CHAPTER 15

システム管理

一般的なシステム管理は、主に Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）の [System Administration] メニューから実行します。一部のシステム管理機能は、Command Line Interface（CLI; コマンド ライン インターフェイス）のみからアクセスできます。

さらに、IronPort の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）から、IronPort アプライアンスのシステム モニタリング機能にアクセスすることもできます（Other Tasks in the GUI, page -441 を参照してください）。

（注） このセクションに記載されている機能またはコマンドには、ルーティングの優先順位に影響を与えるものや、影響を受けるものが含まれています。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-588）を参照してください。

この章は、次の内容で構成されています。

AsyncOS のアップグレード

アップグレードする前に

AsyncOS をアップグレードするには、次の 2 つの手順を実行します。

ステップ 1　**アップグレード設定値を設定します。**電子メール セキュリティ アプライアンスがアップグレード情報をダウンロードする方法に関する設定値を設定します。たとえば、アップグレード イメージのダウンロード元の選択などが含まれます。詳細については、「GUI からのアップグレード設定値の設定」（P.15-480）を参照してください。

ステップ 2　**AsyncOS をアップグレードします。**アップグレード設定値を設定した後は、アプライアンスの AsyncOS のバージョンをアップグレードします。詳細については、「GUI からの AsyncOS のアップグレード」（P.15-473）および「CLI からの AsyncOS のアップグレード」（P.15-474）を参照してください。

ベスト プラクティスとして、アップグレードの準備に次の手順を実行することを推奨します。

ステップ 1　XML コンフィグ ファイルのオフボックスを保存します。

ステップ 2　セーフリスト/ブロックリスト機能を使用している場合、リストのオフボックスをエクスポートします。

ステップ 3　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 からのアップグレードを実行する場合は、リスナーの停止が自動的に実行されます。

ステップ 4　メール キューと配信キューを排出します。

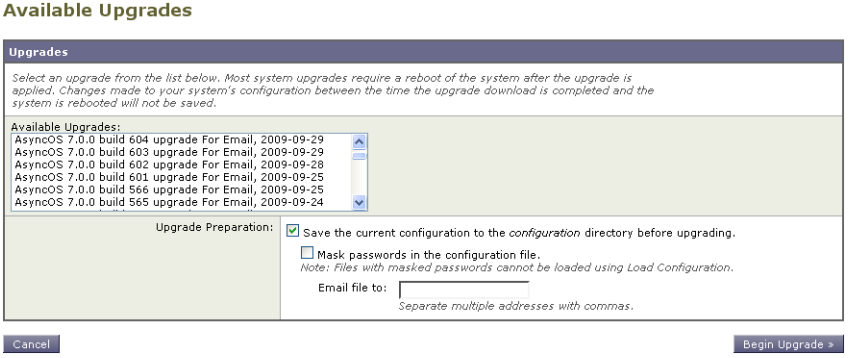
（注）　アップグレード後、再びリスナーをイネーブルにします。

GUI からの AsyncOS のアップグレード

アップデート設定値を設定した後に 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　[System Administration] > [System Upgrade] ページで、[Available Upgrades] をクリックします。[Available Upgrades] ページが表示されます。

図 15-1　[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　現在の設定を `configuration` ディレクトリに保存するかどうかを選択します。

ステップ 4　コンフィギュレーション ファイルでパスワードをマスクするかどうかを選択します。

（注）　マスクされたパスワードが記載されたコンフィギュレーション ファイルは、GUI の [Configuration File] ページや CLI の `loadconfig` コマンドからロードできません。

ステップ 5　コンフィギュレーション ファイルのコピーを電子メールで送信する場合は、ファイルの送信先の電子メール アドレスを入力します。複数の電子メール アドレスを指定する場合は、カンマで区切ります。

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

ステップ 7　アップグレードが完了すると、アプライアンスをリブートするように求められます。

ステップ 8　[Reboot Now] をクリックします。

CLI からの AsyncOS のアップグレード

`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。メッセージの確認やライセンス契約書への合意などを求められる場合があります。現在の設定を `configuration` ディレクトリに保存するかどうかを選択します。保存する場合、コンフィギュレーション ファイルでパスワードをマスクするかどうかを選択します。コンフィギュレーション ファイルのコピーを電子メールで送信するかどうかも選択します。

（注）　マスクされたパスワードが記載されたコンフィギュレーション ファイルは、`loadconfig` コマンドからロードできません。

アップグレード時には、さまざまなプロンプトで長い時間作業を中断しないでください。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。

従来のアップグレード方法との違い

従来の方法と比較して、ローカル サーバから AsyncOS をアップグレードする際は、次の違いがあることに注意してください。

ステップ 1　*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 プロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間に Ctrl キーを押した状態で C キーを押して、ダウンロードが開始する前にアップグレード プロセスを終了することもできます。

AsyncOS アップグレード設定値の設定

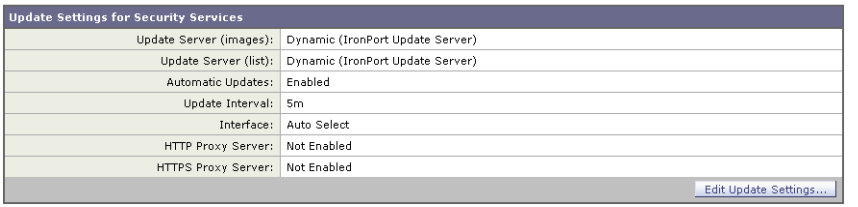
電子メール セキュリティ アプライアンスが AsyncOS アップグレードをダウンロードする方法を設定します。IronPort では、ストリーミング アップグレードとリモート アップグレードの 2 つの方法（または「ソース」）を用意しています。

ストリーミング アップグレードでは、IronPort アプライアンスは直接 IronPort アップデート サーバから AsyncOS アップグレードをダウンロードします。各 IronPort アプライアンスは、個別にアップグレードをダウンロードします。詳細については、「ストリーミング アップグレードの概要」（P.15-476）を参照してください。

リモート アップグレードでは、IronPort アプライアンスはネットワーク内のサーバから AsyncOS アップグレードをダウンロードします。アップグレード イメージを IronPort から一度だけダウンロードし、その後イメージを IronPort アプライアンスに供給します。詳細については、「リモート アップグレードの概要」（P.15-477）を参照してください。

[Security Services] > [Service Updates] ページを使用して、2 つのアップグレード方法を切り替えるとともに（デフォルトはストリーミング アップグレード）、アップグレードとプロキシ サーバ設定をダウンロードするために使用するインターフェイスを設定します。詳細については、「GUI からのアップグレード設定値の設定」（P.15-480）を参照してください。オプションで、CLI の `updateconfig` コマンドを使用することもできます。

図 15-2　[Service Updates] ページ



（注） 使用するアップグレード方法を問わず、アップグレードが完了した後に `saveconfig` コマンドで設定を保存することも検討してください。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Managing the Configuration File」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 Configuration Guide*』の「Centralized Management」の章の「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、IronPort アプライアンスは直接 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 15-3　　ストリーミング アップデートの方法

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、世界中のお客様が AsyncOS アップグレードをすぐにダウンロードできるようにしています。この分散サーバ アーキテクチャにより、IronPort 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。ファイアウォール ポリシーを厳しく設定している場合、AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。詳細については、「ストリーミング アップグレード用のスタティック アドレスの設定」（P.15-477）を参照してください。

ポート 80 および 443 による IronPort アップデート サーバからのアップグレードのダウンロードを許可する、ファイアウォールのルールを作成する必要があります。ポート 22、25、80、4766 などによる `upgrades.ironport.com` からのレガシー アップグレードのダウンロードを許可するファイアウォールのルールがすでに設定されている場合、そのルールを削除するか、修正したファイアウォールのルールで置き換えるか、もしくはこの両方の必要があります。詳細については、付録 C「ファイアウォール情報」を参照してください。

ストリーミング アップグレード用のスタティック アドレスの設定

McAfee Anti-Virus および IronPort AsyncOS アップデート サーバでは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、アップデートおよび AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。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、次の手順を実行します。

ステップ 1　IronPort カスタマー サポートに問い合わせて、スタティック URL アドレスを取得します。

ステップ 2　ポート 80 によるスタティック IP アドレスからのアップグレードのダウンロードを許可する、ファイアウォールのルールを作成します。

ステップ 3　[Security Services] > [Service Updates] ページに移動し、[Edit Update Settings] をクリックします。

ステップ 4　[Edit Update Settings] ページの [Update Servers (images)] セクションで、[Local Update Servers] を選択し、手順 1 で受け取った AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルのスタティック URL を [Base URL] フィールドに入力します。

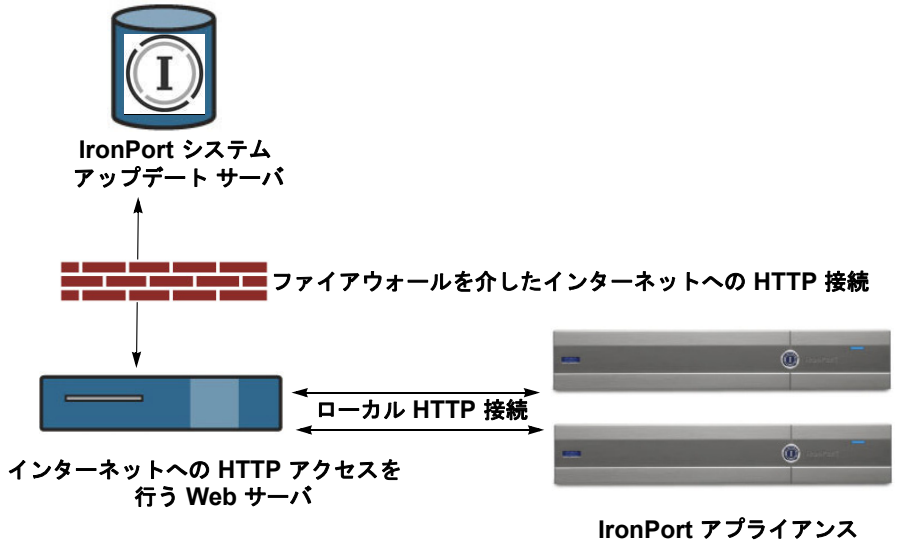
ステップ 5　IronPort アップデート サーバが [Update Servers (list)] セクションで選択されていることを確認します。

