CHAPTER 12

一般的な管理タスク

大部分のシステム管理タスクは、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行えます。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-4）を参照してください。

この章は、次の項で構成されています。

- 「CLI コマンドを使用したメンテナンス タスクの実行」（P.12-2）
- 「Security Management アプライアンスのバックアップ」（P.12-8）
- 「新しい Security Management アプライアンス ハードウェアのアップグレード」（P.12-16）
- 「AsyncOS のアップグレード」（P.12-18）
- 「アップグレードおよびサービス アップデートの設定」（P.12-34）
- 「Security Management アプライアンスでのディザスタ リカバリ」（P.12-39）
- 「管理タスクの分散について」（P.12-43）
- 「Security Management アプライアンスへのアクセス権の設定」（P.12-76）
- 「アクティブなセッションの表示」（P.12-81）

- 「生成されたメッセージの返信アドレスの設定」（P.12-81）
- 「アラートの管理」（P.12-82）
- 「ネットワーク設定値の変更」（P.12-95）
- 「システム時刻の設定」（P.12-105）
- 「コンフィギュレーション ファイルの管理」（P.12-110）
- 「ディスク使用量の管理」（P.12-123）

CLI コマンドを使用したメンテナンス タスクの実行

ここで説明されている操作およびコマンドを使用して、Security Management アプライアンスでメンテナンス関連のタスクを実行できます。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**

Security Management アプライアンスのシャットダウン

Security Management 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。

Security Management アプライアンスのリブート

Security Management 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。

Security Management 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、Security Management アプライアンスをオフライン状態にします。`suspend` および `offline` コマンドを使用して、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。

アプライアンスをオフライン状態に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。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アプライアンスをリブートする場合、システムをオンライン状態に戻すには **resume** コマンドを使用する必要があります。

関連項目：

- 『*Cisco IronPort AsyncOS for Email 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>
```

出荷時デフォルト値へのリセット

アプライアンスを物理的に移動するときに、出荷時の初期状態に戻すことができます。[Management Appliance] > [System Administration] > [Configuration File] ページの [Reset Configuration] セクションか、**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お勧めします。

（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　Security Management 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。

Security Management 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

Security Management 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」Security Management アプライアンスにコピーし、元の「ソース」Security Management 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。Security Management 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 Security Management 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 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 スパム検疫、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。

バックアップ機能では **backupconfig** コマンドを使用して、Security Management 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。

バックアップの制約事項

バックアップをスケジュール設定する前に、次の制約事項を考慮してください。

制約事項	要件
アプライアンスの容量	ターゲット アプライアンスには、ソース アプライアンスの容量以上の容量が必要です。
アプライアンスのバージョン	セキュリティ管理データ用の AsyncOS 7.7 は、セキュリティ管理用の AsyncOS 7.7 を実行している別の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 Security Management アプライアンスをアップグレードしてください。
アプライアンス間の通信	ソースとターゲットの Security Management アプライアンスは、SSH を使用して通信できる必要があります。このため次のようになります。 • 両方のアプライアンスでポート 22 が開いている。デフォルトで、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。 • A レコードと PTR レコードの両方を使用して、ドメイン ネーム サーバ（DNS）が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る。

制約事項	要件
複数、同時、および チェーン バックアップ	Security Management アプライアンスからのデータは、1 つの Security Management アプライアンスだけ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。 ある Security Management アプライアンスでバックアップがスケジュール設定されている場合、その Security Management アプライアンスに別のバックアップをスケジュール設定することはできません。別の Security Management アプライアンスにバックアップをスケジュール設定するには、まず、現在実行中のバックアップまたは将来のバックアップをすべてキャンセルします。

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。日次バックアップには、それぞれ 3 時間かかることがあります。週次および月次のバックアップには、さらに時間がかかる可能性があります。この時間は一定ではありません。

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。

バックアップ中のサービスのアベイラビリティ

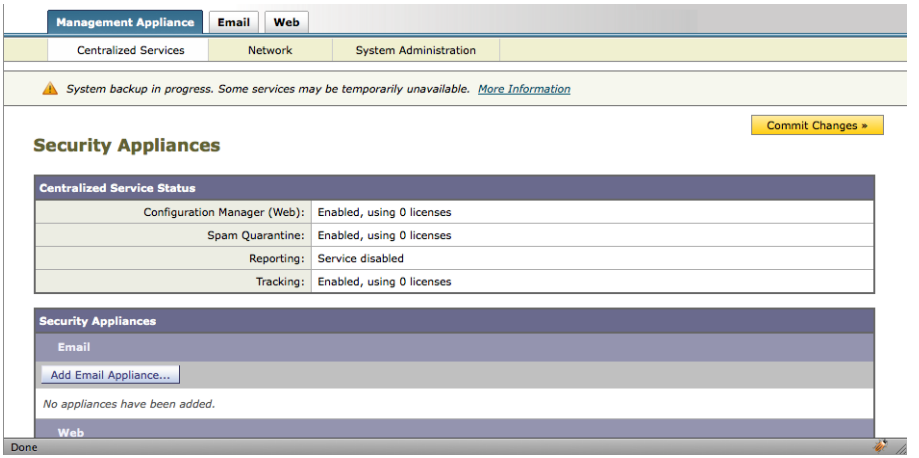
バックアップ プロセスのフェーズと、それらがサービスのアベイラビリティに及ぼす影響は次のとおりです。

- 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。初期シャットダウン後、ソースとターゲットのアプライアンス間でデータを転送しているときに収集されたすべての差が、ターゲット アプライアンスにコピーされ、ソースとターゲットの両方でサービスが開始されます。これにより、ソース アプライアンスで最大限の稼動時間が維持され、どちらのアプライアンスでもデータは失われなくなります。

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、Security Management 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。バックアップがキャンセルされても、バックアップ プロセスによって、ターゲット マシンにバックアップ済みのデータが消去されることはありません。

バックアップのスケジュール作成

（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。

Security Management アプライアンスでは、次の 2 つのタイプのバックアップをスケジュール設定できます。

- 定期バックアップ：定期バックアップには、事前設定した時間内に繰り返し行うバックアップと、事前設定した時間に 1 回行うバックアップがあります。
- 即時バックアップ：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。

定期バックアップ

（注） ログ ファイルは、定期的に保存することもできます。このプロセスの詳細については、「ログ サブスクリプション」（P.13-37）を参照してください。

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　コマンド プロンプトで **Schedule** と入力し、Enter を押します。

ステップ 4　ターゲット Security Management 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、Security Management 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 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、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]：即時バックアップを開始できます。

ステップ 5　**1** を入力して、Enter を押します。

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

ステップ 6　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 7　バックアップを開始する特定の日時を入力し、Enter を押します。

ステップ 8　バックアップ プロセスの名前を入力します。

後でこのバックアップ プロセスを確認できるよう、わかりやすい任意の名前にしてください。

これがバックアップのフェーズ 1 です。

コマンドライン プロンプトに **Status** と入力すると、次のように表示されます。

```
Phase: One
Centralized Email Tracking: Completed
Centralized Spam Quarantine: Completed
Centralized Email Reporting: Completed
Centralized Web Reporting: In Progress
```

この出力は、データを新しいターゲット マシンに転送中であることを示しています。

フェーズ 2 の最後で、データの転送は完了します。コマンドライン プロンプトに **Status** と入力すると、次のように表示されます。

```
Phase: Two
Centralized Email Tracking: Completed
Centralized Spam Quarantine: Completed
Centralized Email Reporting: Completed
Centralized Web Reporting: Completed
```

ステップ 9　データの転送が完了したら、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** と入力して、Enter を押します。

ステップ 10　完全なバックアップの詳細については、「その他の重要なバックアップ タスク」（P.12-15）を参照してください。

即時バックアップ

インスタント バックアップを開始するには、次の手順を実行します。

（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 Security Management 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、Security Management 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 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　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するには、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 7　完全なバックアップの詳細については、「その他の重要なバックアップ タスク」（P.12-15）を参照してください。

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、次のことを検討してください。

- 設定内容を保存する方法については、「コンフィギュレーション ファイルの管理」（P.12-110）を参照してください。
- Security Management 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、第 13 章「ロギング」を参照してください。

新しい Security Management アプライアンス ハードウェアのアップグレード

古い Security Management 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 Security Management 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 12-1　新しい Security Management 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 Security Management 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、Security Management 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 Security Management 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 Security Management 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、Security Management アプライアンスでのソフトウェア アップグレードに関連する次の内容について説明します。

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します。

- 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.12-123）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。

（注）　アップグレード後、再びリスナーをイネーブルにします。

AsyncOS をアップグレードする前に、アップグレードおよびアップデート設定が正しく設定されていることを確認します。詳細については、「アップグレードおよびサービス アップデートの設定」（P.12-34）を参照してください。

リモート アップグレードと ストリーミング アップグレード

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」）である、リモート アップグレードとストリーミング アップグレードを使用できます。

リモート アップグレードでは、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。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。

ストリーミング アップグレードでは、Cisco IronPort アプライアンスは HTTP を介して Cisco IronPort アップデート サーバから直接 AsyncOS アップグレードをダウンロードします。各 Cisco IronPort アプライアンスは、アップグレードを別個にダウンロードします。

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。

2 つのアップグレード方式を切り替えるには、[Management Appliance] > [System Administration] > [Update Settings] ページを使用します（ストリーミング アップグレードがデフォルトです）。CLI で **updateconfig** コマンドを使用する方法もあります。

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。

（注）　どちらのアップグレード方式を使用しても、アップグレードの完了後は、**saveconfig** コマンドを使用して設定を保存するかどうか判断する必要があります。詳細については、「コンフィギュレーション ファイルの管理」（P.12-110）を参照してください。

クラスタ化されたシステムのアップグレード

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。

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、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。

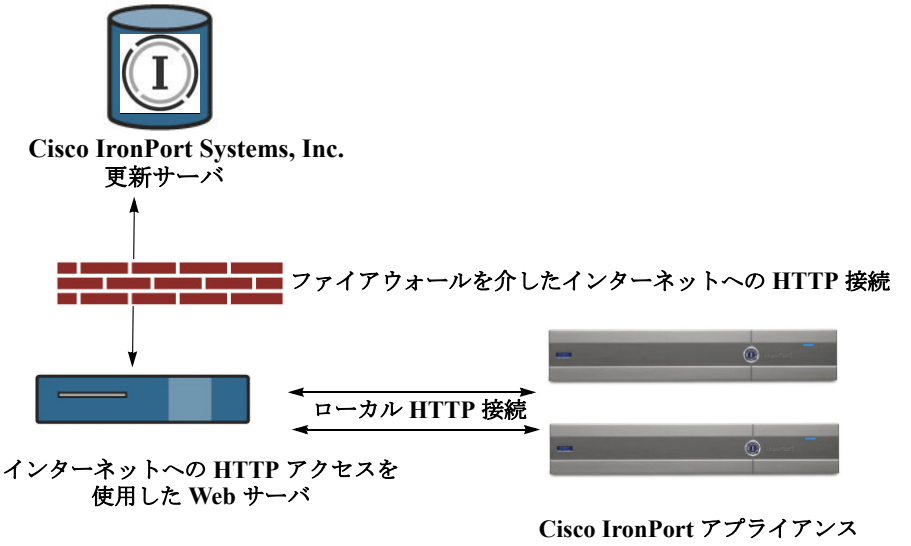
図 12-2　　ストリーミング アップデート方式

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 12-3　　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　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 2　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 3　[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 4　[Management Appliance] > [System Administration] > [System Upgrade] を選択します。

ステップ 5　[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。

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）。

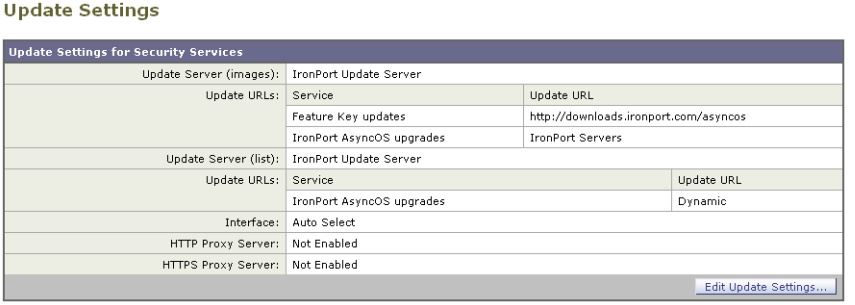
ネットワーク上の Cisco IronPort アプライアンスに使用可能なアップグレードを、`http://updates.ironport.com/fetch_manifest.html` で選択したバージョンに限定する XML ファイルを、ローカル サーバでホスティングすることもできます。この場合でも、Cisco IronPort アプライアンスは Cisco IronPort Systems アップデート サーバからアップグレードをダウンロードします。アップグレード リストをローカル サーバにホスティングする場合は、zip ファイルをダウンロードして、`asyncos/phoebe-my-upgrade.xml` 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。

GUI を使用したアップグレードの取得

（ストリーミングまたはローカル ソースで）アップグレードを取得する場所を指定するには、Security Management アプライアンスで、[Management Appliance] > [System Administration] > [Update Settings] を選択します。

図 12-4　[Update Settings] ページ



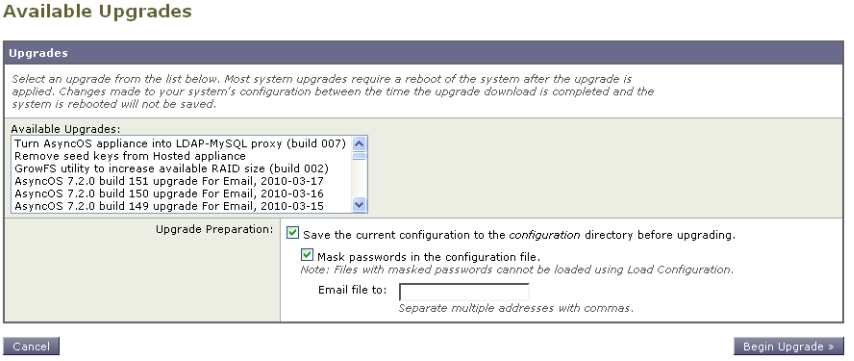
GUI からの AsyncOS のアップグレード

アップデートを設定後に 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　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [System Upgrade] > [Available Upgrades] を選択します。

[Available Upgrades] ページが表示されます。

図 12-5　[Available Upgrades] ページ



ステップ 2　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。

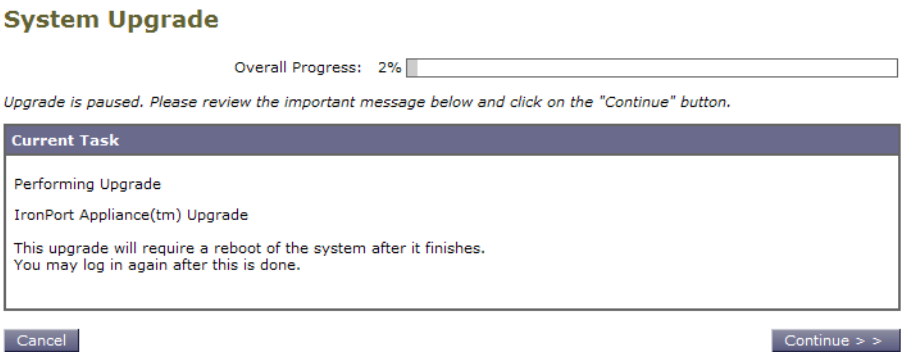
ステップ 3　アップグレード前に設定ディレクトリに現在の設定を保存する場合は、[Upgrade Preparation] セクションでチェックボックスをオンにします。この設定が推奨されます。

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。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。

ステップ 4　[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。

ステップ 5　プロンプトが表示されたら、変更点を確認するか、新しいライセンス契約を読んで、同意します。

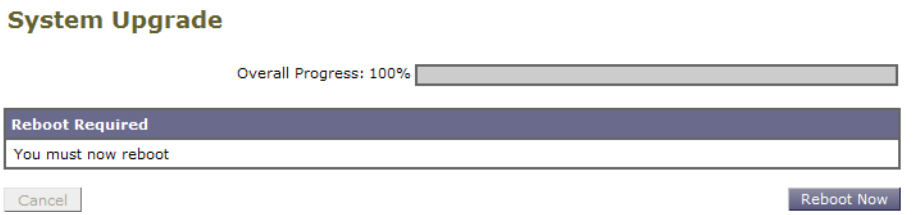
図 12-6　アップグレードの経過表示



ステップ 6　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 7　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。

図 12-7　アップグレードの完了



ステップ 8　[Reboot Now] をクリックします。

ステップ 9　アプライアンスが再度起動したら、サインインします。

ステップ 10　AsyncOS 7.2 よりも前のリリースからアップグレードする場合は、[Web] タブを最初にクリックしたときに、最新の Configuration Master を開始するようにプロンプトが出されます。詳細については、「Configuration Master の初期化」（P.8-8）を参照してください。

以前のバージョンの AsyncOS 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。

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　Email Security 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　Email Security 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動します。

（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。

CLI を使用したアップグレードの取得

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。

（注）　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。

updateconfig コマンド

updateconfig コマンドを使用すると、Cisco IronPort アプライアンスに AsyncOS アップグレードなどのサービス アップデートを探す場所を指示できます。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。リモート アップグレードの場合、updateconfig コマンドを発行して、アプライアンスがローカル アップデート サーバ（上記で設定したローカル サーバ）を使用するように設定します。

