セットアップおよび設置

この章は、次の項で構成されています。

- インストール計画 （1 ページ）
- E メール セキュリティ アプライアンスのネットワークへの物理接続 （5 ページ）
- システム セットアップの準備 （9 ページ）
- システム セットアップ ウィザードの使用 （17 ページ）
- 設定と次の手順の確認 （47 ページ）

インストール計画

- 計画決定に影響を与える情報の確認 （1 ページ）
- ネットワーク境界に E メール セキュリティ アプライアンスを配置する （1 ページ）
- DNS への E メール セキュリティ アプライアンスの登録 （2 ページ）
- インストールのシナリオ （3 ページ）

計画決定に影響を与える情報の確認

- 仮想 E メール セキュリティ アプライアンスを設定する場合は、この章に進む前に『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。
- M シリーズ Cisco コンテンツ セキュリティ管理アプライアンスを設定する場合は、Cisco コンテンツ（M シリーズ）セキュリティ管理アプライアンスの集中型サービスを参照してください。
- インフラストラクチャへのアプライアンスの配置に影響する可能性のある一部の機能について、設置前に電子メール パイプラインについてを参照することを推奨します。

ネットワーク境界にEメールセキュリティアプライアンスを配置する

お使いの E メール セキュリティ アプライアンスが、Mail Exchange（MX）とも呼ばれる SMTP ゲートウェイとして機能するように設計されています。最適な結果を得るために、機能によっては、アプライアンスが電子メールを送受信するためにインターネットに直接アクセスできる

IP アドレス（つまり、外部 IP アドレス）を割り当てられた最初のマシンである必要があります。

受信者ごとのレピュテーションフィルタリング、スパム対策、ウイルス対策、およびウイルスアウトブレイク フィルタの機能（SenderBase Network Participation、IronPort スパム対策フィルタリング、Sophos アンチウイルス フィルタリング、およびアウトブレイク フィルタを参照）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（接続を許可するホストの定義の概要）のためにアプライアンスを設定できます。

E メール セキュリティ 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満たすことを確認します。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、E メール セキュリティ 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 レピュテーション サービスに送信者の SenderBase レピュテーション スコア（SBRS）を問い合わせたり、Anti-Spam 機能やアウトブレイク 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アプライアンスを設定できない場合でも、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。詳細については、着信リレー構成における送信者の IP アドレスの決定を参照してください。

E メール セキュリティ 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（電子メール セキュリティ モニタの使用方法を参照）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 トラフィックを把握できます。
- 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（LDAP クエリを参照）では、ディレクトリ インフラストラクチャを統合でき、更新を単純化できます。
- エイリアス テーブル（エイリアス テーブルの作成を参照）、ドメイン ベースのルーティング（ドメイン マップ機能を参照）、およびマスカレード（マスカレードの構成を参照）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 E メール セキュリティ 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。Anti-Spam、アウトブレイク フィルタ、McAfee Antivirus および Sophos Anti-Virus のすべての機能を利用するために、E メール セキュリティ アプライアンスが DNS に登録されていることを確認します。

