外部脅威フィードを使用する電子メールゲートウェイの設定

この章は、次の項で構成されています。

- 外部脅威フィードの概要 （1 ページ）
- 外部脅威フィードを使用する電子メールゲートウェイの設定方法 （2 ページ）
- 外部脅威フィード機能キーの取得 （3 ページ）
- 電子メールゲートウェイでの外部脅威フィードエンジンの有効化 （4 ページ）
- 外部脅威フィード ソースの設定 （5 ページ）
- 脅威が含まれているメッセージの処理 （9 ページ）
- 脅威が含まれているメッセージの処理に向けた送信者グループの設定 （9 ページ）
- 脅威が含まれているメッセージの処理に向けたコンテンツまたはメッセージ フィルタの設定 （10 ページ）
- 受信メール ポリシーへのコンテンツ フィルタのアタッチ （18 ページ）
- 外部脅威フィードおよびクラスタ （19 ページ）
- 外部脅威フィード エンジンの更新のモニタリング （19 ページ）
- アラートの表示 （19 ページ）
- メッセージ トラッキングの脅威詳細の表示 （20 ページ）

外部脅威フィードの概要

外部の脅威フィード（ETF）フレームワークによって、電子メールゲートウェイは次の外部脅威情報を使用できます。

- TAXII プロトコルで通信される STIX 形式。
- Cisco XDR ポータルからの JavaScript Object Notation（JSON）形式。

電子メールゲートウェイで外部脅威情報を使用する機能によって、組織は以下が可能です。

- マルウェア、ランサムウェア、フィッシング攻撃、標的型攻撃などのサイバー脅威にプロアクティブに対応する。

- ローカルおよびサードパーティの脅威インテリジェンス ソースに登録する。
- 電子メールゲートウェイの有効性を向上する。

電子メールゲートウェイで ETF 機能を使用するには、有効な機能キーが必要です。機能キーの入手方法の詳細は、シスコの販売担当者にお問い合わせください。

STIX（構造化された脅威情報表現）は、サイバー脅威情報を表す業界標準の構造化言語です。STIX ソースは、悪意のある、または疑わしいサイバー アクティビティを検出するために使用されるパターンを含むインジケータで構成されています。

TAXII（検知指標情報自動交換手順）は、異なる組織または製品ラインにかけて、サービス（TAXII サーバ）によってサイバー脅威情報を交換するための一連の仕様を定義します。

本リリースでは、STIX 1.1.1 および 1.2 と TAXII 1.1 の STIX/TAXII バージョンがサポートされています。

Cisco XDR ポータルでは、監視対象を継続的に収集するためのカスタムフィードを作成し、フィードURLを使用して電子メールゲートウェイでそれらを利用できます。フィードは、JSON 形式の監視対象の単純なリストです。フィードは、XDR ポータルの [インテリジェンス（Intelligence）] > [フィード（Feeds）] ページで作成および管理します。

以下は、本リリースでサポートされる STIX および XDR のセキュリティ侵害の指標（IOC）のリストです。

- ファイル ハッシュ ウォッチリスト（疑わしい、悪意のあるファイルの一連のハッシュを説明）
- IP ウォッチリスト（疑わしい、悪意のある一連の IP アドレスを説明）
- ドメイン ウォッチリスト（疑わしい、悪意のある一連のドメインを説明）
- URL ウォッチリスト（疑わしい、悪意のある一連の URL を説明）

外部脅威フィードを使用する電子メールゲートウェイの設定方法

次の手順を順番に実行します。

手順	操作内容	詳細情報
ステップ 1	外部脅威フィード機能キーを取得します。	外部脅威フィード機能キーの取得 （3 ページ）
ステップ 2	電子メールゲートウェイで ETF エンジンを有効化します。	電子メールゲートウェイでの外部脅威フィードエンジンの有効化 （4 ページ）

手順	操作内容	詳細情報
ステップ 3	ETF ソースを設定して、電子メールゲートウェイが TAXII サーバから STIX 形式で脅威フィードを取得することを許可します。	外部脅威フィード ソースの設定 （5 ページ）
ステップ 7	以下を使用して、脅威を含むメッセージを処理します。 • HAT • コンテンツ フィルタまたはメッセージ フィルタ	脅威が含まれているメッセージの処理 （9 ページ）
ステップ 8	メッセージの悪意のあるドメイン、URL、ファイル ハッシュを検出するように設定したコンテンツ フィルタを受信メール ポリシーにアタッチします。	受信メール ポリシーへのコンテンツ フィルタのアタッチ （18 ページ）