```
mail3.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
```

（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。

upgrade コマンド

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。

```
mail3.example.com> upgrade

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

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

Email a copy? [N]> y

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

Upgrades available.
1. AsyncOS 7.7.0 For Security Management upgrade

[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
IronPort Security Management Appliance(tm) Upgrade
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]>

System rebooting.  Please wait while the queue is being closed.
```

アップグレード方式の違い（リモートとストリーミング）

従来の方式（ストリーミング アップグレード）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

時間帯ルールや AsyncOS アップグレードなど、Security Management アプライアンスがセキュリティ サービス アップデート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 の [Management Appliance] > [System Administration] > [Update Settings] ページか、CLI で `updateconfig` コマンドを使用して設定できます。

[Update Settings] ページまたは `updateconfig` CLI コマンドを使用して Cisco IronPort AsyncOS をアップグレードすることもできます。詳細については、「AsyncOS のアップグレード」（P.12-18）を参照してください。

（注） 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。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。アップデートに関して、ファイアウォール設定にスタティック IP アドレスが必要だと判断した場合、次の指示に従ってアップデート設定値を編集し、Cisco IronPort カスタマー サポートに必要な URL アドレスを問い合わせて取得します。

アップデート設定の編集

Cisco IronPort アプライアンスのアップデート設定を編集するには、[Edit Update Settings] ボタンをクリックして、[Edit Update Settings] ページを表示します。

表 12-1 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 12-1　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。 次の条件のいずれかが該当する場合は、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できますが、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ります。 • 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、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。

表 12-1　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セキュリティ 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。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、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、「リモート アップグレードと ストリーミング アップグレード」（P.12-19）および「リモート アップグレードの概要」（P.12-21）を参照してください。
Automatic Updates	時間帯ルールなど、リストされているセキュリティ アップデートに対する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	リストされたセキュリティ コンポーネントのアップデート、および Cisco IronPort AsyncOS のアップグレードをアップデート 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。

表 12-1　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
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。

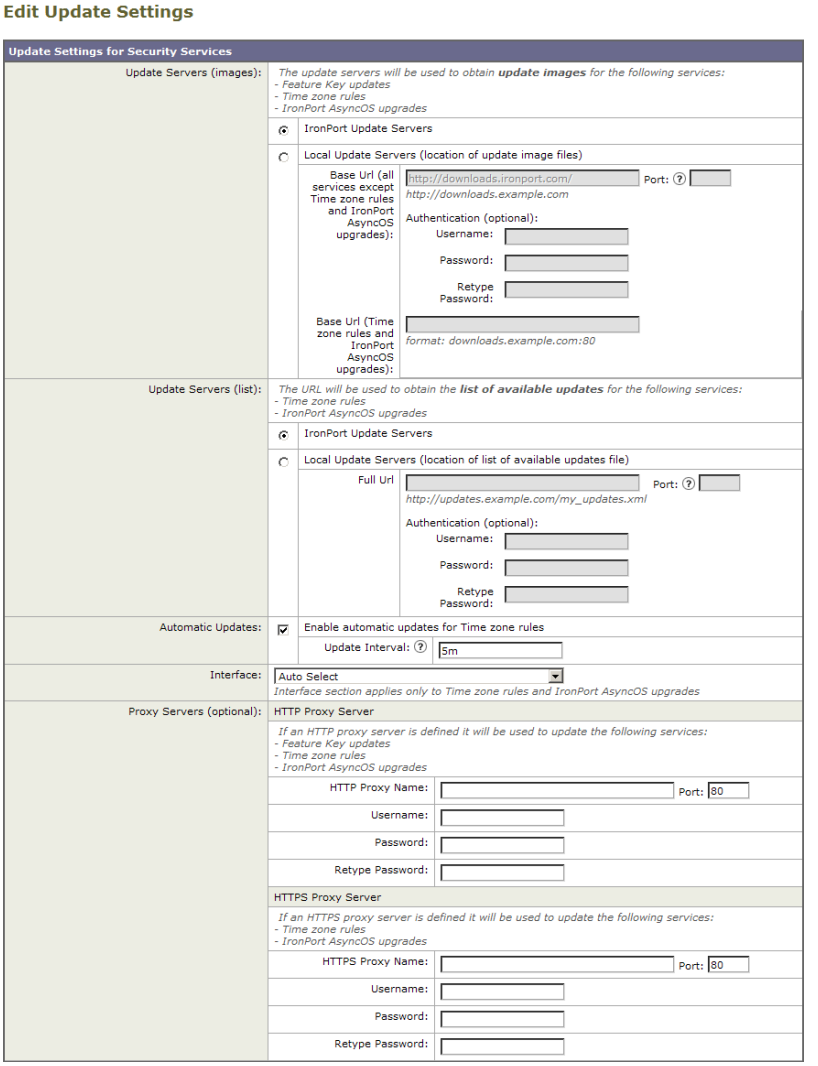
GUI からのアップデートおよびアップグレード設定値の設定

AsyncOS 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。[Edit Update Settings] ページが表示されます。

図 12-8 に、[Edit Update Settings] ページで設定できるオプションを示します。

図 12-8　[Edit Update Settings] ページ



ステップ 2　表 12-1（P.12-35）にある設定値を設定します。

ステップ 3　変更を送信し、保存します。

Security Management アプライアンスでのディザスタ リカバリ

ディザスタ リカバリによって、Security Management アプライアンスに突然障害が生じた場合に備えることができます。このような時点で障害管理やディザスタ リカバリを行うことは、データの保全に不可欠です。その場合は、システムでデータ整合性が保たれるように、データの実装および回復方法を把握しておくことが重要です。

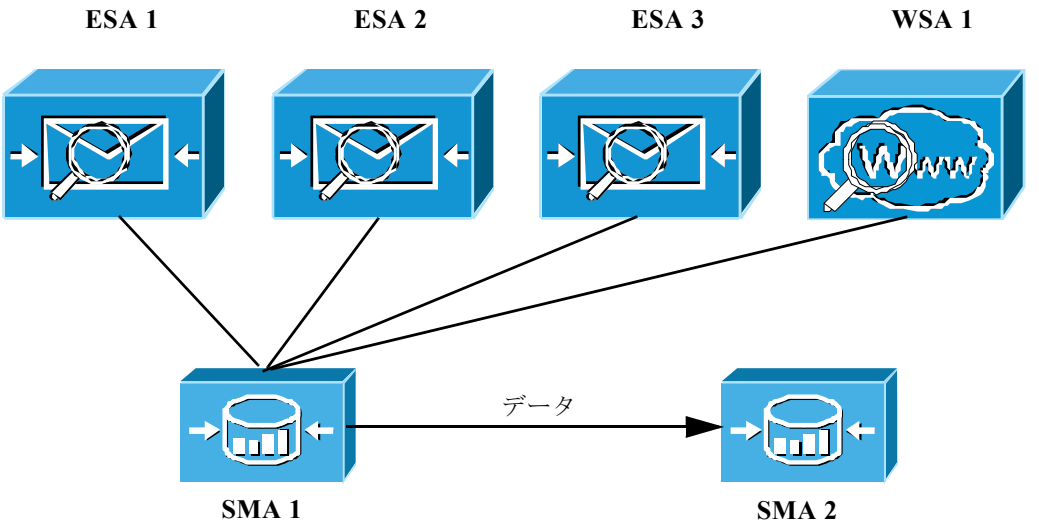
（注）　異なるサイズの Security Management アプライアンス間でデータを転送することはできますが、データの転送先となるアプライアンスには同等以上のサイズが割り当てられている必要があります。

これは推奨事項であり、Security Management アプライアンスのサイズの大きいものから小さいものへのディザスタ リカバリおよびバックアップを禁止する厳密なルールはありません。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 Security Management アプライアンスにあれば、ソースからターゲットへのバックアップをスケジュール設定できます。つまり、ターゲット アプライアンスのすべてのデータに割り当てられているディスク容量が、ソース アプライアンスのものよりも大きい必要があります。

たとえば、ソース アプライアンスが M1060 でターゲット アプライアンスが M650 であり、ソースよりもターゲットのほうが小さい場合、大きいほうの M1060 ですべてのデータに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 のアプライアンスにあるスペースと数字が一致するようにしてください。これは、GUI の [Disk Management] ページから行えます。また、小さいほうの M650 に格納できるサイズよりも多くのデータを、大きいほうの M1060 に置かないでください。

最初に、一般的な環境と設定を確認しておきます。一般的な環境では、アプライアンス設定は次の図 12-9 の設定のようになります。

図 12-9　ディザスタ リカバリ：一般的な環境



この環境では、SMA 1 がプライマリ Security Management アプライアンスであり、電子メール レポーティング、トラッキング、ISQ、および Web レポーティングの各データを ESA 1-3 および WSA 1 から受け取ります。SMA 2 がデータを受け取ると、SMA 1 でバックアップが実行され、フェールオーバー用に SMA 1 にあるすべてのデータがコピーされて SMA 2 に保存されます。Security Management アプライアンスのバックアップの詳細については、「Security Management アプライアンスのバックアップ」（P.12-8）を参照してください。

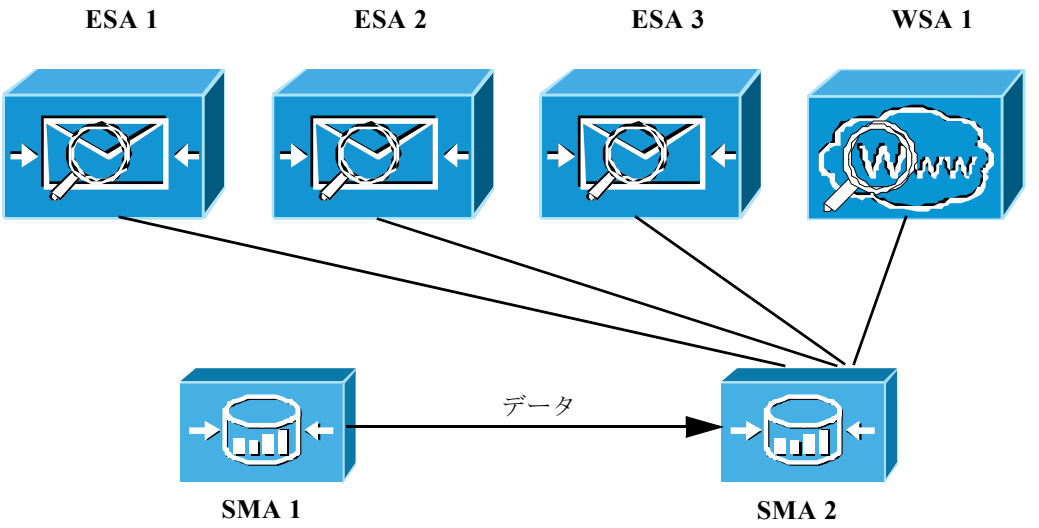
ここで、SMA 1 に障害が発生し始めていることが検出されたとします。レポートの受信速度が遅くなったり、データが壊れていたり、Security Management アプライアンスで障害が発生し始めていることを示す兆候が出ているなどです。次の手順に従って、ディザスタ リカバリを開始します。

ステップ 1　SMA1 から SMA 2 にインスタント バックアップを開始します。

この実行方法については、「即時バックアップ」（P.12-14）の手順を参照してください。

バックアップの実行後、環境設定は図 12-10 のようになります。

図 12-10　ディザスタ リカバリ：パート 1：インスタント バックアップ



すべてのデータが SMA 1 から SMA 2 へすぐに転送されます。また、ESA 1-3 と WSA 1 からもすべてのデータが SMA 2 に転送されます。これで、SMA 2 がプライマリ アプライアンスになりました。この時点で、手動で SMA 2 を設定する必要があります。

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。

- SMA 2 で、[Network] > [IP Interfaces] > [Add IP Interfaces] を選択します。
- [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　すべてのアプライアンスを新しい Security Management アプライアンス（SMA 2）に追加します。

アプライアンスの追加方法については、「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。

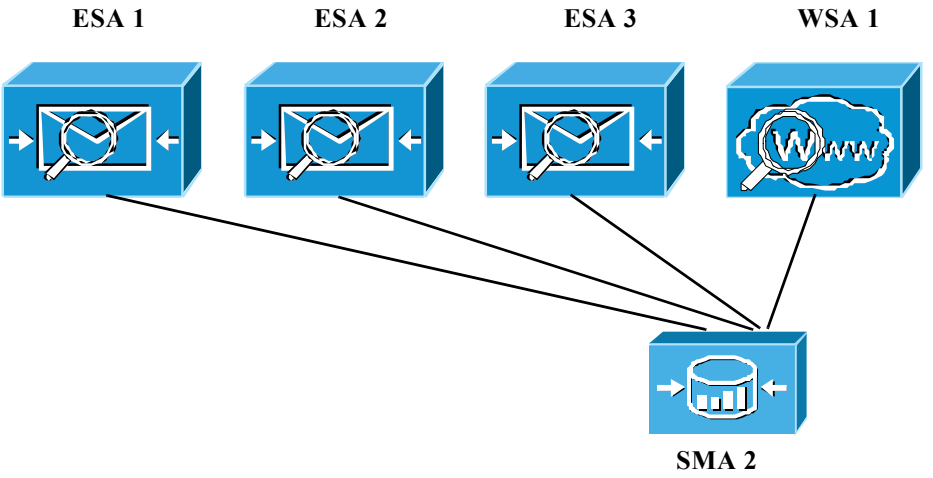
ステップ 5　新しい Security Management アプライアンス（SMA 2）ですべてのサービスをイネーブルにします。

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。サービスのイネーブル化の詳細については、「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 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、図 12-11 に示すように、すべてのデータが SMA2 に送られるようになりました。

図 12-11　ディザスタ リカバリ：パート 2：新しい Security Management アプライアンス



（注）　**saveconfig** コマンドを使用して定期的に設定を保存していた場合、**loadconfig** コマンドを使用して、保存したこのコンフィギュレーション ファイルを新しい Security Management アプライアンス（この例では SMA 2）にロードし、ステップ 2 で説明されているように、新しい ID アドレスを設定できます。コンフィギュレーション ファイルには、SMA 2 が機能するために必要なすべての情

報が含まれているわけではありません。新しい Security Management アプライアンスに、すべてのアプライアンスを追加する必要があります。ここで、各アプライアンスへの接続を確立し、接続をテストする必要があります。

管理タスクの分散について

ユーザ アカウントに割り当てたユーザ ロールに基づいて、他のユーザに管理タスクを分散できます。

Security Management アプライアンスには、電子メールと Web セキュリティ アプライアンスのモニタリングおよび管理を行うための、事前定義ユーザ ロールとカスタム ユーザ ロールの両方が用意されています。

事前定義ロールの詳細については、「ユーザ ロール」（P.12-43）を参照してください。

カスタム ユーザ ロールの詳細については、「カスタム ユーザ ロールへの管理委任」（P.12-49）を参照してください。

ユーザ アカウントの詳細については、「GUI でのユーザ管理」（P.12-59）を参照してください。

ユーザ ロール

特記のない限り、次の表で説明されている権限を持つ事前設定ユーザ ロール、またはカスタム ユーザ ロールを各ユーザに割り当てることができます。

表 12-2　ユーザ ロールの説明

ユーザ ロール名	説明	Web レポーティング / スケジュール設定されたレポート機能	アプライアンス
admin	**admin** ユーザはシステムのデフォルト ユーザ アカウントであり、すべての管理権限を持っています。便宜上、admin ユーザ アカウントをここに記載しましたが、これはユーザ ロールを使用して割り当てることはできず、パスワードの変更以外、編集や削除もできません。 **resetconfig** コマンド、および **revert**（**ESA のみ**）コマンドを発行できるのは **admin** ユーザだけです。	あり / あり	Security Management アプライアンス
Administrator	Administrator ロールを持つユーザ アカウントはシステムのすべての設定に対する完全なアクセス権を持っています。 Email Security アプライアンスでは、以前は **admin** ユーザだけが使用できた機能を、Administrator ロールが割り当てられたユーザがすべて使用できるようになりました。	あり / あり	Security Management アプライアンス、Web セキュリティ アプライアンス Email Security アプライアンス

表 12-2　ユーザ ロールの説明（続き）

ユーザ ロール名	説明	Web レポーティング / スケジュール設定されたレポート機能	アプライアンス
Operator	Operator ロールを持つユーザ アカウントは次のことができません。 • ユーザ アカウントの作成または編集 • `resetconfig` コマンドの発行 • `upgradecheck` コマンドによる、使用可能なアップグレードの確認 • **upgradeinstall** コマンドによる、アップグレードのインストール • システム セットアップ ウィザードの実行 • LDAP が外部認証用にイネーブルになっている場合の、ユーザ名とパスワードを除く LDAP サーバ プロファイル設定の変更 これら以外は、Administrator ロールと同じ権限を持ちます。	あり / あり	Security Management アプライアンス、Web セキュリティ アプライアンス、Email Security アプライアンス
