電子メールゲートウェイと Cisco Secure Awareness クラウドサービスの統合

この章は、次の項で構成されています。

概要

Cisco Secure Awareness クラウドサービスを使用すると、フィッシング シミュレーション、意識向上トレーニング、またはその両方を効果的に展開して、結果を測定およびレポートできます。これにより、セキュリティ運用チームは、エンドユーザの状況緩和ではなく、リアルタイムの脅威に集中できます。

Cisco Secure Awareness クラウドサービスは、リピートクリッカー（任意の URL またはメッセージ内の添付ファイルを繰り返しクリックするユーザ）のレポートを提供します。これらのユーザは、Cisco Secure Awareness クラウドサービスによって定義されたフィッシング シミュレーション キャンペーンによって識別されます。

Cisco Secure Awareness クラウドサービスの詳細については、https://secat.cisco.com を参照してください。

電子メールゲートウェイと Cisco Secure Awareness クラウドサービスを統合することで、次のことが可能になります。

- 実際のフィッシング攻撃に対するエンドユーザの認識が向上します。
- 電子メール管理者は、リピートクリッカーと識別されたエンドユーザに対して厳格なポリシーを設定できます。

電子メールゲートウェイと Cisco Secure Awareness 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	操作手順	詳細情報
ステップ 1	（Cisco Secure Awareness で）地域に基づいて、組織の Cisco Security Awareness クラウドサービスアカウントを作成します。	Cisco Secure Awareness クラウドサービスアカウントの作成（3 ページ）
ステップ 2	電子メールゲートウェイが Cisco Secure Awareness クラウドサービスにアクセスできるようにファイアウォールを設定します。	Cisco Secure Awareness クラウドサービスにアクセスするためのファイアウォール設定の構成 （4 ページ）
ステップ 3	電子メールゲートウェイで Cisco Secure Awareness クラウドサービスからのフィッシングメッセージをシミュレートできるように、新しい送信者グループを作成します。	電子メールゲートウェイでシミュレートされたフィッシングメッセージを許可する送信者グループの作成 （5 ページ）
ステップ 4	（Cisco Secure Awareness で）Cisco Secure Awareness クラウドサービスの新しいユーザを作成し、リピートクリッカーを識別します。 ：	次の URL にある 『CSA Administrator Guide』を参照してください。 • https://secat.cisco.com/portal/Support（米国のユーザに適用） • https://secat-eu.cisco.com/portal/Support（欧州連合（EU）のユーザに適用）

手順	操作手順	詳細情報
ステップ 5	（Cisco Secure Awareness で）Cisco Secure Awareness クラウドサービスでシミュレートされたフィッシングメッセージを作成し、組織内のエンドユーザに送信します。このプロセスは、メッセージ内の添付ファイルまたはURL を繰り返しクリックするエンドユーザを追跡するために使用されます。	次の URL にある『CSA Administrator Guide』を参照してください。 • https://secat.cisco.com/portal/Support（米国のユーザに適用） • https://secat-eu.cisco.com/portal/Support（欧州連合（EU）のユーザに適用）
ステップ 6	Cisco Secure Awareness クラウドサービスから認証トークンを取得します。	Cisco Secure Awareness クラウドサービスからの認証トークンの取得 （6 ページ）
ステップ 7	電子メールゲートウェイで Cisco Secure Awareness クラウドサービスを有効にします。	電子メールゲートウェイでの Cisco Secure Awareness クラウドサービスの有効化 （7 ページ）
ステップ 8	カスタム着信メールポリシーを作成して、リピートクリッカーとして分類されるエンドユーザのアグレッシブメールポリシーを設定します。	リピートクリッカーとして分類されたエンドユーザのカスタム着信メールポリシーの作成 （8 ページ）