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 E メール セキュリティ 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、E メール セキュリティ 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
```

E メール セキュリティ 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、ウイルス対策エンジンの性能を徹底的に評価するには、E メール セキュリティ 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。

インストールのシナリオ

E メール セキュリティ 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。

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大幅に異なっており、設置計画の支援を必要とする場合は、シスコ カスタマー サポートにお問い合わせください（シスコ カスタマー サポートを参照）。

- 設定の概要 （3 ページ）
- 着信（Incoming） （4 ページ）
- 発信（Outgoing） （4 ページ）
- イーサネット インターフェイス （4 ページ）
- 拡張設定 （5 ページ）
- ファイアウォール設定値（NAT、ポート） （5 ページ）

設定の概要

次の図は、エンタープライズ ネットワーク環境における E メール セキュリティ アプライアンスの一般的な設置方法を示します。

いくつかのシナリオでは、E メール セキュリティ 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、E メール セキュリティ 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。

- ファイアウォールの内側：リスナー 2 個の設定（図「ファイアウォールの内側のシナリオ：リスナー 2 個の設定」）

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、システムセットアップの準備 （9 ページ）に進んでください。

着信（Incoming）

- 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
- 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 E メール セキュリティ アプライアンスに直接接続し、E メール セキュリティ 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（ローカル ドメインの電子メールのルーティングを参照）。

発信（Outgoing）

- 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 E メール セキュリティ アプライアンスにルーティングされます。
- E メール セキュリティ 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発信電子メールを受け入れます（詳細については、リスナーの使用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、E メール セキュリティ 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、Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイおよびネットワークと IP アドレスの割り当てを参照してください。

ハードウェアのポート

ハードウェア アプライアンスのポートの数とタイプはモデルによって異なります。

ポート	タイプ（Type）	C170	C370	C670	X1070	C380	C680	C190	C390	C690
管理	Ethernet	[0]	1	1	1	1	1	[0]	1	1

ポート	タイプ（Type）	C170	C370	C670	X1070	C380	C680	C190	C390	C690
データ	Ethernet	2*	3	3	3	3	3	2*	5	5
コンソール	シリアル	9 ピン	9 ピン	9 ピン	9 ピン	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45
リモート電源管理（RPC）	Ethernet	N	N	N	N	Y	Y	Y	Y	Y

* 専用管理ポートのないアプライアンスでは、Data1 ポートを管理用に使用します。

ポートの詳細については、お使いのアプライアンス モデルの『Hardware Installation Guide』を参照してください。

関連項目

- ネットワーク インターフェイスの設定 （23 ページ）
- シリアル接続経由での E メール セキュリティ アプライアンスへのアクセス
- リモート電源再投入の有効化

拡張設定

「ファイアウォールの内側のシナリオ：リスナー 2 個の設定」、および「リスナー 1 個の設定」の図に示す設定に加えて、次も設定できます。

- 中央管理機能を使用する複数の E メール セキュリティ アプライアンス。クラスタを使用した中央集中型管理を参照してください。
- E メール セキュリティ 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。高度なネットワーク構成を参照してください

ファイアウォール設定値（NAT、ポート）

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。他のサービスも場合によってはファイアウォール ポートを開く必要があります。詳細は、ファイアウォール情報を参照してください。

E メール セキュリティ 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 （6 ページ）

設定シナリオ

E メール セキュリティ 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、E メール セキュリティ 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入れ、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。
  - ホスト アクセス テーブル（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。
  - 受信者アクセステーブル（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、Cisco 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。
  - E メール セキュリティ 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。

関連項目

- 着信メールと発信メールの分離 （6 ページ）

着信メールと発信メールの分離

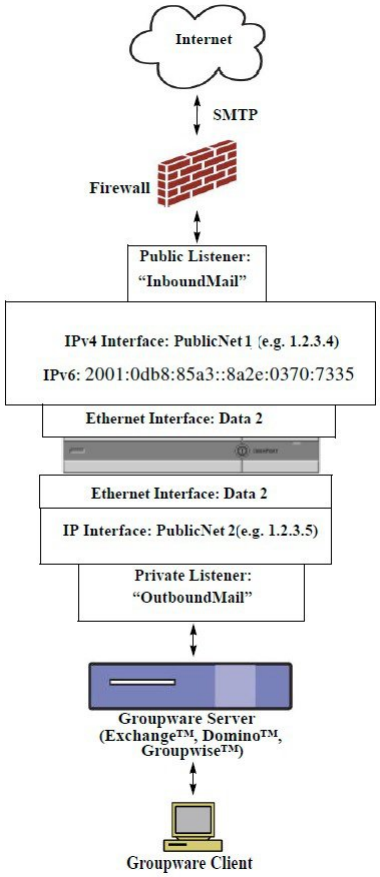
着信と発信の電子メール トラフィックを個別のリスナーおよび個別の IP アドレスで分離できます。インターネット プロトコル バージョン 4（IPv4）およびバージョン 6（IPv6）アドレスを使用できます。ただし、アプライアンスのシステム セットアップ ウィザードでは、次の設定を持つ初期設定をサポートしています。

- 個別の物理インターフェイスに設定された 2 個の論理 IPv4 アドレスおよび 2 個の IPv6 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
  - IPv4 アドレスおよび IPv6 アドレスを各リスナーに割り当てることができます。
- 1 つの物理インターフェイスに設定された 1 つの論理 IPv4 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
- IPv4アドレスおよびIPv6アドレスの両方ともリスナーに割り当てることができます。

リスナー1つと2つの両方の設定に対する設定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 （13 ページ）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 *1 :* ファイアウォールの内側のシナリオ：リスナー *2* 個の設定



（注）

- リスナー x 2
- IPv4 アドレス x 2
- IPv6 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）

- IPv4 アドレス：1.2.3.4

- IPv6 アドレス: 2001:0db8:85a3::8a2e:0370:7334
- 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）

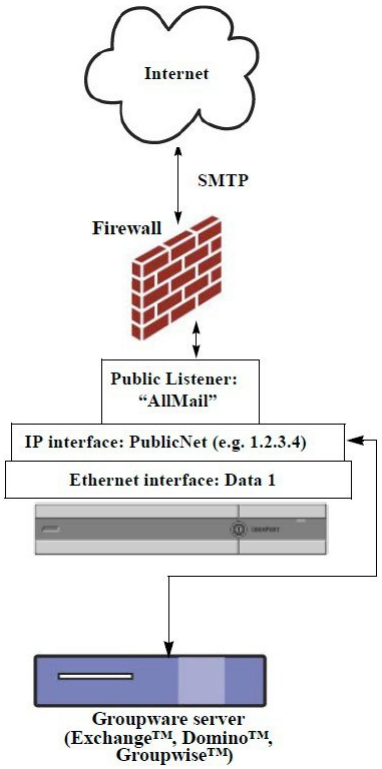
- IP アドレス：1.2.3.5
- IPv6 アドレス: 2001:0db8:85a3::8a2e:0370:7335
- Data 2 インターフェイスのリスナーでポート 25 をリッスン
