電子メールゲートウェイと Cisco Advanced Phishing Protection の統合

この章は、次の項で構成されています。

Cisco Advanced Phishing Protection の概要

Cisco Advanced Phishing Protection は、ビジネスメール詐欺（BEC）とフィッシングの検出機能を提供します。高度な機械学習技術および追加されたインテリジェンスを駆使して、送信者アドレスのレピュテーションをチェックし、アイデンティティ詐欺による脅威を検出します。このインテリジェンスは継続的な適応機能を備え、送信者をリアルタイムで把握して、保護を強化します。

電子メールゲートウェイの高度なフィッシング防御エンジンは、組織に送信された過去の電子メールトラフィックに基づいて、すべての正当な送信者固有の動作を確認します。Cisco Advanced Phishing Protection のクラウドサービスインターフェイスは、悪意のある可能性があるメッセージを正常なメッセージと区別するためにリスク分析を実行します。

Cisco Advanced Phishing Protection クラウドサービスは、電子メールゲートウェイを組織への着信メッセージのメタデータのコピーを受信するためのセンサーエンジンとして使用します。このセンサーエンジンが、電子メールゲートウェイから送られるメッセージヘッダーなどのメタデータを収集し、それらを分析するために Cisco Advanced Phishing Protection クラウドサービスに中継します。分析後に、悪意のある可能性があるメッセージは、Advanced Phishing Protection

クラウドサービスで事前に設定したポリシーに基づいて、受信者のメールボックスから自動的に修復されます。

電子メールゲートウェイをセンサーエンジンとして使用できると、組織が次のことを行うときに役立ちます。

- 受信者のメールボックスのメッセージヘッダーで検出された脅威を特定、調査、および修復する。
- 組織内の複数の電子メールゲートウェイからメッセージのメタデータのレポートデータを表示する。

Cisco Advanced Phishing Protection の利点

電子メールゲートウェイに Cisco Advanced Phishing Protection を展開すると、次のような利点があります。

- センサーベースのソリューションを迅速に展開することで、ユーザを侵害による損害から完全に保護できます。
- 電子メール環境をより効果的に保護するための追加の防御層を提供します。
- BEC 攻撃を防御するため、送信者をリアルタイムで把握し、電子メールのアイデンティティと動作関係を学習して認証します。
- 受信者の受信トレイから悪意のある電子メールを自動的に削除し、アイデンティティ偽装の手法に関する注意を呼びかけ、アイデンティティ詐称やその他の高度な攻撃を防御します。
- 保護されたメッセージや防御された攻撃の総数など、電子メール攻撃のアクティビティを詳細に可視化します。
- 次の攻撃を防御します。
  - 侵害されたアカウントやソーシャルエンジニアリングを使用した攻撃。
  - フィッシング、ランサムウェア、ゼロデイ攻撃、スプーフィング。
  - 悪意のあるペイロードや URL がない BEC。

ワークフロー

1. Cisco Advanced Phishing Protection クラウドサービスにアクセスするためのライセンスをアクティブ化します。
2. 電子メールゲートウェイを Cisco Advanced Phishing Protection クラウドサービスのセンサーエンジンとして設定します。これにより、クラウドまたはオンプレミス経由で電子メールゲートウェイが軽量センサーとして展開されます。

3. 電子メールゲートウェイのセンサーエンジンを Cisco Advanced Phishing Protection クラウドサービスに登録します。
4. 電子メールゲートウェイのセンサーエンジンは、正常と見なされたメッセージのメタデータを Cisco Advanced Phishing Protection クラウドサービスに転送します。
5. Cisco Advanced Phishing Protection クラウドサービスは、メッセージのメタデータが悪意のあるものかどうかを判断します。
6. Cisco Advanced Phishing Protection クラウドサービスで事前設定されたポリシーが「適用」センサーで設定されている場合、さらに詳細なインシデント調査のために、メッセージがブロックまたはリダイレクトされます。