Technician	Technician ロールを持つユーザ アカウントは、管理機能キーのアップグレードやリブートなどのシステム管理アクティビティを開始できます。このロールには、ポリシー、HAT、または RAT など、電子メール特有の機能へのアクセス権はありません。	なし / なし	Security Management アプライアンス、Web セキュリティ アプライアンス Email Security アプライアンス

表 12-2　ユーザ ロールの説明（続き）

ユーザ ロール名	説明	Web レポーティング / スケジュール設定されたレポート機能	アプライアンス
Read-Only Operator	Read-Only Operator ロールを持つユーザは、設定情報を参照するアクセス権を持っています。Read-Only Operator ロールを持つユーザは、機能の設定方法を確認するために変更を行って送信できますが、保存できません。また、このロールを持つユーザは Cisco IronPort スパム検疫でメッセージを管理できます（アクセスがイネーブルな場合）。このロールを持つユーザは、ファイル システム、FTP、または SCP にアクセスできません。	あり / なし	Security Management アプライアンス、Web セキュリティ アプライアンス Email Security アプライアンス
Guest	Guest ロールを持つユーザ アカウントはステータス情報だけを参照できます。また、Guest ロールを持つユーザは Cisco IronPort スパム検疫でメッセージを管理することもできます（アクセスがイネーブルな場合）。Guest ロールを持つユーザはメッセージ トラッキングにアクセスできません。	あり / なし	Security Management アプライアンス、Web セキュリティ アプライアンス、Email Security アプライアンス
Web Administrator	Web Administrator ロールを持つユーザ アカウントは、[User Role] メニューでのみ、すべての設定へのアクセス権を持っています。	あり / なし	Security Management アプライアンス

表 12-2　ユーザ ロールの説明（続き）

ユーザ ロール名	説明	Web レポーティング / スケジュール設定されたレポート機能	アプライアンス
Web Policy Administrator	Web Policy Administrator ロールを持つユーザ アカウントは、[Web Appliance Status] ページと、Configuration Master のすべてのページにアクセスできます。Web ポリシー管理者は、ID、アクセス ポリシー、暗号化ポリシー、ルーティング ポリシー、プロキシ バイパス、カスタム URL カテゴリ、および時間範囲を設定できます。Web ポリシー管理者は、設定を公開できません。	なし / なし	Security Management アプライアンス
URL Filtering Administrator	URL Filtering Administrator ロールを持つユーザ アカウントは、URL フィルタリングだけを設定できます。	なし / なし	Security Management アプライアンス
Email Administrator	Email Administrator ロールを持つユーザ アカウントは、Cisco IronPort スパム検疫およびシステム検疫権など、[Email] メニューでのみ、すべての設定へのアクセス権を持ちます。	なし / なし	Security Management アプライアンス
Help Desk User	Help Desk User ロールを持つユーザがアクセスできるのは次のものに制限されます。 • メッセージ トラッキング • Cisco IronPort スパム検疫の管理 このロールを持つユーザは、CLI を含めたこれ以外のシステムにはアクセスできません。このロールを持つユーザが Cisco IronPort スパム検疫の管理を行うには、そのスパム検疫へのアクセス権をイネーブルにする必要があります。	なし / なし	Security Management アプライアンス、Email Security アプライアンス

表 12-2　ユーザ ロールの説明（続き）

ユーザ ロール名	説明	Web レポーティング / スケジュール設定されたレポート機能	アプライアンス
カスタム ロール	カスタム ユーザ ロールに割り当てられているユーザ アカウントは、ポリシー、機能、またはこのロールに特に与えられた特定のポリシーまたは機能インスタンスに対してのみ、表示および設定を行えます。 新しい Custom Email User ロールまたは新しい Custom Web User ロールは、[Add Local User] ページから作成できます。ただし、ロールを使用できるようにするには、このカスタム ユーザ ロールに権限を割り当てる必要があります。権限を割り当てるには、[Management Appliance] > [System Administration] > [User Roles] に移動して、ユーザ名をクリックします。 **（注）** Custom Email User ロールに割り当てられているユーザは、CLI にアクセスできません。 詳細については、「カスタム ユーザ ロールへの管理委任」（P.12-49）を参照してください。	なし / なし	Security Management アプライアンス、Email Security アプライアンス

一部のロール（Administrator、Operator、Guest、Technician、および Read-Only Operator）は、GUI と CLI の両方にアクセスできます。他のロール（Help Desk User、Email Administrator、Web Administrator、Web Policy Administrator、URL Filtering Administrator、およびカスタム ユーザ）は GUI だけにアクセスできます。

ユーザを認証するために LDAP ディレクトリを使用する場合は、ユーザ ロールに個々のユーザではなくディレクトリ グループを割り当てます。ユーザ ロールにディレクトリ グループを割り当てると、そのグループの各ユーザはそのユーザ ロールで定義された権限を受け取ります。詳細については、「外部認証」（P.12-71）を参照してください。

ユーザがスパム検疫にアクセスできるようにするには、そのアクセス権をイネーブルにする必要があります。「Cisco IronPort スパム検疫の管理ユーザの設定」（P.7-6）を参照してください。

カスタム ユーザ ロールへの管理委任

Administration 権限を持つユーザは、Security Management アプライアンスを使用してカスタム ロールに管理権限を委任できます。カスタム ロールは、事前定義されたユーザ ロールよりも、ユーザのアクセス権に対して柔軟な制御を行えます。

カスタム ユーザ ロールを割り当てたユーザは、アプライアンス、機能、またはエンド ユーザのサブセットに関して、ポリシーの管理またはレポートへのアクセスを行えます。たとえば、別の国にある組織の支社では、許容可能な使用ポリシーが組織の本社とは異なっている場合に、Web サービスに関して委任を受けた管理者に、支社のポリシーの管理を許可できます。カスタム ユーザ ロールを作成して、それらのロールにアクセス権を割り当てることで、管理を委任します。委任された管理者が表示および編集できるポリシー、機能、レポート、カスタム URL カテゴリなどを決定します。

詳細については、次を参照してください。

- 「Custom Email User ロールについて」（P.12-49）
- 「Custom Web User ロールについて」（P.12-55）

Custom Email User ロールについて

カスタム ロールを割り当てると、委任された管理者が Security Management アプライアンスにある次の項目にアクセスすることを許可できます。

- すべてのレポート（オプションでレポーティング グループによって制限）
- メール ポリシー レポート（オプションでレポーティング グループによって制限）
- DLP レポート（オプションでレポーティング グループによって制限）
- メッセージ トラッキング
- スパム検疫

これらの各項目の詳細については、以下のセクションで説明します。また、これらの権限を付与されたすべてのユーザは、[Management Appliance] タブ > [Centralized Services] メニューを使用して、[System Status] を表示できます。Custom Email User ロールに割り当てられているユーザは、CLI にアクセスできません。

（注）　カスタム ユーザ ロールは各 Email Security アプライアンスから直接作成することもできます。Email Security アプライアンスのカスタム ユーザ ロールは、Security Management アプライアンスのカスタム ユーザ ロールが使用できない機能へのアクセス権を提供します。たとえば、メールおよび DLP ポリシーと、コンテンツ フィルタへのアクセス権を委任できます。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administration」の章にある「Managing Custom User Roles for Delegated Administration」セクションを参照してください。

電子メール レポーティング

次のセクションで説明するように、電子メール レポートへのアクセス権をカスタム ユーザ ロールに付与できます。

Security Management アプライアンスの [Email Security Monitor] ページの詳細については、「中央集中型電子メール レポーティングの使用」の該当する章を参照してください。

すべてのレポート

カスタム ロールにすべてのレポートへのアクセス権を付与すると、このロールを割り当てられたユーザは、すべての Email Security アプライアンス、または選択したレポーティング グループのいずれかに対する、次の [Email Security Monitor] ページを表示できます。

- Overview
- Incoming Mail
- Outgoing Destinations
- Outgoing Sender
- Internal Users
- DLP Incidents
- Content Filters

- Virus Types
- TLS Connections
- Outbreak Filters
- System Capacity
- Reporting Data Availability
- Scheduled Reports
- Archived Reports

メール ポリシー レポート

カスタム ロールにメール ポリシー レポートへのアクセス権を付与すると、このロールを割り当てられたユーザは、すべての Email Security アプライアンス、または選択したレポーティング グループのいずれかに対する、次の [Email Security Monitor] ページを表示できます。

- Overview
- Incoming Mail
- Outgoing Destinations
- Outgoing Senders
- Internal Users
- Content Filters
- Virus Types
- Outbreak Filters
- Reporting Data Availability
- Archived Reports

DLP レポート

カスタム ロールに DLP レポートへのアクセス権を付与すると、このロールを割り当てられたユーザは、すべての Email Security アプライアンス、または選択したレポーティング グループのいずれかに対する、次の [Email Security Monitor] ページを表示できます。

- DLP Incidents
- Reporting Data Availability
- Archived Reports

メッセージ トラッキング

カスタム ロールにメッセージ トラッキングへのアクセス権を付与すると、このロールを割り当てられたユーザは、Security Management アプライアンスによってトラッキングされたすべてのメッセージのステータスを表示できます。

DLP ポリシーに違反するメッセージ内の機密情報へのアクセスを制御するには、「メッセージ トラッキングでの機密情報へのアクセスのディセーブル化」（P.12-63）を参照してください。

Security Management アプライアンスでメッセージ トラッキングへのアクセスをイネーブルにするためのアプライアンスの設定方法など、メッセージ トラッキングの詳細については、「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。

検疫

カスタム ロールに検疫へのアクセス権を付与すると、このロールを割り当てられたユーザは、この Security Management アプライアンスのスパム検疫メッセージを検索、表示、配信、または削除できます。

ユーザがスパム検疫にアクセスできるようにするには、そのアクセス権をイネーブルにする必要があります。「Cisco IronPort スパム検疫の管理ユーザの設定」（P.7-6）を参照してください。

Security Management アプライアンスからこの検疫へのアクセスをイネーブルにするためのアプライアンスの設定方法など、スパム検疫の詳細については、「Cisco IronPort スパム検疫の管理」の章を参照してください。

Custom Email User ロールの作成

電子メール レポーティング、メッセージ トラッキング、およびスパム検疫へのアクセスに対して、Custom Email User ロールを作成できます。

これらの各オプションに許可されたアクセス権の詳細については、Custom Email User ロールについてとそのサブセクションを参照してください。

（注） より詳細なアクセス権、または他の機能、レポート、ポリシーへのアクセス権を付与するには、各 Email Security アプライアンスで直接カスタム ユーザ ロールを作成してください。

ステップ 1　メイン Security Management アプライアンスで、[Management Appliance] > [System Administration] > [User Roles] を選択します。

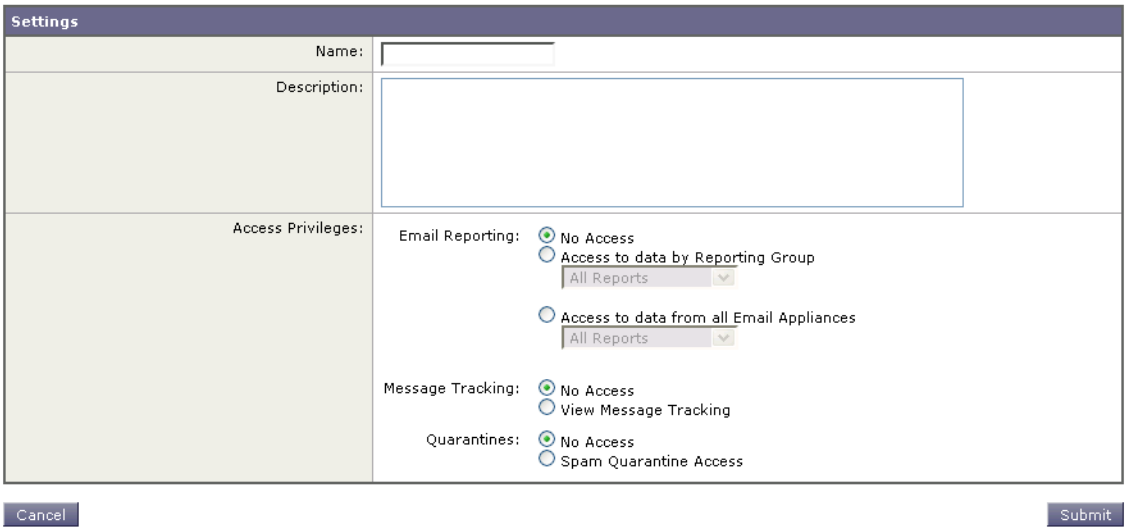
[User Roles] ページが表示されます。

ステップ 2　[Add Email User Role] をクリックします。

ヒント　または、既存の Email User ロールを複製して、新しいロールを作成できます。それには、該当するテーブルの行で [Duplicate] アイコンをクリックし、生成されたコピーを編集します。

[Add Email User Role] ページが表示されます。

図 12-12　[Add Email User Role] ページ



ステップ 3　ユーザ ロールの一意の名前（たとえば「dlp-auditor」）と説明を入力します。Email と Web のカスタム ユーザ ロール名を同じにしないでください。

（注）　名前には、小文字、数字、およびダッシュのみを使用してください。先頭をダッシュまたは数字にすることはできません。

ステップ 4　このロールに対してイネーブルにするアクセス権限を選択します。

ステップ 5　[Submit] をクリックして [User Roles] ページに戻ると、新しいユーザ ロールが表示されます。