- HAT（ローカル ドメイン宛てをリレー、その他すべてを拒否）

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 E メール セキュリティ 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 *2:* リスナー *1* 個の設定



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

システム セットアップの準備

- アプライアンスへの接続方式の決定 （10 ページ）
- ネットワーク アドレスと IP アドレスの割り当ての決定 （11 ページ）
- セットアップ情報の収集 （13 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	アプライアンスへの接続方法を決定します。	アプライアンスへの接続方式の決定 （10 ページ）を参照してください
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を決定します。 • すでにアプライアンスをネットワークに配線済みの場合は、E メールセキュリティ アプライアンスのデフォルト IP アドレスが、ネットワーク上の他の IP アドレスと競合していないことを確認します。	参照先： アプライアンスへの接続方式の決定 （10 ページ）およびネットワーク アドレスと IP アドレスの割り当ての決定 （11 ページ）
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。	セットアップ情報の収集 （13 ページ）を参照してください。

	コマンドまたはアクション	目的
ステップ 4	アプライアンスの最新の製品リリース ノートを確認します。	資料のリンクから、リリース ノートを入手できます。
ステップ 5	アプライアンスを開梱し、物理的にラックに設置し、オンにします。	お使いのアプライアンスのクイック スタート ガイドを参照してください。このガイドは、資料のリンクから入手できます。
ステップ 6	コマンドライン インターフェイス（CLI）を使用してセットアップ ウィザードを実行すると、CLI にアクセスします。	コマンドライン インターフェイス（CLI）システム セットアップ ウィザードの実行 （32 ページ）を参照してください。
ステップ 7	Web インターフェイスを使用してセットアップ ウィザードを実行する場合、	1. （仮想アプライアンスの場合のみ）コマンドライン インターフェイスにアクセスし、`interfaceconfig` コマンドを使用して、HTTP および HTTPS を有効にします。 2. 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
ステップ 8	仮想電子メール セキュリティ アプライアンスをセットアップする場合は、お使いの仮想アプライアンスのライセンスをロードしてください。	`loadlicense` コマンドを使用します。詳細については、資料のリンクから利用できる『*Content Security Virtual Appliance Installation Guide*』を参照してください。
ステップ 9	システムの基本設定を行います。	システム セットアップ ウィザードの使用 （17 ページ）を参照してください

アプライアンスへの接続方式の決定

E メール セキュリティ アプライアンスを環境に正常にセットアップするには、E メール セキュリティ 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。

関連項目

- アプライアンスへの接続 （10 ページ）

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 *1:* 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管理ポートの間のイーサネット接続です。工場出荷時に管理ポートに割り当てられている IPv4 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管理ポートに適用できるまでの代用になります。ピン割り当ての詳細については、シリアル接続経由での E メール セキュリティ アプライアンスへのアクセス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。 **ビット/秒**：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） 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、FTP、SSH、および SCP 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、ユーザの追加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

IPv4 アドレスと IPv6 アドレスの両方を使用できます。

- 管理およびデータ ポート用のデフォルト IP アドレス （11 ページ）
- 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 （12 ページ）
- 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 （12 ページ）
- 接続用ネットワーク設定値の選択 （12 ページ）

管理およびデータ ポート用のデフォルト IP アドレス

管理ポート（C170 および C190 アプライアンスの Data 1 ポート）に事前に設定されている IP アドレスは、192.168.42.42 です。

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、E メール セキュリティ 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。インターネット プロトコル バージョン 4（IPv4）およびバージョン 6（IPv6）アドレスを使用できます。ただし、アプライアンスのシステム セットアップ ウィザードでは、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 IPv4 アドレスおよび 2 個の IPv6 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
  - IPv4 アドレスおよび IPv6 アドレスを各リスナーに割り当てることができます。
- 1 つの物理インターフェイスに設定された 1 つの論理 IPv4 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
  - IPv4 アドレスおよび IPv6 アドレスの両方ともリスナーに割り当てることができます。

E メール セキュリティ アプライアンスは、1 つのリスナーで IPv4 アドレスと IPv6 アドレスの両方をサポートできます。リスナーは両方のアドレスでメールを受け入れます。リスナーの設定はすべて、IPv4 と IPv6 両方のアドレスに適用されます。

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（IPv4 または IPv6、あるいはその両方）
- CIDR 形式の IPv4 アドレスのネットマスク
- CIDR 形式の IPv6 アドレスのプレフィックス

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（シスコのタイム サーバを使用する場合は不要）

詳細については、ネットワークと 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 E メール セキュリティ アプライアンスの間でファイアウォールを稼働しているネットワークの場合は、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、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、システム セットアップ ウィザード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、ネットワークと IP アドレスの割り当てを参照してください。Cisco コンテンツ セキュリティ管理アプライアンスを設定する場合は、Cisco コンテンツ（M シリーズ）セキュリティ管理アプライアンスの集中型サービスを参照してください。

表 *2:* システム セットアップ ワークシート：*2*個のリスナーによる電子メール トラフィックの分離

システム設定（System Settings）		
デフォルトのシステム ホスト名（Default System Hostname）：		
システム アラート メールの送信先（Email System Alerts To）：		
定期レポートの送信先:（Deliver Scheduled Reports To:）		
タイムゾーン情報（Time Zone Information）：		
NTP サーバ（NTP Server）：		
管理者パスフレーズ（Admin Passphrase）：		

システム設定（System Settings）		
SenderBase ネットワークに参加:（SenderBase Network Participation:）	イネーブル/ディセーブル（Enable / Disable）	