電子メールゲートウェイと Cisco Advanced Phishing Protection クラウドサービスの統合方法

次の手順を順番に実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	前提条件を確認します。	前提条件 （4 ページ）
ステップ 2	Cisco Advanced Phishing Protection クラウドサービスからプロビジョニングキーを取得します。	Cisco Advanced Phishing Protection クラウドサービスからのプロビジョニングキーの取得 （4 ページ）
ステップ 3	電子メールゲートウェイをセンサーエンジンとして Cisco Advanced Phishing Protection クラウドサービスに登録します。	電子メールゲートウェイでの Cisco Advanced Phishing Protection センサーの登録 （5 ページ）
ステップ 4	電子メールゲートウェイで Advanced Phishing Protection を有効にします。	電子メールゲートウェイでの Advanced Phishing Protection の有効化 （6 ページ）
ステップ 5	Cisco Advanced Phishing Protection クラウドサービスから API アクセスキーを取得します。	Cisco Advanced Phishing Protection クラウドサービスからの API アクセスキーの取得 （7 ページ）
ステップ 6	メッセージメタデータの転送を有効にするための受信メールポリシーを設定します。	メッセージメタデータの転送を有効にするための受信メールポリシーの設定 （8 ページ）

	コマンドまたはアクション	目的
ステップ 7	Advanced Phishing Protection クラウドサービスに転送されたメッセージのメタデータをモニタします。	Cisco Advanced Phishing Protection クラウドサービスでのメッセージメタデータのモニタリング （10 ページ）

前提条件

- Cisco Advanced Phishing Protection クラウドサービスのアカウントの利用 （4 ページ）
- Cisco Advanced Phishing Protection クラウドサービスのセンサーのインストール （4 ページ）

Cisco Advanced Phishing Protection クラウドサービスのアカウントの利用

次の内容について確認してください。

- URL https://www.cisco.com/c/en/us/buy.html から Cisco Advanced Phishing Protection クラウドサービスを利用するためのライセンスを取得していること。
- Cisco Advanced Phishing Protection クラウドサービスでプロビジョニングを行うため、電子メール通知で受信したアクティベーションリンクを使用して、アカウントがアクティブ化されていること。

Cisco Advanced Phishing Protection クラウドサービスのセンサーのインストール

組織の要件に従って、センサーエンジンとして電子メールゲートウェイを設定していることを確認します。詳細については、『*Cisco Advanced Phishing Protection* ユーザーガイド』を参照してください。

Cisco Advanced Phishing Protection クラウドサービスからのプロビジョニングキーの取得

始める前に

管理者権限を使用して、Cisco Advanced Phishing Protection クラウドサービスにアクセスできることを確認します。詳細については、前提条件 （4 ページ）を参照してください。Cisco Advanced Phishing Protection クラウドサービスにアクセスできない場合は、Cisco TAC にお問い合わせください。

手順

ステップ 1 Cisco Advanced Phishing Protection クラウドサービスにログインします。

ステップ 2 [管理（Manage）] > [センサー（Sensors）] を選択します。

ステップ 3 [インストール（Installation）] > [センサーインストーラのダウンロード（Download Sensor Installer）] を選択します。

ステップ 4 ドロップダウンから、組織の要件に従って設定したセンサーのインストールスクリプトを選択します（例：Cisco SEG）。

詳細については、Cisco Advanced Phishing Protection クラウドサービスのセンサーのインストール （4 ページ）を参照してください。

ステップ 5 6 文字のプロビジョニングキーをコピーします。

このプロビジョニングキーを使用して、Cisco E メール セキュリティ ゲートウェイをセンサーとして設定します。

（注） 電子メールゲートウェイをセンサーとして登録するには、プロビジョニングキーを生成から 7 日以内に使用する必要があります。

次のタスク

電子メールゲートウェイを Cisco Advanced Phishing Protection クラウドサービスに登録します。詳細については、電子メールゲートウェイでの Cisco Advanced Phishing Protection センサーの登録 （5 ページ）を参照してください。

