メール ポリシー

この章は、次の項で構成されています。

メール ポリシーの概要

E メール セキュリティ アプライアンスはメール ポリシーを使用して、組織とユーザとの間で送信されるメッセージについての組織のポリシーを適用します。これらは、組織が社内のネットワークに入ったり出たりして欲しくない、疑わしい、機密な、または悪意のあるコンテンツのタイプを指定する一連のルールです。このコンテンツは次のようなものがあります。

- スパム
- 問題のないマーケティング メッセージ
- グレーメール
- ウイルス
- フィッシングおよび他のメール攻撃のターゲット
- 機密企業データ
- 個人情報

組織内の異なるユーザ グループの個別のセキュリティ ニーズを満たすために複数のポリシーを作成できます。E メール セキュリティ アプライアンスはこれらのポリシーに定義されているルールを使用して各メッセージをスキャンし、必要に応じて、ユーザを保護するアクションを実行します。たとえば、ポリシーは、スパムの疑いのあるメッセージが幹部に配信されないようにすると共に、そのコンテンツについて警告する件名に変更して IT スタッフへの配信を許可することができます。システム管理者グループ以外のすべてのユーザで、危険な実行可能プログラムの添付ファイルをドロップします。

メール ポリシーをユーザ単位で適用する方法

手順

	コマンドまたはアクション	目的
ステップ 1	E メール セキュリティ アプライアンスが着信または発信メッセージに使用するコンテンツ スキャン機能をイネーブルにします。	この機能で、次の 1 つ以上をイネーブル化し、設定できます。 • アンチウイルス • 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（着信メッセージのみ） • スパムおよびグレイメールの管理 • グレイメールの検出と安全な配信停止。「スパムおよびグレイメールの管理」を参照してください。 • アウトブレイク フィルタ • データ損失の防止（発信メッセージのみ） • コンテンツ フィルタ
ステップ 2	（任意）特定のデータを含むメッセージに対して実行するアクションの場合にコンテンツ フィルタを作成します。	コンテンツ フィルタを参照してください。
ステップ 3	（任意）メール ポリシーのルールが適用されるユーザを指定する LDAP グループ クエリーを定義します。	受信者がグループ メンバーであるかどうかを判別するグループ LDAP クエリの使用を参照してください。
ステップ 4	（任意）着信または発信メッセージのデフォルトのメール ポリシーを定義します。	着信または発信メッセージのデフォルトのメール ポリシーの設定 （8 ページ）を参照してください。
ステップ 5	ユーザ特定のメール ポリシーを設定するユーザ グループを定義します。	着信または発信メール ポリシーを作成します。 詳細については、メール ポリシーの設定 （8 ページ）を参照してください。
ステップ 6	コンテンツ セキュリティ機能とアプライアンスがメッセージに対して実行するコンテンツ フィルタ アクションを設定します。	メール ポリシーの異なるコンテンツのセキュリティ機能を設定します。 • コンテンツ フィルタ（Content Filters）：特定のユーザ グループに対するメッセージへのコンテンツ フィルタの適用

	コマンドまたはアクション	目的
		• ウイルス対策（Anti-Virus）：ユーザのウイルス スキャン アクションの設定 • ファイル レピュテーション フィルタリングおよびファイル分析：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 • スパム対策（Anti-Spam）：スパム対策ポリシーの定義 • グレイメールの検出と安全な配信停止：グレイメールの検出と安全な配信停止の着信メール ポリシーの設定 • アウトブレイク フィルタ（Outbreak Filters）：アウトブレイク フィルタ機能とアウトブレイク隔離 • データ漏洩防止（DLP）：発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て。

着信メッセージと発信メッセージの異なる処理

E メール セキュリティ アプライアンスはメッセージ コンテンツ セキュリティに 2 つの異なるメール ポリシーのセットを使用します。

- メッセージの着信メール ポリシーは、リスナーの ACCEPT HAT ポリシーに一致する接続から受信されるメッセージです。
- メッセージの発信メール ポリシーは、リスナーの RELAY HAT ポリシーに一致する接続からのメッセージです。この接続には、SMTP AUTH で認証された任意の接続が含まれます。