Cisco Secure Awareness クラウドサービスアカウントの作成

地域に応じて、次のいずれかの URL を使用して、組織の管理者権限を持つ Cisco Secure Awareness クラウドサービスアカウントを作成します。

- https://secat.cisco.com（アメリカ地域のユーザに適用）
- https://secat-eu.cisco.com（欧州連合（EU）のユーザに適用）

次の作業

電子メールゲートウェイが Cisco Secure Awareness クラウドサービスに接続できるようにファイアウォールを設定します。詳細については、「Cisco Secure Awareness クラウドサービスにアクセスするためのファイアウォール設定の構成 （4 ページ）」を参照してください。

Cisco Secure Awareness クラウドサービスにアクセスするためのファイアウォール設定の構成

電子メールゲートウェイを Cisco Secure Awareness クラウドサービスに接続するには、次のホスト名または IP アドレス用にファイアウォール上で HTTPS（Out）443 ポートを開く必要があります（以下の表を参照）。

サービス	アメリカ地域		欧州連合	
	ホスト名（Hostname）	IP アドレス（IP Address）	ホスト名（Hostname）	IP アドレス（IP Address）
Cisco Secure Awareness クラウドサービス	secat.cisco.com	52.242.31.199	secat-eu.cisco.com	40.127.163.97
コース通知（アウトバウンド）	-	167.89.98.161	-	40.127.163.97
ランディングページとフィードバックページ（アウトバウンド）	-	52.242.31.199	-	
電子メール添付ファイル（アウトバウンド）	-		-	

（注） 上記の表に記載されている IP アドレスは変更される場合があります。IP アドレスの最新のリストについては、Cisco Secure Awareness クラウドサービスの「IP Allowlist Guide」https://secat.cisco.com/portal/Support/IpWhitelistingGuide を参照してください

次の作業

電子メールゲートウェイで Cisco Secure Awareness クラウドサービスからのフィッシングメッセージをシミュレートできるように、新しい送信者グループを作成します。詳細については、「電子メールゲートウェイでシミュレートされたフィッシングメッセージを許可する送信者グループの作成 （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シミュレートされたフィッシングメッセージを許可する送信者グループの作成

電子メールゲートウェイで Cisco Secure Awareness クラウドサービスからのフィッシングメッセージをシミュレートできるように、新しい送信者グループを作成する必要があります。

始める前に

電子メールゲートウェイが Cisco Secure Awareness クラウドサービスにアクセスできるようにファイアウォールが設定されていることを確認します。詳細については、Cisco Secure Awareness クラウドサービスにアクセスするためのファイアウォール設定の構成 （4 ページ）を参照してください。

手順

ステップ 1 **[メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）]** の順にクリックします。

ステップ 2 [送信者グループを追加（Add Sender Group）] をクリックします。

ステップ 3 送信者グループの名前を入力します。

ステップ 4 優先順位を **1** に選択します。

ステップ 5 **CYBERSEC_AWARENESS_ALLOWED** としてポリシーを選択します。

ステップ 6 **[SBRSを未使用にする（SBRS to Not in Use）]** チェックボックスをオンにして、IP レピュテーション フィルタリングを無効にします。

ステップ 7 **[送信者を送信して追加（Submit and Add Senders）]** をクリックします。

ステップ 8 次の Cisco Secure Awareness クラウドサービスの IP アドレスのいずれかを追加して、地域に基づく送信元 IP アドレスとして設定します。

- アメリカ地域 - 207.200.3.14 または 173.244.184.143
- 欧州連合（EU）- 77.32.150.153

（注） Cisco Secure Awareness クラウドサービスの IP アドレスは、電子メールゲートウェイがシミュレートされたフィッシングメッセージを実際のフィッシングとして解釈しないようにするために使用されます。

ステップ 9 変更を送信し、保存します。

次のタスク

1. Cisco Secure Awareness クラウドサービスで新しいユーザを作成し、リピートクリッカーを識別します。

2. Cisco Secure Awareness クラウドサービスでシミュレートされたフィッシングメッセージを作成し、組織内のエンドユーザに送信します。

   上記の2つのタスクを完了する方法の詳細については、次のURLにある『CSA Administrator Guide』を参照してください：

   - https://secat.cisco.com/portal/Support（米国のユーザに適用）
   - https://secat-eu.cisco.com/portal/Support（欧州連合（EU）のユーザに適用）

