Firepower eStreamer 統合ガイド

バージョン 6.1
２０１７年7月２８日

Cisco Systems, Inc.
www.cisco.com
シスコは世界各国 200 箇所にオフィスを開設しています。
所在地、電話番号、FAX 番号
は以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

CONTENTS

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 6.1 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 6.1 の主要な変更点

Firepower システム展開を バージョン 6.1 にアップグレードする場合、次に示す変更に注意してください。これらの変更の一部では、eStreamer クライアントを更新する必要があります。

- 以下のブロックが追加されました:
  - ポリシー UUID をセンサー名およびポリシー名にマッピングするために、アクセス コントロール ポリシー メタデータ ブロック 6.0+（4-209 ページ）が追加されました。

- 以下のメタデータ レコードが追加されました:
  - アクセス コントロール ポリシー メタデータ (4-28 ページ)
  - プレフィルタ ポリシー メタデータ (4-30 ページ)
  - トンネルまたはプレフィルタのルールのメタデータ (4-31 ページ)
- 次のブロックを置き換えました:
  - 接続統計データ ブロック 6.0.x (B-198 ページ) を接続統計データ ブロック 6.1+ (4-123 ページ) に置き換えてプレフィルター フィールドおよびトンネル フィールドを追加しました。
  - 接続チャンク データ ブロック 5.1.1 ～ 6.0.x (B-147 ページ) を6.1+ の接続チャンク データ ブロック (4-104 ページ) に置き換えて、元のクライアント IP フィールドを追加しました。
  - ユーザ ログイン情報データ ブロック 6.0.x (B-112 ページ) をユーザ ログイン情報データ ブロック 6.1+ (4-199 ページ) に置き換えて、ポート フィールドとトンネリング フィールドを追加しました。

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 データに精通している必要があります。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 Device 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

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 Device のバージョン
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
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

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 Deviceのバージョン
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

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	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とき、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: `20010db80000000000000000000004321`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 `00000000000000000000FFFF0A050F01` として保存されます。

eStreamer アプリケーション プロトコルについて

Firepower システム Event Streamer（eStreamer）は、メッセージ指向のプロトコルを使用して、イベントおよびホスト プロファイル情報をクライアント アプリケーションにストリーミングします。クライアントは、Management Center からイベント データとホスト プロファイル データを要求でき、管理対象デバイスからは侵入イベント データのみを要求できます。クライアント アプリケーションは、送信されるデータを指定する要求メッセージを送信することでデータ ストリームを開始し、ストリーミング開始後に Management Center または管理対象デバイスからのメッセージ フローを制御します。

このドキュメントでは、Management Center または管理対象デバイス上の eStreamer サービスを eStreamer サーバまたは eStreamer と呼ぶことがあります。

以下の項では、eStreamer サービスに接続するための要件を説明し、eStreamer プロトコルで使用されるコマンドとデータ形式について紹介します。

- 接続の仕様（2-1 ページ）では、eStreamer サービスとクライアントとの間の通信フローについて説明し、クライアントがそのサービスとどのようにやりとりするかについて説明します。
- eStreamer 通信段階について（2-2 ページ）では、クライアント アプリケーションがデータ要求を eStreamer サーバに送信し、eStreamer が要求された情報をクライアントに配信するための通信プロトコルについて説明します。
- eStreamerメッセージ タイプについて（2-6 ページ）では、eStreamer プロトコルで使用されるメッセージ タイプについて説明し、侵入イベント データ、検出イベント データ、メタデータ、およびホスト データをクライアントに返すために eStreamer によって使用されるデータ パケットの基本構造について説明します。また、eStreamer メッセージを解釈できるクライアントの作成に役立つその他の情報を提供します。

接続の仕様

eStreamer サービス：

- SSL 接続を介する TCP を使用した通信（クライアント アプリケーションは SSL ベースの認証をサポートしている必要があります）。
- ポート 8302 で接続要求を受け入れます。
- クライアントがすべての通信セッションを開始するまで待機します。
- すべてのメッセージ フィールドをネットワーク バイト順（ビッグ エンディアン）で書き込みます。
- UTF-8 でテキストをエンコードします。

eStreamer 通信段階について

クライアントと eStreamer サービスとの間には、次の 4 つの主要な通信段階があります。

1. クライアントは eStreamer サーバとの接続を確立し、接続が両方の当事者によって認証されます。

   詳細については、認証された接続の確立（2-2 ページ）を参照してください。

2. クライアントはeStreamer サービスからデータを要求し、ストリーミングされるデータのタイプを指定します。単一のイベント要求メッセージは、イベント メタデータを含む利用可能なイベント データの任意の組み合わせを指定できます。単一のホスト プロファイル要求では、単一のホストまたは複数のホストを指定できます。

   イベント データを要求するための 2 つの要求モードを使用できます。

   - イベント ストリーム要求: クライアントは、要求されたイベント タイプと各タイプのバージョンを指定する要求フラグを含むメッセージを送信し、eStreamer サーバは要求されたデータをストリーミングすることで応答します。
   - 拡張要求: クライアントは、イベント ストリーム要求と同じメッセージ形式で要求を送信しますが、拡張要求用のフラグを設定します。これにより、クライアントと eStreamer サーバ間のメッセージのやりとりが開始され、クライアントはイベント ストリーム要求では利用できない追加の情報とバージョンの組み合わせを要求します。

   データの要求の詳細については、eStreamer からのデータの要求（2-3 ページ）を参照してください。

3. eStreamer は要求されたデータ ストリームをクライアントに確立します。

   詳細については、eStreamer からのデータの受け取り（2-5 ページ）を参照してください。

4. 接続が終了します。
   詳細については、接続の終了（2-6 ページ）を参照してください。

認証された接続の確立

クライアントが eStreamer からデータを要求できるようになるには、クライアントはeStreamer サービスとの SSL 対応 TCP 接続を開始する必要があります。クライアントは、Management Center または管理対象デバイス上の設定済みの管理インターフェイスで要求できます。クライアント接続は管理インターフェイスのトラフィック チャネル構成を強制しないため、接続用のインターフェイスを選択する場合は構成を無視できます。クライアントが接続を開始すると、eStreamer サーバが応答し、クライアントとの SSL ハンドシェイクを開始します。SSL ハンドシェイクの一部として、eStreamer サーバはクライアントの認証証明書を要求し、証明書が有効である（eStreamer サーバで内部認証局（内部 CA）によって署名されている）ことを確認します。

（注）　シスコは、クライアントが eStreamer サーバによって提示された証明書が信頼できる認証局によって署名されていることを確認するように要求することを推奨しています。これは PKCS＃12 ファイルに含まれる内部 CA 証明書で、シスコでは、新しい eStreamer クライアントを Management Center または管理対象デバイスに登録するときに提供しています。詳細については、eStreamer クライアントの認証の追加（6-3 ページ）を参照してください。

SSL セッションが確立された後、eStreamer サーバは証明書の追加の接続後検証を実行します。この検証では、クライアント接続が証明書で指定されたホストから始まり、証明書のサブジェクト名に適切な値が含まれているか確認されます。いずれかの接続後のチェックが失敗すると、eStreamer サーバは接続を閉じます。必要に応じて、クライアント ホスト名のチェックを実行しないように eStreamer サービスを設定できます（詳細については、eStreamer サービスのオプション（6-5 ページ）を参照）。

クライアントは接続後の検証を実行する必要はありませんが、シスコでは、クライアントがこの検証手順を実行することを推奨しています。認証証明書には、証明書のサブジェクト名に次のフィールド値が含まれています。

表 2-1　証明書のサブジェクト名フィールド

フィールド	値
タイトル	eStreamer
generationQualifier	サーバ

接続後の検証が終了すると、eStreamer サーバはクライアントからのデータ要求を待ちます。

eStreamer からのデータの要求

クライアントが実行する、データ要求の管理におけるタスクの概略は次のとおりです。

- 要求セッションの初期化：セッションの確立（2-3 ページ）を参照してください。
- eStreamer イベント アーカイブからのイベントの要求：イベント ストリーム要求と拡張要求を使用したイベント ストリーミングの開始（2-4 ページ）。
- ホスト データの要求：ホスト データの要求（2-5 ページ）を参照してください。
- 要求の変更：要求の変更（2-5 ページ）を参照してください。

セッションの確立

クライアントは、eStreamer サービスに最初のイベント ストリーム要求を送信することによってセッションを確立します。

この最初のメッセージでは、データ要求フラグを含めるか、または後続のメッセージでデータ要求を送信することができます。この最初のイベント ストリーム要求メッセージ自体は、イベント データ用であれ、ホスト データ用であれ、すべての eStreamer 要求の前提条件です。イベント ストリーム要求メッセージの使用方法については、イベント ストリーム要求メッセージの形式（2-11 ページ）を参照してください。

（注）　eStreamer クライアントは、Management Center または管理対象デバイス上の設定済みの管理インターフェイスで要求できます。クライアント接続は管理インターフェイスのトラフィック チャネル構成を強制しないため、接続用のインターフェイスを選択する場合は構成を無視できます。

イベント ストリーム要求と拡張要求を使用したイベント ストリーミングの開始

eStreamer サービスでは、イベント ストリーミング用の 2 つの要求モードが提供されます。モードを組み合わせた要求も可能です。どちらのモードでも、クライアントはイベント ストリーム要求メッセージで要求を開始しますが、要求フラグ ビットは別々に設定します。イベント スト

リームのメッセージ形式に関する詳細については、イベント ストリーム要求メッセージの形式 (2-11 ページ) を参照してください。

eStreamer はイベント ストリーム要求メッセージを受信すると、次のようにクライアント要求を処理します。

- 要求メッセージが要求フラグ フィールドにビット 30 を設定していない場合、eStreamer は要求フラグ フィールド内の他のセット ビットによって要求されたイベントのストリーミングを開始します。詳細については、イベント ストリーム要求の送信 (2-4 ページ) を参照してください。
- イベント ストリーム要求でビット 30 が設定されている場合、eStreamer は拡張要求処理を行います。このビットが設定されている場合は、拡張要求フラグを送信する必要があります。詳細については、拡張要求の送信 (2-4 ページ) を参照してください。eStreamer は重複する要求をすべて解決することに注意してください。複数のフラグまたは複数の拡張要求のいずれかによって同じデータの複数のバージョンを要求する場合は、最新のバージョンが使用されます。たとえば、eStreamer が検出イベント バージョン 1 および 6 のフラグ要求と、バージョン 3 の拡張要求を受信すると、バージョン 6 が送信されます。

イベント ストリーム要求の送信

イベント ストリーム要求は単純なプロセスを使用します。

- クライアントは、開始日時と、データ ストリームに含めるイベントとそのバージョン レベルを指定する要求フラグ フィールドを含む要求メッセージを eStreamer サービスに送信します。
- eStreamer は、指定された時刻にイベントのストリーミングを開始します。ストリーミング プロトコルについては、eStreamer からのデータの受け取り (2-5 ページ) を参照してください。

クライアントのイベント ストリーム要求メッセージの形式と内容については、イベント ストリーム要求メッセージの形式 (2-11 ページ) を参照してください。

クライアントが要求できるイベントのタイプとイベントのバージョンについては、表 2-6 (2-13 ページ) を参照してください。

拡張要求の送信

イベント ストリーム要求メッセージの要求フラグ フィールドにビット 30 を設定すると、拡張要求が開始され、サーバとのネゴシエーションが開始されます。このビットが設定されている場合は、拡張要求フラグを送信する必要があります。拡張要求で使用可能なイベント タイプについては、表 2-21 (2-38 ページ) を参照してください。

拡張要求の手順は次のとおりです。

- クライアントは、イベント ストリーミング要求メッセージを、要求フラグ ビット 30 を 1 に設定 (拡張要求を示す) して eStreamer に送信します。メッセージ形式の詳細については、イベント ストリーム要求メッセージの形式 (2-11 ページ) を参照してください。
- eStreamer は、クライアントが使用可能なサービスのリストをアドバタイズするストリーミング情報メッセージで応答します。ストリーミング情報メッセージの詳細については、ストリーミング情報メッセージの形式 (2-32 ページ) を参照してください。
- クライアントは、使用したいサービスを示すストリーミング要求メッセージと、そのサービスから使用可能なイベントのタイプとバージョンの要求リストを返します。要求リストは、標準イベント ストリーム要求を行う場合の要求フラグ フィールドの設定ビットに対応します。ストリーミング要求メッセージを使用してイベントを要求する方法の詳細については、「拡張要求メッセージの例」セクション (2-40 ページ) を参照してください。

- eStreamer は、クライアントのストリーミング要求メッセージを処理し、メッセージで指定された時刻にデータのストリーミングを開始します。ストリーミング プロトコルについては、eStreamer からのデータの受け取り（2-5 ページ）を参照してください。

ホスト データの要求

セッションを確立すると、ホスト データの要求をいつでも送信できます。eStreamer は、要求されたホストの情報を Firepower システム ネットワーク マップから生成します。

要求の変更

確立されたセッションの要求パラメータを変更するには、クライアントは切断して新しいセッションを要求する必要があります。

eStreamer からのデータの受け取り

（注）　eStreamer サーバは、送信したイベントの履歴を保持しません。クライアント アプリケーションは重複したイベントがないかチェックする必要があります。イベントの重複は、いくつかの理由で不注意に発生する可能性があります。たとえば、新しいストリーミング セッションを開始するときに、新しいセッションの開始点としてクライアントによって指定された時間に複数のメッセージがあり、前のセッションで送信されたものもあれば、送信されていないものもある可能性があります。eStreamer は、指定された要求基準を満たすすべてのメッセージを送信します。アプリケーションは、結果の重複を検出する必要があります。

非アクティブの期間中、eStreamer はクライアントに定期的なヌル メッセージを送信して、接続を開いたままにします。クライアントまたは中間ホストからエラー メッセージを受信すると、接続を終了します。

eStreamer は、要求モードに応じて、要求されたデータをクライアントに異なる方法で送信します。

イベント ストリーム要求

クライアントがイベント ストリーム要求を送信すると、eStreamer はメッセージごとにデータ メッセージを返します。クライアントの確認応答を待つことなく、複数のメッセージを連続して送信することができます。特定の時点で、中断し、クライアントの応答を待ちます。クライアント オペレーティング システムは、受信したデータをバッファリングし、クライアントが独自のペースで処理できるようにします。

クライアント要求にメタデータの要求が含まれている場合、eStreamer は最初にメタデータを送信します。クライアントは、後続のイベント レコードを処理するときに使用できるように、それをメモリに保存する必要があります。

拡張要求

クライアントが拡張要求を送信すると、eStreamer はメッセージをキューに入れてバンドルで送信します。eStreamer は、クライアントの確認応答を待つことなく、複数のバンドルを連続して送信することができます。特定の時点で、中断し、クライアントの応答を待ちます。クライアント オペレーティング システムは、受信したデータをバッファリングし、クライアントが独自のペースで読み取ることができるようにします。

クライアントは各バンドルをメッセージごとに解凍し、レコードとブロックの長さを使用して各メッセージを解析します。各メッセージ ヘッダーのメッセージ全体の長さを使用して、各メッセージの終わりに達した時点を計算し、バンドル全体の長さを使用して、バンドルの終わりに達した時点を知ることができます。バンドルを正しく解析するためにそのコンテンツのインデックスは必要ありません。

メッセージのバンドリング メカニズムについては、メッセージ バンドルの形式（2-41 ページ）を参照してください。

クライアントが追加のフロー制御に使用できるヌル メッセージについては、ヌル メッセージの形式（2-8 ページ）を参照してください。

接続の終了

eStreamer サーバは、接続を閉じる前にエラー メッセージの送信を試行します。エラー メッセージについては、エラー メッセージの形式（2-9 ページ）を参照してください。

eStreamer サーバは、次の理由でクライアント接続を閉じる可能性があります。

- メッセージを送信するとエラーが発生する。これには、非アクティブの期間中に eStreamer が送信するイベント データ メッセージとヌル キープアライブ メッセージの両方が含まれます。
- クライアント要求の処理中にエラーが発生する。
- クライアント認証が失敗する（エラー メッセージは送信されません）。
- eStreamer サービスがシャットダウンしている（エラー メッセージは送信されません）。

クライアントはいつでも eStreamer サーバへの接続を閉じることができ、エラー メッセージ形式を使用して理由を eStreamer サーバに通知することを試行する必要があります。

eStreamerメッセージ タイプについて

eStreamer アプリケーション プロトコルは、標準メッセージ ヘッダーと、メッセージのペイロードを含むレコード データが続く様々なサブヘッダー フィールドを含む単純なメッセージ形式を使用します。メッセージ ヘッダーはすべての eStreamer メッセージ タイプで同じです。詳細については、eStreamer メッセージ ヘッダー（2-8 ページ）を参照してください。

表 2-2　eStreamer メッセージ タイプ

Message Type	名前	説明
0	ヌル メッセージ	eStreamer サーバとクライアントの両方が、データ フローを制御するためのヌル メッセージを送信します。詳細については、ヌル メッセージの形式（2-8 ページ）を参照してください。
1	エラー メッセージ	eStreamer サーバとクライアントの両方がエラー メッセージを使用して、接続が閉じた理由を示します。詳細については、エラー メッセージの形式（2-9 ページ）を参照してください。

表 2-2　eStreamer メッセージ タイプ(続き)

Message Type	名前	説明
2	イベント ストリーム要求	クライアントは、このメッセージ タイプをeStreamer サービスに送信して、新しいストリーミング セッションを開始し、データを要求します。詳細については、イベント ストリーム要求メッセージの形式(2-11 ページ)を参照してください。
4	イベント データ	eStreamer サービスは、このメッセージ タイプを使用して、イベント データとメタデータをクライアントに送信します。詳細については、イベント データ メッセージの形式(2-18 ページ)を参照してください。
5	ホスト データ要求	クライアントはこのメッセージ タイプをeStreamer サービスに送信し、ホスト データを要求します。セッションは、すでにイベント ストリーム要求メッセージを介して開始されていなければなりません。詳細については、ホスト要求メッセージの形式(2-27 ページ)を参照してください。
6	単一ホスト データ	eStreamer サービスは、このメッセージ タイプを使用して、クライアントが要求した単一のホスト データを送信します。詳細については、ホストデータおよびマルチホスト データ メッセージの形式(2-31 ページ)を参照してください。
7	複数のホスト データ	eStreamer サービスは、このメッセージ タイプを使用して、クライアントが要求した複数のホスト データを送信します。詳細については、ホストデータおよびマルチホスト データ メッセージの形式(2-31 ページ)を参照してください。
2049	ストリーミング要求	クライアントは、このメッセージ タイプを拡張要求で使用して、希望するストリーム情報メッセージからアドバタイズされたイベントを指定します。詳細については、拡張要求メッセージの例(2-40 ページ)を参照してください。
2051	ストリーミング情報	eStreamer サービスは、このメッセージ タイプを拡張要求で使用して、クライアントが使用可能なサービスのリストをアドバタイズします。詳細については、ストリーミング情報メッセージの形式(2-32 ページ)を参照してください。
4002	メッセージ バンドル	eStreamer サービスは、このメッセージ タイプを使用して、クライアントにストリーミングするメッセージをパッケージ化します。詳細については、メッセージ バンドルの形式(2-41 ページ)を参照してください。

eStreamer メッセージ ヘッダー

すべての eStreamer メッセージは、次の図に示すメッセージ ヘッダーで始まります。次の表では、フィールドについて説明しています。

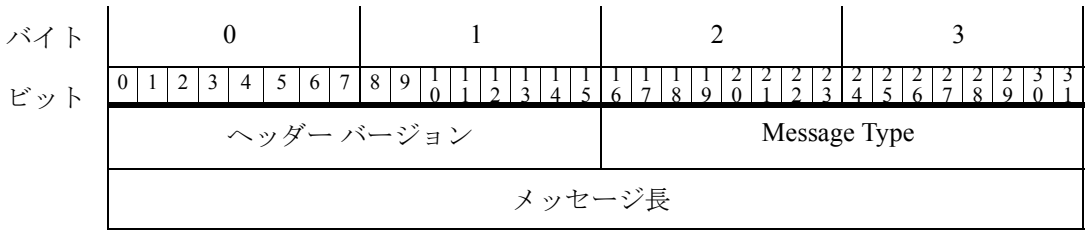


表 2-3　標準の eStreamer メッセージ ヘッダー フィールド

フィールド	データ タイプ	説明
ヘッダー バージョン	uint16	メッセージで使用されるヘッダーのバージョンを示します。eStreamer の現在のバージョンの場合、この値は常に 1 となります。
Message Type	uint16	送信されるメッセージのタイプを示します。現在の値のリストについては、表 2-2（2-6 ページ）を参照してください。
メッセージ長	uint32	後続のコンテンツの長さを示し、メッセージ ヘッダー自体のバイトを除外します。ヘッダーがありデータのないメッセージのメッセージ長はゼロです。

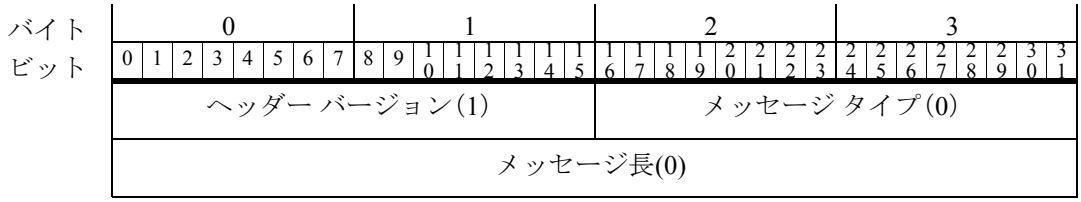
ヌル メッセージの形式

クライアント アプリケーションと eStreamer サービスの両方がヌル メッセージを送信します。ヌル メッセージのタイプは 0 で、メッセージ ヘッダーの後ろにデータはありません。

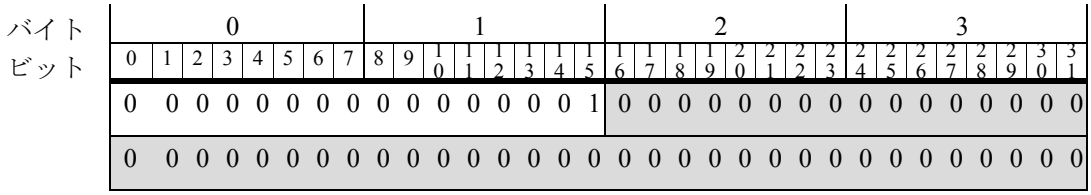
クライアントは、追加のデータを受け入れる準備ができていることを示すために、ヌル メッセージを eStreamer サーバに送信します。eStreamer サービスは、データが送信されていないときに接続のアクティブ状態を維持するために、ヌル メッセージをクライアントに送信します。ヌル メッセージのメッセージ長の値は、常に 0 に設定されています。

ヒント　本書のデータ構造図では、(1) や (115) のようなカッコ内の整数は、定数フィールド値を表します。たとえば、ヘッダー バージョン (1) は、議論中のデータ構造のフィールドが常に 1 の値を持つことを意味します。

ヌル メッセージの形式を以下に示します。メッセージ内のゼロ以外の値のみがヘッダー バージョンです。



バイナリ形式のヌル メッセージの例を次に示します。ゼロ以外の値だけが、ヘッダー バージョン値 1 を示す 2 番目のバイトに存在することに注目してください。メッセージのタイプと長さのフィールド(網掛け)の値はそれぞれ 0 です。



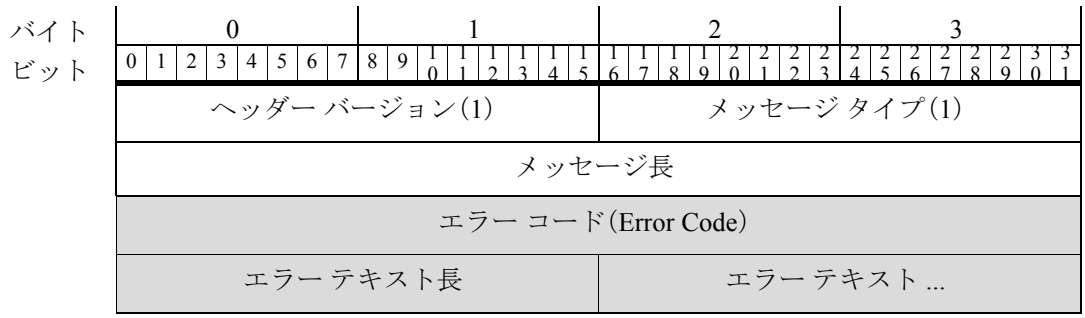
ヒント　このガイドの例は、どのビットが設定されているかを明確に示すためにバイナリ形式で表示されています。これは、イベント要求メッセージ フィールドやイベント影響フィールドなど、一部のメッセージにとって重要です。

エラー メッセージの形式

クライアント アプリケーションと eStreamer サービスの両方でエラー メッセージが使用されます。エラー メッセージのメッセージタイプは 1 で、ヘッダー、エラー コード、エラー テキスト長、および実際のエラー テキストが含まれています。エラー テキストには、0 ～ 65,535 バイトを含めることができます。

クライアント アプリケーションのカスタム エラー メッセージを作成する場合、シスコは、エラー コードとして -1 を使用することを推奨します。

次の図は、基本的なエラー メッセージの形式を示しています。網掛けのフィールドは、エラー メッセージに固有のフィールドです。



次の表では、エラー コード メッセージの各フィールドについて説明します。

表 2-4　エラー メッセージのフィールド

フィールド	データ タイプ	説明
エラー コード（Error Code）	int32	エラーを表す数値。
エラー テキスト長	uint16	エラー テキスト フィールドに含まれるバイト数。
エラー テキスト	変数	エラー メッセージ。最大 65,535 バイト。

次の図に、エラー メッセージの例を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
A	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
B	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
C	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1
D	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	1	0	0	1	1	1	0	0	1	1	0	1	1	1	1
	0	0	1	0	0	0	0	0	0	1	1	1	0	0	1	1	0	1	1	1	0	0	0	0	0	1	1	0	0	0	0	1
	0	1	1	0	0	0	1	1	0	1	1	0	0	1	0	1																

上記の例では、次の情報が表示されます。

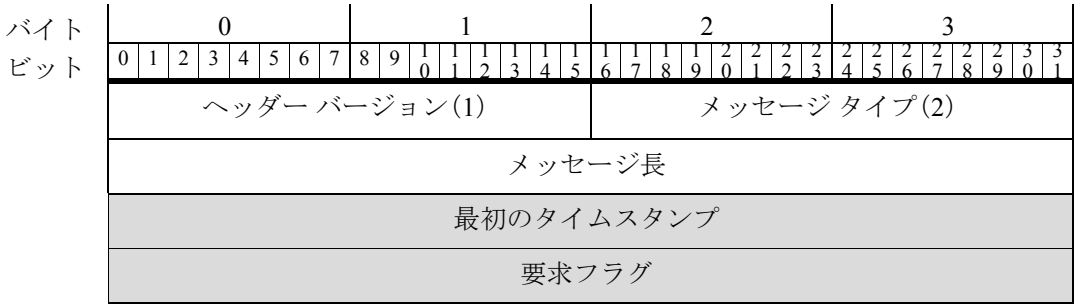
文字	説明
A	最初の 2 バイトは、標準ヘッダー値 1 を示します。2 番目の 2 バイトは値 1 を示し、送信がエラー メッセージであることを示します。
B	この行は、それに続くメッセージ データの量を示します。この例では、15 バイト（バイナリで 1111）のデータが続きます。
C	この行には、エラー コードが表示されます。この例では、メッセージに値 19（10011）が含まれています。したがって、エラー番号 19 がメッセージで送信されます。
D	この行には、エラー メッセージのバイト数（1001、または 9 バイト）が含まれ、エラー メッセージ自体が次の 9 バイトに続きます。エラー メッセージの値は、ASCII テキストに変換された場合、エラー コード 19 に付随するエラー メッセージである「スペースなし（No space）」と等しくなります。

イベント ストリーム要求メッセージの形式

eStreamer クライアントは、イベント ストリーム要求メッセージを使用して、ストリーミング セッションを開始します。要求メッセージには、開始時間と、eStreamer サービスが含むべきデータを指定するためのビット フラグ フィールドが含まれ、イベントの任意の組み合わせ、および侵入イベントの追加データやメタデータにすることができます。イベント ストリーム要求メッセージは、イベント ストリーム要求と拡張要求の両方を開始することができます。メッセージ タイプは 2 です。

ホスト プロファイル情報専用の要求を含む、すべてのデータ要求に対するイベント ストリーム要求メッセージを送信する必要があります。このような場合は、最初にイベント ストリーム要求メッセージを送信し、次にホスト要求メッセージ（タイプ 5）を送信してホスト データを指定します。

次の図に、イベント ストリーム要求メッセージの形式を示します。このメッセージは、標準ヘッダーを使用しています。網掛けのフィールドは要求メッセージに固有のフィールドで、次の表で説明します。



次の表では、イベント ストリーム要求メッセージの各フィールドについて説明します。

表 2-5　イベント ストリーム要求メッセージのフィールド

フィールド	データ タイプ	説明
最初のタイムスタンプ	uint32	セッションの開始を定義します。開始するタイミング： • クライアントが eStreamer に接続するときに開始するには、すべてのタイムスタンプ ビットを 1 に設定します。 • 使用可能な最も古いデータから開始するには、すべてのタイムスタンプ ビットをゼロに設定します。 • 特定の日時に開始するには、UNIX タイムスタンプ（1970 年 1 月 1 日以降の秒数）を指定します。 詳細については、以下の最初のタイムスタンプ（2-12 ページ）を参照してください。
要求フラグ	bits[32]	イベント ストリーム要求で返されるイベントとメタデータのタイプとバージョンを指定します。フラグの定義については、要求フラグ（2-12 ページ）を参照してください。 ビット 30 を設定すると、同じメッセージ内のイベント ストリーム要求と共存できる拡張要求が開始されます。

最初のタイムスタンプ

（注）　以下で説明するように、クライアント アプリケーションは、イベント ストリーム要求を送信するときに、[最初のタイムスタンプ（Initial Timestamp）] フィールドのアーカイブ タイムスタンプを使用する必要があります。これにより、誤ってイベントを除外しないようにします。デバイスは、送信遅延を伴う「ストア アンド フォワード」メカニズムを使用して、データをManagement Center に送信します。検出したデバイスによって割り当てられた生成タイムスタンプによってイベントを要求した場合、遅延イベントが除外される可能性があります。

セッションを開始するときは、前のセッションの最後のレコードのアーカイブ タイムスタンプ（「サーバ タイムスタンプ」とも呼ばれる）から起動することを推奨します。これは技術的な要件ではありませんが、強く推奨されます。特定の状況下では、生成タイムスタンプを使用すると、意図せずに新しいストリーミング セッションからイベントを除外してしまう可能性があります。

ストリーミングされたイベントにアーカイブ タイムスタンプを含めるには、要求フラグ フィールドにビット 23 を設定する必要があります。

時間ベースのイベントだけがアーカイブ タイムスタンプを持つことに注意してください。ビット 23 が設定された拡張イベント ヘッダーが要求された場合、メタデータなどの eStreamer が生成するイベントのこのフィールドはゼロになります。

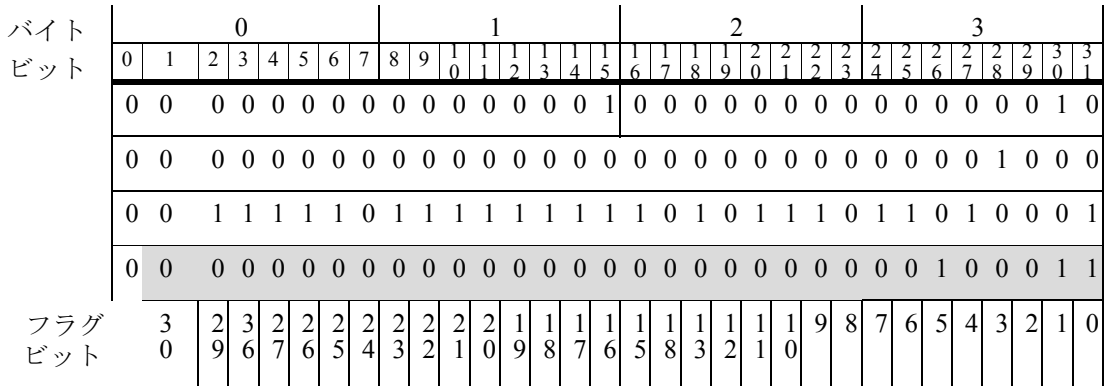
要求フラグ

eStreamer が送信するイベントのタイプを選択するには、イベント データ要求のフラグ フィールドにビット 0 ～ 29 を設定します。拡張要求モードをアクティブにするには、ビット 30 を設定します。ビット 30 を設定しても、データは直接要求されません。このビットが設定されている場合は、拡張要求フラグを送信する必要があります。クライアントは、イベント ストリーム要求メッセージの送信後のサーバ/クライアント メッセージ ダイアログ中にデータを要求します。拡張要求については、eStreamer からのデータの要求（2-3 ページ）を参照してください。

[要求フラグ（Request Flags）] フィールドのビット設定の定義については、表 2-6（2-13 ページ）を参照してください。異なるフラグは、異なるバージョンのイベント データを要求します。たとえば、4.10 形式ではなくFirepower システム 4.9 形式でデータを取得するには、異なるフラグ ビットを設定します。特定の製品バージョンのデータを要求するときに使用するフラグの固有情報については、表 2-7（2-16 ページ）を参照してください。

個々のメタデータ レコードではなく、バージョン別にメタデータを要求することに注意してください。サポートされている各メタデータのバージョンについては、要求フラグ（2-12 ページ）を参照してください。

次の図では、現在使用されているフラグ フィールドのビットを網掛けにしています。



各要求フラグ ビットについては、次の表を参照してください。

表 2-6　　要求フラグ

ビット フィールド	説明
ビット 0	侵入イベントに関連付けられたパケット データの送信を要求します。1 に設定すると、パケット データが侵入イベントとともに送信されます。0 に設定すると、パケット データは送信されません。
ビット 1	侵入、検出、相関、および接続イベントに関連するバージョン 1 メタデータの送信を要求します。1 に設定すると、バージョン 1 のメタデータがイベントとともに送信されます。0 に設定すると、バージョン 1 のメタデータは送信されません。 メタデータを使用して、イベントのコード化されたフィールドおよび数値フィールドを解決できます。eStreamer がメタデータをクライアントに送信する方法と、クライアントがメタデータを使用する方法に関する一般的な情報については、メタデータについて（2-42 ページ）を参照してください。
ビット 2	侵入イベントの送信を要求します。ビット 2、ビット 6、またはビット 2 および 6 の両方が 1 に設定されているが、拡張要求フラグであるビット 30 が 0 に設定されている場合、システムはこれをバージョン 4.x クライアントからの要求として解釈し、レコード タイプ 104/105 が送信されます。ビット 2、ビット 6、またはビット 2 と 6 の両方が 1 に設定され、ビット 30 が 1 に設定されているときにイベント タイプが指定されていない場合、システムはこれをバージョン 5.0-5.1 クライアントからの要求として解釈し、レコード タイプ 207/208 が送信されます。ビット 30 が 1 に設定され、特定のイベント タイプが要求された場合は、ビット 2 および 6 に関係なく、侵入イベントが送信されます。 レコード タイプの要求の詳細については、拡張要求の送信（2-4 ページ）を参照してください。 ビット 2、ビット 6、ビット 30 がすべて 0 に設定されている場合、侵入イベントは送信されません。 ビット 6 は、ビット 2 と同じ方法で使用されます。いずれかのビットを設定して侵入イベントを要求することができます。これらのビットの 1 つを 0 に設定しても、他のビットは上書きされません。ビット 2 を 0 に設定してビット 6 を 1 に設定するか、またはビット 2 を 1 に設定してビット 6 を 0 に設定すると、侵入イベントの要求として解釈されます。
ビット 3	検出データ バージョン 1（Management Center 3.2）の送信を要求します。0 に設定すると、検出データ バージョン 1 は送信されません。 検出イベントの詳細については、検出と接続データ構造の概要（4-1 ページ）を参照してください。
ビット 4	相関データ バージョン 1（Management Center 3.2）の送信を要求します。0 に設定すると、相関データ バージョン 1 は送信されません。

表 2-6　要求フラグ（続き）

ビット フィールド	説明
ビット 5	影響相関イベント（侵入影響アラート）の送信を要求します。1 に設定すると、侵入影響アラートが送信されます。0 に設定すると、侵入影響アラートは送信されません。 侵入影響アラートの詳細については、侵入の影響アラート データ 5.3 以上（3-18 ページ）を参照してください。
ビット 6	ビット 6 は、ビット 2 と同じ方法で使用されます。ビット 2（2-13 ページ）を参照してください。
ビット 7	検出データ バージョン 2（Management Center 4.0 ～ 4.1）の送信を要求します（1 に設定されている場合）。0 に設定すると、検出データ バージョン 2 は送信されません。
ビット 8	接続データ バージョン 1（Management Center 4.0 ～ 4.1）の送信を要求します（1 に設定されている場合）。0 に設定すると、接続データ バージョン 1 は送信されません。
ビット 9	相関データ バージョン 2（Management Center 4.0 ～ 4.1.x）の送信を要求します（1 に設定されている場合）。0 に設定すると、相関ポリシー データ バージョン 2 は送信されません。
ビット 10	検出データ バージョン 3（Management Center 4.5 ～ 4.6.1）の送信を要求します（1 に設定されている場合）。0 に設定すると、検出データ バージョン 3 は送信されません。 レガシー検出イベントの詳細については、レガシー ディスカバリ データ構造（B-93 ページ）を参照してください。
ビット 11	イベントの送信を無効にします。
ビット 12	接続データ バージョン 3（Management Center 4.5 ～ 4.6.1）の送信を要求します（1 に設定されている場合）。0 に設定すると、接続データ バージョン 3 は送信されません。
ビット 13	相関データ バージョン 3（Management Center 4.5 ～ 4.6.1）の送信を要求します。0 に設定すると、相関データ バージョン 3 は送信されません。
ビット 14	侵入、検出、相関、および接続イベントに関連するバージョン 2 メタデータの送信を要求します。1 に設定すると、バージョン 2 のメタデータがイベントとともに送信されます。0 に設定すると、バージョン 2 のメタデータは送信されません。 eStreamer がメタデータをクライアントに送信する方法と、クライアントがメタデータを使用する方法に関する一般的な情報については、メタデータについて（2-42 ページ）を参照してください。
ビット 15	侵入、相関、検出、および接続イベントに関連するバージョン 3 メタデータの送信を要求します。1 に設定すると、バージョン 3 のメタデータがイベントとともに送信されます。0 に設定すると、バージョン 3 のメタデータは送信されません。 eStreamer がメタデータをクライアントに送信する方法と、クライアントがメタデータを使用する方法に関する一般的な情報については、メタデータについて（2-42 ページ）を参照してください。
ビット 16	未使用（Unused）
ビット 17	検出データ バージョン 4（Management Center 4.7 ～ 4.8.x）の送信を要求します。0 に設定すると、検出データ バージョン 4 は送信されません。
ビット 18	接続データ バージョン 4（Management Center 4.7 ～ 4.9.0.x）の送信を要求します（1 に設定されている場合）。0 に設定すると、接続データ バージョン 4 は送信されません。詳細については、接続チャンク メッセージ（4-55 ページ）を参照してください。
ビット 19	相関データ バージョン 4（Management Center 4.7）の送信を要求します。0 に設定すると、相関データ バージョン 4 は送信されません。 Management Center 4.7 形式で送信される相関イベントについては、レガシー相関イベントのデータ構造（B-252 ページ）を参照してください。

表 2-6　要求フラグ(続き)

ビット フィールド	説明
ビット 20	侵入、検出、ユーザ アクティビティ、相関、および接続イベントに関連するバージョン 4 メタデータの送信を要求します。1 に設定すると、バージョン 4 のメタデータがイベントとともに送信されます。0 に設定すると、バージョン 4 のメタデータは送信されません。 バージョン 4 のメタデータには、次のものが含まれます。 • 相関(コンプライアンス)ルールの情報 • 相関(コンプライアンス)ポリシーの情報 • フィンガープリント レコード • クライアント アプリケーション レコード • クライアント アプリケーション タイプのレコード • 脆弱性レコード • ホストの重要度レコード • ネットワーク プロトコル レコード • ホストの属性レコード • スキャン タイプのレコード • ユーザ レコード • サービス検出デバイス(バージョン 2)のレコード • イベント分類(バージョン 2)のレコード • 優先順位レコード • ルール情報(バージョン 2) • マルウェアの情報 ビット 22 を使用してビット 20 を要求すると、ユーザのメタデータも送信されます。 eStreamer がメタデータをクライアントに送信する方法と、クライアントがメタデータを使用する方法に関する一般的な情報については、メタデータについて(2-42 ページ)を参照してください。
ビット 21	バージョン 1 ユーザ イベントの送信を要求します。ユーザ イベントの詳細については、ユーザ レコード(4-21 ページ)を参照してください。
ビット 22	相関データ バージョン 5(Management Center 4.8.0.2 ～ 4.9.1)の送信を要求します。0 に設定すると、相関データ バージョン 5 は送信されません。 ビット 22 を使用してビット 20 を要求すると、ユーザのメタデータも送信されます。 レガシー相関(コンプライアンス)イベントの詳細については、レガシー相関イベントのデータ構造(B-252 ページ)を参照してください。
ビット 23	拡張イベント ヘッダーを要求します。1 に設定すると、イベントは、eStreamer サーバが処理するためにイベントがアーカイブされたときに適用されたタイムスタンプと、将来の使用のために予約された 4 バイトが付いて送信されます。このフィールドが 0 に設定されている場合、イベントは、レコード タイプとレコード長のみを含む標準のイベント ヘッダーが付いて送信されます。 イベント メッセージ ヘッダーについては、eStreamer メッセージ ヘッダー(2-8 ページ)を参照してください。

表 2-6　要求フラグ（続き）

ビット フィールド	説明
ビット 24	検出データ バージョン 5（Management Center 4.9.0.x）の送信を要求します。0 に設定すると、検出データ バージョン 5 は送信されません。 検出イベントの詳細については、検出と接続データ構造の概要（4-1 ページ）を参照してください。
ビット 25	検出データ バージョン 6（Management Center 4.9.1+）の送信を要求します。0 に設定すると、検出データ バージョン 6 は送信されません。 検出イベントの詳細については、検出と接続データ構造の概要（4-1 ページ）を参照してください。
ビット 26	接続データ バージョン 5（Management Center 4.9.1 ～ 4.10.x）の送信を要求します（1 に設定されている場合）。0 に設定すると、接続データ バージョン 5 は送信されません。詳細については、接続チャンク メッセージ（4-55 ページ）を参照してください。
ビット 27	追加データ レコード内の侵入イベントに関連するイベント追加データを要求します。 イベント データの詳細については、表 3-11侵入イベント追加データのデータ ブロック フィールド（3-30 ページ）を参照してください。
ビット 28	検出データ バージョン 7（Management Center 4.10.0+）の送信を要求します。0 に設定すると、検出データ バージョン 7 は送信されません。 検出イベントの詳細については、検出と接続データ構造の概要（4-1 ページ）を参照してください。
ビット 29	相関データ バージョン 6（Management Center 4.10 ～ 4.10.x）の送信を要求します。0 に設定すると、相関ポリシー データ バージョン 6 は送信されません。 ビット 29 を使用してビット 20 を要求すると、ユーザのメタデータも送信されます。 相関イベントの詳細については、製品の以前のバージョンを参照してください。
ビット 30	eStreamer への拡張要求を示します。このビットが設定されている場合は、拡張要求フラグを送信する必要があります。拡張要求については、拡張要求の送信（2-4 ページ）を参照してください。

特定のバージョンのデータを要求するために使用するフラグを決定するには、次の表を参照してください。バージョン 5.0 以降の場合は、ビット 30 の使用の詳細について、拡張要求の送信（2-4 ページ）を参照してください。

表 2-7　製品バージョン別のイベント要求フラグ

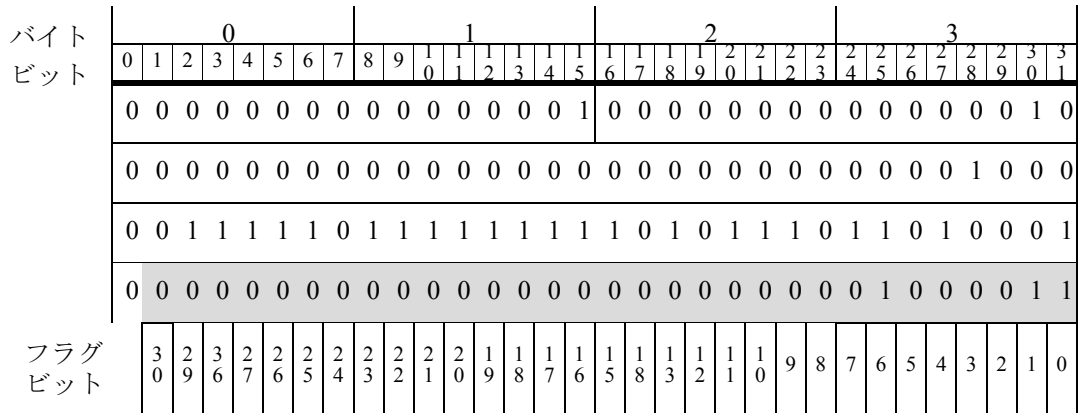
要求されたデータのタイプ	4.9.0.x	4.9.1.x	4.10.x	5.0+	5.1	5.1.1+
パケット データ	ビット 0	ビット 0	ビット 0	ビット 0	ビット 0	ビット 0
侵入イベント	ビット 2	ビット 2	ビット 2	ビット 2	ビット 2	ビット 30
メタデータ	ビット 20	ビット 20	ビット 20	ビット 20	ビット 20	ビット 20
検出イベント	ビット 24	ビット 25	ビット 28	ビット 30	ビット 30	ビット 30
相関イベント	ビット 22	ビット 22	ビット 29	ビット 30	ビット 30	ビット 30
イベント追加データ	—	—	ビット 27	ビット 27	ビット 27	ビット 27
影響イベント アラート	ビット 5	ビット 5	ビット 5	ビット 5	ビット 5	ビット 5
接続データ	ビット 18	ビット 26	ビット 26	ビット 30	ビット 30	ビット 30
ユーザ イベント	ビット 21	ビット 21	ビット 21	ビット 30	ビット 30	ビット 30