異なるポリシーのセットを持つことで、ユーザに送信またはユーザから送信されたメッセージに対し異なるセキュリティ ルールを定義することができます。これらのテーブルを管理するには、GUI の [メールポリシー（Mail Policies）]>[着信メールポリシー（Incoming Mail Policies）] ページまたは [発信メールポリシー（Outgoing Mail Policies）] ページ、あるいは CLI の policyconfig コマンドを使用します。

（注） 一部の機能は発信メール ポリシーのみ、または着信メール ポリシーのみに適用できます。データ消失防止スキャンは、発信メッセージに対してのみ実行できます。高度なマルウェア防御（ファイル レピュテーション スキャンおよびファイルの分析）は着信メール ポリシーおよび発信メール ポリシーで使用できます。

特定のインストールでは、Cisco アプライアンスを経由する「内部」メールは、すべての受信者が内部アドレスにアドレス指定されている場合でも、発信と見なされます。たとえばデフォルトでは、システム セットアップ ウィザードによって C170 および C190 アプライアンスに対して、着信電子メールの受信および発信電子メールのリレー用に、リスナー 1 つの物理イーサネット ポート 1 つのみが設定されます。

メール ポリシーへのユーザの一致

メッセージがアプライアンスによって受信されると同時に、E メール セキュリティ アプライアンスは、メッセージが着信か発信かによって、各メッセージ受信者と送信者を着信または発信メッセージ ポリシー テーブルのメール ポリシーに一致させようとします。

一致は受信者のアドレス、送信者のアドレス、または両方に基づきます。

- 受信者アドレスは、エンベロープ受信者アドレスとマッチングされます。

  受信者アドレスが一致すると、入力された受信者アドレスは、電子メール パイプラインの先行部分による処理後の最終アドレスです。たとえば、イネーブルの場合、デフォルト ドメイン、LDAP ルーティングまたはマスカレード、エイリアス テーブル、ドメイン マップ、メッセージ フィルタ機能はエンベロープ受信者アドレスを書き換えることができ、メッセージがメール ポリシーに一致するかどうかに影響することがあります。

- 送信者アドレスは、次のアドレスと照合されます。
  - エンベロープ送信者（RFC821 MAIL FROM アドレス）
  - RFC822 From: ヘッダーのアドレス
  - RFC822 Reply-To: ヘッダーのアドレス

アドレス マッチングは、完全な電子メール アドレス、ユーザ、ドメインまたは部分的なドメインのいずれか、あるいは LDAP グループ メンバーシップで行われます。

関連項目

- 最初に一致したものが有効 （4 ページ）
- ポリシー マッチングの例 （5 ページ）

最初に一致したものが有効

各ユーザは（送信者または受信者）トップダウン方式の適切なメール ポリシー テーブルで定義したメール ポリシーごとに評価されます。

ユーザごとに、最初に一致したポリシーが適用されます。ユーザが特定のポリシーと一致しない場合、ユーザは自動的にテーブルのデフォルト ポリシーと一致します。

送信者アドレスに基づいて一致する場合、メッセージの残りのすべての受信者がそのポリシーに一致します。（これは、メッセージごとに存在する送信者が 1 人だけのためです）。

エンベロープ送信者とエンベロープ受信者は、メッセージをメールポリシーに突き合わせるときに送信者ヘッダーよりも高いプライオリティを持ちます。メールポリシーを特定のユーザに合わせて構成すると、メッセージはエンベロープ送信者とエンベロープ受信者に基づいてメール ポリシーに自動的に分類されます。