オートサポート:（AutoSupport:）	イネーブル/ディセーブル（Enable / Disable）	
ネットワーク インテグレーション（Network Integration）		
[ゲートウェイ（Gateway）]：		
DNS:（インターネットまたは独自指定）		
インターフェイス		
データ1ポート（Data 1 Port）		
IPv4アドレス/ネットマスク:（IPv4 Address / Netmask:）		
IPv6アドレス/プレフィックス:（IPv6 Address / Prefix:）		
完全なホスト名:（Fully Qualified Hostname:）		
受信メールの受け入れ:（Accept Incoming Mail:）	**[ドメイン（Domain）]**	**[送信先（Destination）]**
外部への送信メールを中継:（Relay Outgoing Mail:）	**System**	
データ2ポート（Data 2 Port）		
IPv4アドレス/ネットマスク:（IPv4 Address / Netmask:）		
IPv6アドレス/プレフィックス:（IPv6 Address / Prefix:）		
完全なホスト名:（Fully Qualified Hostname:）		

システム設定（System Settings）		
受信メールの受け入れ:（Accept Incoming Mail:）	**[ドメイン（Domain）]**	**[送信先（Destination）]**
外部への送信メールを中継:（Relay Outgoing Mail:）	**System**	
管理ポート（Management Port）		
IP アドレス：		
ネットワークマスク:（Network Mask:）		
IPv6アドレス:（IPv6 Address:）		
プレフィックス:（Prefix:）		
完全なホスト名:（Fully Qualified Hostname:）		
受信メールの受け入れ:（Accept Incoming Mail:）	**[ドメイン（Domain）]**	**[送信先（Destination）]**
外部への送信メールを中継:（Relay Outgoing Mail:）	**System**	
メッセージセキュリティ（Message Security）		
SenderBaseレピュテーションフィルタ:（SenderBase Reputation Filtering:）	イネーブル/ディセーブル	
スパム対策スキャン エンジン	なし/IronPort	
McAfee ウイルス対策スキャンエンジン	イネーブル/ディセーブル	
Sophos ウイルス対策スキャンエンジン	イネーブル/ディセーブル	
アウトブレイク フィルタ（Outbreak Filters）	イネーブル/ディセーブル	

表 *3:* システム セットアップ ワークシート：*1*個のリスナーをすべての電子メール トラフィックに使用

システム設定（System Settings）		
デフォルトのシステム ホスト名（Default System Hostname）：		
システム アラート メールの送信先（Email System Alerts To）：		
定期レポートの送信先:（Deliver Scheduled Reports To:）		
タイム ゾーン:（Time Zone:）		
NTP サーバ:（NTP Server:）		
管理者パスフレーズ（Admin Passphrase）：		
SenderBase ネットワークに参加:（SenderBase Network Participation:）	イネーブル/ディセーブル（Enable / Disable）	
オートサポート:（AutoSupport:）	イネーブル/ディセーブル（Enable / Disable）	
ネットワーク インテグレーション（Network Integration）		
[ゲートウェイ（Gateway）]：		
DNS:（インターネットまたは独自指定）		
インターフェイス		
データ2ポート（Data 2 Port）		
IPv4アドレス/ネットマスク:（IPv4 Address / Netmask:）		
IPv6アドレス/プレフィックス:（IPv6 Address / Prefix:）		

システム設定（System Settings）		
完全なホスト名:（Fully Qualified Hostname:）		
受信メールの受け入れ:（Accept Incoming Mail:）	**[ドメイン（Domain）]**	**[送信先（Destination）]**
外部への送信メールを中継:（Relay Outgoing Mail:）	**System**	
データ1ポート（Data 1 Port）		
IPv4アドレス/ネットマスク:（IPv4 Address / Netmask:）		
IPv6アドレス/プレフィックス:（IPv6 Address / Prefix:）		
完全なホスト名:（Fully Qualified Hostname:）		
メッセージセキュリティ（Message Security）		
SenderBaseレピュテーションフィルタ:（SenderBase Reputation Filtering:）	イネーブル/ディセーブル	
スパム対策スキャン エンジン	なし/IronPort	
McAfee ウイルス対策スキャン エンジン	イネーブル/ディセーブル	
Sophos ウイルス対策スキャン エンジン	イネーブル/ディセーブル	
アウトブレイク フィルタ（Outbreak Filters）	イネーブル/ディセーブル	

システム セットアップ ウィザードの使用

- Web ベースのグラフィカル ユーザ インターフェイス（GUI）へのアクセス （19 ページ）
- Web ベースのシステム セットアップ ウィザードを使用した基本設定の定義 （20 ページ）
- Active Directory への接続の設定 （29 ページ）

- 次の手順 （30 ページ）
- コマンドライン インターフェイス（CLI）へのアクセス （30 ページ）
- コマンドライン インターフェイス（CLI）システム セットアップ ウィザードの実行 （32 ページ）
- エンタープライズ ゲートウェイとしてシステムを設定 （47 ページ）

初期セットアップではシステム セットアップ ウィザードを使用して、設定に漏れがないようにする必要があります。後で、システム セットアップ ウィザードで利用できないカスタム オプションを設定できます。

ブラウザまたはコマンドラインインターフェイス（CLI）を使用して、システム設定ウィザードを実行できます。詳細については、Web ベースのグラフィカル ユーザ インターフェイス（GUI）へのアクセス （19 ページ）またはコマンドライン インターフェイス（CLI）システム セットアップ ウィザードの実行 （32 ページ）を参照してください。

開始する前に、システム セットアップの準備 （9 ページ）にある前提条件をクリアします。

注意 仮想 E メール セキュリティ アプライアンスをセットアップする場合は、システム セットアップ ウィザードを実行する前に、仮想アプライアンスのライセンスをロードするために loadlicense コマンドを使用する必要があります。詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。

注意 システムセットアップ ウィザードでは、システムを完全に再設定します。システムセットアップ ウィザードは、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。

注意 E メール セキュリティ アプライアンスは、すべてのハードウェアの管理ポートにデフォルト IP アドレスの 192.168.42.42 を設定した状態で出荷されます（Data 1 ポートを代わりに使用する C170 および C190 アプライアンスを除く）。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。Cisco コンテンツ セキュリティ管理アプライアンスを設定する場合は、Cisco コンテンツ（M シリーズ）セキュリティ管理アプライアンスの集中型サービスを参照してください。

工場出荷時の設定を持つ複数のコンテンツ セキュリティ アプライアンスをネットワークに接続する場合は、1 つずつ追加して、各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）へのアクセス

Web ベースのグラフィカル ユーザ インターフェイス（GUI）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。

関連項目

- 工場出荷時のデフォルト ユーザ名とパスフレーズ （19 ページ）

工場出荷時のデフォルト ユーザ名とパスフレーズ

新しい仮想またはハードウェア アプライアンスをインストールする場合、完全なアクセス権を取得してアプライアンスを設定するために、デフォルトのパスフレーズを変更する必要があります。初めてアプライアンスにログインすると、Webインターフェイスによってデフォルトのパスフレーズを変更するように指示されます。デフォルトのパスフレーズを変更するまで、CLI で以下のコマンドへのアクセスが制限されます。

- Commit
- Interfaceconfig
- passphrase
- Loadconfig
- Systemsetup
- loadlicense（仮想アプライアンス向け）
- ライセンス キー
- Ping
- Telnet
- netstat

- ユーザ名：**admin**
- パスフレーズ：**ironport**

例：