ステップ 6　レポーティング グループごとにアクセス権を制限する場合は、該当するユーザ ロールの [Email Reporting] カラムにある [no groups selected] リンクをクリックして、少なくとも 1 つのレポーティング グループを選択します。

ステップ 7　変更を保存します。

ステップ 8　このロールにスパム検疫へのアクセス権を付与する場合は、このロールに対してアクセス権をイネーブルにします。「Cisco IronPort スパム検疫の管理ユーザの設定」（P.7-6）を参照してください。

Custom Email User ロールの編集

ステップ 1　[User Roles] ページでロール名をクリックし、[Edit Email User Role] ページを表示します。

ステップ 2　設定を編集します。

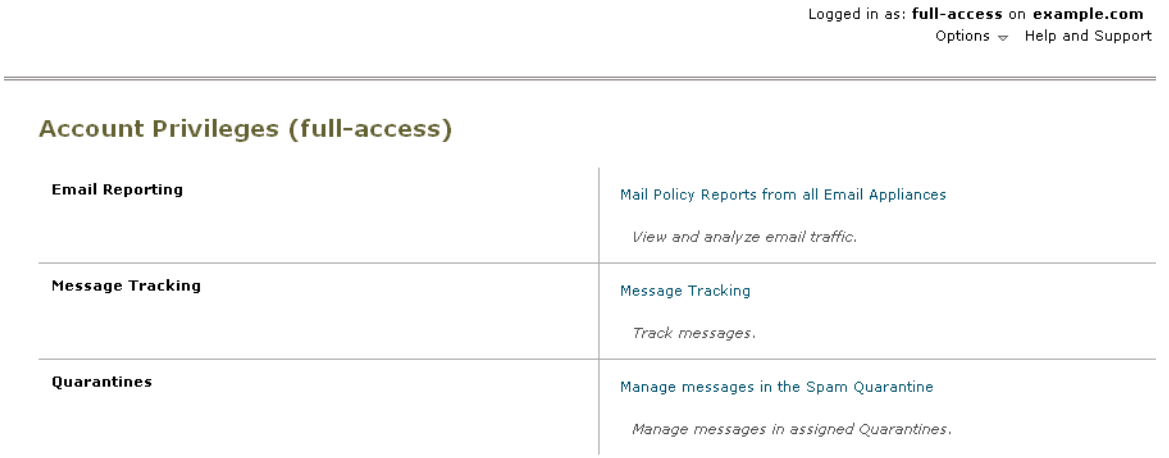
ステップ 3　変更を送信し、保存します。

ステップ 4　このロールにスパム検疫へのアクセス権を付与する場合は、このロールに対してアクセス権をイネーブルにします。「Cisco IronPort スパム検疫の管理ユーザの設定」（P.7-6）を参照してください。

Custom Email User ロールの使用

Custom Email User ロールに割り当てられているユーザがアプライアンスにログインすると、そのユーザには、ユーザがアクセス権を持つセキュリティ機能へのリンクだけが表示されます。そのユーザは、[Options] メニューで [Account Privileges] を選択することで、いつでもこのメインページに戻ることができます。これらのユーザは、Web ページの上部にあるメニューを使用して、アクセス権を持つ機能にアクセスすることもできます。次の例では、ユーザは Custom Email User ロールによって、Security Management アプライアンスで使用可能なすべての機能へのアクセス権を持ちます。

図 12-13　Custom Email User ロールが割り当てられている委任管理者の [Account Privileges] ページ



Custom Web User ロールについて

Custom Web User ロールでは、ユーザがポリシーを別の Web セキュリティ アプライアンスに公開することができ、カスタム設定を編集したり、別のアプライアンスに公開できるようになります。

Security Management アプライアンスの [Web] > [Configuration Master] > [Custom URL Categories] ページでは、管理および公開できる URL カテゴリとポリシーを表示できます。また、[Web] > [Utilities] > [Publish Configuration Now] ページに移動して、可能な設定を表示することもできます。

（注）　公開権限を持つカスタム ロールを作成した場合、ユーザがログインすると、使用可能なメニューが表示されないことに注意してください。URL やポリシー タブが機能を持たないため、このようなユーザには公開メニューが表示されず、編集不可の固定画面が表示されます。つまり、どのカテゴリまたはポリシーも公開または管理できないユーザを作ってしまうことになります。

この問題の回避策としては、ユーザが公開はできるが、どのカテゴリまたはポリシーも管理できないようにする場合、どのポリシーでも使用されていないカスタ

ム カテゴリを作成し、そのユーザに、そのカスタム カテゴリを管理する権限と公開する権限を付与する**必要があります**。このようにすると、ユーザがそのカテゴリで URL を追加または削除しても、他に影響が及びません。

カスタム ユーザ ロールを作成および編集して、Web 管理を委任できます。

- Custom Web User ロールの作成
- Custom Web User ロールの編集

Custom Web User ロールの作成

Custom Web User ロールを作成するには、次の手順を実行します。

ステップ 1　メイン Security Management アプライアンスで、[Management Appliance] > [System Administration] > [User Roles] を選択します。

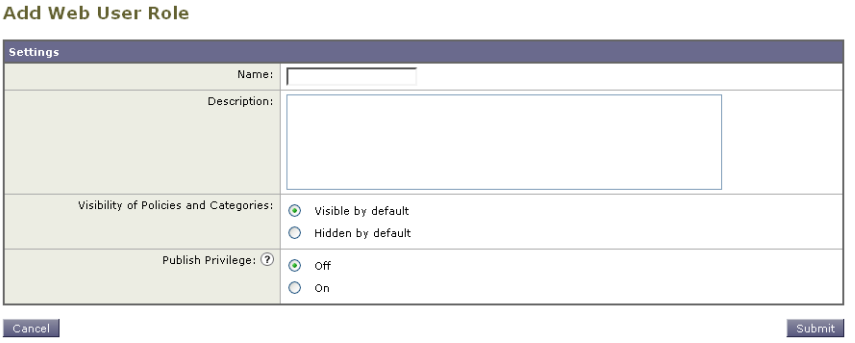
[User Roles] ページが表示されます。

ステップ 2　[Add Web User Role] をクリックします。

ヒント　または、既存の Web User ロールを複製して、新しいロールを作成できます。それには、該当するテーブルの行で [Duplicate] アイコンをクリックし、生成されたコピーを編集します。

[Add Web User Role] ページが表示されます。

図 12-14　[Add Web User Role] ページ



ステップ 3　ユーザ ロールの一意の名前（たとえば「canadian-admins」）と説明を入力します。

（注）　名前には、小文字、数字、およびダッシュのみを使用してください。先頭をダッシュにすることはできません。

ステップ 4　デフォルトで、ポリシーとカスタム URL カテゴリを表示するか、非表示にするかを選択します。

ステップ 5　公開権限をオンにするか、オフにするかを選択します。

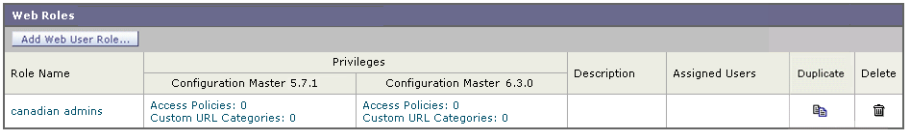
この権限を持つユーザは、ユーザがアクセス ポリシーまたは URL カテゴリを編集できるすべての Configuration Master を公開できます。

ステップ 6　新しい（空の）設定で始めるか、既存のカスタム ユーザ ロールをコピーするかを選択します。既存のユーザ ロールをコピーする場合は、コピーするロールをリストから選択します。

ステップ 7　[Submit] をクリックして [User Roles] ページに戻ると、新しいユーザ ロールが表示されます。

（注）　Web レポーティングで匿名機能をイネーブルにしていた場合、Web レポーティングへのアクセス権を持つすべてのユーザ ロールには、インタラクティブなレポート ページで認識できないユーザ名とロールが表示されるようになります。第 5 章「中央集中型 Web レポーティングの使用」のスケジュール設定されたレポートの管理のセクションを参照してください。Administrator ロールの場合は例外的に、スケジュール設定されたレポートで実際のユーザ名を確認できます。匿名機能がイネーブルになっている場合、オペレータおよび Web 管理者によって作成されたスケジュール設定されたレポートは匿名になります。

図 12-15　[User Roles] ページ



（注）　[Web] > [Utilities] > [Security Services Display] > [Edit Security Services Display] ページを使用して Configuration Master の 1 つを非表示にしている場合、[User Roles] ページでも対応する [Configuration Master] カラムが非表示になりますが、非表示になっている Configuration Master に対する権限設定は保持されます。

Custom Web User ロールの編集

Custom Web User ロール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　[User Roles] ページでロール名をクリックし、[Edit User Role] ページを表示します。

ステップ 2　名前、説明、およびポリシーとカスタム URL カテゴリを表示するかどうかなどの設定を編集します。

ステップ 3　[Submit] をクリックします。

カスタム ユーザ ロールの権限を編集するには、次の手順を実行します。

[User Roles] ページに移動します。

- アクセス ポリシー権限を編集するには、[Access policies] をクリックして、Configuration Master に設定されているアクセス ポリシーのリストを表示します。[Include] カラムで、ユーザ編集アクセス権を付与するポリシーのチェックボックスをオンにします。[Submit] をクリックして、[User Roles] ページに戻ります。

または

- カスタム URL カテゴリ権限を編集するには、カスタム URL カテゴリをクリックして、Configuration Master に定義されているカスタム URL カテゴリのリストを表示します。[Include] カラムで、ユーザ編集アクセス権を付与するカスタム URL カテゴリのチェックボックスをオンにします。[Submit] をクリックして、[User Roles] ページに戻ります。

GUI でのユーザ管理

管理タスクを実行するには、ユーザ アカウントを使用して、ユーザ ロールを割り当てることができます。

Cisco IronPort アプライアンスにはユーザ アカウントを追加するための 2 つの方法が用意されています。1 つは、ユーザ アカウントをアプライアンス自体に作成する方法で、もう 1 つは、独自の中央集中型認証システムを使用してユーザ認証をイネーブルにする方法です。これには、LDAP または RADIUS ディレクトリを使用できます。ユーザ、または外部認証ソースへの接続の管理は、GUI の [Management Appliance] > [System Administration] > [Users] ページで（または CLI で **userconfig** コマンドを使用して）行うことができます。ユーザの認証に外部ディレクトリを使用する方法の詳細については、「外部認証」（P.12-71）を参照してください。

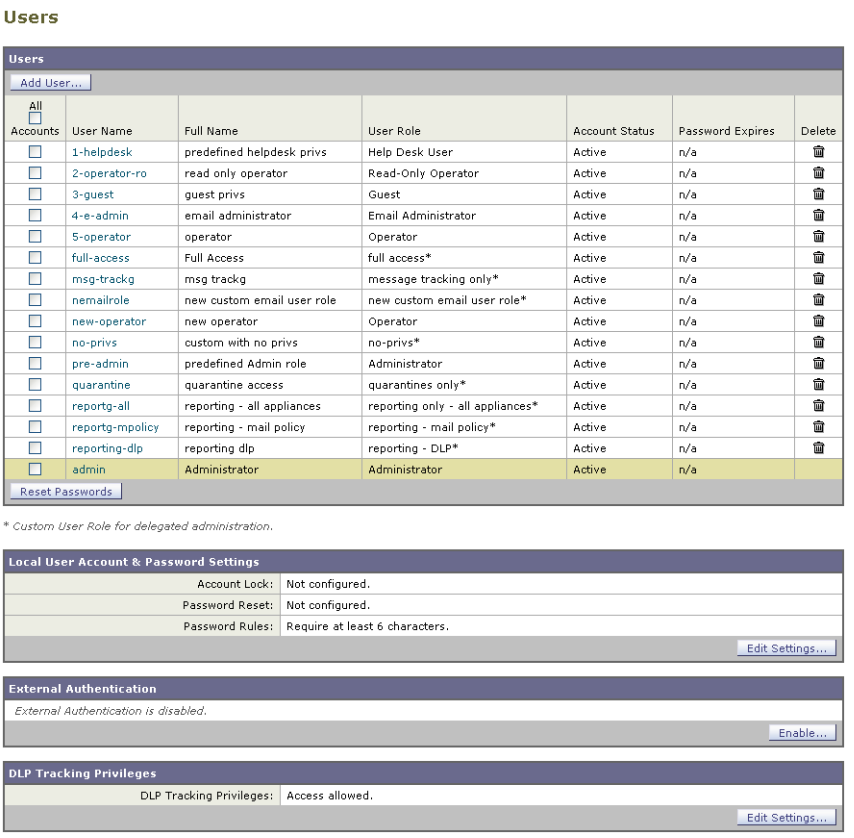
アプライアンスに作成できるユーザ アカウントの数に制限はありません。

ユーザ アカウントを管理するには、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] > [System Administration] > [Users] を選択します。

[Users] ページが表示されます。

図 12-16　[Users] ページ



[Users] ページには、システムの既存の管理ユーザが一覧（ユーザ名、氏名、およびユーザ ロールを含む）で表示されます。[Users] ページには、外部認証がイネーブルであるかどうかと、認証タイプも表示されます。

（注）　アスタリスクは、委任された管理に応じてユーザに割り当てられたカスタム ユーザ ロールを示します。ユーザのカスタム ロールが削除された場合は、[Unassigned] と赤く表示されます。ユーザ ロールの詳細（説明など）については、「ユーザ ロール」（P.12-43）を参照してください。

[Users] ページからは、次の操作が行えます。

- 新しいユーザの追加。
- ユーザの削除。
- ユーザの編集（admin ユーザのパスワード変更など）。
- 外部認証設定の編集。

ユーザの追加

外部認証を使用していない場合は、次の手順に従って、ユーザを Security Management アプライアンスに直接追加します。

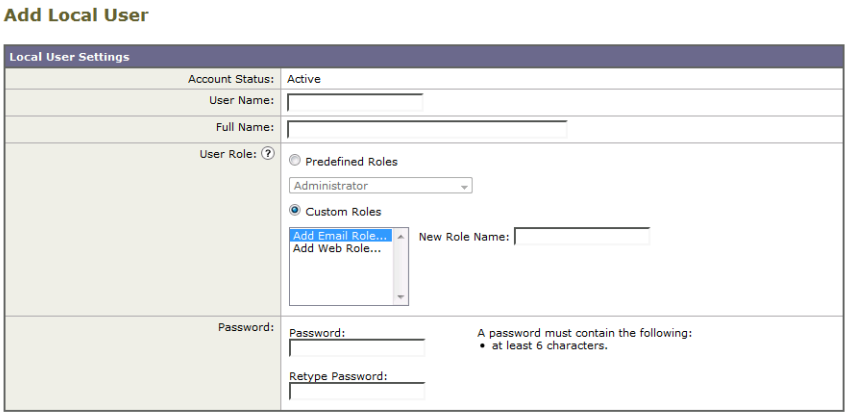
ステップ 1　カスタム ユーザ ロールを割り当てる場合は、そのロールを先に定義しておくことをお勧めします。「カスタム ユーザ ロールへの管理委任」（P.12-49）を参照してください。

ステップ 2　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [Users] を選択します。

ステップ 3　[Add User] をクリックします。

[Add Local User] ページが表示されます。

図 12-17　　ユーザの追加



ステップ 4　ユーザの一意の名前を入力します。システムで予約されている語（「operator」や「root」など）を入力することはできません。

ステップ 5　ユーザの氏名を入力します。

ステップ 6　事前定義されたロールまたはカスタム ロールを選択します。ユーザ ロールの詳細については、表 12-2 を参照してください。

新しい Email ロールまたは Web ロールをここに追加する場合は、ロールの名前を入力します。命名上の制限については、「Custom Email User ロールの作成」（P.12-52）または「Custom Web User ロールの作成」（P.12-56）を参照してください。

ステップ 7　パスワードを入力し、パスワードを再入力します。パスワードは、6 文字以上にする必要があります。

ステップ 8　[Submit] をクリックして、ユーザを追加します。

ステップ 9　[Commit] をクリックして変更を確定します。

ステップ 10　このページにカスタム ユーザ ロールを追加する場合は、この時点でそのロールに権限を割り当てます。「カスタム ユーザ ロールへの管理委任」（P.12-49）を参照してください。

ユーザの編集

ユーザを編集（パスワードの変更など）するには、次の手順を実行します。

ステップ 1　[Users] 一覧でユーザの名前をクリックします。[Edit Local User] ページが表示されます。

ステップ 2　ユーザに対して変更を行います。

ステップ 3　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

ユーザの削除

ユーザを削除するには、次の手順を実行します。

ステップ 1　[Users] 一覧でユーザの名前に対応するゴミ箱の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　[Commit] をクリックして変更を確定します。

メッセージ トラッキングでの機密情報へのアクセスのディセーブル化

データ消失防止（DLP）ポリシーに違反するメッセージには、通常、企業の機密情報や個人情報（クレジット カード番号や健康診断結果など）といった機密情報が含まれています。デフォルトで、この内容はメッセージ トラッキング結果に表示されているメッセージの [Message Details] ページにある [DLP Matched Content] タブに表示されます。

このタブとその内容は、メッセージ トラッキングへのアクセス権を持つ、管理者以外のユーザには表示されないようにすることができます。管理者ユーザは、常にこのコンテンツを表示できます。

管理者以外のユーザに機密情報を表示しないようにするには、次の手順を実行します。

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

ステップ 2　[DLP Tracking Privileges] の下にある [Edit Settings] をクリックします。

[DLP Tracking Privileges] ページが表示されます。

図 12-18　[DLP Tracking Privileges] ページ

ステップ 3　[Allow access to DLP Matched Content in Message Tracking results] チェックボックスをオフにします。

ステップ 4　変更を送信し、保存します。

この設定を有効にするには、[Management Appliance] > [Centralized Services] で中央集中型電子メール メッセージ トラッキング機能をイネーブルにする必要があります。

複数のユーザをサポートする追加コマンド：who、whoami、last

次に、アプライアンスへの複数ユーザ アクセスをサポートするコマンドを示します。

- **who** コマンドは、CLI からシステムにログインしたすべてのユーザ、ログイン時間、アイドル時間、およびユーザがログインしたリモート ホストを一覧表示します。