ポリシー マッチングの例

次の例では、ポリシー テーブルがどのように上から順に照合されるかを説明します。

次の表に示す着信メールの電子メール セキュリティ ポリシーの表では、着信メッセージはさまざまなポリシーとマッチングされます。

表 *1*: ポリシー マッチングの例

順序	ポリシー名	ユーザ	
		Sender	受信者（Recipient）
1	special_people	ANY	joe@example.com ann@example.com
2	from_lawyers	@lawfirm.com	ANY
3	acquired_domains	ANY	@newdomain.com @anotherexample.com
4	engineering	ANY	PublicLDAP.ldapgroup: engineers
5	sales_team	ANY	jim@john@larry@
6	デフォルト ポリシー	ANY	ANY

関連項目

- 例 1 （5 ページ）
- 例 2 （6 ページ）
- 例 3 （6 ページ）

例 1

送信者 `bill@lawfirm.com` から受信者 `jim@example.com` に送信されるメッセージは次に一致します。

- ポリシー#2、ユーザの説明が送信者（@lawfirm.com）と受信者（ANY）に一致する場合。
- ポリシー #2、エンベロープ送信者が bill@lawfirm.com である場合。
- ポリシー#5、ヘッダー送信者はbill@lawfirm.comだが、エンベロープ送信者が@lawfirm.comと一致しない場合。

例 2

送信者 joe@yahoo.com は、3 人の受信者、john@example.com、jane@newdomain.com および bill@example.com に着信メッセージを送信します。

- 受信者 jane@newdomain.com へのメッセージは、ポリシー #3 で定義されたスパム対策、ウイルス対策、アウトブレイク フィルタおよびコンテンツ フィルタを受信します。
- 受信者 john@example.com へのメッセージはポリシー #5 で定義されている設定を受信します。
- 受信者bill@example.comはエンジニアリングLDAPクエリーに一致しないため、メッセージはデフォルト ポリシーで定義された設定を受け取ります。

次の例では、受信者が複数あるメッセージでメッセージ分裂がどのように発生するかについて示します。 詳細については、メッセージ分裂 （6 ページ）を参照してください。

例 3

送信者 bill@lawfirm.com（bill@lawfirm.com はエンベロープ送信者に使用される）は、メッセージを受信者 ann@example.com および larry@example.com に送信します。

- 受信者 ann@example.com は、ポリシー#1 で定義されているスパム対策、ウイルス対策、アウトブレイク フィルタおよびコンテンツ フィルタを受信します。
- 受信者 larry@example.com は、ポリシー#2 で定義されているスパム対策、ウイルス対策、アウトブレイク フィルタおよびコンテンツ フィルタを受信します。これは、送信者（@lawfirm.com）と受信者（jim@）が一致するためです。

メッセージ分裂

インテリジェントなメッセージ分裂は、受信者に基づいたコンテンツの異なるセキュリティ ルールを複数の受信者に対するメッセージに個別に適用できるメカニズムです。

各受信者は、該当するメール ポリシー テーブル（着信または発信）の各ポリシーに対して上から順に評価されます。

メッセージに一致する各ポリシーは、これらの受信者に新しいメッセージを作成します。このプロセスが、「メッセージ分裂」と定義されます。

- 一部の受信者が異なるポリシーと一致する場合、受信者は一致したポリシーに基づいてグループ化され、メッセージは一致したポリシー数と同数のメッセージに分裂されます。これらの受信者は、それぞれ適切な「分裂先」に設定されます。

- すべての受信者が同じポリシーと一致する場合、メッセージは分裂されません。反対に、最も多くの分裂が行われるのは、単一のメッセージがメッセージ受信者1人1人に分裂される場合です。
- その後、各メッセージ分裂は、アンチスパム、アンチウイルス、高度なマルウェア防御（着信メッセージのみ）、DLP スキャン（発信メッセージのみ）、アウトブレイク フィルタおよびコンテンツ フィルタにより電子メール パイプラインで個別に処理されます。