```
login: admin
passphrase: ironport
```

（注） セッションがタイムアウトした場合は、ユーザ名とパスフレーズの再入力が求められます。システム セットアップ ウィザード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 ベースのシステム セットアップ ウィザードを使用した基本設定の定義

ステップ 1 システム セットアップ ウィザードの起動

- Web ベースのグラフィカル ユーザ インターフェイス（GUI）へのアクセス （19 ページ）に記載されている方法で、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。
- 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、ブラウザがシステム セットアップ ウィザードに自動的にリダイレクトされます。
- それ以外の場合は、[システム管理（System Administration）] タブで、左方のリンク リストから [システムセットアップウィザード（System Setup Wizard）] をクリックします。

ステップ 2 [開始（Start）]。手順 1：開始 （21 ページ）を参照してください。

- ライセンス契約書の参照と受諾

ステップ 3 システム。手順 2：システム （21 ページ）を参照してください。

- アプライアンスのホスト名の設定
- アラート、レポート配信、および AutoSupport の設定
- システム時刻と NTP サーバの設定
- admin パスフレーズのリセット
- SenderBase Network Participation のイネーブル化

ステップ 4 [ネットワーク（Network）]。手順 3：ネットワーク （23 ページ）を参照してください。

- デフォルト ルータおよび DNS 設定値の定義
- ネットワーク インターフェイスの有効化および構成：これには受信メール（受信リスナー）の設定、SMTP ルートの定義（任意）、送信メール（送信リスナー）の設定、およびアプライアンスを介したメールの中継が許可されるシステムの定義が含まれます。

ステップ 5 [セキュリティ（Security）]。手順 4：セキュリティ （27 ページ）を参照してください。

- SenderBase レピュテーション フィルタリングのイネーブル化
- スパム対策サービスのイネーブル化
- スパム隔離のイネーブル化
- Anti-Virus サービスのイネーブル化
- 高度なマルウェア防御のイネーブル化（ファイル レピュテーションおよび分析サービス）
- アウトブレイク フィルタサービスのイネーブル化

ステップ 6 [レビュー（Review）]。手順 5：レビュー （29 ページ）を参照してください。

- セットアップのレビューおよび設定のインストール
- 手順の最後に表示されるプロンプト

ステップ 7 変更点の確定

確定するまで、変更は有効になりません。

手順 1：開始

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、[セットアップの開始（Begin Setup）] をクリックして続行します。

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：システム

- ホスト名の設定 （21 ページ）
- システム アラートの設定 （21 ページ）
- レポート配信の設定 （21 ページ）
- 時間の設定 （22 ページ）
- パスフレーズの設定 （22 ページ）
- SenderBase ネットワークへの参加 （22 ページ）
- AutoSupport のイネーブル化 （22 ページ）

ホスト名の設定

E メール セキュリティ 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、Cisco 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

E メール セキュリティ アプライアンス上にタイム ゾーンを設定して、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表示されるようにします。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、ネットワーク タイム プロトコル（NTP）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、Cisco Systems のタイム サーバ（**time.ironport.com**）と時刻を同期するエントリ 1 つがアプライアンスにすでに設定されています。

パスフレーズの設定

admin アカウントのパスフレーズを設定します。この手順は必須です。Cisco AsyncOS の admin アカウントのパスフレーズを変更する場合、新しいパスフレーズは、6 文字以上でなければなりません。パスフレーズは、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、電子メールのレピュテーション サービスです。

SenderBase ネットワークへの参加に同意した場合、シスコは、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 E メール セキュリティ 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、シスコは、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、[共有対象データの詳細については、ここをクリック（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（FAQを参照）。

SenderBase ネットワークに参加する場合は、[メールをベースとする脅威の特定、排除を目的として、IronPortがメールの匿名統計を収集およびSenderBaseに対しレポートすることを許可（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、[承認（Accept）] をクリックします。

詳細については、SenderBase Network Participationを参照してください。

AutoSupport のイネーブル化

AutoSupport 機能（デフォルトで有効）では、ご使用のアプライアンスに関する問題をシスコ 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。（詳細については、AutoSupportを参照してください）。

[次へ（Next）] をクリックして続行します。

手順 3：ネットワーク

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 （23 ページ）
- ネットワーク インターフェイスの設定 （23 ページ）
- メールの受け入れ （24 ページ）
- メール リレー（任意） （25 ページ）
- C170 および C190 のインストール （26 ページ）

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。IPv4 アドレス、IPv6 アドレス、またはその両方を使用できます。

次に、Domain Name Service（DNS）を設定します。Cisco 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。システム セットアップ ウィザードから入力できる 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）設定値の構成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、稼働中の 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、[インターネットルート DNSサーバを使用（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、システム セットアップ ウィザードを完了できます。

ネットワーク インターフェイスの設定

E メール セキュリティ アプライアンスには、マシンの物理イーサネット 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。

インターフェイスを使用するには、[有効（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。IPv4 アドレス、IPv6 アドレス、またはその両方を使用できます。両方使用すると、インターフェイスは両方のタイプの接続を受け入れます。

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。ほとんどのアプライアンスでは、通常、インターフェイスの 1 つを着信用、1 つを発信用、1 つをアプライアンス管理用に使用します。C170 および C190 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。

C370、C670、X1070、C380、C680、C390、および C690 アプライアンスの場合：シスコでは、パブリック リスナーを介して着信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 リスナーを介して発信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。

C170 および C190 アプライアンスの場合：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、システム セットアップ ウィザード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 （12 ページ）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**。IPv4 アドレス、IPv6 アドレス、またはその両方を使用できます。
- IPv4 アドレスの場合：インターフェイスのネットマスク。AsyncOS は、CIDR 形式のネットマスクだけを受け入れます。たとえば、`255.255.255.0` サブネットの `/24` など。

  IPv6 アドレスの場合：CIDR 形式の**プレフィックス**。64 ビット プレフィックスの `/64` など。

- （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、ネットワークと 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）

[受信メールの受け入れ（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。

[宛先（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（受信者アクセステーブル（RAT）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、[行を追加（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（ローカル ドメインの電子メールのルーティング を参照）。

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、受信者アドレスの定義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を参照してください。

[外部への送信メールを中継（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。

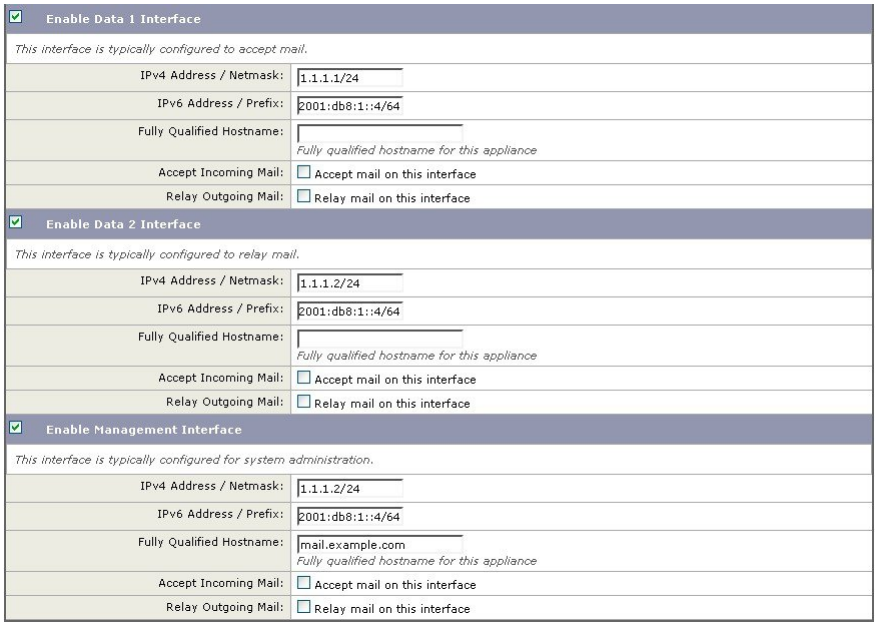
