Cisco SecureX Threat Response との統合

この章は、次の項で構成されています。

電子メールゲートウェイと Cisco SecureX Threat Response の統合

Cisco SecureXは、すべてのシスコセキュリティ製品に組み込まれたセキュリティプラットフォームです。これは新しいテクノロジーを導入する必要のないクラウドネイティブです。Cisco SecureX は、可視性を統合し、自動化を可能にして、ネットワーク、エンドポイント、クラウド、およびアプリケーション全体のセキュリティを強化するプラットフォームを提供することで、脅威からの保護の要求を簡素化します。統合プラットフォームで技術を連携することで、Cisco SecureXは測定可能な分析情報、望ましい成果、比類のないチーム間のコラボレーションを実現します。Cisco SecureX では、セキュリティ インフラストラクチャを連携させて機能を拡張できます。

電子メールゲートウェイと Cisco SecureX Threat Response の統合には、次のセクションが含まれています。

電子メールゲートウェイを Cisco SecureX Threat Response と統合し、Cisco SecureX Threat Response で以下のアクションを実行できます。

- 組織内の複数の電子メールゲートウェイから電子メールデータを表示および送信します。

- 電子メールレポート、送信者とターゲットの関係、複数の電子メールアドレスと件名行の検索、およびメッセージトラッキングで確認された脅威を特定、調査、修復します。
- 侵害されたユーザまたは発信電子メールポリシーに違反するユーザをブロックします。
- 特定した脅威を迅速に解決し、特定した脅威に対して推奨されるアクションを実行します。
- 脅威をドキュメント化して調査内容を保存し、他のデバイスと情報を共有します。
- 悪意のあるドメインのブロック、不審な観測対象の追跡、承認ワークフローの開始、または電子メールポリシーを更新するための IT チケットの作成を行います。

Cisco SecureX Threat Response には、次の URL を使用してアクセスできます。

https://securex.us.security.cisco.com/login

Cisco Secure Email Gateway は高度な脅威からの保護機能を備えており、脅威を迅速に検出、ブロック、修復します。また、データ損失を防ぎ、送信中の重要な情報をエンドツーエンド暗号化によって保護します。ESA モジュールで強化できる観測対象の詳細については、https://securex.us.security.cisco.com/settings/modules/availableに移動し、Cisco SecureX と統合するモジュールに移動して、[詳細情報（Learn More）] をクリックしてください。

電子メールゲートウェイと Cisco SecureX Threat Response の統合方法

表 *1*：電子メールゲートウェイと *Cisco SecureX Threat Response* の統合方法

	操作内容	詳細
ステップ 1	前提条件を確認します。	前提条件 （4 ページ）

	操作内容	詳細
ステップ 2	（クラシックライセンスモードを使用するユーザにのみ適用されます）。 （注） スマートライセンスモードを使用している場合は、Cisco Cloud Services ポータルが電子メールゲートウェイで自動的に有効になるため、この手順は省略できます。 電子メールゲートウェイで Cisco Cloud Services ポータルを有効にします。	電子メールゲートウェイでの Cisco Cloud Services ポータルの有効化 （5 ページ）
ステップ 3	Cisco SecureX で、電子メールゲートウェイをデバイスとして追加し、登録して、登録トークンを生成します。	詳細については、次を参照してください。https://securex.us.security.cisco.com/help/settings-devices
ステップ 4	（クラシックライセンスモードを使用するユーザにのみ適用されます）。 （注） スマートライセンスモードを使用している場合は、電子メールゲートウェイが Cisco Cloud Services ポータルに自動的に登録されるため、この手順は省略できます。 Cisco Cloud Services ポータルに電子メールゲートウェイを登録します。	Cisco Cloud Services ポータルへの電子メールゲートウェイの登録 （6 ページ）
ステップ 5	登録が成功したかどうかを確認します。	登録が成功したかどうかの確認 （6 ページ）
ステップ 6	電子メールゲートウェイでの Cisco SecureX Threat Response の有効化	電子メールゲートウェイでの Cisco SecureX Threat Response の有効化 （7 ページ）

	操作内容	詳細
ステップ 7	Cisco SecureX で、Cisco Secure Email Gateway モジュールを追加します。	詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動して、Cisco SecureX と統合するために必要な Cisco Secure Email Gatewayモジュールを選択し、**[新しいモジュールの追加（Add New Module）]** をクリックして、そのページに記載されている手順を参照してください。

前提条件

（注） すでに Cisco Threat Response ユーザアカウントを持っている場合は、Cisco SecureX ユーザアカウントを作成する必要はありません。Cisco Threat Response ユーザアカウントのクレデンシャルを使用して Cisco SecureX にログインできます。

