連絡ください。

CLI コマンドを使用したメンテナンス作業の実行

ここで説明する操作とコマンドを利用すると、セキュリティ管理アプライアンス上でメンテナンスに関連する作業を実行できます。ここでは、次の操作とコマンドについて説明します。

- **shutdown**
- **reboot**
- **suspend**
- **offline**
- **resume**
- **resetconfig**
- **version**

セキュリティ管理アプライアンスのシャットダウン

セキュリティ管理アプライアンスをシャットダウンするには、[Management Appliance] > [System Administration] > [Shutdown/Reboot] ページを使用するか、コマンドライン プロンプトで **shutdown** コマンドを使用します。

アプライアンスをシャットダウンすると、AsyncOS が終了し、アプライアンスの電源を安全にオフにできます。アプライアンスは、配信キューのメッセージを失わずに後で再起動できます。アプライアンスをシャットダウンする遅延値を入力する必要があります。デフォルト遅延値は 30 秒です。AsyncOS では、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が強制的に閉じられます。

セキュリティ管理アプライアンスのリブート

セキュリティ管理アプライアンスをリブートするには、GUI の [System Administration] メニューで利用可能な [Shutdown/Reboot] ページを使用するか、CLI で reboot コマンドを使用します。

アプライアンスをリブートすると、AsyncOS が再起動されるため、アプライアンスの電源を安全にオフにし、アプライアンスをリブートできます。アプライアンスをシャットダウンする遅延値を入力する必要があります。デフォルト遅延値は 30 秒です。AsyncOS では、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が強制的に閉じられます。アプライアンスを再起動しても、配信キューのメッセージは失われません。

セキュリティ管理アプライアンスをメンテナンス状態にする

システム メンテナンスを行う場合は、セキュリティ管理アプライアンスをオフライン状態にします。suspend および offline コマンドは、AsyncOS をオフライン状態にします。オフライン状態では、次のようになります。

- 着信電子メール接続は受け入れられません。
- 発信電子メール配信は停止されます。
- ログ転送は停止されます。
- CLI はアクセス可能のままになります。

オフライン状態にするアプライアンスの遅延値を入力する必要があります。デフォルト遅延値は 30 秒です。AsyncOS では、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が強制的に閉じられます。オープン中の接続がない場合は、すぐにオフライン状態になります。

（注）　**suspend** コマンドと **offline** コマンドの相違点は、**suspend** コマンドはマシンがリブートされた後でもその状態を保つことです。**suspend** コマンドを発行してからアプライアンスをリブートする場合は、**resume** コマンドを使用してシステムをオンライン状態に戻す必要があります。

関連項目：

- 『*Cisco IronPort AsyncOS for Email Security Advanced User Guide*』の「Suspending Email Delivery」、「Resuming Email Delivery」、「Suspending Receiving」、および「Resuming Receiving」

suspend および offline コマンド

```
mail3.example.com> suspend

Enter the number of seconds to wait before abruptly closing connections.
[30]> 45

Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.

mail3.example.com> offline

Enter the number of seconds to wait before abruptly closing connections.
[30]> 45
```

```
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
```

オフライン状態からの再開

resume コマンドは、**suspenddel** コマンドまたは **suspend** コマンドを使用した後に、AsyncOS を通常の動作状態に戻します。

resume コマンド

```
mail3.example.com> r
esume

Receiving resumed.
Mail delivery resumed.
mail3.example.com>
```

出荷時の初期状態へのリセット

アプライアンス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。[Management Appliance] > [System Administration] > [Configuration File] ページの [Reset Configuration] セクションの [Reset] ボタンか、**resetconfig** コマンドを使用すると、*すべての* AsyncOS 設定値が出荷時の初期状態にリセットされます。このコマンドは非常に破壊的であるため、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。設定のリセット後は、システム セットアップ ウィザードを実行することを推奨します。

（注） resetconfig コマンドは、アプライアンスがオフライン状態であるときにのみ機能します。**resetconfig** コマンドが完了すると、アプライアンスは自動的にオンライン状態に戻ります。**resetconfig** コマンドを実行する前に電子メールの送信が中断された場合は、**resetconfig** コマンドが完了したときに電子メールの送信が再試行されます。

警告 **resetconfig コマンドを実行すると、すべてのネットワーク設定が出荷時デフォルト値に戻ります。場合によっては、CLI から切断され、アプライアンスに接続するために使用したサービス（FTP、Telnet、SSH、HTTP、HTTPS）がディセーブルにされ、userconfig コマンドで作成した追加のユーザ アカウントが削除されます。このコマンドは、シリアル インターフェイスを使用するか、またはデフォルトの Admin ユーザ アカウントから管理ポート上のデフォルト設定を使用して CLI に再接続できない場合は使用しないでください。**

resetconfig コマンド

```
mail3.example.com> offline

Delay (seconds, minimum 30):
[30]> 45
```

```
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.

mail3.example.com> resetconfig

Are you sure you want to reset all configuration values? [N]> Y

All settings have been restored to the factory default.
```

AsyncOS のバージョン情報の表示

Cisco IronPort アプライアンスに現在インストールされている AsyncOS のバージョンを判別するには、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 Appliances] > [Centralized Services] > [System Status] を選択します。

ステップ 2　ページの下部までスクロールして、[Version Information] で、現在インストールされている AsyncOS のバージョンを確認します。

あるいは、コマンドライン プロンプトで **version** コマンドを使用することもできます。

セキュリティ管理アプライアンスのバックアップ

データのバックアップについて

バックアップ データには、Web トラッキングおよびトレンド レポーティング、電子メール レポーティング、メッセージ トラッキング、Cisco IronPort スパム隔離、および Safelist/Blocklist データが含まれます。この処理を行っても、設定とログはバックアップされません。

セキュリティ管理アプライアンスでは、アクティブなデータ セットを「ソース」アプライアンスから「ターゲット」セキュリティ管理アプライアンスにコピーし、元の「ソース」セキュリティ管理アプライアンスの中断を最小限に抑えることができます。セキュリティ管理アプライアンスは、マシンを「プライマリ」または「バックアップ」アプライアンスではなく、「ソース」アプライアンスと「ターゲッ

ト」アプライアンスと見なします。つまり、データを送信するマシンが「ソース」であり、スケジュール設定されたバックアップの一部として、別のセキュリティ管理アプライアンスからデータを受信するアプライアンスが「ターゲット」です。

データの転送が完了すると、2 台のボックス上のデータが同一になります。バックアップ機能では **backupconfig** コマンドを使用して、セキュリティ管理アプライアンスの GUI を使用せずにデータ ファイルをバックアップできます。また、スケジュール設定されたバックアップと実行中のバックアップの表示またはキャンセル、バックアップ ステータスの確認、またはバックアップをリモート マシンにスケジュール設定できるかどうかの確認を行うこともできます。

最初のバックアップ後の各バックアップは、前回のバックアップ後に生成された情報のみをコピーします。

バックアップの制約事項および要件

バックアップをスケジュール設定する前に、次の制約事項および要件を考慮してください。

制約事項	要件
AsyncOS バージョン	セキュリティ管理データ用のこのリリースの AsyncOS は、セキュリティ管理用の同じリリースの AsyncOS を実行している別のセキュリティ管理アプライアンスに対してのみバックアップできます。バージョンが一致しない場合は、バックアップのスケジュールを設定する前に、ターゲット セキュリティ管理アプライアンスをアップグレードしてください。
ネットワーク上のターゲット アプライアンス	ターゲット アプライアンスがネットワーク上に設定されている必要があります。 ターゲット アプライアンスが新規の場合は、システム セットアップ ウィザードを実行して必要な情報を入力します。手順については、第 2 章「セットアップ、インストール、および基本設定」を参照してください。
アプライアンス間の通信	ソースおよびターゲット セキュリティ管理アプライアンスは、SSH を使用して通信できるようになっている必要があります。このため次のようになります。 • 両方のアプライアンスのポート 22 を開いておく必要があります。デフォルトでは、このポートはシステム セットアップ ウィザードを実行すると開きます。 • ドメイン ネーム サーバ（DNS）で、A レコードと PTR レコードの両方を使用して、両方のアプライアンスのホスト名を解決できる必要があります。

制約事項	要件
アプライアンス キャパシティ	ターゲット アプライアンスのキャパシティが、ソース アプライアンスのキャパシティと同等以上である必要があります。ターゲット アプライアンスのデータの各タイプに割り当てられているディスク領域は、ソース アプライアンスの対応する割り当て未満にできません。 **（注）** すべてのデータのバックアップに十分なスペースがターゲット上にあれば、大きいソースから小さいターゲット セキュリティ管理アプライアンスへのバックアップをスケジュール設定できます。たとえば、ソース アプライアンスが M1060 で、小さいほうの M650 がターゲットの場合、大きいほうの M1060 で割り当てられているスペースを削減して、小さいほうの M650 アプライアンスで使用可能なスペースと一致するようにしてください。ディスク領域の割り当てについては、「ディスク使用量の管理」（P.13-57）を参照してください。
複数、同時、および チェーン バックアップ	バックアップ プロセスは一度に 1 つだけ実行できます。前のバックアップが完了する前に実行がスケジュールされているバックアップはスキップされ、警告が送信されます。 セキュリティ管理アプライアンスからのデータは、1 つのセキュリティ管理アプライアンスにバックアップできます。 チェーン バックアップ（バックアップへのバックアップ）はサポートされていません。

バックアップ期間

最初の完全バックアップでは、800GB のバックアップに最大 10 時間かかります。毎日のバックアップは、それぞれ最大 3 時間かかります。毎週または毎月のバックアップはより長くかかる場合があります。これらの数は場合によって異なります。

初期バックアップ後のバックアップ プロセスでは、最後のバックアップから変更されたファイルのみが転送されます。このため、その後のバックアップにかかる時間は初期バックアップの場合よりも短くなります。後続のバックアップに必要な時間は、累積されたデータ量、変更されたファイル数、および最後のバックアップ以降どの程度のファイルが変更されたかによって異なります。

完了したバックアップの所要時間

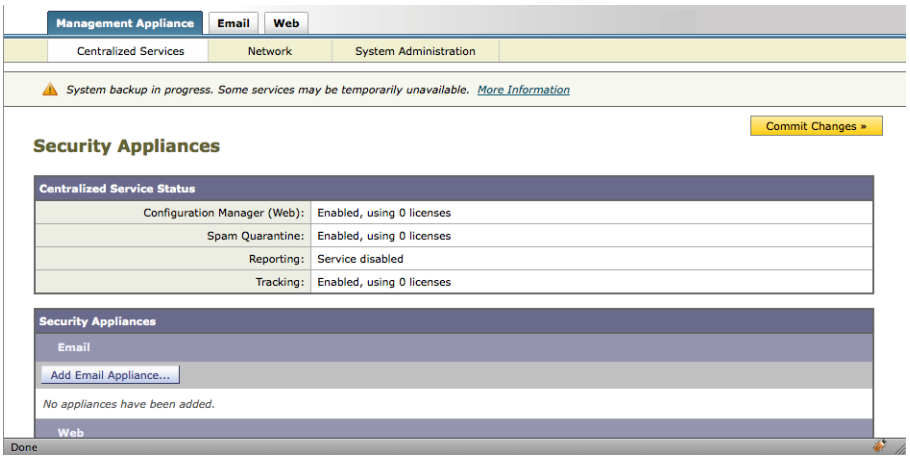
バックアップ中のサービスのアベイラビリティ

バックアップ プロセスのフェーズと、それらがサービスのアベイラビリティに及ぼす影響は次のとおりです。

- フェーズ 1：バックアップ プロセスのフェーズ 1 は、ソース アプライアンスとターゲット アプライアンス間のデータの転送で開始されます。データの転送中、ソース アプライアンスでのサービスは実行されたままになるため、データ収集をそのまま継続できます。ただし、ターゲット アプライアンスではサービスがシャットダウンされます。ソースからターゲット アプライアンスへのデータの転送が完了すると、フェーズ 2 が開始されます。
- フェーズ 2：フェーズ 2 が始まると、ソース アプライアンスでサービスがシャットダウンされます。最初のシャットダウンから、ソースおよびターゲット アプライアンスの間でのデータ転送中に収集された相違点がターゲット アプライアンスにコピーされ、サービスがソースとターゲットの両方のバックアップに戻されます。これにより、ソース アプライアンス上で最大の稼働時間を維持でき、いずれかのアプライアンスのデータが損失することがなくなります。

バックアップ中に、データのアベイラビリティ レポートが機能しなくなる場合があります。また、メッセージ トラッキング結果を表示すると、各メッセージのホスト名に「未解決」というラベルが付くことがあります。

レポートをスケジュール設定しようとしているときに、バックアップが進行中であることを忘れていた場合は、[Management Appliance] > [Centralized Services] を選択して、システムのステータスを確認できます。このウィンドウには、システムのバックアップが進行中であるという警告が表示されます。



バックアップ プロセスの中断

（注）　バックアップの実行中にソース アプライアンスの予期しないリブートがあっても、ターゲット アプライアンスはこの停止を認識しません。ターゲット アプライアンスでバックアップをキャンセルする必要があります。

バックアップ プロセスの中断があり、そのバックアップ プロセスが完了していない場合、バックアップを次に試行したときに、セキュリティ管理アプライアンスは停止した部分からバックアップ プロセスを開始できます。

進行中のバックアップをキャンセルすることは推奨されません。これは、既存のデータが不完全になり、エラーが発生した場合は、次のバックアップが完了するまで使用できないことがあります。進行中のバックアップのキャンセルが必要な場合は、できるだけ早く完全バックアップを実行し、常に使用可能な現在のバックアップを確保してください。

単一または定期バックアップのスケジュール設定

単一または定期バックアップを事前設定した時間に行うようにスケジュール設定できます。

（注）　リモート マシンに実行中のバックアップがある場合、バックアップ プロセスは開始されません。

定期バックアップをスケジュール設定するには、次の手順を実行します。

ステップ 1　管理者として SSH セッションにログインします。

ステップ 2　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

実行する操作を選択します。

- [View]：スケジュール設定したバックアップを確認できます。
- [Verify]：バックアップをリモート マシンでスケジュール設定できるかどうかを確認します。
- [Schedule]：アプライアンスにバックアップをスケジュール設定します。
- [Cancel]：スケジュール設定されたバックアップをキャンセルします。
- [Status]：実行中のバックアップのステータスを表示します。
- [Setup]：バックアップ パラメータを設定します。