電子メールゲートウェイでの Cisco Advanced Phishing Protection センサーの登録

始める前に

次の内容について確認してください。

- 電子メールゲートウェイを Advanced Phishing Protection クラウドサービスに登録するための有効なプロビジョニングキーがあること。詳細については、Cisco Advanced Phishing Protection クラウドサービスからのプロビジョニングキーの取得 （4 ページ）を参照してください。
- Cisco Advanced Phishing Protection クラウドサービスで電子メールゲートウェイを登録するために必要なファイアウォールの HTTPS（In および Out）443 ポートが、FQDN に対して開放されていること。

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 [セキュリティサービス（Security Services）] > [高度なフィッシング防御（Advanced Phishing Protection）] に移動します。

ステップ 3 [Register] をクリックします。

ステップ 4 [URL] ドロップダウンから、Cisco Advanced Phishing Protection クラウドサービスのリージョンを選択します。

ステップ 5 Advanced Phishing Protection クラウドサービスから取得した 6 文字のプロビジョニングキーを入力します。

ステップ 6 [登録（Register）] をクリックして変更を送信します。

電子メールゲートウェイをセンサーに登録すると、Cisco Advanced Phishing Protection クラウドサービスで、汎用一意 ID（UUID）が生成されます。

（注） 登録に成功すると、Cisco Advanced Phishing Protection クラウドサービスでは、電子メールゲートウェイのクラウドサービスでのホスト名が識別されます。

次のタスク

電子メールゲートウェイで Cisco Advanced Phishing Protection エンジンを有効にします。詳細については、電子メールゲートウェイでの Advanced Phishing Protection の有効化 （6 ページ）を参照してください。

電子メールゲートウェイでの Advanced Phishing Protection の有効化

始める前に

Cisco Advanced Phishing Protection クラウドサービスで電子メールゲートウェイがセンサーとして登録され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での Cisco Advanced Phishing Protection センサーの登録 （5 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にログインします。

ステップ 2 [セキュリティサービス（Security Services）] > [高度なフィッシング防御（Advanced Phishing Protection）] に移動します。

ステップ 3 **[有効（Enable）]** をクリックします。

ステップ 4 変更を保存します。

次のタスク

Cisco Advanced Phishing Protection クラウドサービスへのメッセージメタデータの転送を有効にします。詳細については、メッセージメタデータの転送を有効にするための受信メールポリシーの設定 （8 ページ）を参照してください。

Cisco Advanced Phishing Protection クラウドサービスからの API アクセスキーの取得

API アクセスキーを使用して、E メールゲートウェイで次のタスクを実行できます。

- APP ライセンスの有効期限の詳細に関する電子メール通知アラートをユーザに送信します。
- 組織レベルですべての電子メールゲートウェイから Cisco Advanced Phishing Protection クラウドサービスに送信されたメッセージの合計数をダッシュボードウィジェットに表示します。ダッシュボードウィジェットは、新しい Web インターフェイスの [高度なフィッシング防御（Advanced Phishing Protection）] レポートページで使用できます。

始める前に

次の内容について確認してください。

- 電子メールゲートウェイが Cisco Advanced Phishing Protection クラウドサービスのセンサーとして登録されていること。詳細については、電子メールゲートウェイでの Cisco Advanced Phishing Protection センサーの登録 （5 ページ）を参照してください。
- 電子メールゲートウェイで Advanced Phishing Protection が有効になっていること。詳細については、電子メールゲートウェイでの Advanced Phishing Protection の有効化 （6 ページ）を参照してください。

手順

ステップ 1 Cisco Advanced Phishing Protection クラウドサービスにログインします。

ステップ 2 [管理（Manage）] > [ユーザ（Users）] を選択します。

ステップ 3 該当するユーザ名をクリックします。

ステップ 4 [APIシークレットの生成（Generate API Secret）] リンクをクリックして、API アクセスキーを生成します。

ステップ 5 **API アクセス UID** と **API アクセス秘密鍵**をシステムにローカルコピーします。

（注） API アクセスキーをコピーせずに Cisco Advanced Phishing Protection クラウドサービスを閉じる場合は、手順の **1～3** に従い、[APIシークレットの再生成（Regenerate API Secret）] リンクをクリックして新しい API アクセスキーを取得します。