表 2-7　製品バージョン別のイベント要求フラグ（続き）

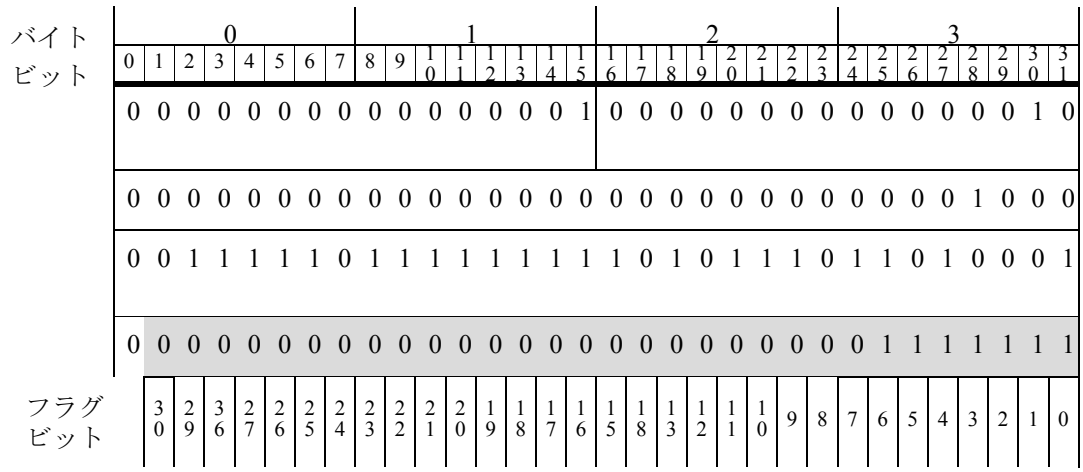
要求されたデータのタイプ	4.9.0.x	4.9.1.x	4.10.x	5.0+	5.1	5.1.1+
マルウェア イベント	—	—	—	—	—	ビット 30
ファイル イベント	—	—	—	—	—	ビット 30

注意　バージョン 5.x より前のすべてのイベント タイプでは、参照クライアントは、検出エンジン ID フィールドをセンサー ID とラベル付けします。

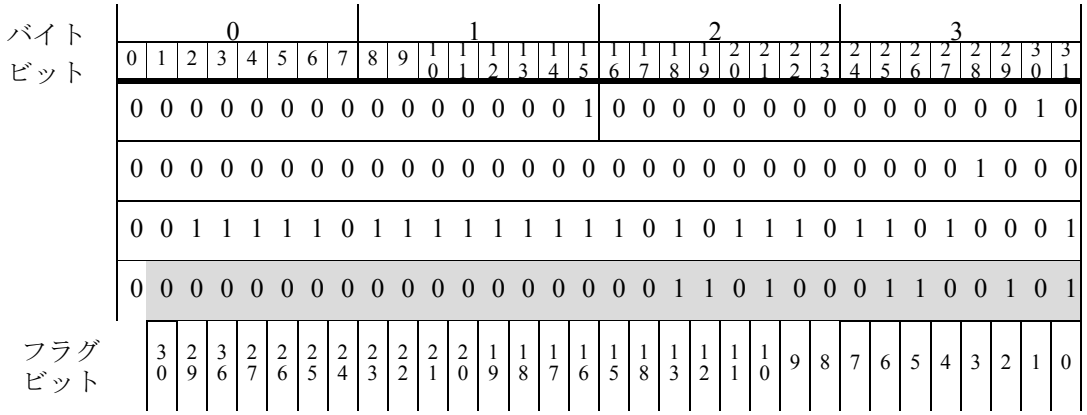
次の例では、バージョン 1 のメタデータとパケット フラグの両方を使用して、タイプ 7（Firepower システム 3.2+ と互換性あり）の侵入イベントを要求しています。



Firepower システム 3.2 と互換性のあるデータ（侵入イベント、パケット、メタデータ、影響アラート、ポリシー違反イベント、およびバージョン 2.0 イベントを含む）のみを要求するには、以下を使用します。



侵入影響アラート、相関イベント、検出イベント、接続イベント、およびパケットとバージョン 3 メタデータを含むタイプ 7 の侵入イベントを Management Center 4.6.1+ 形式で要求するには、以下を使用します。



イベント データ メッセージの形式

eStreamer サービスは、イベント要求を受信すると、イベント データと関連するメタデータをクライアントに送信します。イベント データ メッセージのメッセージ タイプは 3 です。各メッセージには、イベント データまたはメタデータのいずれかを含む単一のデータ レコードが含まれています。

タイプ 3 のメッセージは、イベント データとメタデータのみを伝送することに注意してください。eStreamer は、タイプ 6（単一ホスト）とタイプ 7（マルチホスト）メッセージ内のホスト情報を送信します。ホスト メッセージ形式については、ホスト データおよびマルチ ホスト データ メッセージの形式（2-31 ページ）を参照してください。

イベント データ メッセージの構成について

eStreamer が送信するイベント データおよびメタデータ メッセージには、次のセクションが含まれています。

- eStreamer メッセージ ヘッダー：eStreamer メッセージ ヘッダー（2-8 ページ）で定義されている標準メッセージ ヘッダー。
- イベント固有のサブヘッダー：追加のイベントの詳細を記述し、後続のペイロード データの構造を決定するコードを含む、イベント タイプによって異なるフィールドのセット。
- データ レコード：固定長フィールドとデータ ブロック。

（注）　クライアントは、フィールド長に基づいてすべてのメッセージを展開する必要があります。

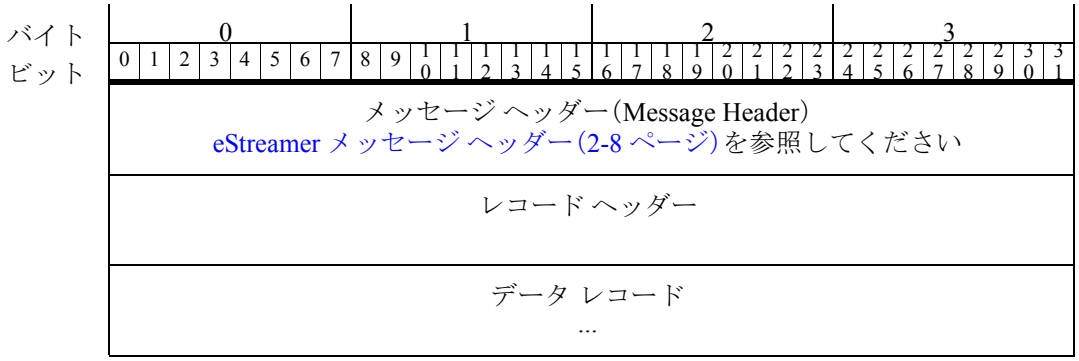
イベント タイプ別のイベント メッセージ形式については、以下を参照してください。

- 侵入イベント データ レコードとすべてのメタデータ レコードについては侵入イベントとメタデータ メッセージの形式（2-19 ページ）。これらのメッセージは固定長フィールドを持ちます。

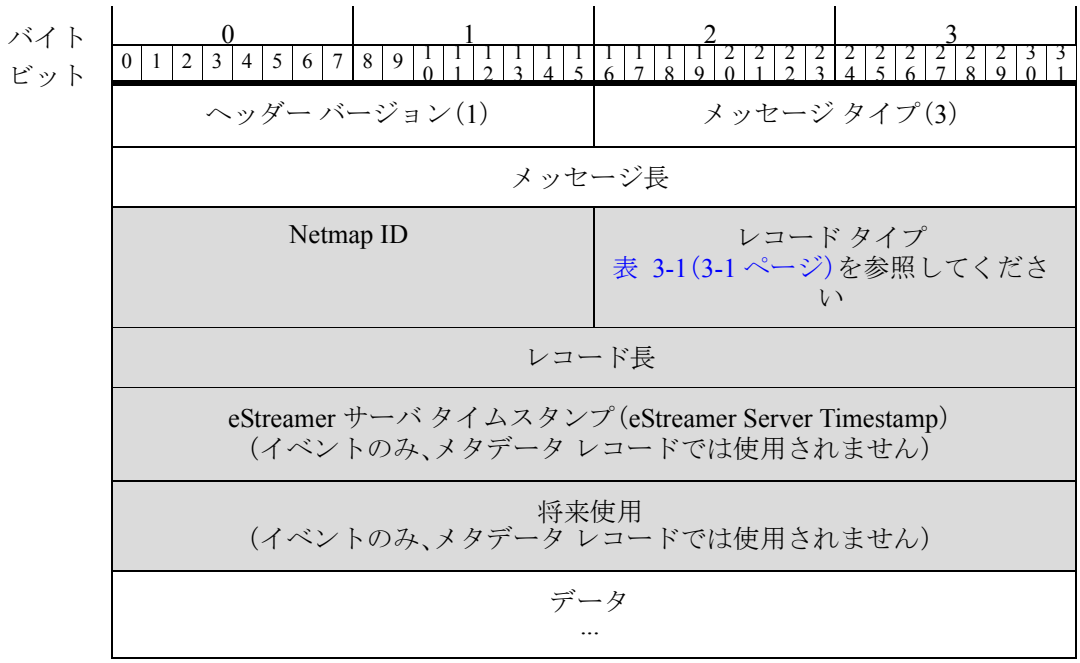
- 検出イベントまたはユーザ イベント データを含むメッセージについては検出イベント メッセージの形式(2-21 ページ)。標準の eStreamer メッセージ ヘッダーおよび侵入イベント メッセージに類似したレコード ヘッダーに加えて、検出メッセージには、イベント タイプとサブタイプ フィールドが含まれた独特の検出イベント ヘッダーがあります。検出イベント メッセージ内のデータ レコードは、可変長フィールドとカプセル化されたブロックの複数の層を持つことができるシリーズ 1 ブロックにパッケージ化されます。
- 接続統計情報を含むメッセージについては接続イベント メッセージの形式(2-23 ページ)。それらの一般的な構造は、検出イベント メッセージと同じです。ただし、データ ブロック タイプは接続統計情報に固有のものです。
- 相関(コンプライアンス)イベント データを含むメッセージについては相関イベント メッセージの形式(2-23 ページ)。これらのメッセージのヘッダーは侵入イベント メッセージと同じですが、データ ブロックはシリーズ 1 ブロックです。
- 可変長フィールドおよび侵入イベントの追加データなどのネストされたデータ ブロックの複数の層を含む侵入関連レコード タイプを配信する一連のメッセージについてはイベント追加データ メッセージの形式(2-25 ページ)。このメッセージ シリーズの構造に関する一般的な情報については、イベント追加データ メッセージの形式(2-25 ページ)を参照してください。シリーズ 1 ブロックに類似しているが、個別に番号が付けられているこのシリーズのブロックの構造に関する情報については、データ ブロック ヘッダー(2-27 ページ)を参照してください。

侵入イベントとメタデータ メッセージの形式

次の図に、侵入イベントおよびメタデータ メッセージの一般的な構造を示します。



次の図に、侵入イベントおよびメタデータ メッセージ形式のレコード ヘッダー部分の詳細を示します。レコード ヘッダー フィールドは網掛けされています。その次にある表では、フィールドを定義しています。



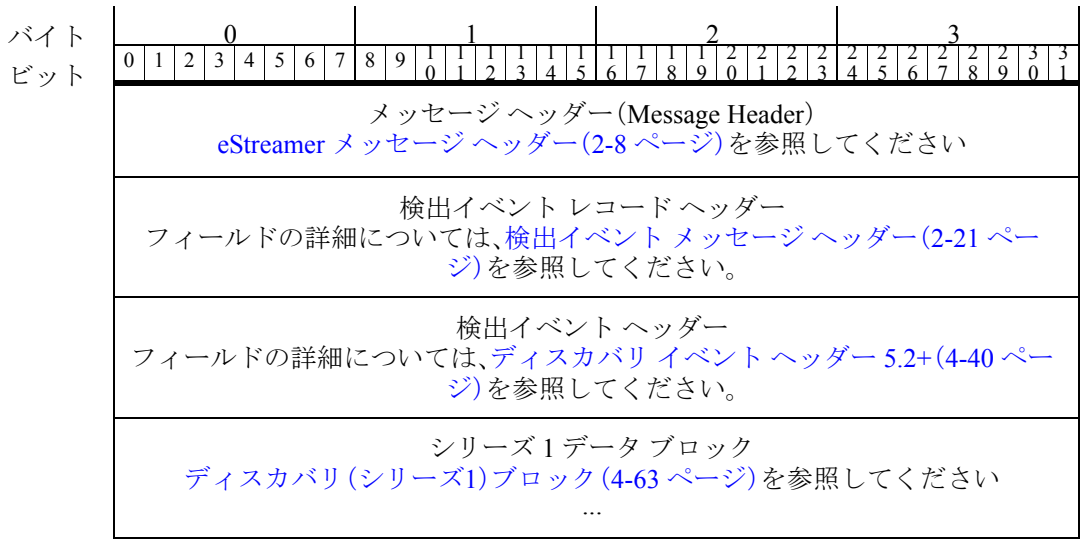
次の表に、侵入イベントおよびメタデータ メッセージのヘッダーの各フィールドについて説明します。

表 2-8　侵入イベントとメタデータ レコード ヘッダー フィールド

フィールド	データ タイプ	説明
Netmap ID	uint16	このフィールドの第 1 ビットは、ヘッダーがアーカイブ タイムスタンプを含む拡張ヘッダーであるかどうかを示すフラグです。残りの 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプションのフィールドです。このフィールドは、使用されていない場合は空のままです。Netmap ID は、メタデータで提供されるドメインにマップされます。
レコード タイプ	uint16	データ レコードのコンテンツ タイプを識別します。レコード タイプのリストについては、表 3-1侵入イベントと一般的なメタデータのレコード タイプ(3-1 ページ)を参照してください。
レコード長	uint32	レコード ヘッダーの後のメッセージのコンテンツの長さ。レコード ヘッダーの 8 または 16 バイトは含まれません。(レコード長 + レコード ヘッダーの長さは、メッセージ長と等しくなります。)
eStreamer サーバ タイムスタンプ(eStreamer Server Timestamp)	uint32	イベントが eStreamer サーバによってアーカイブされたときに適用されるタイムスタンプを示します。アーカイブ タイムスタンプとも呼ばれます。 要求メッセージ フラグにビット 23 が設定されている場合にのみ表示されるフィールド。
将来使用	uint32	今後使用するために予約されています。 要求メッセージ フラグにビット 23 が設定されている場合にのみ表示されるフィールド。

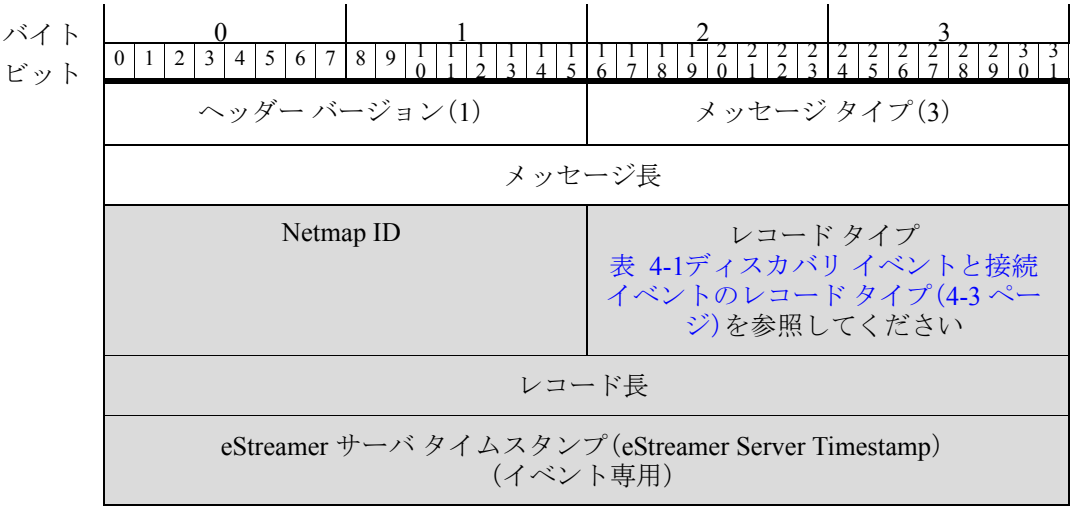
検出イベント メッセージの形式

次の図に、検出イベント メッセージの構造を示します。標準のeStreamer メッセージ ヘッダーとイベント レコード ヘッダーの後には、検出イベント メッセージとユーザ イベント メッセージでのみ使用される検出イベント ヘッダーが続きます。メッセージの検出イベント ヘッダー セクションには、検出イベント タイプおよびサブタイプ フィールドが含まれており、これらのフィールドが一緒になって後続のデータ ブロックへのキーを形成します。現在の検出イベント タイプおよびサブタイプについては、表 4-29タイプ/サブタイプ別のディスカバリ イベントと接続イベント (4-42 ページ)を参照してください。



検出イベント メッセージ ヘッダー

次の図の網掛け部分は、検出イベント データ メッセージ形式のレコード ヘッダーのフィールドを示し、それに続くイベント ヘッダーの位置を示しています。次の表では、検出イベント メッセージ ヘッダーのフィールドを定義しています。



将来使用 （イベント専用）
検出イベント ヘッダー 表 4-28ディスカバリ イベント ヘッダーのフィールド (4-41 ページ) を参照してください
シリーズ 1 データ ブロック ディスカバリ (シリーズ1) ブロック (4-63 ページ) を参照してください ...

次の表では、検出イベント メッセージのレコード ヘッダーとイベント ヘッダーのフィールドについて説明します。

表 2-9　検出イベント メッセージ ヘッダーのフィールド

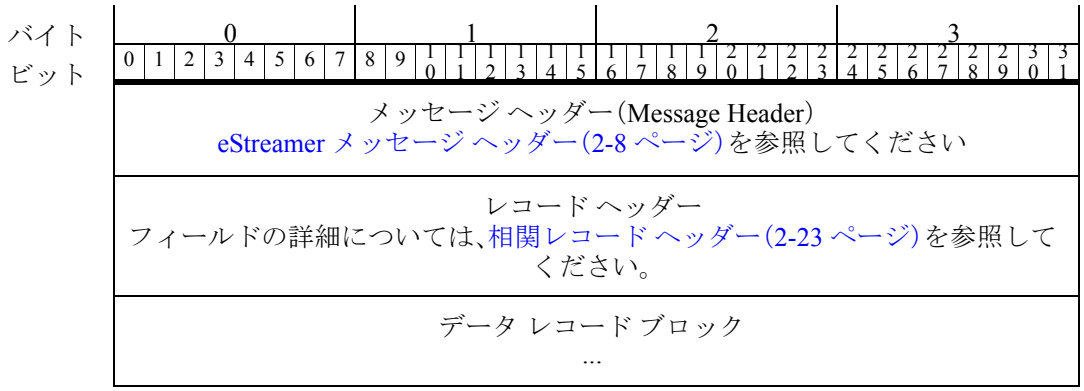
フィールド	データ タイプ	説明
Netmap ID	uint16	このフィールドの第 1 ビットは、ヘッダーがアーカイブ タイムスタンプを含む拡張ヘッダーであるかどうかを示すフラグです。残りの 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプションのフィールドです。このフィールドは、使用されていない場合は空のままです。Netmap ID は、メタデータで提供されるドメインにマップされます。
レコード タイプ	uint16	データ レコードのコンテンツ タイプを識別します。レコード タイプのリストについては、表 4-1ディスカバリ イベントと接続イベントのレコード タイプ (4-3 ページ) を参照してください。
レコード長	uint32	レコード ヘッダーの後のメッセージのコンテンツの長さ。レコード ヘッダーの 8 または 16 バイトは含まれません。（レコード長 + レコード ヘッダーの長さは、メッセージ長と等しくなります。）
eStreamer サーバ タイムスタンプ（eStreamer Server Timestamp）	uint32	イベントが eStreamer サーバによってアーカイブされたときに適用されるタイムスタンプを示します。アーカイブ タイムスタンプとも呼ばれます。イベント ストリーム要求の要求フラグ フィールドにビット 23 が設定されている場合にのみ存在するフィールド。
将来使用	uint32	今後使用するために予約されています。要求メッセージ フラグにビット 23 が設定されている場合にのみ表示されるフィールド。
検出イベント ヘッダー	さまざま	イベント タイプとサブタイプを含む複数のフィールドが含まれており、これらが一緒になって後続のデータ構造への固有キーを形成します。検出イベント ヘッダーのフィールドの定義については、ディスカバリ イベント ヘッダー 5.2+ (4-40 ページ) を参照してください。

接続イベント メッセージの形式

接続統計情報を含むメッセージの構造は、検出イベント メッセージと同じです。一般的なメッセージ形式の情報については、検出イベント メッセージの形式（2-21 ページ）を参照してください。接続イベント メッセージは、それらが組み込むデータ ブロック タイプの点で区別されます。

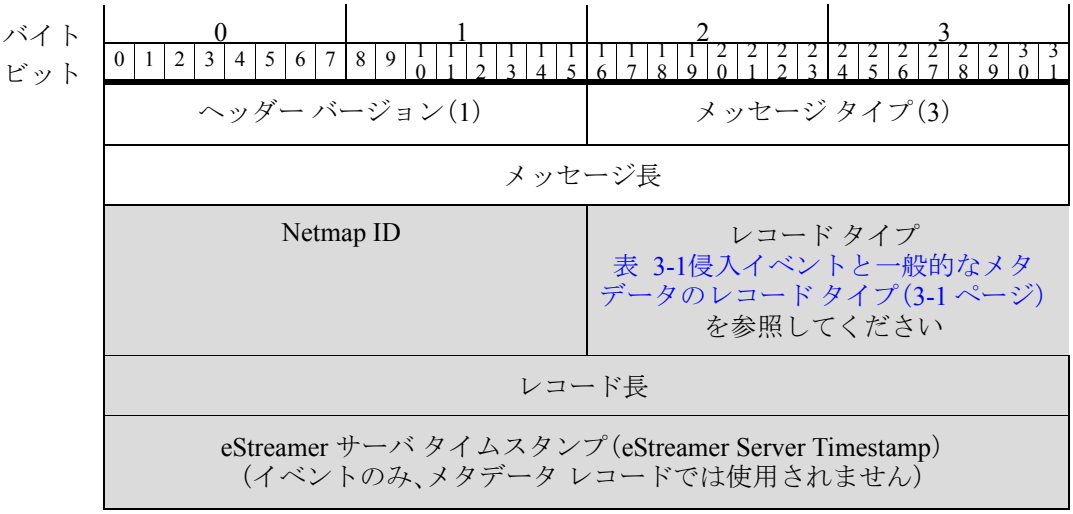
相関イベント メッセージの形式

次の図に、相関（コンプライアンス）イベント メッセージの一般的な構造を示します。標準の eStreamer メッセージ ヘッダーとレコード ヘッダーの直後には、メッセージのデータ レコード セクションのデータ ブロックが続きます。相関メッセージは、シリーズ 1 データ ブロックを使用します。



相関レコード ヘッダー

次の図の網掛け部分は、相関イベント メッセージのレコード ヘッダーのフィールドを示しています。相関メッセージはシリーズ 1 データ ブロックを使用することに注意してください。ただし、検出イベント メッセージに表示される検出ヘッダーは含まれていません。それらのヘッダー フィールドは、侵入イベント メッセージのヘッダー フィールドに似ています。次の図に続く表では、相関イベントのレコード ヘッダー フィールドを定義しています。



将来使用 （イベントのみ、メタデータ レコードでは使用されません）
データ レコード ブロック シリーズ 1 ブロックを使用します（ディスカバリ（シリーズ1）ブロック（4-63 ページ）を参照）。 ...

次の表では、相関イベント メッセージのレコード ヘッダーの各フィールドについて説明します。

表 2-10　相関イベント メッセージ レコード ヘッダーのフィールド

フィールド	データ タイプ	説明
Netmap ID	uint16	このフィールドの第 1 ビットは、ヘッダーがアーカイブ タイムスタンプを含む拡張ヘッダーであるかどうかを示すフラグです。残りの 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプションのフィールドです。このフィールドは、使用されていない場合は空のままです。Netmap ID は、メタデータで提供されるドメインにマップされます。
レコード タイプ	uint16	データ レコードのコンテンツ タイプを識別します。侵入、相関、およびメタデータのレコード タイプのリストについては、表 3-1（3-1 ページ）を参照してください。
レコード長	uint32	レコード ヘッダーの後のメッセージのコンテンツの長さ。レコード ヘッダーの 8 または 16 バイトは含まれません。（レコード長 + レコード ヘッダーの長さは、メッセージ長と等しくなります。）
eStreamer サーバ タイムスタンプ（eStreamer Server Timestamp）	uint32	イベントが eStreamer サーバによってアーカイブされたときに適用されるタイムスタンプを示します。アーカイブ タイムスタンプとも呼ばれます。 要求メッセージ フラグにビット 23 が設定されている場合にのみ表示されるフィールド。 ホスト プロファイルやメタデータなど、Management Center によって生成されたデータの場合フィールドはゼロです。
将来使用	uint32	今後使用するために予約されています。 要求メッセージ フラグにビット 23 が設定されている場合にのみ表示されるフィールド。

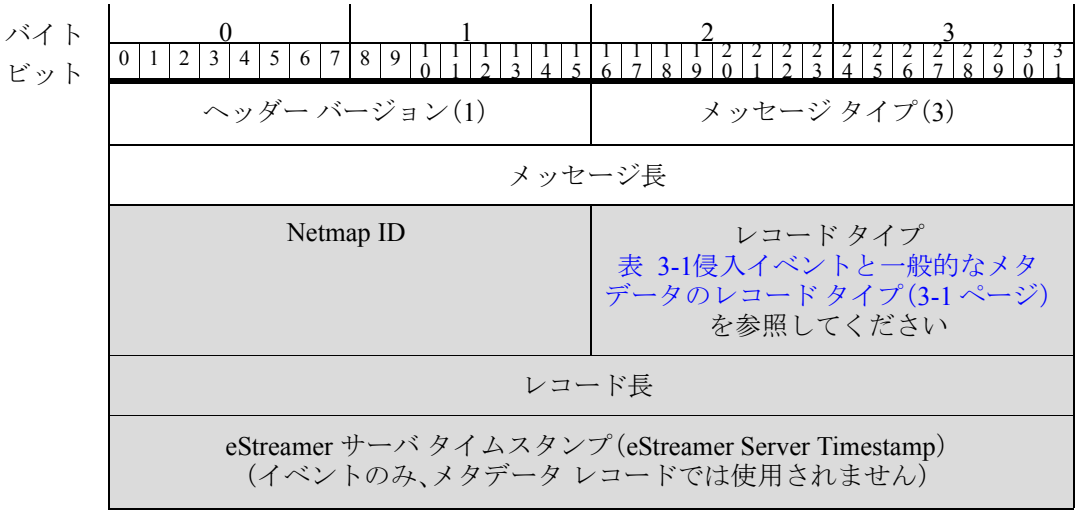
イベント追加データ メッセージの形式

次の図に、イベント追加データ メッセージの構造を示します。侵入イベント追加データ メッセージは、このメッセージ グループの例です。

イベント追加データ メッセージは、相関イベント メッセージと同じ形式で、レコード ヘッダーの直後にデータ ブロックがあります。相関メッセージとは異なり、シリーズ 1 データ ブロックではなくシリーズ 2 データ ブロックが使用され、個別のナンバリング シーケンスがあります。シリーズ 2 ブロックのタイプについては、シリーズ 2 のデータ ブロックの概要（3-57 ページ）を参照してください。

イベント追加データ メッセージのレコード ヘッダー

次の図の網掛け部分は、イベント追加データ メッセージのレコード ヘッダーのフィールドを示しています。その次にある表では、イベント追加データ メッセージのレコード ヘッダー フィールドを定義しています。



将来使用 （イベントのみ、メタデータ レコードでは使用されません）
データ レコード ブロック（Data Record Block） シリーズ 2 ブロックを使用します（シリーズ 2 のデータ ブロックの概要（3-57 ページ）を参照）。 ...

次の表では、イベント追加データ メッセージのレコード ヘッダーの各フィールドについて説明します。

表 2-11　イベント追加データ メッセージのレコード ヘッダー フィールド

フィールド	データ タイプ	説明
Netmap ID	uint16	このフィールドの第 1 ビットは、ヘッダーがアーカイブ タイムスタンプを含む拡張ヘッダーであるかどうかを示すフラグです。残りの 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプションのフィールドです。このフィールドは、使用されていない場合は空のままです。Netmap ID は、メタデータで提供されるドメインにマップされます。
レコード タイプ	uint16	データ レコードのコンテンツ タイプを識別します。イベント追加データ レコード タイプのリストについては、表 3-1侵入イベントと一般的なメタデータのレコード タイプ（3-1 ページ）を参照してください。
レコード長	uint32	レコード ヘッダーの後のメッセージのコンテンツの長さ。レコード ヘッダーの 8 または 16 バイトは含まれません。（レコード長 + レコード ヘッダーの長さは、メッセージ長と等しくなります。）
eStreamer サーバ タイムスタンプ（eStreamer Server Timestamp）	uint32	イベントが eStreamer サーバによってアーカイブされたときに適用されるタイムスタンプを示します。アーカイブ タイムスタンプとも呼ばれます。 要求メッセージ フラグにビット 23 が設定されている場合にのみ表示されるフィールド。Management Center によって生成されたイベントの場合は、フィールドが存在しません。
将来使用	uint32	今後使用するために予約されています。 要求メッセージ フラグにビット 23 が設定されている場合にのみ表示されるフィールド。Management Center によって生成されたイベントの場合は、フィールドが存在しません。

データ ブロック ヘッダー

シリーズ 1 ブロックとシリーズ 2 ブロックは、構造は類似していますが、ナンバリングが異なります。これらのブロックは、検出、相関、接続、またはイベント追加データ メッセージのデータ部分のどこにでも置くことができます。これらのブロックは、複数のネスティング レベルで他のブロックをカプセル化します。

第 1 シリーズと第 2 シリーズの両方のデータ ブロックは、次の図に示すヘッダー構造で始まります。次の表に、ヘッダー フィールドに関する情報を示します。ヘッダーの直後には、データ ブロック タイプに関連付けられたデータ構造が続きます。

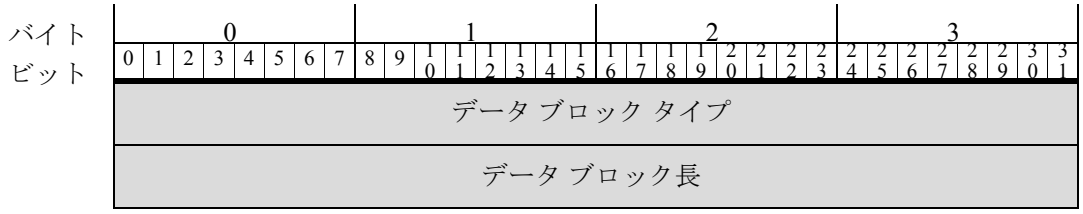


表 2-12

フィールド	データ タイプ	説明
データ ブロック タイプ	uint32	シリーズ 1 ブロックのタイプについては、ディスカバリ（シリーズ1）ブロック (4-63 ページ) を参照してください。 シリーズ 2 ブロックのタイプについては、表 3-26シリーズ 2 のブロック タイプ (3-57 ページ) を参照してください。
データ ブロック長	uint32	データ ブロックの長さ。2 つのデータ ブロック ヘッダー フィールドに 8 バイトを加えたデータのバイト数が含まれます。

ホスト要求メッセージの形式

ホスト プロファイルを受信するには、ホスト要求メッセージを送信します。IP アドレス範囲で定義された単一のホストまたは複数のホストのデータを要求できます。

イベント ストリーム要求メッセージを送信することによって、ホスト プロファイル情報の要求を含むすべてのデータ要求で最初にセッションを初期化することが必須であることに注意してください。ホスト データをストリーミングするだけのために設定するには、最初のイベント ストリーム要求メッセージで次のいずれかの要求フラグ設定を使用できます。

- 適切なバージョンのメタデータのビットを設定する（これは、ホスト データをストリーミングする場合に有益です）
- 要求フラグを設定しない
- ビット 11 を設定する（eStreamer のレガシー バージョンを使用する場合は、デフォルトのイベント ストリーミングを抑制するため）

最初のメッセージの後、ホスト要求メッセージ（タイプ 5）を使用してホストを指定します。

（注） デフォルトのイベント ストリーミングを使用するレガシー eStreamer バージョンの場合、ホスト プロファイル データのみをストリーミングする場合は、デフォルトのイベント メッセージを抑制する必要があります。最初に、要求フラグ フィールドのビット 11 を 1 に設定したイベント ストリーム要求メッセージをサーバに送信します。その後、ホスト要求メッセージを送信します。

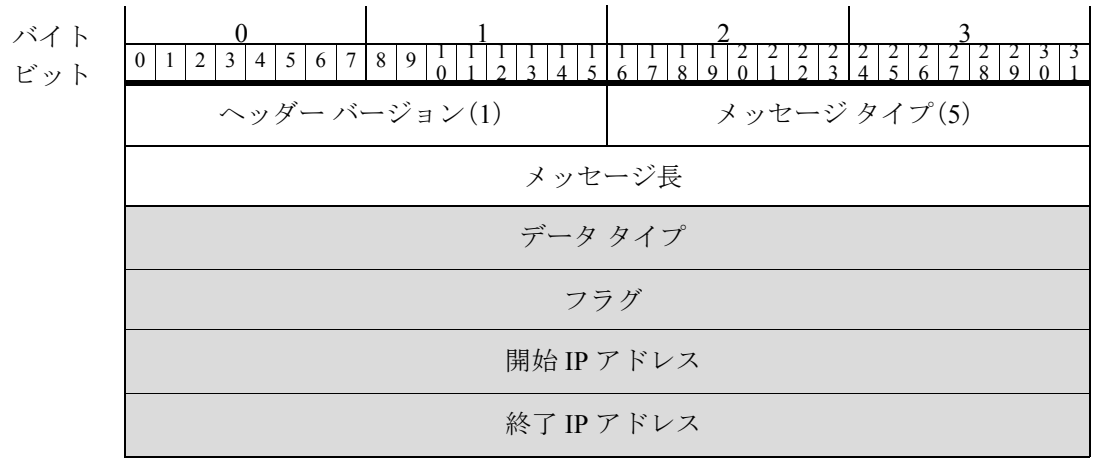
次の図に、ホスト要求メッセージの形式を示します。網掛けのフィールドはホスト要求メッセージの形式に固有であり、次の表で定義されています。上記の 3 つのフィールドは、標準のメッセージ ヘッダーです。

次の表では、メッセージ フィールドについて説明します。

表 2-13　ホスト要求メッセージ フィールド

フィールド	データ タイプ	説明
データ タイプ	uint32	次のコードを使用して、単一のホストまたは複数のホストのデータを要求します。 • 0：単一ホストのバージョン 3.5 ～ 4.6。 • 1：複数のホストのバージョン 3.5 ～ 4.6（ブロック 34 を使用）。 • 2：単一ホストのバージョン 4.7 ～ 4.8（ブロック 47 を使用）。 • 3：複数のホストのバージョン 4.7 ～ 4.8（ブロック 47 を使用）。 • 4：単一ホストのバージョン 4.9 ～ 4.10（ブロック 92 を使用）。 • 5：複数のホストのバージョン 4.9 ～ 4.10（ブロック 92 を使用）。 • 6：単一ホストのバージョン 5.0+ データ（ブロック 111 を使用、全ホスト プロファイル データ ブロック 5.3+（5-1 ページ）を参照）。 • 7：複数のホストのバージョン 5.0+ データ（ブロック 111 を使用、全ホスト プロファイル データ ブロック 5.3+（5-1 ページ）を参照）。
フラグ	32 ビット フィールド	• 0x00000001：ホスト プロファイルの [注（Notes）] フィールドが（Firepower システム に格納されているホストに関するユーザ定義の情報を使用して）読み込まれます。 • 0x00000002：サービス ブロックの [バナー（Banner）] フィールドが（サービスについて検出された最初のパケットの最初の 256 バイトを使用して）読み込まれます。バナーはデフォルトでは無効になっており、設定されている場合にのみ使用できます。
開始 IP アドレス	uint8[16]	データを返す必要があるホストの IP アドレス（要求が単一ホストに対する場合）、または IP アドレス範囲の開始アドレス（要求が複数のホストに対する場合）。IPv4 または IPv6 アドレスにできます。
終了 IP アドレス	uint8[16]	IP アドレス範囲の終了アドレス（要求が複数のホストに対する場合）、または開始 IP アドレスの値（要求が単一ホストに対する場合）。IPv4 または IPv6 アドレスにできます。

次の図に、レガシーのホスト要求メッセージの形式を示します。eStreamer は引き続きこの要求に応答します。現在の要求との唯一の違いは、IPv4 アドレス フィールドが小さいという点です。網掛けのフィールドはホスト要求メッセージの形式に固有であり、次の表で定義されています。上記の 3 つのフィールドは、標準のメッセージ ヘッダーです。



次の表では、メッセージ フィールドについて説明します。

表 2-14　ホスト要求メッセージ フィールド

フィールド	データ タイプ	説明
データ タイプ	uint32	次のコードを使用して、単一のホストまたは複数のホストのデータを要求します。 • 0:単一ホストのバージョン 3.5 ～ 4.6。 • 1:複数のホストのバージョン 3.5 ～ 4.6(ブロック 34 を使用)。 • 2:単一ホストのバージョン 4.7 ～ 4.8(ブロック 47 を使用)。 • 3:複数のホストのバージョン 4.7 ～ 4.8(ブロック 47 を使用)。 • 4:単一ホストのバージョン 4.9 ～ 4.10(ブロック 92 を使用)。 • 5:複数のホストのバージョン 4.9 ～ 4.10(ブロック 92 を使用)。 • 6:単一ホストのバージョン 5.0+ データ(ブロック 111 を使用、全ホスト プロファイル データ ブロック 5.3+(5-1 ページ)を参照)。 • 7:複数のホストのバージョン 5.0+ データ(ブロック 111 を使用、全ホスト プロファイル データ ブロック 5.3+(5-1 ページ)を参照)。
フラグ	32 ビット フィールド	• 0x00000001:ホスト プロファイルの [注(Notes)] フィールドが(Firepower システム に格納されているホストに関するユーザ定義の情報を使用して)読み込まれます。 • 0x00000002:サービス ブロックの [バナー(Banner)] フィールドが(サービスについて検出された最初のパケットの最初の 256 バイトを使用して)読み込まれます。バナーはデフォルトでは無効になっており、設定されている場合にのみ使用できます。

表 2-14　ホスト要求メッセージ フィールド(続き)

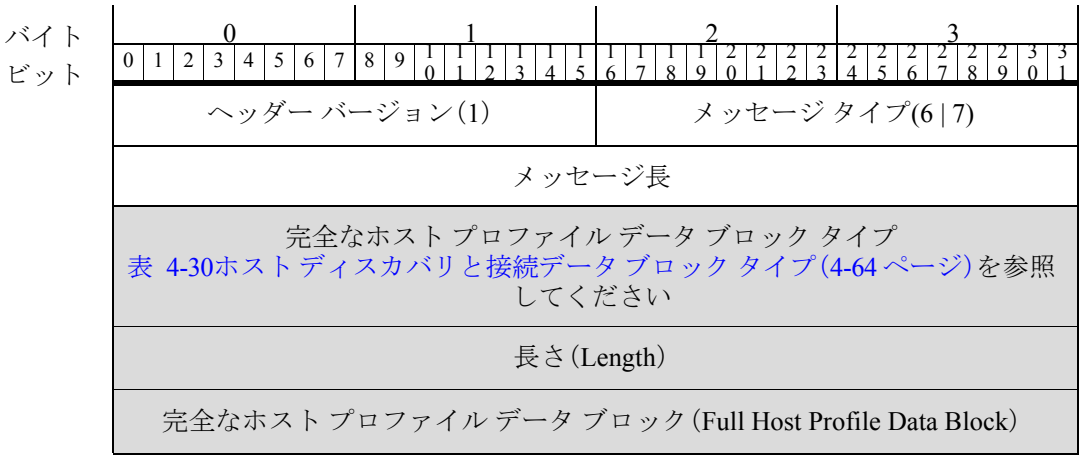
フィールド	データ タイプ	説明
開始 IP アドレス	uint8[4]	データを返す必要があるホストの IP アドレス(要求が単一ホストに対する場合)、または IP アドレス範囲の開始アドレス(要求が複数のホストに対する場合)。IP アドレス オクテットでアドレスを指定します。
終了 IP アドレス	uint8[4]	IP アドレス範囲の終了アドレス(要求が複数のホストに対する場合)、または開始 IP アドレスの値(要求が単一ホストに対する場合)。

ホスト データおよびマルチ ホスト データ メッセージの形式

eStreamer は、完全なホスト プロファイル データ ブロックをそれぞれ含む、ホスト データ メッセージを送信することによって、ホスト要求に応答します。eStreamer は、要求で指定された各ホストに対し 1 つのホスト データ メッセージを送信します。eStreamer は、タイプ 6 のメッセージを使用して単一のホスト プロファイルの要求に応答し、タイプ 7 のメッセージを使用して複数のホストの要求に応答します。タイプ 6 およびタイプ 7 のメッセージの形式は同一であり、メッセージ タイプのみが異なります。

ホスト データ メッセージには、レコード タイプ フィールドはありません。メッセージの構造は、メッセージ タイプと、メッセージに含まれる完全なホスト プロファイルのデータ ブロック タイプによって伝達されます。完全なホスト プロファイル データ ブロックは、一連のブロックのグループです。

次の図はホスト データ メッセージの形式を示しており、その次の表では網掛けフィールドを定義しています。



ホスト要求メッセージに固有のフィールドは次のとおりです。

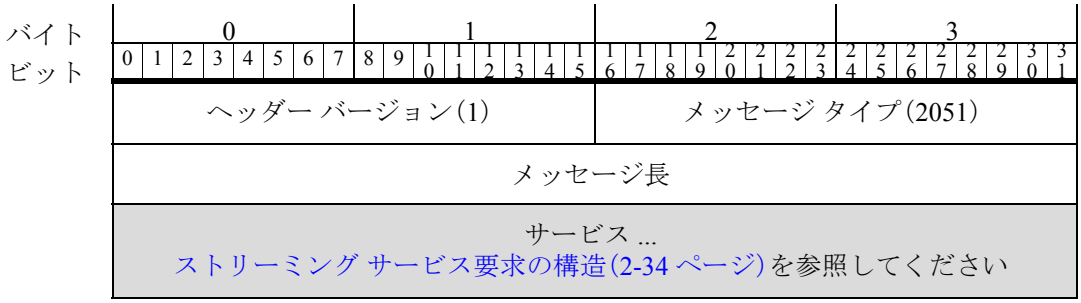
表 2-15

フィールド	データ タイプ	説明
完全なホスト プロファイル データ ブロック タイプ	uint32	メッセージに含まれる完全なホスト プロファイル データのブロック タイプを指定します。表 4-30ホスト ディスカバリと接続データ ブロック タイプ(4-64 ページ)を参照してください。
長さ(Length)	uint32	メッセージ内の完全なホスト プロファイル データの長さ。
完全なホスト プロファイル データ ブロック(Full Host Profile Data Block)	変数	ホストのデータ。現在の完全なホスト プロファイル データ ブロックの定義へのリンクについては、表 4-30ホスト ディスカバリと接続データ ブロック タイプ(4-64 ページ)を参照してください。

ストリーミング情報メッセージの形式

eStreamer サービスは、拡張要求の要求を受信すると、以下に説明するストリーミング情報メッセージをクライアントに送信します。このメッセージは、サーバの使用可能なサービスのリストをアドバタイズします。現在、関連する唯一のオプションは eStreamer サービス(6667)ですが、メッセージには他のサービスがリストされる場合があり、それらは無視する必要があります。アドバタイズされた各サービスは、ストリーミング サービス要求の構造(2-34 ページ)で説明するストリーミング サービス要求構造によって表されます。

次の図に、ストリーミング情報メッセージの形式を示します。網掛けのフィールドは、このメッセージ タイプに固有のものです。上記の 3 つのフィールドは、標準のメッセージ ヘッダーです。



ストリーミング情報メッセージのフィールドは次のとおりです。

表 2-16　ストリーミング情報メッセージのフィールド

フィールド	データ タイプ	説明
ヘッダー バージョン	uint16	1 に設定します。
Message Type	uint16	eStreamer メッセージ タイプ。ストリーミング要求メッセージの場合は 2051 に設定します。

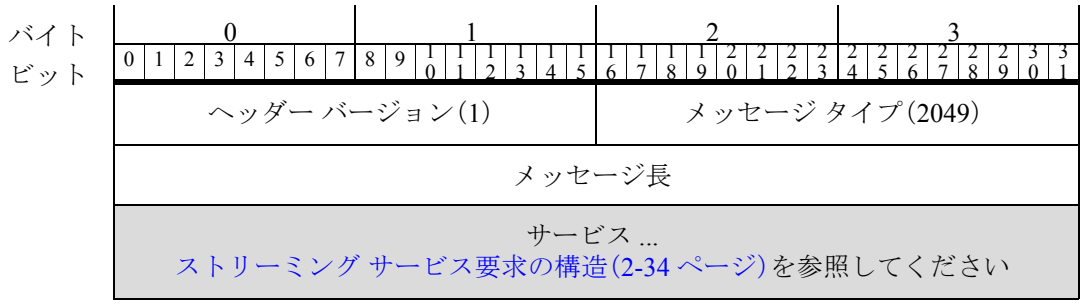
表 2-16　ストリーミング情報メッセージのフィールド(続き)

フィールド	データ タイプ	説明
メッセージ長	uint32	メッセージ ヘッダーの後のメッセージのコンテンツの長さ。[ヘッダー バージョン(Header Version)]、[メッセージ タイプ(Message Type)]、および [メッセージ長(Message Length)] フィールドのバイトは含まれません。
サービス [] (Service[])	アレイ	使用できるサービスのリスト。ストリーミング サービス要求の構造(2-34 ページ)を参照してください。

ストリーミング要求メッセージの形式

クライアントは、ストリーミング要求メッセージを使用して、使用するストリーミング情報メッセージで eStreamer サービスに指定し、その後にストリーミングされるイベント タイプおよびバージョンの要求のセットを指定します。次の図はメッセージの構造を示し、次の表ではフィールドを定義しています。要求されたサービスは、ストリーミング サービス要求の構造(2-34 ページ)で説明するストリーミング サービス要求構造によって表されます。

次の図に、ストリーミング情報メッセージの形式を示します。網掛けのフィールドは、このメッセージ タイプに固有のものです。上記の 3 つのフィールドは、標準のメッセージ ヘッダーです。



ストリーミング要求メッセージのフィールドは次のとおりです。

表 2-17　ストリーミング要求メッセージのフィールド

フィールド	データ タイプ	説明
ヘッダー バージョン	uint16	1 に設定します。
Message Type	uint16	eStreamer メッセージ タイプ。ストリーミング要求メッセージの場合は 2049 に設定します。

表 2-17　ストリーミング要求メッセージのフィールド(続き)