ステップ 3　ソース アプライアンスおよびターゲット アプライアンス間の接続が低速である場合は、データ圧縮をオンにします。

setup と入力して、Y を押します。

ステップ 4　**Schedule** と入力して、Enter を押します。

ステップ 5　ターゲットの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。

ステップ 6　ターゲット アプライアンスを識別する有効な名前を入力します（最大 20 文字）。

ステップ 7　ターゲット アプライアンスの管理ユーザの名前およびパスワードを入力します。

ステップ 8　バックアップするデータに関するプロンプトに応答します。

すべてのデータ、または次のデータの任意の組み合わせをバックアップできます。

- スパム隔離
- 電子メール トラッキング（メッセージ トラッキング）
- Web トラッキング
- レポーティング（電子メールおよび Web）
- セーフリスト / ブロックリスト

これで、セキュリティ管理アプライアンスはターゲット マシンの存在を確認し、ターゲット マシンにデータを受けるのに十分なスペースがあるかどうかを判別します。

ターゲット マシンのスペースが不十分な場合は、次のエラー メッセージが表示されます。「Backup cannot be scheduled.Reason: There is not enough space for Spam Quarantine, Email Tracking, Web Tracking, Reporting.Please increase disk allocation for these services on the target machine」。データは転送されません。

ターゲット マシンが検証されると、次の選択肢が表示されます。

1. [Setup Repeating Backup Schedule]：定期バックアップをスケジュール設定できます。
2. [Schedule a single backup]：単一バックアップをスケジュール設定できます。
3. [Start a Single Backup Now]：即時バックアップを開始できます。

ステップ 9　単一バックアップをスケジュール設定する場合は、2 を入力して、Enter を押します。

ステップ 10　定期バックアップをスケジュール設定する場合は、次の手順を実行します。

a. **1** を入力して、Enter を押します。

b. 次の選択肢が表示されます。`1.[Daily]、2.[Weekly]、3.[Monthly]`。

c. 定期バックアップの時間枠を選択し、Enter を押します。

ステップ 11　バックアップを開始する特定の日付または日および時間を入力して、Enter を押します。

ステップ 12　バックアップ プロセスの名前を入力します。

ステップ 13　バックアップが正常にスケジュール設定されたことを確認します。コマンド プロンプトで **View** または **Status** と入力して、Enter を押します。

ステップ 14　「その他の重要なバックアップ タスク」（P.13-13）も参照してください。

即時バックアップの開始

インスタント バックアップは、CLI で **backupconfig** コマンドを開始するとすぐに実行されます。

（注）　リモート マシンに実行中のバックアップがある場合、バックアップ プロセスは開始されません。

インスタント バックアップを開始するには、コマンドライン インターフェイスで次の手順を実行します。

ステップ 1　管理者として SSH セッションにログインします。

ステップ 2　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

実行する操作を選択します。

- `[View]`：スケジュール設定したバックアップを確認できます。
- `[Verify]`：バックアップをリモート マシンでスケジュール設定できるかどうかを確認します。
- `[Schedule]`：アプライアンスにバックアップをスケジュール設定できます。
- `[Cancel]`：スケジュール設定されたバックアップをキャンセルします。
- `[Status]`：実行中のバックアップのステータスを確認できます。
- `[Setup]`：バックアップ パラメータを設定します。

ステップ 3　ソース アプライアンスおよびターゲット アプライアンス間の接続が低速である場合は、データ圧縮をオンにします。

setup と入力して、Y を押します。

ステップ 4　**Schedule** と入力して、Enter を押します。

ステップ 5　ターゲットの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。

ステップ 6　ターゲット アプライアンスを識別する有効な名前を入力します（最大 20 文字）。

ステップ 7　ターゲット アプライアンスの管理ユーザの名前およびパスワードを入力します。

ステップ 8　バックアップするデータに関するプロンプトに応答します。

すべてのデータ、または次のデータの任意の組み合わせをバックアップできます。

- スパム隔離

- 電子メール トラッキング（メッセージ トラッキング）
- Web トラッキング（レポーティング データを含む）
- レポーティング（電子メール）
- セーフリスト / ブロックリスト

これで、セキュリティ管理アプライアンスはターゲット マシンの存在を確認し、ターゲット マシンにデータを受けるのに十分なスペースがあるかどうかを判別します。

ターゲット マシンのスペースが不十分な場合は、次のエラー メッセージが表示されます。「`Backup cannot be scheduled.Reason: There is not enough space for Spam Quarantine, Email Tracking, Web Tracking, Reporting.Please increase disk allocation for these services on the target machine`」。データは転送されません。

ターゲット マシンが検証されると、コンソールに次の選択肢が表示されます。

1. `[Setup Reoccurring Backup]`：定期バックアップをスケジュール設定できます。
2. `[Schedule a Single backup]`：単一バックアップをスケジュール設定できます。
3. `[Start a Single Backup Now]`：即時バックアップを開始できます。

ステップ 9　**3** と入力して、Enter を押します。

ステップ 10　バックアップ ジョブの有効な名前を入力します。

バックアップ プロセスが数分で開始し、ソース マシンからターゲット マシンへのデータの転送が開始されます。即時バックアップが開始されると、次のメッセージが表示されます。「`Backup has been initiated and will begin in a few seconds`」。

ステップ 11　（任意）バックアップの進捗状況を表示するには、コマンドライン プロンプトで **Status** と入力します。

ステップ 12　「その他の重要なバックアップ タスク」（P.13-13）も参照してください。

バックアップ ステータスの確認

ログ ファイルの確認

バックアップ ログはバックアップ プロセスを開始から終了まで記録します。

バックアップ スケジューリングに関する情報は、SMA ログ内にあります。

スケジュールされたバックアップの確認

ステップ 1　管理者として SSH セッションにログインします。

ステップ 2　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

ステップ 3　`View` 操作を選択します。

進行中のバックアップのステータスの確認

ステップ 1　管理者として SSH セッションにログインします。

ステップ 2　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

ステップ 3　Status 操作を選択します。

その他の重要なバックアップ タスク

ここで説明されているバックアップ プロセスではバックアップされない項目が失われることを防止するため、およびアプライアンスの障害が発生した場合にセキュリティ管理アプライアンスの交換を速めるため、次のことを検討してください。

- プライマリ セキュリティ管理アプライアンスから設定を保存するには、「コンフィギュレーション設定の保存とインポート」（P.13-50）を参照してください。プライマリ セキュリティ管理アプライアンスとは別の安全な場所にコンフィギュレーション ファイルを保存します。
- セキュリティ管理アプライアンスから別の場所にログ ファイルを保存する方法については、「ログ サブスクリプション」（P.14-22）を参照してください。

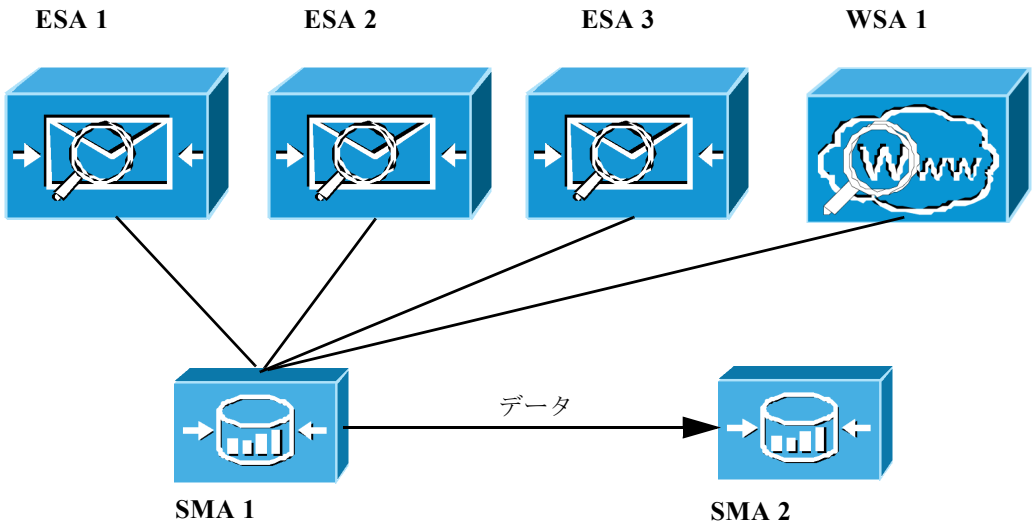
  さらに、バックアップ ログのログ サブスクリプションを設定できます。「GUI でのログ サブスクリプションの作成」（P.14-23）を参照してください。

セキュリティ管理アプライアンスでのディザスタ リカバリ

セキュリティ管理アプライアンスが予期せず失敗した場合は、次の手順を使用して、セキュリティ管理サービスおよびバックアップしたデータを復元します。これは「セキュリティ管理アプライアンスのバックアップ」（P.13-6）の情報を使用して定期的に保存しています。

一般的なアプライアンス設定は図 13-3 のようになります。

図 13-3　ディザスタ リカバリ：一般的な環境



この環境で、SMA 1 は ESA 1 ～ 3 および WSA 1 からデータを受信しているプライマリ セキュリティ管理アプライアンスです。SMA 2 は SMA1 からバックアップ データを受信しているバックアップ **セキュリティ管理アプライアンス**です。

失敗した場合は、SMA 2 がプライマリ セキュリティ管理アプライアンスになるように設定する必要があります。

SMA 2 を新しいプライマリ セキュリティ管理アプライアンスとして設定し、サービスを復元するには、次の手順を実行します。

ステップ 1　バックアップ セキュリティ管理アプライアンス（SMA2）に、プライマリ セキュリティ管理アプライアンス（SMA1）から保存したコンフィギュレーション ファイルをロードします。

詳細については、「コンフィギュレーション ファイルのロード」（P.13-52）を参照するか、`loadconfig` コマンドを使用します。

ステップ 2　次のようにして、障害が発生した SMA 1 から IP アドレスを再作成し、SMA 2 の IP アドレスに設定します。

a. SMA 2 で、[Network] > [IP Interfaces] > [Add IP Interfaces] を選択します。

b. [Add IP Interfaces] ページで、障害が発生した SMA1 のすべての関連 IP 情報をテキスト フィールドに入力して、SMA 2 のインターフェイスを再作成します。

IP インターフェイスの追加の詳細については、「IP インターフェイスの設定」（P.A-2）を参照してください。

ステップ 3　[Submit] と [Commit] をクリックします。

ステップ 4　新しい セキュリティ管理アプライアンス（SMA 2）ですべてのサービスをイネーブルにします。

この場合、ESA 1 ～ 3 と WSA 1 のサービスも再度イネーブルにする必要があります。詳細については、「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）を参照してください。

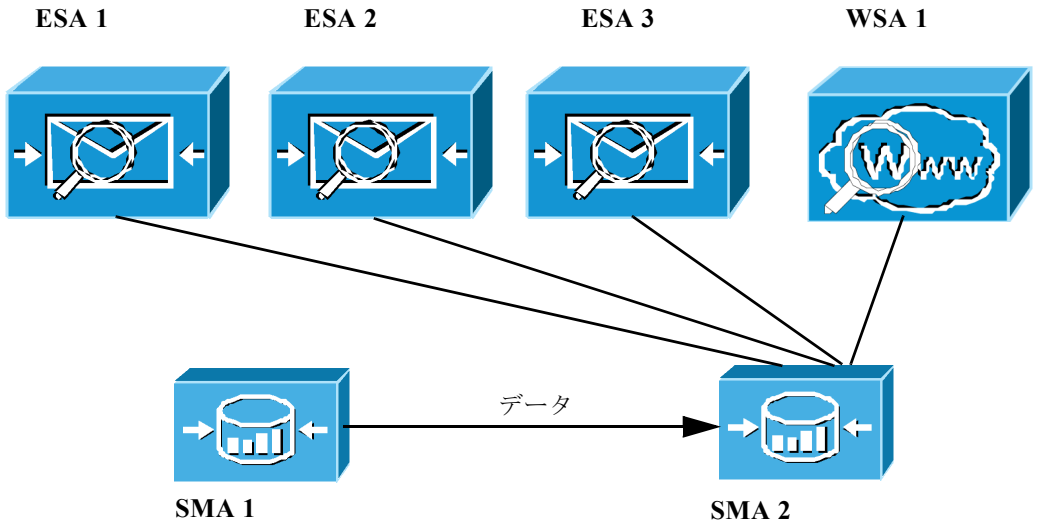
ステップ 5　すべてのアプライアンスを新しい セキュリティ管理アプライアンス（SMA 2）に追加します。

詳細については、「管理対象アプライアンスの追加について」（P.2-16）を参照してください。

ステップ 6　アプライアンスへの接続を確立し、その接続をテストすることで、各アプライアンスがイネーブルとなり、機能していることをテストして確認します。

これで、SMA 2 がプライマリ セキュリティ管理アプライアンスになりました。これで、図 13-4 に示すように、ESA 1 ～ 3 と WSA 1 からもすべてのデータが SMA 2 に送られるようになりました。

図 13-4　ディザスタ リカバリ：最終結果



その他のデータの復元

復元が必要な追加のデータについては、「その他の重要なバックアップ タスク」（P.13-13）を参照してください。

アプライアンス ハードウェアのアップグレード

古い セキュリティ管理アプライアンスから新しいモデルにアップグレードする場合（たとえば、M160 から M650 へのアップグレード）、次の手順を実行して、古いアプライアンスから新しいアプライアンスにデータを正しく転送します。

（注）　異なるサイズの セキュリティ管理アプライアンス間でデータを転送することはできますが、新しいアプライアンスには同等以上のサイズが割り当てられている必要があります。

図 13-5　新しいセキュリティ管理アプライアンス ハードウェアのアップグレード

（注）　以下に示すすべての説明は、コマンド プロンプトに入力する場合のものです。

ステップ 1　管理者として SSH セッションにログインします。

ステップ 2　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

実行する操作を選択します。

- [View]：スケジュール設定したバックアップを確認できます。
- [Verify]：バックアップをリモート マシンでスケジュール設定できるかどうかを確認します。
- [Schedule]：アプライアンスにバックアップをスケジュール設定できます。
- [Cancel]：スケジュール設定されたバックアップをキャンセルします。
- [Status]：実行中のバックアップのステータスを確認できます。

ステップ 3　**Schedule** と入力して、Enter を押します。

ステップ 4　ターゲット セキュリティ管理アプライアンスの IP アドレスと名前を入力します。

これで、セキュリティ管理アプライアンスはターゲット マシンが存在するかどうか、およびターゲット マシンにデータを受けるのに十分なスペースがあるかどうかを確認します。

異なるサイズの セキュリティ管理アプライアンス間でデータを転送することはできますが、新しいアプライアンスには同等以上のサイズが割り当てられている可能性があります。ターゲット マシンのスペースが不十分な場合は、次のエラー メッセージが表示されます。「**Backup cannot be scheduled.Reason: There is not enough space for isq, tracking, reporting, slbl.Please increase disk allocation for these services on the target machine**」。データは転送されません。

