



## はじめに

シスコ 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 Firepower 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、また、7000 および 8000 シリーズのデバイスからの侵入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、Firepower 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 6.2.2 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 6.2.2 の主要な変更点

バージョン 6.2.2 に新しいイベントや変更されたイベントはありません。

# このガイドの使用方法

eStreamer サービスは、最高レベルで Firepower 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 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 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 Firepower 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 データに精通する必要があります。精通していない製品またはその製品固有の用語は、ほとんどが *Firepower eStreamer 統合ガイド* に記述されています。

# Firepower 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。Firepower 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 Firepower システム 製品バージョン

リリース	Management Center のバージョン (Cisco Unified Communications Manager Version)	マスター Management Center バージョン	侵入センサーバージョン	センサー バージョン	管理対象デバイスのバージョン
IMS 3.0	管理コンソール 3.0	該当なし	ネットワークセンサー 3.0	該当なし	該当なし
IMS 3.1	管理コンソール 3.1	該当なし	ネットワークセンサー 3.1	無応答 (RNA) センサー 1.0	該当なし
IMS 3.2	管理コンソール 3.2	該当なし	ネットワークセンサー 3.2	無応答 (RNA) センサー 2.0	該当なし
3D システム 4.0	Management Center 4.0	該当なし	侵入センサー 4.0	無応答 (RNA) センサー 3.0	該当なし
3D システム 4.5	Management Center 4.5	該当なし	侵入センサー 4.5	無応答 (RNA) センサー 3.5	該当なし
3D システム 4.6.1	Management Center 4.6.1	マスター Management Center 4.6.1	該当なし	該当なし	4.6.1
3D システム 4.7	Management Center 4.7	マスター Management Center 4.7	該当なし	該当なし	4.7
3D システム 4.8	Management Center 4.8	マスター Management Center 4.8	該当なし	該当なし	4.8
3D システム 4.8.0.2	Management Center 4.8.0.2	マスター Management Center 4.8.0.2	該当なし	該当なし	4.8.0.2
3D システム 4.9	Management Center 4.9	マスター Management Center 4.9	該当なし	該当なし	4.9
3D システム 4.9.1	Management Center 4.9.1	マスター Management Center 4.9.1	該当なし	該当なし	4.9.1
3D システム 4.10	Management Center 4.10	マスター Management Center 4.10	該当なし	該当なし	4.10

表 1-1 Firepower システム 製品バージョン(続き)

リリース	Management Center のバージョン (Cisco Unified Communications Manager Version)	マスター Management Center バージョン	侵入センサーバージョン	センサーバージョン	管理対象デバイスのバージョン
3D システム 4.10.1	Management Center 4.10.1	マスター Management Center 4.10.1	該当なし	該当なし	4.10.1
3D システム 4.10.2	Management Center 4.10.2	マスター Management Center 4.10.2	該当なし	該当なし	4.10.2
3D システム 4.10.3	Management Center 4.10.3	マスター Management Center 4.10.3	該当なし	該当なし	4.10.3
3D システム 5.0	Management Center 5.0	該当なし	該当なし	該当なし	5.0
3D システム 5.1	Management Center 5.1	該当なし	該当なし	該当なし	5.1
3D システム 5.1.1	Management Center 5.1.1	該当なし	該当なし	該当なし	5.1.1
3D システム 5.2	Management Center 5.2	該当なし	該当なし	該当なし	5.2
3D システム 5.3	Management Center 5.3	該当なし	該当なし	該当なし	5.3
Firepower システム 5.3.1	Management Center 5.3.1	該当なし	該当なし	該当なし	5.3.1
Firepower システム 5.4	Management Center 5.4	該当なし	該当なし	該当なし	5.4
Firepower システム 6.0	Management Center 6.0	該当なし	該当なし	該当なし	6.0
Firepower システム 6.1	Management Center 6.1	該当なし	該当なし	該当なし	6.1
Firepower システム 6.2	Management Center 6.2	該当なし	該当なし	該当なし	6.2
Firepower システム 6.2.1	Management Center 6.2.1	該当なし	該当なし	該当なし	6.2.1
Firepower システム 6.2.2	Management Center 6.2.2	該当なし	該当なし	該当なし	6.2.2

## 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。

表 1-2 eStreamer メッセージデータ タイプの表記法

データ タイプ	説明
nn-ビット フィールド	nn ビットのビット フィールド
バイト	任意の形式のデータを含む 8 ビット バイト
int8	符号付き 8 ビット バイト
uint8	符号なし 8 ビット バイト
int16	符号付き 16 ビット 整数
uint16	符号なし 16 ビット 整数
int32	符号付き 32 ビット 整数
uint32	符号なし 32 ビット 整数
uint64	符号なし 64 ビット 整数
string	文字データを格納する可変長フィールド。
[n]	指定されたデータ タイプの n インスタンスを示す上記のデータ タイプに続く配列添字(たとえば、uint8 [4])
変数(variable)	さまざまなデータ タイプの収集
BLOB	パケットからキャプチャされる時、指定されていないタイプ、通常、生データの 2 進数オブジェクト

## IP アドレス

シスコ データベースは、2 進数形式の同じフィールドに IPv4 アドレスと IPv6 アドレスを保存します。IPv6 アドレスを取得するには、16 進表記に変換します。例:20010db800000000000000000000000004321 データベースでは、RFC に準拠して 80 ~ 95 ビットに 1 を取り込むことによって IPv4 アドレスを保存し、これによって無効な IPv6 アドレスが生成されます。たとえば IPv4 アドレス 10.5.15.1 は 00000000000000000000000000000000FFFF0A050F01 として保存されます。