ステップ 6　変更を送信して確定します。

リモート アップグレードの概要

直接 IronPort アップデート サーバからアップグレードを取得するのではなく、AsyncOS アップグレード イメージをローカル サーバにダウンロードし、所有するネットワーク内からアップグレードをホスティングできます。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 でアップグレード イメージをダウンロードします。アップデート イメージのダウンロードを選択した場合、内部 HTTP サーバ（「アップデート マネージャ」）を設定して AsyncOS イメージを IronPort アプライアンスにホスティングできます。

図 15-4　リモート アップデートの方法



基本プロセスは次のとおりです。

ステップ 1　アップグレード ファイルを取得および供給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　GUI の [Security Services] > [Service Updates] ページまたは CLI の `updateconfig` コマンドのいずれかを使用して、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します。

ステップ 4　[System Administration] > [System Upgrade] ページまたは CLI の `upgrade` コマンドのいずれかを使用して、アプライアンスをアップグレードします。

リモート アップグレードに関するハードウェアおよびソフトウェア要件

AsyncOS アップグレード ファイルの*ダウンロード*では、次の要件を備えた内部ネットワークにシステムを構築する必要があります。

- 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（「ブラウザ要件」（P.2-18）を参照）。

（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 ファイルの*ホスティング*では、次の要件を備えた内部ネットワークにサーバを構築する必要があります。

- Web サーバ：たとえば、Microsoft Internet Information Services（IIS; インターネット インフォメーション サービス）または Apache オープン ソース サーバでは、次の要件を満たしている必要があります。
  - 24 文字を超えるディレクトリまたはファイル名の表示をサポートしていること
  - ディレクトリの参照ができること
  - 匿名認証（認証不要）または基本（「シンプル」）認証の設定ができること
  - 各 AsyncOS アップデート イメージ用に最低 350 MB 以上の空きディスク領域が存在すること

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、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。ダウンロードするアップグレードのバージョンをクリックし、ディレクトリ構造を変更せずにローカル サーバのルート ディレクトリにある ZIP ファイルを解凍します。アップグレード イメージを使用するには、[Edit Update Settings] ページで（または CLI の `updateconfig` を使用して）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します。

ローカル サーバは、ネットワーク上の IronPort アプライアンスで利用可能な AsyncOS アップグレードをダウンロード済みのアップグレード イメージに限定する XML ファイルもホスティングします。このファイルは「マニフェスト」と呼ばれます。マニフェストはアップグレード イメージの ZIP ファイルの `asyncos` ディレクトリに配置されています。ローカル サーバのルート ディレク

トリにある ZIP ファイルを解凍したら、[Edit Update Settings] ページで（または CLI の `updateconfig` を使用して）、XML ファイルの完全な URL（ファイル名を含む）を入力します。

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

（注）　ローカル アップデート サーバは AsyncOS アップグレード イメージ専用に使用し、セキュリティ アップデート イメージには使用しないでください。ローカル アップデート サーバを指定した場合、ローカル サーバは IronPort からアップデートされたセキュリティ アップデートを自動的には受信しないため、ネットワーク上のアプライアンスはいずれ古くなります。AsyncOS のアップグレード用にローカル アップデート サーバを使用して、アップデートおよびアップグレード用の設定値を再び IronPort アップデート サーバを使用するように変更してください。セキュリティ サービスが再び自動的にアップデートされるようになります。

GUI からのアップグレード設定値の設定

アップデート設定には、AsyncOS アップグレードのソース（リモートまたはストリーミング）、アップグレードのダウンロードに使用するインターフェイス、およびプロキシ サーバ設定が含まれています。AsyncOS のアップグレードに加えて、アンチスパム サービス、アンチウイルス サービス、およびウイルス感染フィルタ サービスなどさまざまな IronPort サービスの設定値も編集できます。アップデート サービスの詳細については、「サービスのアップデート」（P.15-486）を参照してください。

AsyncOS 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　[Security Services] > [Service Updates] ページで、[Edit Update Settings] をクリックします。

[Edit Update Settings] ページが表示されます。

ステップ 2　AsyncOS アップグレード イメージを IronPort アップデート サーバからダウンロードするか、またはローカル サーバからダウンロードするかを選択します。

ローカル サーバを選択した場合、AsyncOS アップグレード イメージをホスティングするローカル サーバのベース URL 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。

（注）　AsyncOS アップグレードにローカル サーバを指定した場合、ローカル サーバは IronPort からアップデートされた McAfee Anti-Virus 定義ファイルを自動的には受信しないため、ネットワーク上のアプライアンスはいずれ古くなります。アップグレード後に設定値を再び IronPort アップデート サーバを使用するように変更してください。McAfee Anti-Virus 定義ファイルが再び自動的にアップデートされるようになります。

ステップ 3　ローカル サーバからの AsyncOS アップグレード イメージのダウンロードを選択した場合は、利用可能なアップデートのリスト（マニフェスト XML ファイル）のソースとするローカル サーバを選択します。マニフェストの完全な URL（ファイル名と HTTP ポート番号を含む）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。

ステップ 4　アップグレードに使用するインターフェイスを選択します。

ステップ 5　必要に応じて、HTTP プロキシ サーバまたは HTTPS プロキシ サーバの情報を入力します。

ステップ 6　変更を送信して確定します。

CLI からのアップグレード設定値の設定

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 IronPort サーバ）をアプライアンスに設定するには、`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、`upgradeconfig` コマンドは AsyncOS にアップグレードを取得するために使用されていました。このコマンドは、AsyncOS 6.5 では使用されていません。

updateconfig コマンド

`updateconfig` コマンドは、AsyncOS アップグレードを含むサービス アップデートを参照する場所を IronPort アプライアンスに設定するために使用されます。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 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。

（注）　ping コマンドを使用して、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。

AsyncOS の復元

AsyncOS には、緊急時に AsyncOS オペレーティング システムを以前の認定済みのビルドに戻す機能があります。

（注）　AsyncOS 7.0 にアップグレードした後は、バージョン 6.5 よりも前の AsyncOS には戻せません。

利用可能なバージョン

アップグレードは主要なサブシステムを一方向に変換するため、復元プロセスは複雑で、IronPort Quality Assurance チームによる認定が必要です。IronPort では、AsyncOS バージョンに対して固有のバージョンの CASE、Sophos、ウイルス感染フィルタを認証しています。以前のすべてのバージョンの AsyncOS オペレーティング システムが復元に利用できるわけではありません。最初にこの機能がサポートされた AsyncOS バージョンは AsyncOS 5.5.0 です。これより以前のバージョンの AsyncOS はサポートされていません。

復元の影響に関する重要な注意事項

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。このコマンドはすべての設定ログおよびデータベースを破壊します。管理インターフェイスのネットワーク情報のみが保存されます。他のすべてのネットワーク設定は削除されます。さらに、復元はアプライアンスが再設定さ

れるまでメール処理を中断します。このコマンドはネットワーク設定を破壊するため、revert コマンドを発行する場合は IronPort アプライアンスへの物理的なローカル アクセスが必要になります。

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 ファイルに下位互換性は*ありません*。

AsyncOS 復元の実行

revert コマンドを実行するには、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 ファイルに下位互換性はありません。コンフィギュレーション ファイルを取得するには、ファイルを電子メールでユーザ自身に送信するか、ファイルを FTP で取得します。簡単な方法は、CLI の mailconfig コマンドを実行する方法です。

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。

（注）　このコピーは、バージョンを戻した後にロードする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　メール キューが空になるまで待ちます。

ステップ 5　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 コマンドの実行時には、いくつかの警告プロンプトが発行されます。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、復元に向けた準備手順が完了するまで、復元プロセスを開始しないでください。

ステップ 6　CLI から revert コマンドを発行します。

（注）　復元プロセスは時間のかかる処理です。復元が完了して、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。