ターゲット マシンが検証されると、コンソールに次の選択肢が表示されます。

- 1. [Setup Reoccurring Backup]：定期バックアップをスケジュール設定できます。
- 2. [Schedule a Single backup]：単一バックアップをスケジュール設定できます。
- 3. [Start a Single Backup Now]：即時バックアップを開始できます。

ステップ 5　**3** と入力して、Enter を押します。

バックアップ プロセスが開始し、ソース マシンからターゲット マシンへのデータの転送がすぐに開始されます。即時バックアップが開始されると、次のメッセージが表示されます。「`Backup has been initiated and will begin in a few seconds`」。

ステップ 6　コマンドライン プロンプトに **suspendtransfers** コマンドを入力し、ソース アプライアンスと新しいターゲット アプライアンス間のすべてのデータ転送を一時停止します。

suspendtransfers コマンドによって、古いソース セキュリティ管理アプライアンスのデータ受信が停止されます。

ステップ 7　上記のステップ 2 から 5 を繰り返して、ソース マシンで新しいインスタント バックアップを実行します。

AsyncOS のアップグレード

ここでは、セキュリティ管理アプライアンスでのソフトウェア アップグレードおよびアップデートに関連する次の内容について説明します。

- 「クラスタ化されたシステムのアップグレードについて」（P.13-17）
- 「ネットワーク要件の決定」（P.13-17）
- 「アップグレード方式：リモートまたは ストリーミング」（P.13-17）
- 「アップグレードおよびサービス アップデートの設定」（P.13-20）

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、『*Cisco IronPort AsyncOS for Email Advanced User Guide*』の「Centralized Management」の章にある「Upgrading Machines in a Cluster」を参照してください。

ネットワーク要件の決定

Cisco IronPort Systems では分散アップグレード サーバ アーキテクチャを使用して、顧客がどこからでも AsyncOS アップグレードをすばやくダウンロードできます。この分散サーバ アーキテクチャのため、Cisco IronPort アップデート サーバではダイナミック IP アドレスが使用されます。厳格なファイアウォール ポリシーを適用している場合は、AsyncOS のアップグレード用に静的な場所の設定が必要になることがあります。アップグレードに関して、ファイアウォール設定にスタティック IP が必要であると判断した場合は、Cisco IronPort カスタマー サポートに連絡して、必要な URL アドレスを取得してください。

（注） 既存のファイアウォール ルールで `upgrades.cisco.com` ポート（22、25、80、4766 など）からのレガシー アップグレードのダウンロードが許可されている場合は、それらを削除するか、修正したファイアウォール ルールに置き換える必要があります。

アップグレード方式：リモートまたは ストリーミング

Cisco IronPort では、Cisco IronPort アプライアンスで AsyncOS をアップグレードするための 2 つの方式（または「ソース」）を使用できます。

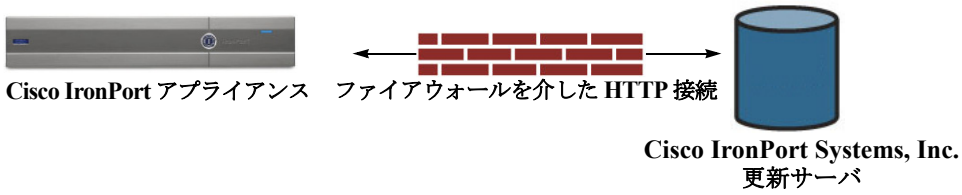
- ストリーミング アップグレード：各 Cisco IronPort アプライアンスは Cisco IronPort アップグレード サーバから HTTP を介して AsyncOS アップグレードを直接ダウンロードします。
- リモート アップグレード：Cisco IronPort からアップグレード イメージを 1 回だけダウンロードし、Cisco IronPort アプライアンスに保存します。Cisco IronPort アプライアンスはネットワーク内のサーバから AsyncOS アップグレードをダウンロードします。

「アップグレードおよびサービス アップデートの設定」（P.13-20）にある、アップグレード方式を設定します。オプションで、CLI で **updateconfig** コマンドを使用します。

ストリーミング アップグレードの概要

ストリーミング アップグレードでは、各 Cisco IronPort アプライアンスが直接 Cisco IronPort アップデート サーバに接続して、アップグレードを検索してダウンロードします。

図 13-6　ストリーミング アップデート方式

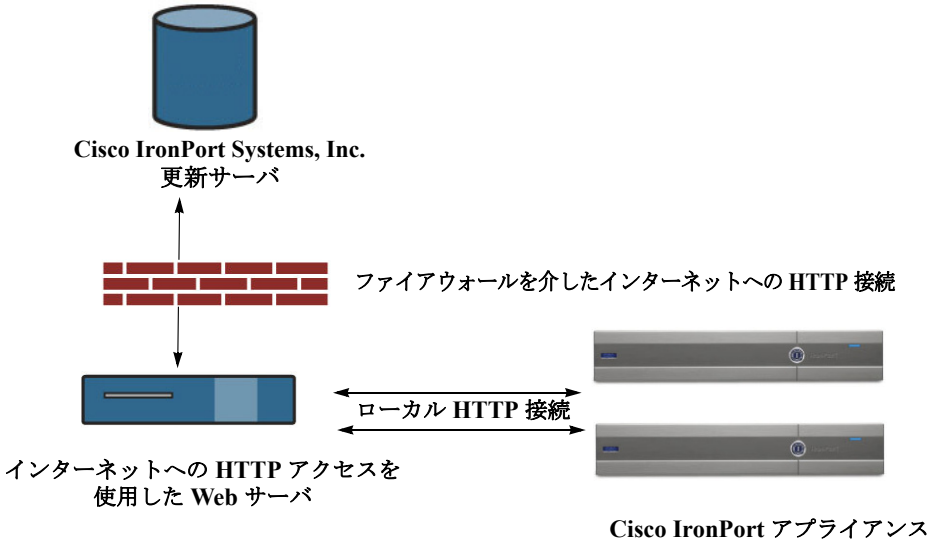


この方式では、Cisco IronPort アプライアンスが Cisco IronPort Systems アップデート サーバにネットワークから直接接続する必要があります。

リモート アップグレードの概要

また、Cisco IronPort のアップデート サーバから直接アップデートを取得する（ストリーミング アップグレード）のではなく、ネットワーク内からローカルで AsyncOS にアップデートをダウンロードおよびホスト（リモート アップグレード）することもできます。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 で暗号化されたアップデート 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、Cisco IronPort 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。

図 13-7　リモート アップデート方式



基本的なプロセスは、次のとおりです。

ステップ 1　「リモート アップグレードのハードウェア要件およびソフトウェア要件」（P.13-19）および「リモート アップグレード イメージのホスティング」（P.13-19）の情報をお読みください。

ステップ 2　アップグレード ファイルを取得して処理するように、ローカル サーバを設定します。

ステップ 3　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 4　[Management Appliance] > [System Administration] > [Update SettingsChoose] を選択します。

このページで、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することを指定します。

ステップ 5　[Management Appliance] > [System Administration] > [System Upgrade] を選択します。

ステップ 6　[Available Upgrades] をクリックします。

（注）　コマンドライン プロンプトから、次を行うこともできます。
updateconfig コマンドを実行してから **upgrade** コマンドを実行する。

詳細については、「AsyncOS のアップグレード」（P.13-16）を参照してください。

リモート アップグレードのハードウェア要件およびソフトウェア要件

AsyncOS アップグレード ファイルを*ダウンロード*するには、内部ネットワークに次を持つシステムが必要です。

- Cisco IronPort 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。

（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 ファイルを*ホスティング*するには、内部ネットワークに次を持つサーバが必要です。

- Web サーバ。たとえば、次のような Microsoft IIS（Internet Information Services）または Apache オープン ソース サーバ。
  - 24 文字を超えた、ディレクトリまたはファイル名の表示をサポート
  - ディレクトリ参照に対応
  - 匿名（認証なし）または基本（「簡易」）認証用に設定されている
  - 各 AsyncOS アップデート イメージに対して少なくとも 350MB の空きディスク領域がある

リモート アップグレード イメージのホスティング

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、Cisco IronPort アプライアンスのシリアル番号と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。アップグレード イメージの zip ファイルをダウンロードするアップグレード バージョンをクリックします。AsyncOS アップグレードのアップグレード イメージを使用するには、ローカル サーバの基本 URL を [Edit Update Settings] ページに入力します（または CLI の `updateconfig` を使用します）。

ネットワーク上の Cisco IronPort アプライアンスに使用可能なアップグレードを、`http://updates.ironport.com/fetch_manifest.html` で選択したバージョンに限定する XML ファイルを、ローカル サーバでホスティングすることもできます。この場合でも、Cisco IronPort アプライアンスは Cisco IronPort Systems アップデート サーバからアップグレードをダウンロードします。アップグレード リストをローカル サーバにホスティングする場合は、zip ファイルをダウンロードして、`asyncos/phoebe-my-upgrade.xml` ファイルをローカル サーバのルート ディレクトリに展開します。AsyncOS アップグレードのアップグレード リストを使用するには、XML ファイルの完全 URL を [Edit Update Settings] ページに入力します（または CLI の `updateconfig` を使用します）。

リモート アップグレードの詳細については、Cisco IronPort ナレッジ ベースを参照するか、Cisco IronPort Support プロバイダーにお問い合わせください。

リモート アップグレード方式における重要な違い

ストリーミング アップグレード方式と比較して、AsyncOS をローカル サーバからアップグレード（リモート アップグレード）する場合には、次の違いがあることに注意してください。

- *ダウンロード中に*、アップグレードによるインストールがすぐに実行されます。
- アップグレード プロセスの最初の 10 秒間、バナーが表示されます。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。

アップグレードおよびサービス アップデートの設定

セキュリティ管理アプライアンスがセキュリティ サービス アップデート（時間帯ルールなど）および AsyncOS アップグレードをダウンロードする方法を設定できます。たとえば、ファイルをダウンロードするときに使用するネットワーク インターフェイスを選択したり、アップデート間隔を設定したり、自動アップデートをディセーブルにしたりすることができます。

AsyncOS は、新しい AsyncOS アップグレードを除く、すべてのセキュリティ サービス コンポーネントへの新しいアップデートがないか、定期的にアップデート サーバに問い合わせます。AsyncOS をアップグレードするには、AsyncOS が使用可能なアップグレードを問い合わせるよう、手動で要求する必要があります。

アップグレードおよびアップデート設定は、GUI（次の 2 つの項を参照）で、または CLI で `updateconfig` コマンドを使用して設定できます。

アップグレードおよびアップデートの設定

表 13-1 に、設定可能なアップデートおよびアップグレード設定を示します。

表 13-1　セキュリティ サービスのアップデート設定

設定	説明
Update Servers (images)	Cisco IronPort アップデート サーバまたはローカル Web サーバから、Cisco IronPort AsyncOS アップグレード イメージおよびサービス アップデート（時間帯ルールや機能キーのアップデートなど）をダウンロードするかどうかを決定します。デフォルトは、Cisco IronPort アップデート サーバです。 次のいずれかの場合、ローカル Web サーバを選択します。 • Cisco IronPort からアップグレードおよびアップデート イメージをダウンロードし、Cisco IronPort カスタマー サポートから提供されたスタティック アドレスを入力する必要がある場合。「厳格なファイアウォール ポリシーを適用している環境のスタティック アップグレードおよびアップデート サーバ設定」（P.13-22）を参照してください。 • 一時的に、ローカル Web サーバに保存されたアップグレード イメージをダウンロードする場合。イメージをダウンロードした後、この設定を変えて Cisco IronPort アップデート サーバ（または使用している場合にはスタティック アドレス）に戻し、アップデートが自動的に行われるようにすることをお勧めします。 ローカル アップデート サーバを選択した場合は、アップグレードとアップデートのダウンロードに使用するサーバの基本 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ワードも入力します。 詳細については、「アップグレード方式：リモートまたは ストリーミング」（P.13-17）および「リモート アップグレードの概要」（P.13-18）を参照してください。

表 13-1　セキュリティ サービスのアップデート設定 （続き）

設定	説明
Update Servers (lists)	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 サーバまたはローカル Web 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、Cisco IronPort アップデート サーバです。 該当する場合は、「厳格なファイアウォール ポリシーを適用している環境のスタティック アップグレードおよびアップデート サーバ設定」（P.13-22）を参照してください。 ローカル Web サーバに保存されたアップグレード イメージを一時的にダウンロードする場合は、ローカル Web サーバを選択できます。イメージをダウンロードした後、この設定を変えて Cisco IronPort アップデート サーバに戻し、セキュリティ コンポーネントが自動的にアップデートされるようにすることを推奨します。 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ポート番号を含む、リストのマニフェスト XML ファイルの完全なパスを入力します。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ワードも入力します。 詳細については、「アップグレード方式：リモートまたは ストリーミング」（P.13-17）および「リモート アップグレードの概要」（P.13-18）を参照してください。
Automatic Updates	時間帯ルールの自動アップデートをイネーブルにするかどうかを選択します。イネーブルにする場合は、アップデートを確認する間隔を入力します。分の場合は **m**、時間の場合は **h**、日の場合は **d** を末尾に追加します。
Interface	時間帯ルールや AsyncOS アップグレードなどをアップデート サーバに問い合わせるときに、どのネットワーク インターフェイスを使用するかを選択します。使用可能なプロキシ 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、使用するインターフェイスがアプライアンスにより選択されます。
HTTP Proxy Server	アップストリームの HTTP プロキシ サーバが存在し、認証が必要な場合は、サーバ情報、ユーザ名、およびパスワードをここに入力します。 プロキシ サーバを指定すると、GUI にリストされているサービスへのアクセスおよびアップデートにそれが使用されます。
HTTPS Proxy Server	アップストリームの HTTPS プロキシ サーバが存在し、認証が必要な場合は、サーバ情報、ユーザ名、およびパスワードをここに入力します。 プロキシ サーバを指定すると、GUI にリストされているサービスへのアクセスおよびアップデートにそれが使用されます。

厳格なファイアウォール ポリシーを適用している環境のスタティック アップグレードおよびアップデート サーバ設定

Cisco IronPort AsyncOS 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。環境にスタティック IP アドレスが必要な厳格なファイアウォール ポリシーを適用している場合は、Cisco IronPort カスタマー サポートに連絡して必要な URL アドレスを取得し、次の手順に従ってそれらをローカル サーバとして入力します。

