Secure Email Threat Defense の設定

Cisco Secure Email Threat Defense の設定には、次の手順が含まれます。

1. アカウントへのサインイン（11 ページ）
2. Cisco Secure Email Gateway（SEG）の有無を表示（12 ページ）
3. メッセージの送信元、可視性と修復モードの選択（12 ページ）
4. メッセージの送信元の設定（13 ページ）
5. ポリシー設定の確認（14 ページ）
6. Microsoft の電子メールドメインのインポート（15 ページ）

次の手順は、**要件（9 ページ）**を満たしていることを前提としています。

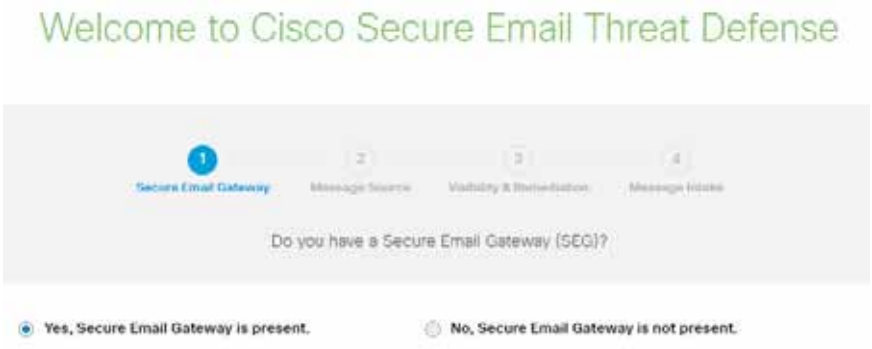
アカウントへのサインイン

1. シスコからのウェルカムメールの指示に従って、ユーザーアカウントを設定します。

   Cisco Secure Email Threat Defense は、Cisco Security Cloud Sign On を使用してユーザー認証を管理します。Security Cloud Sign On サインオンの詳細については、https://cisco.com/go/securesignon を参照してください。既存の SecureX Threat Response、Cisco Secure Malware Analytics（旧 Threat Grid）、または Cisco Secure Endpoint（旧 AMP）のお客様は、既存のクレデンシャルでサインインしてください。既存のユーザーでない場合は、新しい Security Cloud Sign On アカウントを作成する必要があります。

2. ログインに成功したら、利用規約に同意します。

3. [ようこそ（Welcome to）] **Cisco Secure Email Threat Defense** ページにアクセスできるようになりました。次のセクションで説明されているように、セットアップウィザードに従います。



Cisco Secure Email Gateway（SEG）の有無を表示

（次のセクションで選ぶ）メッセージの送信元が何であれ、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、Cisco 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。

1. [はい（Yes）] または [いいえ（No）] を選択して Cisco Secure Email Gateway（SEG）が存在するかどうかを確認し、[次へ（Next）] をクリックします。
2. [はい（Yes）] と答えた場合は、SEG のタイプとヘッダーを入力します。[次へ（Next）] をクリックします。

メッセージの送信元、可視性と修復モードの選択

1. メッセージの送信元を、Microsoft O365 またはゲートウェイのいずれかから選択します。前の手順で [SEG はありません（No SEG）] を選択した場合、メッセージの送信元には Microsoft O365 が選択されていると想定されます。
2. 可視性と修復を選択します。

   可視性と修復モードは、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。

     注：[読み取り/書き込み（Read/Write）] を選択した場合は、セットアップの完了後に**ポリシー設定（17 ページ）**で自動修復ポリシーをオンにする必要があります。すべての内部電子メールに自動修復を適用するには、[ポリシー（Policy）] ページの [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 domain not in domain list）] ボックスがオンに設定されていることを確認します。