フィールド	データ タイプ	説明
メッセージ長	uint32	メッセージ ヘッダーの後のメッセージのコンテンツの長さ。[ヘッダー バージョン(Header Version)]、[メッセージ タイプ(Message Type)]、および [メッセージ長(Message Length)] フィールドのバイトは含まれません。
サービス [] (Service[])	アレイ	要求されたサービス構造のリスト。ストリーミング サービス要求の構造(2-34 ページ)を参照してください。

ストリーミング サービス要求の構造

eStreamer サービスは、アドバタイズする各サービスについて、ストリーミング情報メッセージで 1 つのストリーミング サービス要求のデータ構造を送信します。eStreamer サービスは、ストリーミング サービス要求の最後のフィールドを使用しません。このフィールドは、含まれる予定のイベント タイプのリストを規定します。

クライアントは、eStreamer からのストリーミング サービス要求構造を処理し、サーバに返す応答で同じ構造を使用します。クライアントがサーバに送信するストリーミング サービス要求には、最初に、eStreamer によってアドバタイズされるサービスに対する要求が含まれ、2 番目に、クライアントが受信する要求されたイベント タイプを指定するストリーミング イベント タイプ構造のリストが含まれます。

各ストリーミング イベント タイプ構造には、要求された各イベント タイプのイベント タイプとバージョンを指定する 2 つのフィールドが含まれています。ストリーミング イベント タイプの構造については、ドメイン ストリーミング要求メッセージの形式(2-36 ページ)を参照してください。

次の図に、ストリーミング サービス要求構造のフィールドを示します。その次にある表では、フィールドを定義しています。

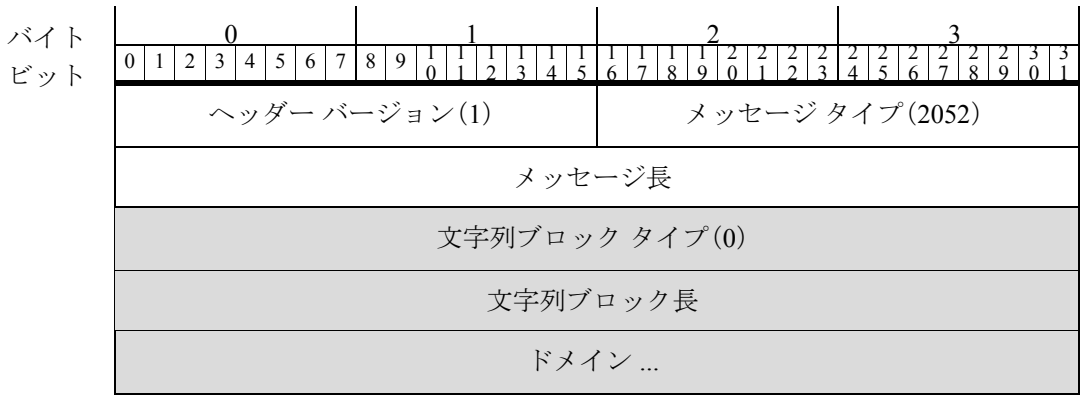
ストリーミング サービス要求構造のフィールドは次のとおりです。

表 2-18　ストリーミング サービス要求フィールド

フィールド	データ タイプ	説明
タイプ	uint32	[サービス ID（Service ID）]。 eStreamer サーバ メッセージでは、これによって利用可能なサービスがアドバタイズされます。 クライアント メッセージでは、要求されたサービスが指定されます。 現在の有効なオプション: • 6667（eStreamer サービスの場合）
長さ（Length）	uint32	サービス要求の長さ。タイプと長さを含むサービス要求の長さを表します。 長さには、メッセージ内のすべてのストリーミング イベント タイプのレコードと、終端レコードを含める必要があることに注意してください。
フラグ	uint32	eStreamer のストリーミング情報メッセージ: 常に 0。 クライアントのストリーミング要求メッセージ: 元のイベント ストリーム要求メッセージのフラグ設定を複製します。
最初のタイムスタンプ	uint32	eStreamer のストリーミング情報メッセージ: 常に 0。 クライアントのストリーミング要求メッセージ: 元のイベント ストリーム要求メッセージのタイムスタンプを複製します。
ストリーミング イベント タイプ	アレイ	eStreamer のストリーミング情報メッセージ: • 今後使用するために予約されています。0 の長さが含まれています。 クライアントのストリーミング要求メッセージ: • 各要求されたイベント タイプの 1 つのストリーミング イベント タイプ エントリ。ドメイン ストリーミング要求メッセージの形式（2-36 ページ）を参照してください。 • [イベント タイプ（Event Type）] と [バージョン] を両方とも 0 に設定して、0 のイベント タイプ エントリを含む要求リストを終了します。 ドメイン ストリーミング要求メッセージの形式（2-36 ページ）を参照してください。

ドメイン ストリーミング要求メッセージの形式

クライアントは、ドメイン ストリーミング要求メッセージを使用して、eStreamer の特定のドメインからのイベントを要求します。次の図はメッセージの構造を示し、次の表ではフィールドを定義しています。網掛けのフィールドは、このメッセージ タイプに固有のものです。上記の 3 つのフィールドは、標準のメッセージ ヘッダーです。



ドメイン ストリーミング要求メッセージのフィールドは次のとおりです。

表 2-19　ドメイン ストリーミング要求メッセージのフィールド

フィールド	データ タイプ	説明
ヘッダー バージョン	uint16	1 に設定します。
Message Type	uint16	eStreamer メッセージ タイプ。ドメイン ストリーミング要求メッセージの場合は 2052 に設定します。
メッセージ長	uint32	メッセージ ヘッダーの後のメッセージのコンテンツの長さ。[ヘッダー バージョン(Header Version)]、[メッセージ タイプ(Message Type)]、および [メッセージ長(Message Length)] フィールドのバイトは含まれません。
文字列ブロック タイプ	uint32	ドメインを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ドメイン文字列データ ブロックに含まれるバイト数。ブロック タイプおよびヘッダー フィールドの 8 バイトにドメイン内のバイト数を加えたものです。
ドメイン	string	ストリーミング イベントの要求元のドメイン。空白のままにすると、サービスはクライアントがアクセスするすべてのドメインのイベントをストリーミングします。

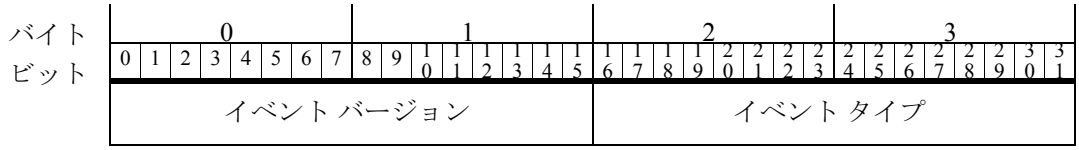
ストリーミング イベント タイプの構造

eStreamer クライアントは、ストリーミング イベント タイプ構造を使用して、イベントのバージョンとバージョンを指定します。各イベント バージョンとタイプの組み合わせは、イベント ストリームの要求です。

ストリーミング イベント タイプ構造のリストは、すべてのフィールドがゼロに設定された構造で終了する必要があります。具体的な場所は次のとおりです。

イベント バージョン = 0
イベント タイプ = 0

次の図に、ストリーミング イベント タイプ構造の形式を示します。



ストリーミング イベント タイプ構造のフィールドは次のとおりです。

表 2-20　ストリーミング イベント タイプのフィールド

フィールド	データ タイプ	説明
イベント バージョン	uint16	イベント タイプのバージョン番号。各イベント タイプでサポートされているバージョンのリストについては、表 2-21拡張要求のイベント タイプとバージョン (2-38 ページ) を参照してください。
イベント タイプ	uint16	要求されたイベント タイプのコード。有効なイベント タイプとバージョン コードの現在のリストについては、表 2-21拡張要求のイベント タイプとバージョン (2-38 ページ) を参照してください。 イベント タイプのリストは、ゼロのイベント タイプとゼロのイベント バージョンで終了する必要があります。

次の表に、クライアントが拡張要求で指定できるイベントのタイプとバージョンを示します。表には、各イベント タイプのバージョンに対応するManagement Center のソフトウェア バージョンが示されています。たとえば、バージョン 4.8.0.2 ～ 4.9.1 でManagement Center によってサポートされていた相関イベントを要求するには、イベント タイプ 31、バージョン 5 を要求する必要があります。イベントが異なるイベント タイプで記録されていた場合は、要求されたイベント タイプの形式に一致するようにアップグレードまたはダウングレードされます。

表 2-21　拡張要求のイベント タイプとバージョン

要求内容	使用するイベント バージョン番号	使用するイベント コード
侵入イベント	1:4.8.x 以前 2:4.9 ～ 4.10.x 3:5.0 ～ 5.1 4:5.1.1.x 5:5.2.x 6:5.3 7:5.3.1 8:5.4.x 9:6.0+	12
メタデータ	1:3.2 ～ 4.5.x 2:4.6.0.x 3:4.6.1 ～ 4.6.x 4:4.7+	21
相関およびコンプライアンスのホワイト リスト イベント	1:3.2 以前 2:4.0 ～ 4.4.x 3:4.5 ～ 4.6.1 4:4.7 ～ 4.8.0.1 5:4.8.0.2 ～ 4.9.1.x 6:4.10.0 ～ 4.10.x 7:5.0 ～ 5.0.2 8:5.1 ～ 5.3.x 9:5.4+	31
検出イベント	1:3.2 以前 2:3.0 ～ 3.4.x 3:3.5 ～ 4.6.x 4:4.7 ～ 4.8.x 5:4.9.0.x 6:4.9.1 ～ 4.9.x.x 7:4.10.0 ～ 4.10.x 8:5.0.x 9:5.1.x 10:5.2 ～ 5.3 11:5.3.1+	61

表 2-21　拡張要求のイベント タイプとバージョン(続き)

要求内容	使用するイベント バージョン番号	使用するイベント コード
接続イベント	1:4.0 ～ 4.1 3:4.5 ～ 4.6.1 4:4.7 ～ 4.9.0.x 5:4.9.1 ～ 4.10.x 6:5.0.x 7:5.1.0.x 8:5.1.1.x 9:5.2.x 10:5.3 11:5.3.1 12:5.4 13:5.4.0.1 ～ 5.4.0.2 14:6.0.x 15:6.1+	71
ユーザ イベント	1:4.7 ～ 4.10.x 2:5.0.x 3:5.1 ～ 5.1.x 4:5.2+	91
マルウェア イベント	1:5.1.0.x 2:5.1.1.x 3:5.2.x 4:5.3 5:5.3.1 6:5.4.x 7:6.0+	101
ファイル イベント	1:5.1.1 ～ 5.1.x 2:5.2.x 3:5.3 4:5.3.1 5:5.4.x 6:6.0+	111
影響相関イベント	1:5.2.x 以前 2:5.3+	131
リスト内の終了イベント タイプ	0	0

拡張要求メッセージの例

ストリーミング情報メッセージ

次の例では、サーバは 2 つのサービス、第 1 のタイプ 6667（eStreamer）と第 2 のタイプ 5000 をアドバタイズします。サーバからのストリーミング情報メッセージでは、[フラグ（flags）] フィールドと [最初のタイムスタンプ（initial timestamp）] フィールドはゼロであり、メッセージではイベント タイプは指定されていません。

表 2-22

ヘッダー バージョン:	1	/*always 1*/
メッセージ タイプ:	2051	/*streaming info msg*/
メッセージ長	32	/*bytes of msg content*/
サービス [1]. タイプ	6667	/*eStreamer service ID*/
サービス [1]. 長さ	8	
サービス [1]. フラグ	0	/*no flags from server*/
サービス [1]. 最初のタイムスタンプ	0	/*always 0*/
サービス [2]. タイプ	5000	/*service-2 ID*/
サービス [2]. 長さ	8	
サービス [2]. フラグ	0	/*no flags from server*/
サービス [2]. 最初のタイムスタンプ	0	/*always 0*/
ヘッダー バージョン:	1	/*always 1*/
メッセージ タイプ:	2051	/*streaming info msg*/

ストリーミング要求メッセージ

以下は、クライアントがサービス タイプ 6667（eStreamer）を要求し、接続イベントのバージョン 6（イベント タイプ 71）とメタデータのバージョン 4（イベント タイプ 21）の 2 つのイベント タイプを指定するストリーミング要求メッセージです。

表 2-23

ヘッダー バージョン:	1	/*always 1*/
メッセージ タイプ:	2049	/*stream request msg*/
メッセージ長	36	/*payload bytes*/
サービス [1]. タイプ	6667	/*eStreamer service ID*/
サービス [1]. 長さ	20	
サービス [1]. フラグ	30	/*original flags value*/
サービス [1]. 最初のタイムスタンプ	0	/*original timestamp*/

表 2-23

サービス [1]. イベント [1]. バージョン	6	/*version 6*/
サービス [1]. イベント [1]. タイプ	71	/*connection events*/
サービス [1]. イベント [2]. バージョン	4	/* version 4*/
サービス [1]. イベント [2]. タイプ	21	/*metadata*/
サービス [1]. イベント [3]. バージョン	0	/*terminate event list*/
サービス [1]. イベント [3]. タイプ	0	/*terminate event list*/

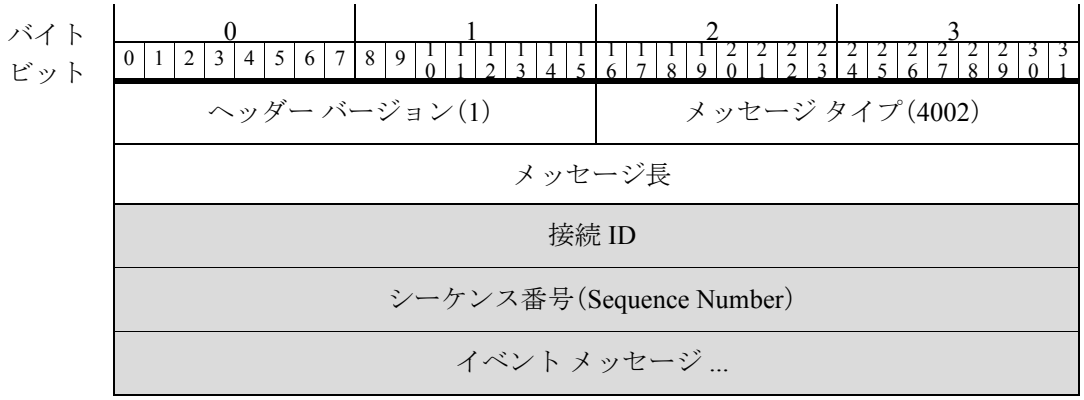
メッセージ バンドルの形式

クライアントが拡張要求を送信すると、eStreamer サーバはバンドル形式でメッセージを送信します。

クライアントはヌル メッセージで応答し、バンドル全体の受信の確認応答を行います。クライアントは、バンドル内の個々のメッセージの受信を確認応答するべきではありません。

メッセージ バンドルのメッセージ タイプは 4002 です。

次の図に、メッセージ バンドルの構造を示します。網掛けのフィールドは、バンドル メッセージ タイプに固有のものです。次の表に、フィールドとデータ構造の内容を示します。



メッセージ バンドル メッセージのフィールドは次のとおりです。

表 2-24　メッセージ バンドル メッセージのフィールド

フィールド	データ タイプ	説明
ヘッダー バージョン	uint16	常に 1 です。
Message Type	uint16	常に 4002 です。
メッセージ長	uint32	メッセージ ヘッダーの後のメッセージのコンテンツの長さ。バンドルの [ヘッダー バージョン（Header Version）]、[メッセージ タイプ（Message Type）]、および [メッセージ長（Message Length）] フィールドのバイトは含まれません。 クライアントがバンドルからメッセージをロードするとき、このフィールドの長さからメッセージのトータル長（ヘッダーを含む）を差し引くことができます。残りの部分が正数であれば、処理するメッセージがさらにあります。
接続 ID	uint32	サーバとの接続用の一意の識別子。
シーケンス番号（Sequence Number）	uint32	1 から始まり、eStreamer サーバによって送信された各バンドルに対して 1 ずつ増分します。
イベント メッセージ []	アレイ	バンドル内のサーバによってストリーミングされたイベント。各メッセージには、メッセージのバージョン番号（1）、要求された場合はアーカイブ タイムスタンプなど、フルセットのヘッダーがあります。

メタデータについて

eStreamer サーバは、要求されたイベント レコードとともにメタデータを提供できます。メタデータを受信するには、明示的に要求する必要があります。特定のバージョンのメタデータを要求する方法については、表 2-6要求フラグ（2-13 ページ）を参照してください。メタデータは、イベント レコードのコードおよび数値識別子のコンテキスト情報を提供します。たとえば、侵入イベントには検出デバイスの内部識別子のみが含まれ、メタデータはデバイスの名前を提供します。

メタデータの伝送

要求メッセージがメタデータを指定する場合、eStreamer は関連するメタデータ レコードを送信してから、関連するイベント レコードを送信します。

eStreamer は、クライアントに送信したメタデータを追跡し、同じメタデータ レコードを再送しません。クライアントは、受信した各メタデータ レコードをキャッシュする必要があります。eStreamer は、あるセッションから次のセッションへのメタデータ送信の履歴を保持しないため、新しいセッションが開始され、要求メッセージがメタデータを指定すると、eStreamer は最初からメタデータのストリーミングを再スタートします。

侵入および相関データ構造の概要

eStreamer サービスは、要求されたイベントとメタデータをクライアントに配信するために多数のデータ レコード タイプを送信します。この章では、次のタイプのイベント データのデータ レコードの構造について説明します。

- 管理対象デバイスによって生成された侵入イベント データとイベント追加データ
- Management Center によって生成された相関（コンプライアンス）イベント
- メタデータ レコード

この章の次の項では、イベント メッセージの構造を定義しています。

- 侵入イベントとメタデータのレコード タイプ（3-1 ページ）。

データ レコードを送信する eStreamer のメッセージ形式の概要の詳細については、イベント データ メッセージの形式（2-18 ページ）を参照してください。

侵入イベントとメタデータのレコード タイプ

次の表は、侵入イベント、侵入イベント追加データ、およびメタデータ メッセージで現在サポートされているすべてのレコード タイプを一覧表示しています。これらのレコード タイプのデータは固定長フィールドです。対照的に、相関イベント レコードには、1 つ以上のレベルの可変長のネストされたデータ ブロックが含まれています。次の表は、関連するデータ レコードの構造を定義している章のサブセクションへのリンクを示します。

一部のレコード タイプでは、eStreamer が複数のバージョンをサポートしています。各バージョンのステータス（現在またはレガシー）を表に示しています。現在のレコードは最新バージョンです。レガシー レコードは、以降のバージョンによって取って代わられていますが、eStreamer から要求することができます。

表 3-1　侵入イベントと一般的なメタデータのレコード タイプ

レコード タイプ	ブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
2	該当なし	該当なし	パケット データ（バージョン 4.8.0.2 以上）	現在（Current）	パケット レコード 4.8.0.2 以上（3-6 ページ）
4	該当なし	該当なし	プライオリティのメタデータ	現在（Current）	プライオリティ レコード（3-8 ページ）
9	20	1	侵入の影響アラート	レガシー	侵入影響アラート データ（B-47 ページ）

表 3-1　侵入イベントと一般的なメタデータのレコード タイプ(続き)

レコード タイプ	ブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
9	153	1	侵入の影響アラート	現在 (Current)	侵入の影響アラート データ 5.3 以上 (3-18 ページ)
62	57	2	ユーザ メタデータ	現在 (Current)	ユーザ レコード(3-21 ページ)
66	該当なし	該当なし	ルール メッセージのメタデータ(バージョン 4.6.1 以上)	現在 (Current)	4.6.1 以上のルール メッセージのレコード (3-23 ページ)
67	該当なし	該当なし	分類のメタデータ(バージョン 4.6.1 以上)	現在 (Current)	4.6.1 以上の分類レコード(3-24 ページ)
69	該当なし	該当なし	相関ポリシーのメタデータ(バージョン 4.6.1 以上)	現在 (Current)	相関ポリシー レコード(3-25 ページ)
70	該当なし	該当なし	相関ルールのメタデータ(バージョン 4.6.1 以上)	現在 (Current)	相関ルール レコード(3-27 ページ)
104	該当なし	該当なし	侵入イベント(IPv4)レコード 4.9 ～ 4.10.x	レガシー	製品の旧バージョン
105	該当なし	該当なし	侵入イベント(IPv6)レコード 4.9 ～ 4.10.x	レガシー	製品の旧バージョン
110	4	2	侵入イベント追加データ(バージョン 4.10.0 以上)	現在 (Current)	侵入イベント追加データ レコード (3-29 ページ)
111	5	2	侵入イベント追加データのメタデータ(バージョン 4.10.0 以上)	現在 (Current)	侵入イベント追加データのメタデータ (3-30 ページ)
112	128	1	5.1 ～ 5.3.x の相関イベント	レガシー	相関イベント 5.1 ～ 5.3.x(B-261 ページ)
112	156	1	5.4 以上の相関イベント	現在 (Current)	5.4 以上の相関イベント(3-46 ページ)
115	18	2	セキュリティ ゾーン名のメタデータ	現在 (Current)	セキュリティ ゾーン名 レコード (3-32 ページ)
116	18	2	インターフェイス名のメタデータ	現在 (Current)	インターフェイス名 レコード(3-34 ページ)
117	18	2	アクセス コントロール ポリシー名メタデータ	現在 (Current)	アクセス コントロール ポリシー名のレコード(3-35 ページ)
118	15	2	侵入ポリシー名のメタデータ	現在 (Current)	侵入ポリシー名 レコード(4-23 ページ)
119	15	2	アクセス コントロール ルール ID のメタデータ	現在 (Current)	アクセス コントロール ルール ID レコードのメタデータ(3-36 ページ)
120	該当なし	該当なし	アクセス コントロール ルール アクションのメタデータ	現在 (Current)	アクセス コントロール ルール アクション レコード メタデータ(4-24 ページ)
121	該当なし	該当なし	URL カテゴリのメタデータ	現在 (Current)	URL カテゴリ レコード メタデータ (4-25 ページ)

表 3-1　侵入イベントと一般的なメタデータのレコード タイプ(続き)

レコード タイプ	ブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
122	該当なし	該当なし	URL レピュテーション メタデータ	現在 (Current)	URL レピュテーション レコード メタデータ (4-26 ページ)
123	該当なし	該当なし	管理対象 デバイス のメタデータ	現在 (Current)	管理対象 デバイス レコードのメタデータ (3-38 ページ)
該当なし	64	2	アクセス コントロール名のデータ ブロック	現在 (Current)	アクセス コントロール ポリシー名のデータ ブロック (3-81 ページ)
124	59	2	アクセス コントロール ポリシー ルール理由データ ブロック	現在 (Current)	6.0 以上のアクセス コントロール ポリシー ルール理由データ ブロック (3-79 ページ)
125	該当なし	2	マルウェア イベント レコード(バージョン 5.1.1 以上)	現在 (Current)	マルウェア イベント レコード 5.1.1 以上 (3-38 ページ)
125	24	2	マルウェア イベント (バージョン 5.1.1 以上)	現在 (Current)	マルウェア イベント データ ブロック 5.1.1.x (B-54 ページ)
125	33	2	マルウェア イベント (バージョン 5.2.x)	レガシー	マルウェア イベント データ ブロック 5.2.x (B-60 ページ)
125	35	2	マルウェア イベント (バージョン 5.3)	レガシー	マルウェア イベントのデータ ブロック 5.3 (B-67 ページ)
125	44	2	マルウェア イベント (バージョン 5.3.1)	レガシー	マルウェア イベント データ ブロック 5.3.1 (B-74 ページ)
125	47	2	マルウェア イベント (バージョン 5.4.x)	現在 (Current)	マルウェア イベント データ ブロック 5.4.x (B-82 ページ)
125	62	2	マルウェア イベント (バージョン 6.0 以上)	現在 (Current)	マルウェア イベントのデータ ブロック 6.0 以上 (3-94 ページ)
127	18	2	Cisco Advanced Malware Protection クラウドのメタデータ (バージョン 5.1 以上)	現在 (Current)	Cisco Advanced Malware Protection クラウド名のメタデータ (3-39 ページ)
128	該当なし	該当なし	マルウェア イベント タイプのメタデータ (バージョン 5.1 以上)	現在 (Current)	マルウェア イベント タイプのメタデータ (3-41 ページ)
129	該当なし	該当なし	マルウェア イベント サブタイプのメタデータ (バージョン 5.1 以上)	現在 (Current)	マルウェア イベント サブタイプのメタデータ (3-42 ページ)
130	該当なし	該当なし	AMP for Endpoints ディテクタ タイプのメタデータ (バージョン 5.1 以上)	現在 (Current)	AMP for Endpoints ディテクタ タイプのメタデータ (3-43 ページ)
131	該当なし	該当なし	AMP for Endpoints ファイル タイプのメタデータ (バージョン 5.1 以上)	現在 (Current)	AMP for Endpoints ファイル タイプのメタデータ (3-44 ページ)

表 3-1　侵入イベントと一般的なメタデータのレコード タイプ(続き)

レコード タイプ	ブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
132	該当なし	該当なし	セキュリティ コンテキスト名	現在 (Current)	セキュリティ コンテキスト名 (3-45 ページ)
140	27	2	5.2 以上のルール ドキュメントのデータ ブロック	現在 (Current)	5.2 以上のルール ドキュメントのデータ ブロック (3-107 ページ)
207	該当なし	該当なし	侵入イベント (IPv4) レコード 5.0.x ～ 5.1	レガシー	侵入イベント (IPv4) レコード 5.0.x ～ 5.1 (B-2 ページ)
208	該当なし	該当なし	侵入イベント (IPv6) レコード 5.0.x ～ 5.1	レガシー	侵入イベント (IPv6) レコード 5.0.x ～ 5.1 (B-8 ページ)
260	19	2	ICMP タイプ データのデータ ブロック	現在 (Current)	ICMP タイプのデータ ブロック (3-69 ページ)
270	20	2	ICMP コードのデータ ブロック	現在 (Current)	ICMP コードのデータ ブロック (3-70 ページ)
282	該当なし	2	5.4.1 以上のセキュリティ インテリジェンス カテゴリのメタデータ	現在 (Current)	5.4.1 以上のセキュリティ インテリジェンス カテゴリのメタデータ (3-72 ページ)
300	該当なし	該当なし	6.0 以上のレルムのメタデータ	現在 (Current)	6.0 以上のレルムのメタデータ (3-73 ページ)
301	58	2	6.0 以上のエンドポイント プロファイル	現在 (Current)	6.0 以上のエンドポイント プロファイルのデータ ブロック (3-74 ページ)
302	該当なし	該当なし	6.0 以上のセキュリティ グループのメタデータ	現在 (Current)	6.0 以上のセキュリティ グループのメタデータ (3-75 ページ)
320	該当なし	該当なし	6.0 以上の DNS レコード タイプのメタデータ	現在 (Current)	6.0 以上の DNS レコード タイプのメタデータ (3-76 ページ)
321	該当なし	該当なし	6.0 以上の DNS レスポンス タイプのメタデータ	現在 (Current)	6.0 以上の DNS レスポンス タイプのメタデータ (3-77 ページ)
322	該当なし	該当なし	6.0 以上のシンクホールのメタデータ	現在 (Current)	6.0 以上のシンクホールのメタデータ (3-77 ページ)
350	該当なし	該当なし	6.0 以上の Netmap ドメインのメタデータ	現在 (Current)	6.0 以上の Netmap ドメインのメタデータ (3-78 ページ)
400	34	2	侵入イベント レコード 5.2.x	レガシー	侵入イベント レコード 5.2.x (B-14 ページ)
400	41	2	侵入イベント レコード 5.3	レガシー	侵入イベント レコード 5.3 (B-20 ページ)
400	54	2	侵入イベント レコード 5.3.1	レガシー	侵入イベント レコード 5.3.1 (B-32 ページ)
400	45	2	侵入イベント レコード 5.4.x	レガシー	侵入イベント レコード 5.4.x (B-38 ページ)
400	60	2	侵入イベント レコード 6.0 以上	現在 (Current)	侵入イベント レコード 6.0 以上 (3-8 ページ)
500	32	2	ファイル イベント (バージョン 5.2.x)	レガシー	ファイル イベント 5.2.x (B-223 ページ)

表 3-1　侵入イベントと一般的なメタデータのレコード タイプ(続き)

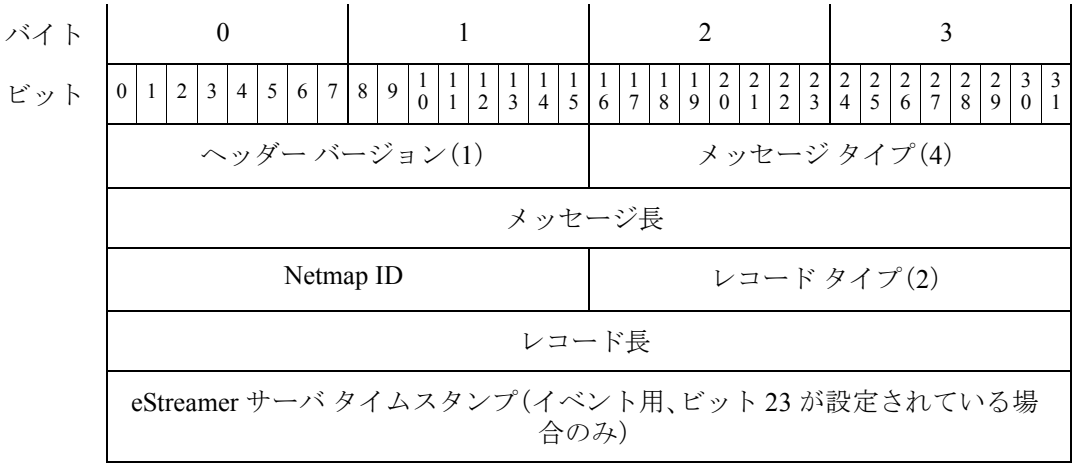
レコード タイプ	ブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
500	38	2	ファイル イベント(バージョン 5.3)	レガシー	ファイル イベント 5.3(B-227 ページ)
500	43	2	ファイル イベント(バージョン 5.3.1)	レガシー	ファイル イベント 5.3.1(B-234 ページ)
500	46	2	ファイル イベント(バージョン 5.4 以上)	現在(Current)	6.0 以上のファイル イベント(3-83 ページ)
502	32	2	ファイル イベント(バージョン 5.2.x)	レガシー	ファイル イベント 5.2.x(B-223 ページ)
502	38	2	ファイル イベント(バージョン 5.3)	レガシー	ファイル イベント 5.3(B-227 ページ)
502	43	2	ファイル イベント(バージョン 5.3.1)	レガシー	ファイル イベント 5.3.1(B-234 ページ)
502	46	2	ファイル イベント(バージョン 5.4.x)	現在(Current)	ファイル イベント 5.4.x(B-240 ページ)
502	72	2	ファイル イベント(バージョン 6.0 以上)	現在(Current)	6.0 以上のファイル イベント(3-83 ページ)
510	該当なし	該当なし	5.3 以上のファイル タイプ ID のメタデータ	現在(Current)	5.3 以上のファイル タイプ ID のメタデータ(3-106 ページ)
511	26	2	5.11 ～ 5.2.x のファイル イベント SHA ハッシュ	レガシー	ファイル イベント SHA ハッシュ 5.1.1 ～ 5.2.x(B-251 ページ)
511	40	2	5.3 以上のファイル イベント SHA ハッシュ	現在(Current)	5.3 以上のファイル イベント SHA ハッシュ(3-104 ページ)
515	該当なし	該当なし	6.0 以上の Filelog ストレージのメタデータ	現在(Current)	6.0 以上の Filelog ストレージのメタデータ(3-111 ページ)
516	該当なし	該当なし	6.0 以上の Filelog サンドボックスのメタデータ	現在(Current)	6.0 以上の Filelog サンドボックスのメタデータ(3-112 ページ)
517	該当なし	該当なし	6.0 以上の Filelog Spero のメタデータ	現在(Current)	6.0 以上の Filelog Spero のメタデータ(3-113 ページ)
518	該当なし	該当なし	6.0 以上の Filelog アーカイブのメタデータ	現在(Current)	6.0 以上の Filelog アーカイブのメタデータ(3-114 ページ)
519	該当なし	該当なし	6.0 以上の Filelog スタティック分析のメタデータ	現在(Current)	6.0 以上の Filelog スタティック分析のメタデータ(3-115 ページ)
520	36	2	5.2 以上の位置情報のデータ ブロック	現在(Current)	5.2 以上の位置情報のデータ ブロック(3-116 ページ)
530	該当なし	該当なし	6.0 以上のファイル ポリシー名	現在(Current)	6.0 以上のファイル ポリシー名(3-117 ページ)
600	該当なし	該当なし	SSL ポリシー名	現在(Current)	SSL ポリシー名(3-118 ページ)
601	51	2	SSL ルール ID	現在(Current)	SSL ルール ID(3-119 ページ)

表 3-1　侵入イベントと一般的なメタデータのレコード タイプ(続き)

レコード タイプ	ブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
602	該当なし	該当なし	SSL 暗号スイート(SSL Cipher Suite)	現在(Current)	5.4 以上の SSL 証明書の詳細のデータ ブロック(3-126 ページ)
604	該当なし	該当なし	SSL バージョン	現在(Current)	SSL バージョン(3-120 ページ)
605	該当なし	該当なし	SSL サーバ証明書ステータス	現在(Current)	SSL サーバ証明書ステータス(3-121 ページ)
606	該当なし	該当なし	実際の SSL アクション	現在(Current)	実際の SSL アクション(3-122 ページ)
607	該当なし	該当なし	予期された SSL アクション	現在(Current)	予期された SSL アクション(3-123 ページ)
608	該当なし	該当なし	SSL フロー ステータス	現在(Current)	SSL フロー ステータス(3-124 ページ)
613	該当なし	該当なし	SSL URL カテゴリ	現在(Current)	SSL URL カテゴリ(3-125 ページ)
614	50	2	5.4 以上の SSL 証明書の詳細のデータ ブロック	現在(Current)	5.4 以上の SSL 証明書の詳細のデータ ブロック(3-126 ページ)
700	該当なし	該当なし	ネットワーク分析ポリシー レコード	現在(Current)	ネットワーク分析ポリシー レコード(3-130 ページ)

パケット レコード 4.8.0.2 以上

eStreamer サービスは、パケット レコードのイベントに関連付けられたパケット データを送信します。形式は次のとおりです。パケット フラグ(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 0)が設定されていると、パケット データが送信されます。要求フラグ(2-12 ページ)を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにパケット レコードを示す値 2 があることに注意してください。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
将来の使用に備えて予約済み（イベントでビット 23 が設定されている場合のみ）																																
デバイス ID																																
イベント ID																																
イベント秒																																
パケット秒																																
パケット マイクロ秒																																
リンク タイプ																																
パケット長																																
パケット データ...																																

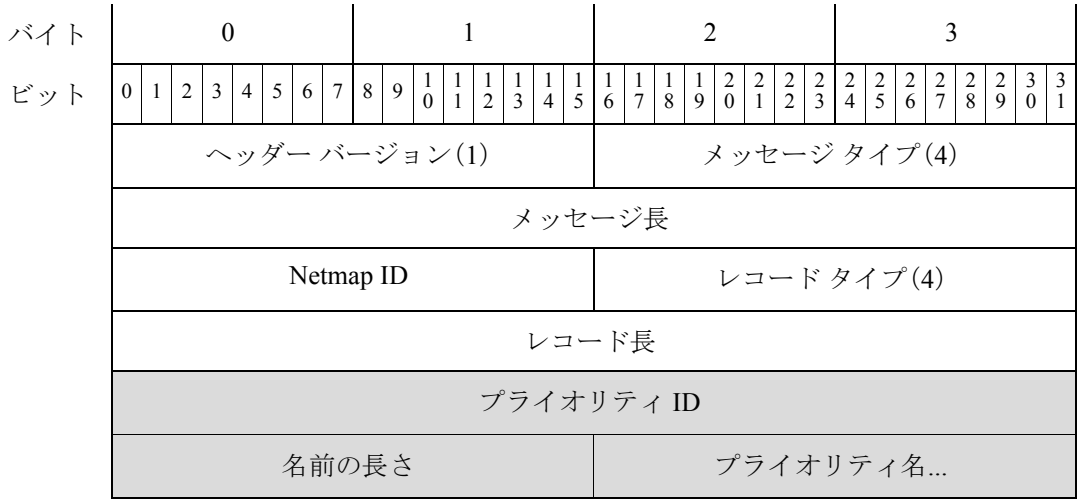
次の表は、パケット レコードのフィールドについての説明です。

表 3-2　パケット レコード フィールド

フィールド	データ タイプ	説明
デバイス ID	uint32	デバイス ID 番号。バージョン 3 または 4 のメタデータの要求により関連付けられているデバイス名を取得できます。詳細については、管理対象 デバイス レコードのメタデータ (3-38 ページ) を参照してください。
イベント ID	uint32	イベント ID 番号。
イベント秒	uint32	イベントが発生した秒（01/01/1970 以降）。
パケット秒	uint32	パケットがキャプチャされた秒（01/01/1970 以降）。
パケット マイクロ秒	uint32	パケットがキャプチャされたマイクロ秒（100 万分の 1 秒）の増分。
リンク タイプ	uint32	リンク層のタイプ。現在、値は常に 1 になります（イーサネット層を示します）。
パケット長	uint32	パケット データに含まれるバイト数。
パケット データ	変数	キャプチャされた実際のパケット データ（ヘッダーとペイロード）。

プライオリティ レコード

eStreamer サービスは、プライオリティ レコードのイベントに関連付けられたプライオリティを送信します。形式は次のとおりです。(メタデータ フラグのいずれか(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 1、14、15、または 20)が設定されていると、プライオリティ情報が送信されます。要求フラグ(2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにプライオリティ レコードを示す値 4 があることに注意してください。



次の表は、各プライオリティ固有のフィールドについての説明です。

表 3-3　プライオリティ レコード フィールド

フィールド	データ タイプ	説明
プライオリティ ID	uint32	プライオリティ ID 番号を表示します。
名前の長さ	uint16	プライオリティ名に含まれるバイト数。
プライオリティ名	変数	プライオリティ ID に対応するプライオリティ名(1 - 高、2 - 中、3 - 低)。

侵入イベント レコード 6.0 以上

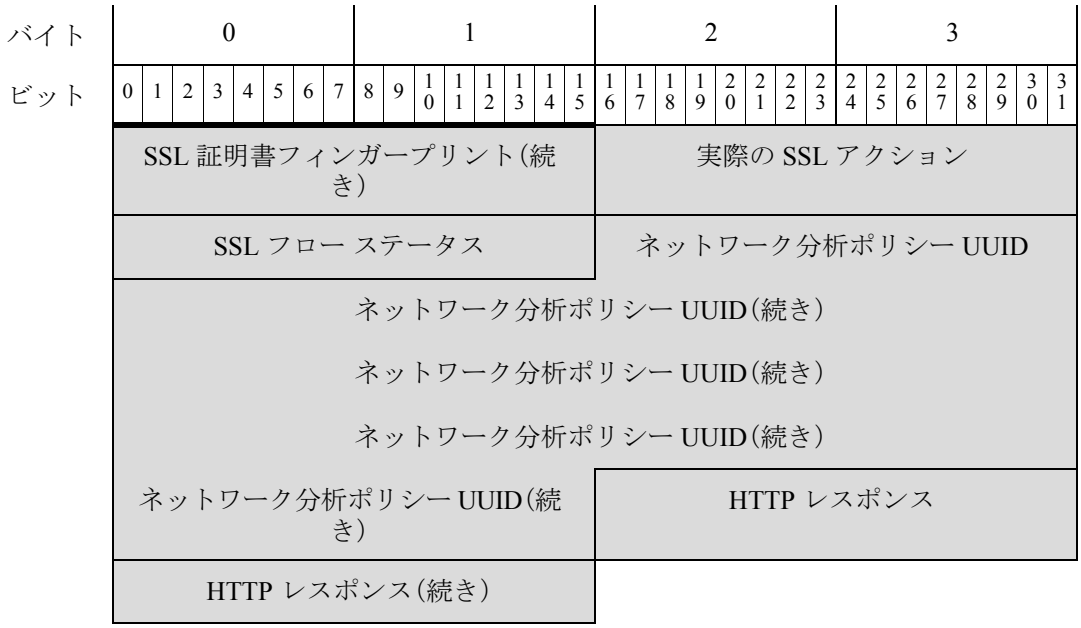
侵入イベント レコードのフィールドは、次の図で網掛けされています。レコード タイプは 400 で、ブロック タイプはシリーズ 2 セットのデータ ブロックの 60 です。これはブロック タイプ 45 に取って代わります。HTTP レスポンス フィールドが追加されました。

ストリーム要求メッセージでイベント タイプ コード 12 とバージョン コード 9 を要求する拡張要求によってのみ、eStreamer から 6.0 以上の侵入イベントを要求できます(拡張要求の送信の詳細については、拡張要求の送信(2-4 ページ) を参照してください)。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																									レコード タイプ(400)							
レコード長																																
eStreamer サーバ タイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																																
将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																																
ブロック タイプ(60)																																
ブロック長																																
デバイスID																																
イベント ID																																
イベント秒																																
イベント マイクロ秒																																
ルール ID(シグネチャ ID)																																
ジェネレータ ID																																
ルール リビジョン																																
分類 ID																																
プライオリティ ID																																
送信元 IP アドレス 送信元 IP アドレス(続き) 送信元 IP アドレス(続き) 送信元 IP アドレス(続き)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
宛先IPアドレス																																
宛先 IP アドレス（続き）																																
宛先 IP アドレス（続き）																																
宛先 IP アドレス（続き）																																
送信元ポートまたは ICMP タイプ																	送信先ポートまたは ICMP コード														
IP プロトコル ID									影響フラグ								影響								ブロック							
MPLSラベル（MPLS Label）																																
VLAN ID																	パッド															
ポリシー UUID																																
ポリシー UUID（続き）																																
ポリシー UUID（続き）																																
ポリシー UUID（続き）																																
ユーザ ID																																
Web アプリケーション ID																																
クライアント アプリケーション ID																																
アプリケーション プロトコル ID																																
アクセス コントロール ルール ID																																
アクセス コントロール ポリシー UUID																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
インターフェイス入力 UUID																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
インターフェイス出力 UUID																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
セキュリティ ゾーン入力 UUID																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン出力 UUID																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
接続タイムスタンプ																																
接続インスタンス ID																	接続数カウンタ															
送信元の国																	宛先の国															
IOC 番号																	セキュリティ コンテキスト															
セキュリティ コンテキスト（続き）																																
セキュリティ コンテキスト（続き）																																
セキュリティ コンテキスト（続き）																																
セキュリティ コンテキスト（続き）																	SSL 証明書フィンガープリント															
SSL 証明書フィンガープリント（続き）																																
SSL 証明書フィンガープリント（続き）																																
SSL 証明書フィンガープリント（続き）																																
SSL 証明書フィンガープリント（続き）																																



次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 3-4　侵入イベント レコード 6.0 以上のフィールド

フィールド	データ タイプ	説明
ブロック タイプ	unint32	侵入イベント データ ブロックを開始します。この値は常に 60 です。
ブロック長	unint32	侵入イベント データ ブロックのバイトの合計数（侵入イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む）。
デバイスID	unit32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ (3-38 ページ) を参照してください。
イベント ID	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
イベント マイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒（100 万分の 1 秒）単位の増分。
ルール ID（シグネチャ ID）	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。

表 3-4　侵入イベント レコード 6.0 以上のフィールド(続き)

フィールド	データ タイプ	説明
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポートまたは ICMP タイプ	uint16	イベント プロトコル タイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
送信先ポートまたは ICMP コード	uint16	イベント プロトコル タイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル ID	uint8	IANA 指定のプロトコル番号。次に例を示します。 • 0:IP • 1:ICMP • 6:TCP • 17:UDP

表 3-4　侵入イベント レコード 6.0 以上のフィールド（続き）

フィールド	データ タイプ	説明
影響フラグ	bits8	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01（ビット 0）：送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02（ビット 1）：送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04（ビット 2）：送信元または宛先ホストはイベントのポート上のサーバを実行しているか（TCP または UDP の場合）、IP プロトコルを使用します。 • 0x08（ビット 3）：イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10（ビット 4）：イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20（ビット 5）：イベントが原因で、管理対象デバイスがセッションをドロップしました（デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます）。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40（ビット 6）：このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80（ビット 7）：イベントで検出されたクライアントにマップされた脆弱性があります。（バージョン 5.0+ のみ） 次の影響レベル値は、Management Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • グレー（0、不明）：00X00000 • 赤（1、脆弱）：xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx（バージョン 5.0+ のみ） • オレンジ（2、潜在的に脆弱）：00X0011X • 黄（3、現在は脆弱でない）：00X0001X • 青（4、不明なターゲット）：00X00001
影響	uint8	イベントの影響フラグ値。値は次のとおりです。 • 1：レッド（脆弱） • 2：オレンジ（脆弱の可能性あり） • 3：イエロー（現在は脆弱でない） • 4：ブルー（不明なターゲット） • 5：グレー（不明なインパクト）

表 3-4　侵入イベント レコード 6.0 以上のフィールド(続き)

フィールド	データ タイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 • 0:ブロックされていない • 1:ブロックされた • 2:ブロックされた可能性がある(設定では許可されていない)
MPLSラベル（MPLS Label）	uint32	MPLS ラベル。
VLAN ID	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルの内部 ID 番号(該当する場合)。
アクセス コントロール ルール ID	uint32	アクセス コントロール ルールの固有識別子として機能するルール ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの固有識別子として機能するポリシー ID 番号。
インターフェイス入力 UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
インターフェイス出力 UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
セキュリティ ゾーン入力 UUID	uint8[16]	入力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
セキュリティ ゾーン出力 UUID	uint8[16]	出力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。

表 3-4　侵入イベント レコード 6.0 以上のフィールド（続き）

フィールド	データ タイプ	説明
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティ コンテキスト	uint8[16]	トラフィックが通過したセキュリティ コンテキスト（仮想ファイアウォール）の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書 フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号（既知のキー）」 • 5:「復号（置換キー）」 • 6:「復号（Resign）」

表 3-4　侵入イベント レコード 6.0 以上のフィールド(続き)

フィールド	データ タイプ	説明
SSL フロー ステータス	uint16	SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。 • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」

表 3-4　侵入イベント レコード 6.0 以上のフィールド（続き）

フィールド	データ タイプ	説明
ネットワーク分析ポリシー UUID	uint8[16]	侵入イベントを作成したネットワーク分析ポリシーの UUID。
HTTP レスポンス	uint32	HTTP 要求の応答コード。

侵入の影響アラート データ 5.3 以上

侵入の影響アラート 5.3 以上のイベントには影響イベントに関する情報が表示されます。これは、侵入イベントがシステム ネットワーク マップ データと比較され、影響が判別されているときに送信されます。レコード タイプ 9 の標準レコード ヘッダーを使用します。この後にシリーズ 1 グループのブロックのシリーズ 1 のデータ ブロック タイプが 153 の侵入の影響アラートのデータ ブロックが続きます。（影響アラート データ ブロック タイプは、シリーズ 1 データ ブロックです。シリーズ 1 データ ブロックの詳細については、ディスカバリ（シリーズ1）ブロック（4-63 ページ）を参照してください）。

要求メッセージのフラグ フィールドにビット 5 を設定することで、eStreamer が侵入の影響イベントを送信するように要求できます。要求メッセージの詳細については、イベント ストリーム要求メッセージの形式（2-11 ページ）を参照してください。これらのアラートのバージョン 1 は、IPv4 のみを処理します。5.3 で導入されたバージョン 2 は、IPv4 に加えて IPv6 イベントを処理します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（9）															
eStreamer サーバ タイムスタンプ（イベント用、ビット 23 が設定されている場合のみ）																																
将来の使用に備えて予約済み（イベントでビット 23 が設定されている場合のみ）																																
侵入影響アラート ブロック長																																
イベント ID																																
デバイス ID																																
イベント秒																																
影響																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	送信元 IP アドレス																															
	送信元 IP アドレス（続き）																															
	送信元 IP アドレス（続き）																															
	送信元 IP アドレス（続き）																															
	宛先IPアドレス																															
	宛先 IP アドレス（続き）																															
	宛先 IP アドレス（続き）																															
	宛先 IP アドレス（続き）																															
影響 説明	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	説明...																															

