CHAPTER 3

セットアップおよび設置

この章では、System Setup Wizard を使用して、電子メール配信用に IronPort C-Series または X-Series アプライアンスを設定するプロセスについて説明します。IronPort M-Series アプライアンスを設定する場合は、第 17 章「IronPort M-Series セキュリティ管理アプライアンス」を参照してください。この章を終了すると、IronPort アプライアンスによって、インターネット越しまたはネットワーク内で SMTP 電子メールを送信できるようになっています。

エンタープライズ ゲートウェイ（インターネットからの電子メールの受け入れ）としてシステムを設定する場合は、まずこの章を完了してから、詳細について第 5 章「電子メールを受信するためのゲートウェイの設定」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。

設置計画

始める前に

IronPort アプライアンスを既存のネットワーク インフラストラクチャに設置する方法は複数あります。ここでは、設置を計画するときに採用可能な複数のオプションについて説明します。

ネットワーク境界に IronPort アプライアンスを配置する

IronPort アプライアンスは、メール エクスチェンジャつまり「MX」とも呼ばれる、SMTP ゲートウェイとして機能することを目的としていることに注意してください。インターネット メッセージング専用に機能強化されたオペレーティング システムに加え、AsyncOS オペレーティング システムの最新機能の多くは、電子メールの送受信のためにインターネット（つまり外部 IP アドレス）に直接アクセスできる IP アドレスを持つ、最初のマシンとしてアプライアンスを設置した場合に、最適な性能を発揮します。次の例を参考にしてください。

- 受信者ごとの評価フィルタリング、アンチスパム、アンチウイルス、およびウイルス感染フィルタの機能（「評価フィルタリング」（P.7-246）、「IronPort Anti-Spam フィルタリング」（P.8-264）、「Sophos Anti-Virus フィルタリング」（P.9-305）、および「ウイルス感染フィルタ」（P.10-335）を参照）は、インターネットからおよび内部ネットワークからのメッセージの*直接のフロー*を扱うことを目的としています。企業が送受信するすべての電子メール トラフィックに対するポリシー施行（「ホスト アクセス テーブル（HAT）：送信者グループとメール フロー ポリシー」（P.5-115））のために IronPort アプライアンスを設定できます。

IronPort アプライアンスは、パブリックインターネットを介してアクセス可能なことと、電子メール インフラストラクチャの「第 1 ホップ」であることの両方を必ず満たす必要があります。別の MTA をネットワーク境界に配置してすべての外部接続を処理させると、IronPort アプライアンスで送信者の IP アドレスを判別できなくなります。送信者の IP アドレスは、メール フロー モニタで送信元を識別および区別したり、SenderBase 評価サービスに送信者の SenderBase Reputation Score（SBRS; SenderBase 評価スコア）を問い合わせたり、IronPort Anti-Spam 機能およびウイルス感染フィルタ機能の有効性を高めたりするために必要です。

（注）インターネットから電子メールを受信する*最初の*マシンとして IronPort アプライアンスを設定できない場合でも、IronPort アプライアンスで使用可能なセキュリティ サービスの一部は利用できます。詳細は「着信リレー」（P.8-288）を参照してください。

IronPort アプライアンスを SMTP ゲートウェイとして使用することにより、次の機能が実現されます。

- メール フロー モニタ機能（『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」を参照）により、内部および外部の両方の送信者から企業に着信するすべての電子メール トラフィックに対する徹底的な可視性が提供されます。
- ルーティング、エイリアシング、およびマスカレードを対象とする LDAP クエリー（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」）では、ディレクトリ インフラストラクチャを統合でき、更新の単純化につながります。
- エイリアス テーブル（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Creating Alias Tables」）、ドメイン ベースのルーティング（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「The Domain Map Feature」）、およびマスカレード（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Masquerading」）などの一般的なツールによって、オープンソースの MTA からの移行が簡単になります。

DNS への IronPort アプライアンスの登録

不正な電子メール送信者は、次の攻撃対象を探してパブリック DNS レコードを積極的に検索します。IronPort Anti-Spam、ウイルス感染フィルタ、McAfee Antivirus、および Sophos Anti-Virus の機能を十分活用するには、IronPort アプライアンスを必ず DNS に登録する必要があります。IronPort アプライアンスを DNS に登録するには、アプライアンスのホスト名を IP アドレスにマッピングする A レコードおよびパブリック ドメインをアプライアンスのホスト名にマッピングする MX レコードを作成します。ドメインのプライマリ MTA またはバックアップ MTA のいずれかとして IronPort アプライアンスをアドバタイズするように MX レコードのプライオリティを指定する必要があります。

次の例では、MX レコードに大きいプライオリティ値（20）が指定されているため、IronPort アプライアンス（IronPort.example.com）は、ドメイン example.com のバックアップ MTA です。言い換えると、数値が大きいほど、MTA のプライオリティは低くなります。

```
$ host -t mx example.com

example.com mail is handled (pri=10) by mail.example.com

example.com mail is handled (pri=20) by ironport.example.com
```

IronPort アプライアンスを DNS に登録するということは、MX レコードのプライオリティに設定する値に関係なく、スパム攻撃にさらされることを意味します。ただし、ウイルス攻撃でバックアップ MTA がターゲットになることはまれです。したがって、アンチウイルス エンジンの性能を徹底的に評価するには、IronPort アプライアンスの MX レコードのプライオリティに、他の MTA のプライオリティ以上の値を設定します。

インストール シナリオ

アプライアンスを設置する前に、すべての機能を検討しなければならない場合があります。第 4 章「電子メール パイプラインの理解」では、インフラストラクチャへの IronPort アプライアンスの配置に影響する可能性のある、アプライアンスの全機能の概要を提供しています。

大部分のお客様のネットワーク コンフィギュレーションは、以降のシナリオで表現されています。ネットワーク コンフィギュレーションが多少異なっており、設置計画の支援を必要とする場合は、IronPort カスタマー サポートにお問い合わせください（「Cisco IronPort カスタマー サポート」（P.1-12）を参照）。

設定の概要

いくつかのシナリオでは、IronPort アプライアンスはネットワークの DMZ 内に配置されます。その場合は、IronPort アプライアンスとグループウェア サーバの間にさらにファイアウォールを設置しています。

次のネットワーク シナリオを説明します。

- ファイアウォール内（図 3-2（P.3-42）を参照）

実際のインフラストラクチャと最も一致する設定を選択してください。その後、「セットアップの準備」（P.3-43）に進んでください。

着信

- 指定したローカル ドメイン宛ての着信メールは受け入れられます（ を参照）。
- その他のドメインはすべて拒否されます。
- 外部システムは、ローカル ドメイン宛て電子メールを転送するために IronPort アプライアンスに直接接続し、IronPort アプライアンスは、SMTP ルートを介して、そのメールを適切なグループウェア サーバ（Exchange™、Groupwise™、Domino™ など）にリレーします（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Routing Email for Local Domains」を参照）。

発信

- 内部ユーザが送信した発信メールは、グループウェア サーバによって IronPort アプライアンスにルーティングされます。
- IronPort アプライアンスでは、プライベート リスナーのホスト アクセス テーブルの設定値に基づいてアウトバウンド電子メールを受け入れます（詳細は、「リスナーによる電子メールの受信」（P.5-108）を参照してください）。

イーサネット インターフェイス

- これらの設定では、IronPort アプライアンスにある使用可能なイーサネット インターフェイスのうち 1 つだけを必要とします。ただし、イーサネット インターフェイスを 2 つ設定すると、内部ネットワークを外部インターネット ネットワーク接続と分離できます。

使用可能なインターフェイスに対する複数 IP アドレスの割り当ての詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Virtual Gateway™ Technology」および付録 B「ネットワーク アドレスと IP アドレスの割り当て」を参照してください。

（注）　IronPort X1050/1060/1070、C650/660/670、および C350/360/370 電子メール セキュリティ アプライアンスには、デフォルトで、使用可能なイーサネット インターフェイスが 3 つあります。IronPort C150/160 電子メール セキュリティ アプライアンスには、使用可能なイーサネット インターフェイスが 2 つあります。

拡張設定

図 3-2 および図 3-3 に示すこの設定に加え、次の設定も可能です。

- 中央集中管理機能を使用する複数 IronPort アプライアンス
- IronPort アプライアンスの 2 つのイーサネット インターフェイスを NIC ペアリング機能によって「チーム化」することによるネットワーク インターフェイス カード レベルでの冗長性

これらの機能については、いずれも『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』を参照してください。

ファイアウォール設定値（NAT、ポート）

ネットワーク コンフィギュレーションによっては、次のポートへのアクセスを許可するように、ファイアウォールを設定する必要がある場合があります。

SMTP サービスおよび DNS サービスでは、インターネットにアクセスできる必要があります。他のシステム機能では、次のサービスが必要な場合があります。

表 3-1　　ファイアウォール ポート

• SMTP：ポート 25 • DNS：ポート 53 • HTTP：ポート 80 • HTTPS：ポート 443 • SSH：ポート 22 • Telnet：ポート 23	• LDAP：ポート 389 または 3268 • NTP：ポート 123 • LDAP over SSL：ポート 636 • グローバル カタログ クエリー用の SSL を使用した LDAP：ポート 3269 • FTP：ポート 21、データ ポート TCP 1024 以上 • IronPort スパム検疫：ポート 6025

IronPort アプライアンスを適切に運用するために開けなければならない可能性のあるポートに関するすべての情報については、付録 C「ファイアウォール情報」を参照してください。たとえば、次の接続のためにファイアウォールでポートを開けなければならない場合があります。

- 外部クライアント（MTA）からの IronPort アプライアンスに対する接続
- グループウェア サーバとの間の接続
- インターネット ルート DNS サーバまたは内部 DNS サーバへの接続
- IronPort ダウンロード サーバへの接続（McAfee および Sophos Anti-Virus のアップデート、ウイルス感染フィルタ ルール、および AsyncOS のアップデートのため）
- NTP サーバへの接続
- LDAP サーバへの接続

物理寸法

IronPort X1050/1060、C650/660 および C350/360 電子メール セキュリティ アプライアンスには、次の物理寸法が適用されます。

- 高さ：8.656 cm（3.40 インチ）
- 幅：レールを取り付けて 48.26 cm（19.0 インチ）（レールを取り付けない場合は 17.5 インチ）

- 奥行：75.68 cm（29.79 インチ）
- 重量：最大 26.76 kg（59 ポンド）

IronPort C370、C670、および X1070 電子メール セキュリティ アプライアンスには、次の物理寸法が適用されます。

- 高さ：8.64 cm（3.40 インチ）
- 幅：レールの取り付け有無によらず 48.24 cm（18.99 インチ）
- 奥行：72.06 cm（28.40 インチ）
- 重量：最大 23.59 kg（52 ポンド）

IronPort C150 および C160 電子メール セキュリティ アプライアンスには、次の物理寸法が適用されます。

- 高さ：4.2 cm（1.68 インチ）
- 幅：レールを取り付けて 48.26 cm（19.0 インチ）（レールを取り付けない場合は 17.5 インチ）
- 奥行：57.6 cm（22.7 インチ）
- 重量：最大 11.8 kg（26 ポンド）

IronPort アプライアンスのネットワークへの物理接続

設定シナリオ

IronPort アプライアンスの一般的な設定シナリオは次のとおりです。

- **インターフェイス**：大部分のネットワーク環境では、IronPort アプライアンスにある使用可能な 3 つのイーサネット インターフェイスのうち 1 つだけを必要とします。ただし、イーサネット インターフェイスを 2 つ設定すると、内部ネットワークを外部インターネット ネットワーク接続と分離できます。