次に、revert コマンドの例を示します。

```
mail.mydomain.com> 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 IronPort Spam Quarantine message and end-user
safelist/blocklist data



Only the network settings for the Management interface will be
preserved.
```

```
Before running this command, be sure you have:

- saved the configuration file of this appliance (with passwords

unmasked)

- exported the 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?

Are you *really* sure you want to continue? yes


 Available version                Install date

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

 Available version                Install date

1. 5.5.0-236                       Tue Aug 28 11:03:44 PDT 2007

2. 5.5.0-330                       Tue Aug 28 13:06:05 PDT 2007

3. 5.5.0-418                       Wed Sep  5 11:17:08 PDT 2007


Please select an AsyncOS version: 2
```

```
You have selected "5.5.0-330".

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

ステップ 7　アプライアンスは 2 回リブートします。

ステップ 8　マシンが 2 回リブートしたら、シリアル コンソールで `interfaceconfig` コマンドを使用して、アクセス可能な IP アドレスをインターフェイスに設定します。

ステップ 9　設定したインターフェイスの 1 つで FTP または HTTP をイネーブルにします。

ステップ 10　作成した XML コンフィギュレーション ファイルを FTP で取得するか、または GUI インターフェイスに貼り付けます。

ステップ 11　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 12　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 13　変更を確定します。

復元が完了した 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。

サービスのアップデート

IronPort アプライアンスがさまざまなサービス（アンチスパム、アンチウイルス、ウイルス感染フィルタ サービスなど）をアップデートする方法の設定には、多くの設定値が使用されています。これらの設定値には、[Security Services] メニューの [Service Updates] ページ、または CLI の `updateconfig` コマンドからアクセスできます。

[Service Updates] ページまたは `updateconfig` コマンドを使用して、IronPort AsyncOS のアップグレードも実行できます。詳細については、「AsyncOS のアップグレード」（P.15-472）を参照してください。

[Service Updates] ページ

[Service Updates] ページ（GUI の [Security Services] メニューから利用可能）では、IronPort アプライアンスのさまざまなサービスのアップデートに関する現在の設定値を表示します。アップデート設定には、アップデート サーバ（イメージ）、アップデート サーバ（リスト）、さまざまなコンポーネントのアップデート URL、自動アップデートのイネーブル化、自動アップデート間隔、HTTP プロキシ サーバおよび HTTPS プロキシ サーバが含まれます。

（注）　McAfee Anti-Virus および IronPort AsyncOS アップデート サーバでは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、McAfee Anti-Virus アップデートおよび AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。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、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。

アップデート設定値の編集

IronPort アプライアンスのアップデート設定値を編集するには、[Edit Update Settings] ボタンをクリックします。[Update Servers (images)]、[Update Servers (list)]、[Automatic Updates]、[Interface]、および [Proxy Servers] の設定値を設定します。アップデート設定値の詳細については、表 15-1（P.15-490）を参照してください。

図 15-5 は、アップデート サーバの利用可能な設定値を示しています。

図 15-5　イメージおよびリストに関するアップデート サーバの設定値

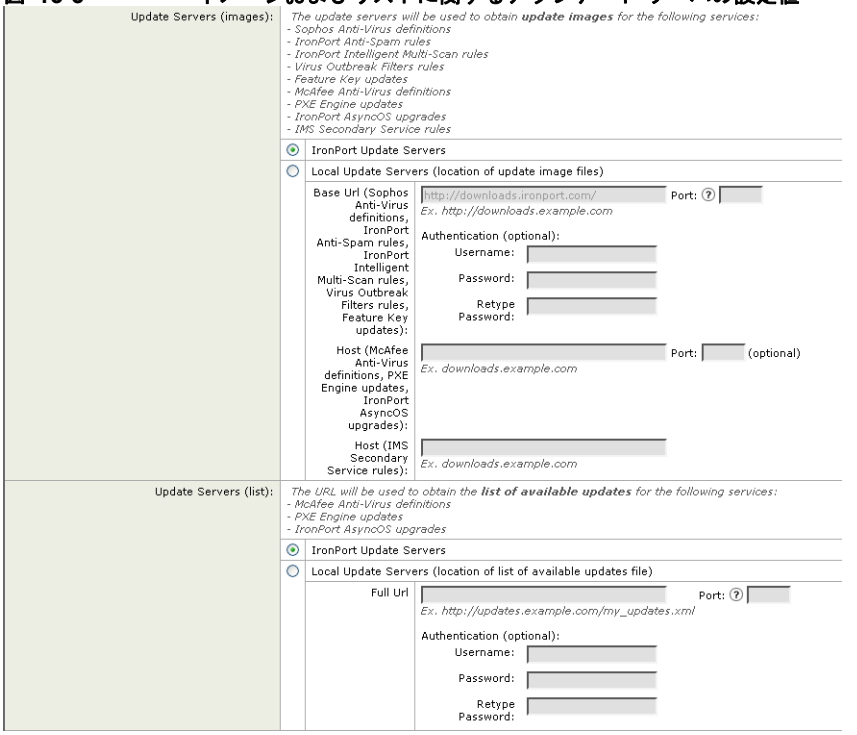


図 15-6 は、[Automatic Updates] および [Interface] で利用可能な設定値を示しています。

図 15-6　[Automatic Updates] および [Interfaces] の設定値

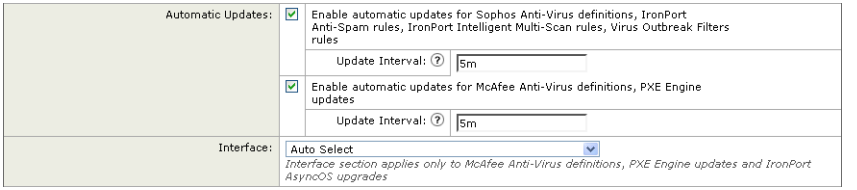


図 15-7 は、プロキシ サーバの利用可能な設定値を示しています。

図 15-7　プロキシ サーバの設定値

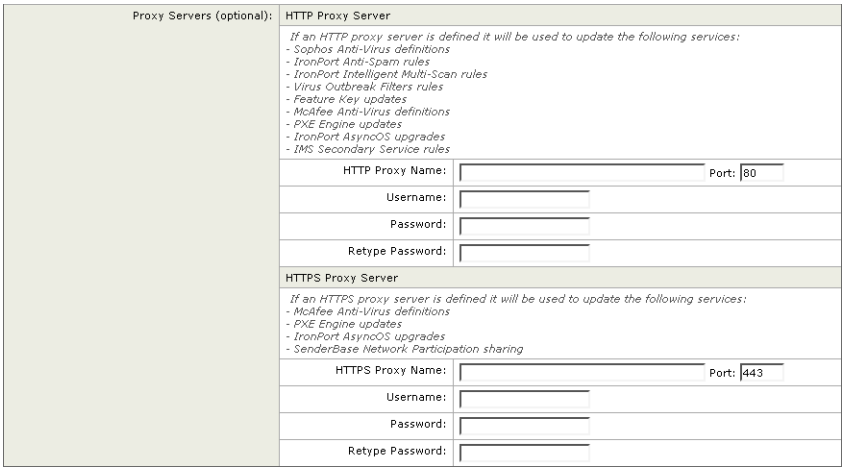


表 15-1　アップデート設定値

設定	説明
[Update Servers (images)]	サービス アップデート イメージおよび IronPort AsyncOS アップグレード イメージを IronPort アップデート サーバからダウンロードするか、またはローカル Web サーバからダウンロードするかを選択します。 デフォルトは、IronPort アップデート サーバです。これらのサーバは AsyncOS アップグレードの他にも、Sophos および McAfee Anti-Virus 定義ファイル、IronPort Anti-Spam および IronPort Intelligent Multi-Scan ルール、ウイルス感染フィルタ ルール、機能キーのアップデート、および PXE Engine のアップデートに関するアップデート イメージの取得に使用されます。 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。 • IronPort からアップグレード イメージおよびアップデート イメージをダウンロードする際に、IronPort カスタマー サポートから提供されるスタティック アドレスを入力する必要がある場合。 • 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は、セキュリティ コンポーネントが引き続き自動アップデートできるように、この設定を再び IronPort アップデート サーバ（または使用していたスタティック アドレス）に戻すことを推奨します。 ローカル アップデート サーバを選択した場合は、アップグレードおよびアップデートのダウンロードに使用するサーバのベース 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。 **（注）** IronPort Intelligent Multi-Scan でサードパーティのアンチスパム ルールのアップデートをダウンロードするには、別のローカル サーバが必要です。

表 15-1　アップデート設定値（続き）

設定	説明
[Update Servers (lists)]	利用可能なアップデートのリスト（マニフェスト XML ファイル）を IronPort アップデート サーバからダウンロードするか、またはローカル Web サーバからダウンロードするかを選択します。マニフェスト XML ファイルには、AsyncOS アップグレードの他に McAfee Anti-Virus および PXE Engine のアップデートが含まれます。 デフォルトは、IronPort アップデート サーバです。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は、ローカル Web サーバを選択します。イメージをダウンロードした後は、セキュリティ コンポーネントが引き続き自動アップデートできるように、この設定を再び IronPort アップデート サーバに戻すことを推奨します。 ローカル アップデート サーバを選択した場合、サーバのファイル名およびポート番号を含む、リストのマニフェスト XML ファイルの完全なパスを入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。 詳細については、「リモート アップグレードの概要」（P.15-477）を参照してください。
[Automatic Updates]	Sophos および McAfee Anti-Virus 定義ファイル、IronPort Anti-Spam ルール、IronPort Intelligent Multi-Scan ルール、PXE Engine アップデート、およびウイルス感染フィルタ ルールに対する自動アップデートとポーリング間隔（アプライアンスがアップデートを確認する頻度）をイネーブルにします。

表 15-1　アップデート設定値（続き）

設定	説明
[Routing Table]	アップデート サーバに McAfee Anti-Virus 定義ファイル、PXE Engine アップデートおよび IronPort AsyncOS アップグレードを問い合わせる際に使用するネットワーク インターフェイスを選択します。利用可能なプロキシ 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、アプライアンスは使用するインターフェイスを選択します。
[HTTP Proxy Server]	IronPort AsyncOS アップグレード、PXE Engine アップデート、Sophos および McAfee Anti-Virus 定義ファイル、IronPort Anti-Spam ルール、IronPort Intelligent Multi-Scan ルール、ウイルス感染フィルタ ルール、Virus Threat Level、および SenderBase Network Participation 共有で使用するオプションのプロキシ サーバ。プロキシ サーバを指定すると、これらのすべてのサービスで指定したプロキシ サーバが使用されることに注意してください。
[HTTPS Proxy Server]	HTTPS を使用したオプションのプロキシ サーバ。HTTPS プロキシ サーバを定義すると、IronPort AsyncOS アップグレード、SenderBase Network Participation 共有、PXE Engine アップデート、および McAfee Anti-Virus 定義ファイルのアップデートで使用されます。

アップデート サーバの設定

IronPort アプライアンスのアップデート サーバを設定するには、次の手順を実行します。

ステップ 1　IronPort アップデート サーバまたはローカル アップデート サーバのいずれかから、サービスのアップデート イメージを取得するサーバを選択します。

（注）　アップグレードのソースとしてローカル サーバを選択した場合、McAfee Anti-Virus 定義ファイルの自動アップデートは停止します。McAfee Anti-Virus 定義ファイルのアップデートを継続するには、アップデート イメージまたはアップデートのリストをローカル サーバでホスティングします。

ステップ 2　アップデート イメージの取得先にローカル アップデート サーバを選択した場合、最初に AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルを除く、すべてのサービス アップデートをホスティングするローカル サーバのベース URL、ポート番号、およびオプションの認証情報を入力します。次に、AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルをホスティングするローカル サーバのベース URL を入力します。

ステップ 3　IronPort アップデート サーバまたはローカル アップデート サーバのいずれかから、利用可能な IronPort AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルのリストを取得するサーバを選択します。

ステップ 4　利用可能なアップグレードのリストの取得先にローカル アップデート サーバを選択した場合、ファイル名、HTTP ポート番号およびオプションの認証情報を含む、リストの XML ファイルへの完全なパスを入力します。

自動アップデートの設定

自動アップデートをイネーブルにし、アップデート間隔を設定するには、次の手順を実行します。

ステップ 1　チェックボックスをオンにして、自動アップデートをイネーブルにします。

ステップ 2　アップデート間隔（次のアップデートの確認までに待機する時間）を入力します。数字の後に **m**（分）、**h**（時）、**d**（日）を追加します。

HTTP プロキシ サーバの指定（任意）

HTTP プロキシ サーバを指定するには、次の手順を実行します。

ステップ 1　サーバの URL とポート番号を入力します。

ステップ 2　必要に応じて、サーバのアカウントのユーザ名とパスワードを入力します。

ステップ 3　変更を送信して確定します。

HTTPS プロキシ サーバの指定（任意）

HTTPS プロキシ サーバを指定するには、次の手順を実行します。

ステップ 1　サーバの URL とポート番号を入力します。

ステップ 2　必要に応じて、サーバのアカウントのユーザ名とパスワードを入力します。

ステップ 3　変更を送信して確定します。

生成されるさまざまなメッセージに対する返信アドレスの設定

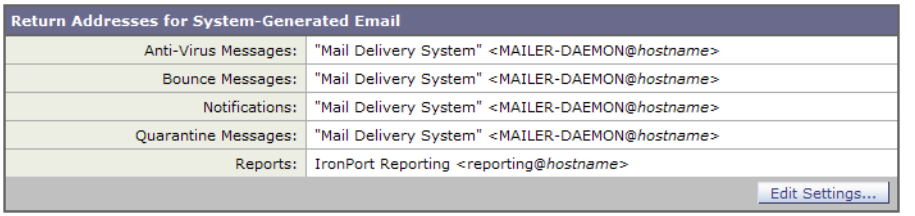
AsyncOS によって、次のタイミングで生成されるメールのエンベロープ送信者を設定できます。

- Anti-Virus 通知
- バウンス
- 通知（`notify()` および `notify-copy()` フィルタの動作）
- 検疫通知（および検疫管理機能における「コピー送信」）
- 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 で [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 15-8　[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 から変更するには、[Return Addresses] ページで [Edit Settings] をクリックします。1 つ以上のアドレスを変更して、[Submit] をクリックし、最後に変更を確定します。

アラート

アラートとは、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、IronPort アプライアンスで生成されます。送信するアラート メッセージの種類、重大度、および送信するユーザを非常に詳細なレベルで指定できます。アラートは、GUI の [System Administration] > [Alerts] ページ（または CLI の `alertconfig` コマンド）で管理します。

アラートの概要

アラート機能は 2 つの主要な部分から構成されます。

- [Alerts]：**アラート受信者**（アラートを受信する電子メール アドレス）、および受信者に送信されるアラート通知（重大度およびアラート タイプ）。
- [Alert Settings]：アラート送信者（[FROM:]）アドレス、次に重複したアラートを送信するまでに待機する秒数、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毎週 AutoSupport レポートを送信するかどうか）などのアラート機能に関する全般的な動作を指定します。

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、アラート受信者に送信される、ハードウェアやアンチウイルスの問題など特定の機能（またはアラート分類）に関する情報が記載された電子メール メッセージまたは通知のことです。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、アラート分類と重大度によって決まります。アラート受信者に送信するアラート分類と重大度を指定できます。アラート エンジンでは、送信するアラートの種類とアラート受信者を詳細に制御できます。たとえば、アラート受信者が System（アラートの種類）に関する Critical（重大度）の情報が送信されたときのみ通知を受信するように設定することで、アラート受信者に特定のアラートのみを送信するように設定できます。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.15-503）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.15-505）を参照してください。

アラート分類

AsyncOS では、次のアラート分類を送信します。

- System
- Hardware
- Updater
- Virus Outbreak Filters
- Anti-Virus
- Anti-Spam
- Directory Harvest Attack Prevention

重大度

アラートは、次の重大度に従って送信されます。

- [Critical]：すぐに対処が必要です。
- [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。
- [Information]：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 System 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 の毎週のステータス 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。増加する秒数は、前回の待機間隔の 2 倍の値を足した秒数です。つまり、この値を 5 秒に設定すると、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、送信間隔は非常に大きな秒数になります。[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。

SMTP ルートおよびアラート

アプライアンスから [Alert Recipient] 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。

IronPort AutoSupport

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 IronPort Systems に送信するように IronPort アプライアンスを設定できます。この機能は AutoSupport と呼ばれ、シスコ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、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.15-503）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

[Edit Settings] ボタンまたは CLI（『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照）を使用して、Header From: アドレスを設定できます。

アラートの件名

アラートの電子メール メッセージの件名は、次の形式に従っています。

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

アラートの配信

アラート メッセージは 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 以前の AsyncOS バージョンでは、アラート メッセージは `smtproutes` を使用しません。
  - 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。

アラート メッセージの例

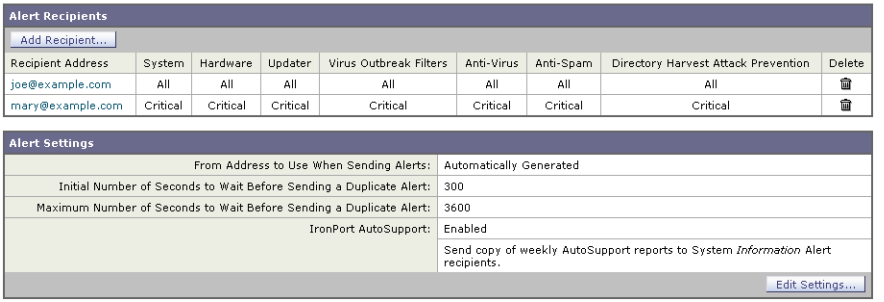
```
Date: 23 Mar 2005 21:10:19 +0000

