ポリシー設定

[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。**Secure Email Threat Defense 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、[保存して適用(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
メッセージの送信元(Message Source)	メッセージの送信元を定義します。	■ **Microsoft 365** ■ **Gateway(ゲートウェイ)**(着信メッセージのみ)	Cisco Secure Email Threat Defense を設定するときに手動で選択します。
可視性と修復(Visibility & Remediation)	適用できる修復ポリシーのタイプを定義します。	■ **Microsoft 365 認証(Microsoft 365 Authentication)** – **読み取り/書き込み(Read/Write)**: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。 – **読み取り(Read)**: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。 [読み取り(Read)] を選択した場合は、[添付ファイルの分析(Attachment Analysis)] および [メッセージの分析(Message Analysis)] の方向のみ設定する必要があります。修復ポリシーは適用されません。 ■ **認証なし(No Authentication)** 可視性のみを許可します。	Cisco Secure Email Threat Defense を設定するときに手動で選択します。 [Microsoft 365 認証(Microsoft 365 Authentication)] 設定を変更すると、Microsoft 365 の権限をリセットするようにリダイレクトされます。 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。 **注:**[Microsoft 365 認証:読み取り/書き込み(Microsoft 365 Authentication: Read/Write)] を選択した場合は、[自動修復ポリシー(Automated Remediation Policy)] の設定も確認する必要があります。

表 1　ポリシー設定(続き)

設定	説明	オプション	デフォルト
Cisco Secure Email Gateway(SEG)	Cisco Secure Email Gateway(SEG)の有無は、Secure Email Threat Defense 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)) ■ **SEG があります(SEG is present)** – **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)。 – **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。	Cisco Secure Email Threat Defense を設定するときに手動で選択します。 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(19 ページ)を参照してください。
メッセージの分析(Message Analysis)	動的に分析されるメッセージ。次のものが含まれます。 ■ メッセージの方向(Direction of messages) ■ Cisco Secure Malware Analytics によって分析されるメールの添付ファイルの方向 ■ スパムとグレイメールの分析(Analysis of Spam and Graymail)	■ **メッセージの方向(Direction of Messages)** – **着信(Incoming)** – **発信(Outgoing)** – **内部(Internal)** ■ **添付ファイルの方向(Direction of Attachments)** – **着信(Incoming)** – **発信(Outgoing)** – **内部(Internal)** ■ **スパムおよびグレイメール(Spam and Graymail)** – [オン(On)] または [オフ(Off)]	■ **メッセージの方向(Direction of Messages)** – メッセージの送信元が Microsoft O365 の場合は [すべて(All)] – メッセージの送信元がゲートウェイの場合は [着信(Incoming)] ■ **添付ファイルの方向(Direction of Attachments)** – **着信(Incoming)** ■ **スパムおよびグレイメール(Spam and Graymail)** – 2023 年 5 月 9 日以降に作成されたすべてのアカウントで [オフ(Off)]
自動修復ポリシー(Automated Remediation Policy)	次であることが判明したメッセージの修復アクション: ■ **脅威**(BEC、詐欺、フィッシング、または悪意のある) ■ **Spam** ■ **グレイメール**	■ **アクションなし(No Action)** ■ **隔離に移動(Move to Quarantine)** ■ **ゴミ箱に移動(Move to Trash)** ■ **迷惑メールに移動(Move to Junk)** **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。	■ [自動修復ポリシー(Automated Remediation Policy)] の切り替え:オフ ■ 脅威:[隔離に移動(Move to Quarantine)] ■ [スパム(Spam)] - [迷惑メールに移動(Move to Junk)] ■ [グレイメール(Graymail)] - [アクションなし(No Action)]

表 1　ポリシー設定(続き)

設定	説明	オプション	デフォルト
Safe Sender: Microsoft Safe Sender メッセージをスパムまたはグレイメールの判定で修復しないでください。	このボックスがオンになっている場合、ジャーナルヘッダーで Microsoft により Safe Sender としてタグ付けされたメッセージのうち、Secure Email Threat Defense によってスパムまたはグレイメールと判定されたものは修復されません。	[選択(Checked)] または [選択解除(Unchecked)]	**選択解除(Unchecked)**
インポート済みのドメイン: メッセージの方向を決定するためにドメインがインポートされます。自動修復ポリシーからドメインを除外できます。			
自動修復の適用(Apply Auto-Remediation)	特定のドメインに自動修復を適用します。	[選択(Checked)] または [選択解除(Unchecked)]	選択解除(Unchecked)。[読み取り/書き込み(Read/Write)] 修復モードをオンにする場合は、これらのチェックボックスをオンにして特定のドメインに自動修復が適用されるようにします。
上のドメインリストにないドメインに自動修復を適用する(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、Secure Email Threat Defense にインポートされていない場合などです。	[選択(Checked)] または [選択解除(Unchecked)]	**選択解除(Unchecked)**。[読み取り/書き込み(Read/Write)] 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して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	[発信(Outgoing)] と [内部(Internal)]
Attachment Analysis	**なし**
Remediation Actions	■ 脅威:[隔離に移動(Move to Quarantine)] ■ [スパム(Spam)] - [迷惑メールに移動(Move to Junk)]

Cisco Secure Email Gateway(SEG)が存在することと、受信ジャーナルでの SEG の識別に使用できるヘッダーを示すことにより、Secure Email Threat Defense 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、メッセージの送信元に Microsoft 365 を使用している場合は、ジャーナルが Microsoft 365 から Secure Email Threat Defense 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、Secure Email Threat Defense 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。

メッセージの送信元の切り替え

メッセージの送信元を変更するには、[ポリシー（Policy）] ページに移動します。

1. 新しいメッセージの送信元に対応するラジオボタンを選択します。
2. メッセージの送信元を切り替えることを示す通知が表示されます。[Continue] をクリックします。
3. [メッセージの送信元の切り替え（Switch Message Source）] ダイアログが表示されます。Cisco Secure Email Threat Defense へのメッセージの送信を停止するには、以前のメッセージの送信元を設定する必要があります。この設定方法の詳細については、Cisco Secure Email Threat Defense ジャーナルルールの削除（61 ページ）またはメッセージの送信を停止するようにゲートウェイを構成する（62 ページ）を参照してください。
4. 以前の送信元でジャーナルまたはメッセージの送信を停止したことを示すチェックボックスをオンにしてから、[次へ（Next）] をクリックします。
5. ダイアログに表示されるメッセージ受信アドレスまたはジャーナルアドレスを使用して、新しいメッセージの送信元を設定します。各タイプのメッセージの送信元を設定する手順については、メッセージの送信元の設定（13 ページ）で詳しく説明します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。