- **パブリック リスナー（着信電子メール）**：パブリック リスナーでは、多数の外部ホストからの接続を受けいれ、一定の数の内部グループウェア サーバにメッセージを振り向けます。
  - HAT の設定値に基づいて外部メール ホストからの接続を受け入れます。HAT は、デフォルトでは、すべての外部メール ホストからの接続を受け入れるように設定されています。
  - RAT で指定されているローカル ドメイン宛ての着信メールに限って受け入れます。その他のドメインはすべて拒否されます。
  - SMTP ルートの定義に従って、適切な内部グループウェア サーバにメールをリレーします。
- **プライベート リスナー（発信電子メール）**：プライベート リスナーは、一定の数の内部グループウェア サーバからの接続を受け入れ、多数の外部メール ホストにメッセージを振り向けます。
  - 内部グループウェア サーバは、IronPort C-Series または X-Series アプライアンスに発信メールをルーティングするように設定されます。
  - IronPort アプライアンスは、HAT の設定値に基づいて、内部グループウェア サーバからの接続を受け入れます。HAT は、デフォルトでは、すべての内部メール ホストからの接続を受け入れるように設定されています。

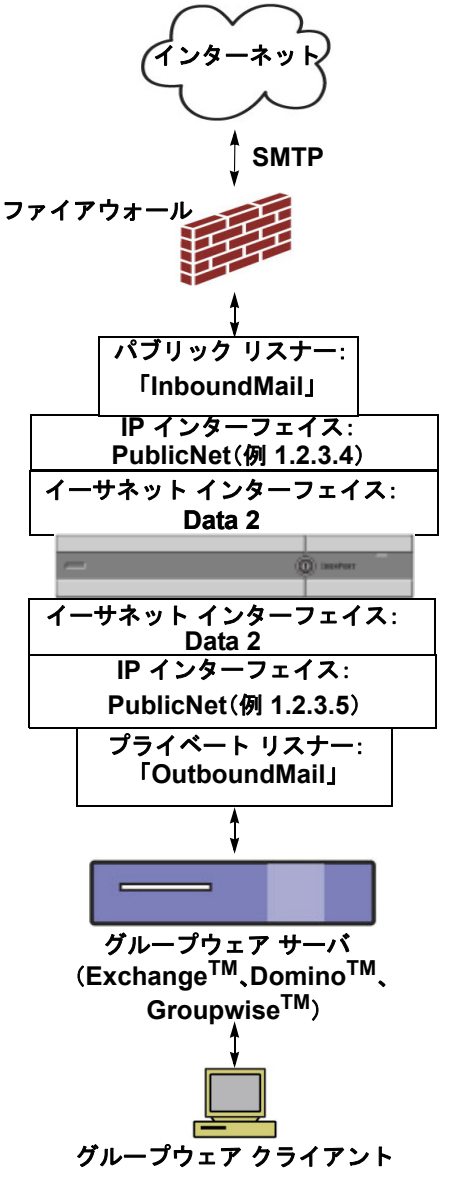
着信メールと発信メールの分離

着信と発信の電子メール トラフィックを個別のリスナーおよび個別の IP アドレスで分離できます。ただし、アプライアンスの System Setup Wizard では、次の設定を持つ初期設定をサポートしています。

- *個別の*物理インターフェイスに設定された 2 個の論理 IP アドレス上の 2 つの個別リスナー
  ―― 着信と発信のトラフィックの分離
- 1 つの物理インターフェイスに設定された 1 つの論理 IP アドレス上の 1 つのリスナー
  ―― 着信と発信の両トラフィックの組み合わせ

リスナー 1 つと 2 つの両方の設定に対するコンフィギュレーション ワークシートが以下にあります（「セットアップ情報の収集」（P.3-47）を参照）。大部分の設定シナリオは、次の 3 つの図のいずれかで表現されます。

図 3-2　ファイアウォール越しのシナリオ：リスナー 2 個、IP アドレス 2 個の設定



注：

- リスナー x 2
- IP アドレス x 2
- イーサネット インターフェイス x 1 または 2（表示されるインターフェイスは 1 個のみ）
- 設定済みの SMTP ルート

インバウンド リスナー：「InboundMail」（パブリック）

- IP アドレス：1.2.3.4
- Data 2 インターフェイスのリスナーでポート 25 をリッスン
- HAT（すべてを受け入れ）
- RAT（ローカル ドメイン宛てメールを受け入れ、その他すべてを拒否）

アウトバウンド リスナー：「OutboundMail」（プライベート）

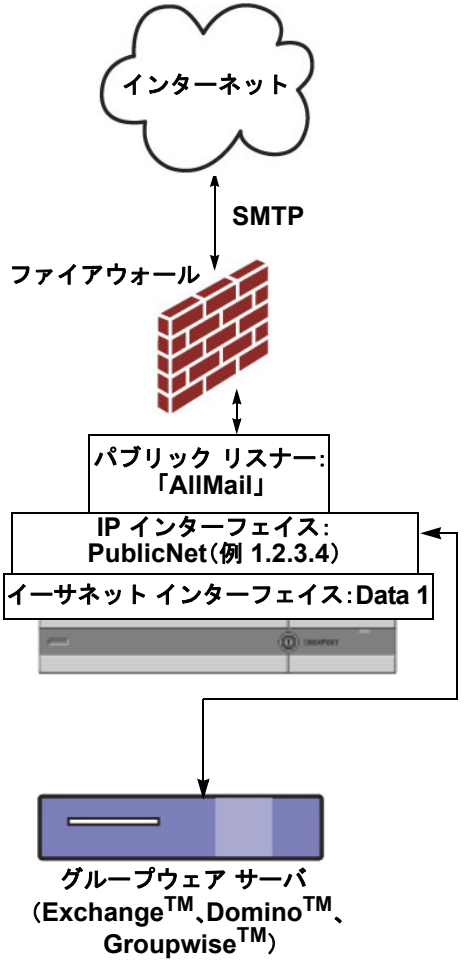
- IP アドレス：1.2.3.5
- Data 2 インターフェイスのリスナーでポート 25 をリッスン
- HAT（ローカル ドメイン宛てをリレー、その他すべてを拒否）

インターネット ルート サーバまたは内部 DNS サーバを使用するように DNS を設定可能

SMTP ルートでは、適切なグループウェア サーバにメールを振り向け

適切なサービスと IronPort アプライアンスの双方向の通信用にファイアウォール ポートをオープン

図 3-3　　リスナー x 1、IP アドレス x 1 の設定



注：

- リスナー x 1
- IP アドレス x 1
- イーサネット インターフェイス x 1
- 設定済みの SMTP ルート

インバウンド リスナー：「InboundMail」（パブリック）

- IP アドレス：1.2.3.4
- Data 2 インターフェイスのリスナーでポート 25 をリッスン
- HAT（すべてを受け入れ）では、RELAYLIST にあるグループウェア サーバ用のエントリが組み込まれます。
- RAT（ローカル ドメイン宛てメールを受け入れ、その他すべてを拒否）

インターネット ルート サーバまたは内部 DNS サーバを使用するように DNS を設定可能

SMTP ルートでは、適切なグループウェア サーバにメールを振り向け

適切なサービスと IronPort アプライアンスの双方向の通信用にファイアウォール ポートをオープン

セットアップの準備

IronPort アプライアンスのセットアップ処理は、5 つの手順にわかれています。

ステップ 1　アプライアンスへの接続方法を決定します。

ステップ 2　ネットワーク アドレスと IP アドレスの割り当て（IP アドレスは 1 個か 2 個か）を決定します。

ステップ 3　システム セットアップに関する情報を収集します。

ステップ 4　Web ブラウザを起動し、アプライアンスの IP アドレスを入力します（または、「コマンド ライン インターフェイス（CLI）System Setup Wizard の実行」（P.3-70）で説明されている Command Line Interface（CLI; コマンド ライン インターフェイス）を使用することもできます）。

ステップ 5　System Setup Wizard を実行してシステムを設定します。

アプライアンスへの接続方式の決定

IronPort アプライアンスを環境に正常にセットアップするには、IronPort アプライアンスをネットワークに接続する方法に関する重要なネットワーク情報をネットワーク管理者から収集する必要があります。

アプライアンスへの接続

初期セットアップ時に、次の 2 つのいずれかの方式で、アプライアンスに接続できます。

表 3-2　アプライアンスに接続するオプション

Ethernet	PC とネットワークの間およびネットワークと IronPort 管理ポートの間のイーサネット接続です。工場出荷時に Management ポートに割り当てられている IP アドレスは 192.168.42.42 です。ご使用のネットワーク コンフィギュレーションで使用可能であれば、この方法による接続が手軽です。
シリアル	シリアル通信によって PC と IronPort シリアル コンソール ポートが接続されます。イーサネット方式を使用できない場合は、コンピュータとアプライアンスをシリアル同士でストレート接続すると、代替ネットワーク設定値を Management ポートに適用できるまでの代用になります。ピン割り当については、「シリアル接続によるアクセス」（P.A-583）を参照してください。シリアル ポートの通信設定値は次のとおりです。 **Bits per second**：9600 **データ ビット**：8 **パリティ**：なし **ストップビット**：1 **フロー制御**：ハードウェア **（注）** FIPS 準拠の電子メール セキュリティ アプライアンスに接続している場合、セッションは、シリアル コンソール ポートの切断後 30 分でタイムアウトされます。

（注） 初期接続方式は、最終的な方式でないことに留意してください。このプロセスは、初期設定だけに適用されます。ネットワーク設定値を後で変更して、別の接続方式を使用できます（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）。アプライアンスを利用するための管理者権限が異な

る、複数のユーザ アカウントを作成することもできます（詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Adding Users」を参照してください）。

ネットワーク アドレスと IP アドレスの割り当ての決定

電子メールを受信および配信するネットワーク接続の選択

大部分のユーザは、IronPort アプライアンスから 2 つのネットワークに接続することによって、アプライアンス上の 2 つの Data イーサネット ポートを利用します。

- プライベート ネットワークでは、内部システム宛てのメッセージを受け入れて配信します。
- パブリック ネットワークでは、インターネット宛てのメッセージを受け入れて配信します。

1 つの Data ポートだけを両方の機能に使用するユーザもいます。Management イーサネット ポートでは任意の機能をサポートできますが、グラフィカル ユーザ インターフェイスとコマンド ライン インターフェイスを利用するために事前設定されています。

物理イーサネット ポートへの論理 IP アドレスのバインド

着信と発信の電子メール トラフィックを個別のリスナーおよび個別の IP アドレスで分離できます。ただし、アプライアンスの System Setup Wizard では、次の設定を持つ初期設定をサポートしています。

- *個別の*物理インターフェイスに設定された 2 個の論理 IP アドレス上の 2 つの個別リスナー
  ―着信と発信のトラフィックの分離
- 1 つの物理インターフェイスに設定された 1 つの論理 IP アドレス上の 1 つのリスナー
  ―着信と発信の両トラフィックの組み合わせ

接続用ネットワーク設定値の選択

使用することを選択した各イーサネット ポートに関する次のネットワーク情報が必要になります。

- IP アドレス
- ネットマスク

さらに、ネットワーク全体に関する次の情報も必要になります。

- ネットワークのデフォルト ルータ（ゲートウェイ）の IP アドレス
- DNS サーバの IP アドレスおよびホスト名（インターネット ルート サーバを使用する場合は不要）
- NTP サーバのホスト名または IP アドレス（IronPort のタイム サーバを使用する場合は不要）