外部脅威フィード機能キーの取得

クラシックライセンスモードを使用した電子メールゲートウェイの管理

クラシックライセンシングモードを使用していて、外部脅威フィードの機能キーをお持ちでない場合は、以下の手順でシスコの Global Licensing Operations（GLO）チームに連絡して機能キーを取得してください。

手順

ステップ 1 件名を「外部脅威フィード機能キーのリクエスト」にして、GLO チーム（licensing@cisco.com）に電子メールを送信します。

ステップ 2 電子メールには製品認証キー（PAK）ファイルと発注書（PO）の詳細を入力します。

GLO チームが機能キーを手動でプロビジョニングし、電子メールゲートウェイにインストール可能なライセンスキーを電子メールで送信します。

次のタスク

（注）
- ハードウェアモデルまたは仮想電子メールゲートウェイモデルのユーザで、シスコ サーバから機能キーやソフトウェアライセンスを直接取得できる場合、外部脅威フィード機能キーは自動的に提供されます。
- 仮想電子メールゲートウェイモデルのユーザで、シスコ サーバから機能キーやライセンスを直接取得できない場合は、次の手順に従って外部脅威フィード機能キーを取得します。
  1. LRP ユーザアカウントのログイン情報を使用して、ライセンス登録ポータル（LRP）にログインします。
  2. [ライセンスの取得（Get License）] を選択します。
  3. [移行（Migration）] を選択します。
  4. [セキュリティ製品（Security Products）] を選択します。
  5. [Eメールセキュリティ（ESA）（Email Security (ESA)）] を選択します。
  6. VLN 番号を入力し、ライセンスファイルを生成します。

     生成されたライセンスファイルには、ETF 機能が含まれています。ETF 機能を使用するには、電子メールゲートウェイに新しいライセンスファイルをインストールする必要があります。

     （注） LRP アカウントにログインできない場合は、GLO チーム（licensing@cisco.com）に連絡してライセンスファイルを生成してください。

スマート ソフトウェア ライセンス モードを使用した電子メールゲートウェイの管理

電子メールゲートウェイでスマートライセンスモードをすでに使用している場合、または新規ユーザの場合、自動的に外部脅威フィード機能キーが提供されます。

電子メールゲートウェイでの外部脅威フィードエンジンの有効化

始める前に

電子メールゲートウェイで ETF 機能を使用するための、有効な機能キーがあることを確認します。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [外部脅威フィード（External Threat Feeds）] をクリックします。

ステップ 2 **[有効（Enable）]** をクリックします。

ステップ 3 ライセンス契約書ページの下部にスクロールし、[承認（Accept）] をクリックしてライセンス契約に合意します。

（注）
ライセンス契約に合意しない場合、Cisco E メール セキュリティ ゲートウェイで ETF が有効になりません。

ステップ 4 [外部脅威フィードの有効化] をチェックします。

ステップ 5 （オプション）[はい（Yes）] を選択して、ETF エンジンのルックアップの失敗のために ETF エンジンによって脅威をスキャンされなかったすべてのメッセージにカスタムヘッダーを追加します。

ステップ 6 変更を送信し、保存します。

次のタスク

ETF ソースを設定します。外部脅威フィード ソースの設定 （5 ページ） を参照してください。

外部脅威フィード ソースの設定

TAXII サーバで利用可能な脅威のコレクションについての情報をダウンロードするために、ETF ソースが使用されます。ETF ソースを設定して、電子メールゲートウェイが TAXII サーバから STIX 形式で脅威フィードを取得することを許可する必要があります。

（注） 電子メールゲートウェイでは、最大 8 個の ETF ソースを設定できます。

ETF ソースは、「ポーリングパス」と「コレクション名」で構成されるポーリング サービスを使用して設定できます。

始める前に

- 電子メールゲートウェイで ETF エンジンを有効化していることを確認します。

- ゲートウェイが外部脅威フィードを使用することを許可するために、ファイアウォールで HTTP（80）と HTTPS（443）のポートが開いていることを確認します。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。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [外部脅威フィードマネージャ（External Threat Feeds Manager）] をクリックします。