To: joe@example.com

From: IronPort C60 Alert [alert@example.com]

Subject: Critical-example.com: (Anti-Virus) update via
http://newproxy.example.com failed



The Critical message is:



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



Version: 4.5.0-419

Serial Number: XXXXXXXXXXXX-XXXXXXX

Timestamp: Tue May 10 09:39:24 2005



For more information about this error, please see

    http://support.ironport.com

If you desire further information, please contact your support
provider.
```

アラート受信者の管理

Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）にログインして、[System Administration] タブをクリックします（GUI へのアクセス方法については、「GUI へのアクセス」（P.2-19）を参照してください）。左のメニューにある [Alerts] リンクをクリックします。

図 15-9　[Alerts] ページ

Alerts



（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 アドレスにすべての重大度およびクラスのアラートを受信します（デフォルト）。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。

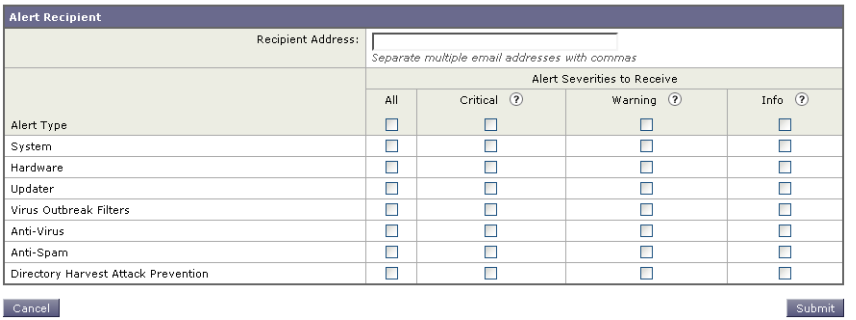
- アラート受信者の追加、設定、または削除
- アラート設定値の変更

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 15-10　新規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　受信するアラートの重大度を選択します。

ステップ 4　変更を送信して確定します。

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　変更を送信して確定します。

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、削除を確定します。

ステップ 3　変更を確定します。

アラート設定値の設定

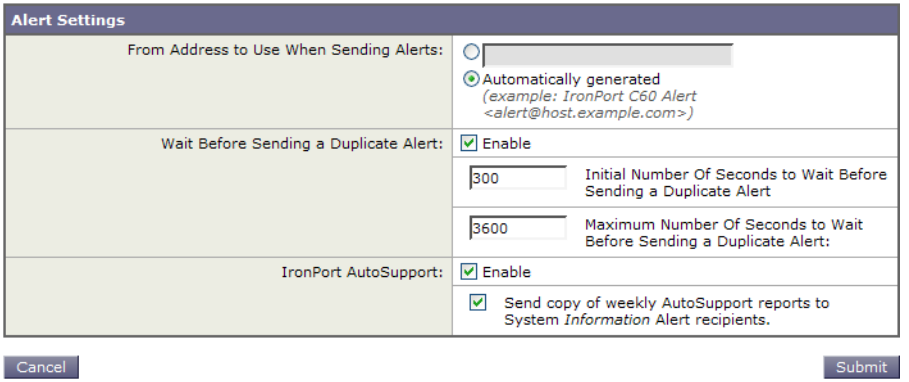
アラート設定はグローバルな設定であるため、すべてのアラートの動作に影響します。

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 15-11　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.15-497）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　[IronPort AutoSupport] オプションをオンにすることで、AutoSupport をイネーブルにできます。AutoSupport の詳細については、「IronPort AutoSupport」（P.15-498）を参照してください。

- AutoSupport がイネーブルの場合、Information レベルの System 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、毎週 AutoSupport レポートが送信されます。チェックボックスを外すことでディセーブルにできます。

ステップ 5　変更を送信して確定します。

アラート リスト

次の表に、分類したアラートのリストを示します。表には、アラート名（IronPort で使用される内部記述子）、アラートの実際のテキスト、説明、重大度（critical、information、または warning）およびメッセージのテキストに含まれるパラメータ（存在する場合）が含まれています。アラートの実際のテキストでは、パラメータ値は置き換えられます。たとえば、次のアラート メッセージではメッセージのテキストに 「$ip」が記述されています。アラート生成時に「$ip」は実際の IP アドレスに置き換えられます。

アンチスパム アラート

表 15-2 に、AsyncOS で生成される可能性があるさまざまなアンチスパムに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-2　発生する可能性があるアンチスパム アラートのリスト

アラート名	メッセージと説明	パラメータ
AS.SERVER.ALERT	$engine anti-spam - $message $tb	「**engine**」：アンチスパム エンジンのタイプ。 「**message**」：ログ メッセージ。 「**tb**」：イベントのトレースバック。
	Critical。アンチスパム エンジンに障害が発生した場合に送信されます。	
AS.UPDATE_ENOSPC	Anti-Spam Update: Out of disk space.	
	Critical。ディスク領域不足により、アンチスパム エンジンに障害が発生した場合に送信されます。	
AS.TOOL.INFO_ALERT	Update - $engine - $message	「**engine**」：アンチスパム エンジンの名前。 「**message**」：メッセージ。
	Information。アンチスパム エンジンに問題が発生した場合に送信されます。	
AS.TOOL.ALERT	Update - $engine - $message	「**engine**」：アンチスパム エンジンの名前。 「**message**」：メッセージ。
	Critical。アンチスパム エンジンの管理に使用されるツールの 1 つに問題があり、アップデートが中止される場合に送信されます。	

表 15-2　発生する可能性があるアンチスパム アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
AS.UPDATE.ALERT	Update - $engine - $message	「**engine**」：アンチスパム エンジンの名前。 「**message**」：メッセージ。
	Critical。アンチスパム エンジンのアップデート時にエラーが発生した場合に送信されます。	
AS.UPDATE_FAILURE	$engine update unsuccessful.This may be due to transient network or DNS issues, HTTP proxy configuration causing update transmission errors or unavailability of downloads.ironport.com.The specific error on the appliance for this failure is: $error	「**engine**」：アップデートに失敗したエンジン。 「**error**」：発生したエラー。
	Warning。アンチスパム エンジンまたは CASE ルールのアップデートに失敗した場合に送信されます。	

アンチウイルス アラート

表 15-3 に、AsyncOS で生成される可能性があるさまざまなアンチウイルスに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-3　発生する可能性があるアンチウイルス アラートのリスト

アラート名	メッセージと説明	パラメータ
AV.SERVER.ALERT/ AV.SERVER.CRITICAL	$engine antivirus - $message $tb	「**engine**」：アンチウイルス エンジンのタイプ。 「**message**」：ログ メッセージ。 「**tb**」：イベントのトレースバック。
	Critical。アンチウイルス スキャン エンジンに重大な問題が発生した場合に送信されます。	
AV.SERVER.ALERT.INFO	$engine antivirus - $message $tb	「**engine**」：アンチウイルス エンジンのタイプ。 「**message**」：ログ メッセージ。 「**tb**」：イベントのトレースバック。
	Information。アンチウイルス スキャン エンジンに情報イベントが発生した場合に送信されます。	

表 15-3　発生する可能性があるアンチウイルス アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
AV.SERVER.ALERT.WARN	$engine antivirus - $message $tb	「**engine**」：アンチウイルス エンジンのタイプ。 「**message**」：ログ メッセージ。 「**tb**」：イベントのトレースバック。
	Warning。アンチウイルス スキャン エンジンに問題が発生した場合に送信されます。	
AV.UPDATE.ALERT.INFO	$message	「**message**」：ログ メッセージ。
	Information。アンチウイルスのアップデート時に情報イベントが発生した場合に送信されます。	
AV.UPDATE.ALERT.WARN	$message	「**message**」：ログ メッセージ。
	Warning。アンチウイルスのアップデート時に問題が発生した場合に送信されます。	
AV.UPDATE.ALERT	$message	「**message**」：ログ メッセージ。
	Critical。アンチウイルスのアップデート時に重大な問題が発生した場合に送信されます。	
AV.UPDATE_ENOSPC	Anti-Virus Update: Out of disk space.	
	Critical。ディスク領域不足により、アンチウイルス エンジンがアップデートできない場合に送信されます。	
MAIL.ANTIVIRUS. ERROR_MESSAGE	MID $mid antivirus $what error $tag	「**mid**」：MID 「**what**」：発生したエラー。 「**tag**」：ウイルス発生名（設定されている場合）。
	Critical。メッセージのスキャン中に、アンチウイルス スキャンがエラーを生成した場合に送信されます。	

表 15-3　発生する可能性があるアンチウイルス アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
MAIL.SCANNER. PROTOCOL_MAX_RETRY	MID $mid is malformed and cannot be scanned by $engine.	「**mid**」：MID 「**engine**」：使用されているエンジン。
	Critical。メッセージが不正なため、スキャン エンジンはメッセージのスキャンに失敗しました。再試行の最大回数を超過したため、メッセージはエンジンにスキャンされずに処理されます。	

ディレクトリ獲得攻撃（DHAP）アラート

表 15-4 に、AsyncOS で生成される可能性があるさまざまな DHAP に関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-4　発生する可能性があるディレクトリ獲得攻撃アラートのリスト

アラート名	メッセージと説明	パラメータ
LDAP.DHAP_ALERT	LDAP: Potential Directory Harvest Attack detected.See the system mail logs for more information about this attack.	
	Warning。ディレクトリ獲得攻撃の可能性を検出した場合に送信されます。	

ハードウェア アラート

表 15-5 に、AsyncOS で生成される可能性があるさまざまなハードウェア アラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-5　発生する可能性があるハードウェア アラートのリスト

アラート名	メッセージと説明	パラメータ
INTERFACE.ERRORS	Port $port: has detected $in_err input errors, $out_err output errors, $col collisions please check your media settings. Warning。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。	「**port**」：インターフェイス名。 「**in_err**」：最後のメッセージからの入力エラー数。 「**out_err**」：最後のメッセージからの出力エラー数。 「**col**」：最後のメッセージからのパケット衝突数。
MAIL.MEASUREMENTS_FILESYSTEM	The $file_system partition is at $capacity% capacity Warning。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。	「**file_system**」：ファイル システムの名前。 「**capacity**」：ファイル システムの使用率（%）。
MAIL.MEASUREMENTS_FILESYSTEM.CRITICAL	The $file_system partition is at $capacity% capacity 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。	「**file_system**」：ファイル システムの名前。 「**capacity**」：ファイル システムの使用率（%）。
SYSTEM.RAID_EVENT_ALERT	A RAID-event has occurred: $error Warning。重大な RAID-event が発生した場合に送信されます。	「**error**」：RAID エラーのテキスト。
SYSTEM.RAID_EVENT_ALERT_INFO	A RAID-event has occurred: $error Information。RAID-event が発生した場合に送信されます。	「**error**」：RAID エラーのテキスト。

IronPort スパム検疫アラート

表 15-6 に、AsyncOS で生成される可能性があるさまざまな IronPort スパム検疫に関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-6　発生する可能性がある IronPort スパム検疫アラートのリスト

アラート名	メッセージと説明	パラメータ
ISQ.CANNOT_CONNECT_OFF_BOX	ISQ: Could not connect to off-box quarantine at $host:$port Information。AsyncOS が（オフボックス）IP アドレスに接続できない場合に送信されます。	「**host**」：オフボックス検疫のアドレス。 「**port**」：オフボックス検疫に接続するポート。
ISQ.CRITICAL	ISQ: $msg Critical。IronPort スパム検疫に重大なエラーが発生した場合に送信されます。	「**msg**」：表示されるメッセージ
ISQ.DB_APPROACHING_FULL	ISQ: Database over $threshold% full Warning。IronPort スパム検疫データベースがフルに近い場合に送信されます。	「**threshold**」：アラートを開始する使用率のしきい値
ISQ.DB_FULL	ISQ: database is full Critical。IronPort スパム検疫データベースがフルになった場合に送信されます。	
ISQ.MSG_DEL_FAILED	ISQ: Failed to delete MID $mid for $rcpt: $reason Warning。IronPort スパム検疫からの電子メールの削除に失敗した場合に送信されます。	「**mid**」：MID 「**rcpt**」：受信者または "all"（全員） 「**reason**」：メッセージが削除されない理由

表 15-6　発生する可能性がある IronPort スパム検疫アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
ISQ.MSG_NOTIFICATION_FAILED	ISQ: Failed to send notification message: $reason	「**reason**」：通知が送信されない理由
	Warning。通知メッセージの送信に失敗した場合に送信されます。	
ISQ.MSG_QUAR_FAILED		
	Warning。メッセージの検疫に失敗した場合に送信されます。	
ISQ.MSG_RLS_FAILED	ISQ: Failed to release MID $mid to $rcpt: $reason	「**mid**」：MID 「**rcpt**」：受信者または "all"（全員） 「**reason**」：メッセージが開放されない理由
	Warning。メッセージの開放に失敗した場合に送信されます。	
ISQ.MSG_RLS_FAILED_UNK_RCPTS	ISQ: Failed to release MID $mid: $reason	「**mid**」：MID 「**reason**」：メッセージが開放されない理由
	Warning。受信者が不明のため、メッセージの開放に失敗した場合に送信されます。	
ISQ.NO_EU_PROPS	ISQ: Could not retrieve $user's properties.Setting defaults	「**user**」：エンドユーザ名
	Information。AsyncOS がユーザの情報を取得できない場合に送信されます。	
ISQ.NO_OFF_BOX_HOST_SET	ISQ: Setting up off-box ISQ without setting host	
	Information。AsyncOS が外部検疫を参照するように設定されているものの、外部検疫が定義されていない場合に送信されます。	

セーフリスト/ブロックリスト アラート

次の表に、AsyncOS で生成される可能性があるさまざまな セーフリスト/ブロックリスト に関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-7　発生する可能性があるセーフリスト/ブロックリスト アラートのリスト

アラート名	メッセージと説明	パラメータ
SLBL.DB.RECOVERY_FAILED	SLBL: Failed to recover End-User Safelist/Blocklist database: '$error'. Critical。セーフリスト/ブロックリスト データベースの復旧に失敗しました。	「**error**」：エラーの理由
SLBL.DB.SPACE_LIMIT	SLBL: End-User Safelist/Blocklist database exceeded allowed disk space: $current of $limit. Critical。セーフリスト/ブロックリスト データベースが許容されたディスク領域を超過しました。	「**current**」：データベース使用量（MB） 「**limit**」：設定された制限使用量（MB）