次の表は、影響イベントの各データ フィールドについての説明です。

表 3-5　影響イベント データ フィールド

フィールド	データ タイプ	説明
侵入影響アラート ブロック タイプ	uint32	侵入影響アラート データ ブロックが続くことを示します。このフィールドの値は、常に 20 です。侵入イベントとメタデータのレコード タイプ（3-1 ページ）を参照してください。
侵入影響アラート ブロック長	uint32	侵入の影響アラートのブロック タイプの長さを示します。後続のすべてのデータ、および侵入の影響アラートのブロック タイプと長さの 8 バイトを含みます。
イベント ID	uint32	イベント ID 番号を表示します。
デバイス ID	uint32	管理対象デバイス ID 番号を表示します。
イベント秒	uint32	イベントが検出された秒（1970 年 1 月 1 日からの経過秒数）を示します。

表 3-5　影響イベント データ フィールド(続き)

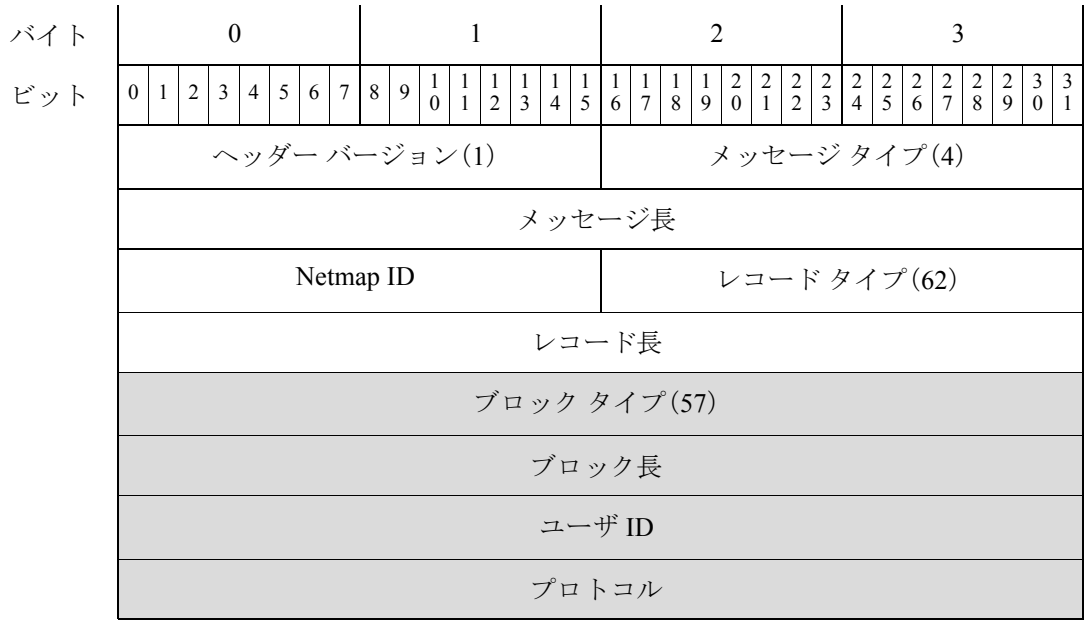
フィールド	データ タイプ	説明
影響	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) 次の影響レベル値は、Management Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • グレー(0、不明):00X00000 • 赤(1、脆弱):XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX (バージョン 5.0+ のみ) • オレンジ(2、潜在的に脆弱):00X0011X • 黄(3、現在は脆弱でない):00X0001X • 青(4、不明なターゲット):00X00001
送信元 IP アドレス	uint8[16]	影響イベントに関連付けられているホストの IP アドレス。これは、IPv4 または IPv6 アドレスにできます。詳細については、IP アドレス(1-6 ページ)を参照してください。
宛先IPアドレス	uint8[16]	影響イベントに関連付けられた宛先 IP アドレスの IP アドレス(該当する場合)。これは、IPv4 または IPv6 アドレスにできます。詳細については、IP アドレス(1-6 ページ)を参照してください。宛先 IP アドレスがない場合、この値は 0 です。

表 3-5　影響イベント データ フィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	影響名を含む文字列データのブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、文字列データ ブロック (4-74 ページ)を参照してください。
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数。これには文字列ブロック タイプ用の 4 バイト、文字列ブロック長用の 4 バイト、および説明のバイト数が含まれます。
説明	string	影響イベントについての説明。

ユーザ レコード

メタデータを要求すると、Firepower システムのコンポーネントによって生成されたイベントで参照されるユーザに関する情報を取得できます。eStreamer サービスは、ユーザ レコード内のイベントのユーザ情報を含むメタデータを送信します。形式は次のとおりです。ユーザの脆弱性の変更のデータ ブロック、ユーザ ホストの削除のデータ ブロック、ユーザ サービスの削除のデータ ブロック、ユーザの重要度の変更のブロック、属性定義のデータ ブロック、ユーザ属性値のデータ ブロック、またはスキャン結果のデータ ブロックのユーザ ID の値とメタデータを関連付けることで、イベントに関連付けられているユーザ名を判別するのにユーザ メタデータ レコードを使用できます。(メタデータ フラグのいずれか(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 1、14、15、または 20)が設定されていると、ユーザ情報が送信されます。要求フラグ (2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにユーザ レコードを示す値があることに注意してください。ユーザ レコードには、シリーズ 2 のデータ ブロックのブロック タイプ 57 のユーザのデータ ブロックが含まれます。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
名前	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	名前...																															

次の表は、ユーザ レコードのフィールドについての説明です。

表 3-6　ユーザ レコードのフィールド

フィールド	データ タイプ	説明
ブロック タイプ	unint32	ユーザ データ ブロックを開始します。この値は常に 57 です。
ブロック長	unint32	ユーザのデータ ブロックの合計バイト数です。ユーザのブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
ユーザ ID	uint32	ユーザ ID 番号。
プロトコル	uint32	ユーザの検出やレポートに使用するプロトコル。値は以下のとおりです。 • 165:FTP • 426:SIP • 547:AOL Instant Messenger • 683:IMAP • 710:LDAP • 767:NTP • 773:Oracle データベース • 788:POP3 • 1755:MDNS
文字列ブロック タイプ	uint32	この名前を含む文字列データ ブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、文字列データ ブロック (4-74 ページ)を参照してください。
名前の長さ	uint32	ユーザ名に含まれるバイト数。
名前	string	ユーザの名前。

4.6.1 以上のルール メッセージのレコード

イベントのルール メッセージ情報は、ルール メッセージ レコード内で送信されます。形式は次のとおりです。eStreamer サービスは、バージョン 2 またはバージョン 3 のメタデータを要求すると、4.6.1 以上のルール メッセージのレコードを送信します。4.6.1 以上のルール メッセージのレコードには、4.6 以前のルール メッセージのレコードと同じフィールドのほかに、UUID およびリビジョン UUID フィールドが新たに加わりました。（該当するメタデータ フラグ（要求メッセージの [要求フラグ（Request Flags）] フィールドでバージョン 2 はビット 14、バージョン 3 はビット 15、バージョン 4 はビット 20）が設定されていると、バージョン 2、バージョン 3、またはバージョン 4 のメタデータ情報が送信されます。要求フラグ（2-12 ページ） を参照してください）。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにルール メッセージのバージョン 2 のレコードを示す値 66 があることに注意してください。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		ヘッダー バージョン（1）																メッセージ タイプ（4）															
		メッセージ長																															
		Netmap ID																レコード タイプ（66）															
		レコード長																															
シグネチャー（Key）		ジェネレータ ID																															
		ルール ID																															
		リビジョン番号																															
		表示されるシグネチャ ID																															
		メッセージ長																ルール UUID															
ルール（Rule）UUID		ルール UUID（続き）																															
		ルール UUID（続き）																															
		ルール UUID（続き）																															
		ルール UUID（続き）																ルール リビジョン UUID															
ルール リビジョン UUID		ルール リビジョン UUID（続き）																															
		ルール リビジョン UUID（続き）																															
		ルール リビジョン UUID（続き）																															
		ルール リビジョン UUID（続き）																メッセージ...															

次の表は、各ルール固有のフィールドについての説明です。

表 3-7　ルール メッセージのレコードのフィールド

フィールド	データ タイプ	説明
ジェネレータ ID	uint32	ジェネレータ ID 番号。
ルール ID	uint32	ローカル コンピュータのルール ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。これは、すべてのルール メッセージで 0 に現在設定されています。
表示されるシグネチャ ID	uint32	Firepower システム インターフェイスに表示されるルール ID 番号。
メッセージ長	uint16	ルールのテキストに含まれるバイト数。
UUID	uint8[16]	ルールの固有識別子として機能するルール ID 番号。
リビジョン UUID	uint8[16]	リビジョンの固有識別子として機能するルール リビジョン ID 番号。
メッセージ	変数	イベントをトリガーしたルール メッセージ。

4.6.1 以上の分類レコード

eStreamer サービスは、4.6.1 以上の分類レコードのイベントの分類情報を送信します。形式は次のとおりです。4.6.1 以上の分類レコードには、4.6 以前の分類レコードと同じフィールドに加えて、新しい UUID およびリビジョン UUID フィールドがあります。(バージョン 3 またはバージョン 4 のメタデータ フラグ(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 15 または 20)が設定されていると、分類情報が送信されます。要求フラグ(2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに分類バージョン 2 のレコードを示す値 67 があることに注意してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(67)															
レコード長																																
分類 ID																																
名前の長さ																	名前...															
名前(続き)																																
説明の長さ																	説明...															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	説明（続き）																															
分類 UUID	分類 UUID 分類 UUID（続き） 分類 UUID（続き） 分類 UUID（続き）																															
分類リビジョン UUID	分類リビジョン UUID 分類リビジョン UUID（続き） 分類リビジョン UUID（続き） 分類リビジョン UUID（続き）																															

次の表は、分類レコードのフィールドについての説明です。

表 3-8　　分類レコード フィールド

フィールド	データ タイプ	説明
分類 ID	uint32	分類 ID 番号。
名前の長さ	uint16	名前に含まれるバイト数。
名前	string	分類の名前。
説明の長さ	uint16	説明に含まれるバイト数。
説明	string	分類の説明。
UUID	uint8[16]	分類の固有識別子として機能する分類 ID 番号。
リビジョン UUID	uint8[16]	分類リビジョンの固有識別子として機能する分類リビジョン ID 番号。

相関ポリシー レコード

eStreamer サービスは、相関ポリシー レコード内の相関イベントの相関ポリシーを含むメタデータを送信します。形式は次のとおりです。（バージョン 3 またはバージョン 4 のメタデータ フラグ（要求メッセージの [要求フラグ（Request Flags）] フィールドのビット 15 または 20）が設定されていると、相関ポリシー情報が送信されます。要求フラグ（2-12 ページ） を参照してください）。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに相関ポリシー レコードを示す値 69 があることに注意してください。

次の表は、相関ポリシー レコードのフィールドについての説明です。

表 3-9　相関ポリシー レコード フィールド

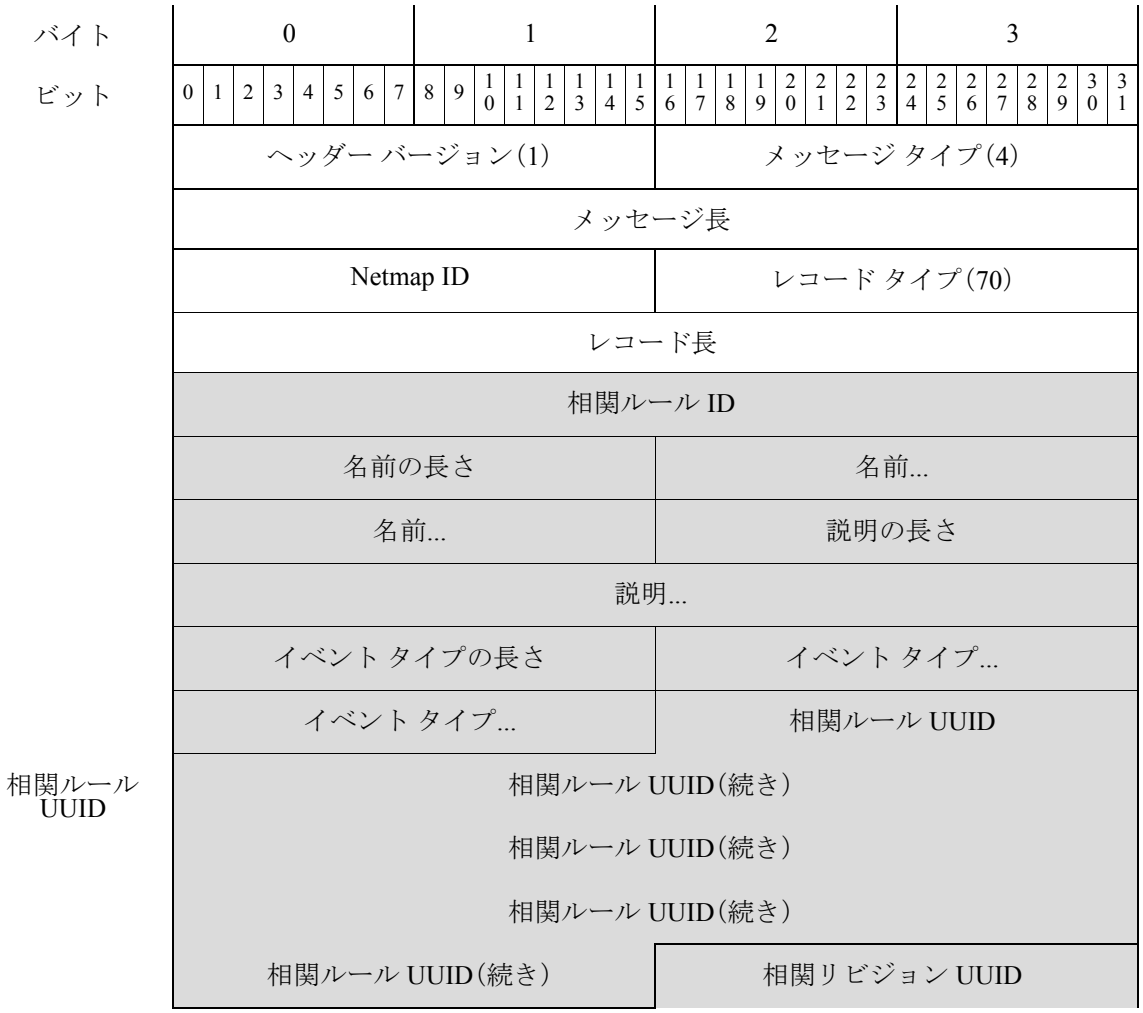
フィールド	データ タイプ	説明
相関ポリシー ID	uint32	相関ポリシー ID 番号。
名前の長さ	uint16	相関ポリシー名に含まれるバイト数。
名前	string	イベントをトリガーした相関ポリシーの名前。
説明の長さ	uint16	相関ポリシーの説明に含まれるバイト数。
説明	string	イベントをトリガーした相関ポリシーの説明。

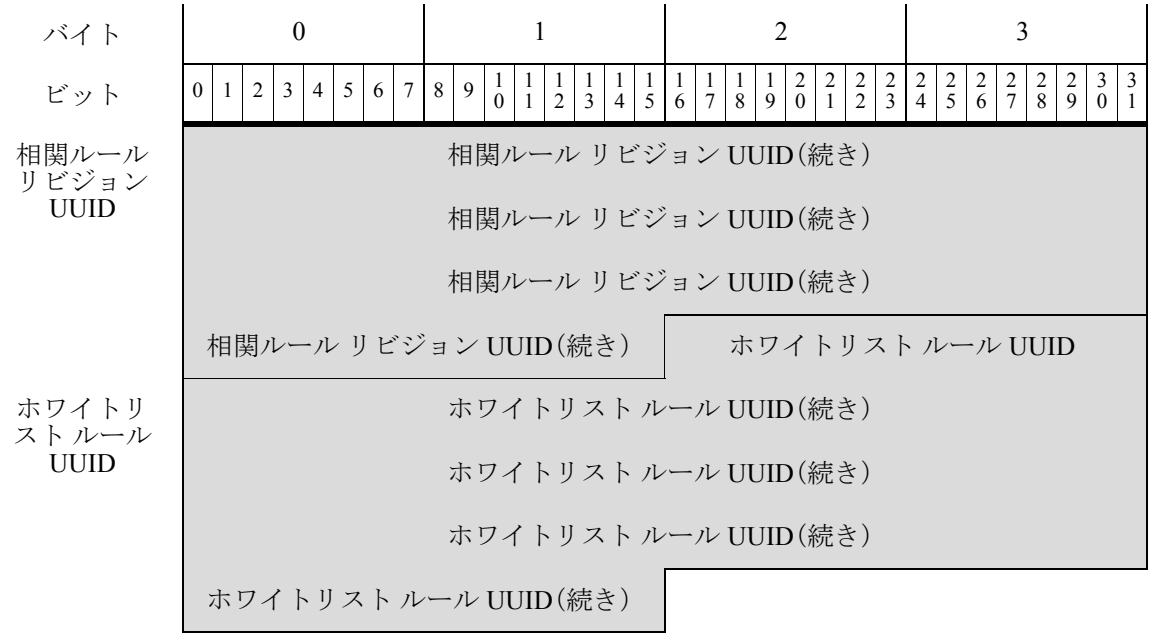
表 3-9　相関ポリシー レコード フィールド(続き)

フィールド	データ タイプ	説明
UUID	uint8[16]	相関ポリシーの固有識別子として機能する相関ポリシー ID 番号。
リビジョン UUID	uint8[16]	相関ポリシーの固有識別子として機能する相関ポリシー リビジョン ID 番号。

相関ルール レコード

eStreamer サービスは、相関ルール レコード内の相関イベントをトリガーした相関ルールの情報を含むメタデータを送信します。形式は次のとおりです。(バージョン 3 またはバージョン 4 のメタデータ フラグ(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 15 または 20)が設定されていると、相関ルール情報が送信されます。要求フラグ(2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに相関ルール レコードを示す値 70 があることに注意してください。





次の表は、相関ルール レコードのフィールドについての説明です。

表 3-10　相関ルール レコード フィールド

フィールド	データ タイプ	説明
相関ルール ID	uint32	相関ルール ID 番号。
名前の長さ	uint16	相関ルール名に含まれるバイト数。
名前	string	イベントをトリガーした相関ルールの名前。
説明の長さ	uint16	相関ルールの説明に含まれるバイト数。
説明	string	イベントをトリガーした相関ルールの説明。
イベント タイプの長さ	uint16	イベント タイプの説明に含まれるバイト数。
イベント タイプ	string	相関ルールをトリガーしたイベントの説明。
UUID	uint8[16]	相関ルールの固有識別子として機能する相関ルール ID 番号。
リビジョン UUID	uint8[16]	相関ルール リビジョンの固有識別子として機能する相関ルール リビジョン ID 番号。
ホワイトリスト UUID	uint8[16]	ホワイトリスト違反の結果として送信されるイベントの固有識別子として機能する相関 ID 番号。

侵入イベント追加データ レコード

eStreamer サービスは、侵入イベント追加データ レコードの侵入イベントに関連付けられたイベント追加データを送信します。レコード タイプは常に 110 です。

イベント追加データは、カプセル化されたイベント追加データのデータ ブロックに表示されます。データ ブロック タイプの値は常に 4 です。(イベント追加データのデータ ブロックは、シリーズ 2 のデータ ブロックです。シリーズ 2 のデータ ブロックの詳細については、シリーズ 2 のデータ ブロックの概要 (3-57 ページ)を参照してください)。

サポートされる追加データのタイプには、IPv6 の送信元と宛先のアドレスに加えて、HTTP プロキシやロードバランサ経由で Web サーバに接続しているクライアントの発信元 IP アドレス (v4 または v6) が含まれています。次の図に、侵入イベント追加データ レコードの形式を示します。

要求メッセージの [要求フラグ (Request Flags)] フィールドにビット 27 を設定すると、各侵入イベントのイベント追加データを受信します。ビット 20 を設定すると、侵入イベント追加データのメタデータ (3-30 ページ)に記載されているイベント追加データのメタデータも受信されます。ビット 23 を有効にすると、eStreamer は拡張イベント ヘッダーを表示します。要求フラグの設定方法の詳細については、要求フラグ (2-12 ページ)を参照してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン (1)																	メッセージ タイプ (4)															
メッセージ長																																
Netmap ID																	レコード タイプ (110)															
レコード長																																
eStreamer サーバ タイムスタンプ (イベント用、ビット 23 が設定されている場合のみ)																																
将来の使用に備えて予約済み (イベントでビット 23 が設定されている場合のみ)																																
イベント追加データのデータ ブロック タイプ (4)																																
イベント追加データのデータ ブロック長																																
デバイス ID																																
イベント ID																																
イベント秒																																
タイプ																																
BLOB ブロック タイプ (1)																																
BLOB 長																																
イベント追加データ																																

イベント追加データのブロック構造には、Firepower システム のバージョン 4.10 で導入された複数の可変長データ構造の 1 つである BLOB ブロック タイプが含まれることに注意してください。

次の表は、侵入イベント追加データ レコードのフィールドについての説明です。

表 3-11　侵入イベント追加データのデータ ブロック フィールド

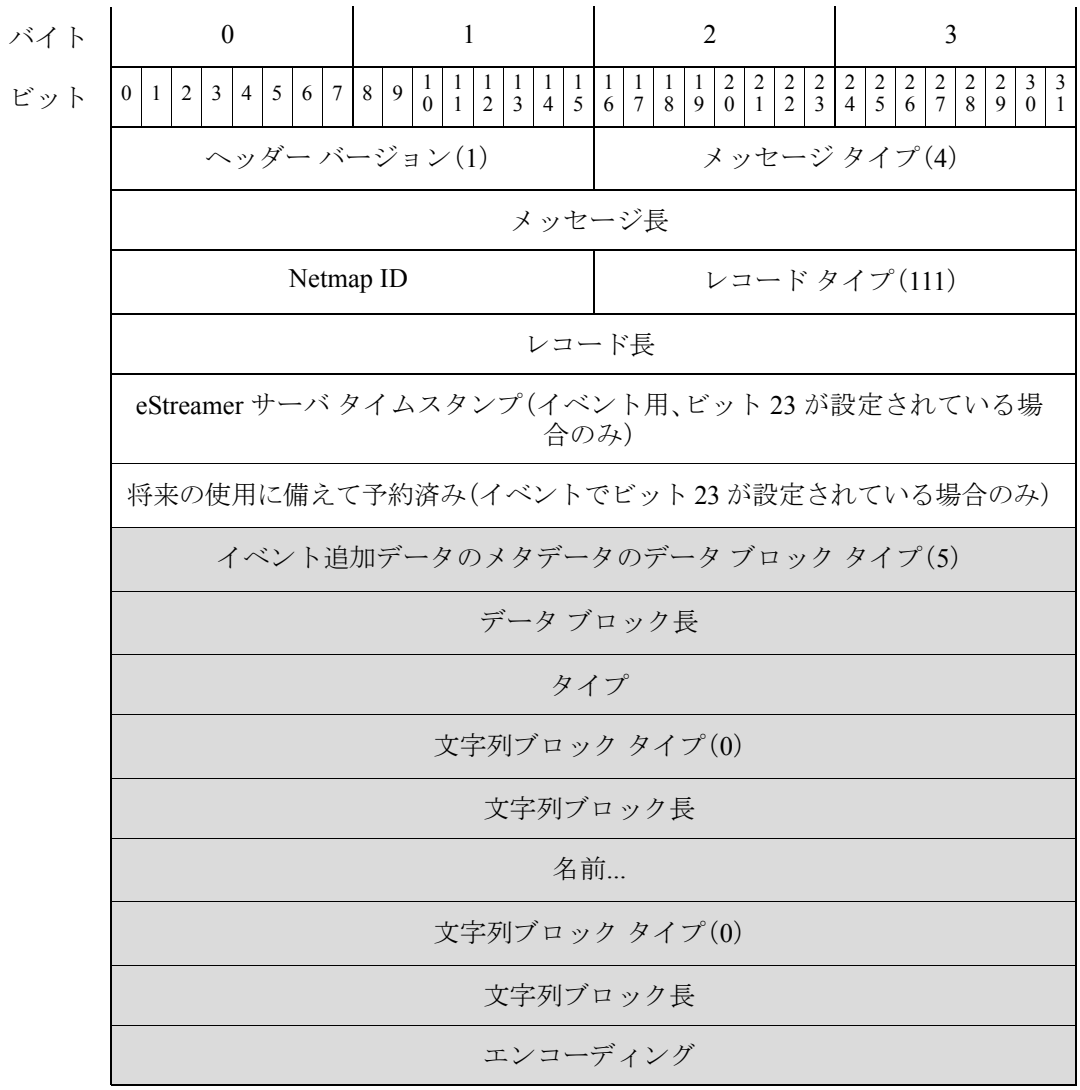
フィールド	データ タイプ	説明
イベント追加データのデータ ブロック タイプ	uint32	イベント追加データのデータ ブロックを開始します。この値は常に 4 です。ブロック タイプは、シリーズ 2 ブロックです。詳細については、シリーズ 2 のデータ ブロックの概要（3-57 ページ）を参照してください。
イベント追加データのデータ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
デバイス ID	uint32	管理対象デバイス ID 番号。
イベント ID	uint32	イベント ID 番号。
イベント秒	uint32	イベントの UNIX タイムスタンプ（01/01/1970 からの経過秒数）。
タイプ	uint32	追加データのタイプの識別子。次に例を示します。 • 1：XFF クライアント（IPv4） • 2：XFF クライアント（IPv6） • 9：HTTP URI
BLOB ブロック タイプ	uint32	追加データを含む BLOB データ ブロックを開始します。この値は常に 1 です。ブロック タイプは、シリーズ 2 ブロックです。
長さ（Length）	uint32	BLOB データ ブロックの合計バイト数。
追加データ	変数	追加データの内容。データ タイプはタイプ フィールドに表示されます。

侵入イベント追加データのメタデータ

eStreamer サービスは、侵入イベント追加データのメタデータ レコードの侵入イベント追加データ レコードに関連付けられたイベント追加データのメタデータを送信します。レコード タイプは常に 111 です。

イベント追加データのメタデータは、カプセル化されたイベント追加データのメタデータのデータ ブロックに表示されます。データ ブロック タイプの値は常に 5 です。イベント追加データのデータ ブロックは、シリーズ 2 のデータ ブロックです。

要求メッセージの [要求フラグ（Request Flags）] フィールドにビット 20 を設定すると、イベント追加データのメタデータを受信します。侵入イベントおよびイベント追加データのメタデータのどちらも受信するには、ビット 2 も設定する必要があります。要求フラグ（2-12 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(111)															
レコード長																																
eStreamer サーバ タイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																																
将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																																
イベント追加データのメタデータのデータ ブロック タイプ(5)																																
データ ブロック長																																
タイプ																																
文字列ブロック タイプ(0)																																
文字列ブロック長																																
名前...																																
文字列ブロック タイプ(0)																																
文字列ブロック長																																
エンコーディング																																

ブロック構造には、Firepower システム バージョン 4.10 で導入された複数のシリーズ 2 の可変長データ構造の 1 つであるカプセル化された文字列ブロック タイプが含まれることに注意してください。

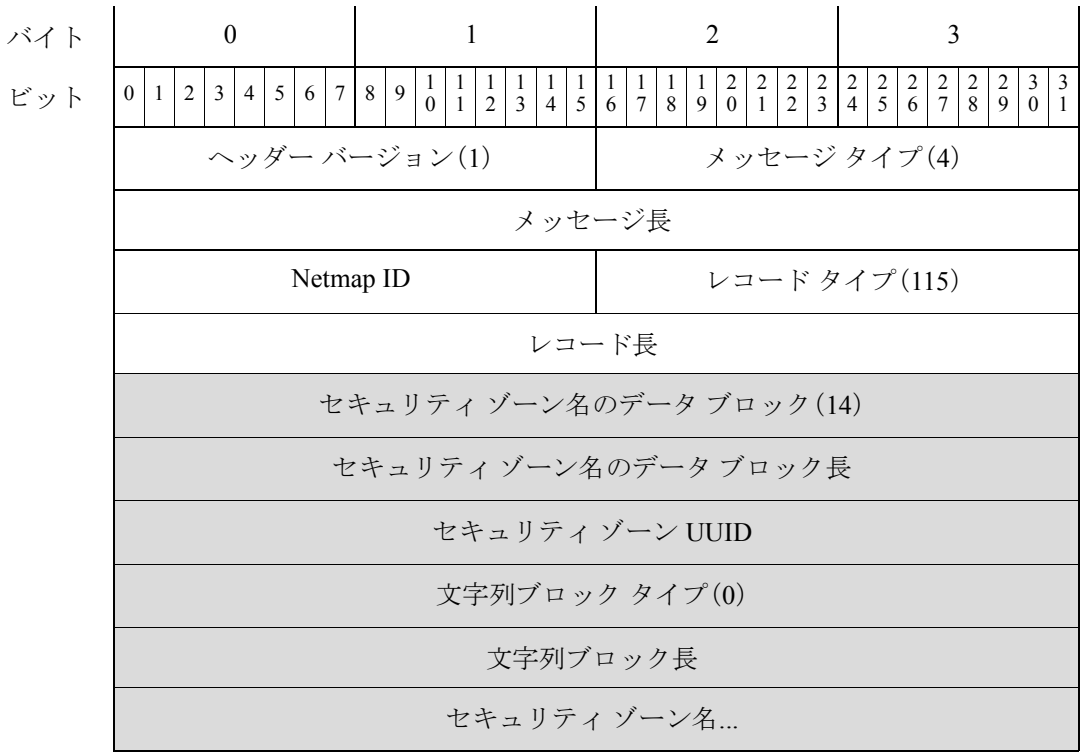
次の表は、イベント追加データのメタデータのレコードのフィールドについての説明です。

表 3-12　イベント追加データのメタデータのデータ ブロック フィールド

フィールド	データ タイプ	説明
イベント追加データのメタデータのデータ ブロック タイプ	uint32	イベント追加データのメタデータのデータ ブロックを開始します。この値は常に 5 です。このブロック タイプは、シリーズ 2 ブロックです。
イベント追加データのメタデータのデータ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
タイプ	uint32	追加データのタイプ。関連付けられたイベント追加データ レコードのタイプ フィールドと一致します。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。このブロック タイプは、シリーズ 2 ブロックです。
文字列ブロック長	uint32	クライアントアプリケーションのバージョンの文字列データ ブロックのバイト数です。文字列ブロック タイプとブロック長フィールドの 8 バイトとバージョン文字列のバイト数が含まれます。
名前	string	イベント追加データのタイプ名（たとえば、XFF クライアント（IPv6）、HTTP URI）。
文字列ブロック タイプ	uint32	クライアント アプリケーション URL の文字列データ ブロックを開始します。この値は常に 0 です。このブロック タイプは、シリーズ 2 ブロックです。
文字列ブロック長	uint32	クライアント アプリケーション URL の文字列データ ブロックのバイト数です。文字列ブロック タイプとブロック長フィールドの 8 バイトと URL 文字列のバイト数が含まれます。
エンコーディング	string	イベント追加データで使用されるエンコーディング（たとえば、IPv4、IPv6、または文字列）。

セキュリティ ゾーン名レコード

eStreamer サービスは、セキュリティ ゾーン名レコード内の侵入イベントまたは接続イベントに関連付けられたセキュリティ ゾーンの名前の情報を含むメタデータを送信します。形式は次のとおりです。（バージョン 4 のメタデータ フラグ（要求メッセージの [要求フラグ（Request Flags）] フィールドのビット 20）が設定されていると、セキュリティ ゾーン情報が送信されます。要求フラグ（2-12 ページ） を参照してください）。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにセキュリティ ゾーン名レコードを示す値 115 があることに注意してください。シリーズ 2 セットのデータ ブロックのブロック タイプ 14 の UUID 文字列データ ブロックが含まれています。



次の表は、セキュリティ ゾーン名のデータ ブロックのフィールドについての説明です。

表 3-13　セキュリティ ゾーンの名のデータ ブロック フィールド

フィールド	データ タイプ	説明
セキュリティ ゾーン名のデータ ブロック タイプ	uint32	セキュリティ ゾーン名のデータ ブロックを開始します。この値は常に 14 です。ブロック タイプは、シリーズ 2 ブロックです。
セキュリティ ゾーン名のデータ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
セキュリティ ゾーン UUID	uint8[16]	接続イベントに関連付けられたセキュリティ ゾーンの固有識別子。
文字列ブロック タイプ	uint32	セキュリティ ゾーンの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	セキュリティ ゾーン名の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとこの名前のバイト数が含まれます。
セキュリティ ゾーン名	string	セキュリティ ゾーン名。

インターフェイス名レコード

eStreamer サービスは、インターフェイス名レコード内の侵入イベントまたは接続イベントに関連付けられたインターフェイスの名前の情報を含むメタデータを送信します。形式は次のとおりです。(バージョン 4 のメタデータ フラグ(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 20)が設定されていると、インターフェイス名の情報が送信されます。要求フラグ(2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにインターフェイス名レコードを示す値 116 があることに注意してください。シリーズ 2 セットのデータ ブロックのブロック タイプ 14 の UUID 文字列データ ブロックが含まれています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(116)															
レコード長																																
インターフェイス名のデータ ブロック(14)																																
インターフェイス名のデータ ブロック長																																
インターフェイス UUID																																
文字列ブロック タイプ(0)																																
文字列ブロック長																																
インターフェイス名...																																

次の表は、インターフェイス名のデータ ブロックのフィールドについての説明です。

表 3-14　インターフェイス名のデータ ブロック フィールド

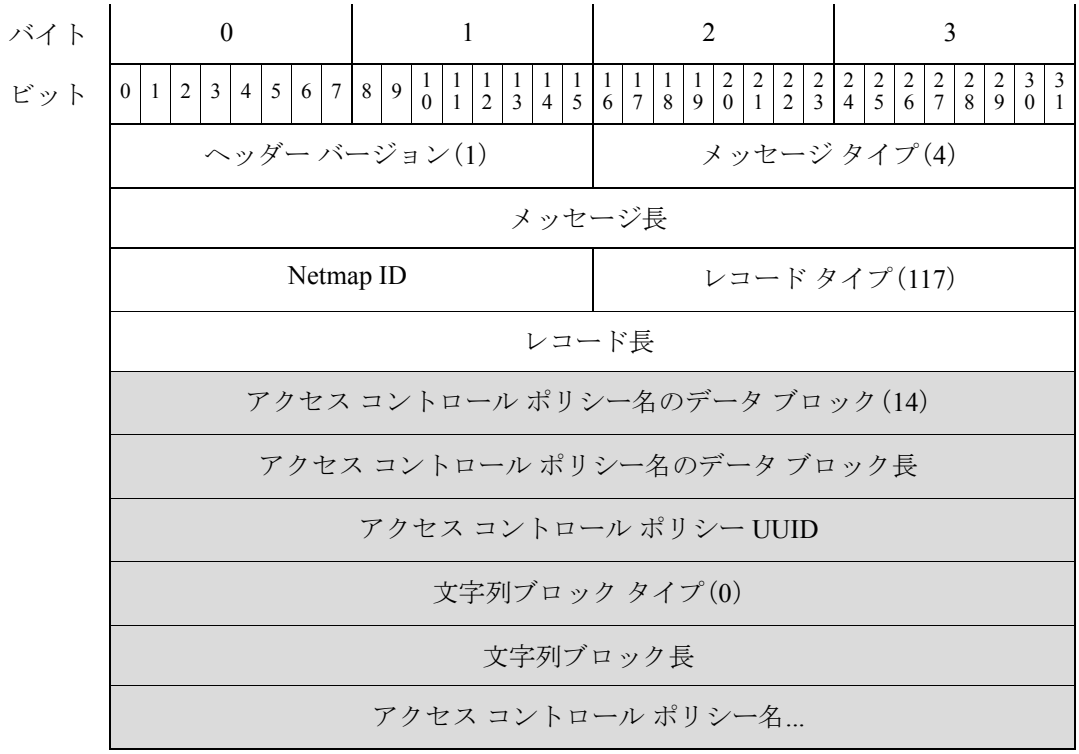
フィールド	データ タイプ	説明
インターフェイス名のデータ ブロック タイプ	uint32	インターフェイス名のデータ ブロックを開始します。この値は常に 14 です。ブロック タイプは、シリーズ 2 ブロックです。
インターフェイス名のデータ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
インターフェイス UUID	uint8[16]	接続イベントに関連付けられたインターフェイスの固有識別子として機能するインターフェイス ID 番号。

表 3-14　インターフェイス名のデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	インターフェイスの名前を含む文字列データのブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	インターフェイス名の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとインターフェイス名のバイト数が含まれます。
インターフェイス名	string	インターフェイス名。

アクセス コントロール ポリシー名のレコード

eStreamer サービスは、アクセス コントロール ポリシー名レコード内の侵入イベントまたは接続イベントをトリガーしたアクセス コントロール ポリシーの名前に関するメタデータを送信します。形式は次のとおりです。(バージョン 4 のメタデータ フラグ(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 20)が設定されていると、アクセス コントロール ポリシー名の情報が送信されます。要求フラグ(2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにアクセス コントロール ポリシー名レコードを示す値 117 があることに注意してください。シリーズ 2 セットのデータ ブロックのブロック タイプ 14 の UUID 文字列データ ブロックが含まれています。



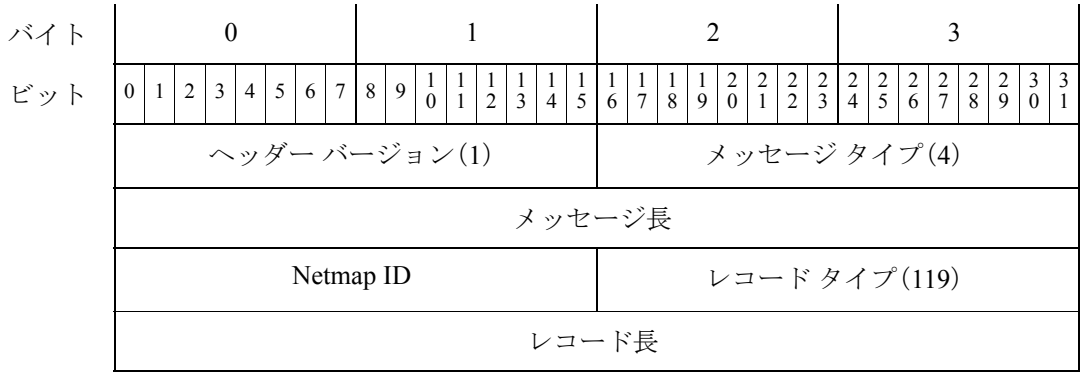
次の表は、アクセス コントロール ポリシー名のデータ ブロックのフィールドについての説明です。

表 3-15　アクセス コントロール ポリシー名のデータ ブロック フィールド

フィールド	データ タイプ	説明
アクセス コントロール ポリシー名のデータ ブロック タイプ	uint32	アクセス コントロール ポリシー名のデータ ブロックを開始します。この値は常に 14 です。ブロック タイプは、シリーズ 2 ブロックです。
アクセス コントロール ポリシー名のデータ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
アクセス コントロール ポリシー UUID	uint8[16]	侵入イベントまたは接続イベントに関連付けられたアクセス コントロール ポリシーの固有識別子として機能する ID 番号
文字列ブロック タイプ	uint32	アクセス コントロール ポリシーの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	アクセス コントロール ポリシー名の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとアクセス コントロール ポリシー名のバイト数が含まれます。
アクセス コントロール ポリシー名	string	アクセス コントロール ポリシー名。

アクセス コントロール ルール ID レコードのメタデータ

eStreamer サービスは、アクセス コントロール ルール ID レコード内の侵入イベントまたは接続イベントをトリガーしたアクセス コントロール ルールの情報を含むメタデータを送信します。形式は次のとおりです。（バージョン 4 のメタデータ フラグ（要求メッセージの [要求フラグ（Request Flags）] フィールドのビット 20）が設定されていると、アクセス コントロール ルールのメタデータが送信されます。要求フラグ（2-12 ページ） を参照してください）。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにアクセス コントロール ルール ID レコードを示す値 119 があることに注意してください。シリーズ 2 セットのデータ ブロックのブロック タイプ 15 のルール ID データ ブロックが含まれています。



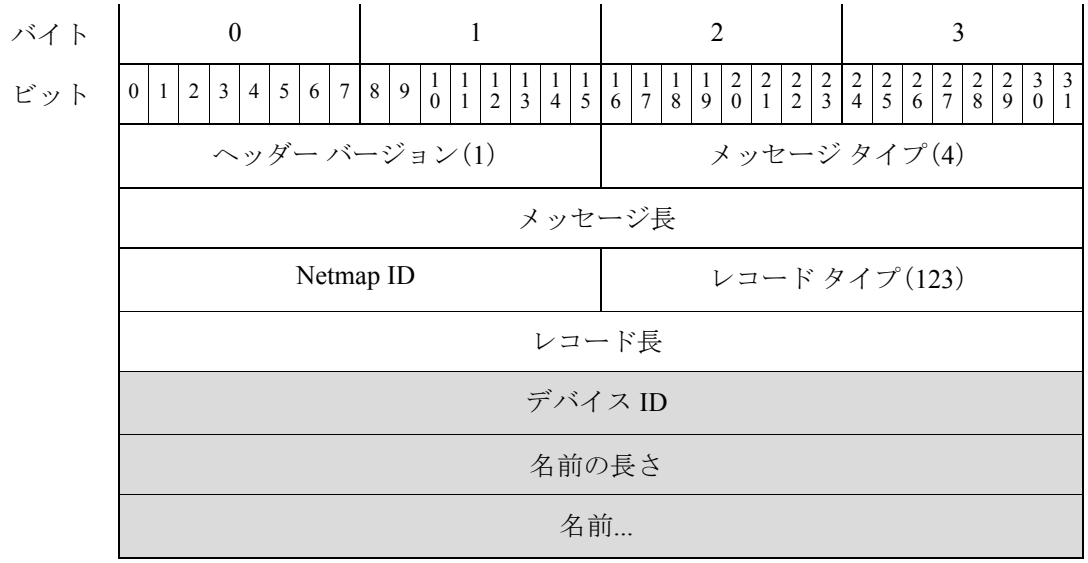
次の表は、アクセス コントロール ルール ID のデータ ブロックのフィールドについての説明です。

表 3-16　アクセス コントロール ルール ID のデータ ブロック フィールド

フィールド	データ タイプ	説明
アクセス コントロール ルール ID のデータ ブロック タイプ	uint32	アクセス コントロール ルール ID のデータ ブロックを開始します。この値は常に 15 です。ブロック タイプは、シリーズ 2 ブロックです。
アクセス コントロール ルール ID のデータ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
アクセス コントロール ルール UUID	uint8[16]	接続イベントに関連付けられたアクセス コントロール ポリシーのルールの固有識別子として機能するルール ID。
アクセス コントロール ルール ID	uint32	接続イベントに関連付けられたアクセス コントロール ポリシーのルールの内部 ID。
文字列ブロック タイプ	uint32	アクセス コントロール ルールの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとルール名のバイト数が含まれます。
アクセス コントロール ルール名	string	アクセス コントロール ルールの名前。

管理対象 デバイス レコードのメタデータ

eStreamer サービスは、管理対象 デバイス レコード内の侵入イベントに関連付けられた管理対象デバイスの情報を含むメタデータを送信します。形式は次のとおりです。(バージョン 4 のメタデータ フラグ(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 20)が設定されていると、管理対象デバイスのメタデータが送信されます。要求フラグ (2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに管理対象 デバイス レコードを示す値 123 があることに注意してください。



次の表は、管理対象 デバイス レコードのフィールドについての説明です。

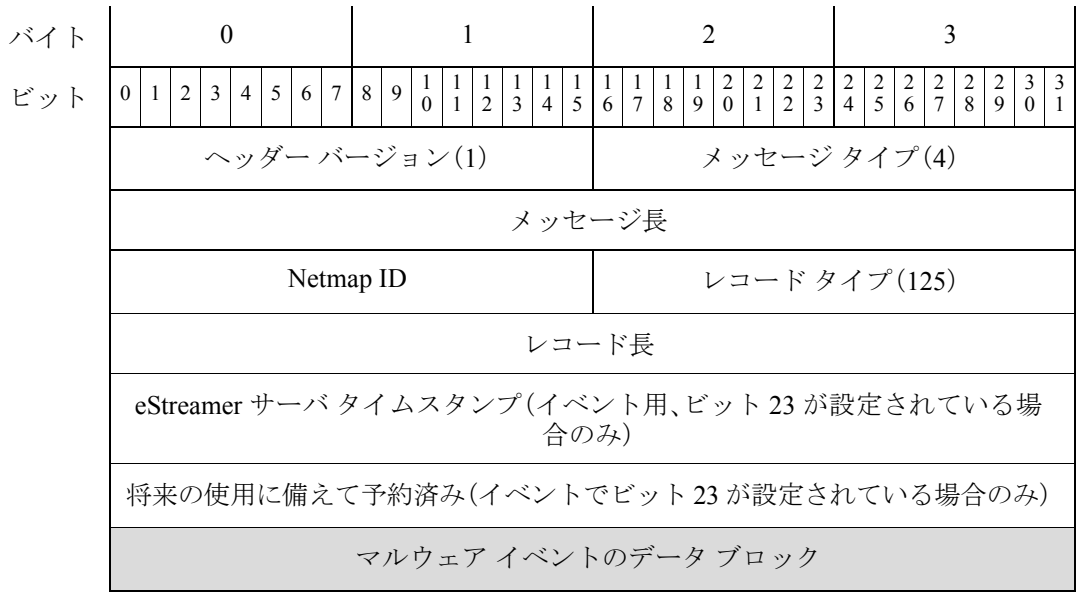
表 3-17　管理対象 デバイス レコード フィールド

フィールド	データ タイプ	説明
デバイス ID	uint32	管理対象デバイス ID 番号。
名前の長さ	uint32	名前に含まれるバイト数。
名前	string	管理対象デバイス名。