ステップ 2 [ソースに追加（Add to Source）] をクリックします。

ステップ 3 以下の表に記載される必須パラメータを入力して、ETF ソースを設定します。

パラメータ ソースの詳細	説明
ソース名（Source Name）	ETF ソースの名前を入力します。
説明（Description）	ETF ソースの説明を入力します。
TAXII の詳細（TAXII Details）	
ホスト名（Hostname）	完全修飾ドメイン名のホスト名または TAXII サーバの IP アドレスを入力します。
ポーリングパス（Polling Path）	TAXII サーバのポーリング サービスを特定するポーリング パスを入力します（例：/taxii-data）。
コレクション名（Collection Name）	TAXII サーバでホストされる脅威フィードのコレクション名を入力します（例：guest.Abuse_ch）。
ポーリング間隔（Polling Interval）	TAXII サーバから脅威フィードを取得する頻度を定義するポーリング間隔を入力します。最小値は 15 分で、デフォルト値は 60 分です。
脅威フィードの期間経過（Age of Threat Feeds）	TAXII サーバから取得できる脅威フィードの最大経過時間を入力します。経過時間の値は、365 日以内にする必要があります。

パラメータ ソースの詳細	説明
ポーリング セグメントの期間（Time Span for Poll Segment）	各ポーリングセグメントの期間を入力します。 ポーリングセグメントの最小期間は1日です。ポーリングセグメントの最大期間は、[脅威フィードの経過時間（Age of Threat Feeds）] フィールドに入力した値です。 以下のシナリオでは、[ポーリングセグメントの期間（Time Span for Poll Segment）] オプションを使用できます。 • TAXII サーバに脅威フィードの経過時間の既知の制限が存在しない場合、[脅威フィードの経過時間（Age of Threat Feeds）] オプションに入力した値を使用します。 • TAXII サーバに脅威フィードの経過時間の既知の制限が存在する場合、既知の制限値を使用します。 • TAXII サーバに脅威フィードの経過時間の既知の制限が不明な場合は、デフォルト値の 30 日を使用します。 • [脅威フィードの経過時間（Age of Threat Feeds）] オプションに入力した値が TAXII サーバにサポートされていない場合、脅威フィードの経過時間を入力した期間に基づく異なるポーリング セグメントに分割できます。 たとえば、脅威フィードの経過時間が 100 日間で、 TAXII サーバに脅威フィードの経過時間の固定の制限（「40 日」など）が設定されている場合、ポーリング セグメントの期間として 40 を入力します。 （注） ポーリング セグメントの期間が小さい値（「5 日」など）の場合、脅威フィード ソースのポーリングが完了するまでに長い時間がかかる場合があります。これにより、ゲートウェイのパフォーマンスに影響が出る可能性があります。

パラメータ ソースの詳細	説明
HTTPS の使用（Use HTTPS）	HTTPS を使用して TAXII サーバに接続する場合は [はい（Yes）] を選択します。
クレデンシャルの設定（Configure Credentials）	TAXII サーバで作成したユーザ クレデンシャルを使用して TAXII サーバにアクセスする場合は [はい（Yes）] を選択します。 ユーザ名とパスワードを入力します。
プロキシの詳細	
グローバル プロキシの使用（Use Global Proxy）	プロキシサーバを介して電子メールゲートウェイと TAXII サーバを接続するには **[はい（Yes）]** を選択します。 次のいずれかの方法でプロキシ サーバを設定できます。 • Web インターフェイスの [セキュリティ サービス（Security Services）] > [サービス アップデート（Service Updates）] ページ • CLI の *updateconfig* コマンド

ステップ 4 変更を送信し、保存します。

ETF ソースを設定した後、電子メールゲートウェイは TAXII ソースからの脅威フィードの取得を開始します。

次のタスク

- CLI で **threatfeedsconfig > sourceconfig** サブコマンドを使用して ETF ソースを設定することもできます。
- （オプション）[メールポリシー（Mail Policies）] > [外部脅威フィードマネージャ（External Threat Feeds Manager）] ページで**ポーリングの一時停止**（ ）アイコンをクリックして、設定した ETF ソースのポーリング サービスを一時停止します。
- （オプション）[メールポリシー（Mail Policies）] > [外部脅威フィードマネージャ（External Threat Feeds Manager）] ページで**ポーリングの再開**（ ）アイコンをクリックして、ETF ソースのポーリング サービスを再開します。
- （オプション）（オプション）[メールポリシー（Mail Policies）] > [外部脅威フィードマネージャ（External Threat Feeds Manager）] ページで [今すぐポーリング（Poll Now）] をクリックして、最後に成功したポーリング間隔ですぐに脅威フィードを取得します。