- 管理者アクセス権を使用して、Cisco SecureX でユーザアカウントを作成していることを確認します。新しいユーザアカウントを作成するには、URL（https://securex.us.security.cisco.com/login）を使用して **Cisco SecureX のログイン**ページに移動し、ログインページで [SecureXサインオンアカウントの作成（Create a SecureX Sign-on Account）] をクリックします。新しいユーザアカウントを作成できない場合は、Cisco TAC に連絡してサポートを受けてください。
- 電子メールゲートウェイにアクセスするために指定したホスト名を、設定した DNS サーバーが解決できることを確認します。
- （プロキシサーバを使用していない場合のみ）電子メールゲートウェイを Cisco SecureX Threat Response に登録する場合、ファイアウォールで HTTPS（インおよびアウト）443 ポートが次の FQDN に対してオープンになっていることを確認してください。
  - api-sse.cisco.com（NAM ユーザのみに対応）
  - api.eu.sse.itd.cisco.com（欧州連合（EU）のユーザのみに対応）
  - api.apj.sse.itd.cisco.com（APJC ユーザのみに対応）
  - est.sco.cisco.com（APJC、EU、および NAM ユーザに対応）

  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。
- （電子メールゲートウェイにスマートライセンスが登録されているユーザの場合）（Cisco Smart Software Manager ポータルで作成された）スマートアカウントが Cisco Security Services Exchange にすでにリンクされていることを確認します。詳細については、次の資料を参照してください。

- （NAM ユーザに適用）https://admin.sse.itd.cisco.com/assets/static/online-help/index.html#!t_link_accounts.html
- （欧州連合（EU）のユーザに適用）https://admin.eu.sse.itd.cisco.com/assets/static/online-help/index.html#!t_link_accounts.html
- （APJC ユーザに適用）https://admin.apj.sse.itd.cisco.com/assets/static/online-help/index.html#!t_link_accounts.html

電子メールゲートウェイでの Cisco Cloud Services ポータルの有効化

手順

ステップ 1 電子メールゲートウェイにログインします。

ステップ 2 [ネットワーク（Networks）]>[クラウドサービス設定（Cloud Service Settings）] を選択します。

ステップ 3 **[有効（Enable）]** をクリックします。

ステップ 4 [Cisco Cloud Servicesの有効化（Enable Cisco Cloud Services）] チェックボックスをオンにします。

ステップ 5 必要な Cisco Secure サーバを選択して、電子メールゲートウェイを Cisco Cloud Services ポータルに接続します。

ステップ 6 変更を送信し、保存します。

ステップ 7 数分待ってから、**[登録（Register）]** ボタンが [クラウドサービス設定（Cloud Services Settings）] ページに表示されるかどうかを確認します。

クラスタ化された設定では、ログイン中の電子メールゲートウェイはマシンモードの Cisco Cloud Services ポータルにのみ登録できます。電子メールゲートウェイを Cisco Cloud Services ポータルにスタンドアロンモードですでに登録している場合は、電子メールゲートウェイをクラスタに参加させる前に手動で登録を解除してください。

（注） CLI を使用して Cisco Cloud Services ポータルを有効にするには、`cloudserviceconfig` コマンドを使用します。

次のタスク

Cisco Cloud Services ポータルに電子メールゲートウェイを登録します。詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動して、Cisco SecureX と統合するモジュールを選択し、**[新しいモジュールの追加（Add New Module）]** をクリックしてページに記載されている手順を参照してください。

Cisco Cloud Services ポータルへの電子メールゲートウェイの登録

手順

ステップ 1 [ネットワーク（Networks）] > [クラウドサービスの設定（Cloud Service Settings）] に移動します。

ステップ 2 [クラウドサービス設定（Cloud Services Settings）] の下に、登録トークンを入力し、**[登録（Register）]** をクリックします。

（注） CLI を使用して電子メールゲートウェイを Cisco Cloud Services ポータルに登録するには、`cloudserviceconfig` サブコマンドを使用します。

次のタスク

登録が成功したかどうかの確認 （6 ページ）

登録が成功したかどうかの確認

- Security Services Exchange で、Security Services Exchange のステータスを確認して、正常に登録されたことを確認します。
- Cisco SecureX で、[デバイス（Devices）] ページに移動し、Security Services Exchange に登録されている ESA を表示します。