```
mail3.example.com> who


Username  Login Time  Idle Time  Remote Host  What

========  ==========  =========  ===========  ====

admin     03:27PM     0s         10.1.3.201   cli
```

- whoami コマンドは、現在ログインしているユーザのユーザ名および氏名と、ユーザが属しているグループを表示します。

```
mail3.example.com> whoami


Username: admin

Full Name: Administrator

Groups: admin, operators, config, log, guest
```

- last コマンドは、アプライアンスに最近ログインしたユーザを表示します。リモート ホストの IP アドレス、ログイン、ログアウト、および合計時間も表示されます。

```
mail3.example.com> last
```

```
Username  Remote Host  Login Time        Logout Time       Total Time
========  ===========  ================  ================  ==========
admin     10.1.3.67    Sat May 15 23:42  still logged in   15m
admin     10.1.3.67    Sat May 15 22:52  Sat May 15 23:42  50m
admin     10.1.3.67    Sat May 15 11:02  Sat May 15 14:14  3h 12m
admin     10.1.3.67    Fri May 14 16:29  Fri May 14 17:43  1h 13m
shutdown                                 Fri May 14 16:22
shutdown                                 Fri May 14 16:15
admin     10.1.3.67    Fri May 14 16:05  Fri May 14 16:15  9m
admin     10.1.3.103   Fri May 14 16:12  Fri May 14 16:15  2m
admin     10.1.3.103   Thu May 13 09:31  Fri May 14 14:11  1d 4h 39m
admin     10.1.3.135   Fri May 14 10:57  Fri May 14 10:58  0m
admin     10.1.3.67    Thu May 13 17:00  Thu May 13 19:24  2h 24m
```

制限ユーザ アカウントとパスワードの設定

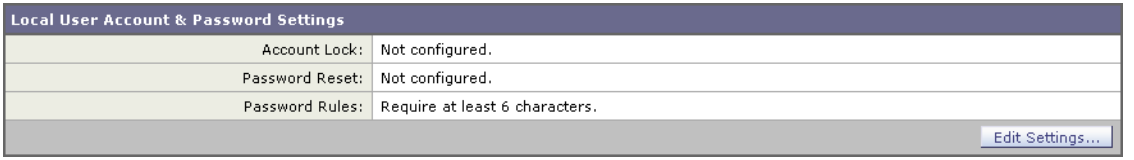
ユーザ アカウントとパスワードの制限を定義して、組織全体にパスワード ポリシーを強制的に適用することができます。ユーザ アカウントとパスワードの制限は、Cisco IronPort アプライアンスに定義されたローカル ユーザに適用されます。次の設定値を設定できます。

- **ユーザ アカウントのロック。**ユーザがアカウントからロックアウトされるまでの、ログイン試行の失敗回数を定義できます。
- **パスワード期限の規則。**ログイン後にユーザがパスワードの変更を要求されるまでの、パスワードの使用期間を定義できます。
- **パスワードの規則。**どの文字が任意で、どの文字が必須かなど、ユーザが選択できるパスワードの種類を定義できます。

ユーザ アカウントおよびパスワードの制限は、[Local User Account] および [Password Settings] セクションの、[Management Appliance] > [System Administration] > [Users] ページで定義できます。

図 12-19 に、[Users] ページの [Local User Account] および [Password Settings] セクションを示します。

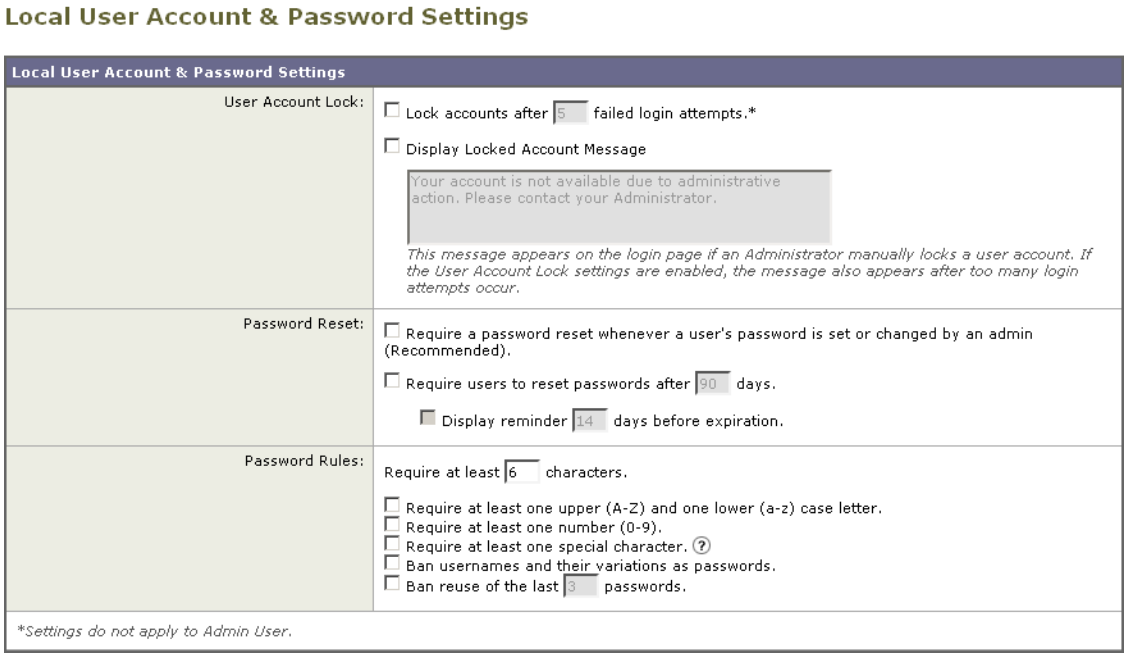
図 12-19　[Users] ページ、[Local User Account] および [Password Settings] セクション



ユーザ アカウントとパスワードの制限を設定するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [System Administration] > [Users] ページの [Local User Account and Password Settings] セクションで、[Edit Settings] をクリックします。[Local User Account and Password Settings] ページが表示されます。

図 12-20　ユーザ アカウントとパスワード制限の設定



ステップ 2　表 12-4 に示す設定値を設定します。

表 12-4　ローカル ユーザ アカウントとパスワードの設定

設定	説明
User Account Lock	ユーザが正常にログインできない場合に、ユーザ アカウントをロックするかどうかを決定します。アカウントがロックされるまでの、ログイン失敗回数を指定します。1 ～ 60 の範囲で任意の数字を入力できます。デフォルト値は 5 です。 アカウントのロックを設定する場合は、ログインしようとしているユーザに表示されるメッセージを入力します。7 ビットの ASCII 文字を使用して、テキストを入力します。このメッセージは、ユーザがロックされたアカウントに正しいパスワードを入力した場合だけ表示されます。 ユーザ アカウントがロックされた場合は、管理者が GUI の [Edit User] ページか、`userconfig` CLI コマンドを使用して、ロック解除できます。 ユーザが接続に使用したマシン、または接続の種類（SSH または HTTP）に関係なく、失敗したログイン試行はユーザごとに追跡されます。ユーザが正常にログインすると、失敗したログイン試行回数はゼロ（0）にリセットされます。 失敗したログイン試行の最大数に達したためにユーザ アカウントがロックアウトされた場合、アラートが管理者に送信されます。このアラートは「Info」セキュリティ レベルに設定されます。 **（注）**　個々のユーザ アカウントを手動でロックすることもできます。

表 12-4　ローカル ユーザ アカウントとパスワードの設定（続き）

設定	説明
Password Reset	管理者がユーザのパスワードを変更後、ユーザにパスワードの変更を強制するかどうかを決定します。 また、パスワードの有効期限が切れた後に、ユーザにパスワードの変更を強制するかどうかを決定することもできます。ユーザによるパスワードの変更が必要になるまでの、パスワードの有効日数を入力します。1 ～ 366 の範囲で任意の数字を入力できます。デフォルトは 90 です。 パスワードの期限が切れた後、ユーザにパスワードの変更を強制する場合は、次回のパスワード期限切れについての通知を表示できます。期限切れの何日前に通知が行われるかを選択します。 パスワードが期限切れになると、ユーザは次回のログイン時にアカウント パスワードの変更を強制されます。 **（注）** ユーザ アカウントがパスワード チャレンジではなく SSH キーを使用している場合も、パスワードのリセット規則は適用されます。SSH キーを持つユーザ アカウントが期限切れになると、そのユーザは古いパスワードを入力するか、管理者に依頼して、パスワードを手動で変更し、アカウントに関連付けられたキーを変更してもらう必要があります。
Password Rules: Require at <number> least characters.	パスワードに含める最小文字数を入力します。 6 ～ 128 の範囲で任意の数字を入力できます。デフォルトは 6 です。
Password Rules: Require at least one number (0-9).	パスワードに 1 文字以上の数字を含める必要があるかどうかを決定します。

表 12-4　ローカル ユーザ アカウントとパスワードの設定（続き）

設定	説明
Password Rules: Require at least one special character.	パスワードに 1 文字以上の特殊文字を含める必要があるかどうかを決定します。パスワードには、次の特殊文字を使用できます。 ~ ?!@ # $ % ^ & * - _ + = ¥ | / [ ] ( ) < > { } ` ' " ; : , .
Password Rules: Ban usernames and their variations as passwords.	対応するユーザ名またはユーザ名の変化形と同じものを、パスワードに使用できるかどうかを決定します。ユーザ名の変化形の使用を禁止する場合、次の規則がパスワードに適用されます。 • 大文字か小文字かに関係なく、パスワードはユーザ名と同じであってはならない。 • 大文字か小文字かに関係なく、パスワードはユーザ名を逆にしたものと同じであってはならない。 • パスワードは、次の文字置換が行われたユーザ名、またはユーザ名を逆にしたものと同じであってはならない。 – 「a」の代わりに「@」または「4」 – 「e」の代わりに「3」 – 「i」の代わりに「|」、「!」、または「1」 – 「o」の代わりに「0」 – 「s」の代わりに「$」または「5」 – 「t」の代わりに「+」または「7」
Password Rules: Ban reuse of the last <number> passwords.	ユーザにパスワードの変更を強制する場合に、最近使用したパスワードを選択できるかどうかを決定します。最近のパスワードの再利用を禁止した場合、再利用を禁止する最近のパスワードの個数を入力します。 1 ～ 15 の範囲で任意の数字を入力できます。デフォルトは 3 です。

ステップ 3　変更を送信し、保存します。

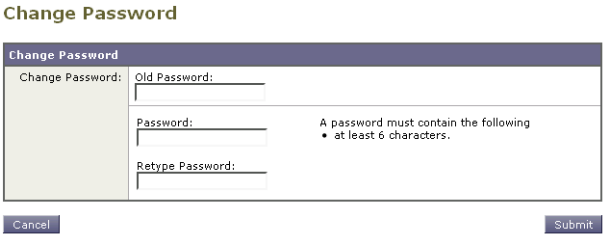
パスワードの変更

システムに設定されたユーザのパスワードを変更するには、GUI の [Edit User] ページを使用します（詳細は、「ユーザの編集」（P.12-62）を参照してください）。

