# 暗号化された可視性エンジン

Encrypted Visibility Engine（EVE）は、TLS 暗号化を使用するクライアント アプリケーションとプロセスを識別するために使用されます。可視性を実現し、管理者が環境内でアクションを実行してポリシーを適用できるようにします。EVEテクノロジーは、マルウェアの特定と阻止にも使用できます。



## Encrypted Visibility Engine の概要

暗号化された可視性エンジン（EVE）は、復号を必要とせずに暗号化セッションの可視性を高めるために使用されます。暗号化されたセッションに関する洞察は、シスコの脆弱性データベース（VDB）にパッケージ化されているシスコのオープンソースライブラリによって取得されます。ライブラリは、着信暗号化セッションをフィンガープリントして分析し、一連の既知のフィンガープリントと照合します。この既知のフィンガープリントのデータベースも、Cisco VDB で利用できます。

（注） 暗号化された可視性エンジンの機能は、Snort 3 を実行している Management Center の管理対象デバイスでのみサポートされます。この機能は、Snort 2 デバイス、Device Manager の管理対象管理デバイス、または CDO ではサポートされていません。

EVE の重要な機能の一部を次に示します。

- EVEから取得した情報を使用して、トラフィックに対してアクセス コントロール ポリシー アクションを実行できます。
- Cisco Secure Firewall に含まれる VDB には、EVE によって高い信頼値で検出された一部のプロセスにアプリケーションを割り当てる機能があります。または、次の目的でカスタム アプリケーション ディテクタを作成できます。

- EVE で検出されたプロセスを新しいユーザー定義アプリケーションにマッピングする。
- EVE で検出されたプロセスにアプリケーションを割り当てるために使用されるプロセス確実性の組み込み値を上書きする。

  『Cisco Secure Firewall Management Center Device Configuration Guide』の「**Application Detection**」の章にある項「**Configuring Custom Application Detectors**」と「**Specifying EVE Process Assignments**」を参照してください。

- EVE は、暗号化されたトラフィックで Client Hello パケットを作成したクライアントのオペレーティングシステムのタイプとバージョンを検出できます。
- EVE は、Quick UDP Internet Connections（QUIC）トラフィックのフィンガープリントと分析もサポートします。Client Hello パケットからのサーバー名は、[接続イベント（Connection Events）] ページの [URL] フィールドに表示されます。

**注目** Management Center で EVE を使用するには、デバイスに有効な 脅威 ライセンスが必要です。脅威ライセンスがない場合、ポリシーによって警告が表示され、展開は許可されません。

**（注）** EVE は SSL セッションのオペレーティングシステムのタイプとバージョンを検出できます。アプリケーションやパッケージ管理ソフトウェアの実行など、オペレーティングシステムの通常の使用により、OS 検出がトリガーされる可能性があります。クライアント OS 検出を表示するには、EVE トグルボタンを有効にすることに加えて、**[ポリシー（Policies）]**>**[ネットワークの検出（Network Discovery）]** で [ホスト（Hosts）] を有効にする必要があります。ホスト IP アドレスで使用可能なオペレーティングシステムのリストを表示するには、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[ネットワークマップ（Network Map）]** をクリックし、該当するホストを選択します。

**関連リンク**

EVE の設定 （3 ページ）

# EVE の仕組み

Encrypted Visibility Engine（EVE）は、TLS ハンドシェイクの Client Hello 部分を検査して、クライアントプロセスを識別します。Client Hello は、サーバーに送信される最初のデータパケットです。これにより、ホスト上のクライアントプロセスがよくわかります。このフィンガープリントと、宛先 IP アドレスなどの他のデータが組み合わされて、EVE のアプリケーション識別の基礎となります。TLS セッションの確立で特定のアプリケーション フィンガープリントを識別することで、システムはクライアントプロセスを識別し、適切なアクション（許可/ブロック）を実行することができます。

EVEは、5,000を超えるクライアントプロセスを識別できます。システムは、アクセス制御ルールの基準として使用するために、多数のこれらのプロセスをクライアントアプリケーションにマッピングします。これにより、システムは TLS 復号を有効にすることなく、これらのアプリケーションを識別して制御することができます。既知の悪意のあるプロセスのフィンガープリントを使用することで、EVEテクノロジーを使用して、アウトバウンド復号を使用せずに暗号化された悪意のあるトラフィックを識別してブロックすることもできます。

機械学習（ML）テクノロジーにより、シスコは 10 億を超える TLS フィンガープリントと 10,000 を超えるマルウェアサンプルを毎日処理し、EVE フィンガープリントを作成および更新しています。これらの更新は、その後、シスコの脆弱性データベース（VDB）パッケージを使用してお客様に配信されます。