（注） 別の Cisco SecureX Threat Response サーバ（欧州用の「api.eu.sse.itd.cisco.com」など）に切り替える場合は、最初に Cisco SecureX Threat Response から電子メールゲートウェイの登録を解除して、電子メールゲートウェイと Cisco SecureX Threat Response の統合方法 （2 ページ）のステップを実行する必要があります。

電子メールゲートウェイを Cisco SecureX Threat Response と統合した後は、Cisco Secure Manager Email and Web Gateway を Cisco SecureX Threat Response と統合する必要はありません。

Security Services Exchange に電子メールゲートウェイが正常に登録されたら、Cisco SecureX に ESA 電子メールモジュールを追加します。詳細については、https://securex.us.security.cisco.com/settings/modules/availableに移動して、Cisco SecureX と統合するモジュールを選択し、[新しいモジュールの追加（Add New Module）] をクリックしてページに記載されている手順を参照してください。

電子メールゲートウェイでの Cisco SecureX Threat Response の有効化

手順

ステップ 1 電子メールゲートウェイにログインします。
ステップ 2 [ネットワーク（Networks）]>[クラウドサービス設定（Cloud Service Settings）] を選択します。
ステップ 3 SecureX の下の **[有効（Enable）]** チェックボックスをオンにします。
ステップ 4 変更を送信し、保存します。

Cisco SecureX Ribbon を使用した攻撃分析の実行

（注） Cisco Secure Email Gateway 13.5.1 以前のバージョンからアップグレードする場合、**[ケースブック（Casebook）]** は Cisco SecureX Ribbon の一部となります。

Cisco SecureX は、可視性の統合、自動化の実現、インシデント対応ワークフローの迅速化、脅威ハンティングの改善を行う一連の分散型機能をサポートします。Cisco SecureX の分散機能は、SecureX リボンでアプリケーションおよびツールの形式で利用できます。

この章で説明する内容は、次のとおりです。

- Cisco SecureX Ribbon へのアクセス （8 ページ）
- Cisco SecureX Ribbon およびピボットメニューを使用した攻撃分析のためのケースブックへの観察対象の追加 （9 ページ）

Cisco SecureX Ribbon はページの下部ペインにあり、ダッシュボードと環境内の他のセキュリティ製品間を移動しても保持されます。Cisco SecureX Ribbon は、次のアイコンと要素で構成されています。

- [リボンの展開/縮小（Expand/Collapse Ribbon）]
- Home
- ケースブックアプリ
- Incidents アプリ
- Orbital アプリ
- [エンリッチメント（Enrichment）] 検索ボックス
- 観測対象の検索
- 設定

Cisco SecureX Ribbon の詳細については、https://securex.us.security.cisco.com/help/ribbon を参照してください。

Cisco SecureX Ribbon へのアクセス

始める前に

前提条件 （4 ページ）に記載されているすべての前提条件を満たしていることを確認してください。

（注） Cisco Secure Email Gateway 13.5.1 以前のバージョンで [ケースブック（Casebook）] を設定していたものとします。次の手順で説明するように、追加のスコープを持つ Cisco SecureX API クライアントで新しい [クライアントID（Client ID）] と [クライアントのシークレット（Client Secret）] を作成する必要があります。

 ボタンを使用して、ページの下部ペインにある Cisco SecureX リボンを右からドラッグできます。

手順

ステップ 1 電子メールゲートウェイの新しいWebインターフェイスにログインします。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）へのアクセスを参照してください。

ステップ 2 [Cisco SecureX Ribbon] をクリックします。

ステップ 3 **SecureX API クライアント**で [クライアントID（Client ID）] と [クライアントのシークレット（Client Secret）] を作成します。API クライアントのクレデンシャルを生成する方法の詳細については、「Creating an API Client」を参照してください。

クライアント ID とクライアントパスワードの作成時には、次の範囲を選択してください。

- casebook
- enrich:read
- global-intel:read
- inspect:read
- integration:read
- profile
- private-intel
- response

- registry/user/ribbon
- telemetry:write
- users:read
- orbital (アクセス権がある場合)

ステップ 4 電子メールゲートウェイの **[SecureXリボンを使用するにはログインしてください（Login to use SecureX Ribbon）]** ダイアログボックスのステップ 3 で取得したクライアント ID とクライアントパスワードを入力します。

ステップ 5 [SecureXリボンを使用するにはログインしてください（Login to use SecureX Ribbon）] ダイアログボックスで必要な Cisco SecureX サーバを選択します。

ステップ 6 [認証（Authenticate）] をクリックします。

（注） クライアント ID、クライアントパスワード、および Cisco SecureX サーバを編集する場合は、Cisco SecureX リボンを右クリックして詳細を追加します。