3. Cisco Secure Awareness クラウドサービスから認証トークンを取得し、Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードします。詳細については、「Cisco Secure Awareness クラウドサービスからの認証トークンの取得 （6 ページ）」を参照してください。

Cisco Secure Awareness クラウドサービスからの認証トークンの取得

Cisco Secure Awareness クラウドサービスから認証トークンを取得し、それを使用して Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードする必要があります。

始める前に

管理者権限を持つ Cisco Secure Awareness クラウドサービスのアカウントがあることを確認します。詳細については、Cisco Secure Awareness クラウドサービスアカウントの作成 （3 ページ）を参照してください。Cisco Secure Awareness クラウドサービスにアクセスできない場合は、Cisco サポートにお問い合わせください。

手順

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

ステップ 2 [環境（Environment）] > [設定（Settings）] に移動します

ステップ 3 [レポートAPI（Reports API）] タブをクリックします。

ステップ 4 **[レポートAPIを有効にする（Enable Report API）]** チェックボックスをオンにします。

ステップ 5 認証トークンをコピーします。

この認証トークンを使用して、Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードします。

次のタスク

電子メールゲートウェイで Cisco Secure Awareness クラウドサービスを有効にします。詳細については、「電子メールゲートウェイでの Cisco Secure Awareness クラウドサービスの有効化（7 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 Secure Awareness クラウドサービスの有効化

始める前に

次のように設定されていることを確認します。

- 管理者権限を持つ Cisco Secure Awareness クラウドサービスの有効なアカウント。
- Cisco Secure Awareness クラウドサービスから有効な認証トークンを取得しました。詳細については、Cisco Secure Awareness クラウドサービスからの認証トークンの取得 （6 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）] > [Cisco Secure Awareness]** に移動します。

ステップ 2 [有効（Enable）] をクリックします。

ステップ 3 **[Cisco Security Awarenessの有効化（Enable Cisco Secure Awareness）]** チェックボックスをオンにします。

ステップ 4 必要なサーバを選択して、電子メールゲートウェイを Cisco Secure Awareness クラウドサービスに接続します。

ステップ 5 Cisco Secure Awareness クラウドサービスから取得した認証トークンを入力します。

ステップ 6 （任意）Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードするためのポーリング間隔を入力します。

ステップ 7 変更を送信し、保存します。

次のタスク

- Cisco Secure Awareness クラウドサービスを有効にすると、電子メールゲートウェイは Cisco Secure Awareness クラウドサービスからリピートクリッカーリストを自動的にダウンロードします。電子メールゲートウェイの Web インターフェイスで **[セキュリティサービス（Security Services）] > [Cisco Secure Awareness] > [リピートクリッカーリストの設定（Repeat Clickers List Settings）]** セクションに移動すると、リピートクリッカーリストのリピートクリッカーユーザの数を表示できます。リピートクリッカーリストの詳細については、Cisco Secure Awareness クラウドサービスにログインし、[分析（Analytics）] > [標準

レポート（Standard Reports）] > [フィッシングシミュレーション（Phishing Simulations）] > [リピートクリッカー（Repeat Clickers）] セクションに移動します。

- カスタム着信メールポリシーを作成して、リピートクリッカーとして分類されるエンドユーザのアグレッシブメールポリシーを設定します。詳細については、「リピートクリッカーとして分類されたエンドユーザのカスタム着信メールポリシーの作成（8ページ）」を参照してください。

リピートクリッカーとして分類されたエンドユーザのカスタム着信メールポリシーの作成

リピートクリッカーとして分類されるエンドユーザのアグレッシブメールポリシーを設定するには、カスタム着信メールポリシーを作成する必要があります。

手順

ステップ 1 [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 2 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 3 ポリシーの名前を入力します。