詳細については、付録 B「ネットワーク アドレスと IP アドレスの割り当て」を参照してください。

（注）　インターネットと IronPort アプライアンスの間でファイアウォールを稼動しているネットワークの場合は、IronPort アプライアンスを正常に機能させるために、特定のポートを開ける必要がある場合があります。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。

セットアップ情報の収集

これで、System Setup Wizard で必要な内容を選択するための要件および戦略が判明したため、この項を参照しながら次の表を使用して、システムのセットアップに関する情報を収集してください。

ネットワークおよび IP アドレスの詳細については、付録 B「ネットワーク アドレスと IP アドレスの割り当て」を参照してください。IronPort M-Series アプライアンスを設定する場合は、第 17 章「IronPort M-Series セキュリティ管理アプライアンス」を参照してください。

表 3-3　システム セットアップ ワークシート：2 個の IP アドレスによる電子メール トラフィックの分離

[System Settings]		
[Default System Hostname:]		
[Email System Alerts To:]		
[Deliver Scheduled Reports To:]		
[Time Zone Information:]		
[NTP Server:]		
[Admin Password:]		
[SenderBase Network Participation:]	イネーブル/ディセーブル	
[AutoSupport:]	イネーブル/ディセーブル	
[Network Integration]		
[Gateway:]		
[DNS:]（インターネットまたは独自指定）		
[Interfaces]		
[Data 1 Port]		
[IP Address:]		
[Network Mask:]		
[Fully Qualified Hostname:]		
[Accept Incoming Mail:]	**[Domain]**	**[Destination]**
[Relay Outgoing Mail:]	**[System]**	
[Data 2 Port]		
[IP Address:]		
[Network Mask:]		
[Fully Qualified Hostname:]		
[Accept Incoming Mail:]	**[Domain]**	**[Destination]**
[Relay Outgoing Mail:]	**[System]**	

表 3-3　システム セットアップ ワークシート：2 個の IP アドレスによる電子メール トラフィックの分離（続き）

[Management Port]		
[IP Address:]		
[Network Mask:]		
[Fully Qualified Hostname:]		
[Accept Incoming Mail:]	**[Domain]**	**[Destination]**
[Relay Outgoing Mail:]	**[System]**	
[Message Security]		
[SenderBase Reputation Filtering:]	イネーブル/ディセーブル	
[Anti-Spam Scanning Engine]	なし/IronPort	
[McAfee Anti-Virus Scanning Engine]	イネーブル/ディセーブル	
[Sophos Anti-Virus Scanning Engine]	イネーブル/ディセーブル	
[Virus Outbreak Filters]	イネーブル/ディセーブル	

表 3-4　システム セットアップ ワークシート：1 個の IP アドレスをすべての電子メール トラフィックに使用

[System Settings]	
[Default System Hostname:]	
[Email System Alerts To:]	
[Deliver Scheduled Reports To:]	
[Time Zone:]	
[NTP Server:]	
[Admin Password:]	
[SenderBase Network Participation:]	イネーブル/ディセーブル
[AutoSupport:]	イネーブル/ディセーブル
[Network Integration]	
[Gateway:]	
[DNS:]（インターネットまたは独自指定）	

表 3-4　システム セットアップ ワークシート：1 個の IP アドレスをすべての電子メール トラフィックに使用（続き）

[Interfaces]		
[Data 2 Port]		
[IP Address:]		
[Network Mask:]		
[Fully Qualified Hostname:]		
[Accept Incoming Mail:]	**[Domain]**	**[Destination]**
[Relay Outgoing Mail:]	**[System]**	
[Data 1 Port]		
[IP Address:]		
[Network Mask:]		
[Fully Qualified Hostname:]		
[Message Security]		
[SenderBase Reputation Filtering:]	イネーブル/ディセーブル	
[Anti-Spam Scanning Engine]	なし/IronPort	
[McAfee Anti-Virus Scanning Engine]	イネーブル/ディセーブル	
[Sophos Anti-Virus Scanning Engine]	イネーブル/ディセーブル	
[Virus Outbreak Filters]	イネーブル/ディセーブル	

System Setup Wizard の使用方法

IronPort AsyncOS オペレーティング システムには、システム コンフィギュレーションの 5 つの手順を実行するための、ブラウザベースの System Setup Wizard が用意されています。Command Line Interface（CLI; コマンド ライン インターフェイス）バージョンの System Setup Wizard も含まれています。詳細については、「コマンド ライン インターフェイス（CLI）System Setup Wizard の実行」（P.3-70）を参照してください。System Setup Wizard では使用できないカスタム コンフィギュレーション オプションを利用するユーザもいます。ただし、初期

セットアップでは System Setup Wizard を使用して、設定に漏れがないようにする必要があります。「セットアップの準備」（P.3-43）で必要な情報を収集済みであれば、コンフィギュレーション プロセスを完了するための時間はわずかです。

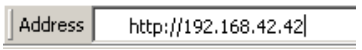
警告　**System Setup Wizard では、システムを完全に再設定します。System Setup Wizard は、アプライアンスをまったく初めて設置する場合か、既存の設定を上書きする場合に限り使用してください。**

警告　**C650/660/670、C350/360/370、および X1050/1060/1070 システムの Management ポートおよび C150/160 システムの Data 1 ポートの出荷時設定による IronPort アプライアンスのデフォルト IP アドレスは、192.168.42.42 です。IronPort アプライアンスをネットワークに接続する前に、他の装置の IP アドレスが、この工場出荷時のデフォルト設定と競合していないことを確認してください。IronPort M-Series アプライアンスを設定する場合は、「IronPort M-Series セキュリティ管理アプライアンス」（P.17-563）を参照してください。**

工場出荷時の設定を持つ IronPort アプライアンスをネットワークに複数接続する場合は、各 IronPort アプライアンスのデフォルト IP アドレスを順に再設定しながら、1 台ずつ追加してください。

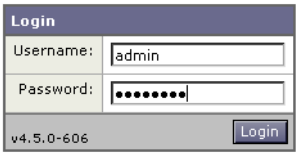
Web ベースのグラフィカル ユーザ インターフェイス（GUI）の利用

Web ベースの Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を利用するには、Web ブラウザを開き、192.168.42.42 を表示します。



ログイン画面が表示されます。

図 3-4　アプライアンスへのログイン



下記のユーザ名およびパスワードを入力してアプライアンスにログインします。

工場出荷時のデフォルト ユーザ名とパスワード

- ユーザ名：**admin**
- パスワード：**ironport**

（注）　アイドル時間が 30 分以上続くか、ログアウトしないでブラウザを閉じた場合は、セッションがタイムアウトされます。その場合は、ユーザ名およびパスワードの再入力が要求されます。System Setup Wizard の実行中にセッションがタイムアウトした場合は、最初からやり直す必要があります。

Web ベースの System Setup Wizard の実行

System Setup Wizard を起動するには、「Web ベースのグラフィカル ユーザ インターフェイス（GUI）の利用」（P.3-51）の説明に従って、グラフィカル ユーザ インターフェイスにログインします。[System Administration] タブで、左方のリンク リストから [System Setup Wizard] をクリックします。新規のシステム（先行リリースの AsyncOS からのアップグレードなし）の場合は、ブラウザが System Setup Wizard に自動的にリダイレクトされます。

System Setup Wizard では、5 つのカテゴリに分割された、次のコンフィギュレーション タスクが順に示されます。

ステップ 1　[Start]

- ライセンス契約書の参照と受諾

ステップ 2　[System]

- アプライアンスのホスト名の設定

- アラート設定値、レポート配信設定値、および AutoSupport の設定
- システム時刻設定値および NTP サーバの設定
- admin パスワードのリセット
- SenderBase Network Participation のイネーブル化

ステップ 3　[Network]

- デフォルト ルータおよび DNS 設定値の定義
- 次のようなネットワーク インターフェイスのイネーブル化および設定
  着信メールの設定（インバウンド リスナー）
  SMTP ルートの定義（任意）
  発信メール（アウトバウンド リスナー）の設定およびアプライアンスを介してメールをリレーできるシステムの定義（任意）

ステップ 4　[Security]

- SenderBase 評価フィルタリングのイネーブル化
- アンチスパム サービスのイネーブル化
- IronPort スパム検疫のイネーブル化
- Anti-Virus サービスのイネーブル化
- ウイルス感染フィルタサービスのイネーブル化

ステップ 5　[Review]

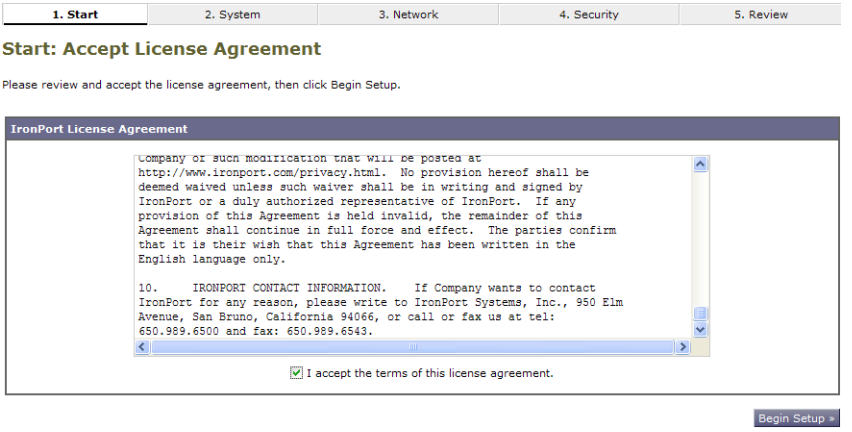
- セットアップのレビューおよび設定のインストール

各手順を完了して [Next] をクリックしながら、System Setup Wizard を進めてください。[Previous] をクリックすると、前の手順に戻ることができます。プロセスの最後に、変更を確定するようプロンプトが表示されます。確定するまで、変更は有効になりません。[Next] をクリックしたときに必須フィールドをブランクにした場合（または正しくない情報を入力した場合）は、そのフィールドの外枠が赤で表示されます。修正し、もう一度 [Next] をクリックしてください。

手順 1：[Start]

ライセンス契約書の参照から開始します。ライセンス契約書を参照し、同意する場合は、同意することを示すボックスをオンにし、[Begin Setup] をクリックして続行します。

図 3-5　System Setup Wizard：手順 1：[Start]



契約書の文面は次の場所でも参照できます。
`https://support.ironport.com/license/eula.html`

手順 2：[System]

ホスト名の設定

IronPort アプライアンスの完全修飾ホスト名を定義します。この名前は、ネットワーク管理者が割り当てる必要があります。

システム アラートの設定

ユーザの介入を必要とするシステム エラーが発生した場合、IronPort AsyncOS では、電子メールでアラート メッセージを送信します。このアラートの送信先として使用する電子メール アドレス（複数可）を入力します。

システム アラートを受信する電子メール アドレスを 1 つ以上追加する必要があります。単一の電子メール アドレスか、カンマで区切った複数アドレスを入力します。当初、この電子メール受信者は、ディレクトリ獲得攻撃対策アラート以外のすべてのタイプおよびすべてのレベルのアラートを受信します。後で、アラート コンフィギュレーションをさらに詳細化できます。詳細については、「アラート」（P.15-495）を参照してください。

レポート配信の設定

デフォルトのスケジュール済みレポートの送信先にするアドレスを入力します。この値をブランクにしても、スケジュール済みレポートは引き続き実行されます。スケジュール済みレポートは配信されませんが、アプライアンス上にアーカイブされます。