システム アラート

表 15-8 に、AsyncOS で生成される可能性があるさまざまなシステム アラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-8　発生する可能性があるシステム アラートのリスト

アラート名	メッセージと説明	パラメータ
COMMON.APP_FAILURE	An application fault occurred: $error Warning。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。	「**error**」：エラーのテキスト（通常はトレースバック）

表 15-8　発生する可能性があるシステム アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
COMMON.KEY_EXPIRED_ALERT	Your "$feature" key has expired.Please contact your authorized IronPort sales representative.	「**feature**」：有効期限が切れる機能の名前。
	Warning。機能キーの有効期限が切れた場合に送信されます。	
COMMON.KEY_EXPIRING_ALERT	Your "$feature" key will expire in under $days day(s).Please contact your authorized IronPort sales representative.	「**feature**」：有効期限が切れる機能の名前。 「**days**」：有効期限が切れるまでの日数。
	Warning。機能キーの有効期限が切れる場合に送信されます。	
COMMON.KEY_FINAL_EXPIRING_ALERT	This is a final notice.Your "$feature" key will expire in under $days day(s).Please contact your authorized IronPort sales representative.	「**feature**」：有効期限が切れる機能の名前。 「**days**」：有効期限が切れるまでの日数。
	Warning。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。	
DNS.BOOTSTRAP_FAILED	Failed to bootstrap the DNS resolver.Unable to contact root servers.	
	Warning。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。	
INTERFACE.FAILOVER.FAILURE_BACKUP_DETECTED	Standby port $port on $pair_name failure	「**port**」：検出されたポート 「**pair_name**」：フェールオーバーのペア名。
	Warning。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。	

表 15-8　発生する可能性があるシステム アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
INTERFACE.FAILOVER.FAILURE_BACKUP_RECOVERED	Standby port $port on $pair_name okay Information。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。	「**port**」：故障したポート 「**pair_name**」：フェールオーバーのペア名。
INTERFACE.FAILOVER.FAILURE_DETECTED	Port $port failure on $pair_name, switching to $port_other Critical。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。	「**port**」：故障したポート。 「**port_other**」：新しいポート。 「**pair_name**」：フェールオーバーのペア名。
INTERFACE.FAILOVER.FAILURE_DETECTED_NO_BACKUP	Port $port_other on $pair_name is down, can't switch to $port_other Critical。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。	「**port**」：故障したポート。 「**port_other**」：新しいポート。 「**pair_name**」：フェールオーバーのペア名。
INTERFACE.FAILOVER.FAILURE_RECOVERED	Recovered network on $pair_name using port $port Information。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。	「**port**」：故障したポート 「**pair_name**」：フェールオーバーのペア名。
INTERFACE.FAILOVER.MANUAL	Manual failover to port $port on $pair_name Information。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。	「**port**」：新しいアクティブ ポート。 「**pair_name**」：フェールオーバーのペア名。
COMMON.INVALID_FILTER	Invalid $class: $error Warning。無効なフィルタが存在する場合に送信されます。	「**class**」：次のいずれか「Filter」、「SimpleFilter」など。 「**error**」：フィルタが無効な理由に関する追加の情報。

表 15-8　発生する可能性があるシステム アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
LDAP.GROUP_QUERY_ FAILED_ALERT	LDAP: Failed group query $name, comparison in filter will evaluate as false	「**name**」：クエリーの名前。
	Critical。LDAP グループ クエリーに失敗した場合に送信されます。	
LDAP.HARD_ERROR	LDAP: work queue processing error in $name reason $why	「**name**」：クエリーの名前。 「**why**」：エラーが発生した理由。
	Critical。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。	
LOG.ERROR.*	Critical。さまざまなロギング エラー。	
MAIL.PERRCPT.LDAP_ GROUP_QUERY_FAILED	LDAP group query failure during per-recipient scanning, possible LDAP misconfiguration or unreachable server.	
	Critical。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。	
MAIL.QUEUE.ERROR.*	Critical。メール キューのさまざまなハード エラー。	

表 15-8　発生する可能性があるシステム アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
MAIL.RES_CON_START_ ALERT.MEMORY	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources.RAM utilization for this system has exceeded the resource conservation threshold of $memory_threshold_start%.The allowed receiving rate for this system will be gradually decreased as RAM utilization approaches $memory_threshold_halt%.	「**hostname**」：ホストの名前。 「**memory_threshold_start**」：メモリのターピットを開始するパーセントしきい値。 「**memory_threshold_halt**」：メモリがフルのためにシステムが停止するパーセントしきい値。
	Critical。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。	
MAIL.RES_CON_START_ ALERT.QUEUE_SLOW	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources.The queue is overloaded and is unable to maintain the current throughput.	「**hostname**」：ホストの名前。
	Critical。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。	

表 15-8　発生する可能性があるシステム アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
MAIL.RES_CON_START_ ALERT.QUEUE	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources.Queue utilization for this system has exceeded the resource conservation threshold of $queue_threshold_start%.The allowed receiving rate for this system will be gradually decreased as queue utilization approaches $queue_threshold_halt%.	「**hostname**」：ホストの名前。 「**queue_threshold_start**」：キューのタービットを開始するパーセントしきい値。 「**queue_threshold_halt**」：キューがフルのためにシステムが停止するパーセントしきい値。
	Critical。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。	
MAIL.RES_CON_START_ ALERT.WORKQ	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources.Listeners have been suspended because the current work queue size has exceeded the threshold of $suspend_threshold.Listeners will be resumed once the work queue size has dropped to $resume_threshold.These thresholds may be altered via use of the 'tarpit' command on the system CLI.	「**hostname**」：ホストの名前。 「**suspend_threshold**」：リスナーが一時停止されるワーク キューの下限サイズ。 「**resume_threshold**」：リスナーが再開されるワーク キューの上限サイズ。
	Information。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。	

表 15-8　発生する可能性があるシステム アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
MAIL.RES_CON_START_ALERT	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources.	「**hostname**」：ホストの名前。
	Critical。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。	
MAIL.RES_CON_STOP_ALERT	This system (hostname: $hostname) has exited 'resource conservation' mode as resource utilization has dropped below the conservation threshold.	「**hostname**」：ホストの名前。
	Information。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。	
MAIL.WORK_QUEUE_PAUSED_NATURAL	work queue paused, $num msgs, $reason	「**num**」：ワーク キューに存在するメッセージ数。 「**reason**」：ワーク キューが中断された理由。
	Critical。ワーク キューが中断された場合に送信されます。	
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	work queue resumed, $num msgs	「**num**」：ワーク キューに存在するメッセージ数。
	Critical。ワーク キューが再開された場合に送信されます。	
NTP.NOT_ROOT	Not running as root, unable to adjust system time	
	Warning。NTP がルートとして動作していないため、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。	

表 15-8　発生する可能性があるシステム アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
QUARANTINE.ADD_DB_ ERROR	Unable to quarantine MID $mid - quarantine system unavailable	「**mid**」: MID
	Critical。メッセージを検疫エリアに送ることができない場合に送信されます。	
QUARANTINE.DB_ UPDATE_FAILED	Unable to update quarantine database (current version: $version; target $target_version)	「**version**」: 検出されたスキーマ バージョン。 「**target_version**」: 対象のスキーマ バージョン。
	Critical。検疫データベースがアップデートできない場合に送信されます。	
QUARANTINE.DISK_ SPACE_LOW	The quarantine system is unavailable due to a lack of space on the $file_system partition.	「**file_system**」: ファイルシステムの名前。
	Critical。検疫用のディスク領域がフルになった場合に送信されます。	
QUARANTINE.THRESHOLD _ALERT	Quarantine "$quarantine" is $full% full	「**quarantine**」: 検疫エリアの名前。 「**full**」: 検疫エリアの容量使用率。
	Warning。検疫エリアの容量使用率が 5 %、50 %、または 75 % に達した場合に送信されます。	
QUARANTINE.THRESHOLD _ALERT.SERIOUS	Quarantine "$quarantine" is $full% full	「**quarantine**」: 検疫エリアの名前。 「**full**」: 検疫エリアの容量使用率。
	Critical。検疫エリアの容量使用率が 95 % に達した場合に送信されます。	

表 15-8　発生する可能性があるシステム アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
REPORTD.DATABASE_ OPEN_FAILED_ALERT	The reporting system has encountered a critical error while opening the database.In order to prevent disruption of other services, reporting has been disabled on this machine.Please contact customer support to have reporting enabled.The error message is: $err_msg	「**err_msg**」：発生したエラー メッセージ
	Critical。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。	
REPORTD.AGGREGATION_ DISABLED_ALERT	Processing of collected reporting data has been disabled due to lack of logging disk space.Disk usage is above $threshold percent.Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc.).Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.	「**threshold**」：しきい値
	Warning。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。	

表 15-8　発生する可能性があるシステム アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
REPORTING.CLIENT. UPDATE_FAILED_ALERT	Reporting Client: The reporting system has not responded for an extended period of time ($duration).	「**duration**」：クライアントがレポート デーモンへの問い合わせを試行する時間。この値は、人間が読み取れる形式の文字列です（「1h 3m 27s」）。
	Warning。レポート エンジンがレポート データを保存できなかった場合に送信されます。	
REPORTING.CLIENT. JOURNAL.FULL	Reporting Client: The reporting system is unable to maintain the rate of data being generated.Any new data generated will be lost.	