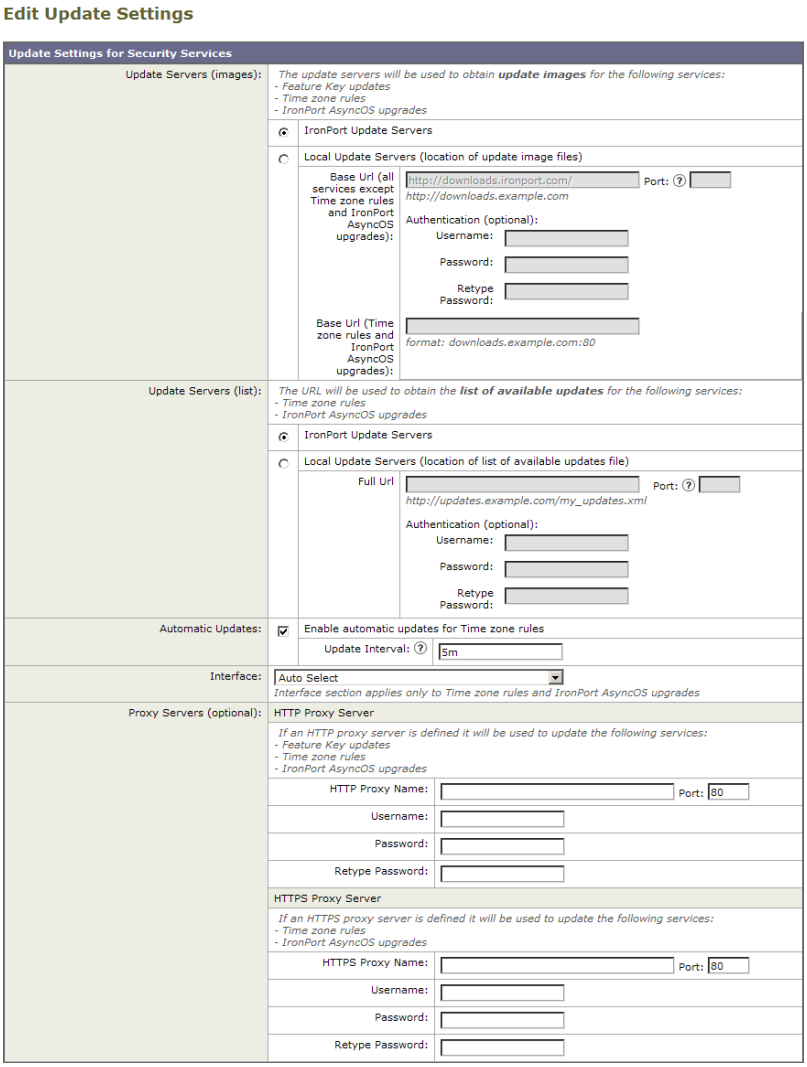
GUI からのアップデートおよびアップグレード設定値の設定

アップデートおよびアップグレード設定を編集するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [System Administration] > [Update Settings] ページに移動し、[Edit Update Settings] をクリックします。

表 13-1（P.13-21）の説明を参考にして、次の各設定値を設定します。

図 13-8　[Edit Update Settings] ページ



ステップ 2　[Update Servers (images)] セクションで、アップデートとアップグレード用のイメージのダウンロード元のサーバを指定します。

ステップ 3　[Update Servers (list)] セクションで、使用可能なアップデートおよび AsyncOS アップグレードのリストの取得の設定を指定します。

ステップ 4　時間帯ルールおよびインターフェイスの設定を指定します。

ステップ 5　（任意）プロキシ サーバの設定を指定します。

ステップ 6　変更を送信し、保存します。

CLI からのアップデートおよびアップグレード設定値の設定

updateconfig コマンドを使用すると、Cisco IronPort アプライアンスにサービス アップデートおよび AsyncOS アップグレードを探す場所を指示できます。リモート アップグレードの場合、updateconfig コマンドを発行して、アプライアンスがその目的でローカル アップデート サーバを使用するように設定します。

```
sma.example.com> updateconfig

Service (images):                Update URL:
-------------------------------------------------------------------
Feature Key updates              http://downloads.ironport.com/asyncos
Timezone rules                   IronPort Servers
IronPort AsyncOS upgrades        IronPort Servers

Service (list):                  Update URL:
-------------------------------------------------------------------
Timezone rules                   IronPort Servers
IronPort AsyncOS upgrades        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.
[]> setup

For the following services, please select where the system will download updates from:
Service (images):                          Update URL:
-------------------------------------------------------------------
Feature Key updates
http://downloads.ironport.com/asyncos

1. Use Cisco IronPort update servers (http://downloads.ironport.com)
2. Use own server
[1]> 2

Enter the HTTP base URL of the update server using the format
(http://optionalname:password@local.server:port/directory/). The
default HTTP port is 80; you do not need to specify the port unless you wish to use a
non-standard port. The optional username/password will be presented using HTTP BASIC_AUTH.
[http://downloads.ironport.com/]>enter URL of the local server here
```

忘れずに変更を確定してください。

（注）　ping コマンドを使用すると、アプライアンスがローカル サーバに接続できることを確認できます。また、telnet コマンドを使用してローカル サーバのポート 80 に Telnet 接続することで、ローカル サーバが該当のポートをリッスンしていることが確認できます。

アップグレードする前に：重要な手順

次の手順を実行して、アップグレードの準備を行います。

ステップ 1　次のようにして、データの消失を防止する、または最小限に抑えます。

- 新しいアプライアンスに十分なディスク容量があり、転送される各データ タイプに同等以上のサイズが割り当てられていることを確認します。「使用可能な最大ディスク領域」（P.13-58）を参照してください。
- ディスク領域についての何らかの警告を受け取った場合は、アップグレードを開始する前に、ディスク領域に関する問題をすべて解決してください。

ステップ 2　アプライアンスから、XML コンフィギュレーション ファイルを保存します。

ステップ 3　セーフリスト/ブロックリスト機能を使用している場合は、リストをボックスからエクスポートします。

ステップ 4　CLI からアップグレードを実行している場合は、**suspendlistener** コマンドを使用してリスナーを停止します。GUI からアップグレードを実行した場合は、自動的にリスナーの一時停止が発生します。

ステップ 5　メール キューとデリバリ キューを解放します。

ステップ 6　アップグレード設定が希望どおりに設定されていることを確認します。「アップグレードおよびサービス アップデートの設定」（P.13-20）を参照してください。

GUI からの AsyncOS のアップグレード

AsyncOS をアップグレードするには、次の手順を実行します。

ステップ 1　「アップグレードする前に：重要な手順」（P.13-25）に示された作業を完了したことを確認します。

ステップ 2　セキュリティ管理アプライアンスで、[Management Appliance] > [System Administration] > [System Upgrade] を選択します。

ステップ 3　[Available Upgrades] をクリックします。

[Available Upgrades] ページが表示されます。

ステップ 4　利用可能なアップグレードのリストから、アップグレードを選択します。

ステップ 5　アップグレード前に設定ディレクトリに現在の設定を保存する場合は、[Upgrade Preparation] セクションでチェックボックスをオンにします。この設定が推奨されます。また、テキスト フィールドにメール アドレスを入力することで、選択した電子メールにこのパスワード ファイルを送信できます。

このセクションでは、[Configuration File] チェックボックスの [Mask Passwords] をオンにすることで、コンフィギュレーション ファイルにパスワードが表示されないようにすることもできます。

ステップ 6　[Begin Upgrade] をクリックします。ページの上部に経過表示バーが表示されます。変更の確定や新しいライセンス契約書への合意を 1 回以上求められる場合があります。

ステップ 7　アップグレードを完了するには、[Continue] をクリックします。

ステップ 8　アップグレードが完了すると、アプライアンスをリブートするように求められます。

ステップ 9　[Reboot Now] をクリックします。

ステップ 10　他の推奨される作業については、「アップグレード後」（P.13-27）を参照してください。

CLI を使用したアップグレードの実行

AsyncOS アップグレードを取得する場所（ローカル サーバまたは Cisco IronPort サーバ）を指定するには、updateconfig コマンドを実行します。アップグレードをインストールするには、upgrade コマンドを実行します。デフォルトでは、upgrade コマンドを入力すると、アプライアンスは Cisco IronPort アップグレード サーバに最新のアップデートを問い合わせます。

（注）　6.5 以前のバージョンの AsyncOS では、AsyncOS のアップグレードの取得に upgradeconfig コマンドが使用されていました。このコマンドは、現在サポートされていません。

（注）　アップグレード中は、さまざまなプロンプトを一時停止のまま長時間放置しないでください。TCP セッションがダウンロード中にタイムアウトしてしまった場合、アップグレードが失敗する可能性があります。

アップグレードする前に、「アップグレードする前に：重要な手順」（P.13-25）の関連する手順を完了します。

upgrade コマンドを発行して、利用可能なアップグレードのリストを表示します。リストから目的のアップグレードを選択して、インストールします。メッセージを確認するか、ライセンス契約を読んで、同意するように求められる場合があります。

```
Welcome to the IronPort M650 Security Management(tm) Appliance

sma.example.com> upgrade

Would you like to save the current configuration to the configuration directory before
upgrading? [Y]> y

Would you like to email the current configuration before upgrading? [N]> y

Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig. [Y]> y

Enter email addresses. Separate multiple addresses with commas.
[]> email@example.com

Upgrades available:
1. AsyncOS test.test

[1]> 1

Performing an upgrade may require a reboot of the system after the upgrade is applied. You
may log in again after this is done. Do you wish to proceed with the upgrade? [Y]> y

Preserving configuration ...
Finished preserving configuration
Cisco IronPort Security Management Appliance(tm) Upgrade

Warning: The 5.7 configuration master will be deleted on upgrade.
All settings in that configuration master will be deleted and will not be recoverable.

Do you wish to proceed with the upgrade? [y]> y
```

```
Finding partitions... done.
Setting next boot partition to current partition as a precaution... done.
Erasing new boot partition... done.
Installing application... done.
Installing CASE... done.
Installing Sophos Anti-Virus... done.
Reinstalling AsyncOS... done.
Installing Scanners... done.
Installing Brightmail Anti-Spam... done.
Installing Tracking Tools... done.
Configuring AsyncOS disk partitions... done.
Configuring AsyncOS user passwords... done.
Configuring AsyncOS network interfaces... done.
Configuring AsyncOS timezone... done.
Moving new directories across partitions... done.
Syncing... done.
Reinstalling boot blocks... done.
Will now boot off new boot partition... done.

Upgrade complete.  It will be in effect after this mandatory reboot.

Upgrade installation finished.
Enter the number of seconds to wait before forcibly closing connections.
[30]>
```

アップグレードが完了したら、「アップグレード後」（P.13-27）の作業を実行します。

アップグレード後

アップグレードが完了したら、次の手順を実行します。

- （関連する電子メール セキュリティ アプライアンスのある導入環境の場合）リスナーを再度イネーブルにします。
- 自動アップデート用の設定が AsyncOS アップグレードのダウンロードに使用する設定とは異なっている場合、これらの設定を適宜調整します。「アップグレードおよびサービス アップデートの設定」（P.13-20）を参照してください。
- システムが最新の Configuration Master をサポートするように設定します。「Configuration Master を使用するための設定の概要」（P.8-2）を参照してください。
- 設定を保存するかどうか判断します。詳細については、「コンフィギュレーション設定の保存とインポート」（P.13-50）を参照してください。

AsyncOS の以前のバージョンへの復元

緊急時には、前の認定バージョンの AsyncOS に戻すことができます。

アップグレードによって主要なサブシステムの一方向の変換が行われるため、バージョンの復元プロセスは複雑であり、Cisco IronPort 品質保証チームの認定が必要です。復元できるのは、前の 2 つのバージョンの中の 1 つだけです。最初にこの機能がサポートされた AsyncOS バージョンは AsyncOS 6.5 です。これよりも前のバージョンの AsyncOS はサポートされていません。

アプライアンス上のすべてのデータをクリアし、新しい、クリーンな設定から始める場合は、現在実行中のビルドに戻すこともできます。

復元による影響に関する重要な注意事項

Cisco IronPort アプライアンスにおける revert コマンドの使用は、非常に破壊的な操作になります。このコマンドにより、すべての設定ログとデータベースが破壊されます。さらに、復元ではアプライアンスが再設定されるまでメール処理が中断されます。このコマンドはすべての設定を破壊するため、revert コマンドを発行する場合は、Cisco IronPort アプライアンスへの物理的なローカル アクセスを必ず用意するようにしてください。

警告　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 ファイルには、後方互換性が*ありません*。

AsyncOS 復元の実行

前の認定バージョンの AsyncOS に復元するには、次の手順を実行します。

ステップ 1　戻し先のバージョンのコンフィギュレーション ファイルがあることを確認してください。コンフィギュレーション ファイルには、後方互換性がありません。

ステップ 2　アプライアンスの現在の設定のバックアップ コピーを、（パスワードをマスクしない状態で）別のマシンに保存します。それには、電子メールで自分に送信したり、ファイルを FTP で転送します。簡単に行うには、mailconfig CLI コマンドを実行すると、アプライアンスの現在のコンフィギュレーション ファイルが指定したメール アドレスに送信されます。

（注）　復元後にロードするのは、このコンフィギュレーション 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　電子メール セキュリティ アプライアンスで、すべてのリスナーを一時停止します。

ステップ 5　メール キューが空になるまで待ちます。

ステップ 6　バージョンを戻すアプライアンスの CLI にログインします。

revert コマンドを実行すると、いくつかの警告プロンプトが出されます。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、復元前の手順を完了するまで、復元プロセスを開始しないでください。

ステップ 7　コマンドライン プロンプトから **revert** コマンドを入力し、プロンプトに応答します。

次に、**revert** コマンドの例を示します。

```
m650p03.prep> revert

This command will revert the appliance to a previous version of AsyncOS.

WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy
quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all Cisco IronPort Spam Quarantine message and end-user safelist/blocklist data
```

```
Only the network settings will be preseved.

Before running this command, be sure you have:
- saved the configuration file of this appliance (with passwords
unmasked)
- exported the Cisco IronPort Spam Quarantine safelist/blocklist database
   to another machine (if applicable)
- waited for the mail queue to empty

Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots again to the desired
version.

Do you want to continue? yes

Are you sure you want to continue? yes

Available versions
==================
 1. 7.2.0-390
 2. 6.7.6-020

Please select an AsyncOS version: 1

You have selected "7.2.0-390".

Reverting to "testing" preconfigure install mode.

The system will now reboot to perform the revert operation.
```