時間の設定

IronPort アプライアンス上の時間帯を設定して、メッセージ ヘッダーおよびログ ファイルのタイムスタンプが正確になるようにします。ドロップダウン メニューを使用して時間帯を見つけるか、GMT オフセットによって時間帯を定義します（詳細については、「GMT オフセットの選択」（P.15-542）を参照してください）。

システム クロック時刻は、後で手動によって設定するか、Network Time Protocol（NTP; ネットワーク タイム プロトコル）を使用してネットワーク上またはインターネット上の他のサーバと時刻を同期することもできます。デフォルトでは、IronPort Systems のタイム サーバ（`time.IronPort.com`）と時刻を同期するエントリ 1 つが、IronPort アプライアンスにすでに設定されています。

パスワードの設定

admin アカウントのパスワードを設定します。この手順は必須です。IronPort AsyncOS の admin アカウントのパスワードを変更する場合、新しいパスワードは、6 文字以上でなければなりません。パスワードは、必ず安全な場所に保管してください。

SenderBase ネットワークへの参加

SenderBase は、電子メール管理者による送信者の調査、電子メールの正規送信元の識別、およびスパム送信者のブロックに役立つように設計された、電子メールの評価サービスです。

SenderBase ネットワークへの参加に同意した場合、IronPort は、組織の電子メール トラフィックを集約した統計情報を収集します。これには、メッセージ属性の要約データおよび IronPort アプライアンスがどのように各種メッセージを処理したかに関する情報のみが含まれています。たとえば、IronPort は、メッセージの本文もメッセージの件名も収集しません。個人を特定できる情報や、組織を特定する情報は、機密情報として扱われます。収集されるデータの例など、

SenderBase の詳細については、[Click here for more information about what data is being shared] リンクをクリックしてください（「よくあるご質問」（P.13-423）を参照）。

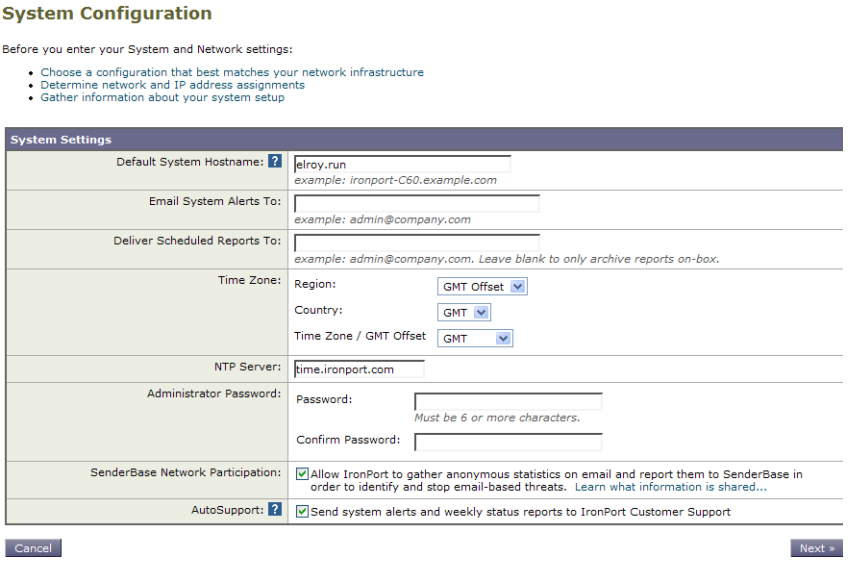
SenderBase ネットワークに参加する場合は、[Allow IronPort to gather anonymous statistics on email and report them to SenderBase in order to identify and stop email-based threats] の横のボックスをオンにし、[Accept] をクリックします。

詳細については、第 13 章「SenderBase Network Participation」を参照してください。

AutoSupport のイネーブル化

IronPort AutoSupport 機能（デフォルトでイネーブル）では、ご使用の IronPort アプライアンスに関する問題を IronPort カスタマー サポート チームが認識しておくことで、適切なサポートを提供できるようにします（詳細は、「IronPort AutoSupport」（P.15-498）を参照してください）。

図 3-6　System Setup Wizard：手順 2：[System]



[Next] をクリックして続行します。

手順 3：[Network]

手順 3 では、デフォルト ルータ（ゲートウェイ）を定義し、DNS 設定値を設定してから、Data 1 インターフェイス、Data 2 インターフェイス、および Management インターフェイスを設定することにより、電子メールの受信やリレーを行うようにアプライアンスをセットアップします。

DNS とデフォルト ゲートウェイの設定

ネットワーク上のデフォルト ルータ（ゲートウェイ）の IP アドレスを入力します。

次に、Domain Name Service（DNS）設定値を設定します。IronPort AsyncOS には、インターネットのルート サーバに直接問い合わせできる、高性能な内部 DNS リゾルバ/キャッシュが組み込まれていますが、指定した DNS サーバを使用することもできます。独自のサーバを使用する場合は、各 DNS サーバの IP アドレスおよびホスト名を指定する必要があります。System Setup Wizard から入力できる DNS サーバは 4 台までです。入力した DNS サーバの初期プライオリティは 0 になっていることに注意してください。詳細については、「ドメイン ネーム システム（DNS）設定値の設定」（P.15-531）を参照してください。

（注）　アプライアンスでは、着信接続のための DNS ルックアップを実行するために、稼動中の DNS サーバを利用できる必要があります。アプライアンスをセットアップするときにアプライアンスからアクセス可能な稼動中の DNS サーバを指定できない場合は、[Use Internet Root DNS Server] を選択するか、Management インターフェイスの IP アドレスを一時的に指定することを回避策として、System Setup Wizard を完了できます。

ネットワーク インターフェイスの設定

IronPort アプライアンスには、マシンの物理ポートに関連付けられたネットワーク インターフェイスがあります。たとえば、C650/660/670、C350/360/370、および X1050/1060/1070 アプライアンスでは、3 個の物理イーサネット インターフェイスが使用可能です。C150/160 アプライアンスでは、2 個の物理イーサネット インターフェイスが使用可能です。

インターフェイスを使用するには、[Enable] チェックボックスをオンにし、IP アドレス、ネットワーク マスク、および完全修飾ホスト名を指定します。入力する IP アドレスは、DNS レコードに反映されている、インバウンド メール用のアドレスである必要があります。通常、このアドレスには、DNS で MX レコードと関連付けられています。

各インターフェイスは、メールを受け入れる（着信）、電子メールをリレーする（発信）、またはアプライアンスを管理するように設定できます。セットアップ時は、このいずれかに制限されます。通常は、インターフェイスの 1 つを着信用、1 つを発信用、および 1 つをアプライアンス管理用に使用します。C150 アプライアンスおよび C160 アプライアンスでは、1 つのインターフェイスを着信と発信の両方のメール用に使用し、もう 1 つのインターフェイスを管理用に使用することが一般的です。

インターフェイスの 1 つは、電子メールの受信用に設定する必要があります。

アプライアンスのいずれかの物理イーサネット インターフェイスに論理 IP アドレスを割り当てて、設定します。Data 1 イーサネット ポートと Data 2 イーサネット ポートの両方を使用する場合は、両方の接続に対してこの情報が必要です。

C650/660/670、C350/360/370、および X1050/1060/1070 をご利用のお客様：IronPort では、パブリック リスナーを介してインバウンド電子メールを受信するためにインターネットに直接接続するように物理イーサネット ポートの 1 つを使用し、プライベート リスナーを介してアウトバウンド電子メールをリレーするために内部ネットワークに直接接続するようにもう 1 つの物理イーサネット ポートを使用することを推奨しています。

C150/160 をご利用のお客様：通常は、インバウンド電子メールの受信とアウトバウンド電子メールのリレーの両方のために、リスナー 1 つの物理イーサネット ポート 1 つだけが、System Setup Wizard によって設定されます。

「物理イーサネット ポートへの論理 IP アドレスのバインド」（P.3-46）を参照してください。

次の情報が必要です。

- ネットワーク管理者によって割り当てられた **IP アドレス。**
- インターフェイスの**ネットマスク**。

  ネットマスクは、標準のドット付き 10 進形式にするか、16 進形式にすることができます。

- （任意）IP アドレスの完全修飾ホスト名。

（注）　同じサブネットに含まれる IP アドレスを、別々の物理イーサネット インターフェイスには設定できません。ネットワークおよび IP アドレスのコンフィギュレーションの詳細については、付録 B「ネットワーク アドレスと IP アドレスの割り当て」を参照してください。

メールの受け入れ

メールを受け入れるようにインターフェイスを設定する場合は、次の内容を定義します。

- 受け入れるメールの宛先のドメイン
- 各ドメインの宛先（SMTP ルート）（任意）

[Accept Incoming Mail] のチェックボックスをオンにし、メールを受け入れるインターフェイスを設定します。受け入れるメールのドメインの名前を入力します。

[Destination] を入力します。これは、SMTP ルートまたは指定したドメイン宛ての電子メールをルーティングするマシンの名前です。

これは、最初の SMTP ルート エントリです。SMTP ルート テーブルを使用すると、入力する各ドメイン宛てのすべての電子メール（Recipient Access Table（RAT; 受信者アクセス テーブル）エントリとも呼ぶ）を特定の Mail Exchange（MX）ホストにリダイレクトできます。標準インストールの場合、SMTP ルート テーブルでは、特定のグループウェア サーバ（たとえば、Microsoft Exchange）やインフラストラクチャの電子メール配信における次のホップを定義します。

たとえば、ドメイン `example.com` かそのすべてのサブドメイン `.example.com` のいずれか宛てメールを受け入れた場合に、グループウェア サーバ `exchange.example.com` にルーティングするよう指定するルートを定義できます。

ドメインおよび宛先は、複数入力できます。ドメインをさらに追加するには、[Add Row] をクリックします。行を削除するには、ゴミ箱アイコンをクリックします。

（注）この手順での SMTP ルートの設定は任意です。SMTP ルートを定義していない場合は、リスナーが受信した着信メールの配信ホストの検索と決定に、DNS が使用されます（詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Routing Email for Local Domains」を参照してください）。

ドメインを受信者アクセス テーブルに少なくとも 1 つ追加する必要があります。ドメイン、たとえば、example.com を入力します。example.net のいずれのサブドメイン宛てのメールとも必ず一致させるために、ドメイン名の他に .example.net も受信者アクセス テーブルに入力します。詳細については、「受信者の定義」（P.5-178）を参照してください。

メール リレー（任意）

メールをリレーするようにインターフェイスを設定するときは、アプライアンスを介して電子メールのリレーを許可するよう、システムを定義します。

リスナーのホスト アクセス テーブルにある RELAYLIST 内のエントリを使用します。詳細については、「送信者グループの構文」（P.5-132）を参照してください。

[Relay Outgoing Mail] のチェックボックスをオンにし、メールをリレーするインターフェイスを設定します。アプライアンスを介してメールをリレーできるホストを入力します。

アウトバウンド メールをリレーするようにインターフェイスを設定すると、そのインターフェイスを使用するパブリック リスナーが設定されている場合を除き、そのインターフェイスの SSH が System Setup Wizard によってオンにされます。

次の例では、2 つのインターフェイスが作成されます。

- 192.168.42.42 は、引き続き Management インターフェイスに設定されます。
- 192.168.1.1 は、Data 1 イーサネット インターフェイスでイネーブルになります。.example.com で終わるドメイン宛てのメールを受け入れるように設定されており、exchange.example.com 宛ての SMTP ルートが定義されています。
- 192.168.2.1 は、Data 2 イーサネット インターフェイスでイネーブルになります。exchange.example.com からのメールをリレーするように設定されます。