ステップ 6 電子メールゲートウェイのレガシー Web インターフェイスにログインします。

ステップ 7 [セキュリティサービス（Security Services）] > [高度なフィッシング防御（Advanced Phishing Protection）] に移動します。

ステップ 8 [高度なフィッシング防御APIアクセス（Advanced Phishing Protection API Access）] セクションで [設定の編集（Edit Settings）] をクリックします。

ステップ 9 [APIアクセスUID（API Access UID）] フィールドに **API アクセス UID** キーを入力します。

ステップ 10 [APIアクセスキー（API Access key）] フィールドに **API アクセス秘密**鍵を入力します。

ステップ 11 [送信（Submit）] をクリックします。

次のタスク

Cisco Advanced Phishing Protection クラウドサービスへのメッセージメタデータの転送を有効にします。詳細については、メッセージメタデータの転送を有効にするための受信メールポリシーの設定 （8 ページ）を参照してください。

メッセージメタデータの転送を有効にするための受信メールポリシーの設定

メッセージのメタデータが Cisco Advanced Phishing Protection クラウドサービスに転送されるようにメールポリシーを設定できます。

電子メールゲートウェイで Cisco Advanced Phishing Protection クラウドサービスを有効にすると、次のメッセージヘッダーが Cisco Advanced Phishing Protection クラウドサービスと共有されます。

- Authentication-Results
- Authentication-Results-original
- DMARC-result
- DKIM-domain
- DKIM-result
- DKIM-selector
- DKIM-signatures
- From-header
- Full-Header-From
- HELO_domain
- Last-Hop-IP-Address
- List-ID
- Mail-From
- Mailing-list
- Message-ID
- Rcpt-To
- Received-Header
- Received-SPF

- Received-Timestamps
- Reply-To
- SPF-result
- Subject-header
- To-header
- Originator-Return-Address
- X-Mailer
- X-Original-Authentication-Results
- X-Original-From
- X-Original-To
- X-Original-Sender
- X-Originating-IP
- X-OriginatorOrg
- X-Received

始める前に

次の内容について確認してください。

- 電子メールゲートウェイが Cisco Advanced Phishing Protection クラウドサービスのセンサーとして登録されていること。詳細については、電子メールゲートウェイでの Cisco Advanced Phishing Protection センサーの登録 （5 ページ）を参照してください。
- 電子メールゲートウェイで Advanced Phishing Protection が有効になっていること。詳細については、電子メールゲートウェイでの Advanced Phishing Protection の有効化 （6 ページ）を参照してください。

手順

ステップ 1 E メール セキュリティ ゲートウェイにログインします。

ステップ 2 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] に移動します。

ステップ 3 APP フィルタの下にあるリンクをクリックします。

ステップ 4 ドロップダウンリストから [Advanced Phishing Protectionの有効化（設定のカスタマイズ）（Enable Advanced Phishing Protection (Customize Settings)）] を選択します。

ステップ 5 [転送の有効化（Enable Forwarding）] チェックボックスをオンにします。

ステップ 6 [送信（Submit）] をクリックし、変更をコミットします。

Cisco Advanced Phishing Protection クラウドサービスでのメッセージメタデータのモニタリング

E メール セキュリティ ゲートウェイから Cisco Advanced Phishing Protection クラウドサービスに転送されたメッセージのメタデータをモニタできます。クラウドサービスの[分析（Analyze）] > [メッセージ（Messages）] ページには、メッセージの送信元、およびメッセージと送信者に関連するリスク情報が表示されます。

Cisco Advanced Phishing Protection クラウドサービスのメッセージメタデータは、以下に基づいてレピュテーションスコアが付けられます。