	Critical。レポート エンジンが新規データを保存できない場合に送信されます。	
REPORTING.CLIENT. JOURNAL.FREE	Reporting Client: The reporting system is now able to handle new data.	
	Information。レポート エンジンが再び新規データを保存できるようになった場合に送信されます。	
PERIODIC_REPORTS. REPORT_TASK.BUILD_ FAILURE	A failure occurred while building periodic report '$report_title'.This subscription has been removed from the scheduler.	「**report_title**」：レポートのタイトル
	Critical。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。	
PERIODIC_REPORTS. REPORT_TASK.EMAIL_ FAILURE	A failure occurred while emailing periodic report '$report_title'.This subscription has been removed from the scheduler.	「**report_title**」：レポートのタイトル
	Critical。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。	

表 15-8　発生する可能性があるシステム アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
PERIODIC_REPORTS. REPORT_TASK.ARCHIVE_FAILURE	A failure occurred while archiving periodic report '$report_title'.This subscription has been removed from the scheduler.	「**report_title**」：レポートのタイトル
	Critical。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。	
SENDERBASE.ERROR	Error processing response to query $query: response was $response	「**query**」：クエリーするアドレス。 「**response**」：受信した応答の raw データ。
	Information。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。	
SMTPAUTH.FWD_SERVER_FAILED_ALERT	SMTP Auth: could not reach forwarding server $ip with reason: $why	「**ip**」：リモート サーバの IP。 「**why**」：エラーが発生した理由。
	Warning。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。	
SMTPAUTH.LDAP_QUERY_FAILED	SMTP Auth: LDAP query failed, see LDAP debug logs for details.	
	Warning。LDAP クエリーが失敗した場合に送信されます。	
SYSTEM.HERMES_SHUTDOWN_FAILURE. **REBOOT**	While preparing to ${what}, failed to stop mail server gracefully: ${error}$what:=reboot	「**error**」：発生したエラー。
	Warning。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。	

表 15-8　発生する可能性があるシステム アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
SYSTEM.HERMES_SHUTDOWN_FAILURE.SHUTDOWN	While preparing to ${what}, failed to stop mail server gracefully: ${error}$what:=shut down	「**error**」：発生したエラー。
	Warning。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。	
SYSTEM.RCPTVALIDATION.UPDATE_FAILED	Error updating recipient validation data: $why	「**why**」：エラー メッセージ。
	Critical。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。	
SYSTEM.SERVICE_TUNNEL.DISABLED	Tech support: Service tunnel has been disabled	
	Information。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。	
SYSTEM.SERVICE_TUNNEL.ENABLED	Tech support: Service tunnel has been enabled, port $port	「**port**」：サービス トンネルに使用されるポート。
	Information。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。	

アップデータ アラート

表 15-9 に、AsyncOS で生成される可能性があるさまざまなアップデータ アラートのリストを示します。

表 15-9　発生する可能性があるアップデータ アラートのリスト

アラート名	メッセージと説明	パラメータ
UPDATER.APP.UPDATE_ABANDONED	$app abandoning updates until a new version is published.The $app application tried and failed $attempts times to successfully complete an update.This may be due to a network configuration issue or temporary outage	「**app**」：アプリケーションの名前。 「**attempts**」：試行した回数。
	Warning。アプリケーションはアップデートを中止しています。	
UPDATER.UPDATERD.MANIFEST_FAILED_ALERT	The updater has been unable to communicate with the update server for at least $threshold.	「**threshold**」：人間が読み取れるしきい値の文字列。
	Warning。サーバのマニフェストの取得に失敗しました。	
UPDATER.UPDATERD.RELEASE_NOTIFICATION	$mail_text	「**mail_text**」：通知するテキスト。 「**notification_subject**」：通知するテキスト。
	Warning。リリースの通知です。	
UPDATER.UPDATERD.UPDATE_FAILED	Unknown error occured: $traceback	「**traceback**」：トレースバック。
	Critical。アップデートの実行に失敗しました。	

ウイルス感染フィルタ アラート

表 15-10 に、AsyncOS で生成される可能性があるさまざまなウイルス感染フィルタに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が記載されています。ウイルス感染フィルタは、検疫（具体的には Outbreak 検疫）で使用されるシステム アラートでも参照される場合があることに注意してください。

表 15-10　発生する可能性があるウイルス感染フィルタ アラートのリスト

アラート名	メッセージと説明	パラメータ
VOF.GTL_THRESHOLD_ALERT	IronPort Virus Outbreak Filters Rule Update Alert:$text All rules last updated at: $time on $date.	「**text**」：アップデート アラートのテキスト。 「**time**」：最終アップデートの時刻。 「**date**」：最終アップデートの日付。
	Information。ウイルス感染フィルタのしきい値が変更された場合に送信されます。	
AS.UPDATE_FAILURE	$engine update unsuccessful.This may be due to transient network or DNS issues, HTTP proxy configuration causing update transmission errors or unavailability of downloads.ironport.com.The specific error on the appliance for this failure is: $error	「**engine**」：アップデートに失敗したエンジン。 「**error**」：発生したエラー。
	Warning。アンチスパム エンジンまたは CASE ルールのアップデートに失敗した場合に送信されます。	

クラスタリング アラート

表 15-11 に、AsyncOS で生成される可能性があるさまざまなクラスタリングに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が記載されています。

表 15-11　発生する可能性があるクラスタリング アラートのリスト

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR.AUTH_ERROR	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Machine does not appear to be in the cluster Critical。認証エラーが発生した場合に送信されます。マシンがクラスタのメンバでない場合に起きる可能性があります。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR.DROPPED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Existing connection dropped Warning。クラスタへの接続がドロップされた場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR.FAILED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Connection failure Warning。クラスタへの接続に失敗した場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR.FORWARD_FAILED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Message forward failed, no upstream connection Critical。アプライアンスがクラスタのマシンにデータを転送できなかった場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。

表 15-11　発生する可能性があるクラスタリング アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR.NOROUTE	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=No route found	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
	Critical。マシンがクラスタの別のマシンへのルートを取得できなかった場合に送信されます。	
CLUSTER.CC_ERROR.SSH_KEY	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Invalid host key	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
	Critical。無効な SSH ホスト キーがあった場合に送信されます。	
CLUSTER.CC_ERROR.TIMEOUT	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Operation timed out	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
	Warning。指定された操作がタイムアウトした場合に送信されます。	
CLUSTER.CC_ERROR_NOIP	Error connecting to cluster machine $name - $error - $why	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
	Critical。アプライアンスがクラスタの別のマシンの有効な IP アドレスを取得できなかった場合に送信されます。	

表 15-11　発生する可能性があるクラスタリング アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR_NOIP.AUTH_ERROR	Error connecting to cluster machine $name - $error - whyerror:=Machine does not appear to be in the cluster Critical。クラスタのマシンに接続する際に認証エラーが発生した場合に送信されます。マシンがクラスタのメンバでない場合に起きる可能性があります。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.DROPPED	Error connecting to cluster machine $name - $error - whyerror:=Existing connection dropped Warning。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、クラスタへの接続がドロップした場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.FAILED	Error connecting to cluster machine $name - $error - whyerror:=Connection failure Warning。不明な接続エラーが発生し、マシンがクラスタの別のマシンの有効な IP アドレスを取得できなかった場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。

表 15-11　発生する可能性があるクラスタリング アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR_ NOIP.FORWARD_FAILED	Error connecting to cluster machine $name - $error - whyerror:=Message forward failed, no upstream connection	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
	Critical。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、アプライアンスがマシンにデータを転送できなかった場合に送信されます。	
CLUSTER.CC_ERROR_ NOIP.NOROUTE	Error connecting to cluster machine $name - $error - whyerror:=No route found	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
	Critical。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、別のマシンへのルートを取得できなかった場合に送信されます。	
CLUSTER.CC_ERROR_ NOIP.SSH_KEY	Error connecting to cluster machine $name - $error - whyerror:=Invalid host key	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
	Critical。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、有効な SSH ホスト キーを取得できなかった場合に送信されます。	
CLUSTER.CC_ERROR_ NOIP.TIMEOUT	Error connecting to cluster machine $name - $error - whyerror:=Operation timed out	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
	Warning。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、指定された操作がタイムアウトした場合に送信されます。	

表 15-11　発生する可能性があるクラスタリング アラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
CLUSTER.SYNC.PUSH_ALERT	Overwriting $sections on machine $name	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**sections**」：送信中のクラスタ セクションのリスト。
	Critical。設定データが同期から外れ、リモート ホストに送信された場合に送信されます。	

ネットワーク設定値の変更

このセクションでは、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、「System Setup Wizard の使用方法」（P.3-50）で System Setup Wizard（または `systemsetup` コマンド）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 および `dnsconfig` コマンドを利用）
- ルーティング設定（GUI、`routeconfig` コマンドおよび `setgateway` コマンドを利用）
- `dnsflush`
- パスワード
- ネットワーク アクセス
- ログイン バナー

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、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 01 12:00:01 2003
```