（注）　次の例は、X1050/1060/1070、C650/660/670、および C350/360/370 アプライアンスに該当します。C150/160 アプライアンスの場合は、着信と発信の両方のメール用に Data 2 インターフェイスを設定し、アプライアンス管理用に Data 1 インターフェイスを設定することが一般的です（「C150/160 の設置」（P.3-61）を参照）。

図 3-7　ネットワーク インターフェイス：Management および追加の IP アドレス x 2（トラフィックの分離）

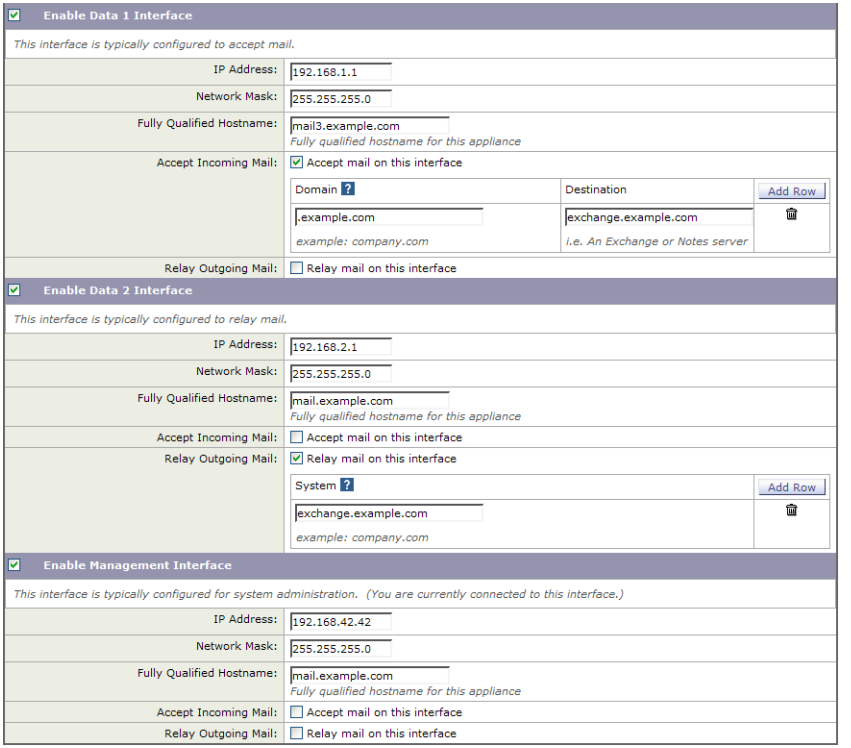


図 3-2（P.3-42）のようなネットワークを構築する場合に、この設定を使用します。

C150/160 の設置

すべての電子メール トラフィック用に単一の IP アドレスを設定する場合（トラフィックの分離なし）、System Setup Wizard の手順 3 は次のようになります。

図 3-8　ネットワーク インターフェイス：着信と発信の（分離されない）トラフィック用に 1 つの IP アドレス

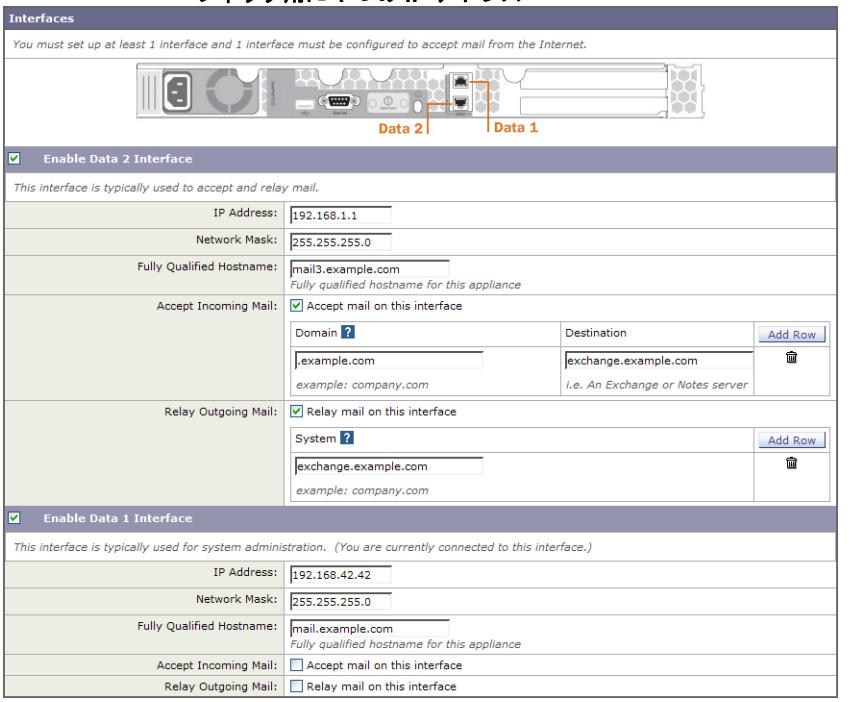


図 3-3（P.3-43）のようなネットワークを構築する場合に、この設定を使用します。

[Next] をクリックして続行します。

手順 4：[Security]

手順 4 では、アンチスパム設定値およびアンチウイルス設定値を設定します。アンチスパム オプションには、SenderBase 評価フィルタリングとアンチスパム スキャン エンジンの選択が含まれます。アンチウイルスについては、ウイルス感染フィルタおよび Sophos または McAfee のアンチウイルス スキャンをイネーブルにできます。

SenderBase 評価フィルタリングのイネーブル化

SenderBase 評価サービスは、スタンドアロンのアンチスパム ソリューションとしても使用できますが、IronPort Anti-Spam など、コンテンツ ベースのアンチスパム システムの有効性を高めることを主な目的としています。

SenderBase 評価サービス（http://www.SenderBase.org）には、リモート ホストの接続 IP アドレスに基づいて、陽性と疑わしいスパムをユーザが拒否したり、制限したりするための正確で柔軟な方法が備わっています。SenderBase 評価サービスは、特定の送信元からのメッセージがスパムである確率に基づく評点を返します。SenderBase 評価サービスは、電子メール メッセージの量をグローバルに表示して、電子メールの送信元の識別とグループ化を容易にする方法でデータを編成している点で独特です。IronPort では、SenderBase 評価フィルタリングをイネーブルにすることを強く推奨しています。

イネーブルにした SenderBase 評価フィルタリングは、着信（受け入れ）リスナーで適用されます。

アンチスパム スキャンのイネーブル化

IronPort アプライアンスには、IronPort Anti-Spam ソフトウェアの 30 日間評価キーが付属している場合があります。System Setup Wizard のこの部分では、アプライアンスで IronPort Anti-Spam をグローバルでイネーブルにすることを選択できます。アンチスパム サービスをイネーブルにしないことも選択できます。

アンチスパム サービスをイネーブルにする場合は、スパムおよび陽性と疑わしいスパム メッセージをローカル IronPort スパム検疫エリアに送信するように、AsyncOS を設定できます。IronPort スパム検疫は、アプライアンスのエンドユーザ検疫として機能します。エンドユーザのアクセス権を設定していないうちは、管理者だけが検疫を利用できます。

アプライアンスで使用可能なすべての IronPort Anti-Spam 設定オプションについては、第 8 章「アンチスパム」を参照してください。IronPort スパム検疫については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」を参照してください。

アンチウイルス スキャンのイネーブル化

IronPort アプライアンスには、Sophos Anti-Virus または McAfee Anti-Virus スキャン エンジンの 30 日間評価キーが付属している場合があります。System Setup Wizard のこの部分では、アプライアンスでアンチウイルス スキャン エンジンをグローバルでイネーブルにすることを選択できます。

アンチウイルス スキャン エンジンをイネーブルにすると、デフォルトの着信メール ポリシーおよびデフォルトの発信メール ポリシーの*両方*についてイネーブルになります。IronPort アプライアンスでは、メールをスキャンしてウイルスを検出しますが、感染した添付ファイルの修復は行いません。アプライアンスでは、感染したメッセージをドロップします。

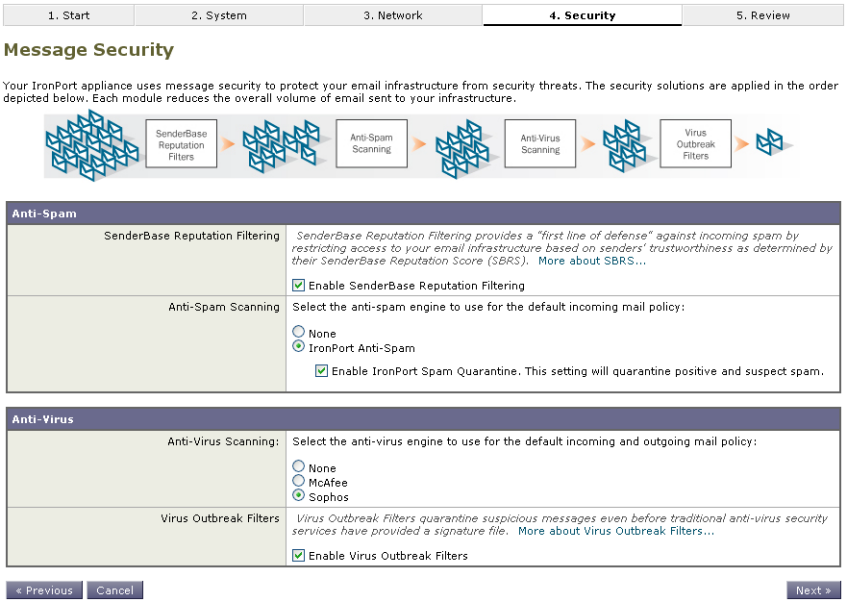
アプライアンスで使用可能なすべてのアンチウイルス コンフィギュレーション オプションについては、第 9 章「アンチウイルス」を参照してください。

ウイルス感染フィルタのイネーブル化

IronPort アプライアンスには、ウイルス感染フィルタの 30 日間評価キーが付属している場合があります。ウイルス感染フィルタは、疑わしいメッセージを検疫することによって、従来のアンチウイルス セキュリティ サービスを新しいウイルス シグニチャ ファイルで更新できるまで新しいウイルスの拡散に対抗する、「防衛の最前線」になります。