ステップ 4 **[ユーザの追加（Add User）]** をオンにします。

ステップ 5 **[次の受信者（Following Recipients）]** を選択します。

ステップ 6 **[リピートクリッカーリストを含める（Include Repeat Clicker List）]** チェックボックスをオンにして、Cisco Secure Awareness クラウドサービスによってリピートクリッカーとして分類された受信者のリストを含めます。

ステップ 7 [OK] をクリックします。

ステップ 8 **[送信（Submit）]** をクリックします。

ステップ 9 メールポリシーに必要なサービスエンジン（アンチウイルス、グレイメールなど）を設定します。

ステップ 10 変更を保存します。

Cisco Secure Awareness クラウドサービスとクラスタ

一元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、Cisco Secure Awareness クラウドサービスを有効化できます。スタンドアロンモードで Cisco Secure Awareness クラウドサービスを使用して電子メールゲートウェイを有効にしている場合は、Cisco Secure Awareness クラウドサービスに登録されているクラスタに参加することを選択できます。

（注） マシンレベルで Cisco Secure Awareness クラウドサービスを無効にすると、ログインした電子メールゲートウェイに対してのみ無効になり、クラスタ内の他のマシンはまだ Cisco Secure Awareness クラウドサービスに接続されています。

ログの表示

Cisco Secure Awareness クラウドサービスの情報はメールログに記録されます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

Cisco Secure Awareness ログエントリの例：

- この例では、無効なトークンが原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Tue Oct 13 10:12:59 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
of an invalid token.
```

解決策：Cisco Secure Awareness クラウドサービスから有効な認証トークンを取得してください。

- この例では、接続エラーが原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
of a connection error.
```

解決策：電子メールゲートウェイを Cisco Secure Awareness クラウドサービスに接続するために使用するファイアウォール設定を確認します。

- この例では、内部サーバエラーが原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
of an internal server error.
```

解決策：詳細については、シスコ テクニカル サポートにお問い合わせください。

- この例では、SSL 証明書の検証の失敗が原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 11:02:46 2020 Warning: CSA:
 The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
the SSL certificate verification failed.
```

解決策：必要なプロキシサーバの CA 証明書を電子メールゲートウェイのカスタム認証局リストに追加します。

- この例では、プロキシ認証の失敗が原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 11:09:48 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed
because the proxy authentication failed.
```

解決策：電子メールゲートウェイでプロキシサーバが正しい認証ログイン情報を使用して設定されているかどうかを確認します。

- この例では、Cisco Secure Awareness クラウドサービスでレポート API が有効になっていなかったことが原因で、Cisco Secure Awareness クラウドサービスへの要求が失敗したことがログに示されています。

```
Mon Aug 17 15:35:42 2020 Warning: CSA:
The download of the Repeat Clickers list failed.
A request to the CSA cloud service failed because
the Report API was not enabled on the CSA cloud service
```

解決策：Cisco Secure Awareness クラウドサービスの [環境（Environment）] > [設定（Settings）] > [レポートAPI（Report API）] タブで [レポートAPIを有効にする（Enable Report API）] チェックボックスをオンにします。

- この例では、Cisco Secure Awareness 機能が特定の日付で期限切れになることがログに示されています。

```
2020-10-15 08:00:11,968 INFO csa The Cisco Secure
Awareness feature expires on 2029-12-28T23:59:59Z. You need to
contact your Cisco Account Manager to renew the license.
```

解決策：シスコアカウントマネージャに連絡して、ライセンスを更新します。

- この例では、Cisco Secure Awareness 機能のライセンスの有効期限が切れており、電子メールゲートウェイでこの機能が無効になっていることがログに示されています。