マルウェア イベント レコード 5.1.1 以上

マルウェア イベント レコードのフィールドは、次の図で網掛けされています。レコード タイプは 125 です。

イベント バージョンが 2 でイベント コードが 101 の要求メッセージでマルウェア イベント フラグ([要求フラグ(Request Flags)] フィールドのビット 30)を設定することで、マルウェア イベント レコードを要求します。要求フラグ (2-12 ページ)を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。シリーズ 2 セットのデータ ブロックのブロック タイプ 24、33、35、44、47 のいずれかのマルウェア イベントのデータ ブロックが含まれています。



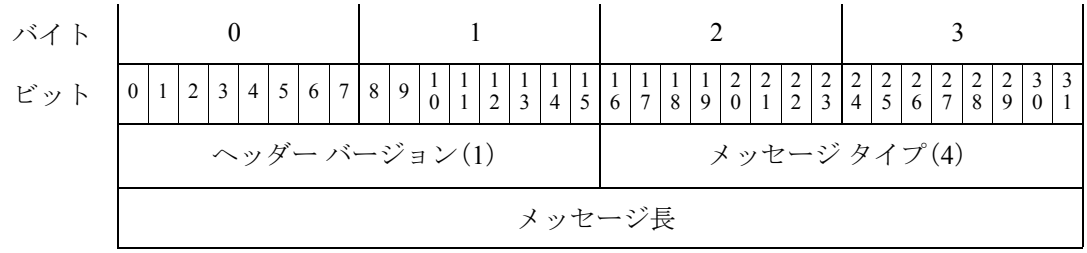
次の表は、各マルウェア イベント レコード データ フィールドについての説明です。

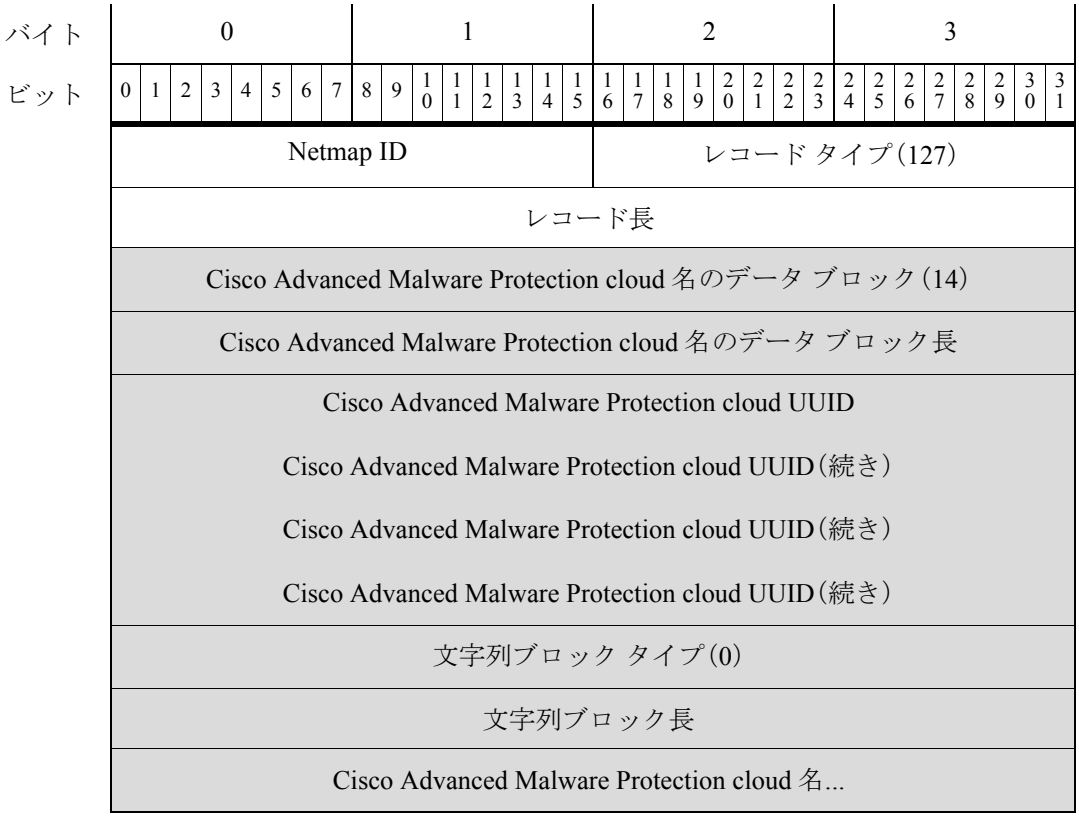
表 3-18　マルウェア イベント レコード フィールド

フィールド	データ タイプ	説明
マルウェア イベントのデータ ブロック	変数	マルウェア イベントのデータ ブロックを示します。詳細については、マルウェア イベントのデータ ブロック 6.0 以上(3-94 ページ)を参照してください。

Cisco Advanced Malware Protection クラウド名のメタデータ

eStreamer サービスは、Cisco Advanced Malware Protection cloud 名レコード内の侵入イベントまたは接続イベントに関連付けられた Cisco Advanced Malware Protection cloud(Cisco Advanced Malware Protection cloud または単にクラウドと呼ばれます)の名前の情報を含むメタデータを送信します。形式は次のとおりです。(バージョン 4 のメタデータ フラグ(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 20)が設定されていると、AMP cloud 名の情報が送信されます。要求フラグ(2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに Cisco Advanced Malware Protection cloud 名のレコードを示す値 127 があることに注意してください。シリーズ 2 セットのデータ ブロックのブロック タイプ 14 の UUID 文字列データ ブロックが含まれています。





次の表は、Cisco Advanced Malware Protection cloud 名のデータ ブロックのフィールドについての説明です。

表 3-19　Cisco Advanced Malware Protection cloud 名のデータ ブロック フィールド

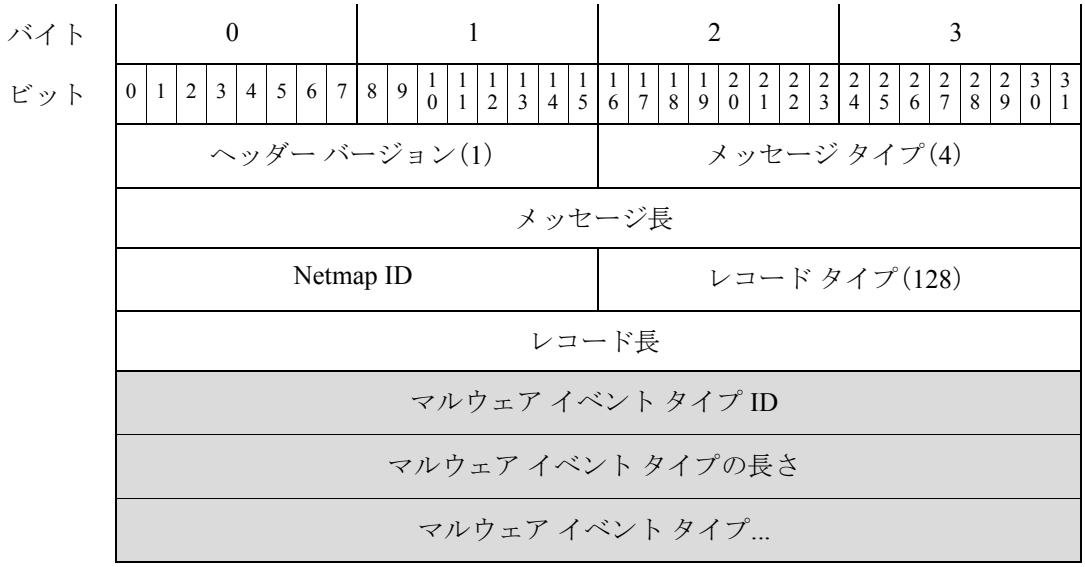
フィールド	データ タイプ	説明
Cisco Advanced Malware Protection cloud 名のデータ ブロック タイプ	uint32	Cisco Advanced Malware Protection cloud 名のデータ ブロックを開始します。この値は常に 14 です。ブロック タイプは、シリーズ 2 ブロックです。
Cisco Advanced Malware Protection cloud 名のデータ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
Cisco Advanced Malware Protection cloud UUID	uint8[16]	接続イベントに関連付けられた Cisco Advanced Malware Protection cloud の固有識別子として機能する Cisco Advanced Malware Protection cloud ID 番号。
文字列ブロック タイプ	uint32	Cisco Advanced Malware Protection cloud の名前を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 3-19　Cisco Advanced Malware Protection cloud 名のデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	Cisco Advanced Malware Protection cloud 名のデータ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと Cisco Advanced Malware Protection cloud 名のバイト数が含まれます。
Cisco Advanced Malware Protection cloud 名	string	Cisco Advanced Malware Protection cloud 名。

マルウェア イベント タイプのメタデータ

eStreamer サービスは、マルウェア イベント タイプ レコード内のイベントのマルウェア イベント タイプ情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグ(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 20)が設定されると、マルウェア イベント タイプ情報が送信されます。要求フラグ(2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにマルウェア イベント タイプ レコードを示す値 128 があることに注意してください。



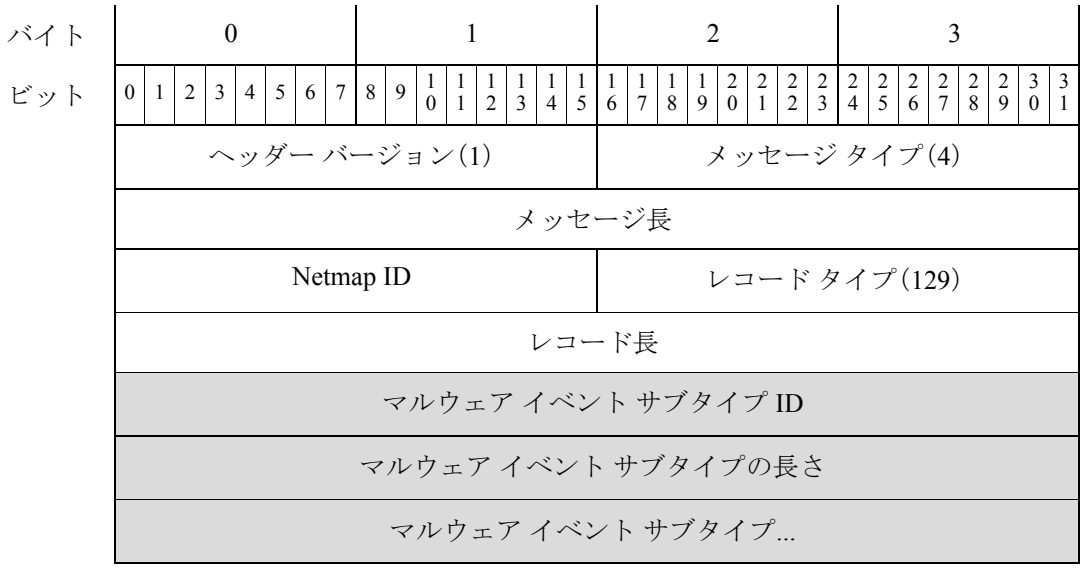
次の表は、マルウェア イベント タイプ レコードのフィールドについての説明です。

表 3-20　マルウェア イベント タイプ レコード フィールド

フィールド	データ タイプ	説明
マルウェア イベント タイプ ID	uint32	マルウェア イベント タイプ ID 番号。
マルウェア イベント タイプの長さ	uint32	マルウェア イベント タイプに含まれるバイト数。
マルウェア イベント タイプ	string	マルウェア イベントのタイプ。

マルウェア イベント サブタイプのメタデータ

eStreamer サービスは、マルウェア イベント サブタイプ レコード内のイベントのマルウェア イベント サブタイプ情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグ(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 20)が設定されると、マルウェア イベント タイプ情報が送信されます。要求フラグ (2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにマルウェア イベント サブタイプ レコードを示す値 129 があることに注意してください。



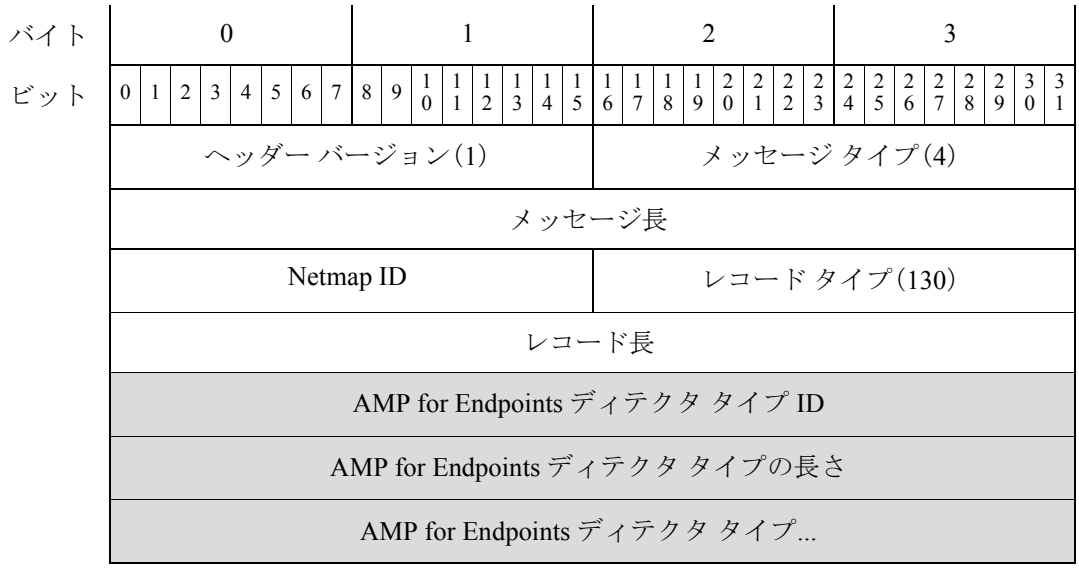
次の表は、マルウェア イベント サブタイプ レコードのフィールドについての説明です。

表 3-21　マルウェア イベント サブタイプ レコード フィールド

フィールド	データ タイプ	説明
マルウェア イベント サブタイプ ID	uint32	マルウェア イベント サブタイプ ID 番号。
マルウェア イベント サブタイプの長さ	uint32	マルウェア イベント サブタイプに含まれるバイト数。
マルウェア イベント サブタイプ	string	マルウェア イベントのサブタイプ。

AMP for Endpoints ディテクタ タイプのメタデータ

eStreamer サービスは、AMP for Endpoints ディテクタ タイプ レコード内のイベントの AMP for Endpoints ディテクタ タイプ情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグのいずれか(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 1、14、15、または 20)が設定されていると、AMP for Endpoints ディテクタ タイプ情報が送信されます。要求フラグ(2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに AMP for Endpoints ディテクタ タイプ レコードを示す値 130 があることに注意してください。



次の表は、AMP for Endpoints ディテクタ タイプ レコードのフィールドについての説明です。

表 3-22　AMP for Endpoints ディテクタ タイプ レコード フィールド

フィールド	データ タイプ	説明
AMP for Endpoints ディテクタ タイプ ID	uint32	AMP for Endpoints ディテクタ タイプ ID 番号。
AMP for Endpoints ディテクタ タイプの長さ	uint32	AMP for Endpoints ディテクタ タイプに含まれるバイト数。
AMP for Endpoints ディテクタ タイプ	string	AMP for Endpoints ディテクタのタイプ。

AMP for Endpoints ファイル タイプのメタデータ

eStreamer サービスは、AMP for Endpoints ファイル タイプ レコード内のイベントの AMP for Endpoints ファイル タイプ情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグのいずれか(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 1、14、15、または 20)が設定されていると、AMP for Endpoints ファイル タイプ情報が送信されます。要求フラグ (2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに AMP for Endpoints ファイル タイプ レコードを示す値 131 があることに注意してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(131)															
レコード長																																
AMP for Endpoints ファイル タイプ ID																																
AMP for Endpoints ファイル タイプの長さ																																
AMP for Endpoints ファイル タイプ...																																

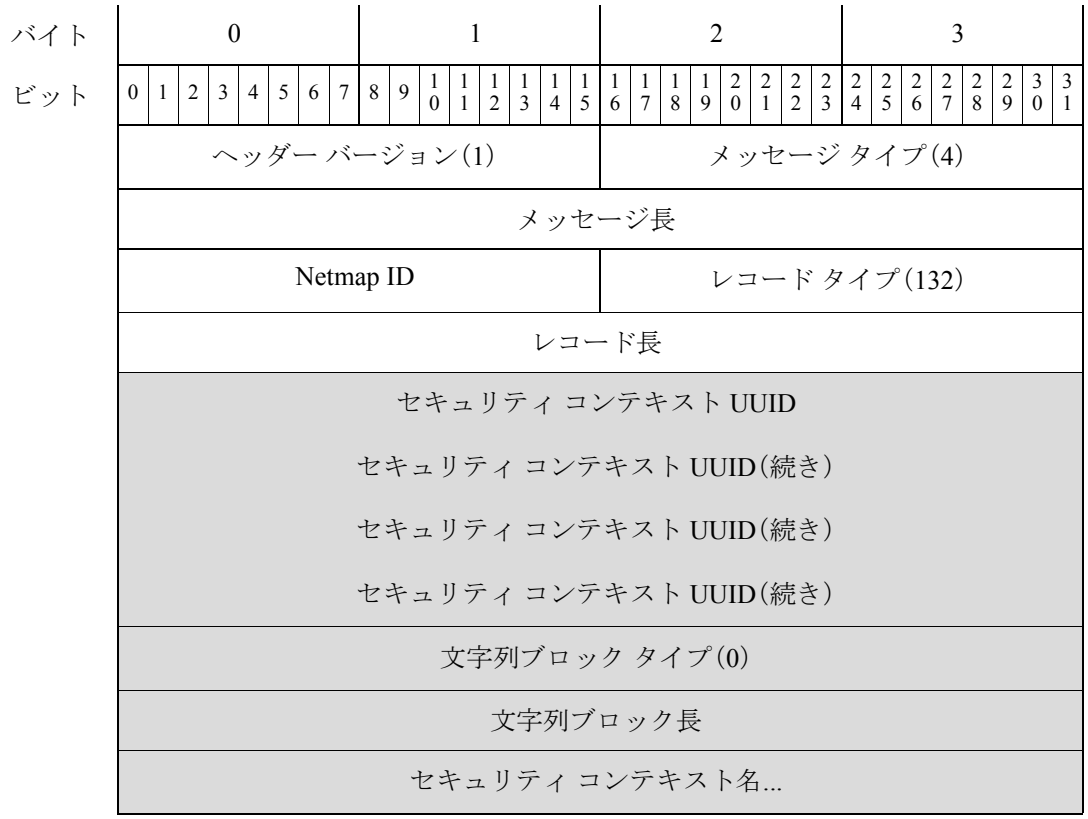
次の表は、AMP for Endpoints ファイル タイプ レコードのフィールドについての説明です。

表 3-23　AMP for Endpoints ファイル タイプ レコード フィールド

フィールド	データ タイプ	説明
AMP for Endpoints ファイル タイプ ID	uint32	AMP for Endpoints ファイル タイプ ID 番号。
AMP for Endpoints ファイル タイプの長さ	uint32	AMP for Endpoints ファイル タイプに含まれるバイト数。
AMP for Endpoints ファイル タイプ	string	検出されたファイルのタイプ。

セキュリティ コンテキスト名

eStreamer サービスは、セキュリティ コンテキスト名の情報を含むメタデータを送信します。形式は次のとおりです。（メタデータ フラグのいずれか（要求メッセージの [要求フラグ（Request Flags）] フィールドのビット 1、14、15、または 20）が設定されていると、セキュリティ コンテキスト名の情報が送信されます。要求フラグ（2-12 ページ） を参照してください）。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにセキュリティ コンテキスト名レコードを示す値 132 があることに注意してください。



次の表は、セキュリティ コンテキスト名のレコードのフィールドについての説明です。

表 3-24　セキュリティ コンテキスト名のレコード フィールド

フィールド	データ タイプ	説明
セキュリティ コンテキスト UUID	uint8[16]	セキュリティ コンテキストの UUID
文字列ブロック タイプ	uint32	セキュリティ コンテキストの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	セキュリティ コンテキスト名の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとセキュリティ コンテキスト名のバイト数が含まれます。
セキュリティ コンテキスト名	string	セキュリティ コンテキスト名。

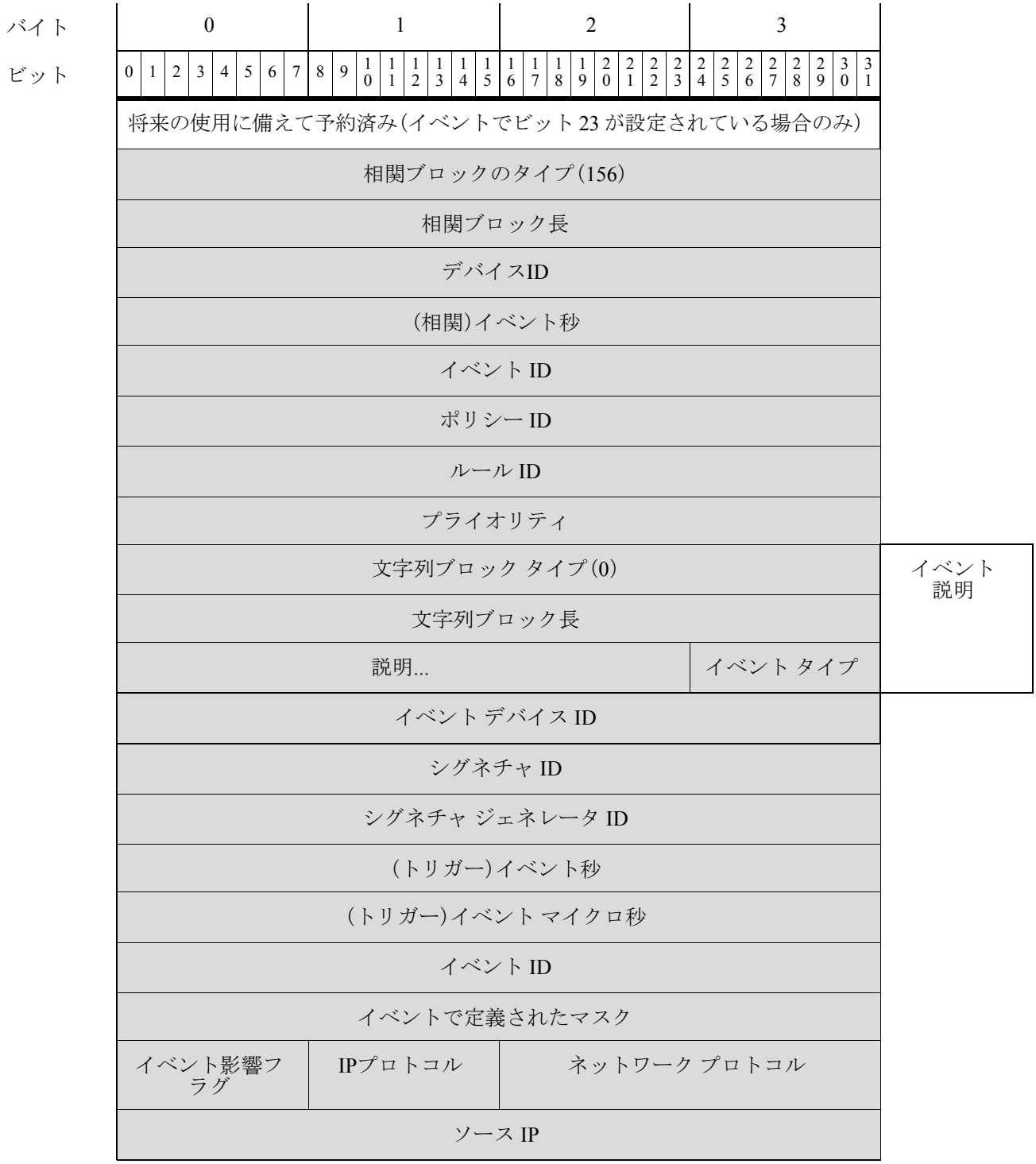
5.4 以上の相関イベント

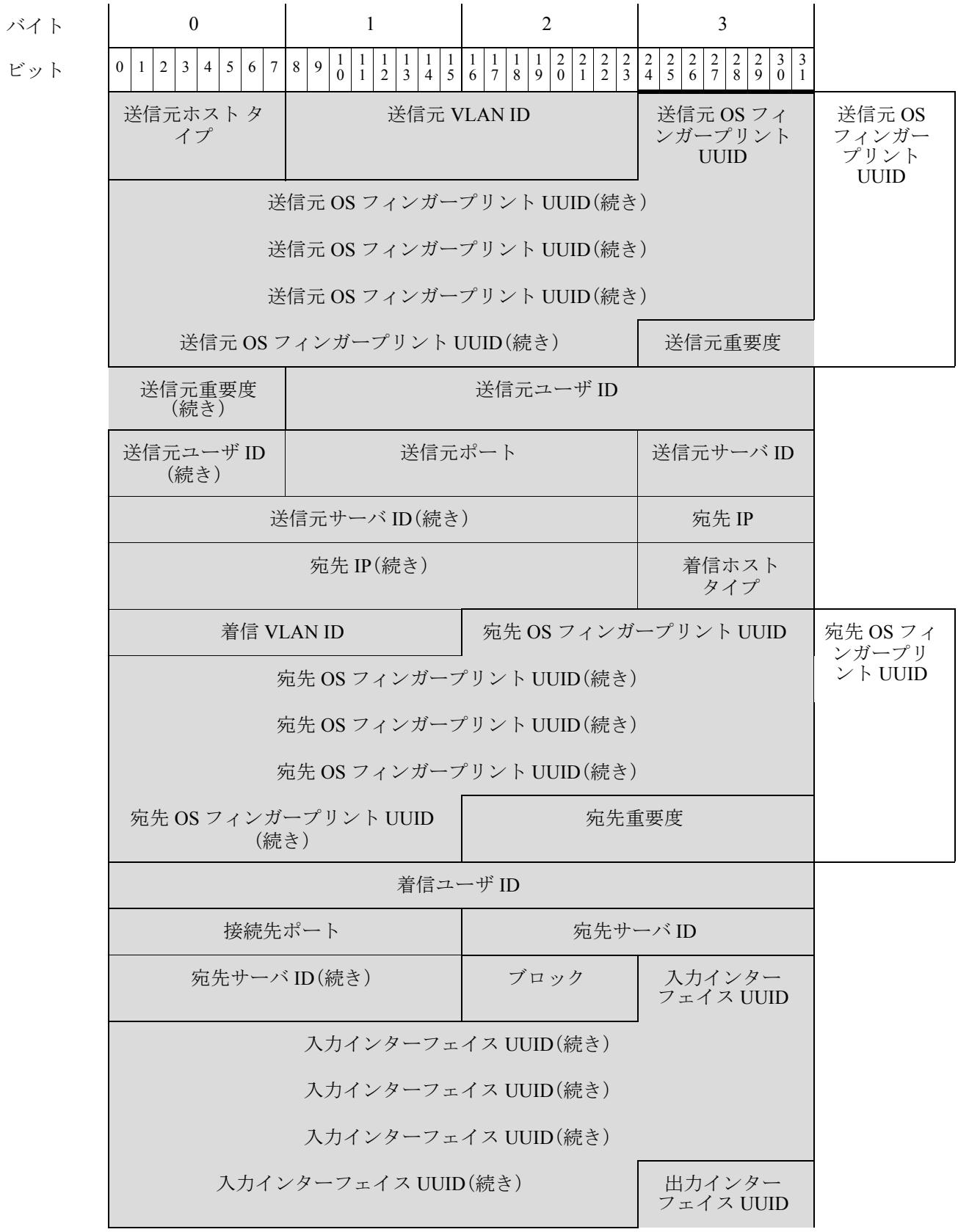
相関イベント（5.0 よりも前のバージョンではコンプライアンス イベントと呼ばれていた）には、相関ポリシー違反に関する情報が含まれます。このメッセージは、標準的な eStreamer メッセージ ヘッダーを使用するため、レコード タイプ 112 を指定します。シリーズ 1 セットのデータ ブロックのタイプ 156 の相関データ ブロックが後に続きます。データ ブロック タイプ 156 は、IPv6 サポートを含む先行オペレーション（ブロック タイプ 128）とは異なります。

バージョン 5.4 以上の相関イベントには、位置情報、セキュリティ インテリジェンス、および SSL サポートのフィールド新たに加わります。

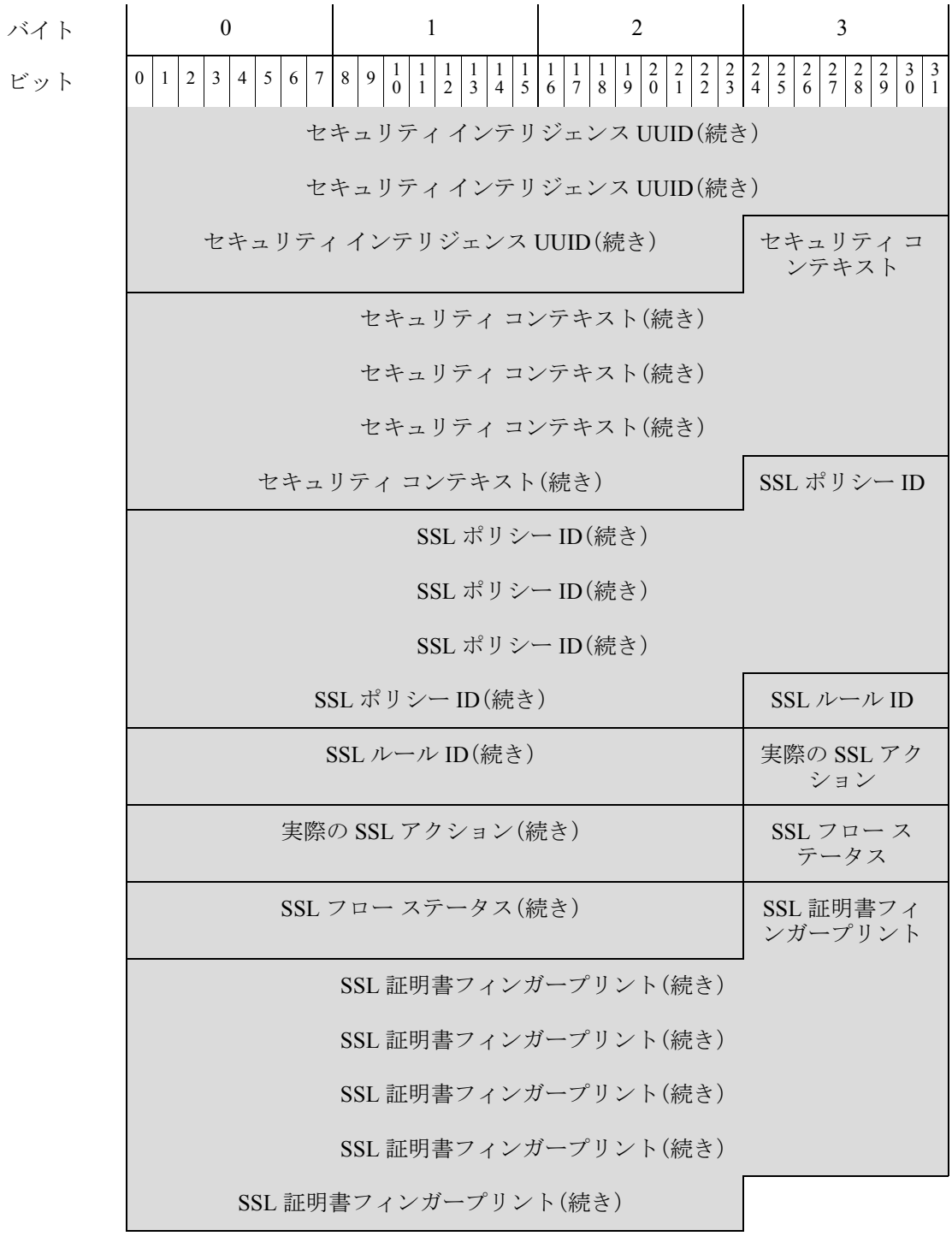
ストリーム要求メッセージでイベント タイプ コード 31 とバージョン コード 9 を要求する拡張要求によってのみ、eStreamer から 5.4 以上の相関イベントを要求できます（拡張要求の送信の詳細については、拡張要求の送信（2-4 ページ）を参照してください）。オプションで、最初のイベント ストリーム要求メッセージのフラグ フィールドでビット 23 を有効にして、拡張イベント ヘッダーを含めることができます。また、フラグ フィールドでビット 20 を有効にして、ユーザ メタデータを含めることもできます。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（112）															
レコード長																																
eStreamer サーバ タイムスタンプ（イベント用、ビット 23 が設定されている場合のみ）																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)
相関ブロックのタイプ(156)
相関ブロック長
デバイスID
(相関)イベント秒
イベント ID
ポリシー ID
ルール ID
プライオリティ
文字列ブロック タイプ(0)
文字列ブロック長
説明...
イベント タイプ
イベント デバイス ID
シグネチャ ID
シグネチャ ジェネレータ ID
(トリガー)イベント秒
(トリガー)イベント マイクロ秒
イベント ID
イベントで定義されたマスク
イベント影響フラグ
IPプロトコル
ネットワーク プロトコル
ソース IP
イベント説明


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
送信元ホスト タイプ
送信元 VLAN ID
送信元 OS フィンガープリント UUID
送信元 OS フィンガープリント UUID
送信元 OS フィンガープリント UUID（続き）
送信元 OS フィンガープリント UUID（続き）
送信元 OS フィンガープリント UUID（続き）
送信元 OS フィンガープリント UUID（続き）
送信元重要度
送信元重要度（続き）
送信元ユーザ ID
送信元ユーザ ID（続き）
送信元ポート
送信元サーバ ID
送信元サーバ ID（続き）
宛先 IP
宛先 IP（続き）
着信ホスト タイプ
着信 VLAN ID
宛先 OS フィンガープリント UUID
宛先 OS フィンガープリント UUID
宛先 OS フィンガープリント UUID（続き）
宛先 OS フィンガープリント UUID（続き）
宛先 OS フィンガープリント UUID（続き）
宛先 OS フィンガープリント UUID（続き）
宛先重要度
着信ユーザ ID
接続先ポート
宛先サーバ ID
宛先サーバ ID（続き）
ブロック
入力インターフェイス UUID
入力インターフェイス UUID（続き）
入力インターフェイス UUID（続き）
入力インターフェイス UUID（続き）
入力インターフェイス UUID（続き）
出力インターフェイス UUID


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
出力インターフェイス UUID（続き）
出力インターフェイス UUID（続き）
出力インターフェイス UUID（続き）
出力インターフェイス UUID（続き）
入力ゾーン UUID
入力ゾーン UUID
入力ゾーン UUID（続き）
入力ゾーン UUID（続き）
入力ゾーン UUID（続き）
出力ゾーン UUID
出力ゾーン UUID
出力ゾーン UUID（続き）
出力ゾーン UUID（続き）
出力ゾーン UUID（続き）
送信元 IPv6 アドレス
送信元 IPv6 アドレス
送信元 IPv6 アドレス（続き）
送信元 IPv6 アドレス（続き）
送信元 IPv6 アドレス（続き）
宛先 IPv6 アドレス
宛先 IPv6 アドレス
宛先 IPv6 アドレス（続き）
宛先 IPv6 アドレス（続き）
宛先 IPv6 アドレス（続き）
送信元の国
送信元の国（続き）
宛先の国
SI UUID
セキュリティ インテリジェンス UUID（続き）



レコード構造には、シリーズ 1 のブロックである、文字列ブロック タイプが含まれることに注目してください。シリーズ 1 ブロックの詳細については、ディスカバリ（シリーズ1）ブロック（4-63 ページ）を参照してください。

表 3-25　相関イベント 5.4 以上のデータ フィールド

フィールド	データ タイプ	説明
相関ブロック タイプ	uint32	相関イベント データ ブロックが続くことを示します。このフィールドの値は常に 156 です。ディスカバリ（シリーズ1）ブロック（4-63 ページ）を参照してください。
相関ブロック長	uint32	相関データ ブロック長（相関ブロック タイプと長さの 8 バイト、およびそれに続く相関データを含む）。
デバイスID	uint32	相関イベントを生成した管理対象デバイスまたは Management Center の内部 ID 番号。ゼロ値は Management Center を示します。バージョン 3 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ（3-38 ページ）を参照してください。
（相関）イベント秒	uint32	相関イベントが生成された時刻を示す UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
イベント ID	uint32	相関イベント ID 番号。
ポリシー ID	uint32	違反された相関ポリシーの ID 番号。データベースからポリシー ID 番号を取得する方法の詳細については、サーバ レコード（4-16 ページ）を参照してください。
ルール ID	uint32	トリガーしてポリシー違反となった相関ルールの ID 番号。データベースからポリシー ID 番号を取得する方法の詳細については、サーバ レコード（4-16 ページ）を参照してください。
プライオリティ	uint32	イベントに割り当てられた優先順位。これは、0 ～ 5 の整数値です。
文字列ブロック タイプ	uint32	相関違反イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、文字列データ ブロック（4-74 ページ）を参照してください。
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数（文字列のブロック タイプのための 4 バイト、文字列ブロック長のための 4 バイト、説明のバイト数を含む）。
説明	string	相関イベントについての説明。
イベント タイプ	uint8	相関イベントが、侵入、ホスト検出、またはユーザ イベントによってトリガーされたかどうかを示します。 • 1：侵入 • 2：ホストの検出 • 3：ユーザ
イベント デバイス ID	uint32	相関イベントをトリガーしたイベントを生成したデバイスの ID 番号。バージョン 3 メタデータを要求するとデバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ（3-38 ページ）を参照してください。
シグネチャ ID	uint32	イベントが侵入イベントであった場合、イベントに対応するルール ID 番号を示します。そうでない場合、この値は 0 になります。
シグネチャ ジェネレータ ID	uint32	イベントが侵入イベントであった場合、イベントを生成した Firepower システム プリプロセッサまたはルール エンジンの ID 番号を示します。

表 3-25　相関イベント 5.4 以上のデータ フィールド(続き)

フィールド	データ タイプ	説明
(トリガー)イベント秒	uint32	相関ポリシー ルールをトリガーしたイベントの時刻を示す UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
(トリガー)イベント マイクロ秒	uint32	イベントが検出されたタイムスタンプの、マイクロ秒(100 万分の 1 秒)の増分。
イベント ID	uint32	シスコ デバイスによって生成されたイベントの ID 番号。
イベントで定義されたマスク	bits[32]	このフィールドに設定されたビットは、メッセージ内の続くどのフィールドが有効であるかを示します。各ビット値のリストの詳細については、表 3-23 (3-45 ページ) を参照してください。
イベント影響フラグ	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) 次の影響レベル値は、Management Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • グレー(0、不明):`00X00000` • 赤(1、脆弱):`xxxx1xxx`, `xxx1xxxx`, `x1xxxxxx`, `1xxxxxxx`(バージョン 5.0+ のみ) • オレンジ(2、潜在的に脆弱):`00X0011X` • 黄(3、現在は脆弱でない):`00X0001X` • 青(4、不明なターゲット):`00X00001`
IPプロトコル	uint8	イベントに関連付けられている IP プロトコルの ID(該当する場合)。
ネットワーク プロトコル	uint16	イベントに関連付けられているネットワーク プロトコル(該当する場合)。

表 3-25　相関イベント 5.4 以上のデータ フィールド(続き)

フィールド	データ タイプ	説明
送信元 IP アドレス	uint8 [4]	このフィールドは予約済みですが、設定されておりません。送信元 IPv4 アドレスは、送信元 IPv6 アドレス フィールドに保存されます。詳細については、IP アドレス(1-6 ページ)を参照してください。
送信元ホスト タイプ	uint8	送信元ホストのタイプ: • 0:ホスト • 1:ルータ • 2:ブリッジ
送信元 VLAN ID	uint16	送信元ホストの VLAN ID 番号(該当する場合)。
送信元 OS フィンガープリント UUID	uint8 [16]	送信元ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID。 フィンガープリント ID にマップする値の取得の詳細については、サーバ レコード(4-16 ページ)を参照してください。
送信元重要度	uint16	送信元ホストの、ユーザ定義の重要度値: • 0:なし • 1:低 • 2:中 • 3:高
送信元ユーザ ID	uint32	システムにより識別される、送信元ホストにログインしたユーザの ID 番号。
送信元ポート	uint16	イベントの送信元ポート。
送信元サーバ ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
宛先IPアドレス	uint8 [4]	このフィールドは予約済みですが、設定されておりません。宛先 IPv4 アドレスは、宛先 IPv6 アドレス フィールドに保存されます。詳細については、IP アドレス(1-6 ページ)を参照してください。
宛先ホスト タイプ	uint8	宛先ホストのタイプ: • 0:ホスト • 1:ルータ • 2:ブリッジ
宛先 VLAN ID	uint16	宛先ホストの VLAN ID 番号(該当する場合)。
宛先 OS フィンガープリント UUID	uint8 [16]	宛先ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID 番号。 フィンガープリント ID にマップする値の取得の詳細については、サーバ レコード(4-16 ページ)を参照してください。
宛先重要度	uint16	宛先ホストの、ユーザ定義の重要度値: • 0:なし • 1:低 • 2:中 • 3:高

表 3-25　相関イベント 5.4 以上のデータ フィールド(続き)

フィールド	データ タイプ	説明
宛先ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
接続先ポート	uint16	イベントの宛先ポート。
宛先サービス ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
ブロック	uint8	侵入イベントをトリガーしたパケットの処理を示す値。 • 0:侵入イベントがドロップされていない • 1:侵入イベントがドロップされている(展開がインライン型、スイッチ型、またはルーティング型である場合はドロップ) • 2:侵入ポリシーが、インライン型、スイッチ型、またはルーティング型展開のデバイスに適用されている場合は、イベントをトリガーしたパケットがドロップされている可能性がある。
入力インターフェイス UUID	uint8 [16]	相関イベントに関連付けられている入力インターフェイスの固有識別子として機能するインターフェイス ID。
出力インターフェイス UUID	uint8 [16]	相関イベントに関連付けられている出力インターフェイスの固有識別子として機能するインターフェイス ID。
入力ゾーン UUID	uint8 [16]	相関イベントに関連付けられている入力セキュリティ ゾーンの固有識別子として機能するゾーン ID。
出力ゾーン UUID	uint8 [16]	相関イベントに関連付けられている出力セキュリティ ゾーンの固有識別子として機能するゾーン ID。
送信元 IPv6 アドレス	uint8 [16]	IPv6 アドレス オクテットの、イベントの送信元ホストの IP アドレス。
宛先 IPv6 アドレス	uint8 [16]	IPv6 アドレス オクテットの、イベントの宛先ホストの IP アドレス。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
セキュリティ インテリジェンス UUID	uint8 [16]	セキュリティ インテリジェンスに設定されたアクセス コントロール ポリシーの UUID。
セキュリティ コンテキスト	uint8 [16]	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL ポリシー ID	uint8 [16]	接続を処理した SSL ポリシーの ID 番号。
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルト アクションの ID 番号。

表 3-25　相関イベント 5.4 以上のデータ フィールド(続き)

フィールド	データ タイプ	説明
実際の SSL アクション	uint32	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

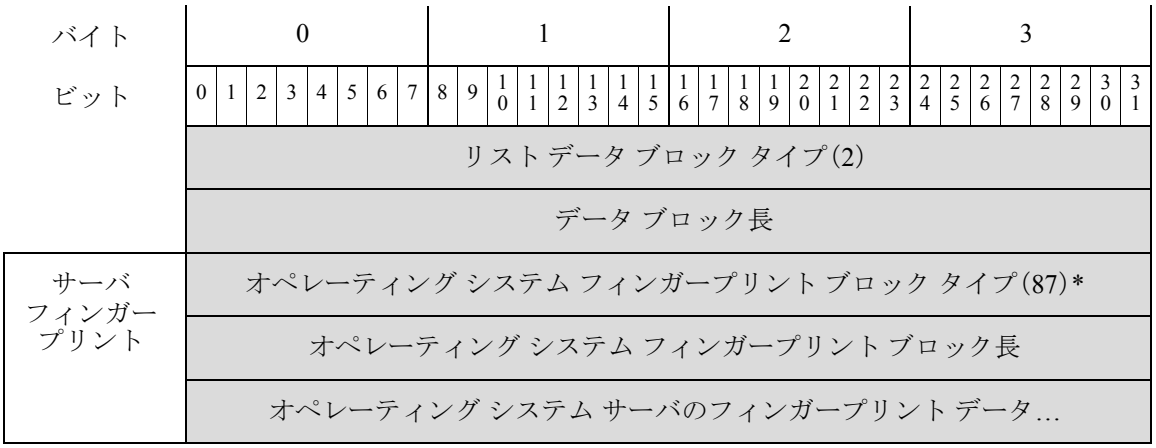
表 3-25　相関イベント 5.4 以上のデータ フィールド(続き)

フィールド	データ タイプ	説明
SSL フロー ステータス	uint32	SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。 • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL 証明書フィンガープリント	uint8 [20]	SSL サーバ証明書の SHA1 ハッシュ。

シリーズ 2 のデータ ブロックの概要

バージョン 4.10.0 から、eStreamer サービスは、2 番目のシリーズのデータ ブロックを使用して、侵入イベント追加データなどの特定のレコードをパッケージしています。このシリーズのすべてのブロック タイプのリストの詳細については、表 3-26 (3-57 ページ) を参照してください。シリーズ 2 のブロックは、シリーズ 1 のブロックと同様に、可変長フィールドとネストされたブロックの階層をサポートします。シリーズ 2 のブロック タイプには、シリーズ 1 のシリーズのプリミティブのブロック タイプと同様に、ネストされた内部のブロックをカプセル化する機能を備えたプリミティブ ブロックが含まれています。ただし、シリーズ 2 のブロックとシリーズ 1 のブロックは別個の番号システムを備えています。