# EVE の設定

**ステップ 1** **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択します。

**ステップ 2** 編集するアクセス コントロール ポリシーの横にある [編集（Edit）]（✎）をクリックします。

**ステップ 3** パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

**ステップ 4** [Encrypted Visibility Engine] の横にある [編集（Edit）]（✎）をクリックします。

**ステップ 5** [Encrypted Visibility Engine] ページで、[Encrypted Visibility Engine (EVE)] トグルボタンを有効にします。

**ステップ 6** [OK] をクリックします。

**ステップ 7** [保存（Save）] をクリックします。

### 次のタスク

設定変更を展開します。

# EVE イベントの表示

[Encrypted Visibility Engine] を有効にして、アクセス コントロール ポリシーを展開すると、システムを介してライブトラフィックの送信を開始できます。ログに記録された接続イベントは、[接続イベント（Connection Events）] ページで表示できます。接続イベントにアクセスするには、Management Center で次の手順を実行します。

**ステップ 1** **[分析（Analysis）]** > **[接続（Connection）]** > **[イベント（Events）]** の順にクリックします。

**ステップ 2** [接続イベントのテーブルビュー（Table View of Connection Events）] タブをクリックします。

[分析（Analysis）] メニューにある [統合イベント（Unified Events）] ビューアに接続イベントフィールドを表示することもできます。

で暗号化された可視性エンジンでは、接続を開始したクライアントプロセス、クライアントのOS、そのプロセスにマルウェアが含まれているかどうかを特定できます。

**ステップ 3** [接続イベント（Connection Events）] ページで、Encrypted Visibility Engine 用に追加された次の列を表示します。以下の列を明示的に有効にする必要があることに注意してください。

- [暗号化された可視性プロセス名（Encrypted Visibility Process Name）]
- [暗号化された可視性プロセスの信頼スコア（Encrypted Visibility Process Confidence Score）]
- [暗号化された可視性脅威の信頼度（Encrypted Visibility Threat Confidence）]
- [暗号化された可視性脅威の信頼スコア（Encrypted Visibility Threat Confidence Score）]
- [Detection Type]

これらのフィールドの詳細については、『Cisco Secure Firewall Management Center Administration Guide』の「**Connection and Security-Related Connection Events**」の章の「**Connection and Security Intelligence Event Fields**」の項を参照してください。

（注） プロセスにアプリケーションが割り当てられている場合、[接続イベント（Connection Events）] ページの [検出タイプ（Detection Type）] 列には、クライアントアプリケーションが EVE によって識別されたことを示す [暗号化された可視性エンジン（Encrypted Visibility Engine）] が表示されます。プロセス名へのアプリケーションの割り当てがない場合、[検出タイプ（Detection Type）] 列には、クライアントアプリケーションを識別したエンジンが AppID であることを示す [AppID] が表示されます。

# EVE ダッシュボードの表示

EVE分析情報は2つのダッシュボードに表示できます。ダッシュボードにアクセスするには、次の手順を実行します。

**ステップ 1** [Overview] > [Dashboards] に移動し、[Dashboard] をクリックします。

**ステップ 2** [概要ダッシュボード（Summary Dashboard）] ウィンドウで、スイッチダッシュボードのリンクをクリックし、ドロップダウンボックスから [アプリケーション統計（Application Statistics）] を選択します。

**ステップ 3** **[Encrypted Visibility Engine]** タブを選択し、次の 2 つのダッシュボードを表示します。

- [上位のTLSフィンガープリントで検出されたプロセス（Top TLS Fingerprint Discovered Processes）] [上位の暗号化された可視性エンジンで検出されたプロセス（Top Encrypted Visibility Engine Discovered Processes）]：ネットワークで使用されている上位の TLS プロセス名と接続数が表示されます。テーブルのプロセス名をクリックすると、[接続イベント（Connection Events）] ページのフィルタリングされたビューが表示されます。このビューはプロセス名でフィルタリングされています。
- [TLSフィンガープリントマルウェア別の接続（Connections by TLS Fingerprint Malware）] [暗号化可視性エンジンの脅威の信頼度別の接続（Connections by Encrypted Visibility Engine Threat Confidence）]：マルウェアの確実性レベル（非常に高い、非常に低いなど）別に接続が表示されます。テーブル内の

脅威の信頼レベルをクリックすると、[接続イベント（Connection Events）] ページのフィルタリングされたビューが表示されます。このビューは、信頼レベルによってフィルタリングされています。

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。