次の表に、電子メール パイプラインでメッセージが分裂されるポイントを示します。

ワーク キュー	**メッセージ フィルタ** **（filters）**	電子メール セキュリティ マネージャ スキャン（受信者1人あたり）	**↓すべての受信者のメッセージ**
	スパム対策 **（antispamconfig、antispamupdate）**		メッセージは、メッセージフィルタ処理直後の、スパム対策処理前に分裂されます。 ポリシー 1 に一致するすべての受信者のメッセージ ポリシー 2 に一致するすべての受信者のメッセージ すべてのその他の受信者向けのメッセージ（デフォルトのポリシーに一致） （注） DLP スキャンは、発信メッセージだけに実行されます。
	ウイルス対策 **(antivirusconfig、antivirusupdate)**		
	ファイル レピュテーションとファイル分析（高度なマルウェア防御） **(ampconfig)**		
	グレイメール管理		
	コンテンツ フィルタ **（policyconfig -> filters）**		
	アウトブレイク フィルタ **（outbreakconfig、outbreakflush、outbreakstatus、outbreakupdate）**		
	データ損失の防止 **（policyconfig）**		

（注） 新しいMID（メッセージID）が、各メッセージ分裂用に作成されます（たとえば、MID 1は、MID 2およびMID 3になります）。詳細については、「ロギング」の章を参照してください。また、トレース機能は、メッセージを分裂したポリシーを示します。

電子メール セキュリティ マネージャ ポリシーのポリシー マッチングおよびメッセージ分裂は、アプライアンスで使用できるメッセージ処理の管理に影響を与えます。

関連項目

- 管理例外 （8 ページ）

管理例外

各分裂メッセージの反復処理はパフォーマンスに影響するため、シスコは管理例外単位で十分なコンテンツ セキュリティ ルールを設定することを推奨します。つまり、組織のニーズを評価し、大多数のメッセージがデフォルト ポリシーで処理され、少数のメッセージが、追加の「例外」ポリシーで処理されるように機能を設定します。このようにすることで、メッセージ分裂が最小化され、ワーク キューの各分裂メッセージの処理により受けるシステム パフォーマンスの影響が少なくなります。

メール ポリシーの設定

メール ポリシーはスパム対策やウイルス対策などの特定のセキュリティ設定に、異なるユーザ グループをマップします。

関連項目

- 着信または発信メッセージのデフォルトのメール ポリシーの設定 （8 ページ）
- 送信者および受信者のグループのメール ポリシーの作成 （9 ページ）
- 送信者または受信者に適用するポリシーの検索 （13 ページ）

着信または発信メッセージのデフォルトのメール ポリシーの設定

デフォルトのメール ポリシーは他のメール ポリシーに該当しないメッセージに適用されます。他のポリシーが設定されていない場合、デフォルト ポリシーはすべてのメッセージに適用されます。

はじめる前に

個々のセキュリティ サービスをメール ポリシーに定義する方法を理解します。メール ポリシーをユーザ単位で適用する方法 （2 ページ）を参照してください。

手順

ステップ 1 要件に応じて、次のいずれかを選択します。

- **[メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）]**
- **[メールポリシー（Mail Policies）] > [送信メールポリシー（Outgoing Mail Policies）] を選択します。**

ステップ 2 デフォルトのメール ポリシーに設定するセキュリティ サービスのリンクをクリックします。

（注） デフォルトのセキュリティ サービス設定の場合、このページの最初の設定では、ポリシーでサービスがイネーブルになるかどうかを定義します。[無効（Disable）] をクリックしてすべてのサービスをディセーブルにできます。