アウトバウンドメールをリレーするようにインターフェイスを設定すると、そのインターフェイスを使用するパブリック リスナーが設定されている場合を除き、そのインターフェイスの SSH がシステム セットアップ ウィザードによってオンにされます。

次の例では、IPv4 アドレスの 2 個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。

C370、C670、X1070、C380、C680、C390、および C690 のインストール

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

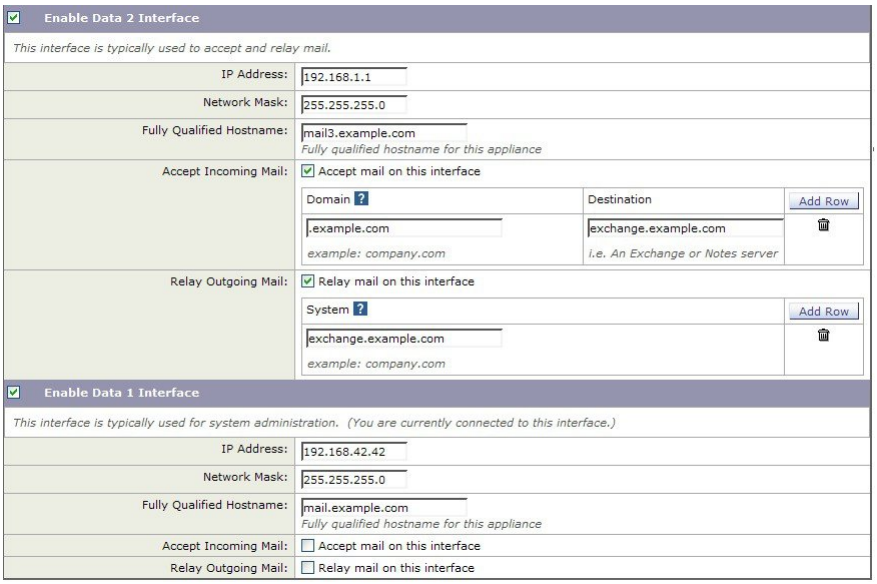


C170 および C190 のインストール

C170 および C190 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。

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）、システム セットアップ ウィザードの手順 3 は次のようになります。

図 *4:* 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



[次へ（Next）] をクリックして続行します。

手順 4：セキュリティ

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 レピュテーション 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、アウトブレイク 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 レピュテーション フィルタリングのイネーブル化 （27 ページ）
- アンチスパム スキャンのイネーブル化 （28 ページ）
- アンチウイルス スキャンのイネーブル化 （28 ページ）
- 高度なマルウェア防御のイネーブル化（ファイル レピュテーションおよび分析サービス）（28 ページ）
- アウトブレイク フィルタのイネーブル化 （28 ページ）

SenderBase レピュテーション フィルタリングのイネーブル化

SenderBase レピュテーション サービスは、スタンドアロンのスパム対策ソリューションとしても使用できますが、コンテンツ ベースのスパム対策システム（Anti-Spam など）の有効性を高めることを主な目的としています。

SenderBase レピュテーション 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 レピュテーション 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 レピュテーション 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。SenderBase レピュテーション 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 レピュテーション 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

アプライアンスには、スパム対策ソフトウェアの 30 日間評価キーが付属している場合があります。システム セットアップ ウィザードのこの部分では、アプライアンスで 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。スパム対策サービスをイネーブルにしないことも選択できます。

スパム対策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 スパム隔離に送信するように、AsyncOS を設定できます。スパム隔離は、アプライアンスのエンドユーザ隔離として機能します。エンドユーザのアクセス権を設定していないうちは、管理者だけが隔離を利用できます。

アプライアンスで使用可能なすべての Anti-Spam 設定オプションについては、スパム対策を参照してください。ポリシー、ウイルス、およびアウトブレイク隔離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

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。システムセットアップ ウィザードのこの部分では、アプライアンスでウイルス対策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。

ウイルス対策スキャン エンジンを有効にすると、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有効になります。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ウイルス対策設定オプションについては、アンチウイルスを参照してください。

高度なマルウェア防御のイネーブル化（ファイル レピュテーションおよび分析サービス）

高度なマルウェア防御では、クラウドベースのサービスから添付ファイルのレピュテーション情報を取得します。

詳細については、ファイル レピュテーション フィルタリングとファイル分析を参照してください。

アウトブレイク フィルタのイネーブル化

アプライアンスには、アウトブレイク 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。アウトブレイク フィルタは、従来のウイルス対策セキュリティ サービスが新しいウイルス シグニチャ ファイルで更新されるまで、疑わしいメッセージを隔離することで、新種ウイルスの発生に対する「第一の防衛ライン」になります。

詳細については、アウトブレイク フィルタを参照してください。

[次へ（Next）] をクリックして続行します。

手順 5：レビュー

設定情報のサマリーが表示されます。[システム設定（System Settings）]、[ネットワークインテグレーション（Network Integration）]、および[メッセージセキュリティ（Message Security）] の情報は、[前へ（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 [編集（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。

表示されている情報が要件を満たしていれば、[この設定をインストール（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。[インストール（Install）] をクリックして、新しい設定をインストールします。

これで、アプライアンスが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（C370、C670、X1070、C380、C680、C390、および C690 アプライアンスの管理インターフェイス、または C170 および C190 アプライアンスの 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、[インストール（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 （47 ページ）を参照してください。

Active Directory への接続の設定

システム セットアップ ウィザードによって E 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、[このステップをスキップ（Skip this Step）] をクリックします。Active Directory Wizard は、[システム管理（System Administration）] > [Active Directory ウィザード（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、[システム管理（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 許可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、[システム管理（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

ステップ 1 [Active Directoryウィザード（Active Directory Wizard）] ページで [Active Directoryウィザードを実行（Run Active Directory Wizard）] をクリックします。

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フレーズを入力します。

ステップ 4 [次へ（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、[ディレクトリ設定のテスト（Test Directory Settings）] ページが表示されます。

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、[テスト（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。結果が [接続ステータス（Connection Status）] フィールドに表示されます。

ステップ 6 [完了（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、[システムセットアップの次のステップ（System Setup Next Steps）] ページが表示されます。

[システムセットアップの次のステップ（System Setup Next Steps）] ページのリンクをクリックして、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 （10 ページ）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フレーズを次に示します。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（ユーザの追加の詳細については、ユーザの追加を参照してください）。システム セットアップ ウィザードで、admin アカウントのパスフレーズを変更するように要求されます。admin アカウントのパスフレーズは、passphrase 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。下記のユーザ名とパスフレーズを入力します。

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 （

10 ページ）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フレーズを入力します。

ユーザ名およびパスフレーズを入力してアプライアンスにログインします。

関連項目

- 工場出荷時のデフォルト ユーザ名とパスフレーズ （19 ページ）

工場出荷時のデフォルト ユーザ名とパスフレーズ

新しい仮想またはハードウェア アプライアンスをインストールする場合、完全なアクセス権を取得してアプライアンスを設定するために、デフォルトのパスフレーズを変更する必要があります。初めてアプライアンスにログインすると、Webインターフェイスによってデフォルトのパスフレーズを変更するように指示されます。デフォルトのパスフレーズを変更するまで、CLI で以下のコマンドへのアクセスが制限されます。

- Commit
- Interfaceconfig
- passphrase
- Loadconfig
- Systemsetup
- loadlicense（仮想アプライアンス向け）
- ライセンス キー
- Ping
- Telnet
- netstat

- ユーザ名：**admin**
- パスフレーズ：**ironport**

例：