次の例に、プリミティブ ブロックがどのように使用されるか示します。リスト データ ブロック (シリーズ 2 のブロック タイプ 31) は、多数のオペレーティング システムのフィンガープリントを定義しています (各データ ブロック自体が可変長のタイプ 87 のブロックです)。一般的なタイプ 31 のデータ ブロックの長さは、データ ブロック長フィールドによる自己記述的です。ブロック タイプとブロック長フィールドの 8 バイトを除いた、メッセージのデータ部分の長さが含まれています。



次の表では、データ ブロック ステータス フィールドは、ブロックが現在 (最新バージョン) とレガシー (旧バージョンで使用したもので、現在も eStreamer で要求可能) のいずれであるかを示します。

表 3-26　シリーズ 2 のブロック タイプ

タイプ	目次	データ ブロック ステータス	説明
0	文字列	現在 (Current)	さまざまな文字列データをカプセル化します。詳細については、文字列データ ブロック (3-62 ページ) を参照してください。
1	BLOB	現在 (Current)	バイナリ データをカプセル化し、バナー専用として使用します。詳細については、BLOB データ ブロック (3-63 ページ) を参照してください。
2	リスト	現在 (Current)	他のデータ ブロックのリストをカプセル化します。詳細については、リスト データ ブロック (3-63 ページ) を参照してください。

表 3-26　シリーズ 2 のブロック タイプ（続き）

タイプ	目次	データ ブロック ステータス	説明
3	汎用リスト	現在（Current）	他のデータ ブロックのリストをカプセル化します。逆シリアル化では、リストのデータ ブロックに相当します。詳細については、汎用リストのデータ ブロック（3-64 ページ）を参照してください。
4	イベント追加データ	現在（Current）	侵入イベント追加データが含まれています。詳細については、侵入イベント追加データ レコード（3-29 ページ）を参照してください。
5	追加データ タイプ	現在（Current）	追加データのメタデータが含まれています。詳細については、侵入イベント追加データのメタデータ（3-30 ページ）を参照してください。
18	UUID 文字列マッピング	現在（Current）	記述文字列に UUID 値をマッピングするためにさまざまなメタデータ メッセージで使用されるブロック。UUID 文字列マッピングのデータ ブロック（3-65 ページ）を参照してください。
15	アクセス コントロール ポリシー ルール ID のメタデータ	現在（Current）	アクセス コントロール ルールのメタデータが含まれています。アクセス コントロール ポリシー ルール ID のメタデータ ブロック（3-68 ページ）を参照してください。
16	マルウェア イベント	レガシー	Cisco Advanced Malware Protection cloud 内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザといったマルウェア イベントに関する情報が含まれています。マルウェア イベントのデータ ブロック 5.1（B-50 ページ）を参照してください。ブロック 24 により廃止される予定ですマルウェア イベント データ ブロック 5.3.1（B-74 ページ）。
19	ICMP タイプのデータ ブロック	現在（Current）	ICMP タイプを示すメタデータが含まれています。ICMP タイプのデータ ブロック（3-69 ページ）を参照してください。
20	ICMP コードのデータ ブロック	現在（Current）	ICMP コードを示すメタデータが含まれています。ICMP コードのデータ ブロック（3-70 ページ）を参照してください。
21	アクセス コントロール ポリシー ルール理由データ ブロック	現在（Current）	アクセス コントロール ポリシー ルールの理由を説明する情報が含まれています。6.0 以上のアクセス コントロール ポリシー ルール理由データ ブロック（3-79 ページ）を参照してください。
22	IP レピュテーション カテゴリのデータ ブロック	現在（Current）	IP アドレスがブロックされた理由を説明する IP レピュテーション カテゴリに関する情報が含まれています。アクセス コントロール ポリシー名のデータ ブロック（3-81 ページ）を参照してください。

表 3-26　シリーズ 2 のブロック タイプ(続き)

タイプ	目次	データ ブロック ステータス	説明
23	ファイル イベント	レガシー	送信元、SHA ハッシュ、およびファイルの特性などのファイル イベントに関する情報が含まれています。ファイル イベント 5.1.1.x (B-215 ページ) を参照してください。これはブロック 32 に取って代わられますアクセス コントロール ポリシー ルール ID のメタデータ ブロック (3-68 ページ)。
24	マルウェア イベント	レガシー	Cisco Advanced Malware Protection cloud 内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザといったマルウェア イベントに関する情報が含まれています。マルウェア イベント データ ブロック 5.1.1.x (B-54 ページ) を参照してください。ブロック 16 は廃止予定ですマルウェア イベントのデータ ブロック 5.1 (B-50 ページ)。ブロック 33 により廃止される予定ですマルウェア イベント データ ブロック 5.3.1 (B-74 ページ)。
25	侵入イベント	レガシー	接続およびマルウェア イベントと侵入イベントを照合するための情報をはじめとして、侵入イベントに関する情報が含まれています。侵入イベント レコード 5.1.1.x (B-26 ページ) を参照してください。ブロック 34 により廃止される予定です侵入イベント レコード 5.2.x (B-14 ページ)。
26	ファイル イベント SHA ハッシュ	レガシー	マルウェアが含まれていると認識されたファイルの SHA ハッシュと名前が含まれています。ファイル イベント SHA ハッシュ 5.1.1 ～ 5.2.x (B-251 ページ) を参照してください。ブロック 40 により廃止される予定です 5.3 以上のファイル イベント SHA ハッシュ (3-104 ページ)。
27	ルール ドキュメントのデータ ブロック	現在 (Current)	イベントの生成に使用されるルールに関する情報が含まれています。詳細については、5.2 以上のルール ドキュメントのデータ ブロック (3-107 ページ) を参照してください。
28	位置情報のデータ ブロック	現在 (Current)	国コードおよび関連付けられた国名が含まれています。5.2 以上の位置情報のデータ ブロック (3-116 ページ) を参照してください。
32	ファイル イベント	レガシー	送信元、SHA ハッシュ、およびファイルの特性などのファイル イベントに関する情報が含まれています。ファイル イベント 5.2.x (B-223 ページ) を参照してください。廃止予定ですファイル イベント 5.1.1.x (B-215 ページ)。ブロック 38 により廃止される予定ですファイル イベント 5.3 (B-227 ページ)。

表 3-26　シリーズ 2 のブロック タイプ（続き）

タイプ	目次	データ ブロック ステータス	説明
33	マルウェア イベント	現在（Current）	Cisco Advanced Malware Protection cloud 内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザといったマルウェア イベントに関する情報が含まれています。マルウェア イベント データ ブロック 5.2.x（B-60 ページ）を参照してください。ブロック 24 は廃止予定ですマルウェア イベント データ ブロック 5.1.1.x（B-54 ページ）。ブロック 35 により廃止される予定ですマルウェア イベントのデータ ブロック 5.3（B-67 ページ）。
34	侵入イベント	レガシー	接続およびマルウェア イベントと侵入イベントを照合するための情報をはじめとして、侵入イベントに関する情報が含まれています。侵入イベント レコード 5.2.x（B-14 ページ）を参照してください。ブロック 25 は廃止予定です。ブロック 41 により廃止される予定です侵入イベント レコード 5.3（B-20 ページ）。
35	マルウェア イベント	レガシー	IOC 情報をはじめとするマルウェア イベントに関する情報が含まれています。マルウェア イベントのデータ ブロック 5.3（B-67 ページ）を参照してください。ブロック 33 は廃止予定ですマルウェア イベント データ ブロック 5.2.x（B-60 ページ）。ブロック 44 により廃止される予定ですマルウェア イベントのデータ ブロック 5.3（B-67 ページ）。
38	ファイル イベント	レガシー	送信元、SHA ハッシュ、およびファイルの特性などのファイル イベントに関する情報が含まれています。ファイル イベント 5.3（B-227 ページ）を参照してください。ブロック 32 は廃止予定です。ブロック 43 により廃止される予定ですマルウェア イベントのデータ ブロック 6.0 以上（3-94 ページ）。
39	IOC 名のデータ ブロック	現在（Current）	IOC に関する情報が含まれています。5.3+ の IOC 名データ ブロック（4-37 ページ）を参照してください
40	ファイル イベント SHA ハッシュ	現在（Current）	マルウェアが含まれていると認識されたファイルの SHA ハッシュと名前が含まれています。5.3 以上のファイル イベント SHA ハッシュ（3-104 ページ）を参照してください。ブロック 26 は廃止予定ですファイル イベント SHA ハッシュ 5.1.1 ～ 5.2.x（B-251 ページ）。
41	侵入イベント	レガシー	IOC と侵入イベントを照合するための情報をはじめとして、侵入イベントに関する情報が含まれています。侵入イベント レコード 5.3（B-20 ページ）を参照してください。ブロック 34 は廃止予定です。ブロック 42 により廃止される予定です侵入イベント レコード 5.3.1（B-32 ページ）。

表 3-26　シリーズ 2 のブロック タイプ(続き)

タイプ	目次	データ ブロック ステータス	説明
42	侵入イベント	現在（Current）	IOC と侵入イベントを照合するための情報をはじめとして、侵入イベントに関する情報が含まれています。侵入イベント レコード 5.3.1（B-32 ページ）を参照してください。ブロック 41 は廃止予定です侵入イベント レコード 5.3（B-20 ページ）。
43	ファイル イベント	レガシー	送信元、SHA ハッシュ、およびファイルの特性などのファイル イベントに関する情報が含まれています。ファイル イベント 5.3.1（B-234 ページ）を参照してください。ブロック 38 は廃止予定ですファイル イベント 5.3（B-227 ページ）。ブロック 46 により廃止される予定です6.0 以上のファイル イベント（3-83 ページ）。
44	マルウェア イベント	レガシー	IOC 情報をはじめとするマルウェア イベントに関する情報が含まれています。マルウェア イベントのデータ ブロック 6.0 以上（3-94 ページ）を参照してください。ブロック 35 は廃止予定ですマルウェア イベントのデータ ブロック 5.3（B-67 ページ）。ブロック 47 により廃止される予定ですマルウェア イベントのデータ ブロック 6.0 以上（3-94 ページ）。
46	ファイル イベント	現在（Current）	送信元、SHA ハッシュ、およびファイルの特性などのファイル イベントに関する情報が含まれています。マルウェア イベントのデータ ブロック 6.0 以上（3-94 ページ）を参照してください。ブロック 43 は廃止予定ですファイル イベント 5.3.1（B-234 ページ）。
47	マルウェア イベント	現在（Current）	IOC 情報をはじめとするマルウェア イベントに関する情報が含まれています。マルウェア イベントのデータ ブロック 6.0 以上（3-94 ページ）を参照してください。ブロック 44 は廃止予定ですマルウェア イベント データ ブロック 5.3.1（B-74 ページ）。

シリーズ 2 のプリミティブ データ ブロック

シリーズ 2 とシリーズ 1 のブロックには、メッセージ内の可変長の文字列と BLOB に加えて、可変長ブロックのリストのカプセル化に使用される一連のプリミティブがあります。こうしたプリミティブ ブロックには、データ ブロック ヘッダー（2-27 ページ）で説明した標準的な eStreamer ブロック ヘッダーがありますが、表示されるのは他のデータ ブロック内のみです。所定のブロック タイプに任意の数値を含めることができます。これらのブロックの構造の詳細については、次の項を参照してください。

- 文字列データ ブロック（3-62 ページ）
- BLOB データ ブロック（3-63 ページ）
- リスト データ ブロック（3-63 ページ）
- 汎用リストのデータ ブロック（3-64 ページ）
- UUID 文字列マッピングのデータ ブロック（3-65 ページ）
- 名前説明マッピングのデータ ブロック（3-66 ページ）

文字列データ ブロック

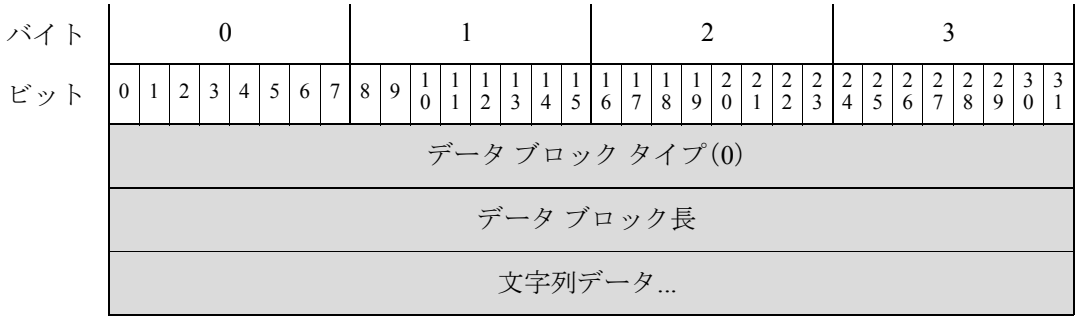
eStreamer サービスは、文字列データ ブロックを使用してメッセージの文字列データを送信します。通常、これらのブロックは、オペレーティング システムやサーバ名などを識別するために他のデータ ブロック内に表示されます。

空の文字列データ ブロック（ヘッダー フィールドのみでデータが含まれていない）のブロック長は 8 です。eStreamer は、文字列の値に内容がない場合に空の文字列データ ブロックを使用します。たとえば、オペレーティング システムのベンダーが不明である場合に、オペレーティング システムのデータ ブロックの OS ベンダー文字列フィールドで使用されます。

文字列データ ブロックは、シリーズ 2 グループのブロックのブロック タイプ 0 です。

（注） このデータ ブロックで戻される文字列は必ずしもヌル終端するとは限りません（つまり、文字列の文字の後に 0 が続くとは限りません）。

次の図に、文字列データ ブロックの形式を示します。



次の表は、文字列データ ブロックのフィールドについての説明です。

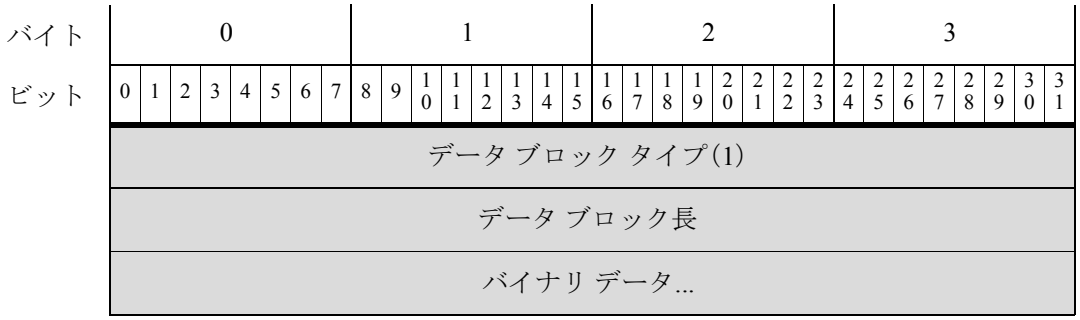
表 3-27　文字列ブロック フィールド

フィールド	データ タイプ	説明
データ ブロック タイプ	uint32	文字列データ ブロックを開始します。この値は常に 0 です。
データ ブロック長	uint32	文字列データ ブロックのヘッダーと文字列データのバイトを組み合わせた長さ。
文字列データ	string	文字列データが含まれています。文字列の末尾に終端文字（ヌル バイト）が含まれている場合があります。

BLOB データ ブロック

eStreamer サービスは、BLOB データ ブロックを使用してバイナリ データを伝送します。たとえば、ホストの検出レコードは、キャプチャされたサーバ バナーを保持するのに BLOB ブロックを使用します。BLOB データ ブロックは、シリーズ 2 グループのブロックのブロック タイプ 1 です。

次の図に、BLOB データ ブロックの形式を示します。



次の表は、BLOB データ ブロックのフィールドについての説明です。

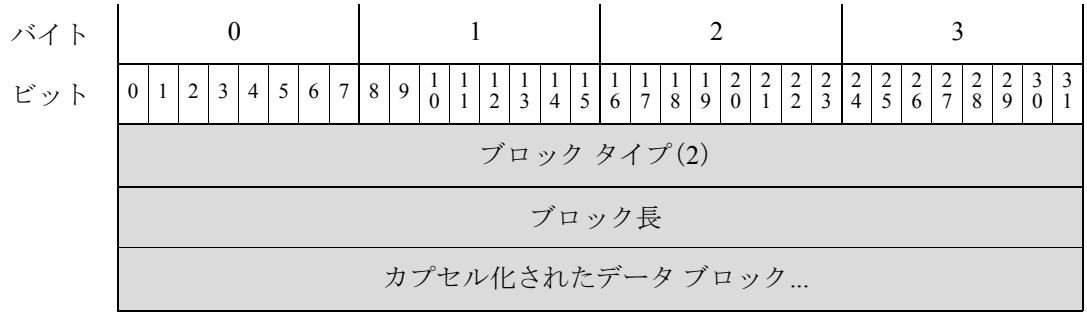
表 3-28　BLOB データ ブロック フィールド

フィールド	データ タイプ	説明
データ ブロック タイプ	uint32	BLOB データ ブロックを開始します。この値は常に 1 です。
データ ブロック長	uint32	BLOB データ ブロックのバイト数です。BLOB ブロック タイプとブロック長フィールドの 8 バイトと後続のバイナリ データの長さが含まれます。
バイナリ データ	変数	サーバ バナーなどのバイナリ データが含まれます。

リスト データ ブロック

eStreamer サービスは、リスト データ ブロックを使用してデータ ブロックのリストをカプセル化します。たとえば、eStreamer は、リスト データ ブロックを使用して、自身がそれぞれデータ ブロックである TCP サーバのリストを送信できます。リスト データ ブロックは、シリーズ 2 グループのブロックのブロック タイプ 2 です。

次の図に、リスト データ ブロックの基本的な形式を示します。



次の表は、リスト データ ブロックのフィールドについての説明です。

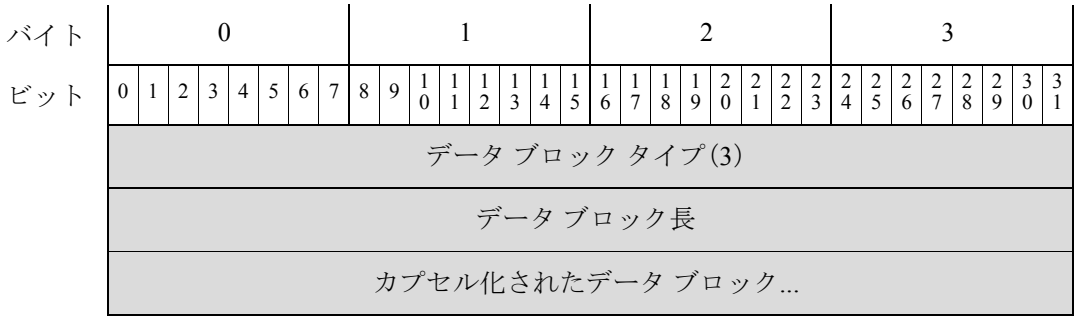
表 3-29　リスト データ フィールド

フィールド	データ タイプ	説明
ブロック タイプ	uint32	リスト データ ブロックを開始します。この値は常に 2 です。
ブロック長	uint32	リスト ブロックとカプセル化されたデータのバイト数。たとえば、リスト内に 3 つのサブサーバ データ ブロックがあるとすると、この値には、サブサーバ ブロックの合計バイト数とリスト ブロック ヘッダーの 8 バイトが含まれることになります。
カプセル化されたデータ ブロック	変数	リスト ブロック長の最大バイト数を上限としてカプセル化したデータ ブロック。

汎用リストのデータ ブロック

eStreamer サービスは、汎用リスト データ ブロックを使用してデータ ブロックのリストをカプセル化します。たとえば、ホスト プロファイルのデータ ブロックには、複数のクライアント アプリケーションに関する情報が含まれているので、汎用リスト ブロックを使用してメッセージのクライアント アプリケーションのデータ ブロックのリストを組み込みます。汎用リストのデータ ブロックは、シリーズ 2 グループのブロックのブロック タイプ 3 です。

次の図に、汎用リストのデータ ブロックの基本的な構造を示します。



次の表は、汎用リストのデータ ブロックのフィールドについての説明です。

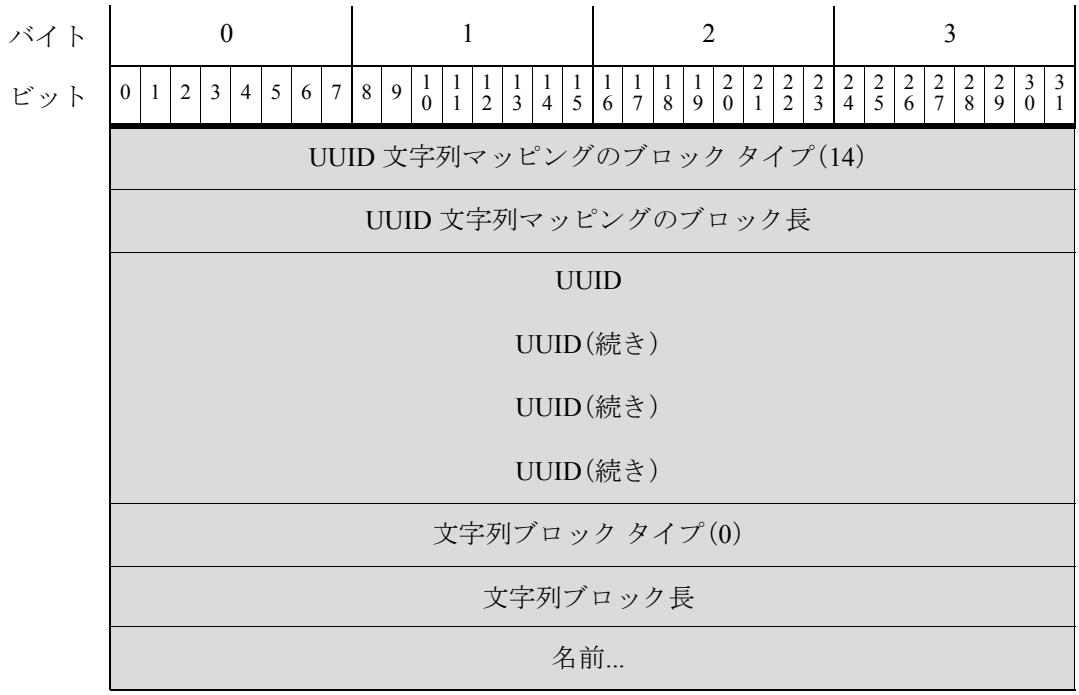
表 3-30　汎用リストのデータ ブロック フィールド

フィールド	バイト数	説明
データ ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 3 です。
データ ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この数値には、汎用リストのブロック ヘッダー フィールドの 8 バイトと、カプセル化されたすべてのデータ ブロックの合計バイト数が含まれます。
カプセル化されたデータ ブロック	変数	汎用リストのブロック長の最大バイト数までカプセル化されるデータ ブロック。

UUID 文字列マッピングのデータ ブロック

eStreamer サービスは、さまざまなメタデータ メッセージの UUID 文字列マッピングのデータ ブロックを使用して、記述文字列に UUID 値をマッピングします。UUID 文字列マッピングのデータ ブロックは、シリーズ 2 のブロック タイプ 14 です。

次の図に、UUID 文字列マッピングのデータ ブロックの構造を示します。



次の表は、UUID 文字列マッピングのデータ ブロックのフィールドについての説明です。

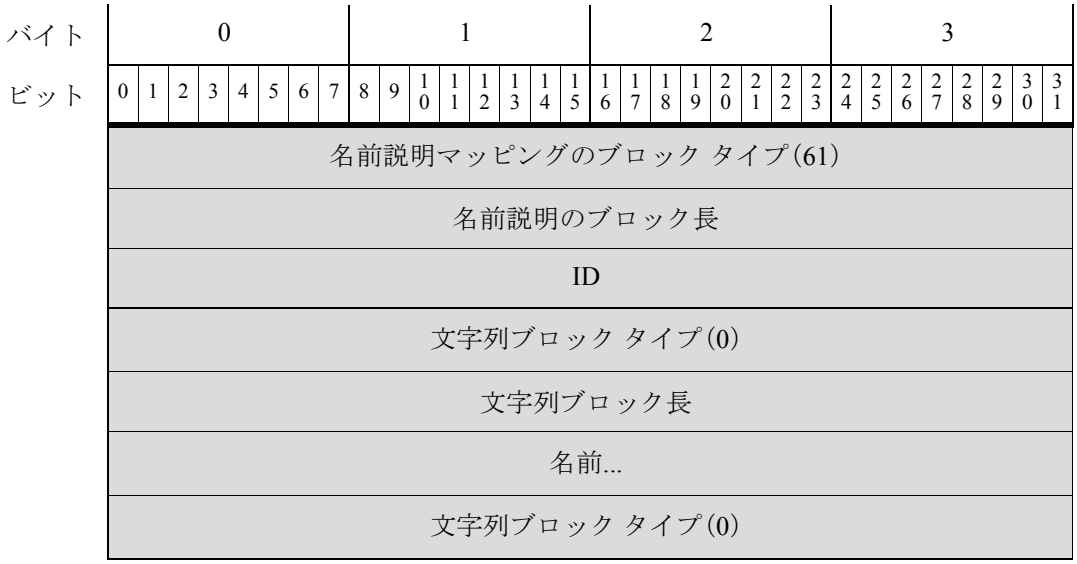
表 3-31　UUID 文字列マッピングのデータ ブロック フィールド

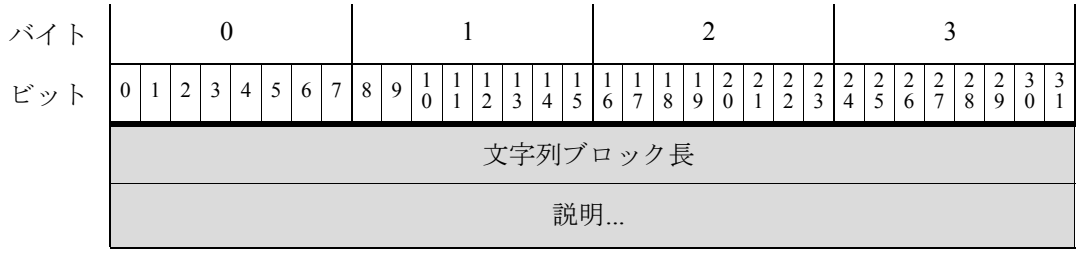
フィールド	データ タイプ	説明
UUID 文字列マッピングのブロック タイプ	uint32	UUID 文字列マッピングのブロックを開始します。この値は常に 14 です。
UUID 文字列マッピングのブロック長	uint32	UUID 文字列マッピングのブロックの合計バイト数です。UUID 文字列マッピングのブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
UUID	uint8[16]	UUID が識別するイベントまたは他のオブジェクトの固有識別子。
文字列ブロック タイプ	uint32	UUID に関連付けられた記述名を含む文字列のデータ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
名前	string	わかりやすい名前。

名前説明マッピングのデータ ブロック

eStreamer サービスは、さまざまなメタデータ メッセージの名前説明マッピングのデータ ブロックを使用して、名前と記述文字列に ID 値をマッピングします。名前説明マッピングのデータ ブロックは、シリーズ 2 のブロック タイプ 61 です。

次の図に、名前説明マッピングのデータ ブロックの構造を示します。





次の表は、名前説明マッピングのデータ ブロックのフィールドについての説明です。

表 3-32　名前説明マッピングのデータ ブロック フィールド

フィールド	データ タイプ	説明
名前説明マッピングのブロック タイプ	uint32	名前説明マッピングのブロックを開始します。この値は常に 61 です。
名前説明マッピングのブロック長	uint32	名前説明マッピングのブロックの合計バイト数です。名前説明マッピングのブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
ID	unit32	ID が識別するイベントまたは他のオブジェクトの固有識別子。
文字列ブロック タイプ	uint32	ID に関連付けられた名前を含む文字列のデータ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
名前	string	イベントまたはオブジェクトの名前。
文字列ブロック タイプ	uint32	ID に関連付けられた説明を含む文字列のデータ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	説明の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	ID に関連付けられたオブジェクトまたはイベントの説明。

アクセス コントロール ポリシー ルール ID のメタデータ ブロック

eStreamer サービスは、アクセス コントロール ポリシー ルール ID のメタデータ ブロックを使用して、アクセス コントロール ポリシー ルール ID に関する情報を表示します。このデータ ブロックは、シリーズ 2 のブロック タイプ 15 です。

次の図に、アクセス コントロール ポリシー ルール ID のメタデータ ブロックの構造を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	アクセス コントロール ポリシー ルール ID のメタデータ ブロック タイプ(15)																															
	アクセス コントロール ポリシー ルール ID のメタデータのブロック長																															
	リビジョン リビジョン(続き) リビジョン(続き) リビジョン(続き)																															
	ルール ID																															
名前	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	名前...																															

次の表は、アクセス コントロール ポリシー ルール ID のメタデータ ブロックのフィールドについての説明です。

表 3-33　アクセス コントロール ポリシー ルール ID のメタデータ ブロック フィールド

フィールド	データ タイプ	説明
アクセス コントロール ポリシー ルール ID のメタデータ ブロック タイプ	uint32	アクセス コントロール ポリシー ルール ID のメタデータ ブロックを開始します。この値は常に 15 です。
アクセス コントロール ポリシー ルール ID のメタデータのブロック長	uint32	アクセス コントロール ポリシー ルール ID のブロックの合計バイト数です。アクセス コントロール ポリシー ルール ID のメタデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
リビジョン	uint8[16]	トリガーされた相関イベントに関連付けられたルールのリビジョン番号。

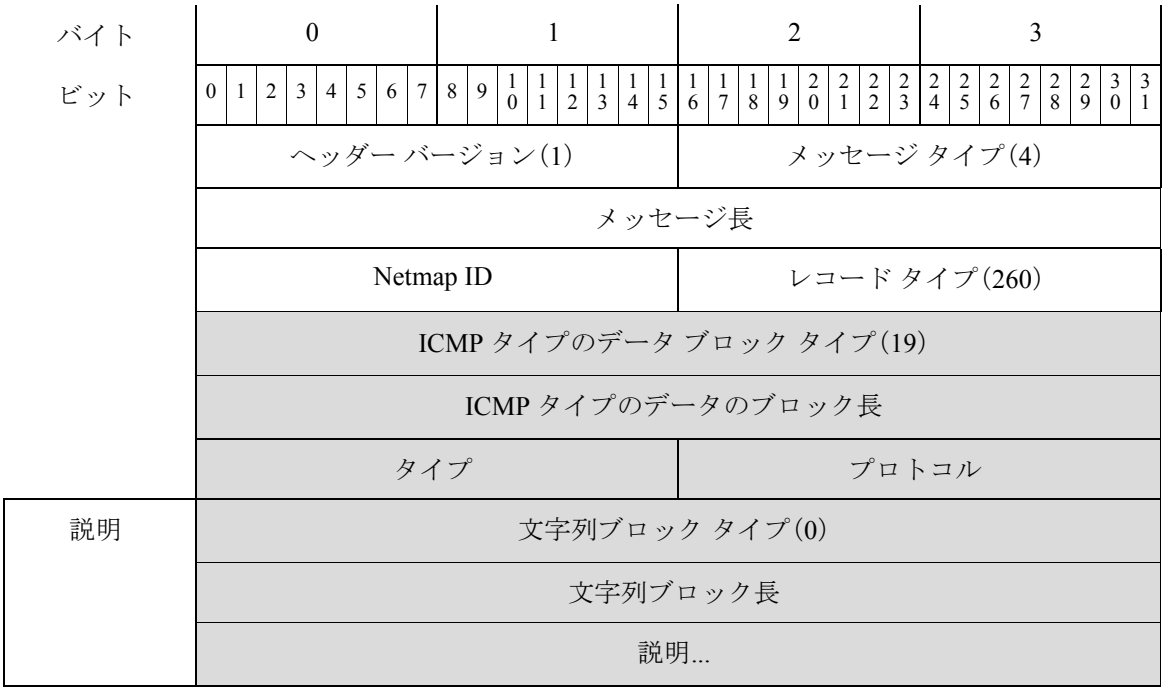
表 3-33　アクセス コントロール ポリシー ルール ID のメタデータ ブロック フィールド（続き）

フィールド	データ タイプ	説明
ルール ID	uint32	イベントをトリガーしたルールの内部 ID。
文字列ブロック タイプ	uint32	アクセス コントロール ポリシー ルールに関連付けれらた記述名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
名前	string	アクセス コントロール ポリシー ルールの記述名。

ICMP タイプのデータ ブロック

eStreamer サービスは、ICMP タイプのデータ ブロックを使用して ICMP タイプに関する情報を表示します。このデータ ブロックのレコード タイプは 260 で、シリーズ 2 のブロック タイプ 19 です。

次の図に、ICMP タイプのデータ ブロックの構造を示します。



次の表は、ICMP タイプのデータ ブロックのフィールドについての説明です。

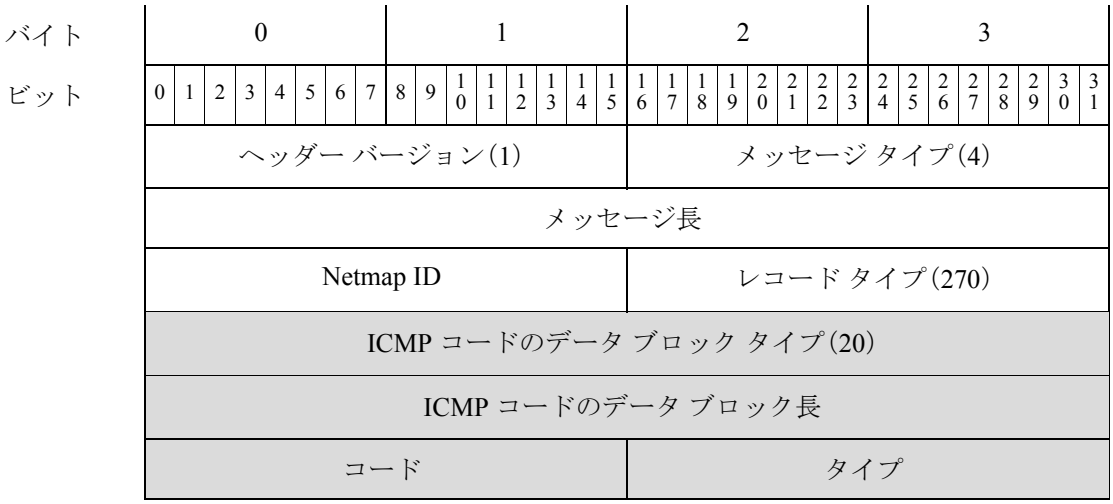
表 3-34　ICMP タイプのデータ ブロック フィールド

フィールド	データ タイプ	説明
ICMP タイプのデータ ブロック タイプ	uint32	ICMP タイプのデータ ブロックを開始します。この値は常に 19 です。
ICMP タイプのデータのブロック長	uint32	ICMP タイプのデータ ブロックの合計バイト数です。ICMP タイプのデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
タイプ	uint16	イベントの ICMP タイプ。
プロトコル	uint16	IANA 指定のプロトコル番号。次に例を示します。 • 0:IP • 1:ICMP • 6:TCP • 17:UDP
文字列ブロック タイプ	uint32	ICMP タイプの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	イベントの ICMP タイプの説明。

ICMP コードのデータ ブロック

eStreamer サービスは、ICMP コードのデータ ブロックを使用してアクセス コントロール ポリシー ルール ID に関する情報を表示します。このデータ ブロックのレコード タイプは 270 で、ブロック タイプはシリーズ 2 のブロック タイプ 20 です。

次の図に、アクセス コントロール ポリシー ルール ID のメタデータ ブロックの構造を示します。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
説明	プロトコル																文字列ブロック タイプ(0)															
	文字列ブロック タイプ(0)(続き)																文字列ブロック長															
	文字列ブロック長(続き)																説明...															

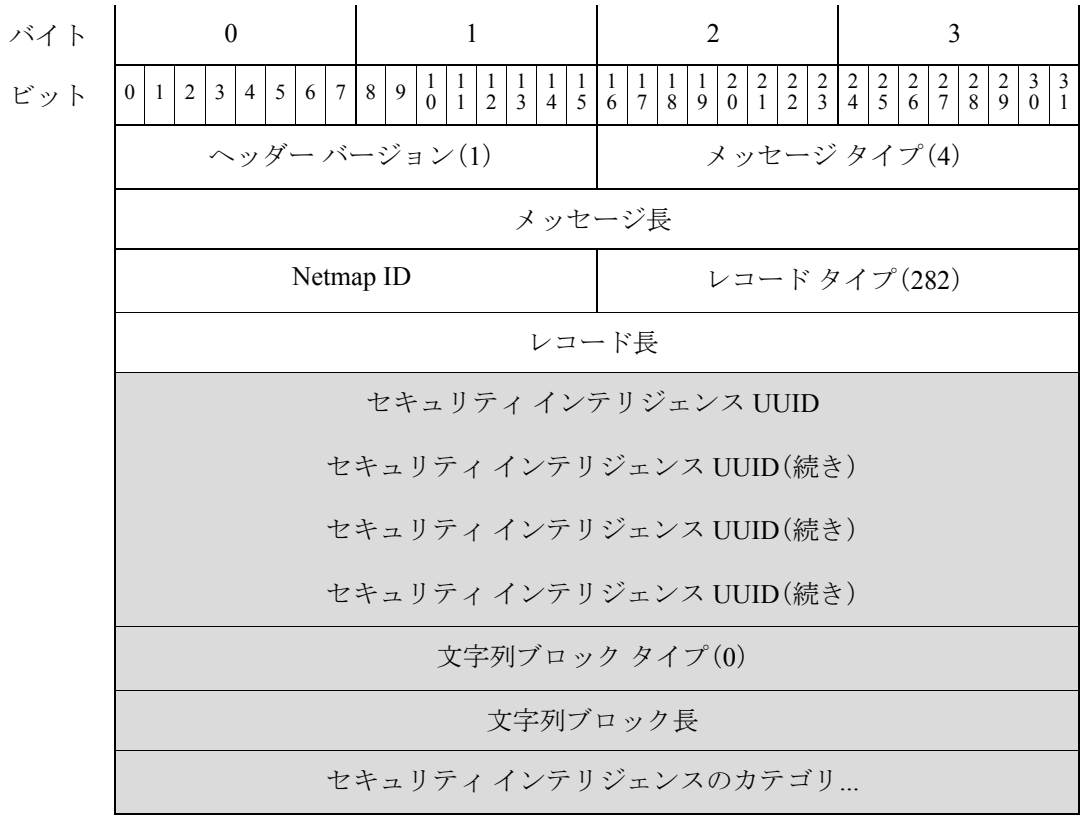
次の表は、ICMP コードのデータ ブロックのフィールドについての説明です。

表 3-35　ICMP コードのデータ ブロック フィールド

フィールド	データ タイプ	説明
ICMP コードのデータ ブロック タイプ	uint32	ICMP コードのデータ ブロックを開始します。この値は常に 20 です。
ICMP コードのデータ ブロック長	uint32	ICMP コードのデータ ブロックの合計バイト数です。ICMP コードのデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
コード	uint16	イベントの ICMP コード。
タイプ	uint16	イベントの ICMP タイプ。
プロトコル	uint16	IANA 指定のプロトコル番号。次に例を示します。 • 0:IP • 1:ICMP • 6:TCP • 17:UDP
文字列ブロック タイプ	uint32	ICMP コードの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	イベントの ICMP コードの説明。

5.4.1 以上のセキュリティ インテリジェンス カテゴリのメタデータ

eStreamer サービスは、セキュリティ インテリジェンス カテゴリの情報を含むメタデータを送信します。形式は次のとおりです。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにセキュリティ インテリジェンス カテゴリ レコードを示す値 282 があることに注意してください。



次の表は、セキュリティ コンテキスト名のレコードのフィールドについての説明です。

表 3-36　セキュリティ コンテキスト名のレコード フィールド

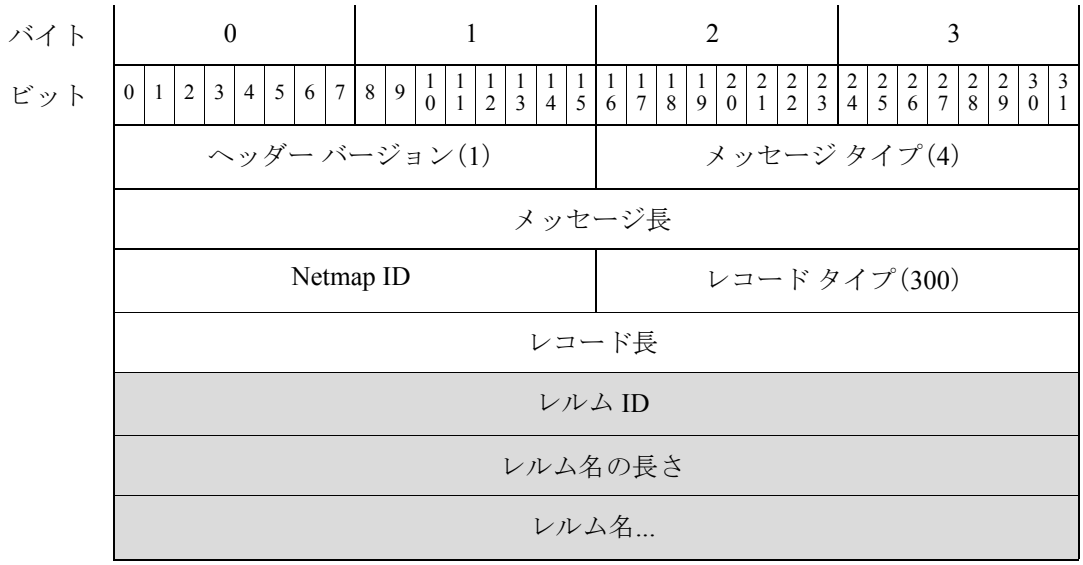
フィールド	データ タイプ	説明
セキュリティ インテリジェンス UUID	uint8[16]	セキュリティ インテリジェンスの UUID。
文字列ブロック タイプ	uint32	セキュリティ インテリジェンス カテゴリを含む文字列データ ブロックを開始します。この値は常に 0 です。

表 3-36　セキュリティ コンテキスト名のレコード フィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	セキュリティ インテリジェンス カテゴリの文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとプロファイル名フィールドのバイト数が含まれます。
セキュリティ インテリジェンスのカテゴリ（Security Intelligence Category）	string	セキュリティ インテリジェンスのカテゴリ。

6.0 以上のレルムのメタデータ

eStreamer サービスは、レルムの情報を含むメタデータを送信します。形式は次のとおりです。メッセージ長フィールドの後に表示されるレコード タイプフィールドにレルムのメタデータ レコードを示す値 300 があることに注意してください。



次の表は、レルムのメタデータのレコードのフィールドについての説明です。

表 3-37　レルムのメタデータのレコード フィールド

フィールド	データ タイプ	説明
レルム ID	uint32	レルム ID 番号。
レルム名の長さ	uint32	レルム名に含まれるバイト数。
レルム名	string	レルム名

6.0 以上のエンドポイント プロファイルのデータ ブロック

eStreamer サービスは、エンドポイント プロファイルのデータ ブロックを使用してネットワークのエンドポイントに関する情報を表示します。このデータ ブロックのレコード タイプは 301 で、ブロック タイプはシリーズ 2 のブロック タイプ 58 です。

次の図に、アクセス コントロール ポリシー ルール ID のメタデータ ブロックの構造を示します。

次の表は、エンドポイント プロファイルのデータ ブロックのフィールドについての説明です。

表 3-38　エンドポイント プロファイルのデータ ブロック フィールド

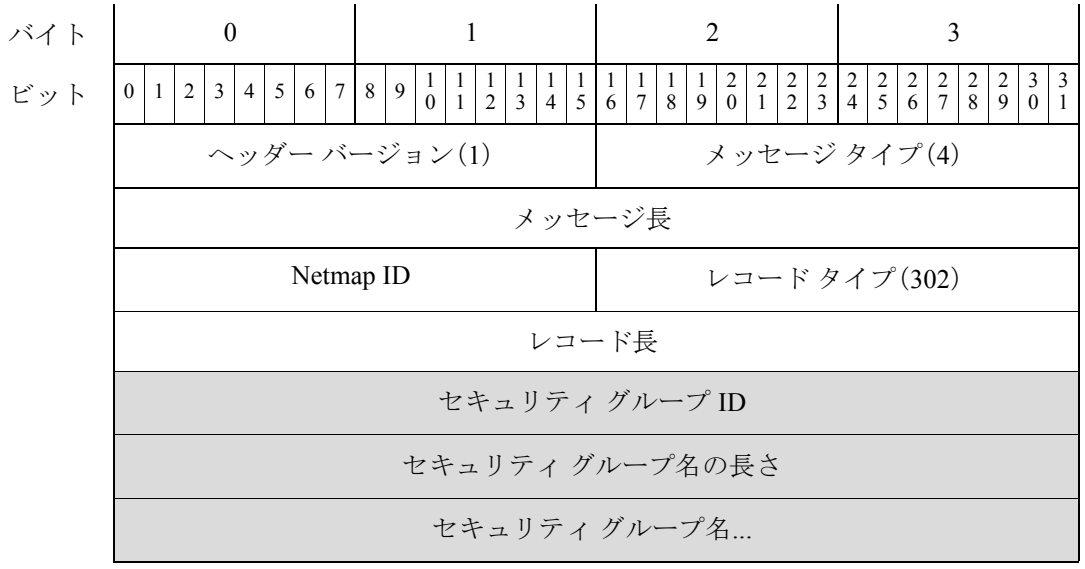
フィールド	データ タイプ	説明
エンドポイント プロファイルのデータ ブロック タイプ	uint32	ICMP コードのデータ ブロックを開始します。この値は常に 58 です。
エンドポイント プロファイルのデータのブロック長	uint32	エンドポイント プロファイルのデータ ブロックの合計バイト数です。エンドポイント プロファイルのデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
ID	uint32	エンドポイント ID 番号。

表 3-38　エンドポイント プロファイルのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	エンドポイントのプロファイルを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	プロファイル名の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとプロファイル名フィールドのバイト数が含まれます。
プロファイル名	string	エンドポイント プロファイルの名前。
文字列ブロック タイプ	uint32	エンドポイントの正式名称を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	正式名称の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと正式名称フィールドのバイト数が含まれます。
正式名称	string	プロファイルの完全修飾名。エンドポイントのタイプの関係階層を示します。

6.0 以上のセキュリティ グループのメタデータ

eStreamer サービスは、セキュリティ グループの情報を含むメタデータを送信します。形式は次のとおりです。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにセキュリティ グループのメタデータのレコードを示す値 302 があることに注意してください。