ステップ 3 セキュリティ サービスの設定値を設定します。

ステップ 4 [送信（Submit）] をクリックします。

ステップ 5 変更を送信し、保存します。

送信者および受信者のグループのメール ポリシーの作成

はじめる前に

- 個々のセキュリティ サービスをメール ポリシーに定義する方法を理解します。メール ポリシーをユーザ単位で適用する方法 （2 ページ）を参照してください。
- 各受信者は、適切なテーブル（着信または発信）の各ポリシーに対して上から順に評価されます。詳細については、最初に一致したものが有効（4 ページ）を参照してください。
- （任意）メール ポリシーの管理を担当する委任管理者を定義します。委任管理者は、ポリシーのアンチスパム、アンチウイルス、高度なマルウェア防御、アウトブレイク フィルタの設定を編集し、ポリシーのコンテンツ フィルタを有効化または無効化できます。オペレータおよび管理者のみがメール ポリシーの名前または送信者、受信者、またはグループを変更できます。メール ポリシーへのフル アクセス権があるカスタム ユーザ ロールはメール ポリシーに自動的に割り当てられます。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] または [メール ポリシー（Mail Policies）] > [送信メール ポリシー（Outgoing Mail Policies）] を選択します。

ステップ 2 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 3 メール ポリシーの名前を入力します。

ステップ 4 （任意）[編集可能なユーザ(役割)（Editable by (Roles)）] のリンクをクリックし、メール ポリシーの管理を担当する委任管理者のカスタム ユーザ役割を選択します。

ステップ 5 ポリシーのユーザを定義します。ユーザを定義する手順については、メール ポリシーの送信者および受信者の定義 （10 ページ）を参照してください。

ステップ 6 [送信（Submit）] をクリックします。

ステップ 7 メール ポリシーを設定するコンテンツ セキュリティ サービスのリンクをクリックします。

ステップ 8 ドロップダウン リストから、デフォルト設定を使用する代わりに、ポリシーの設定をカスタマイズするオプションを選択します。

ステップ 9 セキュリティ サービスの設定をカスタマイズします。

ステップ 10 変更を送信し、保存します。

次のタスク

関連項目

- メール ポリシーの送信者および受信者の定義 （10 ページ）
- メッセージがスパムかどうかスキャンするためのアプライアンスの設定方法

メール ポリシーの送信者および受信者の定義

次の方法で、ポリシーを適用する送信者と受信者を定義できます。

- 完全な電子メール アドレス：`user@example.com`
- 電子メール アドレスの一部：`user@`
- ドメインのすべてのユーザ：`@example.com`
- 部分ドメインのすべてのユーザ：`@.example.com`
- LDAP クエリーとのマッチング

（注） ユーザの入力は、AsyncOS の GUI および CLI の両方で、大文字と小文字が区別されます。たとえば、ユーザの受信者 `Joe@` を入力すると、`joe@example.com` に送信されるメッセージが一致します。

メール ポリシーの送信者と受信者を定義する際、次の点に注意してください。

- 少なくとも 1 人の送信者と受信者を指定する必要があります。
- 次の場合に一致するポリシーを設定できます。
  - メッセージが、任意の送信者、指定した 1 人以上の送信者からのものであるか、指定した送信者からのものでない場合。
  - メッセージが、任意の受信者、指定した 1 人以上の受信者、指定したすべての受信者に送信されるか、指定した受信者に送信されない場合。

手順

ステップ 1 [ユーザ（Users）] セクションで [ユーザの追加（Add User）] をクリックします。

ステップ 2 ポリシーの送信者を定義します。次のいずれかのオプションを選択します。

- **任意の送信者（Any Sender）**。メッセージが任意の送信者からのものである場合、ポリシーと一致します。

- **次の送信者（Following Senders）**。メッセージが指定した 1 人以上の送信者からのものである場合、ポリシーと一致します。このオプションを選択して、テキストボックスに送信者の詳細を入力するか、LDAP グループ クエリーを選択します。
- **次の送信者は該当しません（Following Senders are Not）**。メッセージが指定した送信者からのものでない場合、ポリシーと一致します。このオプションを選択して、テキストボックスに送信者の詳細を入力するか、LDAP グループ クエリーを選択します。