```
login: admin
passphrase: ironport
```

（注） セッションがタイムアウトした場合は、ユーザ名とパスフレーズの再入力が求められます。システム セットアップ ウィザード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。

コマンドライン インターフェイス（CLI）システム セットアップ ウィザードの実行

CLI バージョンのシステム セットアップ ウィザードの手順は、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、グローバルなウイルス対策セキュリティとアウトブレイク フィルタ セキュリティ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。

システム セットアップ ウィザードを実行するには、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システム セットアップ ウィザード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 [はい（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 バージョンのシステム セットアップ ウィザード対話の例には、Web ベースのシステム セットアップ ウィザードを使用した基本設定の定義 （20ページ）で説明した GUI バージョンのシステム セットアップ ウィザードから逸脱する部分だけを含めてあります。

関連項目

- admin パスフレーズの変更 （33 ページ）
- ライセンス契約書の受諾 （33 ページ）
- ホスト名の設定 （33 ページ）
- 論理 IP インターフェイスの割り当てと設定 （33 ページ）

- デフォルト ゲートウェイの指定 （35 ページ）
- Web インターフェイスのイネーブル化 （35 ページ）
- DNS の設定 （35 ページ）
- リスナーの作成 （35 ページ）
- アンチスパムのイネーブル化 （43 ページ）
- デフォルト アンチスパム スキャン エンジンの選択 （44 ページ）
- スパム隔離のイネーブル化 （44 ページ）
- アンチウイルス スキャンのイネーブル化 （44 ページ）
- アウトブレイク 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 （44 ページ）
- アラート設定値および AutoSupport の設定 （45 ページ）
- スケジュール済みレポートの設定 （45 ページ）
- 時刻設定値の設定 （46 ページ）
- 変更の確定 （46 ページ）
- 設定のテスト （46 ページ）
- 即時アラート （47 ページ）

admin パスフレーズの変更

まず、AsyncOS の admin アカウントのパスフレーズを変更します。続行するには、現在のパスフレーズを入力する必要があります。新しいパスフレーズは 6 文字以上の長さにする必要があります。パスフレーズは、必ず安全な場所に保管してください。パスフレーズの変更は、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 ライセンス契約書を参照して受諾します。

ホスト名の設定

次に、E メールセキュリティ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（C370、C670、X1070、C380、C680、C390、および C690 アプライアンス）または Data 1（C170 および C190 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。

C370、C670、X1070、C380、C680、C390、および C690 アプライアンスの場合：シスコでは、パブリック リスナーを介して着信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 リスナーを介して発信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。

C170 および C190 アプライアンスの場合：デフォルトでは、着信電子メールの受信と発信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 つのみが `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**。これは、IPv4 アドレスまたは IPv6 アドレスにできます。1 つの IP インターフェイスに両方のタイプの IP アドレスを割り当てることができます。
- インターフェイスの**ネットマスク**ネットマスクは、CIDR 形式である必要があります。たとえば、`255.255.255.0` サブネットでは `/24` を使用します。

  （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、ネットワークと IP アドレスの割り当てを参照してください。

  C170 および C190 アプライアンスの場合、Data 2 インターフェイスを最初に設定します。

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有効にします。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。

DNS の設定

次に、Domain Name Service（DNS）を設定します。Cisco 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、着信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 E メール セキュリティ 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。Cisco 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）。

C370、C670、X1070、C380、C680、C390、および C690 アプライアンスの場合：デフォルトでは、systemsetup コマンドによって 2 個のリスナー（プライベート 1 つ、パブリック 1 つ）が設定されます。（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を参照してください）。

C170 および C190 アプライアンスの場合：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。C170 および C190 アプライアンスのリスナーの例 （40 ページ）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。ローカル ドメインの電子メールのルーティング を参照してください）。
- パブリック リスナーで SenderBase Reputation Score（SBRS; SenderBase レピュテーション 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、[コンサーバティブ（Conservative）]、[適度（Moderate）]、または [アグレッシブ（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）、あるい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およびメッセージを受け入れるドメインおよびユーザの追加を参照してください。

関連項目

- パブリック リスナー （36 ページ）
- プライベート リスナー （39 ページ）
- C170 および C190 アプライアンスのリスナーの例 （40 ページ）

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、C370、C670、X1070、C380、C680、C390、および C690 アプライアンスのみに適用されます。C170 および C190 アプライアンスの場合は、次のセクション、C170 および C190 アプライアンスのリスナーの例 （40 ページ）まで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 E メール セキュリティ 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、企業への着信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 appliance 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、リスナーの使用を参照してください。

