# ポリシー設定

[設定(Settings)](歯車アイコン)> [ポリシー(Policy)] ページの設定によって、Cisco Secure Email Cloud Mailbox によるメールの処理方法が決まります。ビジネスの設定(11 ページ)の手順では、デフォルト設定が適用されます。設定を変更するには、変更を行い、[Save and Apply] ボタンをクリックします。

**表 1　ポリシー設定**

| 設定 | 説明 | オプション | デフォルト |
|---|---|---|---|
| **Permission Mode** | 適用できる修復ポリシーのタイプを定義します。 | ■ [Audit]:可視性のみを許可し、修復は許可しません。読み取り専用権限が Microsoft 365 から要求されます。<br><br>[Audit] を選択した場合は、[Attachment Analysis] および [Message Analysis] の方向をのみを設定する必要があります。その他のポリシー設定は適用されません。<br><br>■ [Audit with Enforcement]:可視性、およびオンデマンドまたは自動の修復(疑わしいメッセージの移動または削除)が可能です。読み取り/書き込み権限が Microsoft 365 から要求されます。 | ビジネスの設定時に選択します。<br><br>[Permission Mode] を変更すると、Microsoft 365 権限を再設定するようにリダイレクトされます。<br>ジャーナリングを設定するように指示される場合もあります。すでにジャーナリングを設定している場合は、この手順を省略できます。<br><br>注:[監査と施行(Audit with Enforcement)] モードを選択した場合は、[自動修復(Automated Remediation)] の設定も確認する必要があります。 |
| **Cisco Secure Email Gateway(SEG)** | Cisco Secure Email Gateway(SEG)の有無は、Cloud Mailbox が送信者 IP を識別する方法に影響します。 | ■ [何も選択されていません(SEG はありません)(Nothing selected (No SEG))]<br><br>■ [SEG があります(SEG is present)]<br><br>– [Cisco SEG のデフォルトヘッダーを使用する(Use Cisco SEG default header)] (X-IronPort-RemoteIP)。<br><br>– [SEG のカスタムヘッダーを使用する(Use Custom SEG header)]。使用するヘッダーを追加する必要があります。 | [何も選択されていません(SEG はありません)(Nothing selected (No SEG))]。<br><br>この設定が有効になるまでに最大で 5 分かかることがあります。<br><br>詳細については、ゲートウェイを使用している場合のポリシー設定(17 ページ)を参照してください。 |
| **Message Analysis** | 動的に分析されるメッセージの方向。 | ■ **着信**<br><br>■ **発信**<br><br>■ **内部** | **すべて** |

**表 1　ポリシー設定(続き)**

| 設定 | 説明 | オプション | デフォルト |
|---|---|---|---|
| **Attachment Analysis** | Cisco Secure Malware Analytics(以前の Cisco Threat Grid)によって分析されるメールの添付ファイルの方向。 | ■ **着信**<br>■ **発信**<br>■ **内部** | **着信** |
| **Remediation Actions** | **悪意のある**、**フィッシング**、**スパム**、または**グレイメール**のコンテンツを含むことが判明したメッセージの修復アクション。 | ■ [隔離に移動(Move to Quarantine)]<br>■ [Move to Trash]<br>■ [Move to Junk]<br>■ [No Action]<br>**注:**送信者アドレスが Exchange の送信者許可リストに属している場合、またはメッセージが Microsoft 365 によってすでに修復されている場合、修復アクションは適用されません。 | ■ 悪意がある:[隔離に移動(Move to Quarantine)]<br>■ フィッシング:[隔離に移動(Move to Quarantine)]<br>■ [Spam] - [Move to Junk]<br>■ [Graymail] - [No Action] |
| **[安全な送信者(Safe Sender)]** | このボックスがオンになっている場合、スパムまたはグレイメールと判定された安全な送信者メッセージ(Microsoft のジャーナルヘッダーにタグ付け)は修復されません。 | **選択**または**選択解除** | **オフ** |
| **Automated Remediation** | | | |
| **Domain-specific auto-remediation** | 特定のドメインに自動修復を適用します。 | **選択**または**選択解除** | **選択解除**。[監査と施行(Audit with Enforcement)] モードをオンにする場合は、チェックボックスをオンに設定し、特定のドメインに自動修復が適用されるようにします。 |
| **Apply auto-remediation to domains not in the domain list above** | ドメインが明示的にリストに含まれていない場合に適用されます。たとえば、新しいドメインが Microsoft 365 アカウントに追加されているが、クラウドメールボックス にインポートされていない場合などです。 | **選択**または**選択解除** | **選択解除**。[監査と施行(Audit with Enforcement)] モードをオンにする場合は、このチェックボックスをオンに設定し、すべての内部電子メールに自動修復が適用されるようにします。 |

# ゲートウェイを使用している場合のポリシー設定

Cisco E メール セキュリティ アプライアンスまたは同様のゲートウェイを配置している場合は、次のポリシー設定の使用を検討してください。

**表 2　ゲートウェイで推奨されるポリシー設定**

| 設定名 | 推奨される選択 |
|---|---|
| **Cisco Secure Email Gateway（SEG）** | [SEG があります（SEG is present）]。ヘッダーを表示します |
| **Message Analysis** | [Outgoing] と [Internal] |
| **Attachment Analysis** | **なし** |
| **Remediation Actions** | ■ 悪意がある：[隔離に移動（Move to Quarantine）]<br>■ フィッシング：[隔離に移動（Move to Quarantine）]<br>■ [Spam] - [Move to Junk] |

Cisco Secure Email Gateway（SEG）があり、受信ジャーナルで SEG の識別に使用できるヘッダーを示すことで、Cloud Mailbox でメッセージの真の発信者を特定できるようにすることが重要です。この設定を行わないと、SEG から送信されたすべてのメッセージが表示され、誤検出が発生する可能性があります。

Cisco Secure Email Cloud Gateway（旧 CES）または Cisco Secure Email Gateway（旧 ESA）のヘッダーの確認または設定については、
https://docs.ces.cisco.com/docs/configuring-asyncos-message-filter-to-add-sender-ip-header-for-cloud-mailbox
を参照してください。

また、ジャーナルが Microsoft 365 から クラウドメールボックス に直接送信されるように、アプライアンスをバイパスすることを推奨します。バイパスするには、ビジネスの設定（11 ページ）で説明されているように、Microsoft 365 にコネクタを追加します。

# CES IMD のお客様向けのポリシー設定

CES Internal Mailbox Defense（IMD）のお客様の場合、ポリシー設定は標準の クラウドメールボックス を使用している場合とは若干異なります。

- [メッセージ分析（Message Analysis）] は [内部（Internal）] に設定され、[ポリシー（Policy）] ページには表示されません。
- [Attachment Analysis] は、[Enabled] または [Disabled] に設定できます。これを [Enabled] に設定すると、内部添付ファイルがスキャンされます。
- 他のすべてのポリシー設定は、前のセクションで説明したとおりです。