- メッセージの信頼性
- ドメインのレピュテーション
- 送信者の正当性

Advanced Phishing Protection およびクラスタ

中央管理を使用する場合、クラスタ、グループ、およびマシンの各レベルで Advanced Phishing Protection を有効にできます。Cisco Advanced Phishing Protection クラウドサービスに電子メールゲートウェイをスタンドアロンモードで登録している場合は、Cisco Advanced Phishing Protection クラウドサービスに登録されているクラスタへの参加を選択できます。

（注） マシンレベルで Advanced Phishing Protection を無効にすると、グループレベルとクラスタレベルでも無効になります。

[高度なフィッシング防御レポート（Advanced Phishing Protection Reports）] ページ

[モニタ（Monitor）] > [高度なフィッシング防御（Advanced Phishing Protection] レポートページには、次の情報が表示されます。

- Cisco Advanced Phishing Protection クラウドサービスに正常に転送されたメッセージの合計数。
- Cisco Advanced Phishing Protection クラウドサービスに転送されなかったメッセージの合計数。

(注) メッセージメタデータの転送に失敗した場合は、高度なフィッシング防御機能の設定を検証する必要があります。詳細については、電子メールゲートウェイと Cisco Advanced Phishing Protection クラウドサービスの統合方法 （3 ページ）を参照してください。

[高度なフィッシングからの保護（Advanced Phishing Protection）] レポートページを使用すると、次の情報を確認できます。

- Cisco Advanced Phishing Protection クラウドサービスへの転送を試行したメッセージの総数（グラフィック形式）
- Cisco Advanced Phishing Protection クラウドサービスへ転送されたメッセージの概要（グラフィック形式）

Cisco Advanced Phishing Protection クラウドサービスに転送されるメッセージのメタデータの詳細情報を表示するには、リンクをクリックして Cisco Advanced Phishing Protection クラウドサービスにログインします。詳細については、Cisco Advanced Phishing Protection クラウドサービスでのメッセージメタデータのモニタリング （10 ページ）を参照してください。

Cisco Advanced Phishing Protection クラウドサービスでのメッセージメタデータのモニタリング

E メール セキュリティ ゲートウェイから Cisco Advanced Phishing Protection クラウドサービスに転送されたメッセージのメタデータをモニタできます。クラウドサービスの[分析（Analyze）] > [メッセージ（Messages）] ページには、メッセージの送信元、およびメッセージと送信者に関連するリスク情報が表示されます。

Cisco Advanced Phishing Protection クラウドサービスのメッセージメタデータは、以下に基づいてレピュテーションスコアが付けられます。

- メッセージの信頼性
- ドメインのレピュテーション
- 送信者の正当性

Cisco Advanced Phishing Protection クラウドサービスに送信されたメッセージの表示

Cisco Advanced Phishing Protection クラウドサービスに転送するメッセージのメタデータを成功と失敗に応じて表示できます。

始める前に

E メール ゲートウェイでメッセージ トラッキング機能が有効にされていることを確認します。メッセージ トラッキングを有効にするには、Web インターフェイスで [セキュリティサービス（Security Services）] > [集中管理サービス（Centralized Services）] > [メッセージトラッキング（Message Tracking）] ページに移動します。

手順

ステップ 1 E メール セキュリティ ゲートウェイにログインします。

ステップ 2 [モニタ（Monitor）] > [メッセージ トラッキング（Message Tracking）] に移動します。

ステップ 3 [詳細設定（Advanced）] をクリックします。

ステップ 4 [メッセージイベント（Message Event）] の [Advanced Phishing Protectionに転送（Advanced Phishing Protection Forwarding）] チェックボックスをオンにします。

ステップ 5 （オプション）Cisco Advanced Phishing Protection クラウドサービスに正常に転送されたメッセージを表示するには、[成功（Successful）] を選択します。

ステップ 6 （オプション）Cisco Advanced Phishing Protection クラウドサービスへの転送に失敗したメッセージを表示するには、[失敗（Failed）] を選択します。

ステップ 7 **[検索（Search）]** をクリックします。