- 脅威が含まれているメッセージの処理 （9 ページ） を参照してください。

脅威が含まれているメッセージの処理

電子メールゲートウェイで以下を使用して、脅威が含まれているメッセージを処理できます。

- HAT
- コンテンツ フィルタまたはメッセージ フィルタ

関連項目

- 脅威が含まれているメッセージの処理に向けた送信者グループの設定 （9 ページ）。
- 脅威が含まれているメッセージの処理に向けたコンテンツまたはメッセージ フィルタの設定 （10 ページ）。

脅威が含まれているメッセージの処理に向けた送信者グループの設定

既存の送信者グループを設定して、ETF エンジンから取得した判定を使用して悪意のある IP を起源とするメッセージを処理できます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページに移動します。
ステップ 2 脅威を含むメッセージを処理するために設定する既存の送信者グループをクリックします。
ステップ 3 [設定の編集（Edit Settings）] をクリックします。
ステップ 4 悪意のある IP アドレスをフィルタ処理するために必要な ETF ソースを選択します。
ステップ 5 （オプション）[行の追加（Add Row）] をクリックして別の ETF ソースを追加します。
ステップ 6 変更を送信し、保存します。

脅威が含まれているメッセージの処理に向けたコンテンツまたはメッセージ フィルタの設定

ETF エンジンから取得した判定に基づいて脅威を含むメッセージに適切なアクションを実行するために、以下の 1 つ以上のコンテンツまたはメッセージ フィルタを設定できます。

- URL レピュテーション - ETF エンジンによって悪意があるとして分類された URL を検出します。
- ドメイン レピュテーション - ETF エンジンによって悪意があるとして分類されたドメインを検出します。
- ファイル情報による添付ファイル - ファイルのハッシュに基づいて ETF エンジンによって悪意があるとして分類されたファイルを検出します。

関連項目

- コンテンツ フィルタを使用した、メッセージの悪意のあるドメインの検出（10ページ）。
- メッセージ フィルタを使用した、メッセージの悪意のあるドメインの検出 （12 ページ）
- コンテンツ フィルタを使用した、メッセージの悪意のある URL の検出 （12 ページ）
- メッセージ フィルタを使用した、メッセージの悪意のある URL の検出 （14 ページ）
- コンテンツ フィルタを使用した、メッセージの添付ファイルの悪意のあるファイルの検出（16 ページ）。
- メッセージ フィルタを使用した、メッセージの添付ファイルの悪意のあるファイルの検出。

コンテンツフィルタを使用した、メッセージの悪意のあるドメインの検出

‘Domain Reputation’ コンテンツ フィルタを使用して、ETF によって悪意があるとして分類されたメッセージのドメインを検出し、これらのメッセージに対して適切なアクションを実行します。

始める前に

- （オプション）ドメインのみが含まれたアドレス リストを作成します。作成するには、Web インターフェイスの [メールポリシー（Mail Policies）] > [アドレスリスト（Address Lists）] ページに移動するか、CLI で `addresslistconfig` コマンドを使用します。詳細については、メール ポリシーを参照してください。

- （オプション）ドメインの例外リストを作成します。詳細については、7 ページの「ドメインの例外リストの作成」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）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動します。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。

ステップ 3 コンテンツ フィルタの名前と説明を入力します。

ステップ 4 [条件を追加（Add Condition）] をクリックします。

ステップ 5 [ドメインレピュテーション（Domain Reputation）] をクリックします。

ステップ 6 [外部脅威フィード（External Threat Feeds）] を選択します。

ステップ 7 メッセージのヘッダーの悪意のあるドメインを検出するための ETF ソースを選択します。

ステップ 8 ドメインのレピュテーションの確認に必要なヘッダーを選択します。

ステップ 9 （オプション）電子メールゲートウェイで、このコンテンツフィルタによる脅威の検出を避ける許可リストに登録されているドメインのリストを選択します。

ステップ 10 [OK] をクリックします。

ステップ 11 [アクションの追加（Add Action）] をクリックして、悪意のあるドメインを含むメッセージに対して実行する適切なアクションを設定します。

ステップ 12 変更を送信し、保存します。

ドメインの例外リストの作成

ドメインの例外リストは、ドメインのみが含まれるアドレスのリストで構成されています。電子メールゲートウェイで、設定されているすべてのドメインレピュテーションのコンテンツまたはメッセージフィルタでのドメインチェックをスキップするには、ドメインの例外リストを使用します。