ステップ 8　アプライアンスが 2 回リブートするまで待ちます。

ステップ 9　CLI を使用してアプライアンスにログインします。

ステップ 10　戻し先のバージョンの XML コンフィギュレーション ファイルをロードします。

ステップ 11　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 12　電子メール セキュリティ アプライアンスで、すべてのリスナーを再びイネーブルにします。

ステップ 13　変更を保存します。

これで、復元が完了した Cisco IronPort アプライアンスは、選択された AsyncOS バージョンを使用して稼働します。

（注）　復元が完了して、Cisco IronPort アプライアンスへのコンソール 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。

アップデートについて

サービス アップデートは定期的にダウンロード可能にできます。これらのダウンロードの設定を指定するには、「アップグレードおよびサービス アップデートの設定」（P.13-20）を参照してください。

Cisco IronPort Web 使用率制御の URL カテゴリ セット アップデートについて

セキュリティ管理アプライアンス上の一連の URL カテゴリのアップデートについては、次を参照してください。

- 「URL カテゴリ セットの更新と中央集中型コンフィギュレーション管理」（P.8-25）
- 「URL カテゴリ セットの更新とレポート」（P.5-28）

生成されたメッセージの返信アドレスの設定

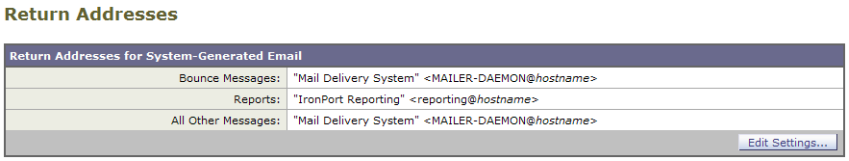
次の場合に対して、AsyncOS で生成されたメールのエンベロープ送信者を設定できます。

- バウンス メッセージ
- レポート

返信アドレスの表示、ユーザ、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。

GUI の [System Administration] メニューから利用できる [Return Addresses] ページを使用するか、CLI で **addressconfig** コマンドを使用します。

図 13-9　[Return Addresses] ページ



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 で変更するには、[Return Addresses] ページで [Edit Settings] をクリックします。1 つまたは複数のアドレスを変更して [Submit] をクリックし、変更を保存します。

アラートの管理

アラートとは、Cisco IronPort アプライアンスで発生しているイベントに関する情報が記載されている、電子メールによる通知のことです。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、一般的にアプライアンス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、Cisco IronPort アプライアンスで生成されます。どのアラート メッセージがどのユーザに送信され、イベントの重大度がどの程度である場合にアラートが送信されるかは、非常にきめ細かなレベルで指定できます。アラートの管理は、GUI の [Management Appliance] > [System Administration] > [Alerts] ページで行います（または、CLI で `alertconfig` コマンドを使用します）。

アラートの概要

次の機能によって、電子メール通知の動作が制御されます。

- **アラート**：電子メール通知を受け取るアラートを作成します。アラートは、アラートの受信者（受信アラートの電子メール アドレス）と、アラート通知（重大度とアラート タイプを含む）で構成されています。
- **アラート設定**：アラート機能の全般的な動作を指定します。たとえば、アラートの送信者（FROM:）のアドレス、重複アラートを送信する秒間隔、および AutoSupport をイネーブルにするかどうか（および、オプションで週次 AutoSupport レポートを送信するかどうか）などを指定します。

アラート：アラート受信者、アラート分類、および重要度

アラートとは、ハードウェア問題などの特定の機能についての情報が含まれている電子メール メッセージまたは通知であり、アラートの受信者に送信されます。アラート受信者とは、アラート通知が送信される電子メール アドレスのことです。通知に含まれる情報は、アラートの分類と重大度によって決まります。どのアラート分類を、どの重大度で、特定のアラート受信者に送信するかを指定できます。アラート エンジンを使用して、受信者に送信されるアラートを詳細に制御できます。たとえば、重大度レベルが Critical であり、アラート タイプが System の場合など、特定のタイプのアラートのみが受信者に送信されるようにシステムを設定できます。また、一般的な設定値も設定できます（「アラート設定値の設定」（P.13-35）を参照してください）。すべてのアラートのリストについては、「アラート リスト」（P.13-36）を参照してください。

アラートの分類

AsyncOS では、次のアラート分類を送信します。

- システム
- ハードウェア

重大度

アラートは、次の重大度に従って送信されます。

- Critical：すぐに対処が必要な問題
- Warning：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
- Info：このデバイスのルーティン機能で生成される情報

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 レベルのシステム 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 の週次ステータス 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。この増加は、待機する秒数に、直前の間隔の 2 倍を加えたものになります。つまり、待機時間が 5 秒間の場合、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、送信間隔は非常に長くなります。[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。

アラートの配信

アラート メッセージは Cisco IronPort アプライアンス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。
  - 5.X よりも前の AsyncOS バージョンでは、アラート メッセージに SMTP ルートが使用されません。
  - 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。

Cisco IronPort AutoSupport

Cisco IronPort による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 Cisco IronPort Systems に送信するように Cisco IronPort アプライアンスを設定できます。「AutoSupport」と呼ばれるこの機能は、Cisco IronPort カスタマー サポート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、Cisco IronPort 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」（P.13-35）を参照してください。

アラート メッセージ

アラート メッセージは標準的な電子メール メッセージです。Header From: アドレスは設定できますが、メッセージのその他の部分は自動的に生成されます。

アラートの From アドレス

Header From: アドレスは、GUI で [Edit Settings] ボタンをクリックするか、CLI（『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照）を使用して設定できます。

アラートの件名

アラート メッセージの件名は、次の形式になります。

```
Subject: [severity]-[hostname]: ([class]) short message
```

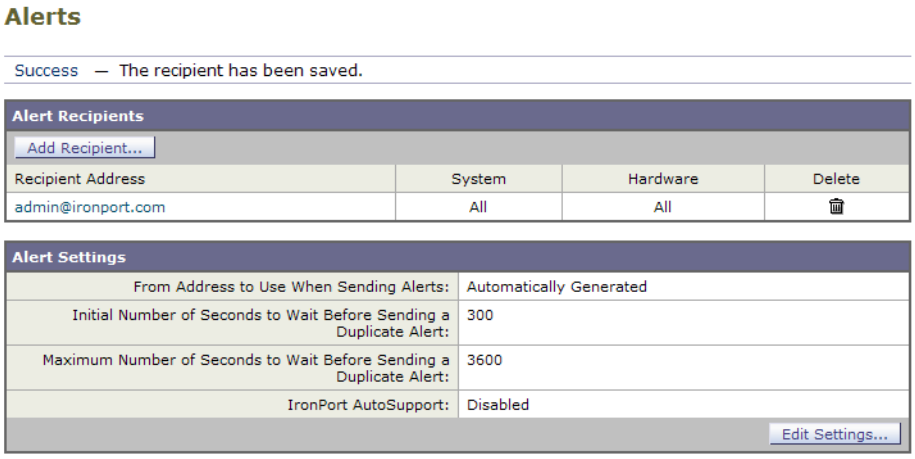
アラート メッセージの例

```
Date: 23 Mar 2007 21:10:19 +0000
To: joe@example.com
From: Cisco IronPort M650 Alert [alert@example.com]
Subject: Critical-example.com: (AntiVirus) update via http://newproxy.example.com failed

The Critical message is:

update via http://newproxy.example.com failed

Version: 6.0.0-419
Serial Number: XXXXXXXXXXXX-XXXXXXX
Timestamp: Tue May 10 09:39:24 2007

For more information about this error, please see
    http://support.ironport.com
If you need further information, contact your support provider.
```

アラート受信者の管理

GUI にログインして、[System Administration] > [Alerts] を選択します。（GUI へのアクセス方法の詳細については、「セキュリティ管理アプライアンスへのアクセス」（P.2-8）を参照してください）。

図 13-10　[Alerts] ページ



（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 アドレスはデフォルトで、すべての重大度およびクラスのアラートを受信します。この設定はいつでも変更できます。

[Alerts] ページは、既存のアラート受信者およびアラート設定のリストを表示します。

[Alerts] ページからは、次の操作ができます。

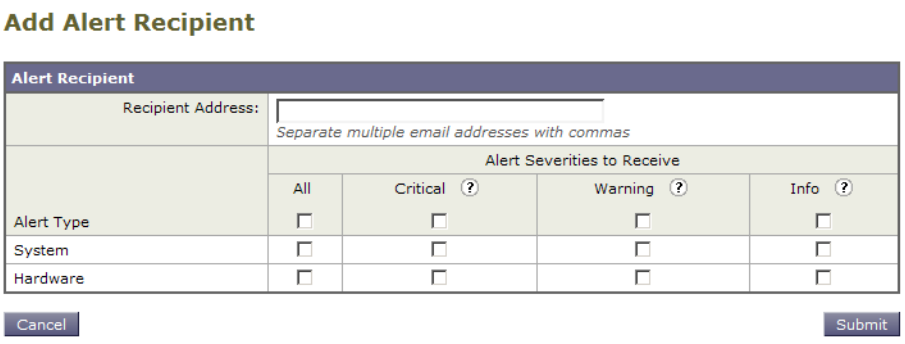
- アラート受信者の追加、設定、または削除。
- アラート設定値の変更。

新規アラート受信者の追加

新規アラート受信者を追加するには、次の手順を実行します。

ステップ 1　[Alerts] ページで [Add Recipient] をクリックします。[Add Alert Recipients] ページが表示されます。

図 13-11　アラート受信者の追加



ステップ 2　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 3　アラート受信者が受信するアラート重大度を選択します。

ステップ 4　[Submit] をクリックして、アラート受信者を追加します。

ステップ 5　変更を保存します。

既存のアラート受信者の設定

既存のアラート受信者を編集するには、次の手順を実行します。

ステップ 1　[Alert Recipients] のリストからアラート受信者をクリックします。[Configure Alert Recipient] ページが表示されます。

ステップ 2　アラート受信者の設定を変更します。

ステップ 3　変更を送信し、保存します。

アラート受信者の削除

アラート受信者を削除するには、次の手順を実行します。

ステップ 1　[Alert Recipient] のリストから、アラート受信者に対応するゴミ箱アイコンをクリックします。

ステップ 2　表示される警告ダイアログで [Delete] をクリックして削除を確認します。

ステップ 3　変更を保存します。

アラート設定値の設定

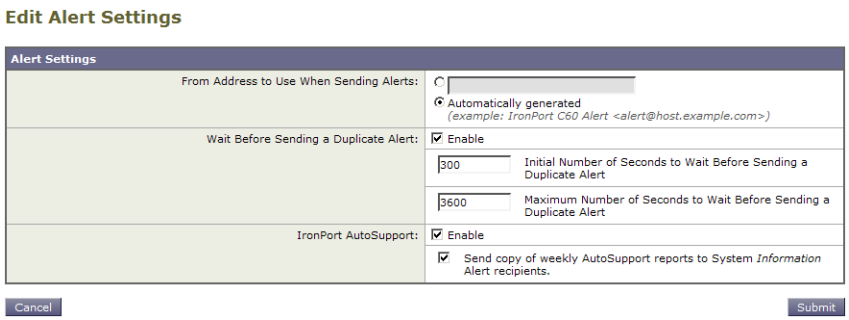
アラート設定は、セキュリティ管理アプライアンスが送信するすべてのアラートに適用されます。

アラート設定値の編集

アラート設定値を編集するには、次の手順を実行します。

ステップ 1　[Alerts] ページで [Edit Settings] をクリックします。[Edit Alert Settings] ページが表示されます。

図 13-12　　アラート設定値の編集



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、[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」（P.13-32）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　必要に応じて、[Cisco IronPort AutoSupport] オプションを選択して、AutoSupport をイネーブルにします。AutoSupport の詳細については、「Cisco IronPort AutoSupport」（P.13-32）を参照してください。

- AutoSupport がイネーブルの場合、Information レベルのシステム 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、週次 AutoSupport レポートが送信されます。チェックボックスを使用して、これを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 リスト

次の表に、アラート名、説明、および重大度など、アラートを分類別に示します。

ハードウェア アラート

表 13-2 には、アラートの説明やアラートの重大度など、AsyncOS によって生成される可能性のあるさまざまなハードウェア アラートを示してあります。

表 13-2　ハードウェア アラートのリスト

アラート名	説明	重大度
INTERFACE.ERRORS	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。	Warning
MAIL.MEASUREMENTS_FILESYSTEM	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。	Warning
MAIL.MEASUREMENTS_FILESYSTEM.CRITICAL	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。	Critical
SYSTEM.RAID_EVENT_ALERT	重大な RAID-event が発生した場合に送信されます。	Warning
SYSTEM.RAID_EVENT_ALERT_INFO	RAID-event が発生した場合に送信されます。	Information

システム アラート

表 13-3 には、アラートの説明やアラートの重大度など、AsyncOS によって生成される可能性のあるさまざまなシステム アラートを示してあります。

表 13-3　システム アラートのリスト

アラート名	説明	重大度
COMMON.APP_FAILURE	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。	Critical
COMMON.KEY_EXPIRED_ALERT	機能キーの有効期限が切れた場合に送信されます。	Warning
COMMON.KEY_EXPIRING_ALERT	機能キーの有効期限が切れる場合に送信されます。	Warning
COMMON.KEY_FINAL_EXPIRING_ALERT	機能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。	Warning
DNS.BOOTSTRAP_FAILED	アプライアンスがルート 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。	Warning
INTERFACE.FAILOVER.FAILURE_BACKUP_DETECTED	バックアップ NIC ペアリング インターフェイスが故障した場合に送信されます。	Warning
INTERFACE.FAILOVER.FAILURE_BACKUP_RECOVERED	NIC ペアのフェールオーバーが復旧した場合に送信されます。	Information
INTERFACE.FAILOVER.FAILURE_DETECTED	インターフェイス故障により、NIC ペアリング フェールオーバーが検出された場合に送信されます。	Critical
INTERFACE.FAILOVER.FAILURE_DETECTED_NO_BACKUP	インターフェイス故障により NIC ペアリング フェールオーバーは検出されたけれども、バックアップ インターフェイスが利用できない場合に送信されます。	Critical
INTERFACE.FAILOVER.FAILURE_RECOVERED	NIC ペアのフェールオーバーが復旧した場合に送信されます。	Information
INTERFACE.FAILOVER.MANUAL	別の NIC ペアへの手動フェールオーバーが検出された場合に送信されます。	Information
COMMON.INVALID_FILTER	無効なフィルタが存在する場合に送信されます。	Warning
LDAP.GROUP_QUERY_FAILED_ALERT	LDAP グループ クエリーに失敗した場合に送信されます。	Critical
LDAP.HARD_ERROR	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。	Critical
LOG.ERROR.*	さまざまなロギング エラー。	Critical