詳細については、第 10 章「ウイルス感染フィルタ」を参照してください。

図 3-9　System Setup Wizard：手順 4：メッセージ セキュリティの設定

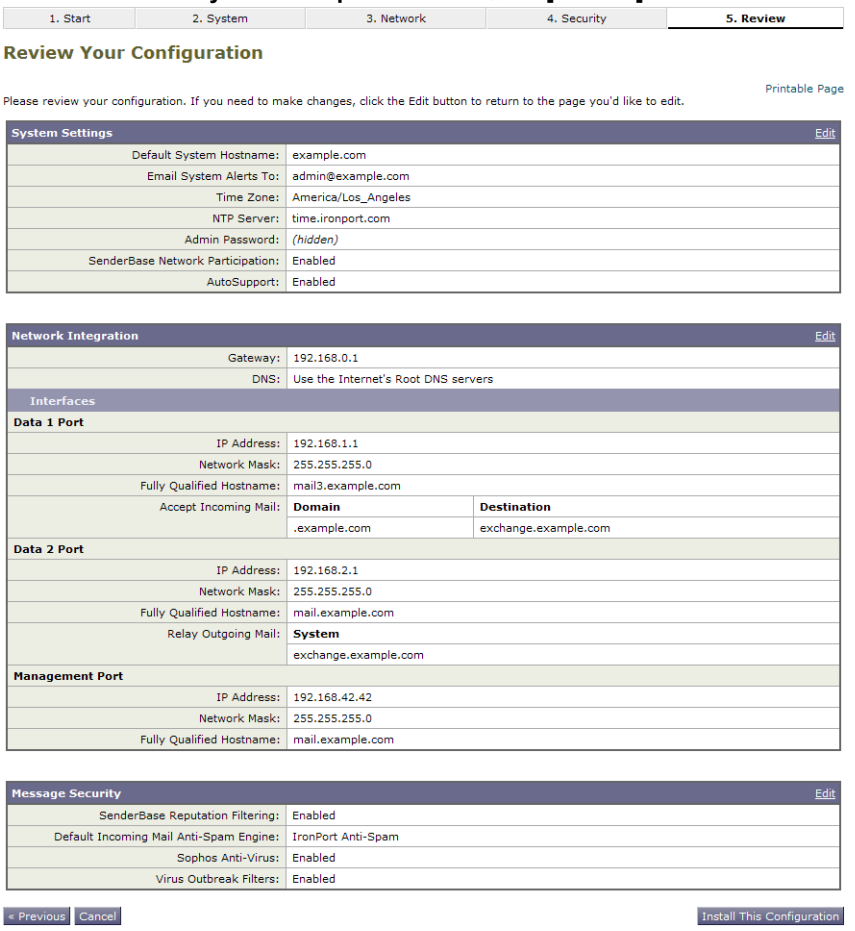


[Next] をクリックして続行します。

手順 5：[Review]

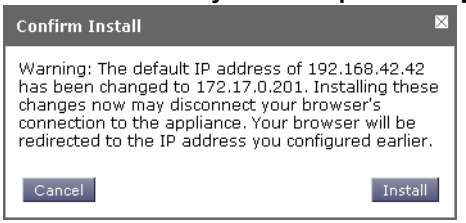
設定情報のサマリーが表示されます。[System Settings]、[Network Integration]、および [Message Security] の情報は、[Previous] ボタンをクリックするか、各セクションの右上にある対応する [Edit] リンクをクリックすることによって編集できます。変更を加える手順まで戻った場合は、再度このレビュー ページに至るまで、残りの手順を進める必要があります。以前に入力した設定は、すべて残っています。

図 3-10　System Setup Wizard：手順 5：[Review]



表示されている情報が要件を満たしていれば、[Install This Configuration] をクリックします。確認のダイアログが表示されます。[Install] をクリックして、新しい設定をインストールします。

図 3-11　System Setup Wizard：[Confirm Install]



これで、IronPort アプライアンスは、電子メールを送信できる状態になりました。

（注） アプライアンスへの接続に使用するインターフェイス（X1050/1060/1070、C650/660/670、および C350/360/370 システムの Management インターフェイスまたは C150/160 システムの Data 1 インターフェイス）の IP アドレスをデフォルトから変更した場合は、[Install] をクリックすると、現在の URL（http://192.168.42.42）への接続が失われます。ただし、ブラウザは、新しい IP アドレスにリダイレクトされます。

システム セットアップが完了すると、複数のアラート メッセージが送信されます。詳細については、「即時アラート」（P.3-88）を参照してください。

Active Directory の設定

System Setup Wizard によって電子メール セキュリティ アプライアンスに設定が正しくインストールされると、Active Directory Wizard が表示されます。ネットワークで Active Directory サーバを稼動している場合は、Active Directory Wizard を使用して、Active Directory サーバ用の LDAP サーバ プロファイルの設定と、受信者検証用リスナーの割り当てを行う必要があります。Active Directory を使用していないか、後で設定する場合は、[Skip this Step] をクリックします。Active Directory Wizard は、[System Administration] > [Active Directory Wizard] ページで実行できます。Active Directory およびその他の LDAP プロファイルは、[System Administration] > [LDAP] ページでも設定できます。

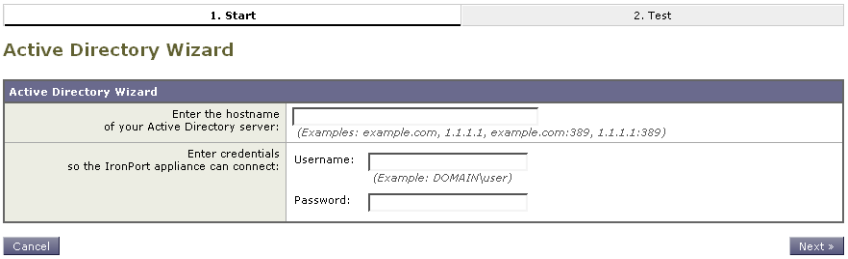
Active Directory Wizard では、認証方式、ポート、ベース DN、および SSL をサポートするかどうかなど、LDAP サーバ プロファイルの作成に必要なシステム情報を取得します。Active Directory Wizard では、LDAP サーバ プロファイル用の LDAP の受け入れクエリーおよびグループ クエリーも作成します。

Active Directory Wizard によって LDAP サーバ プロファイルが作成されてから、[System Administration] > [LDAP] ページを使用して新規プロファイルを表示し、さらに変更を加えます。

Active Directory Wizard を使用する手順は、次のとおりです。

ステップ 1　[Active Directory Wizard] ページで [Run Active Directory Wizard] をクリックします。

図 3-12　Active Directory Wizard：手順 1：[Start]



ステップ 2　Active Directory サーバのホスト名を入力します。

ステップ 3　認証要求のためのユーザ名およびパスワードを入力します。

ステップ 4　[Next] をクリックして続行します。

Active Directory サーバへの接続が Active Directory Wizard によってテストされます。成功すると、[Test Directory Settings] ページが表示されます。

図 3-13　Active Directory Wizard：手順 2：[Directory Lookup Test]

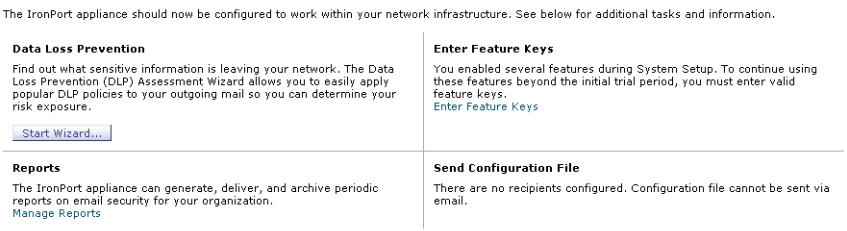
ステップ 5　Active Directory に存在すると判明している電子メール アドレスを入力し、[Test] をクリックすることによって、ディレクトリ設定値をテストします。接続ステータス フィールドに結果が表示されます。

ステップ 6　[Done] をクリックします。

次の手順

Active Directory Wizard と連携するようにアプライアンスを正常に設定するか、処理をスキップすると、[System Setup Next Steps] ページが表示されます。

図 3-14　システム セットアップの完了



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

コマンド ライン インターフェイス（CLI）へのアクセス

CLI へのアクセスは、「アプライアンスへの接続」（P.3-45）で選択した管理接続方式によって異なります。工場出荷時のデフォルト ユーザ名およびパスワードを次に示します。当初は、admin ユーザ アカウントだけが CLI にアクセスできます。admin アカウントを介してコマンド ライン インターフェイスに初回アクセスしたうえで、さまざまな許可レベルの他のユーザを追加できます（ユーザの追加については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」を参照してください）。System Setup Wizard で、admin アカウントのパスワードを変更するよう要求されます。admin アカウントのパスワードは、password コマンドを使用して、任意の時点で直接再設定することもできます。

イーサネットを介して接続する場合は、工場出荷時のデフォルト IP アドレスの 192.168.42.42 を使用して SSH セッションまたは Telnet セッションを開始します。SSH は、ポート 22 を使用するように設定されています。Telnet は、ポート 23 を使用するように設定されています。下記のユーザ名とパスワードを入力します。

シリアル接続を介して接続する場合は、パーソナル コンピュータのシリアル ケーブルが接続されている通信ポートを使用して端末セッションを開始します。「アプライアンスへの接続」（P.3-45）に示されているシリアル ポートの設定値を使用してください。下記のユーザ名とパスワードを入力します。

下記のユーザ名およびパスワードを入力してアプライアンスにログインします。

工場出荷時のデフォルト ユーザ名とパスワード

- ユーザ名：**admin**
- パスワード：**ironport**

次の例を参考にしてください。

```
login: admin
password: ironport
```

コマンド ライン インターフェイス（CLI）System Setup Wizard の実行

CLI バージョンの System Setup Wizard の手順は、基本的に GUI バージョン同様ですが、次のわずかな例外があります。

- CLI バージョンには、Web インターフェイスをイネーブルにするプロンプトが含まれています。
- CLI バージョンでは、作成する各リスナーのデフォルト メール フロー ポリシーを編集できます。
- CLI バージョンには、グローバルなアンチウイルス セキュリティ設定値およびウイルス感染フィルタ セキュリティ設定値を設定するためのプロンプトが含まれています。
- CLI バージョンでは、システム セットアップの完了後に LDAP プロファイルを作成することを指示されません。`ldapconfig` コマンドを使用して LDAP プロファイルを作成してください。

System Setup Wizard を実行するには、コマンド プロンプトで `systemsetup` と入力します。

```
IronPort> systemsetup
```

システムを再設定するよう System Setup Wizard から警告が出されます。アプライアンスをまったく初めて設置する場合か、既存の設定を完全に上書きする場合は、この質問に [Yes] と回答します。

```
WARNING: The system setup wizard will completely delete any existing

'listeners' and all associated settings including the 'Host Access
Table' - mail operations may be interrupted.



Are you sure you wish to continue? [Y]> Y
```

（注）　以降のシステム セットアップ手順については、次で説明します。CLI バージョンの System Setup Wizard 対話の例には、「Web ベースの System Setup Wizard の実行」（P.3-52）で説明した GUI バージョンの System Setup Wizard から逸脱する部分だけを含めてあります。

admin パスワードの変更

まず、IronPort AsyncOS の admin アカウントのパスワードを変更します。続行するには、現在のパスワードを入力する必要があります。新しいパスワードは 6 文字以上の長さである必要があります。パスワードは、必ず安全な場所に保管してください。パスワードの変更は、システム セットアップ プロセスを終了した時点で有効になります。

ライセンス契約書の受諾

表示されるソフトウェア使用許諾契約を参照して受諾します。

ホスト名の設定

次に、IronPort アプライアンスの完全修飾ホスト名を定義します。この名前は、ネットワーク管理者が割り当てる必要があります。

論理 IP インターフェイスの割り当てと設定

次の手順では、Management（X1050/1060/1070、C650/660/670、および C350/360/370 アプライアンス）または Data 1（C150/160 アプライアンス）物理イーサネット インターフェイス上に論理 IP インターフェイスの割り当てと設定を行います。続いて、アプライアンス上で使用可能な他の任意の物理イーサネット インターフェイス上に論理 IP インターフェイスを設定するよう指示されます。

各イーサネット インターフェイスに複数の IP インターフェイスを割り当てることができます。IP インターフェイスは、IP アドレスおよびホスト名を物理イーサネット インターフェイスと関連付ける論理構成概念です。Data 1 と Data 2 の両方のイーサネット ポートを使用する場合は、両方の接続用に IP アドレスとホスト名が必要です。

X1050/1060/1070、C650/660/670、および C350/360/370 をご利用のお客様：IronPort では、パブリック リスナーを介してインバウンド電子メールを受信するためにインターネットに直接接続するように物理イーサネット ポートの 1 つを使用し、プライベート リスナーを介してアウトバウンド電子メールをリレーするために内部ネットワークに直接接続するようにもう 1 つの物理イーサネット ポートを使用することを推奨しています。