手順

ステップ 1 [セキュリティサービス（Security Services）]>[ドメインレピュテーション（Domain Reputation）] に移動します。

ステップ 2 [ドメインの例外リスト（Domain Exception List）] の下の [設定の編集（Edit Settings）] をクリックします。

ステップ 3 ドメインのみが含まれている必要なアドレス リストを選択します。

ステップ 4 変更を送信し、保存します。

次のタスク

CLI で domainrepconfig コマンドを使用してドメインの例外リストを作成することもできます。詳細については、『*CLI Reference Guide for AsyncOS 12.0 for Cisco Email Security Appliances*』を参照してください。

メッセージフィルタを使用した、メッセージの悪意のあるドメインの検出

例として、以下のメッセージ フィルタ ルール構文を使用して、ETF エンジンを使用してメッセージ内の悪意のあるドメインを検出し、そのようなメッセージに対して適切な対応をします。

構文：

```
quarantine_msg_based_on_ETF: if (domain-external-threat-feeds (['etf_source1'],
 ['mail-from', 'from'], <'domain_exception_list'>)) { quarantine("Policy"); }
```

引数の説明

- `'domain-external-threat-feeds'` は、ドメイン レピュテーション メッセージ フィルタのルールです。
- `'etf_source1'`は、メッセージのヘッダーの悪意のあるドメインを検出するために使用される ETF ソースです。
- `'mail-from'`、`'from'` は、ドメインのレピュテーションを確認するために使用される必須ヘッダーです。
- `'domain_exception_list'` は、ドメインの例外リストの名前です。ドメインの例外リストが存在しない場合は「""」と表示されます。

例

以下の例では、‘Errors To:’ カスタム ヘッダーのドメインが ETF によって悪意があるとして検出された場合、メッセージが検疫されます。

```
Quaranting_Messages_with_Malicious_Domains: if domain-external-threat-feeds
(['threat_feed_source'], ['Errors-To'], "")) {quarantine("Policy");}
```

コンテンツ フィルタを使用した、メッセージの悪意のある URL の検出

‘URL Reputation’ コンテンツ フィルタを使用して、ETF によって悪意があるとして分類されたメッセージの URL を検出し、これらのメッセージに対して適切なアクションを実行します。

ETF の ‘URL Reputation’ コンテンツ フィルタは、以下のいずれかの方法で設定できます。

- 'URL Reputation' の条件と適切なアクションを使用する。
- 'URL Reputation' アクションと任意の条件を使用するか、条件を使用しない。

- 'URL Reputation' の条件とアクションを使用する。

'URL Reputation' の条件とアクションを使用して悪意のある URL を検出するには、以下の手順を使用します。

（注）
- 'URL Reputation' の条件と任意の適切なアクションを使用するには、手順のステップ 11 ～ 20 は無視してください。
- 'URL Reputation' アクションと任意の条件を使用するか、条件を使用しない場合は、手順のステップ 4 ～ 10 は無視してください。

始める前に

- 電子メールゲートウェイで URL フィルタリングが有効にされていることを確認します。URL フィルタリングを有効にするには、Web インターフェイスの [セキュリティサービス（ecurity Services）] > [URLフィルタリング（URL Filtering）] ページに移動します。詳細については、悪意のある URL または望ましくない URL からの保護を参照してください。
- 電子メールゲートウェイでアウトブレイクフィルタが有効にされていることを確認します。アウトブレイク フィルタを有効にするには、Web インターフェイスの [セキュリティサービス（ecurity Services）]>[アウトブレイクフィルタ（Outbreak Filters）] ページに移動します。詳細については、アウトブレイク フィルタを参照してください。
- 電子メールゲートウェイでスパム対策エンジンが有効にされていることを確認します。スパム対策エンジンを有効にするには、Web インターフェイスの [セキュリティサービス（ecurity Services）]>[スパム対策（Anti-Spam）] ページに移動します。詳細については、スパムおよびグレイメールの管理を参照してください。
- （オプション）URL リストを作成します。作成するには、Web インターフェイスで [メールポリシー（Mail Polices）] > [URLリスト（URL Lists）] ページに移動します。詳細については、悪意のある URL または望ましくない URL からの保護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）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動します。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。