   認証なし（No Authentication）

   このオプションは、メッセージの送信元として Cisco SEG を使用している場合に使用できます。可視性のみを提供します。メッセージを修復することはできません。

3. Microsoft 365 認証を選択した場合は、Microsoft 365 に接続します。
   a. [次へ（Next）] をクリックして Microsoft 365 に接続します。
   b. 指示に従って、Microsoft 365 アカウントにログインします。このアカウントにはグローバル管理者権限が必要です。このアカウントは Cisco Secure Email Threat Defense で保存または使用されません。これらの権限が必要な理由については、Cisco Secure Email Threat Defense の FAQ「Secure Email Threat Defense を設定するために Microsoft 365 グローバル管理者権限が必要なのはなぜですか（Why are Microsoft 365 Global Admin rights required to set up Secure Email Threat Defense?）」を参照してください。
   c. [承認（Accept）] をクリックして、Cisco Secure Email Threat Defense アプリケーションの権限を承認します。Cisco Secure Email Threat Defense の設定ページにリダイレクトされます。
   d. [次へ（Next）] をクリックします。

メッセージの送信元の設定

選択したメッセージの送信元の手順を完了します。

メッセージの送信元：Microsoft O365

メッセージの送信元に Microsoft O365 を選択した場合は、ジャーナルを Cisco Secure Email Threat Defense へ送信するように Microsoft 365 を設定する必要があります。これを行うには、ジャーナルルールを追加します。ゲートウェイを配置している場合は、ジャーナルルールを追加する前に、Microsoft 365 にコネクタを追加します。

1. **Cisco Secure Email Gateway（SEG）を使用しているユーザーの場合**：Microsoft 365 にコネクタを追加します。

   ジャーナルが Cisco Secure Email Gateway を経由することなく、Microsoft 365 から Cisco Secure Email Threat Defense に直接送信されるようにするため、Microsoft 365 に送信コネクタを追加することをお勧めします。コネクタはジャーナルを設定する前に追加する必要があります。

   Microsoft 365 Exchange 管理センターから、[コネクタの追加（Add a connctor）] ウィザードの次の設定を使用して新しいコネクタを作成します。

   - [接続元（Connection from）]：Office 365
   - [接続先（Connection to）]：パートナー組織
   - [コネクタ名（Connector name）]：Cisco Secure Email Threat Defense へのアウトバウンド（[オンにする（Turn it on）] チェックボックスを選択）
   - [コネクタの使用（Use of connector）]：電子メールメッセージがこれらのドメインに送信される場合のみ（北米環境の場合は **mail.cmd.cisco.com**、ヨーロッパ環境の場合は **mail.eu.cmd.cisco.com**、オーストラリア環境の場合は **mail.au.etd.cisco.com**、インド環境の場合は **mail.in.etd.cisco.com** を追加）
   - [ルーティング（Routing）]：パートナーのドメインに関連付けられた MX レコードを使用
   - [セキュリティの制限（Security restrictions）]：接続を保護するために、常に信頼できる認証局（CA）によって発行されたトランスポート層セキュリティ（TLS）を使用（推奨）
   - [検証用の電子メール（Validation email）]：Cisco Secure Email Threat Defense の設定ページのジャーナルアドレス

     注：O365 テナントで、Exchange トランスポートルールを使用して、送信メールを既存のコネクタにルーティングする条件付きメールルーティングがすでに設定されている場合、コネクタ検証に失敗することがあります。ジャーナルメッセージにはシステム特権があり、トランスポートルールの影響を受けませんが、コネクタ検証テストの電子メールには特権がなく、トランスポートルールの影響を受けます。

     この検証の問題を解決するには、既存のトランスポートルールを見つけて、Cisco Secure Email Threat Defense ジャーナルアドレスの例外を追加します。この変更が有効になるのを待ってから、新しいコネクタの検証を再テストしてください。

2. Cisco Secure Email Threat Defense にジャーナルを送信するように Microsoft 365 を設定します。これを行うには、ジャーナルルールを追加します。

   a. Cisco Secure Email Threat Defense の設定ページから、ジャーナルアドレスをコピーします。後でこのプロセスを繰り返す必要がある場合は、[管理（Administration）] ページでジャーナルアドレスを確認することもできます。

   b. Microsoft Purview コンプライアンスポータル（https://compliance.microsoft.com/homepage）に移動します。

   c. [ソリューション（Solutions）] > [データライフサイクル管理（Data lifecycle management）] > [Exchange（レガシー）（Exchange (legacy)）] > [ジャーナルルール（Journal rules）] の順に移動します。