C150/160 をご利用のお客様：デフォルトでは、インバウンド電子メールの受信とアウトバウンド電子メールのリレーの両方のために、リスナー 1 つの物理イーサネット ポート 1 つだけが、`systemsetup` コマンドによって設定されます。

（注） アウトバウンド メールをリレーするようにインターフェイスを設定すると、そのインターフェイスを使用するパブリック リスナーが設定されている場合を除き、そのインターフェイスの SSH がシステムによってオンにされます。

次の情報が必要です。

- 後でその IP インターフェイスを参照するために作成した**名前**（ニックネーム）。たとえば、イーサネット ポートの 1 つをプライベート ネットワーク用に使用し、もう 1 つをパブリック ネットワーク用にしている場合は、それぞれ PrivateNet および PublicNet などの名前を付けます。

（注） インターフェイス用に定義する名前では、大文字と小文字が区別されます。AsyncOS では、2 つの同じインターフェイス名を作成することはできません。たとえば、**`Privatenet`** および **`PrivateNet`** という名前は、*異なる*（一意の）2 つの名前であると見なされます。

- ネットワーク管理者によって割り当てられた **IP アドレス**。
- インターフェイスの**ネットマスク**。ネットマスクは、標準のドット付き 10 進形式にするか、16 進形式にすることができます。

（注） 同じサブネットに含まれる IP アドレスを、別々の物理イーサネット インターフェイスには設定できません。ネットワークおよび IP アドレスのコンフィギュレーションの詳細については、付録 B「ネットワーク アドレスと IP アドレスの割り当て」を参照してください。

デフォルト ゲートウェイの指定

systemsetup コマンドの次の部分では、ネットワークのデフォルト ルータ（ゲートウェイ）の IP アドレスを入力します。

Web インターフェイスのイネーブル化

systemsetup コマンドの次の部分では、アプライアンス（Management イーサネット インターフェイス）の Web インターフェイスをイネーブルにします。Secure HTTP（https）を介して Web インターフェイスを実行することもできます。HTTPS を使用する場合は、独自の証明書をアップロードするまで、デモ証明書が使用されます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Enabling a Certificate for HTTPS」を参照してください。

DNS 設定値の設定

次に、Domain Name Service（DNS）設定値を設定します。IronPort AsyncOS には、インターネットのルート サーバに直接問い合わせできる、高性能な内部 DNS リゾルバ/キャッシュが組み込まれていますが、独自の DNS サーバを使用することもできます。独自のサーバを使用する場合は、各 DNS サーバの IP アドレスおよびホスト名を指定する必要があります。必要な数の DNS サーバを入力できます（各サーバのプライオリティは 0 になります）。デフォルトでは、独自の DNS サーバのアドレスを入力するよう、systemsetup から示されます。

リスナーの作成

特定の IP インターフェイスに対して設定される、インバウンド電子メール処理サービスをリスナーによって管理します。リスナーは、内部システムまたはインターネットのいずれかから IronPort アプライアンスに着信する電子メールだけに適用されます。IronPort AsyncOS は、メッセージを受け入れて受信者のホストにリレーするために、リスナーを使用してメッセージが満たす必要のある基準を指定します。リスナーは、上記で指定した IP アドレス用に実行されている電子メール リスナーであると見なすことができます（「SMTP デーモン」と見なすことさえ可能）。

X1050/1060/1070、C650/660/670、および C350/360/370 をご利用のお客様：デフォルトでは、パブリックとプライベートのリスナー 1 つずつの合計 2 つのリスナーが systemsetup コマンドによって設定されます（使用可能なリスナー タイプの詳細については、「電子メールを受信するためのゲートウェイの設定」（P.5-107）を参照してください）。

C150/160 をご利用のお客様：デフォルトでは、インターネットからのメールの受信と内部ネットワークからの電子メールのリレーの両方に対応するパブリック リスナー 1 つが systemsetup コマンドによって設定されます。「C150/160 のリスナーの例」（P.3-80）を参照してください。

リスナーを定義するときは、次の属性を指定します。

- 後でそのリスナーを参照するために作成した**名前**（ニックネーム）。たとえば、インターネットに配信される、内部システムからの電子メールを受け入れるリスナーには、OutboundMail などの名前を付けます。
- 電子メールの受信に使用する、systemsetup コマンドで先に作成したいずれかの IP インターフェイス。
- 電子メールのルーティング先にするマシンの名前（パブリック リスナーのみ）。これは、最初の smtproutes エントリです。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Routing Email for Local Domains」を参照してください。
- パブリック リスナーで SenderBase Reputation Score（SBRS; SenderBase 評価スコア）に基づくフィルタリングをイネーブルにするかどうか。イネーブルにする場合は、[Conservative]、[Moderate]、または [Aggressive] から設定値を選択することも指示されます。
- ホストごとのレート制限：1 時間あたりにリモート ホストから受信する受信者の最大数（パブリック リスナーのみ）。
- 受け入れる電子メールの宛先にされている受信者ドメインまたは特定のアドレス（パブリック リスナーの場合）、またはアプライアンスを介した電子メールのリレーを許可するシステム（プライベート リスナーの場合）。これらは、リスナーの受信者アクセス テーブルおよびホスト アクセス テーブルの最初のエントリです。詳細については、「送信者グループの構文」（P.5-132）および「パブリック リスナー（RAT）上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ」（P.5-177）を参照してください。

パブリック リスナー

（注）　パブリック リスナーおよびプライベート リスナーを作成する次の例は、X1050/1060/1070、C650/660/670、および C350/360/370 をご利用のお客様だけに適用されます。IronPort C150/160 をご利用のお客様は、次の「C150/160 のリスナーの例」（P.3-80）にスキップしてください。

`systemsetup` コマンドのこの例の部分では、PublicNet IP インターフェイスで実行されるように InboundMail というパブリック リスナーを設定します。続いて、ドメイン `example.com` 宛てのすべての電子メールを受け入れるように設定します。Mail Exchange `exchange.example.com` への初期 SMTP ルートを設定します。レート制限をイネーブルにし、パブリック リスナーに対して単一のホストから受信する 1 時間あたりの受信者の最大値に 4500 を指定します。

（注）　1 台のリモート ホストから 1 時間あたりに受信する最大受信者数に入力する値は、完全に自由裁量の値です。通常は、管理対象の電子メールを所有している企業の規模に比例します。たとえば、1 時間に 200 通のメッセージを送信する送信者は、「スパム送信者」（未承諾の大量電子メールの送信者）である可能性がありますが、10,000 人規模の会社に対するすべての電子メールを処理する IronPort アプライアンスを設定する場合は、単一のリモート ホストからの 1 時間あたりのメッセージが 200 通であっても、理にかなった値である可能性があります。対照的に、50 人規模の会社の場合に、1 時間あたり 200 通のメッセージを送信してくる送信者は、おそらく、明らかなスパム送信者です。パブリック リスナーで、企業へのインバウンド電子メールのレート制限をイネーブルにする（量を絞る）場合は、適切な値を選択してください。デフォルトのホスト アクセス ポリシーの詳細については、「送信者グループの構文」（P.5-132）を参照してください。

次に、リスナーのデフォルトのホスト アクセス ポリシーが受け入れられます。

```
You are now going to configure how the IronPort C60 accepts mail by

creating a "Listener".

Please create a name for this listener (Ex: "InboundMail"):

[]> InboundMail
```

```
Please choose an IP interface for this Listener.

1. Management (192.168.42.42/24: mail3.example.com)

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 3


Enter the domains or specific addresses you want to accept mail for.


Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

Usernames such as "postmaster@" are allowed.

Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are
allowed.

Separate multiple addresses with commas.

[]> example.com


Would you like to configure SMTP routes for example.com?  [Y]> y


Enter the destination mail server which you want mail for example.com
to be delivered. Separate multiple entries with commas.

[]> exchange.example.com
```

```
Do you want to enable rate limiting for this listener? (Rate limiting
defines the maximum number of recipients per hour you are willing to
receive from a remote domain.) [Y]> y


Enter the maximum number of recipients per hour to accept from a
remote domain.

[]> 4500


Default Policy Parameters

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

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 1,000

Maximum Number Of Messages Per Connection: 1,000

Maximum Number Of Recipients Per Message: 1,000

Maximum Number Of Recipients Per Hour: 4,500

Maximum Recipients Per Hour SMTP Response:

    452 Too many recipients received this hour

Use SenderBase for Flow Control:  Yes

Virus Detection Enabled:  Yes

Allow TLS Connections: No

Would you like to change the default host access policy?  [N]> n


Listener InboundMail created.
```

```
Defaults have been set for a Public listener.

Use the listenerconfig->EDIT command to customize the listener.

*****
```

プライベート リスナー

systemsetup コマンドのこの例の部分では、PrivateNet IP インターフェイスで実行されるように OutboundMail というプライベート リスナーを設定します。次に、ドメイン example.com に含まれる任意のホスト宛てのすべての電子メールをリレーするように設定します（エントリ .example.com の先頭のドットに注意してください）。

続いて、レート制限（イネーブルでない）のデフォルト値およびこのリスナーのデフォルト ホスト アクセス ポリシーが受け入れられます。

プライベート リスナーのデフォルト値は、先に作成したパブリック リスナーのデフォルト値と異なることに注意してください。詳細については、「パブリック リスナーとプライベート リスナー」（P.5-110）を参照してください。

```
Do you want to configure the C60 to relay mail for internal hosts?
[Y]> y



Please create a name for this listener (Ex: "OutboundMail"):

[]> OutboundMail



Please choose an IP interface for this Listener.

1. Management (192.168.42.42/24: mail3.example.com)

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 2
```

```
Please specify the systems allowed to relay email through the
IronPort C60.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addressed are
allowed.

Separate multiple entries with commas.

[]> .example.com


Do you want to enable rate limiting for this listener? (Rate limiting
defines the maximum number of recipients per hour you are willing to
receive from a remote domain.)  [N]> n


Default Policy Parameters

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

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 600

Maximum Number Of Messages Per Connection: 10,000

Maximum Number Of Recipients Per Message: 100,000

Maximum Number Of Recipients Per Hour: Disabled

Use SenderBase for Flow Control:  No

Virus Detection Enabled:  Yes

Allow TLS Connections: No
```

```
Would you like to change the default host access policy?  [N]> n


Listener OutboundMAil created.

Defaults have been set for a Private listener.

Use the listenerconfig->EDIT command to customize the listener.

*****
```

C150/160 のリスナーの例

（注）　リスナーを作成する次の例は、C150/160 をご利用のお客様だけに適用されます。

systemsetup コマンドのこの例の部分では、MailNet IP インターフェイスで実行されるように MailInterface というリスナーを設定します。続いて、ドメイン example.com 宛てのすべての電子メールを受け入れるように設定します。Mail Exchange exchange.example.com への初期 SMTP ルートを設定します。次に、ドメイン example.com に含まれる任意のホスト宛てのすべての電子メールをリレーするように同じリスナーを設定します（エントリ .example.com の先頭のドットに注意してください）。