ステップ 3 コンテンツ フィルタの名前と説明を入力します。

ステップ 4 [条件を追加（Add Condition）] をクリックします。

ステップ 5 [URLレピュテーション（URL Reputation）] をクリックします。

ステップ 6 [外部脅威フィード（External Threat Feeds）] を選択します。

ステップ 7 悪意のある URL を検出する ETF ソースを選択します。

ステップ 8 （オプション）電子メールゲートウェイで脅威を検出しない許可リストに登録されているURLのリストを選択します。

ステップ 9 メッセージの本文および件名および/またはメッセージの添付ファイルの悪意のある URL を検出するために必要な [次に含まれるURLを確認（Check URLs within）] オプションを選択します。

ステップ 10 [OK] をクリックします。

ステップ 11 [アクションを追加（Add Action）] をクリックします。

ステップ 12 [URLレピュテーション（URL Reputation）] をクリックします。

ステップ 13 [外部脅威フィード（External Threat Feeds）] を選択します。

ステップ 14 条件（ステップ 7）で選択した ETF ソースと同じ ETF ソースを選択したことを確認します。

ステップ 15 （オプション）ステップ 8 で選択したものと同じ許可リストに登録されている URL のリストを選択します。

ステップ 16 メッセージの本文および件名および/またはメッセージの添付ファイルの悪意のある URL を検出するために必要な [次に含まれるURLを確認（Check URLs within）] オプションを選択します。

ステップ 17 メッセージの本文および件名および/またはメッセージの添付ファイルの URL に対して実行する必要なアクションを選択します。

（注）
ステップ 16 で [（次に含まれるURLを確認）Check URLs within] オプションに [添付ファイル（Attachments）] を選択した場合、メッセージから添付ファイルを除去することのみが可能です。

ステップ 18 すべてのメッセージにアクションを実行するか、未署名のメッセージにアクションを実行するかを選択します。

ステップ 19 [OK] をクリックします。

ステップ 20 変更を送信し、保存します。

（注）
Web ベースのレピュテーションスコア（WBRS）と電子メールゲートウェイの ETF に対して URL レピュテーション コンテンツ フィルタを設定している場合は、電子メールゲートウェイのパフォーマンスを向上するために、WBRS URL レピュテーション コンテンツ フィルタの順序を ETF URL レピュテーションフィルタの順序よりも高く設定することをお勧めします。

メッセージフィルタを使用した、メッセージの悪意のあるURLの検出

例として、ETF エンジンを使用して悪意のあるメッセージの URL を検出し、URL を無効化するには、‘URL Reputation’ のメッセージ フィルタ ルール構文を使用します。

構文：

```
defang_url_in_message: if (url-external-threat-feeds (['etf_source1'],
<'URL_allowedlist'>,
```

```
<’message_attachments'> , <’message_body_subject’> ,))
 { url-etf-defang(['etf-source1'], "", 0); } <’URL_allowedlist’> ,
<’Preserve_signed’>)}
```

引数の説明

- ‘url-external-threat-feeds’ は、URL レピュテーションのルールです。
- ‘etf_source1’ は、メッセージまたはメッセージの添付ファイルの悪意のある URL を検出するために使用される ETF ソースです。
- 「URL_allowedlist」は、URL 許可リストの名前です。URL の許可リストが存在しない場合は「""」と表示されます。
- 'message_attachments' は、メッセージの添付ファイルの悪意のある URL をチェックするために使用します。メッセージの添付ファイルの悪意のある URL を検出するには '1' の値を使用します。
- 'message_body_subject' は、メッセージ本文と件名の悪意のある URL をチェックするために使用します。メッセージの本文と件名の悪意のある URL を検出するには '1' の値を使用します。

（注） メッセージの本文、件名、添付ファイルの悪意のある URL を検出するには '1,1' の値を使用します。

- ‘url-etf-defang’ は、悪意のある URL を含むメッセージに対して実行できるアクションの 1 つです。

  以下の例は、悪意のある URL を含むメッセージに対して適用できる ETF ベースのアクションです。

  - url-etf-strip(['etf_source1'],"None", 1)
  - url-etf-defang-strip(['etf_source1'], "None", 1, "Attachment removed")
  - url-etf-defang-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1, " Attachment removed")
  - url-etf-replace(['etf_source1'], "", "None", 1)
  - url-etf-replace(['etf_source1'], "URL removed", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed ", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed*", "None", 1, "Attachment removed")

- ‘Preserve_signed’ は、‘1’ または ‘0’ で表されます。‘1’ は、このアクションが未署名のメッセージのみに適用されることを示し、‘0’ はこのアクションがすべてのメッセージに適用されることを示します。

以下の例では、ETFエンジンによってメッセージの添付ファイルで悪意のあるURLが検出された場合、添付ファイルが除去されます。

```
Strip_Malicious_URLs: if (true) {url-etf-strip(['threat_feed_source'], "", 0);}
```