d. まだ実行していない場合は、[配信不能ジャーナルレポートの送信先(Send undeliverable journal reports to)] フィールドに Exchange の受信者を追加して、[保存(Save)] をクリックします。使用される電子メールアドレスはジャーナリングされません。Cisco Secure Email Threat Defense の分析対象とするアドレスを使用しないでください。この目的で使用する受信者がいない場合は、受信者を作成する必要があります。

e. [ジャーナルルール(Journal rules)] ページに戻ります。[+] ボタンをクリックして、新しいジャーナルルールを作成します。

f. Cisco Secure Email Threat Defense の設定ページのジャーナルアドレスを [ジャーナルレポートの送信先(Send journal reports to)] フィールドに貼り付けます。

g. [ジャーナルルール名(Journal rule name)] フィールドに「**Cisco Secure Email Threat Defense**」と入力します。

h. [ジャーナルメッセージの送受信元(Journal messages sent or received from)] で、[全員(Everyone)] を選択します。

i. [ジャーナルするメッセージのタイプ(Type of message to journal)] で、[すべてのメッセージ(All messages)] を選択します。

j. [次へ(Next)] をクリックします。

k. 選択内容を確認してから、[送信(Submit)] をクリックしてルールの作成を終了します。

3. Cisco Secure Email Threat Defense の設定ページに戻ります。[ポリシーの確認(Review policy)] をクリックします。

メッセージの送信元:ゲートウェイ

メッセージの送信元にゲートウェイを選択した場合は、Cisco Secure Email Cloud Gateway の Threat Defense コネクタを有効にし、メッセージを Secure Email Threat Defense に送信できるようにします。

1. Cisco Secure Email Threat Defense の設定ページから、メッセージ受信アドレスをコピーします。後でこのプロセスを繰り返す必要がある場合は、[管理(Administration)] ページでメッセージ受信アドレスを確認できます。
2. Cisco Secure Email Cloud Gateway UI から、[セキュリティサービス(Security Services)] > [Threat Defense Connector] の順に選択します。
3. [Threat Defense Connector の有効化(Enable Threat Defense Connector)] チェックボックスをオンにします。
4. 手順 1 で Cisco Secure Email Threat Defense からコピーしたメッセージ受信アドレスを入力します。
5. [送信(Submit)] をクリックして変更を確定します。
6. Cisco Secure Email Threat Defense の設定ページに戻ります。[ポリシーの確認(Review policy)] をクリックします。

ポリシー設定の確認

ポリシー設定については、**ポリシー設定(17 ページ)**を参照してください。[Microsoft O365 認証:読み取り/書き込み(Microsoft O365 Authentication: Read/Write)] モードを選択した場合は、[自動修復(Automated Remediation Policy)] の設定も確認する必要があります。すべての内部電子メールに自動修復を適用するには、[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 domain not in domain list)] がオンに設定されていることを確認します。ドメインがインポートされたら、**自動修復ポリシー**の切り替えをオンにできます。

Microsoft の電子メールドメインのインポート

Cisco Secure Email Threat Defense は、Microsoft 365 テナントから電子メール機能を持つドメインをインポートします。ドメインをインポートして、特定のドメインに自動修復を適用できるようにします。Cisco Secure Email Threat Defense は、[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）] ボックスがオンかオフかによって、新しくインポートされたドメインを異なる方法で処理します。

- [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）] がオンになっている場合、インポートされるすべての新しいドメインに自動修復が適用されます。
- [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）] がオフになっている場合、インポートされる新しいドメインに自動修復は適用されません。

デフォルトでは、[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）] はオフになっています。

手動インポート

Microsoft 365 電子メールドメインを手動でインポートするには、次の手順を実行します（Cisco Secure Email Threat Defense の初回セットアップ時に推奨）。

1. [ポリシー（Policy）] ページに移動します。
2. [インンポートされたドメインの更新（Update Imported Domains）] ボタンをクリックし、ドメインを Cisco Secure Email Threat Defense にインポートします。
3. 各ドメインの横にあるチェックボックスを使用して、そのドメインの自動修復設定を調整します。
4. また、[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）] を選択して、自動修復がすべての内部メールと後で自動的にインポートされるドメインに適用されるようにすることもお勧めします。
5. [保存して適用（Save and Apply）] をクリックします。

自動インポート

リストを最新にするために、ドメインは 24 時間ごとに自動的にインポートされます。

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。