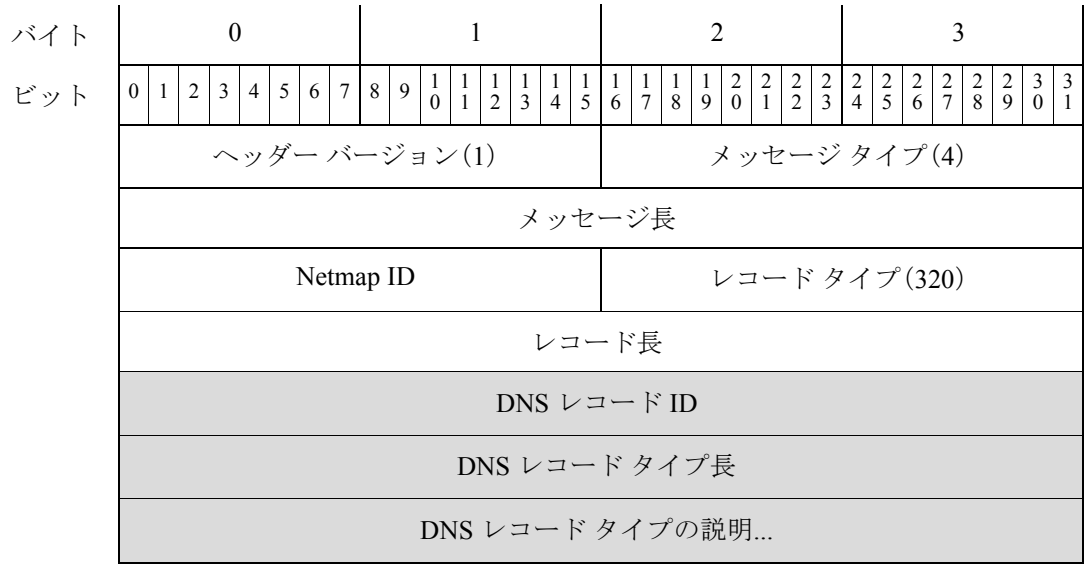
次の表は、セキュリティ グループのメタデータのレコードのフィールドについての説明です。

表 3-39　セキュリティ グループのメタデータのレコード フィールド

フィールド	データ タイプ	説明
セキュリティ グループ ID	uint32	セキュリティ グループ ID 番号。
セキュリティ グループ名の長さ	uint32	セキュリティ グループ名に含まれるバイト数。
セキュリティ グループ名	string	セキュリティ グループ名。

6.0 以上の DNS レコード タイプのメタデータ

eStreamer サービスは、DNS レコード タイプの情報を含むメタデータを送信します。形式は次のとおりです。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに DNS レコード タイプのメタデータのレコードを示す値 320 があることに注意してください。



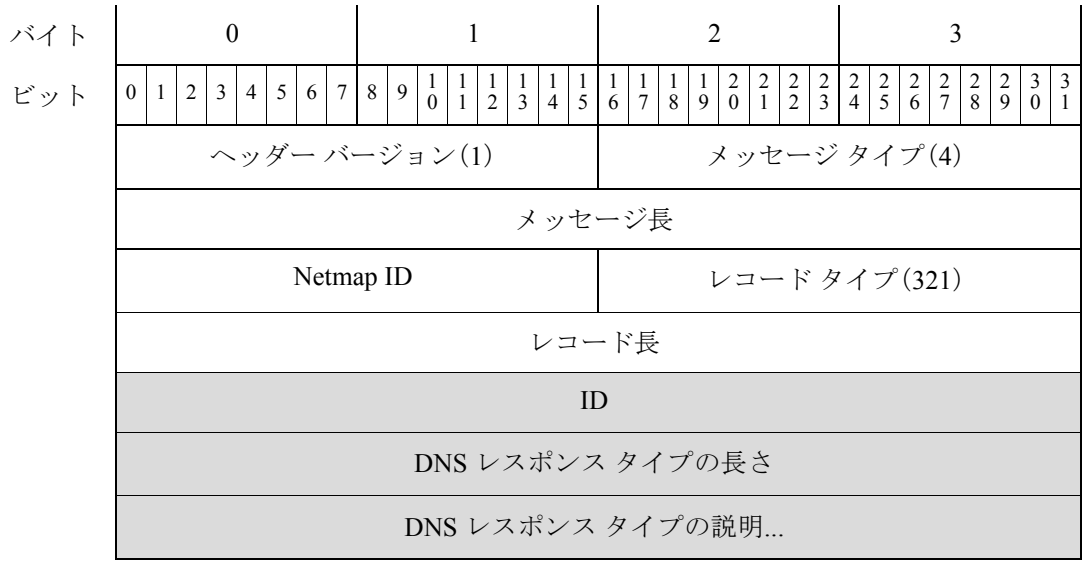
次の表は、DNS レコード タイプのメタデータのレコードのフィールドについての説明です。

表 3-40　DNS レコード タイプのメタデータ フィールド

フィールド	データ タイプ	説明
DNS レコード ID	uint8[16]	DNS レコード ID 番号。
DNS レコード タイプ長	uint32	DNS レコード タイプの説明に含まれるバイト数。
DNS レコード タイプの説明	string	DNS レコード タイプの説明。

6.0 以上の DNS レスポンス タイプのメタデータ

eStreamer サービスは、DNS レスポンス タイプのメタデータを送信します。形式は次のとおりです。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに DNS レスポンス タイプのメタデータのレコードを示す値 321 があることに注意してください。



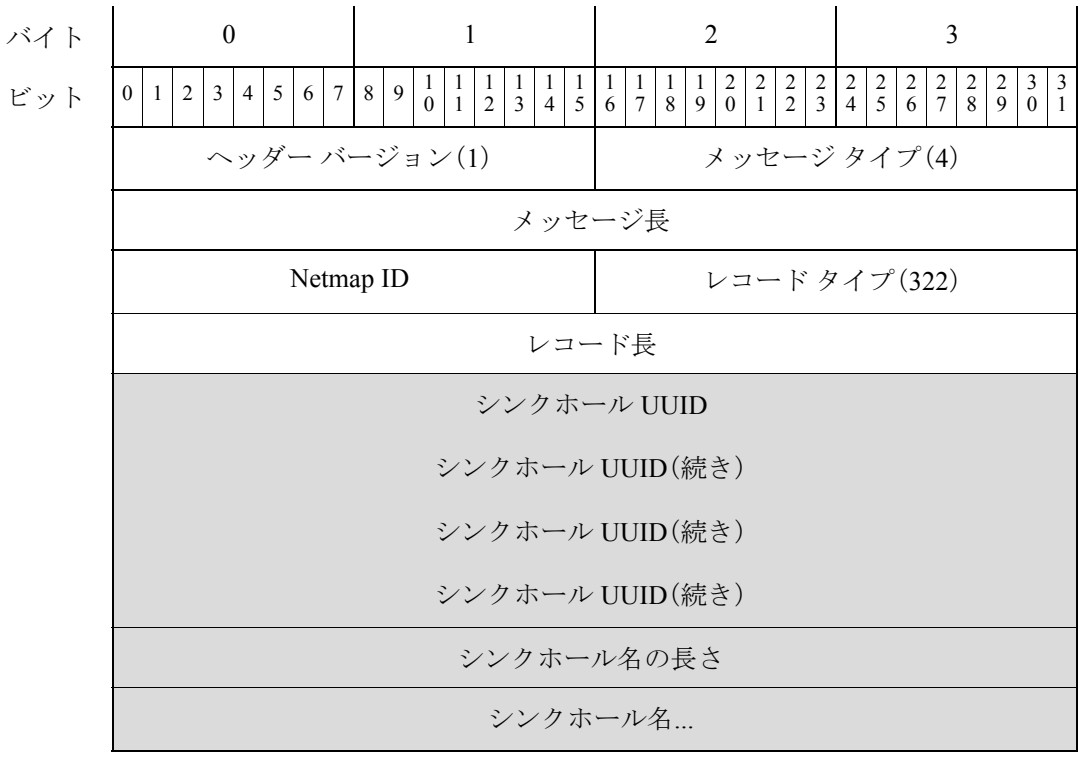
次の表は、DNS レスポンス タイプのメタデータのレコードのフィールドについての説明です。

表 3-41　DNS レスポンス タイプのメタデータ フィールド

フィールド	データ タイプ	説明
ID	uint32	DNS レスポンス ID 番号。
DNS レスポンス タイプの長さ	uint32	DNS レスポンスに含まれるバイト数。
DNS レスポンス タイプの説明	string	DNS レスポンス タイプの説明

6.0 以上のシンクホールのメタデータ

eStreamer サービスは、シンクホールの情報を含むメタデータを送信します。形式は次のとおりです。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにシンクホールのメタデータ レコードを示す値 322 があることに注意してください。



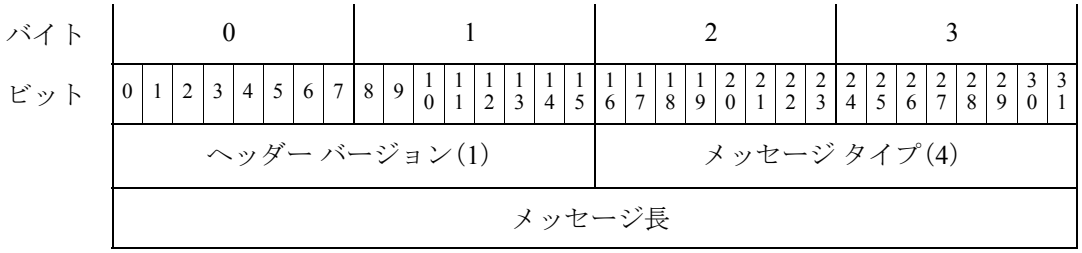
次の表は、シンクホールのメタデータのレコードのフィールドについての説明です。

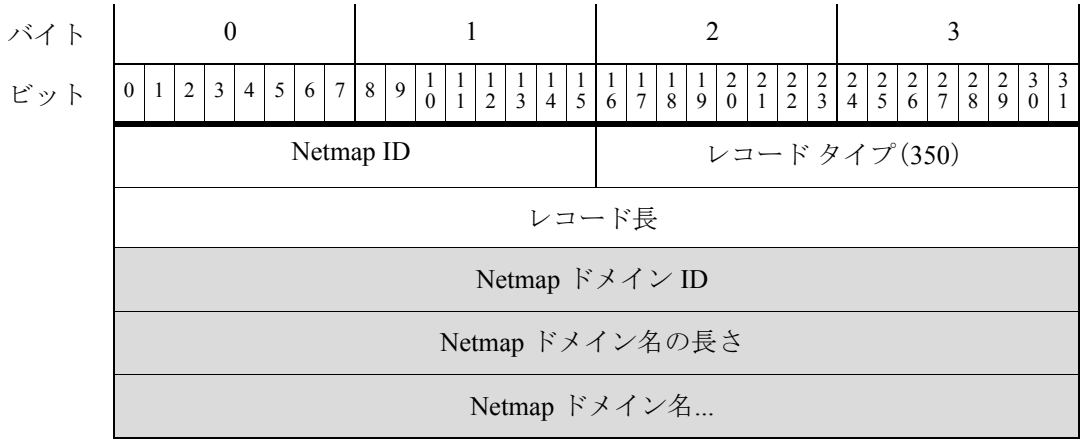
表 3-42　シンクホールのメタデータのレコード フィールド

フィールド	データ タイプ	説明
シンクホール UUID	uint8[16]	シンクホールの UUID 番号。
シンクホール名の長さ	uint32	シンクホール名に含まれるバイト数。
シンクホール名	string	シンクホール名

6.0 以上の Netmap ドメインのメタデータ

eStreamer サービスは、Netmap ドメインの情報を含むメタデータを送信します。形式は次のとおりです。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに Netmap ドメインのメタデータ レコードを示す値 350 があることに注意してください。





次の表は、Netmap ドメインのメタデータのレコードのフィールドについての説明です。

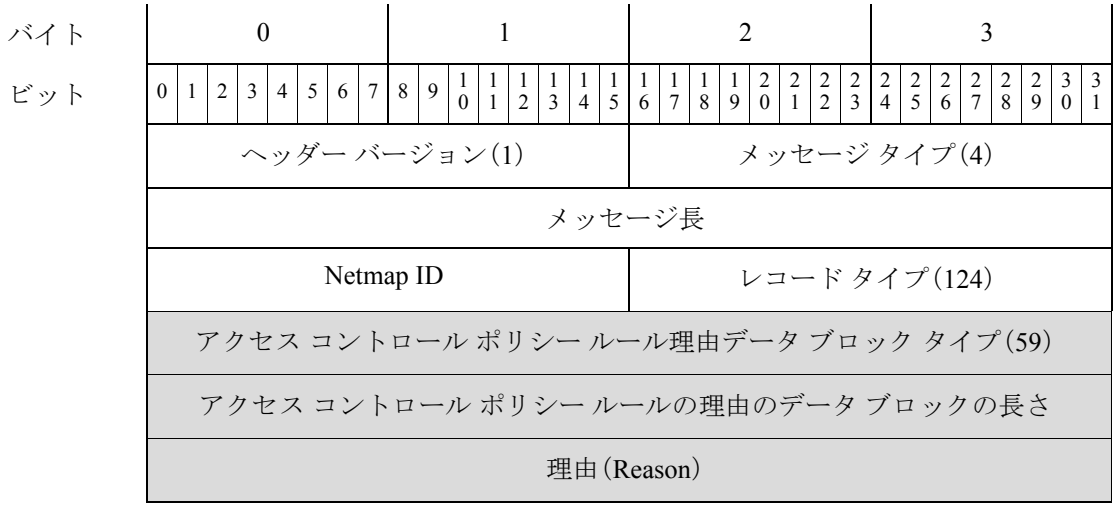
表 3-43　シンクホールのメタデータのレコード フィールド

フィールド	データ タイプ	説明
Netmap ドメイン ID	uint32	Netmap ドメイン ID 番号。
Netmap ドメイン名の長さ	uint32	Netmap ドメイン名に含まれるバイト数。
Netmap ドメイン名	string	Netmap ドメイン名

6.0 以上のアクセス コントロール ポリシー ルール理由データ ブロック

eStreamer サービスは、アクセス コントロール ルールのポリシー ルールの理由のデータ ブロックを使用して、アクセス コントロール ポリシー ルール ID に関する情報を表示します。このデータ ブロックのレコード タイプは 124 で、シリーズ 2 のブロック タイプ 59 です。これはブロック タイプ 21 に取って代わります。理由フィールドが 16 ビットから 32 ビットに拡張されました。

次の図に、アクセス コントロール ポリシー ルール ID のメタデータ ブロックの構造を示します。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	説明...																															

次の表は、アクセス コントロール ポリシー ルールの理由データ ブロックのフィールドについての説明です。

表 3-44　アクセス コントロール ポリシー ルール理由データ ブロックのフィールド

フィールド	データ タイプ	説明
アクセス コントロール ポリシー ルール理由データ ブロック タイプ	uint32	アクセス コントロール ポリシー ルール理由データ ブロックを開始します。この値は常に 59 です。
アクセス コントロール ポリシー ルールの理由のデータ ブロックの長さ	uint32	アクセス コントロール ポリシー ルール理由データ ブロックのバイトの合計数(アクセス コントロール ポリシー ルール理由データ ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
理由(Reason)	uint32	イベントをトリガーしたルールの理由の番号。
文字列ブロック タイプ	uint32	アクセス コントロール ポリシー ルール理由の説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	ルールの理由の説明。

アクセス コントロール ポリシー名のデータ ブロック

eStreamer サービスは、アクセス コントロール ポリシー名のデータ ブロックを使用して、アクセス コントロール ポリシー名に関する情報を表示します。このデータ ブロックは、シリーズ 2 のブロック タイプ 64 です。

次の図に、アクセス コントロール ポリシー名のメタデータのブロックの構造を示します。

次の表は、アクセス コントロール ポリシー名のメタデータ ブロックのフィールドについての説明です。

表 3-45　アクセス コントロール ポリシーのポリシー名のデータ ブロック フィールド

フィールド	データ タイプ	説明
アクセス コントロール ポリシー名のデータ ブロック タイプ	uint32	アクセス コントロール ポリシー名のデータ ブロックを開始します。この値は常に 64 です。
アクセス コントロール ポリシー名のデータ ブロック長	uint32	アクセス コントロール ポリシー名のデータ ブロックの合計バイト数です。アクセス コントロール ポリシー名のデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの UUID
センサー ID	uint32	アクセス コントロール ポリシーに関連付けられたセンサー ID 番号

表 3-45　アクセス コントロール ポリシーのポリシー名のデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	アクセス コントロール ポリシーの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
名前	string	アクセス コントロール ポリシーの名前。

IP レピュテーション カテゴリのデータ ブロック

eStreamer サービスは、IP レピュテーション カテゴリのデータ ブロックを使用して、ルール レピュテーション カテゴリの情報を表示します。このデータ ブロックは、シリーズ 2 のブロック タイプ 22 です。

次の図に、IP レピュテーション カテゴリのデータ ブロックの構造を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IP レピュテーション カテゴリのデータ ブロック タイプ(22)																															
	IP レピュテーション カテゴリのデータ ブロックの長さ																															
	ルール ID																															
	ポリシー UUID ポリシー UUID(続き) ポリシー UUID(続き) ポリシー UUID(続き)																															
説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	カテゴリ名...																															

次の表は、IP レピュテーション カテゴリのデータ ブロックのフィールドについての説明です。

表 3-46　IP レピュテーション カテゴリのデータ ブロック フィールド

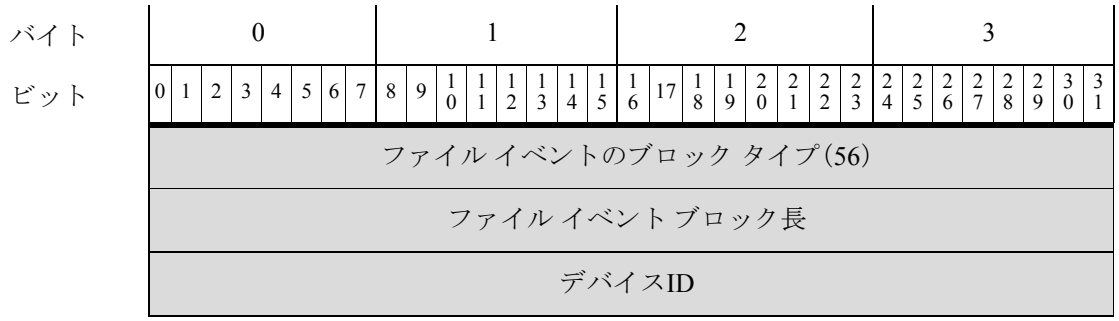
フィールド	データ タイプ	説明
IP レピュテーション カテゴリのデータ ブロック タイプ	uint32	IP レピュテーション カテゴリのデータ ブロックを開始します。この値は常に 22 です。
IP レピュテーション カテゴリのデータ ブロックの長さ	uint32	IP レピュテーション カテゴリのデータ ブロックの合計バイト数です。IP レピュテーション カテゴリのデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID。
ポリシー UUID	uint8[16]	イベントをトリガーしたポリシーの UUID。
文字列ブロック タイプ	uint32	IP レピュテーション カテゴリの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カテゴリ名の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとカテゴリ名フィールドのバイト数が含まれます。
カテゴリ名（Category Name）	string	ルールのカテゴリの名前。

6.0 以上のファイル イベント

ファイル イベントのデータ ブロックには、ネットワーク経由で送信されるファイルの情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントは、シリーズ 2 グループのブロックのブロック タイプ 56 です。これはブロック タイプ 46 に取って代わります。ISE 統合、ファイル分析、ローカルのマルウェア分析、および容量処理ステータスのフィールドが追加されました。

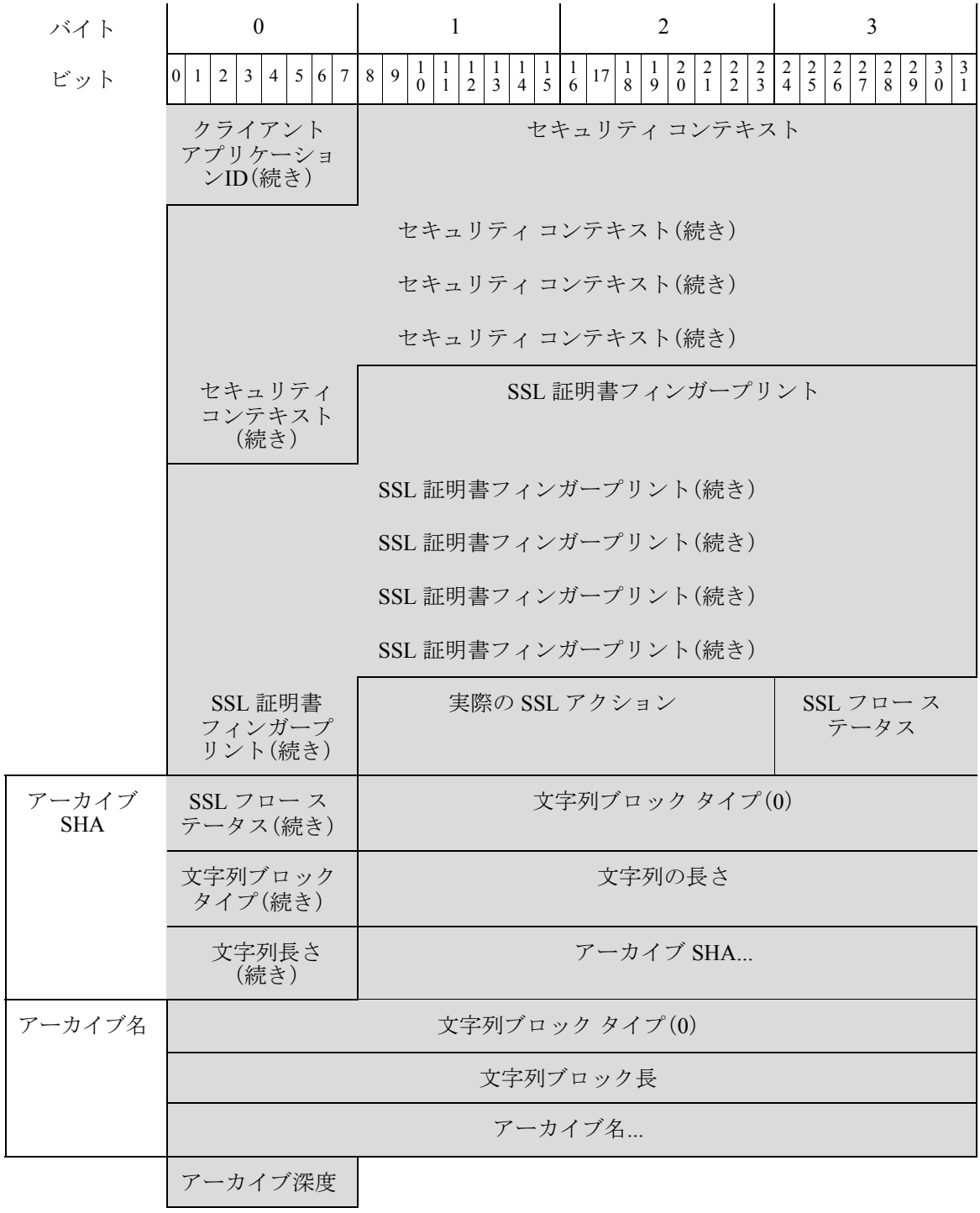
ファイル イベント レコードを要求するには、イベント バージョン 5 およびイベント コード 111 の要求メッセージ内に、ファイル イベント フラグ（要求フラグ フィールドのビット 30）を設定します。要求フラグ（2-12 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

次の図は、ファイル イベント データ ブロックの構造を示しています。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続インスタンス																	接続数カウンタ															
接続タイムスタンプ																																
ファイル イベント タイムスタンプ（File Event Timestamp）																																
送信元 IP アドレス 送信元 IP アドレス（続き） 送信元 IP アドレス（続き） 送信元 IP アドレス（続き）																																
宛先IPアドレス 宛先 IP アドレス（続き） 宛先 IP アドレス（続き） 宛先 IP アドレス（続き）																																
傾向									SPERO 解析結果								ファイル ストレージ ステータス								ファイル分析ステータス							
ローカルのマルウェア分析のステータス									アーカイブ ファイル ステータス								脅威スコア								操作							
SHA ハッシュ SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き）																																
ファイル タイプ ID																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
ファイル名
文字列ブロック タイプ(0)
文字列ブロック長
ファイル名...
ファイル サイズ
ファイル サイズ(続き)
方向
アプリケーション ID
アプリケーション ID(続き)
ユーザ ID
URI
ユーザ ID(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
URI...
シグネチャ
文字列ブロック タイプ(0)
文字列ブロック長
署名...
送信元ポート
接続先ポート
プロトコル
アクセス コントロール ポリシー UUID
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
送信元の国
宛先の国
宛先の国(続き)
Web アプリケーション ID
Web アプリケーションID(続き)
クライアント アプリケーション ID


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
クライアント アプリケーション ID（続き）
セキュリティ コンテキスト
セキュリティ コンテキスト（続き）
セキュリティ コンテキスト（続き）
セキュリティ コンテキスト（続き）
セキュリティ コンテキスト（続き）
SSL 証明書フィンガープリント
SSL 証明書フィンガープリント（続き）
SSL 証明書フィンガープリント（続き）
SSL 証明書フィンガープリント（続き）
SSL 証明書フィンガープリント（続き）
実際の SSL アクション
SSL フロー ステータス
アーカイブ SHA
SSL フロー ステータス（続き）
文字列ブロック タイプ（0）
文字列ブロック タイプ（続き）
文字列の長さ
文字列長さ（続き）
アーカイブ SHA...
アーカイブ名
文字列ブロック タイプ（0）
文字列ブロック長
アーカイブ名...
アーカイブ深度

次の表は、ファイル イベント データ ブロックのフィールドについての説明です。

表 3-47　6.0 以上のファイル イベントのデータ ブロック フィールド

フィールド	データ タイプ	説明
ファイル イベント ブロック タイプ	uint32	ファイル イベント データ ブロックを開始します。この値は常に 56 です。
ファイル イベント ブロック長	uint32	ファイル イベント ブロックのバイトの合計数（ファイル イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む）。
デバイスID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または侵入イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続タイムスタンプ	uint32	関連する接続イベントの UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
ファイル イベント タイムスタンプ（File Event Timestamp）	uint32	ファイル タイプが識別されてファイル イベントが生成されたときの UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1（CLEAN）：ファイルはクリーンであり、マルウェアは含まれていません。 • 2（UNKNOWN）：ファイルにマルウェアが含まれているかどうかは不明です。 • 3（MALWARE）：ファイルにはマルウェアが含まれています。 • 4：UNAVAILABLE。ソフトウェアから AMP cloud に対して、特性を確認する要求を送信できなかったか、または AMP cloud サービスが要求に応答しなかった。 • 5（CUSTOM SIGNATURE）：ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
SPERO 解析結果	uint8	SPERO 署名がファイル分析で使用されたかどうかを示します。値が 1、2、または 3 であれば、SPERO 分析は使用されました。それ以外の値であれば、SPERO 分析は使用されませんでした。

表 3-47　6.0 以上のファイル イベントのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
ファイル ストレージ ステータス	uint8	ファイルの保存ステータス。値は以下のとおりです。 • 1:ファイルが保存されました • 2:ファイルが保存されました • 3:ファイルを保存できません • 4:ファイルを保存できません • 5:ファイルを保存できません • 6:ファイルを保存できません • 7:ファイルを保存できません • 8:ファイル サイズが大きすぎます • 9:ファイル サイズが小さすぎます • 10:ファイルを保存できません • 11:ファイルは保存されておらず、解析結果を入手できません

表 3-47　6.0 以上のファイル イベントのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
ファイル分析ステータス	uint8	ファイルが動的分析のために送信されているかどうかを示します。値は以下のとおりです。 • 0:ファイルが分析のために送信されていません • 1:分析のために送信されました • 2:分析のために送信されました • 4:分析のために送信されました • 5:送信に失敗しました • 6:送信に失敗しました • 7:送信に失敗しました • 8:送信に失敗しました • 9:ファイル サイズが小さすぎます • 10:ファイル サイズが大きすぎます • 11:分析のために送信されました • 12:分析が完了しました • 13:失敗(ネットワークの問題) • 14:失敗(レート制限) • 15:失敗(ファイルが大きすぎます) • 16:失敗(ファイルの読み取りエラー) • 17:失敗(内部ライブラリ エラー) • 19:ファイルは送信されておらず、解析結果を入手できません • 20:失敗(ファイルを実行できません) • 21:失敗(分析タイムアウト) • 22:分析のために送信されました • 23(ファイル送信によるファイル キャパシティの処理):分析のためにファイルをサンドボックスに送信できなかったので、ファイル キャパシティが処理されました(センサーに保存) • 25(ファイル送信サーバ制限超過によるキャパシティの処理):サーバの速度制限が原因でファイル キャパシティが処理されました • 26(通信障害):クラウド接続失敗が原因でファイル キャパシティが処理されました • 27(未送信):設定が原因でファイルは送信されていません。 • 28(事前分類の一致なし):事前分類でファイル内に埋め込みオブジェクトまたは疑わしいオブジェクトが検出されなかったため、ファイルはダイナミック分析用に送信されませんでした • 29(Transmit Sent Sandbox Private Cloud):ダイナミック分析のためにファイルがプライベート クラウドに送信されました。 • 30(送信ボックスはプライベート クラウドに未送信):ファイルは分析のためにプライベート クラウドに送信されませんでした

表 3-47　6.0 以上のファイル イベントのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
ローカルのマルウェア分析ステータス	uint8	ファイルのマルウェア分析ステータス。値は以下のとおりです。 • 0:ファイルが分析されません • 1:分析が実行されました • 2:分析が失敗しました • 3:手動による分析の要求
アーカイブ ファイル ステータス	uint8	調査中のアーカイブのステータス。次のいずれかの値になります。 • 0(N/A):ファイルがアーカイブとして検査されていません。 • 1:保留中。アーカイブは調査中です • 2:取得済み。調査が問題なく正常に実行されました • 3:失敗。システムのリソース不足のため調査に失敗しました。 • 4:深度の超過。調査は正常に実行されましたが、アーカイブがネストされた調査の深度を超過しました • 5:暗号化。部分的に正常に実行されましたが、アーカイブが暗号化されているか、暗号化されたアーカイブが含まれています • 6:調査できませんでした。部分的に正常に実行されましたが、ファイル形式が不正であるか破損しています
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ～ 100)。
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト • 6:クラウド ルックアップのタイムアウト • 7:カスタム検出 • 8:カスタム検出ブロック • 9:アーカイブ ブロック(深度超過) • 10:アーカイブ ブロック(暗号化されている) • 11:アーカイブ ブロック(調査エラー)
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。

表 3-47　6.0 以上のファイル イベントのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
ファイル タイプ ID	uint32	ファイル タイプにマップされている ID 番号。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、AMP for Endpoints ファイル タイプのメタデータ (3-44 ページ) を参照してください。
ファイル名	string	ファイルの名前。
ファイル サイズ	uint64	ファイルのサイズ(バイト単位)。
方向	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示す値。次のいずれかの値になります。 • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
アプリケーション ID	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
URI	string	接続の Uniform Resource Identifier(URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。

表 3-47　6.0 以上のファイル イベントのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 3-47　6.0 以上のファイル イベントのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
SSL フロー ステータス	uint16	SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。 • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
文字列ブロック タイプ	uint32	アーカイブ SHA を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 3-47　6.0 以上のファイル イベントのデータ ブロック フィールド(続き)

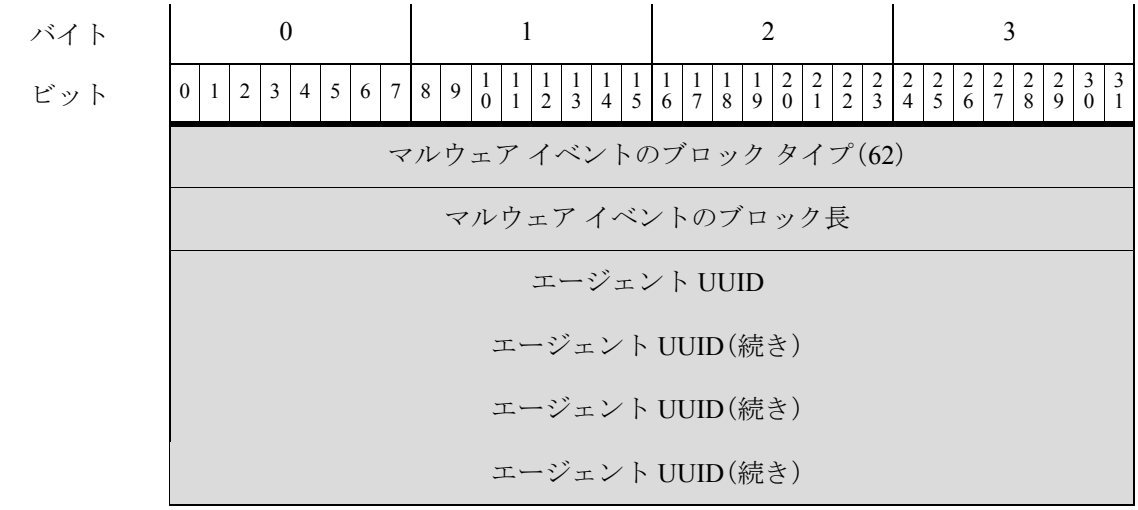
フィールド	データ タイプ	説明
文字列ブロック長	uint32	アーカイブ SHA 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および侵入ポリシー名のバイト数を含む)。
アーカイブ SHA	string	ファイルが含まれる親アーカイブの SHA1 ハッシュ。
文字列ブロック タイプ	uint32	アーカイブ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	アーカイブ名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびアーカイブ名のバイト数を含む)。
アーカイブ名	string	親アーカイブの名前。
アーカイブ深度	uint8	ファイルがネストされている層の数。たとえば、テキスト ファイルが zip アーカイブ内にある場合、この値は 1 になります。

マルウェア イベントのデータ ブロック 6.0 以上

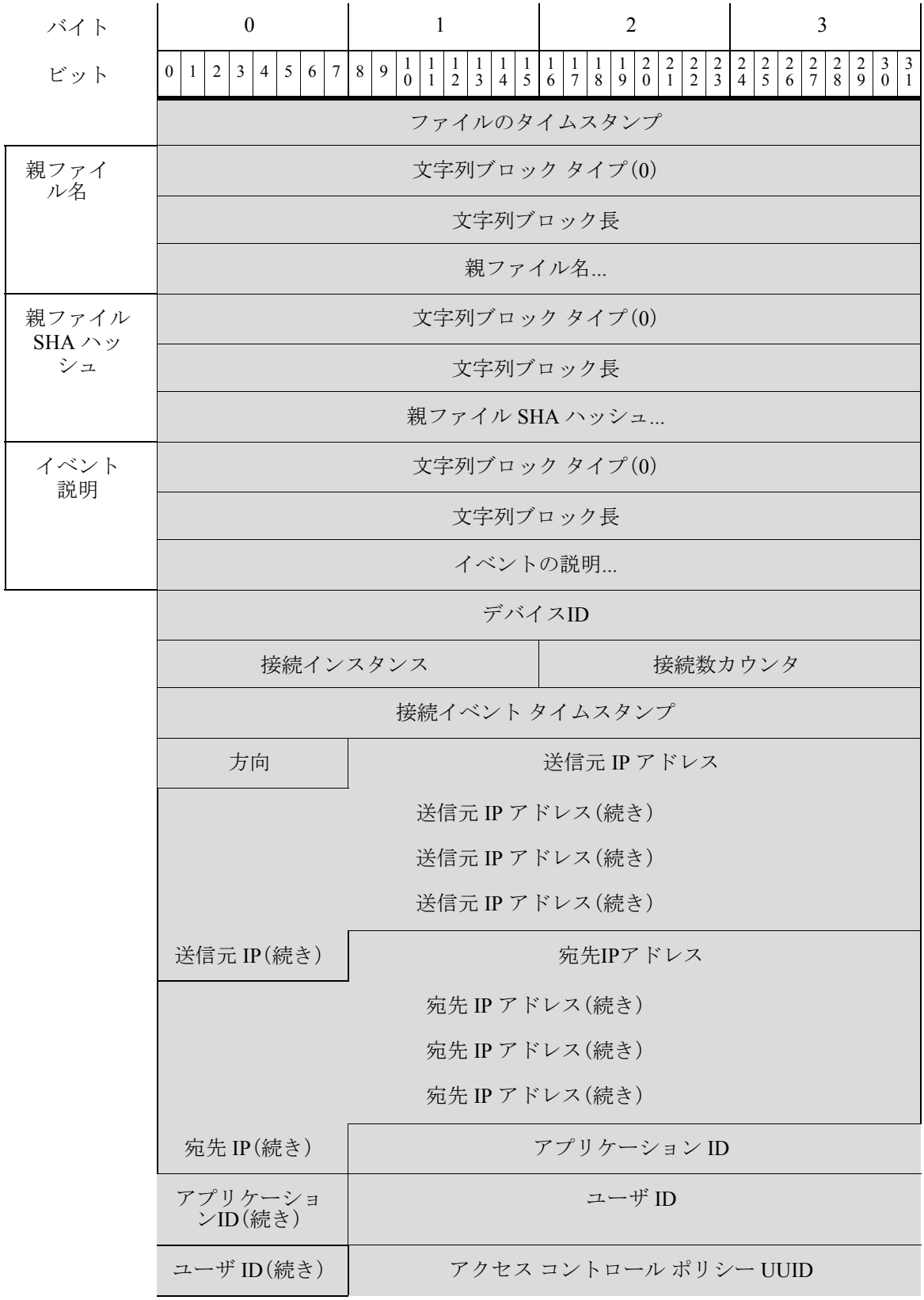
eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェア イベントのデータ ブロックは、シリーズ 2 グループのブロックのブロック タイプ 62 です。これはブロック 47 に取って代わります。HTTP レスポンスのフィールドが追加されました。

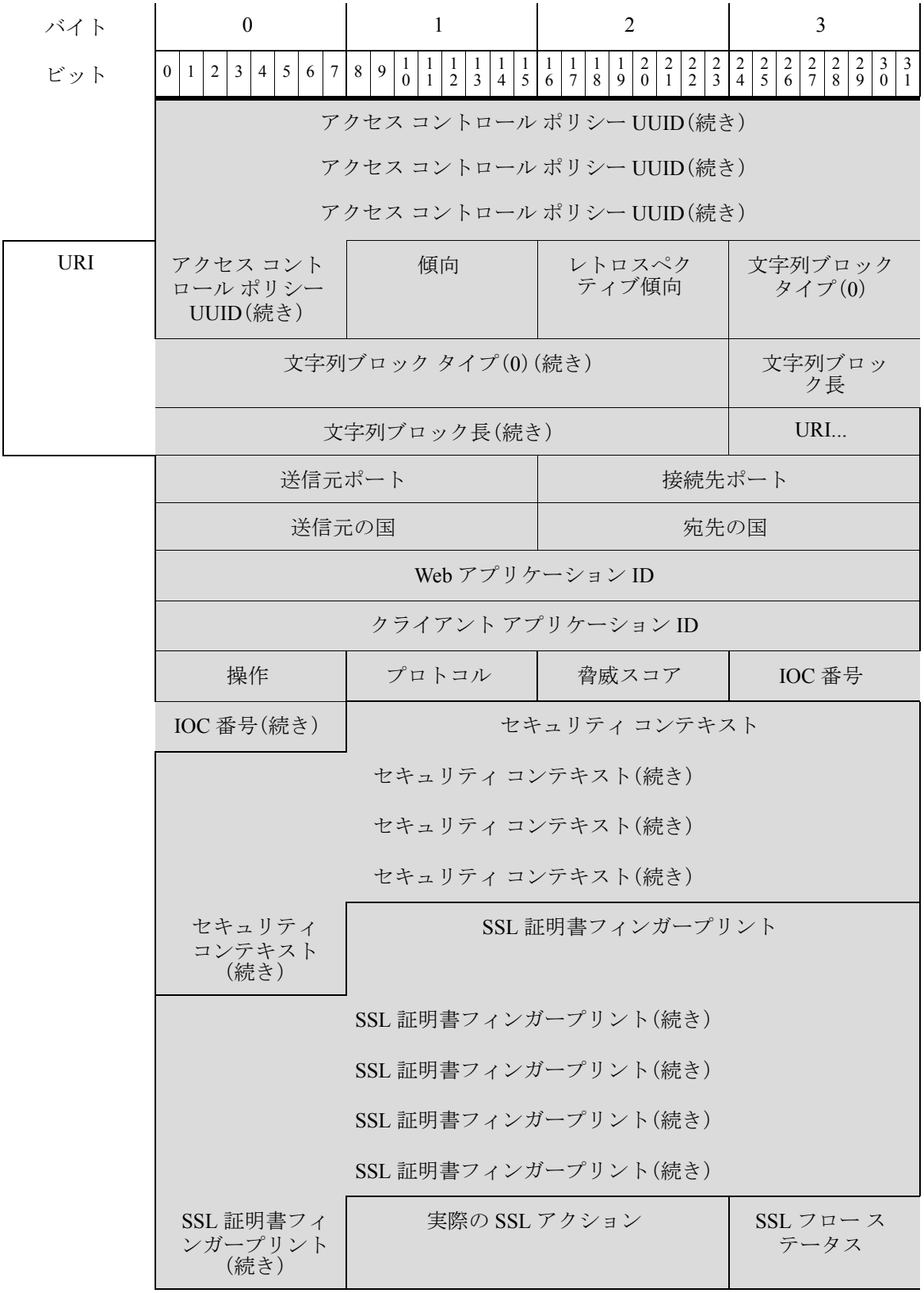
イベント バージョンが 7 でイベント コードが 101 の要求メッセージでマルウェア イベント フラグ([要求フラグ(Request Flags)] フィールドのビット 30)を設定することで、マルウェア イベント レコードの一部としてイベントを要求します。

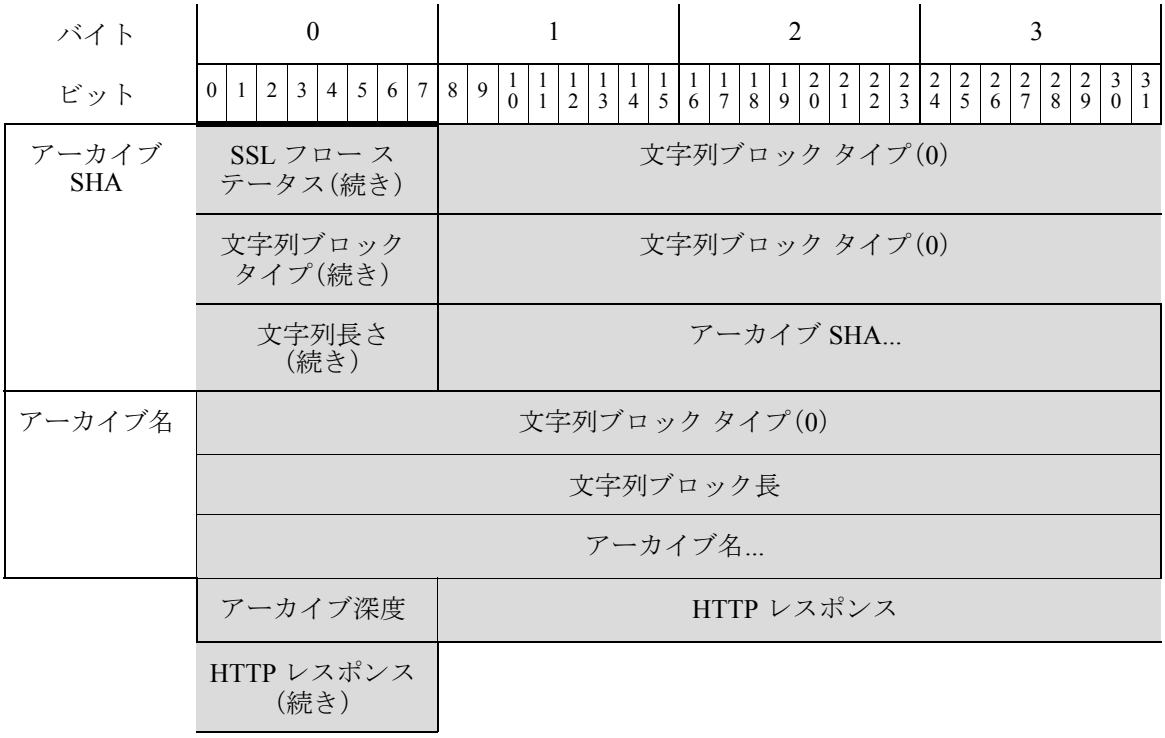
次の図に、マルウェア イベントのデータ ブロックの構造を示します。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	クラウド UUID																															
	クラウド UUID（続き）																															
	クラウド UUID（続き）																															
	クラウド UUID（続き）																															
	マルウェア イベント タイムスタンプ																															
	イベント タイプ ID																															
	イベント サブタイプ ID																															
検出名	ディテクタ ID								文字列ブロック タイプ（0）																							
	文字列ブロック タイプ（0）（続き）								文字列ブロック長																							
	文字列ブロック長（続き）								検出名...																							
ユーザ	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル名...																															
ファイル パス	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル パス...																															
ファイル SHA ハッシュ（Hash）	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイル サイズ																															
	ファイル タイプ																															


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
ファイルのタイムスタンプ
親ファイル名
文字列ブロック タイプ(0)
文字列ブロック長
親ファイル名...
親ファイル SHA ハッシュ
文字列ブロック タイプ(0)
文字列ブロック長
親ファイル SHA ハッシュ...
イベント説明
文字列ブロック タイプ(0)
文字列ブロック長
イベントの説明...
デバイスID
接続インスタンス
接続数カウンタ
接続イベント タイムスタンプ
方向
送信元 IP アドレス
送信元 IP アドレス(続き)
送信元 IP アドレス(続き)
送信元 IP アドレス(続き)
送信元 IP(続き)
宛先IPアドレス
宛先 IP アドレス(続き)
宛先 IP アドレス(続き)
宛先 IP アドレス(続き)
宛先 IP(続き)
アプリケーション ID
アプリケーションID(続き)
ユーザ ID
ユーザ ID(続き)
アクセス コントロール ポリシー UUID


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
アクセス コントロール ポリシー UUID（続き）
アクセス コントロール ポリシー UUID（続き）
アクセス コントロール ポリシー UUID（続き）
URI
アクセス コントロール ポリシー UUID（続き）
傾向
レトロスペクティブ傾向
文字列ブロック タイプ（0）
文字列ブロック タイプ（0）（続き）
文字列ブロック長
文字列ブロック長（続き）
URI...
送信元ポート
接続先ポート
送信元の国
宛先の国
Web アプリケーション ID
クライアント アプリケーション ID
操作
プロトコル
脅威スコア
IOC 番号
IOC 番号（続き）
セキュリティ コンテキスト
セキュリティ コンテキスト（続き）
セキュリティ コンテキスト（続き）
セキュリティ コンテキスト（続き）
セキュリティ コンテキスト（続き）
SSL 証明書フィンガープリント
SSL 証明書フィンガープリント（続き）
SSL 証明書フィンガープリント（続き）
SSL 証明書フィンガープリント（続き）
SSL 証明書フィンガープリント（続き）
SSL 証明書フィンガープリント（続き）
実際の SSL アクション
SSL フロー ステータス