コンテンツフィルタを使用した、メッセージの添付ファイルの悪意のあるファイルの検出

'Attachment File Info' コンテンツ フィルタを使用して、ETF によって悪意があるとして分類されたメッセージの添付ファイルを検出し、これらのメッセージに対して適切なアクションを実行します。

（注） ETF エンジンは、ファイルのファイル ハッシュに基づいてルックアップを実行します。

ETF の 'Attachment File Info' コンテンツ フィルタは、以下のいずれかの方法で設定できます。

- 'Attachment File Info' の条件と適切なアクションを使用する。
- 'Strip Attachment by File Info' のアクションと任意の条件を使用するか、条件を使用しない。
- 'Attachment File Info' の条件と 'Strip Attachment by File Info' のアクションを使用する。

'Attachment by File Info' の条件と 'Strip Attachment by File Info' のアクションを使用してメッセージの悪意のある添付ファイルを検出するには、以下の手順を使用します。

（注）
- 'Attachment File Info' の条件と任意の適切なアクションを使用するには、手順のステップ 10 ～ 15 は無視してください。
- 'Strip Attachment by File Info' のアクションと任意の条件を使用するか、条件を使用しない場合は、手順のステップ 4 ～ 9 は無視してください。

始める前に

（オプション）ファイル ハッシュの例外リストを作成します。作成するには、Web インターフェイスで [メールポリシー（Mail Polices）] > [ファイルハッシュリスト（File Hash Lists）] ページに移動します。詳細については、ファイル ハッシュのリストの作成 （17 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）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動します。
ステップ 2 [フィルタの追加（Add Filter）] をクリックします。
ステップ 3 コンテンツ フィルタの名前と説明を入力します。
ステップ 4 [条件を追加（Add Condition）] をクリックします。
ステップ 5 [添付ファイル情報（Attachment File Info）] をクリックします。
ステップ 6 [外部脅威フィード（External Threat Feeds）] を選択します。
ステップ 7 ファイル ハッシュを使用して悪意のある ファイル を検出する ETF ソースを選択します。
ステップ 8 （オプション）電子メールゲートウェイで脅威を検出しないファイルハッシュのリストを選択します。
ステップ 9 [OK] をクリックします。
ステップ 10 [アクションを追加（Add Action）] をクリックします。
ステップ 11 [ファイル情報によって添付ファイルを除去（Strip Attachment by File Info）] をクリックします。
ステップ 12 [外部脅威フィード（External Threat Feeds）] を選択します。
ステップ 13 条件（ステップ 7）で選択した ETF ソースと同じ ETF ソースを選択したことを確認します。
ステップ 14 （オプション）ステップ 8 で選択したものと同じファイル ハッシュのリストを選択します。
ステップ 15 変更を送信し、保存します。

ファイル ハッシュのリストの作成

手順

ステップ 1 [メールポリシー（Mail Policies）] > [ファイルハッシュのリスト（File Hash Lists）] に移動します。
ステップ 2 [ファイルハッシュのリストの追加（Add File Hash List）] を選択します。
ステップ 3 必要なファイル ハッシュのタイプ（‘SHA256’ または ‘MD5'、または上記のすべて）をチェックします。
ステップ 4 （ステップ 3 で選択した）ファイル ハッシュをカンマで区切って、または改行して入力します。
ステップ 5 変更を送信し、保存します。

メッセージフィルタを使用した、メッセージの添付ファイルの悪意のあるファイルの検出

例として、以下のメッセージフィルタルール構文を使用して、ETFエンジンによってメッセージの添付ファイル内で悪意があるとして分類されるファイルを検出し、そのようなメッセージに対して適切な対応をします。

構文：

```
Strip_malicious_files: if (file-hash-etf-rule (['etf_source1'],
<'file_hash_exception_list'>))
{ file-hash-etf-strip-attachment-action (['etf_source1'], <'file_hash_exception_list>,
 "file stripped from message attachment"); }
```

それぞれの説明は次のとおりです。

- `'file-hash-etf-rule'` は、添付ファイル情報のメッセージ フィルタのルールです。
- `'etf_source1'` は、ファイルのハッシュに基づいてメッセージの悪意のあるファイルを検出するために使用される ETF ソースです。
- `'file_hash_exception_list'` は、ファイル ハッシュの例外リストの名前です。ファイル ハッシュの例外リストが存在しない場合は「""」と表示されます。
- `'file-hash-etf-strip-attachment-action'` は、悪意のあるファイルが含まれるメッセージに対して適用するアクションです。