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（DNS）設定値の設定

GUI の [Network] メニューの [DNS] ページまたは dnsconfig コマンドで、IronPort アプライアンスの DNS 設定値を設定できます。

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、および使用する具体的なサーバ
- 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に待機する秒数
- DNS キャッシュのクリア

DNS サーバの指定

IronPort 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、またはインターネットのルート DNS サーバおよび指定した権威 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、当該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）である必要があります。

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。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。システムは最初のクエリーの有効期限が切れるか「タイムアウト」するまで短時間待機し、その後次のクエリーに対しては前回よりも少し長い時間待機します。その後も同様です。待機時間は、DNS サーバの正確な合計数と設定されているプライオリティに依存します。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 15-12　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 のサーバが 1 つダウンしている場合、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

IronPort 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

IronPort アプライアンスは電子メールの送受信の際、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（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。結果が一致しない場合、または A レコードが存在しない場合は、システムは IP アドレスのみを使用して Host Access Table（HAT; ホスト アクセス テーブル）内のエントリと照合します）。この特別なタイムアウト時間は上記ルックアップのみに適用され、「複数エントリとプライオリティ」（P.15-532）で説明している一般的な DNS タイムアウトとは関係ありません。

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たまにあります。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。

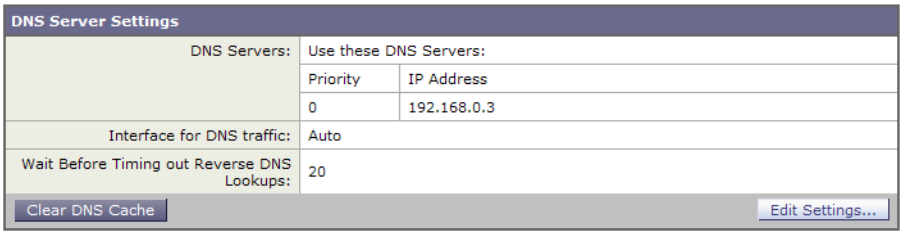
DNS キャッシュのクリア

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

Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）にログインして、[Network] タブの [DNS] リンクをクリックします。

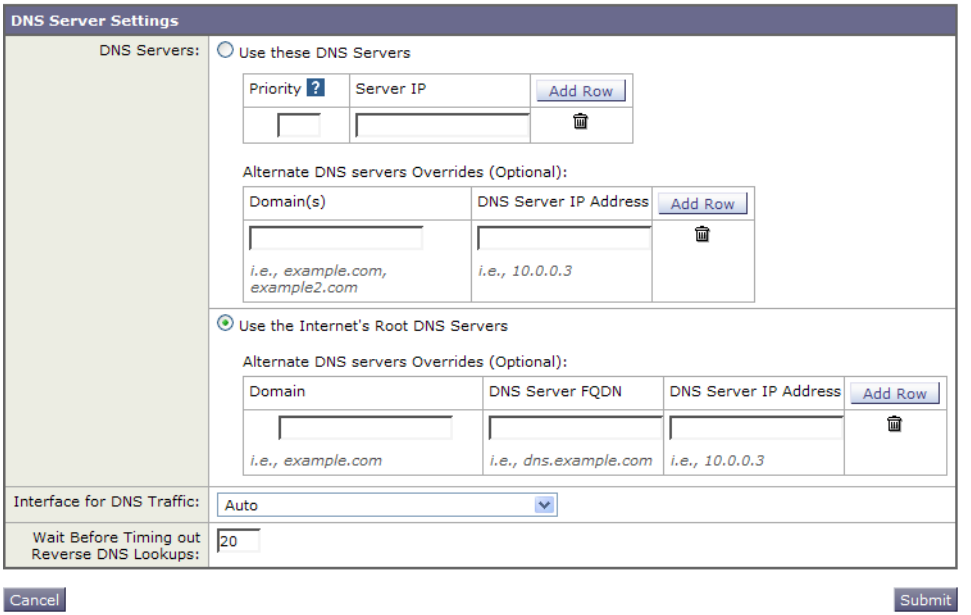
図 15-12　[DNS] ページ



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　[Edit Settings] をクリックします。[Edit DNS] ページが表示されます。