レート制限をイネーブルにし、パブリック リスナーに対して単一のホストから受信する 1 時間あたりの受信者の最大値に 450 を指定します。

（注）　1 台のリモート ホストから 1 時間あたりに受信する最大受信者数に入力する値は、完全に自由裁量の値です。通常は、管理対象の電子メールを所有している企業の規模に比例します。たとえば、1 時間に 200 通のメッセージを送信する送信者は、「スパム送信者」（未承諾の大量電子メールの送信者）である可能性がありますが、10,000 人規模の会社に対するすべての電子メールを処理する IronPort アプライアンスを設定する場合は、単一のリモート ホストからの 1 時間あたりのメッセージが 200 通であっても、理にかなった値である可能性があります。対照的に、50 人規模の会社の場合に、1 時間あたり 200 通のメッセージを送信してくる送信者は、おそらく、明らかなスパム送信者です。パブリック リスナーで、企業へのインバウンド電子メールのレート制限をイネーブルにする（量

を絞る）場合は、適切な値を選択してください。デフォルトのホスト アクセス ポリシーの詳細については、「送信者グループの構文」（P.5-132）を参照してください。

次に、リスナーのデフォルトのホスト アクセス ポリシーが受け入れられます。

```
You are now going to configure how the IronPort C160 accepts mail by
creating a "Listener".

Please create a name for this listener (Ex: "MailInterface"):

[]> MailInterface



Please choose an IP interface for this Listener.

1. MailNet (10.1.1.1/24: mail3.example.com)

2. Management (192.168.42.42/24: mail3.example.com)

[1]> 1



Enter the domain names or specific email addresses you want to accept
mail for.



Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

Usernames such as "postmaster@" are allowed.

Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are
allowed.

Separate multiple addresses with commas.

[]> example.com
```

```
Would you like to configure SMTP routes for example.com?  [Y]> y


Enter the destination mail server where you want mail for example.com
to be delivered.  Separate multiple entries with commas.

[]> exchange.example.com


Please specify the systems allowed to relay email through the
IronPort C160.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addresses are
allowed.

Separate multiple entries with commas.

[]> .example.com


Do you want to enable rate limiting for this listener? (Rate limiting
defines the maximum number of recipients per hour you are willing to
receive from a remote domain.)  [Y]> y


Enter the maximum number of recipients per hour to accept from a
remote domain.

[]> 450


Default Policy Parameters
```

```
==========================

Maximum Message Size: 10M

Maximum Number Of Connections From A Single IP: 50

Maximum Number Of Messages Per Connection: 100

Maximum Number Of Recipients Per Message: 100

Maximum Number Of Recipients Per Hour: 450

Maximum Recipients Per Hour SMTP Response:

    452 Too many recipients received this hour

Use SenderBase for Flow Control:  Yes

Spam Detection Enabled:  Yes

Virus Detection Enabled:  Yes

Allow TLS Connections: No

Would you like to change the default host access policy?  [N]>


Listener MailInterface created.

Defaults have been set for a Public listener.

Use the listenerconfig->EDIT command to customize the listener.

*****
```

（注） この systemsetup コマンドでは、C150/160 を利用しているお客様向けに、インバウンドとアウトバウンドの両方のメールに対してリスナー 1 つだけを設定するため、すべての発信メールがメール フロー モニタ機能（通常はインバウンドメッセージに使用）で評価されます。詳細については、『*Cisco IronPort*

AsyncOS for Email Daily Management Guide』の「Using the Email Security Monitor」を参照してください。

IronPort Anti-Spam のイネーブル化

IronPort アプライアンスには、IronPort Anti-Spam ソフトウェアの 30 日間有効な評価キーが付属しています。`systemsetup` コマンドのこの部分では、ライセンス契約書を受諾し、アプライアンスでグローバルに IronPort Anti-Spam をイネーブルにすることができます。

次に着信メール ポリシーに対する IronPort Anti-Spam スキャンをイネーブルにします。

（注）　ライセンス契約に合意しない場合、IronPort Anti-Spam はアプライアンスでイネーブルになりません。

アプライアンスで使用可能なすべての IronPort Anti-Spam 設定オプションについては、第 8 章「アンチスパム」を参照してください。

デフォルト アンチスパム スキャン エンジンの選択

複数のアンチスパム スキャン エンジンをイネーブルにした場合は、デフォルト着信メール ポリシーに対してイネーブルにするエンジンを選択するように示されます。

IronPort スパム検疫のイネーブル化

アンチスパム サービスをイネーブルにする場合は、スパム メッセージおよび陽性と疑わしいスパム メッセージをローカル IronPort スパム検疫エリアに送信するように、着信メール ポリシーをイネーブルできます。IronPort スパム検疫をイネーブルにすると、アプライアンスでエンドユーザ検疫もイネーブルになります。エンドユーザのアクセス権を設定していないうちは、管理者だけがエンドユーザ検疫を利用できます。

IronPort スパム検疫については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」を参照してください。

アンチウイルス スキャンのイネーブル化

IronPort アプライアンスには、ウイルス スキャン エンジンの 30 日間評価キーが付属しています。`systemsetup` コマンドのこの部分では、1 つまたは複数のライセンス契約書を受諾し、アプライアンスでアンチウイルス スキャンをイネーブルにできます。アプライアンスでイネーブルにするアンチウイルス スキャン エンジンごとにライセンス契約を受諾する必要があります。

契約書を受諾すると、選択したアンチウイルス スキャン エンジンが着信メール ポリシーでイネーブルにされます。IronPort アプライアンスでは、着信メールをスキャンしてウイルスを検出しますが、感染した添付ファイルの修復は行いません。アプライアンスでは、感染したメッセージをドロップします。

アプライアンスで使用可能なアンチウイルス コンフィギュレーション オプションについては、第 9 章「アンチウイルス」を参照してください。

ウイルス感染フィルタおよび SenderBase 電子メール トラフィック モニタリング ネットワークのイネーブル化

続くこの手順では、SenderBase への参加とウイルス感染フィルタの両方をイネーブルにするよう指示されます。IronPort アプライアンスには、ウイルス感染フィルタの 30 日間評価キーが付属しています。

ウイルス感染フィルタ

ウイルス感染フィルタは、疑わしいメッセージを検疫することによって、従来のアンチウイルス セキュリティ サービスを新しいウイルス シグニチャ ファイルで更新できるまで新しいウイルスの拡散に対抗する、「防衛の最前線」になります。ウイルス感染フィルタをイネーブルにした場合は、デフォルト着信メール ポリシーでイネーブルになります。

ウイルス感染フィルタをイネーブルにする場合は、しきい値およびウイルス感染フィルタ アラートを受信するかどうかを入力します。ウイルス感染フィルタおよびしきい値の詳細については、「ウイルス感染フィルタ」（P.10-335）を参照してください。

SenderBase への参加

SenderBase は、電子メール管理者による送信者の調査、電子メールの正規送信元の識別、およびスパム送信者のブロックに役立つように設計された、電子メールの評価サービスです。

SenderBase 電子メール トラフィック モニタリング ネットワークへの参加に同意した場合は、組織宛に送信された電子メールに関する集約された統計が IronPort によって収集されます。メッセージ属性に関する要約データと、さまざまなタイプのメッセージを IronPort アプライアンスで処理した方法に関する情報が含まれます。

詳細については、第 13 章「SenderBase Network Participation」を参照してください。

アラート設定値および AutoSupport の設定

ユーザの介入を必要とするシステム エラーが発生した場合、IronPort AsyncOS では、電子メールでアラート メッセージをユーザに送信します。システム アラートを受信する電子メール アドレスを 1 つ以上追加してください。複数のアドレスを指定する場合は、カンマで区切ります。入力した電子メール アドレスでは、当初、ディレクトリ獲得攻撃対策アラート以外のすべてのタイプおよびすべてのレベルのアラートを受信します。CLI で `alertconfig` コマンドを使用するか、GUI で [System Administration] > [Alerts] ページを使用することにより、後でアラート コンフィギュレーションを詳細化できます。詳細については、「アラート」（P.15-495）を参照してください。

IronPort AutoSupport 機能では、ご使用の IronPort アプライアンスに関する問題を IronPort カスタマー サポート チームが認識しておくことで、業界トップ水準のサポートを提供できます。IronPort サポート アラートおよび週ごとのステータスの更新を送信するには、[Yes] と回答します（詳細は、「IronPort AutoSupport」（P.15-498）を参照してください）。

スケジュール済みレポートの設定

デフォルトのスケジュール済みレポートの送信先にするアドレスを入力します。この値はブランクにすることができ、その場合、レポートは、電子メールで送信される代わりに、アプライアンス上にアーカイブされます。

時刻設定値の設定

IronPort AsyncOS では、Network Time Protocol（NTP; ネットワーク タイム プロトコル）を使用して、ネットワーク上またはインターネット上の他のサーバと時刻を同期するか、システム クロックを手動で設定することができます。IronPort アプライアンス上の時間帯を設定して、メッセージ ヘッダーおよびログ ファイルのタイムスタンプを正確にする必要もあります。IronPort Systems タ

イム サーバを使用して IronPort アプライアンス上の時刻を同期することもできます。

[Continent]、[Country]、および [Timezone] を選択し、NTP を使用するかどうかと、使用する NTP サーバの名前を選択します。

変更の確定

最後に、手順全体で行った設定変更を確定するかどうかの確認が、System Setup Wizard から示されます。変更を確定する場合は、[Yes] と回答します。

System Setup Wizard を正常に完了すると、次のメッセージが表示されて、コマンド プロンプトが出されます。

```
Congratulations! System setup is complete. For advanced
configuration, please refer to the User Guide.

mail3.example.com>
```

これで、IronPort アプライアンスは、電子メールを送信できる状態になりました。

設定のテスト

IronPort AsyncOS の設定をテストするために、`mailconfig` コマンドをすぐに使用して、`systemsetup` コマンドで作成したばかりのシステム コンフィギュレーション データを含むテスト電子メールを送信できます。

```
mail3.example.com> mailconfig



Please enter the email address to which you want to send

the configuration file. Separate multiple addresses with commas.

[]> user@example.com
```

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

mail3.example.com>
```

利用可能なメールボックスに設定を送信して、システムでネットワーク上に電子メールを送信できることを確認します。

即時アラート

IronPort アプライアンスでは、機能キーを使用して機能をイネーブルにします。`systemsetup` コマンドでリスナーを最初に作成した場合、IronPort Anti-Spam をイネーブルにした場合、Sophos または McAfee Anti-Virus をイネーブルにした場合、またはウイルス感染フィルタをイネーブルにした場合は、アラートが生成されて、「手順 2：[System]」（P.3-54）で指定したアドレスに送信されます。

キーの残り時間を定期的に通知するアラートです。次の例を参考にしてください。

```
Your "Receiving" key will expire in under 30 day(s). Please contact
IronPort Customer Support.


Your "Sophos" key will expire in under 30 day(s). Please contact
IronPort Customer Support.


Your "Virus Outbreak Filters" key will expire in under 30 day(s).
Please contact IronPort Customer Support.
```

30 日間の評価期間を超えて機能をイネーブルにする場合は、IronPort 営業担当者にお問い合わせください。キーの残り時間は、[System Administration] > [Feature Keys] ページからか、`featurekey` コマンドを発行することによって確認できます（詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」にある機能キーの使用に関する項を参照してください）。

次の手順：電子メール パイプラインの理解

systemsetup が完了したため、IronPort アプライアンスによって電子メールが送信および受信されます。アンチウイルス、アンチスパム、およびウイルス感染フィルタ セキュリティ機能をイネーブルにした場合は、着信メールおよび発信メールでスパムおよびウイルスのスキャンも行われます。

次の手順では、アプライアンスの設定をカスタマイズする方法を理解します。第 4 章「電子メール パイプラインの理解」では、システムでの電子メールのルーティング方法の詳細な概要を説明しています。各機能は、順次（上から下に）処理されます。各機能については、本書の残りの章で説明します。