表 13-3　システム アラートのリスト （続き）

アラート名	説明	重大度
MAIL.PERRCPT.LDAP_ GROUP_QUERY_FAILED	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。	Critical
MAIL.QUEUE.ERROR.*	メール キューのさまざまなハード エラー。	Critical
MAIL.RES_CON_START_ ALERT.MEMORY	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。	Critical
MAIL.RES_CON_START_ ALERT.QUEUE_SLOW	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。	Critical
MAIL.RES_CON_START_ ALERT.QUEUE	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。	Critical
MAIL.RES_CON_START_ ALERT.WORKQ	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。	Critical
MAIL.RES_CON_START_ ALERT	アプライアンスが「リソース節約」モードに入った場合に送信されます。	Critical
MAIL.RES_CON_STOP_ ALERT	アプライアンスの「リソース節約」モードが解除された場合に送信されます。	Critical
MAIL.WORK_QUEUE_ PAUSED_NATURAL	ワーク キューが中断された場合に送信されます。	Critical
MAIL.WORK_QUEUE_ UNPAUSED_NATURAL	ワーク キューが再開された場合に送信されます。	Critical
NTP.NOT_ROOT	NTP が root として動作していないため、Cisco IronPort アプライアンスが時刻を調整できない場合に送信されます。	Warning
PERIODIC_REPORTS. DOMAIN_REPORT. DOMAIN_FILE_ERRORS	ドメイン指定ファイルでエラーが検出された場合に送信されます。	Critical
PERIODIC_REPORTS. DOMAIN_REPORT.FILE_ EMPTY	ドメイン指定ファイルが空の場合に送信されます。	Critical

表 13-3　システム アラートのリスト （続き）

アラート名	説明	重大度
PERIODIC_REPORTS. DOMAIN_REPORT.FILE_ MISSING	ドメイン指定ファイルが見つからない場合に送信されます。	Critical
REPORTD.DATABASE_ OPEN_FAILED_ALERT	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。	Critical
REPORTD.AGGREGATION_DISABLED_ALERT	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。	Warning
REPORTING.CLIENT. UPDATE_FAILED_ALERT	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。	Warning
REPORTING.CLIENT. JOURNAL.FULL	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。	Critical
REPORTING.CLIENT. JOURNAL.FREE	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。	Information
PERIODIC_REPORTS. REPORT_TASK.BUILD_ FAILURE_ALERT	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。	Critical
PERIODIC_REPORTS. REPORT_TASK.EMAIL_ FAILURE_ALERT	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。	Critical
PERIODIC_REPORTS. REPORT_TASK.ARCHIVE_FAILURE_ALERT	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。	Critical
SENDERBASE.ERROR	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。	Information
SMAD.ICCM.ALERT_ PUSH_FAILED	1 台以上のホストでコンフィギュレーションのプッシュに失敗した場合に送信されます。	Warning
SMAD.TRANSFER. TRANSFERS_STALLED	SMA ログがトラッキング データを 2 時間取得できなかった場合、またはレポーティング データを 6 時間取得できなかった場合に送信されます。	Warning
SMTPAUTH.FWD_SERVER_FAILED_ALERT	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。	Warning

表 13-3　システム アラートのリスト （続き）

アラート名	説明	重大度
SMTPAUTH.LDAP_QUERY_FAILED	LDAP クエリーが失敗した場合に送信されます。	Warning
SYSTEM.HERMES_SHUTDOWN_FAILURE.REBOOT	リブート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。	Warning
SYSTEM.HERMES_SHUTDOWN_FAILURE.SHUTDOWN	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。	Warning
SYSTEM.RCPTVALIDATION.UPDATE_FAILED	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。	Critical
SYSTEM.SERVICE_TUNNEL.DISABLED	Cisco IronPort サポート サービス用に作成されたトンネルがディセーブルの場合に送信されます。	Information
SYSTEM.SERVICE_TUNNEL.ENABLED	Cisco IronPort サポート サービス用に作成されたトンネルがイネーブルの場合に送信されます。	Information

ネットワーク設定値の変更

このセクションでは、Cisco IronPort アプライアンス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 ウィザードの実行」（P.2-10）でシステム セットアップ ウィザー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 で設定。および CLI で `dnsconfig` コマンドを使用して設定）
- ルーティング設定（GUI で設定。および CLI で `routeconfig` コマンドと `setgateway` コマンドを使用して設定）
- `dnsflush`
- パスワード

システム ホスト名の変更

ホスト名は、CLI プロンプトでシステムを識別する際に使用されます。完全修飾ホスト名を入力する必要があります。`sethostname` コマンドは、Cisco IronPort アプライアンスの名前を設定します。新規ホスト名は、`commit` コマンドを発行して初めて有効になります。

sethostname コマンド

```
oldname.example.com> sethostname

[oldname.example.com]> mail3.example.com
```

```
oldname.example.com>
```

ホスト名の変更を有効にするには、commit コマンドを入力する必要があります。ホスト名の変更を確定すると、CLI プロンプトに新しいホスト名が表示されます。

```
oldname.example.com> commit

Please enter some comments describing your changes:
[]> Changed System Hostname
Changes committed: Mon Jan 04 12:00:01 2010
```

プロンプトに新規ホスト名が次のように表示されます。mail3.example.com>

ドメイン ネーム システム設定値の設定

Cisco IronPort アプライアンスのドメイン ネーム システム（DNS）は、GUI の [Management Appliance] > [Network] > [DNS] ページ、または dnsconfig コマンドを使用して設定できます。

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、インターネットのルート DNS サーバ、または指定した権威 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、該当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）になっている必要があります。

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 を設定しているときは、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」をドメインとして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。その 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。次にシステムは最初のクエリーが期限切れになるか、「タイムアウト」になるまで短時間待機した後、さらにそれよりわずかに長い秒数待機するという動作を続けます。待機時間の長さは、DNS サーバの実際の総数と、設定されたプライオリティによって異なります。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 13-4　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 のサーバの 1 つがダウンしている場合は、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ー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

Cisco IronPort アプライアンスは電子メールの送受信の際に、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「ダブル DNS ルックアップ」の実行を試みます。つまり、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、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」（P.13-41）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。

デフォルト値は、20 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ディセーブルにできます。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。

DNS アラート

アプライアンスのリブート時に、メッセージ「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まれにあります。このメッセージは、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。

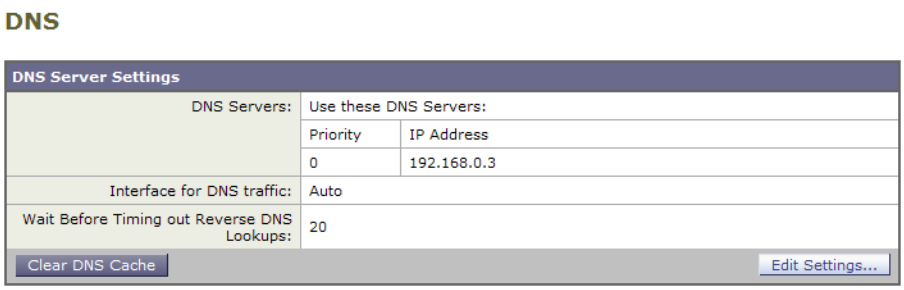
DNS キャッシュのクリア

GUI の [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、『*Cisco IronPort AsyncOS CLI Reference Guide*』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 インターフェイスを使用した DNS 設定値の設定

GUI にログインして、[Management Appliance] > [Network] > [DNS] を選択します。

図 13-13　[DNS] ページ

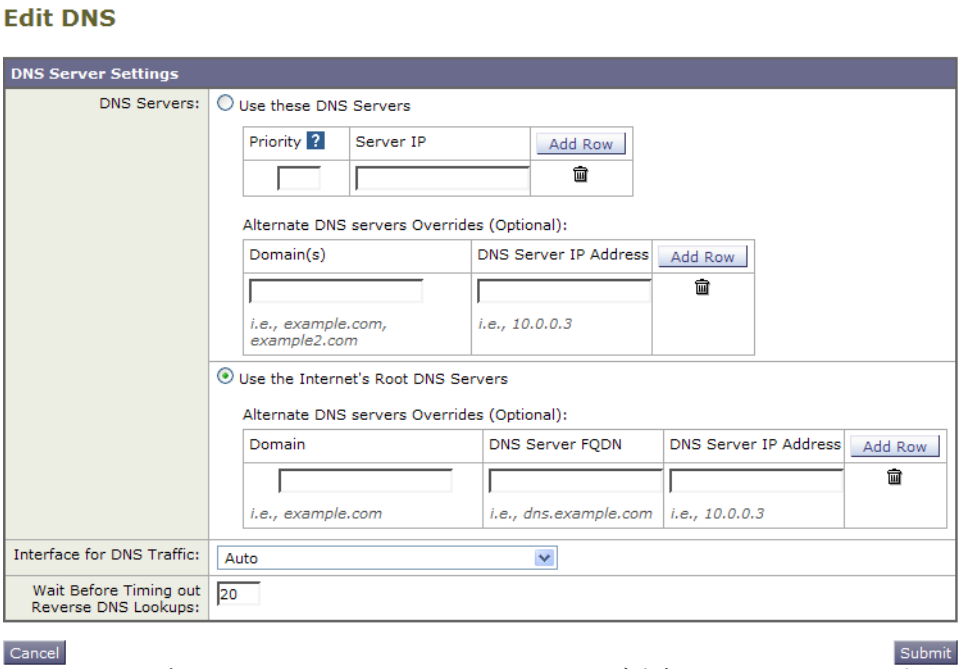


DNS 設定値を GUI から編集するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [Network] > [DNS] ページで、[Edit Settings] ボタンをクリックします。

[Edit DNS] ページが表示されます。

図 13-14　[Edit DNS] ページ



ステップ 2　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 サーバのどちらを使用するかを選択して、権威 DNS サーバを指定します。

ステップ 3　ユーザ独自の DNS サーバを使用するか、権威 DNS サーバを指定する場合は、サーバ ID を入力し [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」（P.13-41）を参照してください。

ステップ 4　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 5　逆引き DNS ルックアップをキャンセルするまでに待機する秒数を入力します。

ステップ 6　必要に応じて、[Clear Chashe] をクリックして、DNS キャッシュをクリアします。

ステップ 7　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。スタティック ルートの管理は、GUI の [Management Appliance] > [Network] > [Routing] ページ、または CLI の `routeconfig` コマンドを使用して行います。

GUI でのスタティック ルートの管理

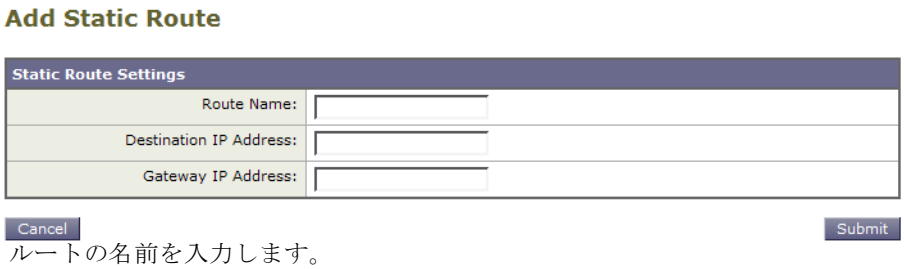
[Management Appliance] > [Network] > [Routing] ページを使用して、スタティック ルートの作成、編集、または削除を行えます。このページからデフォルト ゲートウェイの変更もできます。

スタティック ルートの追加

新しいスタティック ルートを作成するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [Network] > [Routing] ページで、ルート リストの [Add Route] をクリックします。[Add Static Route] ページが表示されます。

図 13-15　スタティック ルートの追加



ステップ 2　ルートの名前を入力します。

ステップ 3　宛先 IP アドレスを入力します。

ステップ 4　ゲートウェイの IP アドレスを入力します。

ステップ 5　変更を送信し、保存します。

スタティック ルートの削除

スタティック ルートを削除するには、次の手順を実行します。

ステップ 1　[Static Routes] のリストから、スタティック ルート名に対応するゴミ箱アイコンをクリックします。

ステップ 2　表示される警告ダイアログで [Delete] をクリックして削除を確認します。

ステップ 3　変更を保存します。

スタティック ルートの編集

スタティック ルートを編集するには、次の手順を実行します。

ステップ 1　[Static Routes] のリストでルートの名前をクリックします。[Edit Static Route] ページが表示されます。

ステップ 2　ルートの設定を変更します。

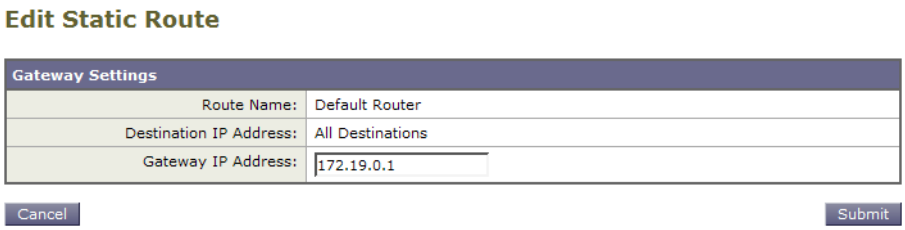
ステップ 3　変更を送信し、保存します。

デフォルト ゲートウェイの変更（GUI）

デフォルト ゲートウェイを変更するには、次の手順を実行します。

ステップ 1　[Routing] ページのルート リストで [Default Route] をクリックします。[Edit Static Route] ページが表示されます。

図 13-16　デフォルト ゲートウェイの編集



ステップ 2　ゲートウェイの IP アドレスを変更します。

ステップ 3　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

GUI の [Management Appliance] > [Network] > [Routing] ページ（「デフォルト ゲートウェイの変更（GUI）」（P.13-45）を参照してください）、または CLI の `setgateway` コマンドを使用して、デフォルト ゲートウェイを設定できます。

admin ユーザのパスワード変更

admin ユーザのパスワードは GUI または CLI から変更できます。

GUI を使用してパスワードを変更するには、[Management Appliance] > [System Administration] > [Users] ページに移動します。詳細については、「パスワードの設定と変更」（P.12-15）を参照してください。

`admin` ユーザのパスワードを CLI から変更するには、`password` コマンドを使用します。パスワードは 6 文字以上である必要があります。`password` コマンドでは、セキュリティのために古いパスワードの入力が必要です。

（注）　パスワードの変更はすぐに有効になり、**commit** コマンドの実行は不要です。

システム時刻の設定

Cisco IronPort アプライアンスのシステム時刻を設定し、時間帯を指定できます。GUI の [Management Appliance] > [System Administration] > [Time Zone] ページと、[Management Appliance] > [System Administration] > [Time Settings] ページを使用します。または、CLI で `ntpconfig`、`settime`、および `settz` コマンドを使用します。

