



はじめに

Cisco Event Streamer (eStreamer とも称されます) により、外部のクライアント アプリケーションに Cisco Secure Firewall システム イベントをストリーミングできます。Management Center からのホストデータ、検出データ、相関データ、コンプライアンスのホワイトリストデータ、侵入データ、ユーザー アクティビティ データ、ファイルデータ、マルウェアデータ、接続データをストリーミングできます。

eStreamer は、NGIPSv、Firepower Services、Firepower Threat Defense Virtual、Firepower Threat Defense には対応していない点にご注意ください。これらのデバイスからのイベントをストリーミングするには、そのデバイスが報告する Management Center 上で eStreamer を設定できます。

eStreamer では、カスタム アプリケーション層プロトコルを使用して接続されたクライアント アプリケーションとの通信を行います。eStreamer の目的は、単にクライアントが要求されたデータを戻すことであるため、このガイドは、主に、リクエストされたデータの eStreamer 形式について記述しています。

eStreamer クライアントを作成し、Cisco Secure Firewall システム と統合するには 3 つの主要な手順があります：

1. eStreamer アプリケーション プロトコルを使用してメッセージを Management Center または管理対象デバイスと交換するクライアント アプリケーションを作成します。eStreamer SDK には、参照クライアント アプリケーションが含まれます。
2. クライアント アプリケーションに必要なイベントのタイプを送信するために Management Center またはデバイスを設定します。
3. クライアント アプリケーションを Management Center またはデバイスに接続し、データの交換を開始します。

このガイドでは、eStreamer バージョン 7.2 クライアント アプリケーションを正常に作成し、実行するのに必要な情報を提供します。

eStreamer バージョン 7.2 の主要な変更点

完全修飾イベントを受信するためのサポートが追加されました。[完全修飾イベントのリクエスト \(2-5 ページ\)](#) を参照してください

新しい Python ベースの参照クライアントが SDK に追加されました。[eStreamer Python 参照クライアントの実行 \(6-14 ページ\)](#) を参照してください

このガイドの使用方法

eStreamer サービスは、最高レベルで Cisco Secure Firewall システム から要求元のクライアントにデータをストリーミングするメカニズムです。このサービスでは、次のデータ カテゴリをストリーミングできます：

- 侵入イベント データおよび追加のイベント データ
- 相関(コンプライアンス)イベント データ
- 検出イベント データ
- ユーザー イベント データ
- イベントのメタデータ
- ホスト情報
- マルウェア イベント データ

本書では、主に、eStreamer から戻されるデータ構造について説明します。本書の各章は、次のとおりです：

- [eStreamer アプリケーションプロトコルについて\(2-1 ページ\)](#)。この章では、eStreamer 通信の概要、eStreamer クライアント アプリケーションの作成に関する要件の詳細を記述し、eStreamer サービスとのコマンドの送受信に使用される 4 種類のメッセージについて説明します。
- [侵入および相関データ構造の概要\(3-1 ページ\)](#)。この章では、侵入検出コンポーネントと相関コンポーネントによって作成されたイベント データを戻すのに使用されるデータ形式および侵入イベントや関連付けイベントを表すのに使用されるデータ形式について説明します。
- [検出と接続データ構造の概要\(4-1 ページ\)](#)。この章では、検出データ、ユーザー データ、接続イベント データを戻すために使用されるデータ形式について説明します。
- [ホスト データ構造の概要\(5-1 ページ\)](#)。この章では、ホスト情報要求メッセージを受信すると完全なホスト情報データを戻すために eStreamer が使用するデータ形式について説明します。
- [eStreamer の設定\(6-1 ページ\)](#)。この章では、Management Center または管理対象デバイスでの eStreamer の設定方法について説明します。この章では、eStreamer コマンドライン スイッチについても説明し、手動で eStreamer サービスを開始し、停止する方法、および eStreamer を自動的に開始させるために Management Center または管理対象デバイスを設定する方法を提示します。
- [データ構造の例\(A-1 ページ\)](#)。この章では、2 進数形式の eStreamer メッセージ パケットの例を示します。
- [レガシー データ構造の概要\(B-1 ページ\)](#)。この章では、現在出荷されている製品では使用されていませんが、旧クライアントが使用する可能性があるレガシー データ構造の構造について説明します。

前提条件

本ガイドの情報を理解するには、一般に Cisco Secure Firewall システム の機能と名称、およびコンポーネントの機能、特に、これらのコンポーネントが生成するさまざまなタイプのイベント データに精通している必要があります。一般的ではない用語、および製品固有の用語の多くは、*Cisco Secure Firewall eStreamer 統合ガイド*に記載されています。

Cisco Secure Firewall システム リリース向け製品バージョン

本ガイドでは、バージョン番号を使用して Management Center および管理対象デバイスによって生成されるイベントのデータ形式を説明します。[Cisco Secure Firewall システム 製品バージョン](#) 表には、主要なリリースごとの各製品バージョンを示します。