```
2020-10-27 13:33:21,714 CRITICAL csa The Cisco Secure
Awareness feature license has expired, and the feature is
disabled on your email gateway. Contact your Cisco Account Manager
to renew the license.
```

解決策：シスコアカウントマネージャに連絡して、ライセンスを更新します。

- この例では、ダウンロードされたリピートクリッカーリストが空であることがログに示されています。

```
Tue Oct 13 10:10:18 2020 Info: CSA: The downloaded
Repeat Clickers list is empty.
```

解決策：Cisco Secure Awareness クラウドサービスでシミュレートされたフィッシングメッセージを作成し、組織内の受信者に送信します。

- この例では、ダウンロード試行の最大数に達したため、Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Fri Oct 16 05:22:08 2020 Warning: CSA: The download
of the Repeat Clickers list from the Cisco Secure Awareness
cloud service failed because you have reached the maximum
number of attempts.
```

解決策：Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードする試行回数を増やすには、シスコサポートに連絡してください。

アラートの表示

以下の表では、Cisco Secure Awareness クラウドサービスに対して生成されるアラート、アラートの説明、アラートの重大度を記載します。

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.CSA.DOWNLOAD_FAILURE	アラートテキスト：Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードに失敗しました。$reason。 アラートレベル：警告（WARNING）。 説明：Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードに失敗するとアラートが送信されます。	パラメータ：reason 理由：Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードできなかった理由。 例：「無効なトークン」、「最大試行回数に達しました」など。
MAIL.CSA.EMPTY_EMAIL_LIST	アラートテキスト：ダウンロードされたリピートクリッカーリストは空です。 アラートレベル：情報（INFO）。 説明：ダウンロードされたリピートクリッカーリストが空の場合にアラートが送信されます。このアラートは、Cisco Secure Awareness クラウドサービスにリピートクリッカーがリストされていないことを示します。	該当なし。

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.CSA.LICENSE_ EXPIRING	アラートテキスト：Cisco Secure Awareness 機能のライセンスは $expiry で期限切れになります。シスコアカウントマネージャに連絡して、ライセンスを更新する必要があります。 リージョン：$region サーバ：$server アラートレベル：情報（INFO） 説明：有効期限の 7 日前、有効期限の 3 日前、および有効期限の 1 日前にアラートが送信されます。	パラメータ：expiry、region、server expiry：Cisco Secure Awareness ライセンスの有効期限が切れる日付。 region：期限が切れる Cisco Secure Awareness ライセンスのリージョン。リージョンは、AMERICAS、EUROPE などです。 server：サーバ URL の名前（例：https://secat.cisco.com）
MAIL.CSA.LICENSE_ EXPIRED	アラートテキスト：Cisco Secure Awareness 機能ライセンスの有効期限が切れており、この機能は電子メールゲートウェイで無効になっています。シスコアカウントマネージャに連絡して、ライセンスを更新してください。 リージョン：$region サーバ：$server アラートレベル：クリティカル（Critical） 説明：Cisco Secure Awareness ライセンスの有効期限が切れるとアラートが送信されます。	パラメータ：region、server region：期限が切れた Cisco Secure Awareness ライセンスのリージョン。リージョンは、AMERICAS、EUROPE などです。 server：サーバ URL の名前（例：https://secat.cisco.com）。

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.CSA.LICENSE_ RETRIVAL_FAILURE	アラートテキスト：Cisco Secure Awareness クラウドサービスからのライセンス有効期限の詳細の取得に失敗しました（$reason） アラートレベル：警告（WARNING） 説明：Cisco Secure Awareness クラウドサービスからライセンスの有効期限の詳細を 3 回連続で取得できなかった場合にアラートが送信されます。ライセンスの有効期限の詳細が正常に取得されるまで、ライセンスの有効期限の詳細の取得が毎日試行されます。	パラメータ：reason reason：Cisco Secure Awareness クラウドサービスからライセンスの有効期限の詳細を取得できなかった理由。 例：「無効なトークン」、「最大試行回数に達しました。」