システムのデフォルト admin ユーザ アカウントのパスワードを変更するには、GUI の [Edit User] ページを使用するか（詳細は、「ユーザの編集」（P.12-62）を参照してください）、CLI で `password` または `passwd` コマンドを使用します。admin ユーザ アカウントのパスワードを忘れた場合は、カスタマー サポート プロバイダーに問い合わせて、パスワードをリセットしてください。

GUI 上部の [Options] メニューをクリックして、[Change Password] オプションを選択することで、ユーザは自分のパスワードを変更できます。

図 12-21　[Change Password] ページ



古いパスワードを入力してから新しいパスワードを入力し、確認のためにもう一度新しいパスワードを入力します。[Submit] をクリックして、ログアウトします。ログイン画面が表示されます。

外部認証

ユーザ情報をネットワーク上の LDAP または RADIUS ディレクトリに保存した場合、アプライアンスにログインするユーザの認証に外部ディレクトリを使用するように Cisco IronPort アプライアンスを設定できます。

認証に外部ディレクトリを使用するようにアプライアンスをセットアップするには、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] > [System Administration] > [Users] を選択します。

（注）　アプライアンスが外部ディレクトリと通信できない場合、ユーザはアプライアンスのローカル ユーザ アカウントでログインできます。

図 12-22　外部認証の確立

（注）　認証に外部ディレクトリを使用するようにアプライアンスをセットアップするには、コマンドライン プロンプトで **userconfig** コマンドと **external** サブコマンドを使用します。

LDAP 認証のイネーブル化

ユーザを認証するために LDAP ディレクトリを使用する以外に、LDAP グループを Cisco IronPort ユーザ ロールに割り当てることができます。たとえば、IT というグループ内のユーザに Administrator ユーザ ロールを割り当て、Support というグループのユーザに Help Desk User ロールを割り当てることができます。ユーザが異なるユーザ ロールを持つ複数の LDAP グループに属する場合は、AsyncOS がユーザに最も制限されたロールの権限を割り当てます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。

LDAP を使用して外部認証をイネーブルにする前に、LDAP サーバ プロファイルと LDAP サーバの外部認証クエリーを定義します。詳細は、『*Cisco IronPort AsyncOS for Email Advanced User Guide*』の LDAP クエリーに関する章を参照してください。

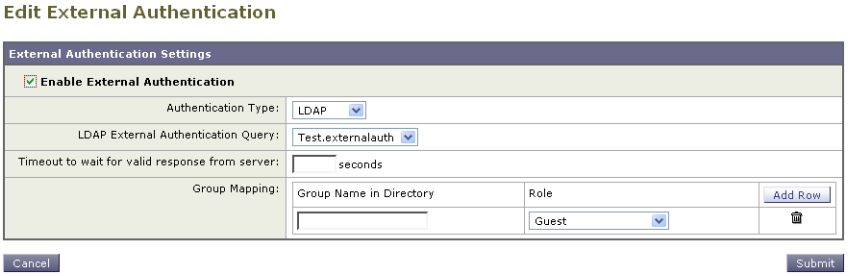
LDAP を使用して外部認証をイネーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [Users] ページを選択します。

ステップ 2　[Enable] をクリックします。

[Edit External Authentication] ページが表示されます。

図 12-23　　LDAP を使用した外部認証のイネーブル化



ステップ 3　[Enable External Authentication] チェックボックスをオンにします。

ステップ 4　認証タイプとして LDAP を選択します。

ステップ 5　ユーザを認証する LDAP 外部認証クエリーを選択します。

ステップ 6　タイムアウトするまでアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。

ステップ 7　アプライアンスで認証する LDAP ディレクトリからのグループ名を入力し、グループのユーザに対するロールを選択します。

ステップ 8　また、[Add Row] をクリックして別のディレクトリ グループを追加することもできます。アプライアンスが認証する各ディレクトリ グループに対して、ステップ 7 とステップ 8 を繰り返します。

ステップ 9　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

RADIUS 認証のイネーブル化

ユーザの認証に RADIUS ディレクトリを使用し、ユーザのグループを Cisco IronPort ロールに割り当てることもできます。RADIUS サーバは CLASS 属性をサポートする必要があります（AsyncOS は RADIUS ディレクトリのユーザを Cisco IronPort ユーザ ロールに割り当てるために CLASS 属性を使用します）。

AsyncOS は、RADIUS サーバと通信するために Password Authentication Protocol（PAP; パスワード認証プロトコル）と Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）の 2 つの認証プロトコルをサポートします。

RADIUS ユーザを Cisco IronPort ユーザ ロールに割り当てるには、最初に RADIUS サーバで <radius-group> という文字列値を使用して CLASS 属性を設定します（これは Cisco IronPort ユーザ ロールにマップされます）。CLASS 属性には文字、数字、およびダッシュを含めることができますが、先頭にダッシュを使用することはできません。AsyncOS は CLASS 属性で複数の値をサポートしません。CLASS 属性またはマップされていない CLASS 属性がないグループに属する RADIUS ユーザはアプライアンスにログインできません。

アプライアンスが RADIUS サーバと通信できない場合、ユーザはアプライアンスのローカル ユーザ アカウントでログインできます。

（注） 外部ユーザが RADIUS グループのユーザ ロールを変更する場合、外部ユーザはアプライアンスからログアウトし、再びログインする必要があります。このユーザは新しいロールの権限を持ちます。

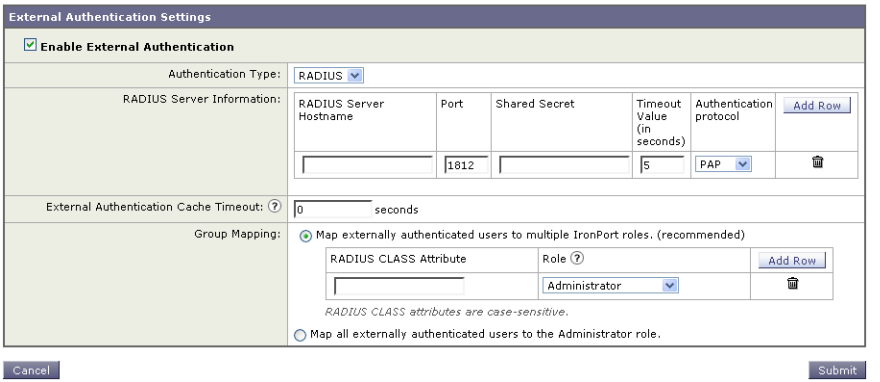
RADIUS を使用して外部認証をイネーブルにするには、次の手順を実行します。

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

ステップ 2　[Enable External Authentication] チェックボックスをオンにします。

ステップ 3　認証タイプとして RADIUS を選択します。

図 12-24　RADIUS を使用した外部認証のイネーブル化



ステップ 4　RADIUS サーバのホスト名を入力します。

ステップ 5　RADIUS サーバのポート番号を入力します。デフォルトのポート番号は 1812 です。

ステップ 6　RADIUS サーバの共有秘密パスワードを入力します。

（注）　Cisco IronPort アプライアンスのクラスタに対して外部認証をイネーブルにするには、クラスタ内のすべてのアプライアンスで同じ共有秘密パスワードを入力します。

ステップ 7　タイムアウトするまでアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。

ステップ 8　RADIUS 認証として PAP を使用するか、CHAP を使用するかを選択します。

ステップ 9　また、[Add Row] をクリックして別の RADIUS サーバを追加することもできます。認証のためにアプライアンスで使用する各 RADIUS サーバに対してステップ 6 とステップ 7 を繰り返します。

ステップ 10　Web ユーザ インターフェイスで、外部認証クレデンシャルを保存する時間を入力します。

ステップ 11　RADIUS ユーザのグループを Cisco IronPort ロールにマップするかどうか、またはすべての RADIUS ユーザに Administrator ロールを割り当てるかどうかを選択します。RADIUS グループを Cisco IronPort ロールにマップすることを推奨します。

ステップ 12　RADIUS グループを Cisco IronPort ロールにマップすることを選択した場合は、グループの RADIUS CLASS 属性を入力し、その CLASS 属性を持つユーザのロールを選択します。

ステップ 13　また、[Add Row] をクリックして別のグループを追加することもできます。アプライアンスが認証するユーザの各グループに対してステップ 11 とステップ 12 を繰り返します。

ステップ 14　変更を送信し、保存します。

Security Management アプライアンスへのアクセス権の設定

AsyncOS では、Security Management アプライアンスへのユーザのアクセス権管理を、管理者が制御できます。これを使用して、Web UI セッションのタイムアウトや、ユーザと組織のプロキシ サーバからアプライアンスへのアクセス元となる IP アドレスを指定する、アクセス リストなどを管理できます。

IP ベースのネットワーク アクセスの設定

組織がリモート ユーザに逆プロキシを使用する場合、アプライアンスに直接接続するユーザ、および逆プロキシを介して接続するユーザのためのアクセス リストを作成することで、ユーザがどの IP アドレスから Security Management アプライアンスにアクセスするのかを制御できます。

直接接続

Security Management アプライアンスに接続できるマシンの IP アドレス、サブネット、または CIDR アドレスを指定できます。ユーザは、アクセス リストの IP アドレスを持つすべてのマシンから、アプライアンスにアクセスできます。リストに含まれていないアドレスからアプライアンスに接続しようとするユーザは、アクセスを拒否されます。

プロキシ経由の接続

組織のネットワークで、リモート ユーザのマシンと Security Management アプライアンスの間で逆プロキシが使用されている場合、AsyncOS では、アプライアンスに接続できるプロキシの IP アドレスのアクセス リストを作成できます。

逆プロキシを使用している場合でも、AsyncOS は、ユーザ接続が許可されている IP アドレスのリストと照合して、リモート ユーザのマシンの IP アドレスを検証します。リモート ユーザの IP アドレスを Email Security アプライアンスに送信するには、プロキシで `x-forwarded-for` HTTP ヘッダーをアプライアンスへの接続要求に含める必要があります。

`x-forwarded-for` ヘッダーは非 RFC 標準 HTTP ヘッダーであり、形式は次のとおりです。