[Time Zone] ページ

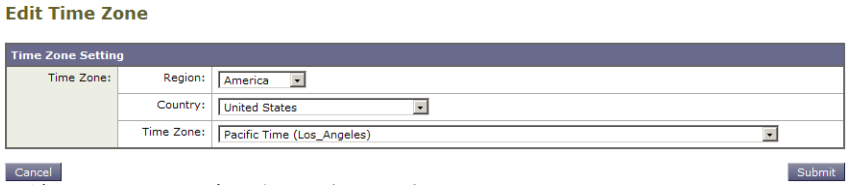
[Time Zone] ページ（GUI の [System Administration] メニューから利用可能）では、Cisco IronPort アプライアンスの時間帯が表示されます。特定の時間帯または GMT オフセットを選択できます。

時間帯の選択

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

ステップ 1　[Management Appliance] > [System Administration] > [Time Zone] ページで、[Edit Settings] をクリックします。[Edit Time Zone] ページが表示されます。

図 13-17　[Edit Time Zone] ページ



ステップ 2　地域、国、および時間帯を選択します。

ステップ 3　変更を送信し、保存します。

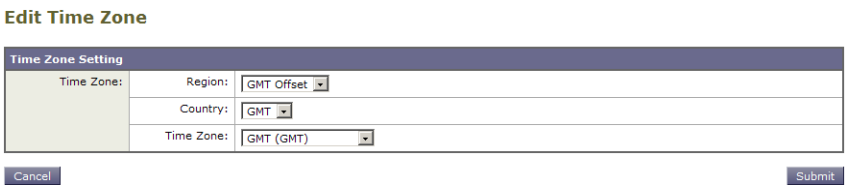
GMT オフセットの選択

Cisco IronPort アプライアンスの GMT オフセットを設定するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [System Administration] > [Time Zone] ページで、[Edit Settings] をクリックします。[Edit Time Zone] ページが表示されます。

ステップ 2　地域のリストから [GMT Offset] を選択します。[Time Zone Setting] ページが更新され、[Time Zone] フィールドに GMT オフセットが含まれるようになります。

図 13-18　GMT オフセットの設定



ステップ 3　[Time Zone] フィールドでオフセットを選択します。オフセットとは、グリニッジ子午線のローカル時間であるグリニッジ標準時（GMT）に、加算または減算する時間のことです。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西側にあたります。プラス記号（「+」）の場合、グリニッジ子午線の東側にあたります。

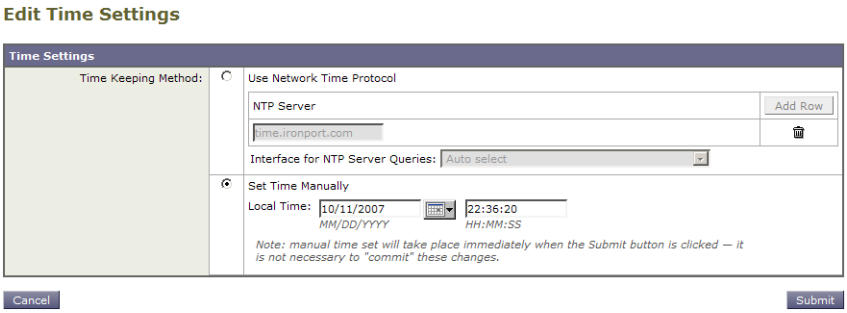
ステップ 4　変更を送信し、保存します。

（注）　セキュリティ管理アプライアンスは、レポートのデータを収集する際に、セキュリティ管理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。セキュリティ管理アプライアンスが情報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。

時刻設定の編集（GUI）

Cisco IronPort アプライアンスの時刻設定を編集するには、[Management Appliance] > [System Administration] > [Time Setting] ページで、[Edit Settings] ボタンをクリックします。[Edit Time Setting] ページが表示されます。

図 13-19　[Edit Time Settings] ページ



ネットワーク タイム プロトコル（NTP）設定の編集（Time Keeping Method）

他のコンピュータとのシステム クロックの同期に NTP サーバを使用し、NTP サーバの設定値を編集するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [System Administration] > [Time Settings] ページで、[Edit Settings] をクリックします。[Edit Time Setting] ページが表示されます。

ステップ 2　[Time Keeping Method] セクションで、[Use Network Time Protocol] を選択します。

ステップ 3　NTP サーバのアドレスを入力し、[Add Row] をクリックします。複数の NTP サーバを追加できます。

ステップ 4　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 5　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 6　変更を送信し、保存します。

NTP サーバを使用しないシステム時刻の設定

NTP サーバを使用せずに手動でシステム時刻を設定するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [System Administration] > [Time Settings] ページで、[Edit Settings] をクリックします。[Edit Time Setting] ページが表示されます。

ステップ 2　[Time Keeping Method] セクションで、[Set Time Manually] を選択します。

ステップ 3　日付を MM/DD/YYYY 形式で入力するか、カレンダーのアイコンをクリックして日付を選択します。

ステップ 4　ローカル時刻を HH:MM:SS の形式で入力します。

ステップ 5　変更を送信し、保存します。

時間帯ファイルの更新

セキュリティ管理アプライアンスの各時間帯ファイルには、特定の時間帯の相対時刻を指定する規則が含まれています。AsyncOS の更新と更新の間であればいつでも、セキュリティ管理アプライアンスの時間帯ファイルを更新できます。いずれかの国の時間帯に変更があった場合は必ず、アプライアンスでこれらのファイルを更新する必要があります。

時間帯ファイルの更新は、GUI で行うか、CLI の `tzupdate` コマンドを使用して行えます。

時間帯ファイルの自動更新

ステップ 1　[Management Appliance] > [System Administration] > [Update Settings] を選択します。

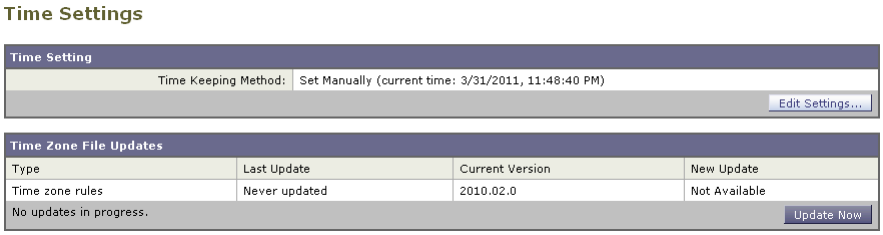
ステップ 2　[Enable automatic updates for Time zone rules] チェックボックスをオンにします。

ステップ 3　間隔を入力します。重要な情報については、ページ上の [?] ヘルプをクリックします。

ステップ 4　まだ実行していない場合は、このページの他の設定値を設定します。「アップグレードおよびサービスアップデートの設定」（P.13-20）を参照してください。

時間帯ファイルの手動更新

ステップ 1　[Management Appliance] > [System Administration] > [Time Settings] ページに移動します。



ステップ 2　使用可能な時間帯ファイルの更新がある場合、[Update Now] をクリックします。

[Configuration File] ページ

次のセクションの詳細について	参照先
現在の設定の保存	「コンフィギュレーション設定の保存とインポート」（P.13-50）
保存されている設定のロード	「コンフィギュレーション設定の保存とインポート」（P.13-50）
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）	「セーフリスト/ブロックリスト データベースのバックアップと復元」（P.7-15）
設定のリセット	出荷時の初期状態へのリセット

コンフィギュレーション設定の保存とインポート

（注）　ここで説明されているコンフィギュレーション ファイルは、セキュリティ管理アプライアンスの設定に使用されます。第 8 章「Web セキュリティ アプライアンスの管理」で説明されているコンフィギュレーション ファイルおよび Configuration Master は、Web セキュリティ アプライアンスの設定に使用されます。

セキュリティ管理アプライアンスの大部分の設定は、1 つのコンフィギュレーション ファイルで管理できます。このファイルは Extensible Markup Language（XML）フォーマットで保持されます。

次のように、このファイルはさまざまな用途に使用できます。

- プライマリ セキュリティ管理アプライアンスで予期しない障害が発生した場合に、2 番目のセキュリティ管理アプライアンスをすばやく設定し、サービスを復元できます。
- コンフィギュレーション 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。アプライアンスの設定中に間違いを犯した場合、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、アプライアンスの全体の設定を素早く確認できます（新しいブラウザの多くには 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）。これは、現在の設定にある可能性のあるマイナー エラー（誤植など）のトラブルシューティングに役立つ場合があります。
- 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て、変更を行い、同じアプライアンス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 GUI の両方が「バイパス」されます。
- FTP を介してコンフィギュレーション ファイル全体をアップロードしたり、コンフィギュレーション ファイルの一部を CLI に直接貼り付けたりすることができます。
- このファイルは XML 形式になっているため、コンフィギュレーション ファイルのすべての XML エンティティが記述された、関連する文書型定義（DTD）も提供されます。XML コンフィギュレーション 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 コンフィギュレーション 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 コンフィギュレーション ファイルを使用した複数のアプライアンスの管理

警告　ある セキュリティ管理アプライアンスから別の セキュリティ管理アプライアンスにコンフィギュレーション ファイルをインポートする場合は、次の点に注意してください。

元の設定内のすべて（IP アドレスを含む）が、コンフィギュレーション ファイルに含まれています。コンフィギュレーション ファイルを編集して IP アドレスを変更するか、元の セキュリティ管理アプライアンスがオフラインになっていることを確認します。

また、SSH 認証接続が終了することに注意してください。そうなった場合は、接続されたすべての 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 アプライアンスとの接続を再確立する必要があります。

- ある Cisco IronPort アプライアンスから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、変更を行い、別のアプライアンスにアップロードできます。これにより、複数の Cisco IronPort アプライアンスのインストール済み環境の管理が容易になります。ただし、電子メール セキュリティ アプライアンスからセキュリティ管理アプライアンスに、コンフィギュレーション ファイルをロードすることはできません。
- あるアプライアンスからダウンロードされた既存のコンフィギュレーション ファイルを、複数のサブセクションに分割できます。（複数のアプライアンス環境の）すべてのアプライアンス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アプライアンスにロードできます。

  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アプライアンスを使用できます。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 アプライアンス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アプライアンスにロードできます。

GUI を使用したコンフィギュレーション ファイルの管理

アプライアンスでコンフィギュレーション ファイルを管理するには、[Management Appliance] > [System Administration] > [Configuration File] を選択します。

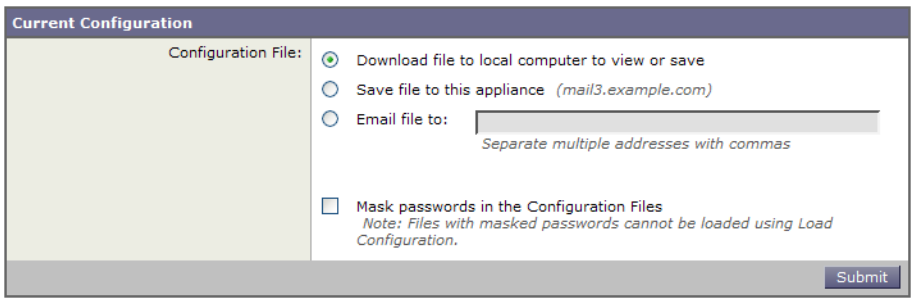
[Configuration File] ページには、次のセクションが含まれています。

- [Current Configuration]：現在のコンフィギュレーション 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
- [Load Configuration]：コンフィギュレーション ファイルの全体または一部をロードするために使用します
- [End-User Safelist/Blocklist Database (Cisco IronPort Spam Quarantine)]：セーフリスト/ブロックリスト データベースの管理に使用します
- [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）

現在のコンフィギュレーション ファイルの保存およびエクスポート

[Management Appliance] > [System Administration] > [Configuration File] ページの [Current Configuration] セクションを使用すると、現在のコンフィギュレーション ファイルを、ローカル マシンに保存したり、アプライアンスで保存したり（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。

図 13-20　現在のコンフィギュレーション ファイル



チェックボックスをオンすると、ユーザのパスワードをマスクできます。パスワードをマスクすると、元の暗号化されたパスワードが、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。

（注）　パスワードがマスクされたコンフィギュレーション ファイルをロードして AsyncOS に戻すことはできません。

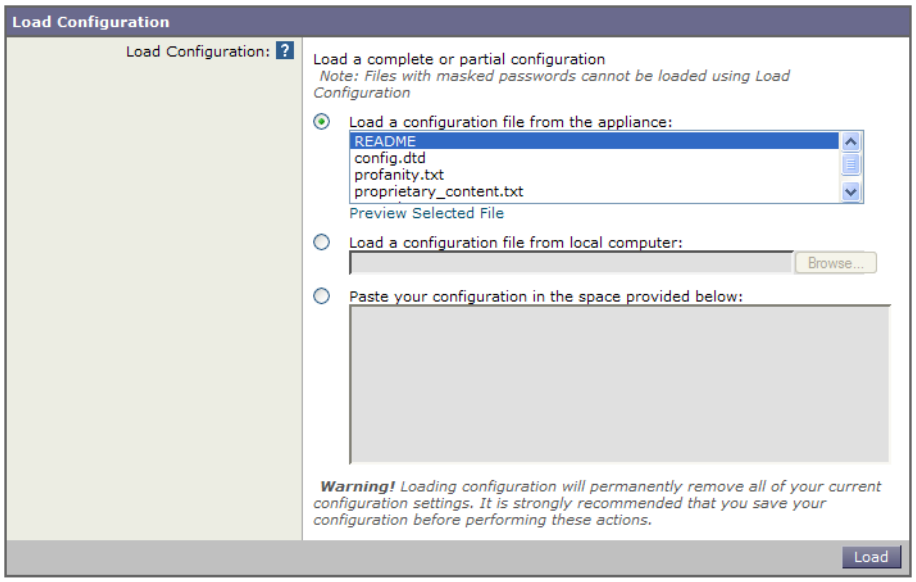
コンフィギュレーション ファイルのロード

[Management Appliance] > [System Administration] > [Configuration File] ページの [Load Configuration] セクションを使用して、新しい設定情報を Cisco IronPort アプライアンスにロードします。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
- コンフィギュレーション ファイルをローカル マシンから直接アップロードする
- GUI に設定情報を直接貼り付ける

パスワードがマスクされたコンフィギュレーション ファイルはロードできません。

図 13-21　コンフィギュレーション ファイルのロード



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、Cisco IronPort アプライアンスの `configuration` ディレクトリにある DTD 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。コンフィギュレーション ファイルをアップロードする前に、アプライアンスの外部で DTD をダウンロードし、コンフィギュレーション ファイルを検証できます。