図 15-13　[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 サーバを使用するか、またはインターネットのルート DNS サーバを使用して代替 DNS サーバを指定するかを選択します。

ステップ 3　ユーザ独自の DNS サーバを使用する場合は、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.15-532）を参照してください。

ステップ 4　あるドメインに対して代替 DNS サーバを指定する場合は、ドメインと代替 DNS サーバの IP アドレスを入力します。[Add Row] をクリックし、ドメインを追加します。

（注）　ドメイン名をカンマで区切ることで、1 つの DNS サーバに対して複数のドメインを入力できます。IP アドレスをカンマで区切ることで、複数の DNS サーバを入力することもできます。

ステップ 5　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 6　逆引き DNS ルックアップを中止するまでに待機する秒数を入力します。

ステップ 7　[Clear Cache] をクリックして、DNS キャッシュをクリアすることもできます。

ステップ 8　変更を送信して確定します。

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。GUI の [Network] タブの [Routing] ページ、または CLI の `routeconfig` コマンドから、スタティック ルートを管理できます。

スタティック ルートの管理（GUI）

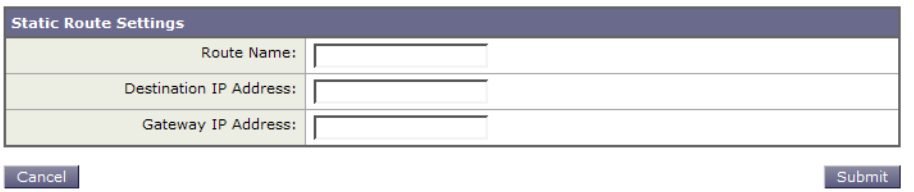
[Network] タブの [Routing] ページから、スタティック ルートの作成、編集または削除ができます。このページからデフォルト ゲートウェイの変更もできます。

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

図 15-14　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　変更を送信して確定します。

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、削除を確定します。

ステップ 3　変更を確定します。

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。

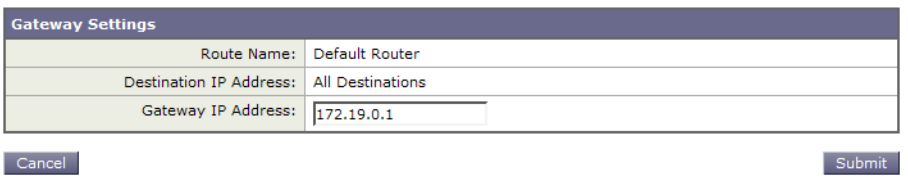
ステップ 3　変更を確定します。

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 15-15　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　変更を送信して確定します。

デフォルト ゲートウェイの設定

GUI の [Network] メニューの [Static Routes] ページ（「デフォルト ゲートウェイの変更（GUI）」（P.15-538）を参照）または CLI の `setgateway` コマンドから、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。

パスワードを GUI から変更するには、[System Administration] タブから利用可能な [Users] ページを使用します。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」にあるユーザ管理に関する項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。

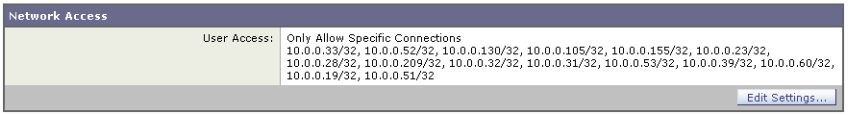
IP ベースのネットワーク アクセスの設定

電子メール セキュリティ アプライアンスにアクセスするユーザの IP アドレスを制御できます。ユーザは、定義したアクセス 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。ネットワーク アクセス リストを作成する際は、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。

AsyncOS では、現在のマシンの IP アドレスがネットワーク アクセス リストに含まれていない場合に警告を表示します。現在のマシンの IP アドレスがリストにない場合、変更を確定するとアプライアンスにアクセスできなくなります。

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 15-16 は、電子メール セキュリティ アプライアンスへの接続が許可されている 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 15-16　[Network Access] ページ



ユーザ アクセス リストを GUI から作成するには、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　[Only Allow Specific Connections] を選択します。

ステップ 4　アプライアンスへの接続を許可する 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。複数のエントリを指定する場合は、カンマで区切ります。

ステップ 5　変更を送信して確定します。

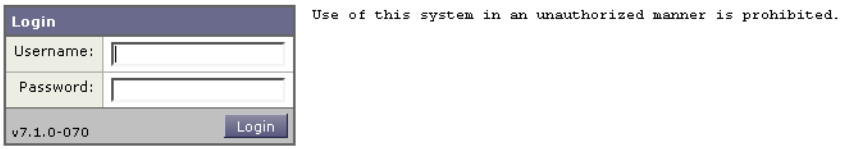
ログイン バナーの追加

ユーザが SSH、Telnet、FTP、または Web UI からログインしようとした際に、「ログイン バナー」と呼ばれるメッセージを表示するように電子メール セキュリティ アプライアンスを設定できます。ログイン バナーは、CLI でログイン プロンプトの上部に表示され、GUI でログイン プロンプトの右側に表示されるカスタマイズ可能なテキストです。ログイン バナーを使用して、内部のセキュリティ情報またはアプライアンスのベスト プラクティスに関する説明を表示できます。たとえば、許可しないアプライアンスの使用を禁止する簡単な注意文言を作成したり、ユーザがアプライアンスに対して行った変更を確認する企業の権利に関する詳細な警告を作成したりできます。

CLI の `adminaccessconfig > banner` コマンドを使用して、ログイン バナーを作成します。ログイン バナーは、80 x 25 のコンソールに収まるように最大 2000 文字になっています。ログイン バナーは、アプライアンスの `/data/pub/configuration` ディレクトリにあるファイルからインポートできます。バナーを作成したら、変更を確定します。

図 15-17 は、Web UI ログイン画面に表示されたログイン バナーを示しています。

図 15-17　バナーが表示された Web UI ログイン画面



システム時刻

IronPort アプライアンスのシステム時刻の設定、使用する時間帯の設定、または NTP サーバとクエリー インターフェイスの選択を行うには、GUI の [System Administration] メニューから [Time Zone] ページまたは [Time Settings] ページを使用するか、CLI の `ntpconfig` コマンド、`settime` コマンドおよび `settz` コマンドを使用します。

[Time Zone] ページ

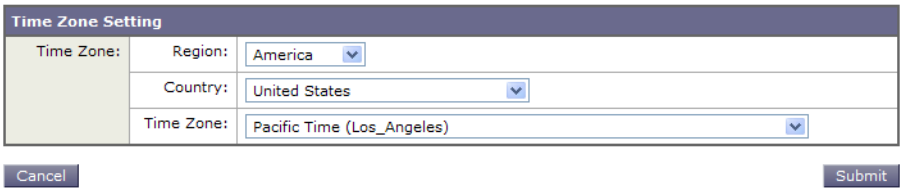
[Time Zone] ページ（GUI の [System Administration] メニューから利用可能）では、IronPort アプライアンスの時間帯を表示します。特定の時間帯または GMT オフセットを選択できます。

時間帯の選択

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　[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 15-18　[Time Zone] ページ



ステップ 2　地域、国、および時間帯をプルダウン メニューから選択します。

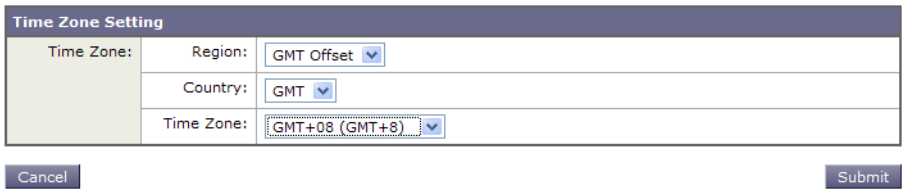
ステップ 3　変更を送信して確定します。

GMT オフセットの選択

ステップ 1　[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] ページが更新されます。

図 15-19　[Time Zone] ページ



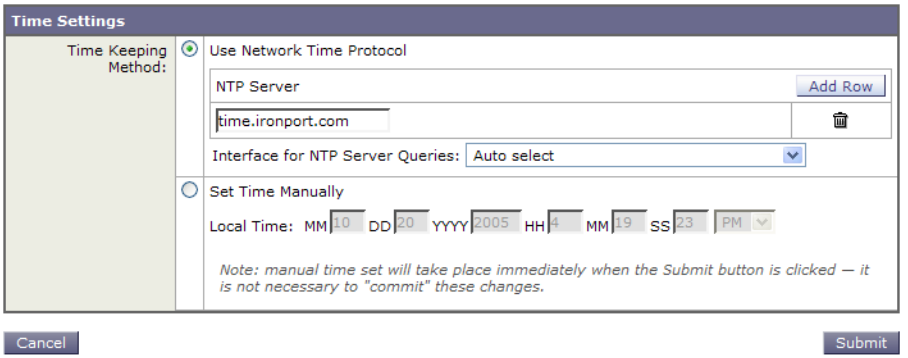
ステップ 3　[Time Zone] リストでオフセットを選択します。オフセットは、GMT（グリニッジ子午線）に達するために足し引きする必要がある時間を示しています。時間の前にマイナス記号（「-」）が付いている場合、グリニッジ子午線の東側にあたります。プラス記号（「+」）の場合、グリニッジ子午線の西側にあたります。

ステップ 4　変更を送信して確定します。

時刻設定の編集（GUI）

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

図 15-20　[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　[System Administration] > [Time Settings] ページで、[Edit Settings] をクリックします。[Edit Time Settings] 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　変更を送信して確定します。

システム時刻の設定（NTP サーバを使用しない方法）

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　[System Administration] > [Time Settings] ページで、[Edit Settings] をクリックします。[Edit Time Settings] 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　月、日、年、時、分、および秒を入力します。

ステップ 4　[A.M.] または [P.M.] を選択します。

ステップ 5　変更を送信して確定します。