```
x-forwarded-for: client-ip, proxy1, proxy2,... CRLF.
```

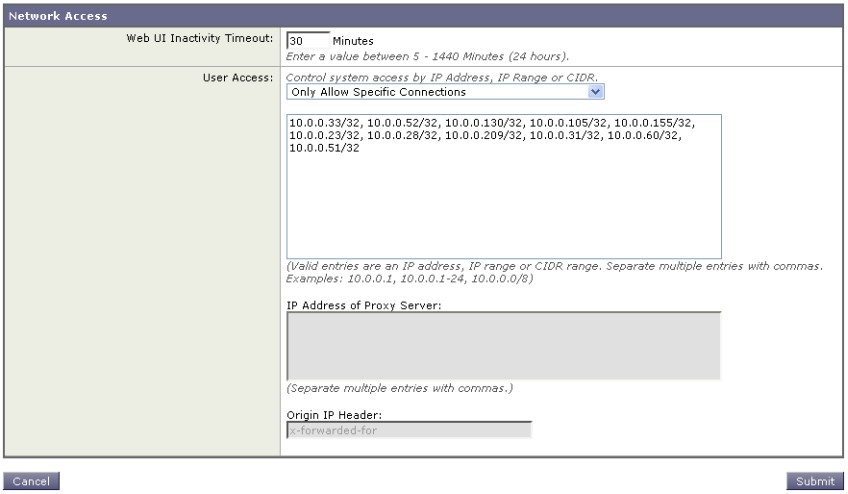
このヘッダーの値はカンマ区切りの IP アドレスのリストであり、左端のアドレスがリモート ユーザ マシンのアドレスで、その後に、接続要求を転送した一連の各プロキシのアドレスが続きます。（ヘッダー名は設定可能です）。Security Management アプライアンスは、ヘッダーから取得したリモート ユーザの IP アドレスおよび接続プロキシの IP アドレスを、アクセス リスト内の許可されたユーザ IP アドレスおよびプロキシ IP アドレスと照合します。

（注） AsyncOS は、`x-forwarded-for` ヘッダーで IPv4 アドレスだけをサポートします。

アクセス リストの作成

GUI の [Network Access] ページまたは CLI の **adminaccessconfig > ipaccess** コマンドから、ネットワーク アクセス リストを作成できます。図 12-25 は、Security Management アプライアンスへの直接的な接続が許可されているユーザ IP アドレスのリストが表示された [Network Access] ページを示しています。

図 12-25　[Network Access] の設定



AsyncOS には、アクセス リストに対する次の 4 つの異なる制御モードが用意されています。

- [Allow All]。このモードでは、アプライアンスへのすべての接続が許可されます。これが、デフォルトの動作モードです。
- [Only Allow Specific Connections]。このモードは、ユーザの IP アドレスが、アクセス リストに含まれている IP アドレス、IP 範囲、または CIDR 範囲と一致する場合に、ユーザのアプライアンスへの接続を許可します。
- [Only Allow Specific Connections Through Proxy]。このモードは、次の条件が満たされた場合に、逆プロキシを介したユーザのアプライアンスへの接続を許可します。
  - 接続プロキシの IP アドレスが、[Proxy Server] フィールドのアクセス リストの IP アドレスに含まれている。
  - プロキシで、接続要求に `x-forwarded-header` HTTP ヘッダーが含まれている。
  - `x-forwarded-header` の値が空ではない。
  - リモート ユーザの IP アドレスが `x-forwarded-header` に含まれ、それがアクセス リスト内の IP アドレス、IP 範囲、または CIDR 範囲と一致する。

- [Only Allow Specific Connections Directly or Through Proxy]。このモードは、ユーザの IP アドレスが、アクセス リストに含まれている IP アドレス、IP 範囲、または CIDR 範囲と一致する場合に、ユーザの逆プロキシを介した、あるいは直接的なアプライアンスへの接続を許可します。プロキシを介した接続の条件は、[Only Allow Specific Connections Through Proxy] モードの場合と同じです。

次のいずれかの条件に該当する場合、変更をサブミットおよびコミットした後に、アプライアンスにアクセスできなくなる可能性があります。

- [Only Allow Specific Connections] を選択し、現在のマシンの IP アドレスがリストに含まれていない場合。
- [Only Allow Specific Connections] を選択し、アプライアンスに現在接続されているプロキシの IP アドレスがプロキシ リストになく、元の IP ヘッダーの値が許可された IP アドレスのリストにない場合。
- [Only Allow Specific Connections Directly or Through Proxy] を選択し、次が当てはまる場合。
  - 元の IP ヘッダーの値が許可される IP アドレスのリストにない

    または
  - 元の IP ヘッダーの値が許可される IP アドレスのリストになく、アプライアンスに接続されているプロキシの IP アドレスが許可されるプロキシのリストにない。

アクセス リストを修正せずに続行した場合、ユーザが変更を確定すると、AsyncOS はアプライアンスからユーザのマシンまたはプロキシを切断します。

Security Management アプライアンスのアクセス リストを作成するには、次の手順を実行します。

ステップ 1　[System Administration] > [Network Access] ページを使用します。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　アクセス リストの制御モードを選択します。

ステップ 4　ユーザがアプライアンスへの接続が許可される IP アドレスを入力します。

IP アドレス、IP アドレス範囲または CIDR 範囲を入力できます。複数のエントリを区切るには、カンマを使用します。

ステップ 5　プロキシ経由の接続が許可されている場合は、次の情報を入力します。

- アプライアンスへの接続が許可されているプロキシの IP アドレス。複数のエントリを区切るには、カンマを使用します。

- プロキシがアプライアンスに送信する発信元の IP ヘッダーの名前。これには、リモート ユーザ マシンの IP アドレスと、要求を転送したプロキシ サーバの IP アドレスが含まれます。デフォルトでは、ヘッダーの名前が `x-forwarded-for` です。

ステップ 6　変更を送信し、保存します。

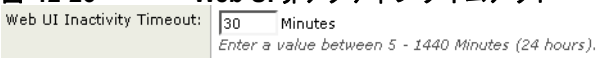
Web UI セッション タイムアウトの設定

Security Management アプライアンスの Web UI から AsyncOS が、非アクティブなユーザをログアウトするまでの時間を指定できます。この Web UI セッション タイムアウトは、admin を含めて、すべてのユーザに適用され、また HTTP セッションと HTTPS セッションの両方に使用されます。

AsyncOS によってユーザがログアウトされると、アプライアンスはユーザの Web ブラウザをログイン ページにリダイレクトします。

（注）　Web UI セッション タイムアウトは IronPort スパム検疫セッションには適用されません。このセッションには 30 分のタイムアウトが設定されており、変更できません。

図 12-26　Web UI 非アクティブ タイムアウト



Web UI セッションに非アクティブ タイムアウトを定義するには、次の手順を実行します。

ステップ 1　[System Administration] > [Network Access] ページを使用します。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　ユーザが非アクティブ状態になった後、何分経過後にログアウトされるかを入力します。タイムアウト時間には 5 ～ 1440 分を定義できます。

ステップ 4　変更を送信し、保存します。

アクティブなセッションの表示

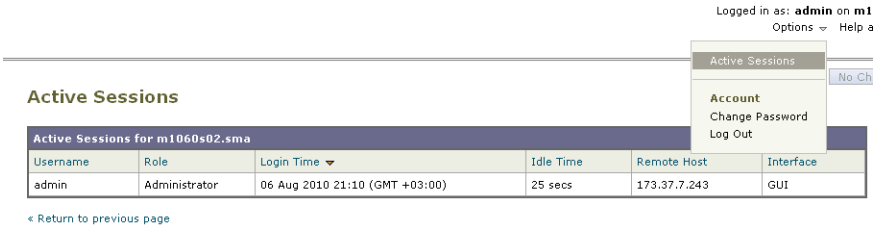
Security Management アプライアンスでは、アプライアンス上のすべてのアクティブなセッションと、ログインしているユーザを表示できます。

アクティブなセッションを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのページで、[Options] > [Active Sessions] を選択します。

[Active Sessions] ページが表示されます。

図 12-27　[Active Sessions] ページ



[Active Sessions] ページから、ユーザ名、ユーザが持っているロール、ユーザのログイン時間、アイドル時間、およびユーザがコマンドラインと GUI のどちらからログインしたかを表示できます。

生成されたメッセージの返信アドレスの設定

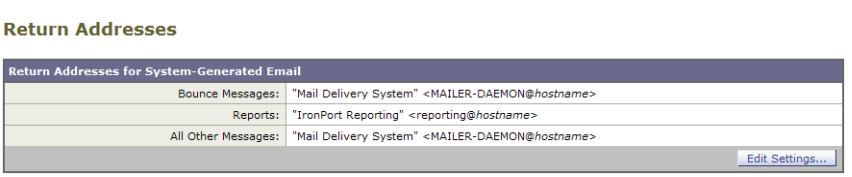
次の場合に対して、AsyncOS で生成されたメールのエンベロープ送信者を設定できます。

- 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 12-28　[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、変更を確定します。

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.12-89）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.12-90）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。

- System
- Hardware

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。

SMTP ルートおよびアラート

アプライアンスから [Alert Recipient] セクションで指定されたアドレスに送信されるアラートは、該当の送信先に対して定義された SMTP ルートに従います。

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 はシステムの稼動時間、**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.12-89）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

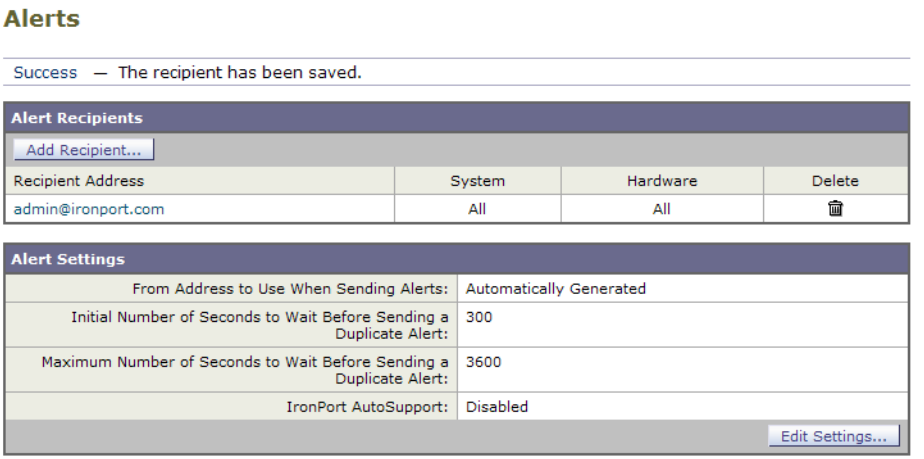
```
Date: 23 Mar 2007 21:10:19 +0000

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、「グラフィカル ユーザ インターフェイスへのアクセス」（P.2-8）を参照してください）。

図 12-29　[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。

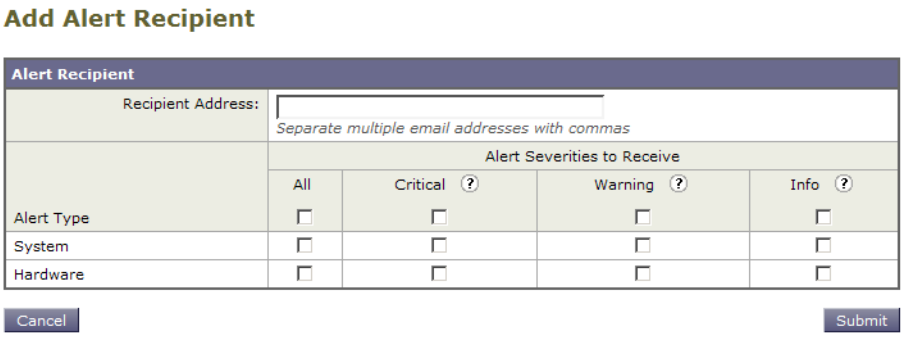
- アラート受信者の追加、設定、または削除。
- アラート設定値の変更。

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 12-30　　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

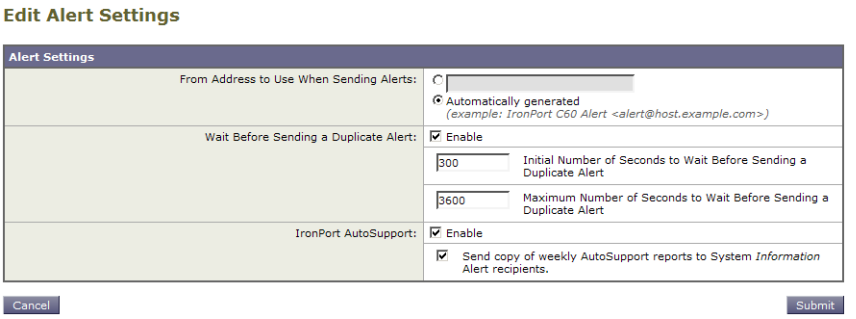
アラート設定はグローバルな設定であるため、すべてのアラートの動作に影響します。

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 12-31　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.12-84）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.12-85）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 12-5 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 12-5　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 12-6 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 12-6　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

表 12-6　システム アラートのリスト（続き）

アラート名	説明	重大度
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
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

表 12-6　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.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
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

表 12-6　システム アラートのリスト（続き）

アラート名	説明	重大度
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
SMTPAUTH.LDAP_QUERY_FAILED	LDAP クエリーが失敗した場合に送信されます。	Warning

表 12-6　システム アラートのリスト（続き）

アラート名	説明	重大度
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 ウィザードについて」（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 12-7　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「二重 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.12-97）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。