表 1-1 Cisco Secure Firewall システム 製品バージョン

リリース	Management Center バージョン	管理対象 デバイスのバージョン
3D システム 5.0	Management Center 5.0	5.0
3D システム 5.1	Management Center 5.1	5.1
3D システム 5.1.1	Management Center 5.1.1	5.1.1
3D システム 5.2	Management Center 5.2	5.2
3D システム 5.3	Management Center 5.3	5.3
Cisco Secure Firewall システム 5.3.1	Management Center 5.3.1	5.3.1
Cisco Secure Firewall システム 5.4	Management Center 5.4	5.4
Cisco Secure Firewall システム 6.0	Management Center 6.0	6.0
Cisco Secure Firewall システム 6.1	Management Center 6.1	6.1
Cisco Secure Firewall システム 6.2	Management Center 6.2	6.2
Cisco Secure Firewall システム 6.2.1	Management Center 6.2.1	6.2.1
Cisco Secure Firewall システム 6.2.2	Management Center 6.2.2	6.2.2
Cisco Secure Firewall システム 6.2.2	Management Center 6.2.3	6.2.3
Cisco Secure Firewall システム 6.3.0	Management Center 6.3.0	6.3.0
Cisco Secure Firewall システム 6.4.0	Management Center 6.4.0	6.4.0
Cisco Secure Firewall システム 6.5.0	Management Center 6.5.0	6.5.0
Cisco Secure Firewall システム 6.6.0	Management Center 6.6.0	6.6.0
Cisco Secure Firewall システム 6.7.0	Management Center 6.7.0	6.7.0
Cisco Secure Firewall システム 7.0	Management Center 7.0	7.0
Cisco Secure Firewall システム 7.1.0	Management Center 7.1.0	7.1.0

表記法

[eStreamer メッセージ データ タイプの表記法](#) 表には、eStreamer メッセージで使用されるさまざまなデータ フィールド形式を説明するために、本書で使用する名前を示します。eStreamer サービスで使用する数値定数は通常、符号なし整数値です。別途注記のない限り、ビットフィールドには下位ビットを使用します。たとえば、フラグデータの 5 ビットを含む 1 バイト フィールドでは、下位 5 ビットにデータが含まれています。

- オブジェクト モデルについて理解する:レコードを相互に関連付ける方法と、レコードに関連付けられるメタデータの内容について理解を深めます。
- 強力なエラー処理とロギングを実装します。これにより、問題が生じたときに、原因となったメッセージや状況を必ずしもエラーを再現することなく確認できるようになります。
- 言語を慎重に選択します。解析にかかるコストは計算的には高くありませんが、1秒あたりのイベント数が何千もある場合に、すべてがカウントされてしまいます。CやC++などの言語をコンパイルします。PythonやJavaScriptより高速になります。このような方法の欠点は、移植性が低いことです。
- マルチスレッディングやプロセスを実装する場合は、メタデータを扱う際に必ずメッセージを順番に処理していく必要があることを理解しておいてください。つまり、配信順序が正しくない場合は修正する必要があります。
- 既存の eStreamer 実装で、他のユーザーがこれまでどのようにして目標を達成したかを確認してください。リソースの一部を以下に示します。
 - <https://splunkbase.splunk.com> で eStreamer を検索します。
 - <https://software.cisco.com/download/home/> で、[製品の選択 (Select a Product)] の横にある [すべてを参照 (Browse All)] を選択してから、[ファイアウォール (Firewalls)], [ファイアウォール管理 (Firewall Management)], [Firepower Management Center仮想アプライアンス (Firepower Management Center Virtual Appliance)], [FirepowerシステムのツールとAPI (Firepower System Tools and APIs)] の順に選択します。
 - <https://community.cisco.com> で「eNcoreCLI」と検索します。
- Cisco Security Technical Alliance チームと連携し、eStreamer および Cisco FirePOWER との統合に関するその他の側面に対する変更に常に迅速に対応します。不明な点は、ask-csta-pm@cisco.com までお問い合わせください。

テスト

- シスコで Firepower の新しいバージョンが導入されたら、速やかにクライアントのテストを実行し、クライアントが収集したデータに変更がないことを確認します。
- 便利なテストベッドをご用意していますので、簡単かつ頻繁にテストできます。
- テストベッドを構築しない場合は、dcloud サンドボックスのテストベッドを使用します。Cisco Security Technical Alliance では、このテストベッドの設定および使用をサポートするリソースを提供しています。dcloud は包括的なテストを無料で実現します。ただし、お客様の用途に完全に対応しているわけではなく、イベントを 100% カバーできるとも限りません。また、インスタンスの使用可能期間も短くなります。dcloud の詳細については、<https://dcloud2-rtp.cisco.com> にアクセスの上、ご確認ください。

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。