上記のフィールドを選択する際にどのように送信者の条件が設定されるかを把握するには、例（11 ページ）を参照してください。

ステップ 3 ポリシーの受信者を定義します。次のいずれかのオプションを選択します。

- **任意の受信者（Any Recipient）**。メッセージが任意の受信者に送信される場合、ポリシーと一致します。
- **次の受信者（Following Recipients）**。メッセージが指定した受信者に送信される場合、ポリシーと一致します。このオプションを選択して、テキストボックスに受信者の詳細を入力するか、LDAP グループ クエリーを選択します。

メッセージが指定した 1 人以上の受信者または指定したすべての受信者に送信される場合、ポリシーが一致するかどうかを選択できます。ドロップダウン リストから [1つ以上の条件が一致した場合（If One or More Conditions Match）] または [すべての条件が一致した場合のみ（Only if all conditions match）] のいずれかのオプションを選択します。

- **次の受信者は該当しません（Following Recipients are Not）**。メッセージが指定した受信者に送信されない場合、ポリシーと一致します。このオプションを選択して、テキストボックスに受信者の詳細を入力するか、LDAP グループ クエリーを選択します。

（注） このオプションは、[次の受信者（Following Recipients）] を選択し、ドロップダウン リストから [すべての条件が一致した場合のみ（Only if all conditions match）] を選択した場合にのみ設定できます。

上記のフィールドを選択する際にどのように受信者の条件が設定されるかを把握するには、例（11 ページ）を参照してください。

ステップ 4 [送信（Submit）] をクリックします。

ステップ 5 [ユーザ（Users）] セクションで選択した条件を確認します。

次のタスク

関連項目

- 送信者および受信者のグループのメール ポリシーの作成 （9 ページ）
- 例 （11 ページ）

例

次の表で、[ユーザの追加（Add User）] ページでさまざまなオプションを選択する際に、どのように条件が設定されるかを示します。

Sender			受信者（**Recipient**）			条件
任意の送信者	次の送信者	次の送信者は該当しません	任意の受信者	次の受信者	次の受信者は該当しません	
オン	-	-	-	オン （デフォルト）[すべての条件が一致した場合のみ（Only if all conditions match）] が選択されています。 値： `user1@`、 `user2@`	-	**送信者**：任意 受信者： `user1@[AND]user2@`

-	オン
	値：
	`u1@a.com`、
	`u2@a.com`
		-	-	オン
				（デフォルト）[すべての条件が一致した場合のみ（Only if all conditions match）] が選択されています。
				値：
				`u1@b.com`、
				`u2@b.com`
					オン
					値：
					`u3@b.com`、
					`u4@b.com`
						送信者：
						`u1@a.com[OR]u2@a.com`
						受信者：
						`[u1@b.com[AND]u2@b.com]`
						`[AND]`
						`[[NOT]`
						`[u3@b.com[AND]u4@b.com]]`

-	-	オン 値： u1@a.com、 u2@a.com	-	オン [1つ以上の条件が一致した場合（If One or More Conditions Match）] オプションも選択されます 値： u1@b.com、 u2@b.com	-	**送信者：** [NOT] [u1@a.com[OR]u2@a.com] 受信者： u1@b.com [OR] u2@b.com

関連項目

- メール ポリシーの送信者および受信者の定義 （10 ページ）

送信者または受信者に適用するポリシーの検索

すでに着信または発信メール ポリシーに定義されているユーザを検索するには、[メールポリシー（Mail Policies）] ページの上部にある [ポリシー検索（Find Policies）] セクションを使用します。

たとえば、bob@example.com と入力して、[ポリシー検索（Find Policies）] ボタンをクリックすると、ポリシーに一致する定義済みのユーザが含まれるポリシーが表示されます。

そのポリシーのユーザを編集するには、ポリシーの名前をクリックします。

ユーザを検索する場合、デフォルト ポリシーは常に表示されるため注意してください。これは、定義上、送信者または受信者が設定されているポリシーと一致しない場合、デフォルトのポリシーが必ず一致するためです。