次のタスク

Cisco SecureX Ribbon およびピボットメニューを使用した攻撃分析のためのケースブックへの観察対象の追加 （9 ページ）

Cisco SecureX Ribbon およびピボットメニューを使用した攻撃分析のためのケースブックへの観察対象の追加

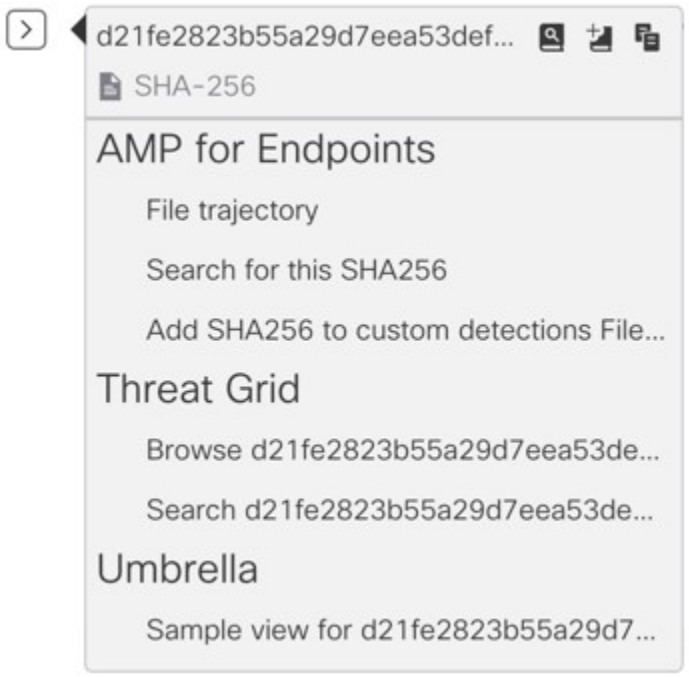
始める前に

電子メールゲートウェイの Cisco SecureX Ribbon とピボット メニュー ウィジェットにアクセスするには、クライアント ID とクライアントパスワードを取得します。詳細については、Cisco SecureX Ribbon へのアクセス （8 ページ）を参照してください。

手順

ステップ 1 電子メールゲートウェイの新しい Web インターフェイスにログインします。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）へのアクセスを参照してください。

ステップ 2 [メールレポート（Email Reporting）] ページへ移動して、該当する観測対象（bit.ly など）の横にあるピボットメニュー ボタンをクリックします。



次の手順を実行します。

- アクティブなケースに観測対象を追加するには、 ボタンをクリックします。
- 新しいケースに観測対象を追加するには、 ボタンをクリックします。

（注） ピボット メニュー ボタンを使用して、ポータルに登録された他のデバイスの観測対象（AMP for Endpoints など）をピボットし、攻撃分析の調査を実行します。

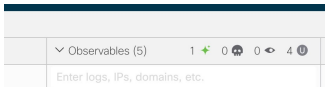
ステップ 3 アイコンにカーソルを合わせ、ボタンをクリックして**ケースブック**を開きます。観測対象が新しいまたは既存のケースに追加されたかどうかを確認します。

ステップ 4 （オプション） ボタンをクリックして、タイトル、説明、またはメモを**ケースブック**に追加します。

（注） 脅威分析の観測対象を検索するには、次の 2 つの方法があります。

- Cisco SecureX の[エンリッチメント（Enrichment）] 検索ボックスをクリックし、観測対象を検索します。

- Cisco SecureX Ribbon 内の [ケースブック（Casebook）] アイコンをクリックし、



フィールドで観測対象を検索します。

Cisco SecureX Ribbon の詳細については、https://securex.us.security.cisco.com/help/ribbon を参照してください。

Cisco SecureX Threat Response 内のメッセージに対する修復アクションの実行

Cisco SecureX Threat Response では、電子メールゲートウェイで処理されたメッセージに対して次の修復アクションを調査して適用できるようになりました。

- 削除（Delete）
- 転送（Forward）
- 転送と削除（Forward and Delete）

始める前に

Cisco SecureX Threat Response のメッセージに対して修復アクションを実行する前に、次の前提条件を満たしていることを確認します。

- Cisco SecureX サーバで電子メールゲートウェイを有効にし、登録した。詳細については、電子メールゲートウェイと Cisco SecureX Threat Response の統合方法 （2 ページ）を参照してください。
- 電子メール ゲートウェイ モジュールを Cisco SecureX に追加し、Cisco SecureX で修復転送アドレスを指定した。詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動して、Cisco SecureX と統合するために必要な Cisco Secure Email Gateway モジュールを選択し、[新しいモジュールの追加（Add New Module）] をクリックして、そのページに記載されている手順を参照してください。
- 電子メールゲートウェイの [システム管理（System Administration）] > [アカウント設定（Account Settings）] ページで修復プロファイルを有効にして設定します。詳細については、メールボックスでのメッセージの修復を参照してください。