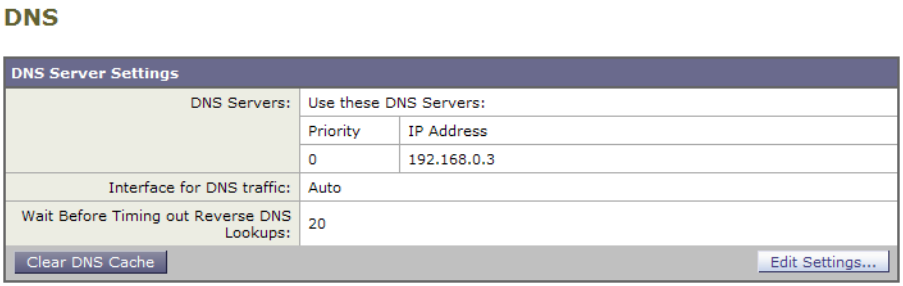
DNS キャッシュのクリア

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 12-32　　[DNS] ページ

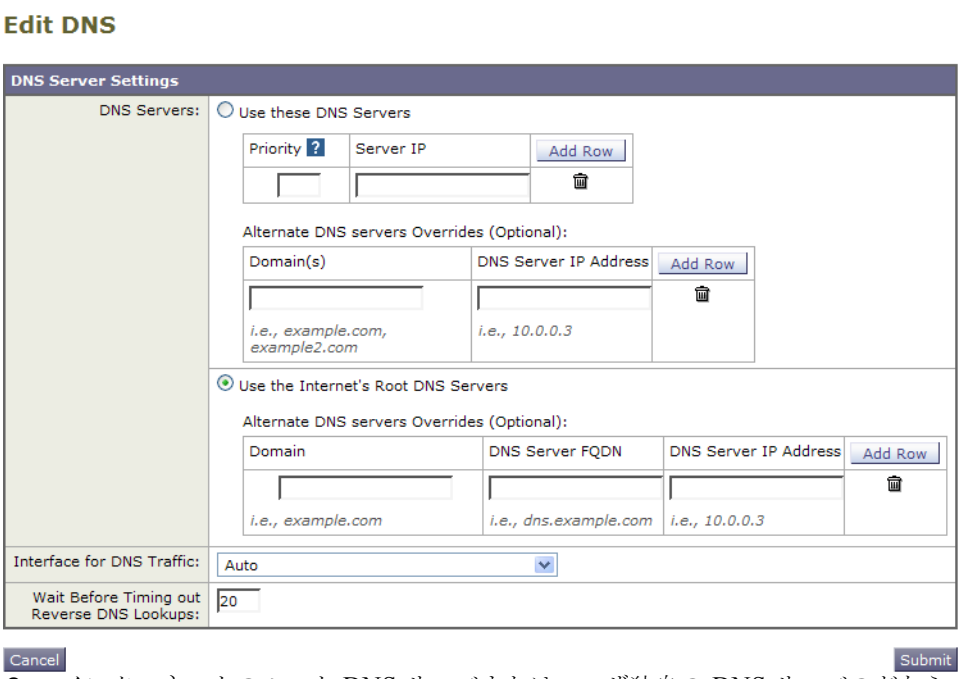


DNS 設定値を GUI から編集するには、次の手順を実行します。

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 12-33　[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.12-97）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

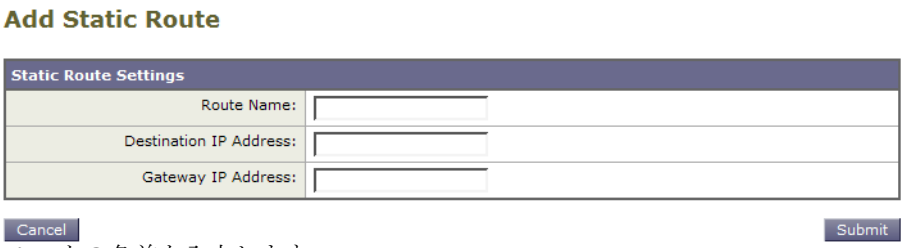
[Management Appliance] > [Network] > [Routing] ページを使用して、スタティック ルートの作成、編集、または削除を行えます。このページからデフォルト ゲートウェイの変更もできます。

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 12-34　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。

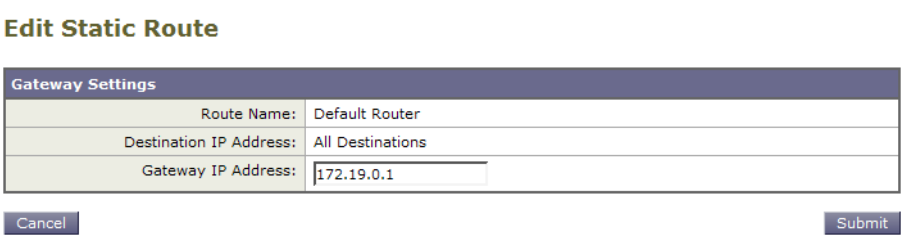
ステップ 3　変更を送信し、保存します。

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 12-35　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.12-103）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、「ユーザの編集」（P.12-62）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

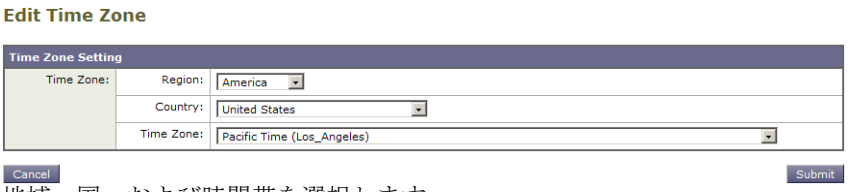
[Time Zone] ページ（GUI の [System Administration] メニューから利用可能）では、Cisco IronPort アプライアンスの時間帯が表示されます。特定の時間帯または GMT オフセットを選択できます。

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 12-36　[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。

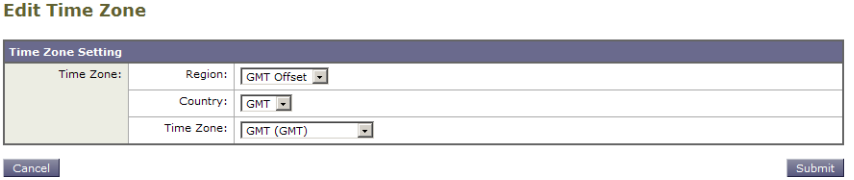
GMT オフセットの選択

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 12-37　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。

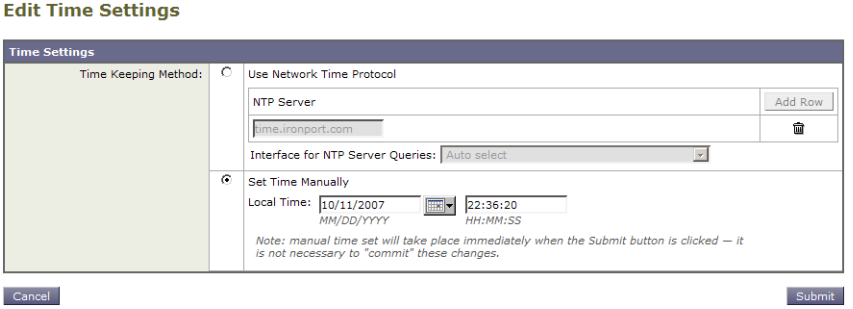
ステップ 4　変更を送信し、保存します。

（注）　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.3-17）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 12-38　[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。

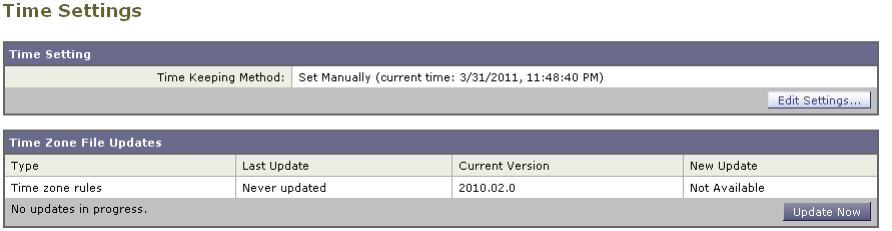
時間帯ファイルの更新

Security Management 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、Security Management 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。

GUI で時間帯ファイルを更新するには、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。

時間ベース ポリシーの時間範囲の定義

「営業時間」や「週末シフト」などの時間範囲を定義して、Web ベースのアクティビティを特定の日および時間に限定できます。たとえば、広帯域幅サイトまたは職務に関係のないサイトへの、業務時間内のアクセスをブロックできます。

詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Working with Time Based Policies」を参照してください。

時間範囲を追加または編集するには、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、[Web] > [Configuration Master] > [Defined Time Ranges] を選択します。

[Time Ranges] ページが表示されます。

ステップ 2　[Add Time Range] をクリックします。

[Add Time Range] ページが表示されます。

ステップ 3　[Time Range Name] テキスト フィールドに、時間範囲の名前を入力します。

ステップ 4　[Time Zone] 領域で、希望する時間帯に対応するオプション ボタンをクリックして選択します。選択肢は次のとおりです。

- Use Time Zone Setting from Appliance
- Specify Time Zone for this Time Range

対応するドロップダウン メニューから、地域、国、および時間帯を選択します。

ステップ 5　[Time Values] 領域で、定義した時間帯の曜日と時刻を選択します。

ステップ 6　[Add Row] をクリックします。

ステップ 7　[Submit] をクリックします。

コンフィギュレーション ファイルの管理

Cisco IronPort アプライアンス内の大部分の設定は、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。

- 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 Security Management アプライアンスから別の Security Management 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 Security Management 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 Email Security 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、Email Security アプライアンスから Security Management 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動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。

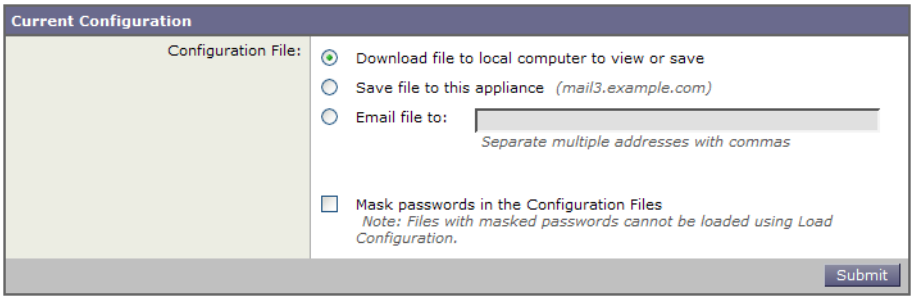
[Configuration File] ページには、次のセクションが含まれています。

- [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 12-39　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。

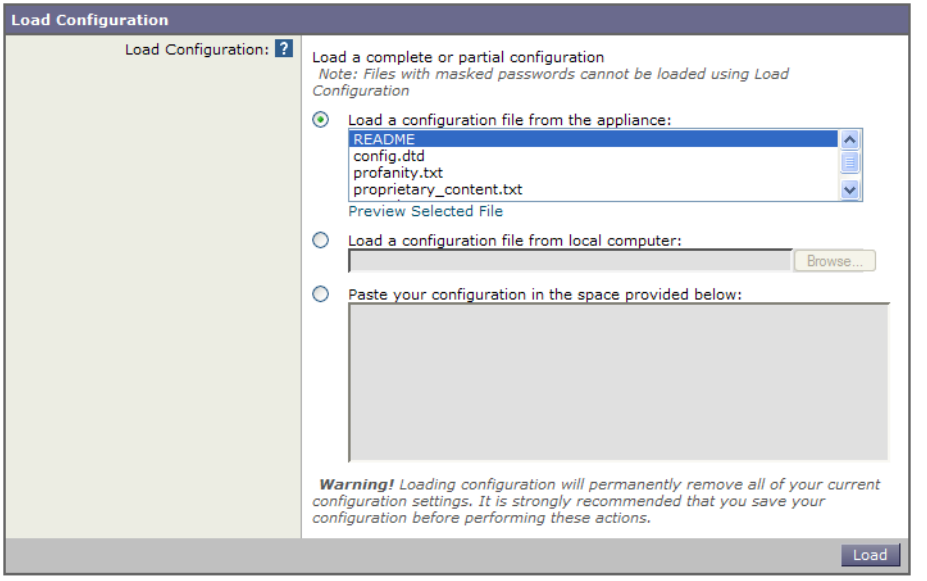
ステップ 1　`configuration` ディレクトリに情報を格納し、アップロードする

ステップ 2　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

ステップ 3　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 12-40　　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」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」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。

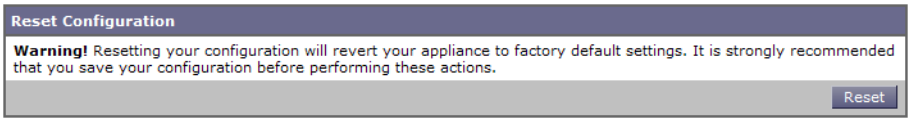
```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

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 12-41　コンフィギュレーション ファイルのリセット



「出荷時デフォルト値へのリセット」（P.12-6）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（「出荷時デフォルト値へのリセット」（P.12-6）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.12-116）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.
```

Security Management 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.12-113）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.2-33）の表 2-5 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、Security Management 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

有効なデータセットを「ソース」アプライアンスから「ターゲット」Security Management アプライアンスに、元の「ソース」Security Management 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、「Security Management アプライアンスのバックアップ」（P.12-8）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「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 ウィザードについて」（P.2-10）を参照してください）。これで、変更が確定されます。

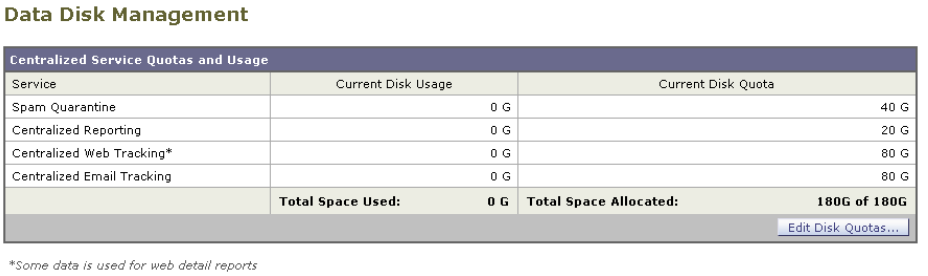
```
mail3.example.com> loadconfig


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、Security Management アプライアンスのモニタリング サービス（Cisco IronPort スパム検疫、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 12-42　[Disk Management] ページ



使用可能な最大ディスク領域

表 12-8 は、特定の Security Management 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 スパム検疫（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 12-8　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	M600	M650	M660	M670	M1000	M1050	M1060	M1070
レポーティング＋電子メール トラッキング＋ISQ＋Web トラッキング	180	186	186	450	700	405	405	800	1500
ISQ 最大値	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 ディスク上の検疫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 ドライブで ISQ 処理を行うと、マシンのロックアップが発生することがあります。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 クォータの編集

[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 スパム検疫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。

新しい割り当て量を変更し、現在の領域占有量よりも少なくなるようにした場合、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。

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で [Enable] チェックボックスをオンにしたが、この操作用に割り当てられたディスク領域がない場合は、ディスク領域が割り当てられるまで Web レポーティングが機能し

ません。この設定の編集の詳細については、「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）を参照してください。

モニタリング サービスのディスク クォータの再割り当て

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　Security Management 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。

そのサービスに対して、0 からディスク領域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 スパム検疫に 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確定します。