```
Do you want to configure the appliance 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 appliance.

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.

*****
```

C170 および C190 アプライアンスのリスナーの例

（注） リスナーを作成する次の例は、C170 および C190 アプライアンスのみに適用されます。

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 domain 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、企業への着信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 appliance 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 appliance.

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、C170 および C190 アプライアンスの受信メールと送信メール両方に対してリスナーを 1 つだけ設定するため、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。電子メール セキュリティ モニタの使用方法を参照してください

アンチスパムのイネーブル化

アプライアンスには、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 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 Anti-Spam スキャンをイネーブルにします。

（注） ライセンス契約書を受諾しない場合、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 Anti-Spam 設定オプションについては、スパム対策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。

スパム隔離のイネーブル化

スパム対策サービスをイネーブルにした場合は、着信メール ポリシーをイネーブルにして、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 スパム隔離に送信できます。スパム隔離をイネーブルにすると、アプライアンスでエンドユーザ隔離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隔離を利用できます。

ローカルのスパム隔離の設定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

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、アプライアンスでウイルス対策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ウイルス対策スキャン エンジンごとにライセンス契約書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。E メール セキュリティ 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ウイルス対策設定オプションについては、アンチウイルスを参照してください。

アウトブレイク 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 への参加とアウトブレイク フィルタの両方をイネーブルにするよう指示されます。アプライアンスには、アウトブレイク フィルタの 30 日間評価キーが付属しています。

関連項目

- アウトブレイク フィルタ （45 ページ）
- SenderBase への参加 （45 ページ）

アウトブレイク フィルタ

アウトブレイク フィルタは、従来のウイルス対策セキュリティ サービスが新しいウイルス シグニチャ ファイルで更新されるまで、疑わしいメッセージを隔離することで、新種ウイルスの発生に対する「第一の防衛ライン」になります。アウトブレイク 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。

アウトブレイク フィルタをイネーブルにする場合は、しきい値およびアウトブレイク フィルタ アラートを受信するかどうかを入力します。アウトブレイク フィルタおよびしきい値の詳細については、アウトブレイク フィルタ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、電子メールのレピュテーション 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シスコによって収集されます。これには、メッセージ属性の要約データおよび E メール セキュリティ 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が含まれています。

詳細については、『Cisco Email Security Appliance Guide』の「SenderBase Network Participation」の章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、Cisco AsyncOS 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 [システム管理（System Administration）] > [アラート（Alerts）] ページを使用することにより、後でアラート設定を詳細化できます。詳細については、『Cisco Email Security Appliance Guide』で、「Distributing Administrative Tasks」の章の「Alerts」の項を参照してください。

AutoSupport 機能では、ご使用のアプライアンスに関する問題をシスコ 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。サポート アラートと週ごとのステータス更新をシスコに送信するには、[はい（Yes）] と回答します（詳細については、『Cisco Email Security Appliance Guide』で、「Distributing Administrative Tasks」の章の「AutoSupport」の項を参照してください）。

スケジュール済みレポートの設定

デフォルトの定期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

Cisco AsyncOS では、ネットワーク タイム プロトコル（NTP）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。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。Cisco Systems タイム サーバを使用してアプライアンス上の時刻を同期することもできます。

[大陸（Continent）]、[国（Country）]、および [タイムゾーン（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、システム セットアップ ウィザードから示されます。変更を確定する場合は、[はい（Yes）] と回答します。

システム セットアップ ウィザード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、アプライアンスが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

Cisco AsyncOS の設定をテストする際は、mailconfig コマンドを使用して、`systemsetup` コマンドで作成したばかりのシステム設定データを含むテスト電子メールをただちに送信できます。

```
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

E メール セキュリティ アプライアンスでは、ライセンス 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、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、あるいはアウトブレイク 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：システム （21ページ）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。次に例を示します。

```
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 "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有効にする場合は、シスコのセールス担当者にお問い合わせください。キーの残り時間は、[システム管理（System Administration）] > [ライセンスキー（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、ライセンス キーを参照してください）。

エンタープライズ ゲートウェイとしてシステムを設定

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。

設定と次の手順の確認

システム セットアップが完了したため、E メール セキュリティ 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。ウイルス対策、スパム対策、およびウイルス アウトブレイク 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。電子メール パイプラインについては、電子メールがシステムをルーティングされる方法を詳しく説明しています。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。