いずれの方法の場合でも、コンフィギュレーション 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）またはコンフィギュレーション 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、次のコードをアップロードまたは貼り付けると、検証エラーが発生します。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <autosupport_enabled>0</autosu
</config>
```

しかし、次のコードをアップロードまたは貼り付けても、検証エラーは発生しません。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <autosupport_enabled>0</autosupport_enabled>
</config>
```

「unique（一意）」とは、アップロードまたは貼り付けられるコンフィギュレーション 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てないため、次のコード（宣言および <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>
```

しかし、システムにはそれぞれ異なる受信者アクセス テーブルが定義された複数のリスナーが定義されている可能性があるため、次のコードのみをアップロードすることは多義的であると見なされます。

```
<rat>
   <rat_entry>
     <rat_address>ALL</rat_address>
     <access>RELAY</access>
   </rat_entry>
 </rat>
```

多義的であるため、「完全」な構文であっても許可されません。

警告　コンフィギュレーション ファイルまたはコンフィギュレーション ファイルのサブセクションをアップロードまたは貼り付ける場合は、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。

空のタグと省略されたタグ

コンフィギュレーション ファイルのセクションをアップロードまたは貼り付け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、次のコード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。

```
<listeners></listeners>
```

警告　**コンフィギュレーション 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、GUI 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アプライアンス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。新しいコンフィギュレーション ファイルをロードする前に、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ワードのロードについての注意事項

パスワードが必要なログ 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ワード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ワード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ます。

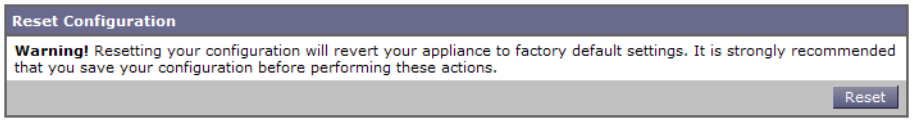
```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

現時点では、このエンコーディングを持つコンフィギュレーション ファイルだけをロードできます。

現在の設定のリセット

現在の設定をリセットすると、Cisco IronPort アプライアンス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してください。GUI の [Reset] ボタンを使用した設定のリセットは、クラスタリング環境ではサポートされていません。

図 13-22　コンフィギュレーション ファイルのリセット



「出荷時の初期状態へのリセット」（P.13-5）を参照してください。

コンフィギュレーション ファイル用の CLI コマンド

次のコマンドを使用すると、コンフィギュレーション ファイルを操作できます。

- `showconfig`
- `mailconfig`
- `saveconfig`
- `loadconfig`
- `resetconfig`（「出荷時の初期状態へのリセット」（P.13-5）を参照）
- `publishconfig`

- backupconfig

showconfig、mailconfig、および saveconfig コマンド

コンフィギュレーション コマンドの showconfig、mailconfig、および saveconfig の場合は、電子メールで送信されるファイルまたは表示されるファイルにパスワードを含めるかどうか選択することを求められます。パスワードを含めないことを選択すると、パスワード フィールドが空白のままになります。セキュリティの問題を心配する場合は、パスワードを含めないことを選択できます。ただし、loadconfig コマンドを使用してロードされた場合、パスワードがないコンフィギュレーション ファイルは失敗します。「ログ サブスクリプションのパスワードのロードについての注意事項」（P.13-54）を参照してください。

（注）　パスワードを含めることを選択した場合（「Do you want to include passwords?」に「yes」と回答します）にコンフィギュレーション ファイルを保存、表示、または電子メールで送信するとき、パスワードは暗号化されます。ただし、秘密キーと証明書は暗号化されていない PEM フォーマットで含まれます。

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 passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig.

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">

<!--
  Product: Cisco 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.]
```

mailconfig コマンドを使用して、現在の設定をユーザに電子メールで送信します。メッセージには config.xml という名前の XML 形式のコンフィギュレーション ファイルが添付されます。

```
mail3.example.com> mailconfig

Please enter the email address to which you want to send
the configuration file.
[]> administrator@example.com

Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig.  [N]> y

The configuration file has been sent to administrator@example.com.
```

セキュリティ管理アプライアンスで saveconfig コマンドを使用すると、一意のファイル名を使用して、すべての Configuration Master ファイル（ESA および WSA）が configuration ディレクトリに保存されます。

```
mail3.example.com> saveconfig

Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig.  [N]> y
```

```
The file C650-00065B8FCEAB-31PM121-20030630T130433.xml has been saved in the configuration
directory.
mail3.example.com>
```

loadconfig コマンド

Cisco IronPort アプライアンスに新しい設定情報をロードするには、loadconfig コマンドを使用します。情報は次の 2 つのいずれかの方法でロードできます。

ステップ 1　configuration ディレクトリに情報を格納し、アップロードする

ステップ 2　CLI に設定情報を直接貼り付ける。

詳細については、「コンフィギュレーション ファイルのロード」（P.13-52）を参照してください。

publishconfig コマンド

変更を Configuration Master に公開するには、publishconfig コマンドを使用します。構文は次のとおりです。

publishconfig *config_master* [*job_name*] [*host_list* | *host_ip*

ここで、*config_master* は、「SMA 互換性マトリクス」（P.2-2）の表 2-3 に示すとおり、サポートされている Configuration Master です。このキーワードは必須です。キーワード *job_name* は省略可能で、指定しなかった場合は生成されます。

キーワード *host_list* は、公開される WSA アプライアンスのホスト名または IP アドレスのリストで、指定しなかった場合は、Configuration Master に割り当てられているすべてのホストに公開されます。オプションの *host_ip* には、カンマで区切って複数のホスト IP アドレスを指定できます。

publishconfig コマンドが成功したことを確認するには、smad_logs ファイルを調べます。[Web] > [Utilities] > [Web Appliance Status] を選択することで、セキュリティ管理アプライアンスの GUI から公開履歴が成功だったことを確認することもできます。このページから、公開履歴の詳細を調べる Web アプライアンスを選択します。また、[Web] > [Utilities] > [Publish] > [Publish History] により、[Publish History] ページに進むことができます。

backupconfig コマンド

アクティブなデータセットを「ソース」アプライアンスから「ターゲット」セキュリティ管理アプライアンスに、元の「ソース」セキュリティ管理アプライアンスの中断を最小限に抑えてコピーするには、backupconfig コマンドを使用します。

このコマンドとその使用法、およびデータセットのバックアップの詳細については、「セキュリティ管理アプライアンスのバックアップ」（P.13-6）を参照してください。

CLI を使用した設定変更のアップロード

ステップ 1　CLI の外部で、アプライアンスの configuration ディレクトリにアクセスできることを確認します。詳細については、付録 A「IP インターフェイスおよびアプライアンスへのアクセス」を参照してください。

ステップ 2　コンフィギュレーション ファイル全体またはコンフィギュレーション ファイルのサブセクションをアプライアンスの configuration ディレクトリに格納するか、saveconfig コマンドで作成した既存の設定を編集します。

ステップ 3　CLI 内で、loadconfig コマンドを使用して、ステップ 2 で示されたディレクトリに格納したコンフィギュレーション ファイルをロードするか、テキスト（XML 構文）を CLI に直接貼り付けます。

この例では、changed.config.xml という名前のファイルがアップロードされ、変更が保存されます。

```
mail3.example.com> loadconfig

1. Paste via CLI
2. Load from file
[1]> 2

Enter the name of the file to import:
[]> changed.config.xml

Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> commit
```

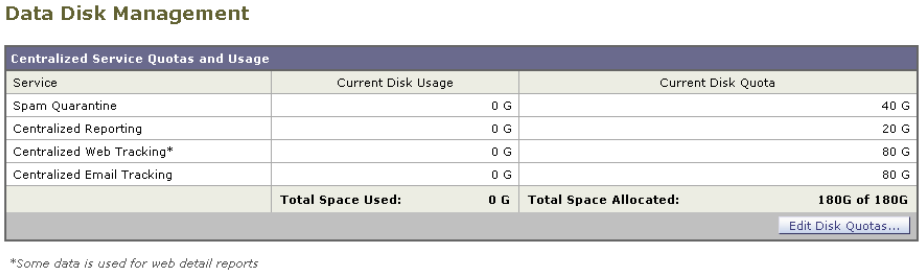
この例では、新しいコンフィギュレーション ファイルをコマンド ラインに直接貼り付けます（空白行で Ctrl を押した状態で D を押すと貼り付けコマンドが終了します）。次に、システム セットアップ ウィザードを使用して、デフォルトのホスト名、IP アドレス、およびゲートウェイ情報を変更します。（詳細は、「システム セットアップ ウィザードの実行」（P.2-10）を参照してください）。これで、変更が確定されます。

```
mail3.example.com> loadconfig

1. Paste via CLI
2. Load from file
[1]> 1

Paste the configuration file now. Press CTRL-D on a blank line when done.

[The configuration file is pasted until the end tag </config>. Control-D is entered on a
separate line.]

Values have been loaded.
Be sure to run "commit" to make these settings active.

mail3.example.com> commit

Please enter some comments describing your changes:
[]> pasted new configuration file and changed default settings
```

ディスク使用量の管理

[Management Appliance] > [System Administration] > [Disk Management] ページを使用して、セキュリティ管理アプライアンスでのモニタリング サービス（Cisco IronPort スパム隔離、中央集中型レポーティング、中央集中型 Web トラッキング、および中央集中型電子メール トラッキング）に割り当てられたディスク領域量を表示または変更します。これらの 4 つのサービスに割り当てられるディスクの合計容量は、次の例に示されているように、アプライアンスのモニタリング サービスに割り当てられるディスク領域の合計容量になります。

図 13-23　[Disk Management] ページ



複数のサービスがイネーブルの場合のディスク領域に関する重要な情報

セキュリティ管理アプライアンスの中央集中型レポーティング ディスク領域は、電子メールと Web の両方のデータに使用されます。中央集中型電子メール レポーティングだけをイネーブルにすると、領域はすべて電子メール レポーティング専用になります。反対に、中央集中型 Web レポーティングをオンにすると、領域はすべて Web レポーティング データに使用されます。両方をオンにした場合、電子メールおよび Web レポーティング データは領域を共有し、領域はファースト カム ベースで割り当てられます。

使用可能な最大ディスク領域

表 13-5 は、セキュリティ管理アプライアンスでの中央集中型レポーティング、中央集中型電子メール トラッキング、中央集中型 Web トラッキング、および Cisco IronPort スパム隔離（ISQ）に使用可能なディスク領域の最大量を示しています。サイズはすべてギガバイト（GB）単位で表示されています。

表 13-5　使用可能な最大ディスク領域

使用可能なディスク領域	ハードウェア プラットフォーム									
	M160	M170	M600	M650	M660	M670	M1000	M1050	M1060	M1070
ISQ + レポーティング + 電子メール トラッキング + Web トラッキング	180	180	186	186	450	700	405	405	800	1500
ISQ 最大	70	70	100	100	150	150	200	200	265	265

（注）　レポーティング（単なるカウンター）や、トラッキング（限定的な量のヘッダー情報だけを保存）とは異なり、ISQ は実際にハード ディスク上の隔離を受けたメッセージのすべてのメッセージ本文を保存するため、他の機能よりも、メッセージごとの使用ディスク領域が非常に多くなります。このように大量のディスク領域が使用されるため、すべてのハード ドライブを ISQ に割り当てると、アプライアンスがロックされる場合があります。このため、ISQ のディスク クォータには、単なる使用可能なディスク領域よりも厳しい制限があります。

ディスク領域量の再割り当てについて

[Edit Disk Quotas] をクリックして、各サービスに割り当てられているディスク領域の量を変更できます。たとえば、中央集中型トラッキングで、中央集中型レポーティングや Cisco IronPort スパム隔離よりも多くのハード ドライブ スペースが継続的に必要な場合は、中央集中型トラッキング サービスに割り当てらた領域を調整できます。Web レポーティングおよびトラッキングに設定するクォータが、現在使用しているディスク領域よりも大きい場合、Web レポーティングおよびトラッキングのデータは失われません。

既存の割り当て量を少なくした場合、新しい割り当て量内にすべてのデータが収まるようになるまで、最も古いデータから削除されます。割り当て量をゼロに設定すると、データは保持されなくなります。

中央集中型 Web レポーティングをイネーブルにしているが、レポーティングにディスク領域が割り当てられていない場合、ディスク領域が割り当てられるまで、中央集中型 Web レポーティングが機能しません。

ディスク領域量の再割り当て

各モニタリング サービスに割り当てられたディスク領域量を変更するには、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] > [System Administration] > [Disk Management] を選択します。

ステップ 2　[Edit Disk Quotas] をクリックします。

ステップ 3　[Edit Disk Quotas] ページで、各サービスに割り当てるディスク領域の量（ギガバイト単位）を入力します。

ISQ 以外のすべてのサービスに対して、0 からディスクの合計量までの値を入力できます。4 つすべてのサービスの合計ディスク クォータが、表示されている合計ギガバイト数になる必要があります。たとえば、使用可能な合計ディスク領域が 200 GB の場合に、中央集中型レポーティングに 25 GB、Cisco IronPort スパム隔離に 10 GB、中央集中型電子メール トラッキングに 35 GB を割り当てた場合、使用可能なディスク合計量の 200 GB を保つには、中央集中型 Web トラッキングに割り当てられるのは最大 130 GB になります。

ステップ 4　[Submit] をクリックします。

ステップ 5　確認ダイアログボックスで、[Set New Quotas] をクリックします。

ステップ 6　[Commit] をクリックして変更を保存します。

プリファレンスの 設定

セキュリティ管理アプライアンス 上で設定されている管理ユーザ

ローカル認証されたユーザは次のプリファレンスを選択できます。このプリファレンスは、ユーザがセキュリティ管理アプライアンスにログインするたびに適用されます。

- 言語（GUI および PDF レポートに適用）
- ランディング ページ（ログイン後に表示されるページ）
- レポート ページのデフォルトの時間範囲（使用可能なオプションは、電子メールおよび Web レポーティング ページのサブセットです）

- レポート ページの表に表示する行数

実際のオプションは、ユーザ ロールによって異なります。

これらのプリファレンスを設定するには、[Options] > [Preferences] を設定します。([Options] メニューは GUI ウィンドウの上部右側にあります)。完了したら変更を送信し、確定します。

ヒント　[Preferences] ページにアクセスする前に表示していたページに戻るには、ページ下部の [Return to previous page] リンクをクリックします。

外部認証されたユーザ

外部認証されたユーザは、[Options] メニューで表示言語を直接選択できます。