以下の例では、メッセージにETFエンジンによって悪意があるとして検出された添付ファイルが含まれる場合、添付ファイルが除去されます。

```
Strip_Malicious_Attachment: if (true) {file-hash-etf-strip-attachment-action
(['threat_feed_source'], "", "Malicious message attachment has been stripped from
the message.");}
```

受信メールポリシーへのコンテンツフィルタのアタッチ

メッセージの悪意のあるドメイン、URL、ファイルハッシュを検出するように設定した1つ以上のコンテンツ フィルタを受信メール ポリシーにアタッチできます。

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 特定のメール ポリシーの [コンテンツフィルタ（Content Filters）] の下のリンクをクリックします。

ステップ 3 [コンテンツフィルタを有効にする（カスタマイズ設定）（Enable Content Filters (Customize Settings)）] を選択します。

ステップ 4 悪意のあるドメイン、URL、ファイル ハッシュを検出するために作成したコンテンツ フィルタを選択します。

ステップ 5 変更を送信し、保存します。

次のタスク

コンテンツフィルタをメールポリシーにアタッチした後、電子メールゲートウェイは、ETFエンジンから受け取った判定に基づいてメッセージに対するアクションの実行を開始します。

外部脅威フィードおよびクラスタ

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、ETFエンジンとメール ポリシーを有効化できます。

外部脅威フィード エンジンの更新のモニタリング

サービス アップデートを有効にすると、ETF エンジンのアップデートがシスコのアップデートサーバから取得されます。しかし、一部のシナリオでは（たとえば、サービスの自動アップデートを無効にした場合またはサービスの自動アップデートが機能していない場合）、ETFエンジンを手動で更新する必要があります。

ETF エンジンは、以下のいずれかの方法で手動アップデートできます。

- Web インターフェイスの [セキュリティサービス（Security Services）] > [外部脅威フィード（External Threat Feeds）] ページに移動し、[今すぐアップデート（Update Now）] をクリックします。
- CLI では、`threatfeedupdate` コマンドを使用します。

既存の ETF エンジンの詳細を確認するには、Web インターフェイスの [セキュリティサービス（Security Services）] > [外部脅威フィード（External Threat Feeds）] ページの [外部脅威フィードのアップデート（External Threat Feeds Engine Updates）] セクションを表示するか、CLI で threatfeedstatus コマンドを使用します。

アラートの表示

以下の表では、ETFエンジンによっ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
ETF ENGINE ALERT	Unable to fetch the observables from the source: $source_name after 3 failed attempts. Reason for failure: $reason	**'source'** - TAXII ソースの名前。 **'reason'** - ポーリングに失敗した理由。
	情報。TAXII ソースからのフィードのポーリングが失敗した場合に送信されます。	
ETF ENGINE ALERT	The storage limit of $count observables exceeded for the observable type: $type.	**$count** - タイプごとに許可された監視対象の数。 **$ type** - は、監視対象のタイプ。
	情報。許可された監視対象の数を超過した場合に送信されます。	

メッセージ トラッキングの脅威詳細の表示

選択した ETF の選択した IOC に対応する、脅威を含むメッセージの詳細を表示できます。

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。
- メッセージの脅威を検出するためのコンテンツまたはメッセージフィルタが動作していることを確認します。

手順

ステップ 1 [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 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [メッセージイベント（Message Event）] の下の [外部脅威フィード（External Threat Feeds）] をクリックします。

ステップ 4 選択した IOC に対応する、脅威を含むメッセージをトラッキングするために必要な IOC を選択します。

ステップ 5 （オプション）**[すべての外部脅威フィードソース（All External Threat Feed Sources）]** を選択して、電子メールゲートウェイで設定した、利用可能および消去された ETF ソースに基づいて脅威を含むメッセージを表示します。

ステップ 6 （オプション）**[現在の外部脅威フィードソース（Current External Threat Feed Sources）]** と必要な ETF ソースを選択して、電子メールゲートウェイで設定した、利用可能な ETF ソースに基づいて脅威を含むメッセージを表示します。

ステップ 7 （オプション）[外部脅威フィードソース（External Threat Feed Sources）] に特定の ETF ソースの名前を入力して、その ETF ソースに基づいて脅威を含むメッセージを表示します。

ステップ 8 **[検索（Search）]** をクリックします。

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。