関連項目

- 管理例外 （8 ページ）

管理例外

前述の2つの例で示されている手順を使用して、管理例外に基づいたポリシーの作成および設定を開始できます。つまり、組織のニーズを評価した後で、メッセージの大部分がデフォルトポリシーで処理されるように、ポリシーを設定できます。また、必要に応じて、異なるポリシーを管理して、特定のユーザまたはユーザ グループの追加「例外」ポリシーを作成できます。このようにすることで、メッセージ分裂が最小化され、ワーク キューの各分裂メッセージの処理により受けるシステム パフォーマンスの影響が少なくなります。

スパム、ウイルスおよびポリシー実行に対する組織またはユーザの許容値に基づいて、ポリシーを定義できます。次の表に、いくつかのポリシーの例の概要を示します。「積極的な」ポリシーでは、エンドユーザのメールボックスに到達するスパムおよびウイルスの量が最小限に抑えられます。「保守的な」ポリシーでは、偽陽性を回避し、ポリシーに関係なく、ユーザによるメッセージの見落としを防ぐことができます。

表 *2*：積極的および保守的な電子メール セキュリティ マネージャ設定

	積極的な設定	保守的な設定
スパム対策	陽性と判定されたスパム：ドロップ 陽性と疑わしいスパム：隔離 マーケティング メール：メッセージの件名の前に「[Marketing]」が追加されて配信	陽性と判定されたスパム：隔離 陽性と疑わしいスパム：メッセージの件名の前に「[Suspected Spam]」が追加されて配信 マーケティング メール：ディセーブル
アンチウイルス	修復されたメッセージ：配信 暗号化されたメッセージ：ドロップ スキャンできないメッセージ：ドロップ 感染メッセージ：ドロップ	修復されたメッセージ：配信 暗号化されたメッセージ：隔離 スキャンできないメッセージ：隔離 感染メッセージ：ドロップ
Advanced Malware Protection **（ファイル レピュテーション フィルタリングおよびファイル分析）**	スキャンされていない添付ファイル：ドロップ マルウェア ファイルが添付されたメッセージ：ドロップ 保留中のファイル分析のあるメッセージ：隔離	スキャンされていない添付ファイル：メッセージの件名の前に「[WARNING: ATTACHMENT UNSCANNED]」が追加されて配信。 マルウェア ファイルが添付されたメッセージ：ドロップ 保留中のファイル分析のあるメッセージ：メッセージの件名の前に「[WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]」が追加されて配信。
ウイルス フィルタ	イネーブル、バイパスできる特定のファイル名拡張子またはドメインなし すべてのメッセージのメッセージ変更の有効化	バイパスできるファイル名拡張子またはドメインの有効化 未署名のメッセージのメッセージ変更の有効化

メッセージ ヘッダーの優先順位の設定

メッセージヘッダーの優先順位を設定して、アプライアンスの受信メッセージと送信メッセージを一致させることができます。

重要 アプライアンスが受信メッセージと送信メッセージのメッセージヘッダーをチェックする際の優先順位を設定できます。最初に、アプライアンスはすべてのメールポリシーで優先順位の最も高いメッセージヘッダーをチェックします。いずれのメールポリシーとも一致するヘッダーがない場合、アプライアンスはすべてのメールポリシーの優先順位リスト内の次のメッセージヘッダーを検索します。いずれのメールポリシーとも一致するメッセージヘッダーがない場合は、デフォルトのメールポリシー設定が使用されます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [メールポリシー設定（Mail Policy Settings）] に移動します。

デフォルトでは、[エンベロープ送信者（Envelope Sender）] ヘッダーは優先度 1 に設定されています。[エンベロープ送信者（Envelope Sender）] リンクをクリックして優先度を変更できます。

ステップ 2 [優先順位の追加（Add Priority）] をクリックし、適切なヘッダー名（たとえば、ヘッダー「送信元（From）」）のチェックボックスをオンにして、新しい優先順位を追加します。

ステップ 3 [送信（Submit）] をクリックし、変更をコミットします。