手順

ステップ 1 クレデンシャルを使用して Cisco SecureX にログインします。

ステップ 2 [調査（Investigate）] パネルで必要な IOC（URL、電子メールメッセージ ID など）を入力して脅威分析の調査を実行し、**[調査（Investigate）]** をクリックします。詳細については、

https://visibility.amp.cisco.com/help/investigate で「ヘルプ」セクションの「調査」のトピックを参照してください。

ステップ 3 対応する **[シスコメッセージID（Cisco Message ID）]** または **[電子メールメッセージID（Email MessageID）]** を使用して、調査結果に基づいて必要なメッセージを選択します。詳細については、https://visibility.amp.cisco.com/help/investigate で「ヘルプ」セクションの「調査」のトピックを参照してください。

ステップ 4 [シスコメッセージID（Cisco Message ID）] または [電子メールメッセージID（Email MessageID）] の横にあるピボットメニュー ボタンをクリックし、必要な修復アクション（[転送（Forward）] など）を選択します。詳細については、https://visibility.amp.cisco.com/help/investigate で「ヘルプ」セクションの「調査」のトピックを参照してください

Cisco Success Network を使用した電子メールゲートウェイのユーザエクスペリエンスの向上

概要

Cisco Success Network（CSN）機能を使用して、電子メールゲートウェイや機能の使用状況の詳細をシスコに送信できます。これらの詳細情報は、電子メールゲートウェイのバージョンと、電子メールゲートウェイでアクティブになっているが有効になっていない機能を識別するために使用されます。

電子メールゲートウェイや機能の使用状況の詳細をシスコに送信する機能により、組織は次のことを行うことができます。

- 収集されたテレメトリデータの分析を実行し、デジタルキャンペーンを使用してユーザに推奨事項を提示することによって、ユーザネットワークでの製品の有効性を向上させます。
- 電子メールゲートウェイの使用により、ユーザエクスペリエンスが向上します。

次の表に、シスコに送信される電子メールゲートウェイと機能の使用状況の詳細情報のサンプルデータを示します。

統計情報（Statistics）	**サンプルデータ**
電子メールゲートウェイの詳細	
UID	4215XXXXXXXXXXXXXXX-XXXXXXXXXXX
モデル	C100V
sIVAN	電子メールゲートウェイ（スマートライセンスの場合）または null（クラシックライセンスの場合）

統計情報（Statistics）	サンプルデータ
配置	クラスタ/スタンドアロン
userAccountID	SLPIID（スマートライセンスの場合）または VLNID（クラシックライセンスの場合）を入力します。
バージョン（Version）	1X.X.X-XXX
インストール日	1582535814000（エポックからミリ秒単位）
機能情報	
名前	電子メールゲートウェイ機能
イネーブル	Yes
ステータス	コンプライアンス
有効期限日	1831591683（エポックからの秒数）
機能 ID	a4deXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

関連項目

- 電子メールゲートウェイでの CSN での有効化 （13 ページ）
- 電子メールゲートウェイでの CSN の無効化 （14 ページ）

電子メールゲートウェイでの CSN での有効化

始める前に

電子メールゲートウェイが Cisco Cloud Service ポータルに登録され、有効になっていることを確認します。詳細については、電子メールゲートウェイと Cisco SecureX Threat Response の統合方法 （2 ページ）を参照してください。

手順

ステップ 1 [セキュリティサービス（Security Services）]>[クラウドサービス設定（Cloud Service Settings）] に移動します。

ステップ 2 [グローバル設定の編集（Edit Global Settings）] をクリックします。

ステップ 3 をオンにします。[Cisco Success Network] の下にある [有効化（Enable）] チェックボックス。

ステップ 4 変更を送信し、保存します。

電子メールゲートウェイでの CSN の無効化

手順

ステップ 1 [セキュリティサービス（Security Services）]>[クラウドサービス設定（Cloud Service Settings）] に移動します。

ステップ 2 [グローバル設定の編集（Edit Global Settings）] をクリックします。

ステップ 3 [Cisco Success Network] の下にある [有効化（Enable）] チェックボックスをオフにします。

ステップ 4 変更を送信し、保存します。