次の表は、マルウェア イベントのデータ ブロックのフィールドについての説明です。

表 3-48　6.0 以上のマルウェア イベントのデータ ブロック フィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 62 です。
マルウェア イベントのブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする AMP for Endpoints エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェア イベントの発生元 AMP cloud の、内部の固有 ID。
マルウェア イベント タイムスタンプ	uint32	マルウェア イベント生成時のタイムスタンプ。
イベント タイプ ID	uint32	マルウェア イベント タイプの内部 ID。
イベント サブタイプ ID	uint32	マルウェア検出につながったアクションの内部 ID。
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。
文字列ブロック タイプ	uint32	検出名を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 3-48　6.0 以上のマルウェア イベントのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	検出名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロック タイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ フィールドのバイト数を含む)。
ユーザ	string	シスコ Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイル パスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル パス文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル パス フィールドのバイト数を含む)。
ファイル パス	string	検出または検疫されたファイルのファイル パス。ファイル名は含まれません。
文字列ブロック タイプ	uint32	ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル SHA ハッシュ フィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値のレンダリングされた文字列。
ファイル サイズ	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイル タイプ	uint32	検出または検疫されたファイルのファイル タイプ。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、AMP for Endpoints ファイル タイプのメタデータ (3-44 ページ) を参照してください。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。

表 3-48　6.0 以上のマルウェア イベントのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	親ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロック タイプ	uint32	親ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル SHA ハッシュ フィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロック タイプ	uint32	イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベント タイプに関連付けられている追加イベント情報。
デバイスID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または IDS イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続イベント タイムスタンプ	uint32	接続イベントのタイムスタンプ。
方向	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示します。次のいずれかの値になります。 • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。

表 3-48　6.0 以上のマルウェア イベントのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する ID 番号。
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4:UNAVAILABLE。ソフトウェアから AMP cloud に対して、特性を確認する要求を送信できなかったか、または AMP cloud サービスが要求に応答しなかった。 • 5(CUSTOM SIGNATURE):ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
レトロスペクティブ特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロック タイプ	uint32	URI を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。

表 3-48　6.0 以上のマルウェア イベントのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト • 6:クラウド ルックアップのタイムアウト • 7:カスタム検出 • 8:カスタム検出ブロック • 9:アーカイブ ブロック(深度超過) • 10:アーカイブ ブロック(暗号化されている) • 11:アーカイブ ブロック(調査エラー)
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ～ 100)。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 3-48　6.0 以上のマルウェア イベントのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
SSL フロー ステータス	uint16	SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。 • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
文字列ブロック タイプ	uint32	アーカイブ SHA を含む文字列データ ブロックを開始します。この値は常に 0 です。

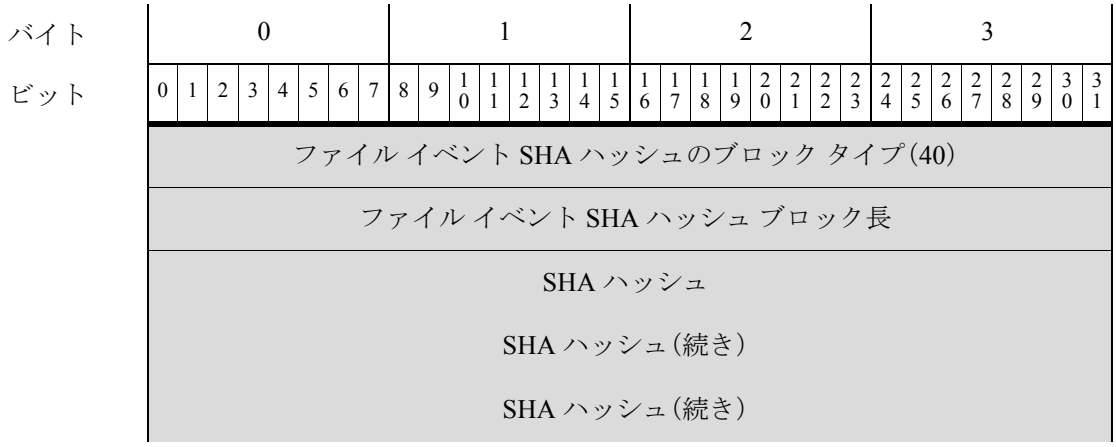
表 3-48　6.0 以上のマルウェア イベントのデータ ブロック フィールド(続き)

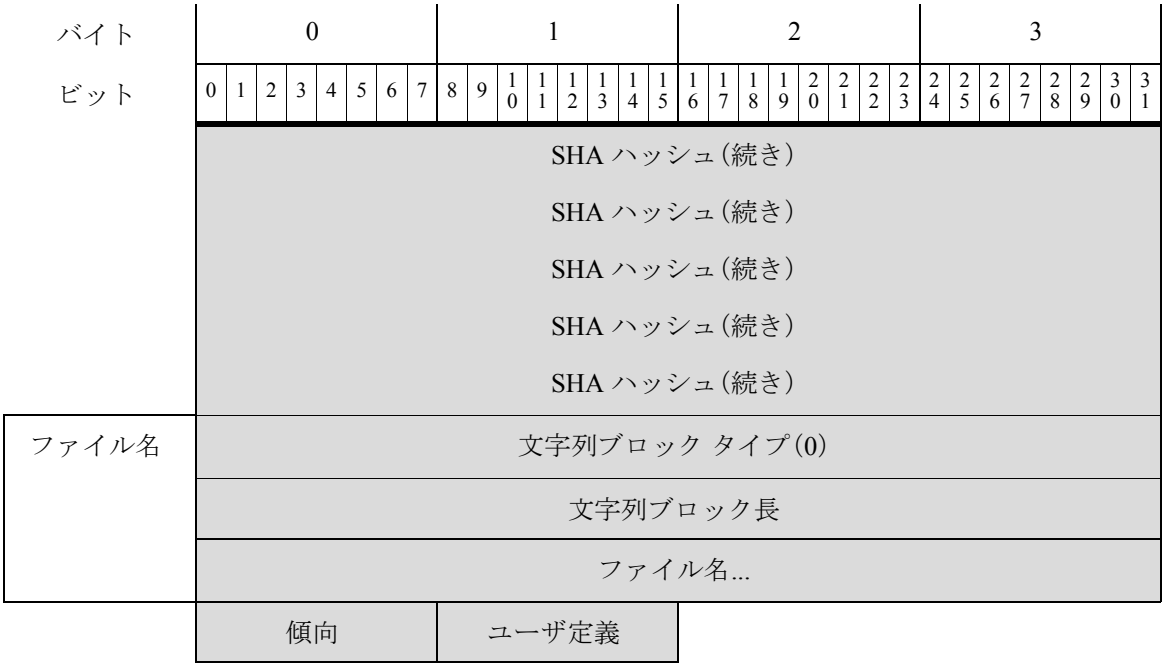
フィールド	データ タイプ	説明
文字列ブロック長	uint32	アーカイブ SHA 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および侵入ポリシー名のバイト数を含む)。
アーカイブ SHA	string	ファイルが含まれる親アーカイブの SHA1 ハッシュ。
文字列ブロック タイプ	uint32	アーカイブ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	アーカイブ名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびアーカイブ名のバイト数を含む)。
アーカイブ名	string	親アーカイブの名前。
アーカイブ深度	uint8	ファイルがネストされている層の数。たとえば、テキスト ファイルが zip アーカイブ内にある場合、この値は 1 になります。
HTTP レスポンス	uint32	HTTP 要求の応答コード。

5.3 以上のファイル イベント SHA ハッシュ

eStreamer サービスは、ファイルの SHA ハッシュとそのファイル名とのマッピングのメタデータを含む、ファイル イベント SHA ハッシュ データ ブロックを使用します。ブロック タイプは、シリーズ 2 リストのデータ ブロックの 40 です。イベント コード 111 の拡張リクエストでファイル ログ イベントが要求されており、ビット 20 が設定されているか、イベント バージョンが 5 でイベント コードが 21 のメタデータが要求されている場合に、要求することができます。

次の図は、ファイル イベント ハッシュ データ ブロックの構造を示しています。





次の表は、ファイル イベント SHA ハッシュ データ ブロックのフィールドについての説明です。

表 3-49　ファイル イベント SHA ハッシュのデータ ブロック フィールド

フィールド	データ タイプ	説明
ファイル イベント SHA ハッシュ ブロック タイプ	uint32	ファイル イベント SHA ハッシュ ブロックを開始します。この値は常に 40 です。
ファイル イベント SHA ハッシュ ブロック長	uint32	ファイル イベント SHA ハッシュ ブロックのバイトの合計数（ファイル イベント SHA ハッシュ ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む）。
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
文字列ブロック タイプ	uint32	ファイルに関連付けられている記述名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
ファイル名または解析結果	string	ファイルの記述名または解析結果。ファイルがクリーンである場合、この値は Clean です。ファイルの解析結果が不明の場合、この値は Neutral です。ファイルにマルウェアが含まれている場合、ファイル名が示されます。

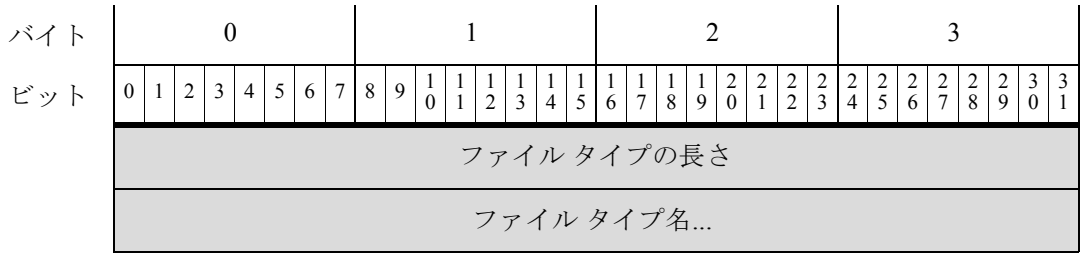
表 3-49　ファイル イベント SHA ハッシュのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4:UNAVAILABLE。ソフトウェアから AMP cloud に対して、特性を確認する要求を送信できなかったか、または AMP cloud サービスが要求に応答しなかった。 • 5(CUSTOM SIGNATURE):ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
ユーザ定義	uint8	ファイル名の表示方法を示します。 • 0:AMP 定義 • 1:ユーザ定義

5.3 以上のファイル タイプ ID のメタデータ

eStreamer サービスは、ファイル タイプ ID のイベントの ファイル タイプ情報を含むメタデータを送信します。形式は次のとおりです。このレコードは、ファイル タイプ名にファイル タイプ ID をマッピングしています。メタデータ フラグのいずれか(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 1、14、15、または 20)が設定されていると、ファイル タイプ ID の情報が送信されます。要求フラグ(2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにファイル タイプ ID レコードを示す値 510 があることに注意してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(510)															
レコード長																																
ファイル タイプ ID																																



次の表は、ファイル タイプ ID のレコードのフィールドについての説明です。

表 3-50　ファイル タイプ ID のレコード フィールド

フィールド	データ タイプ	説明
ファイル タイプ ID	uint32	ファイル タイプ ID 番号。
ファイル タイプの長さ	uint32	ファイル タイプ名に含まれるバイト数。
ファイル タイプ名	string	ファイル タイプ名の記述名。

5.2 以上のルール ドキュメントのデータ ブロック

eStreamer サービスは、ルール ドキュメントのデータ ブロックを使用して、アラートの生成に使用するルールに関する情報を表示します。ブロック タイプは、シリーズ 2 セットのデータ ブロックの 27 です。タイプ 10 のホスト要求メッセージで要求することができます。詳細については、ホスト要求メッセージの形式（2-27 ページ）を参照してください。

次の図に、ルール ドキュメントのデータ ブロックの構造を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
影響	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	影響...																															
詳細情報	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	詳細情報																															
影響を受けるシステム	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	影響を受けるシステム...																															
攻撃のシナリオ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	攻撃のシナリオ...																															
攻撃のしやすさ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	攻撃のしやすさ...																															
誤検出	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	誤検出...																															
検出漏れ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	検出漏れ...																															
修正処置	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	修正処置...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
提供元	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	共同作成者...																															
その他の参考資料	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	その他の参考資料...																															

次の表は、ルール ドキュメントのデータ ブロックのフィールドについての説明です。

表 3-51　　ルール ドキュメントのデータ ブロック フィールド

フィールド	データ タイプ	説明
ルール ドキュメントのデータ ブロック タイプ	uint32	ルール ドキュメントのデータ ブロックを開始します。この値は常に 27 です。
ルール ドキュメントのデータ ブロック長	uint32	ルール ドキュメントのデータ ブロックの合計バイト数です。ルール ドキュメントのデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
ルール ID(シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
文字列ブロック タイプ	uint32	ルールに関連付けられたサマリーを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとサマリー フィールドのバイト数が含まれます。
要約	string	脅威または脆弱性の説明。
文字列ブロック タイプ	uint32	ルールに関連付けられた影響を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと影響フィールドのバイト数が含まれます。
影響	string	この脆弱性を利用した侵害がさまざまなシステムに与える可能性のある影響。

表 3-51　ルール ドキュメントのデータ ブロック フィールド(続き)

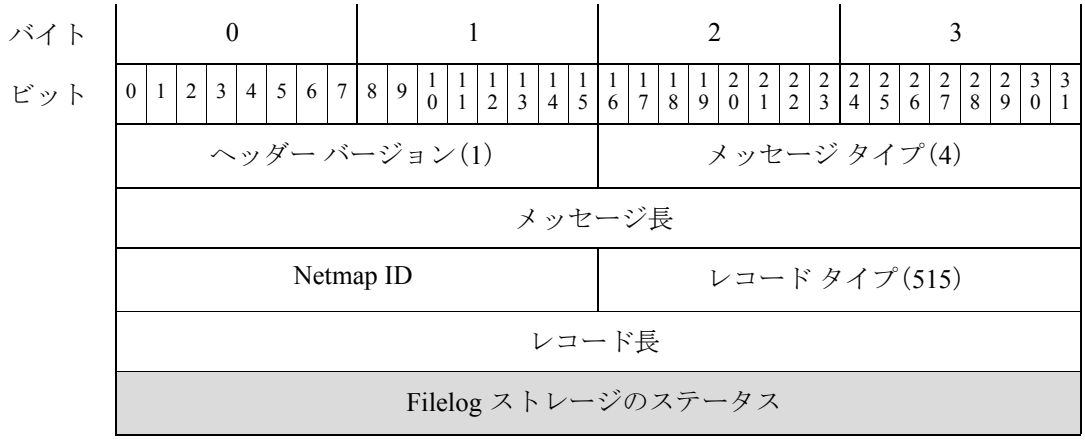
フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	ルールに関連付けられた詳細情報を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと詳細情報 フィールドのバイト数が含まれます。
詳細情報	string	基礎となる脆弱性、ルールが実際に検索する内容、および影響を受けるシステムに関する情報。
文字列ブロック タイプ	uint32	ルールに関連付けられた影響を受けるシステムのリストを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと影響を受ける システム フィールドのバイト数が含まれます。
影響を受けるシステム	string	脆弱性の影響を受けるシステム。
文字列ブロック タイプ	uint32	ルールに関連付けられた潜在的な攻撃のシナリオを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと攻撃のシナリオ フィールドのバイト数が含まれます。
攻撃のシナリオ	string	潜在的な攻撃の例。
文字列ブロック タイプ	uint32	ルールに関連付けられた攻撃のしやすさを含む文字列 データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと攻撃のしやすさフィールドのバイト数が含まれます。
攻撃のしやすさ	string	攻撃の難易度(simple、medium、hard、または difficult)と、その攻撃がスクリプトを使用して実行できるものであるかどうか。
文字列ブロック タイプ	uint32	ルールに関連付けられた潜在的な誤検出を含む文字列 データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと誤検出フィールドのバイト数が含まれます。
誤検出	string	誤検出となる可能性のある例。デフォルト値は `None Known` です。
文字列ブロック タイプ	uint32	ルールに関連付けられた潜在的な検出漏れを含む文字列 データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと検出漏れ フィールドのバイト数が含まれます。
検出漏れ	string	検出漏れとなる可能性のある例。デフォルト値は `None Known` です。

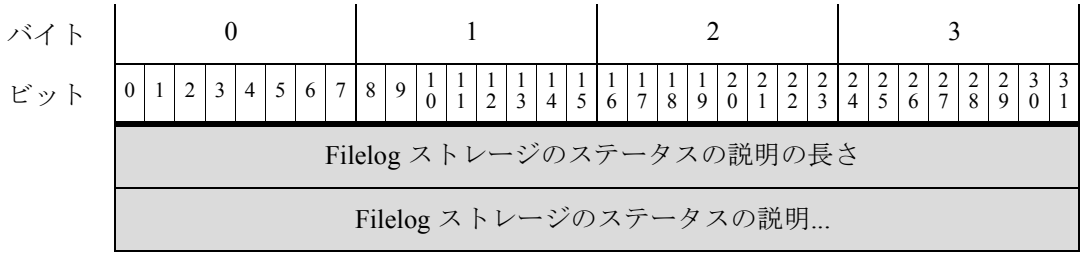
表 3-51　ルール ドキュメントのデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	ルールに関連付けられた修正処置を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと修正処置 フィールドのバイト数が含まれます。
修正処置	string	脆弱性を排除または緩和するためのパッチ、更新、およびその他の手段に関する情報。
文字列ブロック タイプ	uint32	ルールの提供元を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと共同作成者 フィールドのバイト数が含まれます。
提供元	string	ルールおよびその他の関連ドキュメントの作成者の連絡先情報。
文字列ブロック タイプ	uint32	ルールに関連付けられたその他の参考資料を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとその他の参考資料フィールドのバイト数が含まれます。
その他の参考資料	string	その他の情報およびリファレンス。

6.0 以上の Filelog ストレージのメタデータ

eStreamer サービスは、filelog ストレージ情報を含むメタデータを送信します。メッセージ長 フィールドの後に表示されるレコード タイプ フィールドに Filelog ストレージのメタデータ レコードを示す値 515 があることに注意してください。





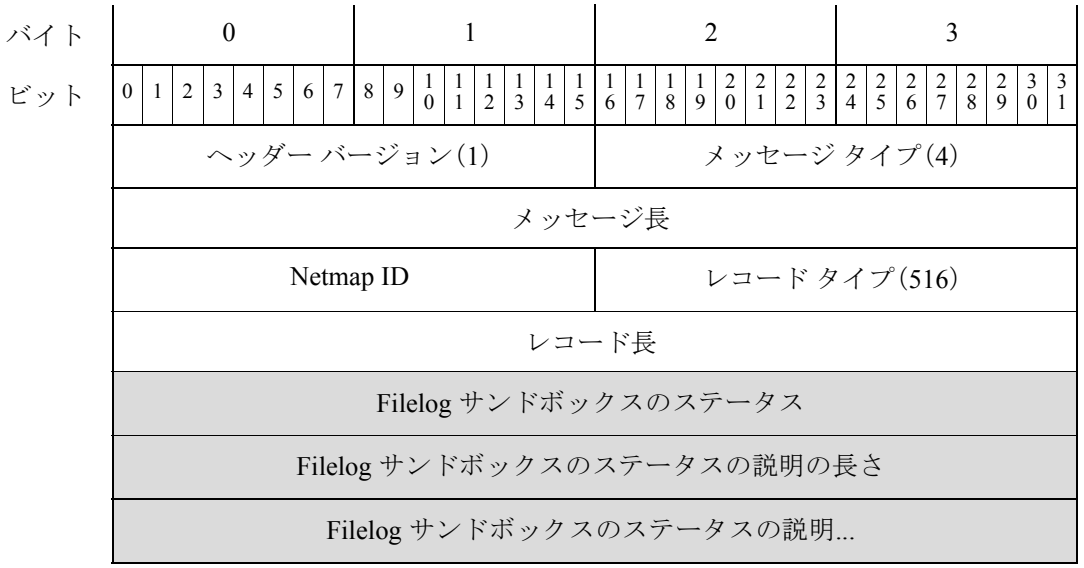
次の表は、Filelog ストレージのメタデータのレコードのフィールドについての説明です。

表 3-52　Filelog ストレージのメタデータのレコード フィールド

フィールド	データ タイプ	説明
Filelog ストレージのステータス	uint32	filelog ストレージのステータスを示す番号
Filelog ストレージのステータスの説明の長さ	uint32	Filelog ストレージのステータスの説明に含まれるバイト数。
Filelog ストレージのステータスの説明	string	filelog ストレージのステータスの記述名。

6.0 以上の Filelog サンドボックスのメタデータ

eStreamer サービスは、filelog サンドボックス情報を含むメタデータを送信します。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに Filelog サンドボックスのメタデータ レコードを示す値 516 があることに注意してください。



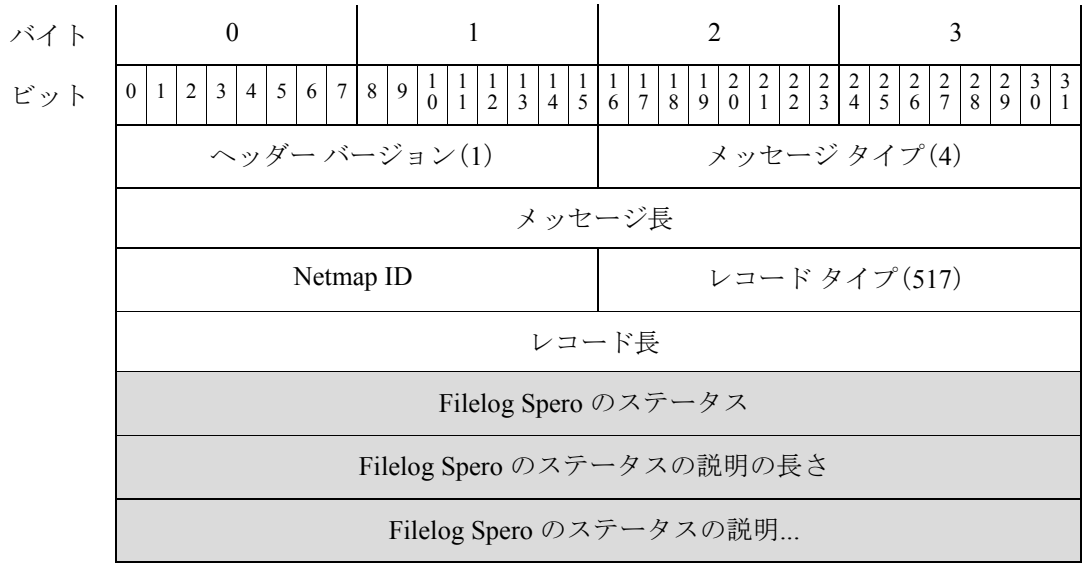
次の表は、Filelog サンドボックスのメタデータのレコードのフィールドについての説明です。

表 3-53　Filelog サンドボックスのメタデータのレコード フィールド

フィールド	データ タイプ	説明
Filelog サンドボックスのステータス	uint32	filelog サンドボックスのステータスを示す番号
Filelog サンドボックスのステータスの説明の長さ	uint32	Filelog サンドボックスのステータスの説明に含まれるバイト数。
Filelog サンドボックスのステータスの説明	string	filelog サンドボックスのステータスの記述名。

6.0 以上の Filelog Spero のメタデータ

eStreamer サービスは、filelog の spero 情報を含むメタデータを送信します。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに filelog spero のメタデータ レコードを示す値 517 があることに注意してください。



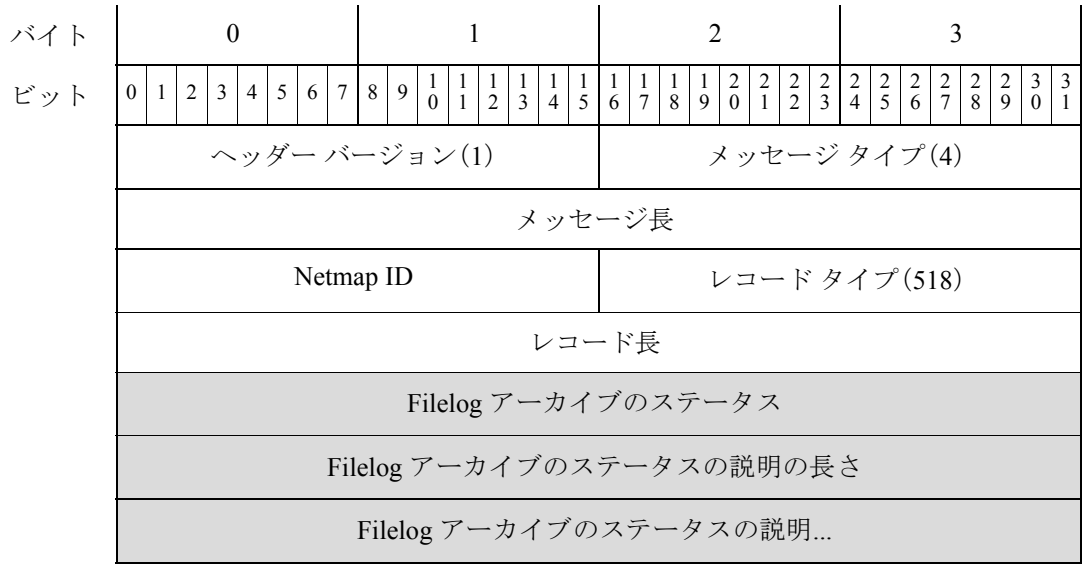
次の表は、Filelog Spero のメタデータのレコードのフィールドについての説明です。

表 3-54　Filelog Spero のメタデータのレコード フィールド

フィールド	データ タイプ	説明
Filelog Spero のステータス	uint32	filelog spero のステータスを示す番号
Filelog Spero のステータスの説明の長さ	uint32	Filelog Spero のステータスの説明に含まれるバイト数。
Filelog Spero のステータスの説明	string	filelog spero のステータスの記述名。

6.0 以上の Filelog アーカイブのメタデータ

eStreamer サービスは、filelog のアーカイブ情報を含むメタデータを送信します。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに Filelog アーカイブのメタデータ レコードを示す値 518 があることに注意してください。



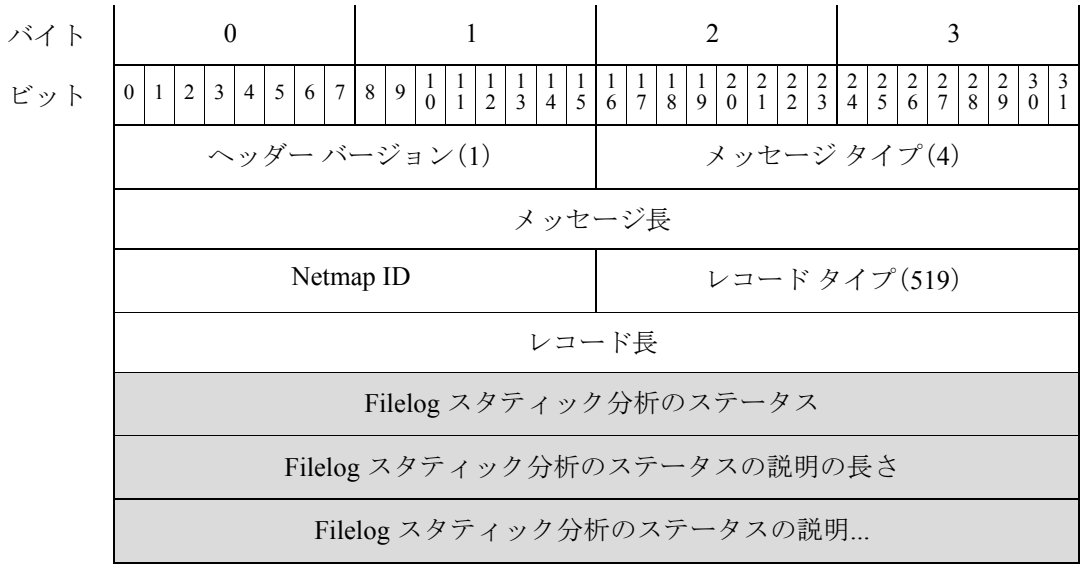
次の表は、Filelog アーカイブのメタデータのレコードのフィールドについての説明です。

表 3-55　Filelog アーカイブのメタデータのレコード フィールド

フィールド	データ タイプ	説明
Filelog アーカイブのステータス	uint32	filelog アーカイブのステータスを示す番号
Filelog アーカイブのステータスの説明の長さ	uint32	Filelog アーカイブのステータスの説明に含まれるバイト数。
Filelog アーカイブのステータスの説明	string	filelog アーカイブ ステータスの記述名。

6.0 以上の Filelog スタティック分析のメタデータ

eStreamer サービスは、filelog のスタティック分析情報を含むメタデータを送信します。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに Filelog スタティック分析のメタデータ レコードを示す値 519 があることに注意してください。



次の表は、Filelog スタティック分析のメタデータのレコードのフィールドについての説明です。

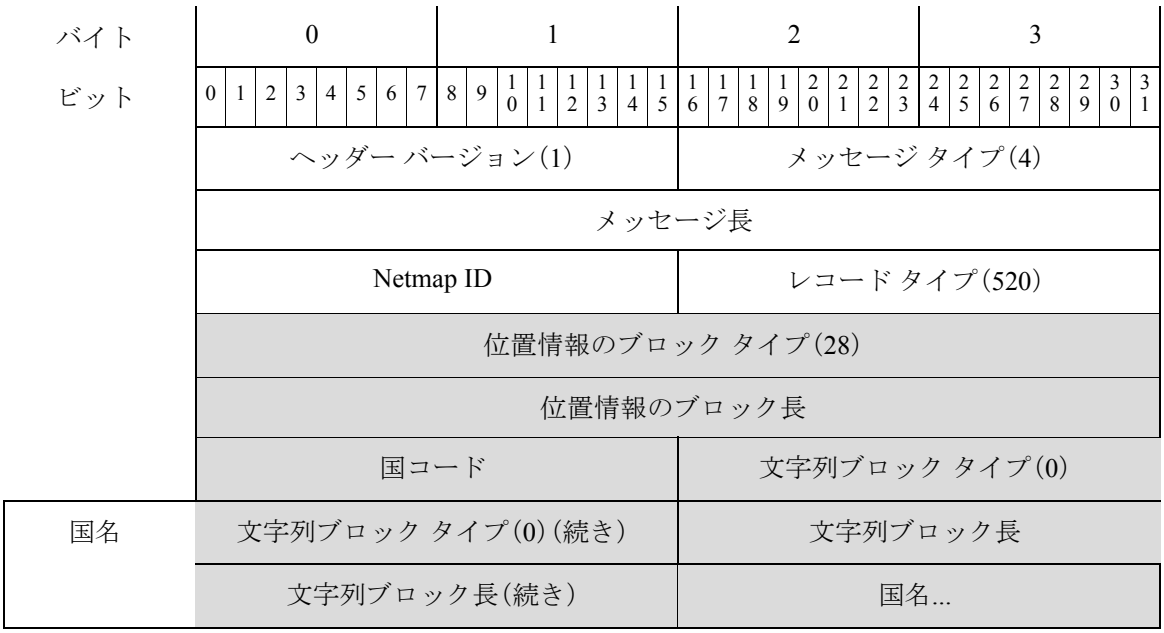
表 3-56　Filelog スタティック分析のメタデータのレコード フィールド

フィールド	データ タイプ	説明
Filelog スタティック分析のステータス	uint32	filelog スタティック分析のステータスを示す番号
Filelog スタティック分析のステータスの説明の長さ	uint32	Filelog スタティック分析のステータスの説明に含まれるバイト数。
Filelog スタティック分析のステータスの説明	string	filelog スタティック分析のステータスの記述名。

5.2 以上の位置情報のデータ ブロック

これは、国名に対する国コードのマッピングを含むデータ ブロックです。レコード タイプは 520 で、ブロック タイプはシリーズ 2 の 28 です。位置情報を持つイベントのメタデータとして公開されます。メタデータが要求されたときにイベントに国コードの値がある場合は、このブロックが他のメタデータとともに戻されます。

次の図に、位置情報のデータ ブロックの構造を示します。



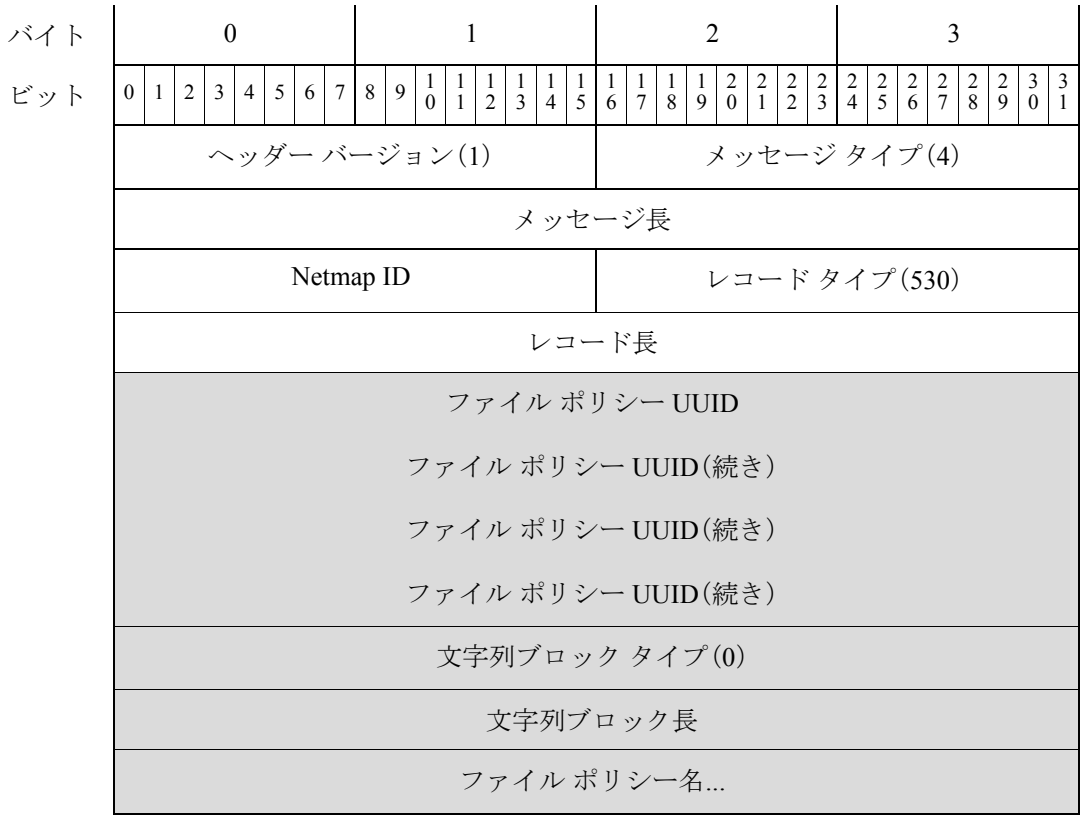
次の表は、位置情報のデータ ブロックのフィールドについての説明です。

表 3-57　位置情報のデータ ブロック フィールド

フィールド	データ タイプ	説明
位置情報のデータ ブロック タイプ	uint32	位置情報のデータ ブロックを開始します。この値は常に 28 です。
位置情報のデータ ブロック長	uint32	位置情報のデータ ブロックの合計バイト数です。位置情報のデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
国コード	uint16	国コード。
文字列ブロック タイプ	uint32	国コードに関連付けられた国名を含む文字列のデータのブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと国名フィールドのバイト数が含まれます。
国名	string	国コードに関連付けられた国の名前。

6.0 以上のファイル ポリシー名

eStreamer サービスは、ファイル ポリシー名の情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグのいずれか(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 1、14、15、または 20)が設定されていると、ファイル ポリシー名の情報が送信されます。要求フラグ(2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにファイル ポリシー名レコードを示す値 530 があることに注意してください。



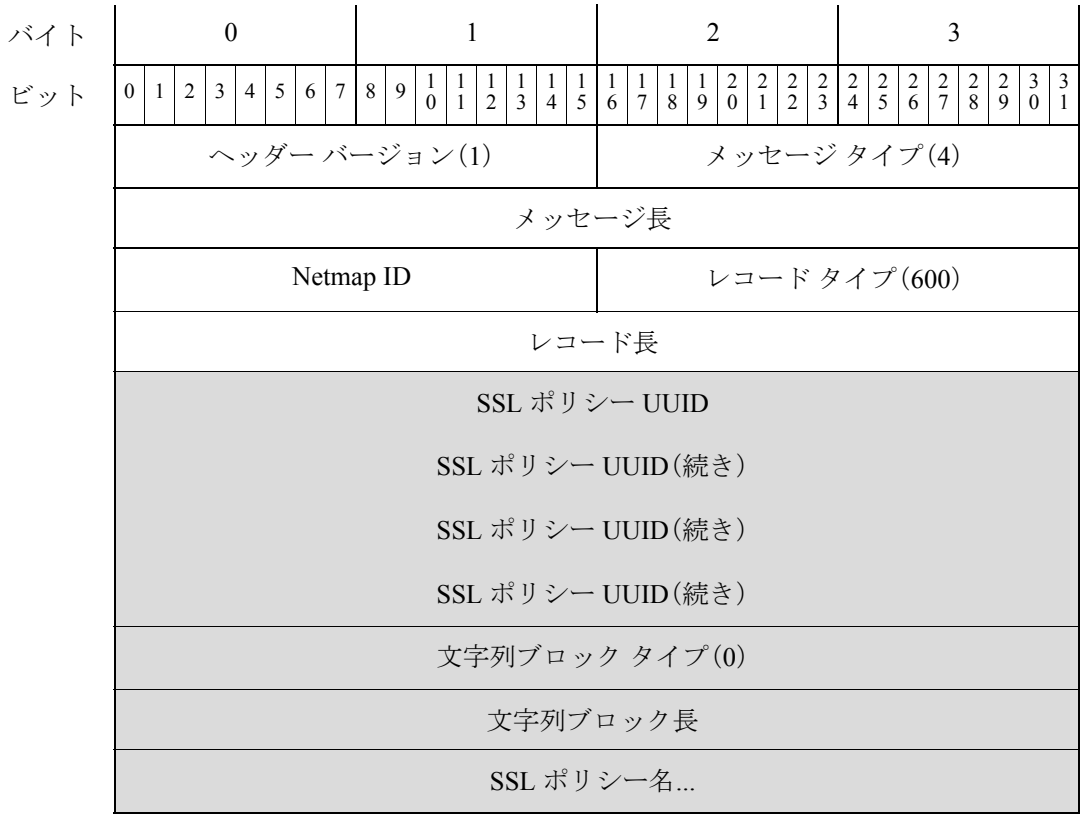
次の表は、ファイル ポリシー名のレコードのフィールドについての説明です。

表 3-58　ファイル ポリシー名フィールド

フィールド	データ タイプ	説明
ファイル ポリシー UUID	uint8[16]	ファイル ポリシーの UUID
文字列ブロック タイプ	uint32	ファイル ポリシー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	SSL ポリシー名の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとファイル ポリシー名のバイト数が含まれます。
ファイル ポリシー名	string	ファイル ポリシーの名前。

SSL ポリシー名

eStreamer サービスは、SSL ポリシー名の情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグのいずれか(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 1、14、15、または 20)が設定されていると、SSL ポリシー名の情報が送信されます。要求フラグ(2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに SSL ポリシー名レコードを示す値 600 があることに注意してください。



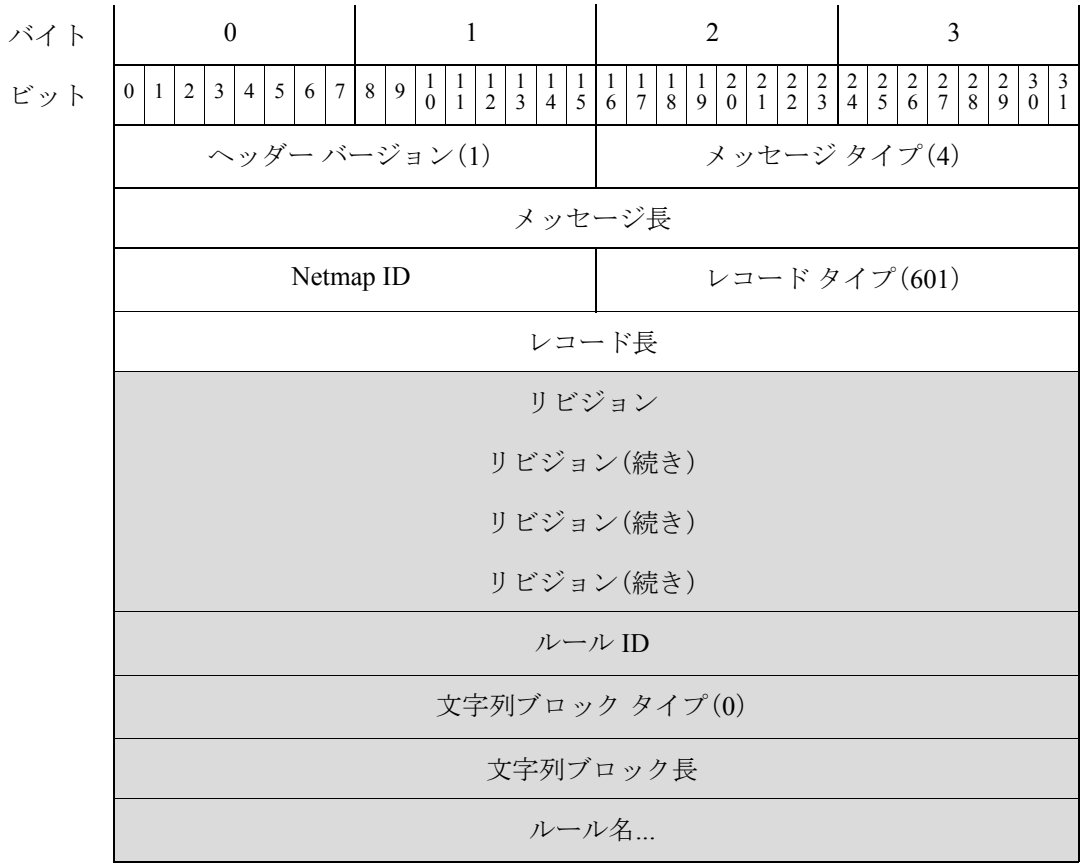
次の表は、SSL ポリシー名のレコードのフィールドについての説明です。

表 3-59　SSL ポリシー名レコード フィールド

フィールド	データ タイプ	説明
SSL ポリシー UUID	uint8[16]	SSL ポリシーの UUID
文字列ブロック タイプ	uint32	SSL ポリシーの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	SSL ポリシー名の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと SSL ポリシー名のバイト数が含まれます。
SSL ポリシー名	string	SSL ポリシーの名前。

SSL ルール ID

eStreamer サービスは、SSL ルール ID の情報を含むメタデータを送信します。形式は次のとおりです。（メタデータ フラグのいずれか（要求メッセージの [要求フラグ（Request Flags）] フィールドのビット 1、14、15、または 20）が設定されていると、SSL ルール ID の情報が送信されます。要求フラグ（2-12 ページ） を参照してください）。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに SSL ルール ID レコードを示す値 `601` があることに注意してください。



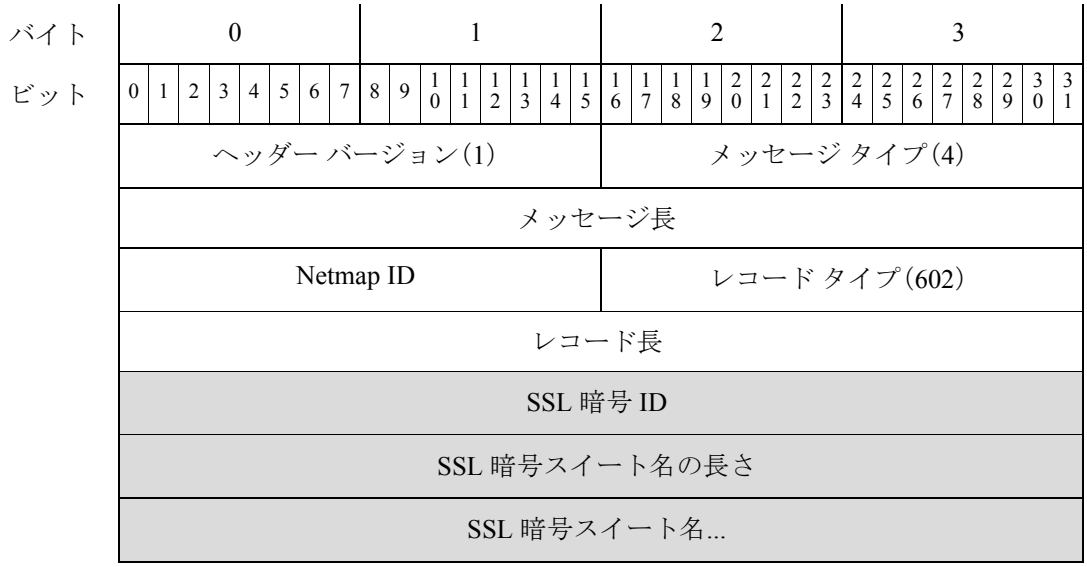
次の表は、SSL ルール ID レコードのフィールドについての説明です。

表 3-60　　SSL ポリシー名レコード フィールド

フィールド	データ タイプ	説明
リビジョン	uint8[16]	SSL ルール リビジョンの UUID
ルール ID	uint32	SSL ルール ID 番号
文字列ブロック タイプ	uint32	SSL ルールの名前を含む文字列データ ブロックを開始します。この値は常に `0` です。
文字列ブロック長	uint32	SSL ルール名の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと SSL ルール名のバイト数が含まれます。
SSL ルール名	string	SSL ルールの名前。

SSL 暗号スイート（SSL Cipher Suite）

eStreamer サービスは、SSL 暗号 ID のイベントの SSL 暗号スイート情報を含むメタデータを送信します。形式は次のとおりです。このレコードは、SSL 暗号スイート名に SSL 暗号 ID をマッピングします。（メタデータ フラグのいずれか（要求メッセージの [要求フラグ（Request Flags）] フィールドのビット 1、14、15、または 20）が設定されていると、SSL 暗号スイートの情報が送信されます。要求フラグ（2-12 ページ） を参照してください）。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに SSL 暗号スイート レコードを示す値 602 があることに注意してください。



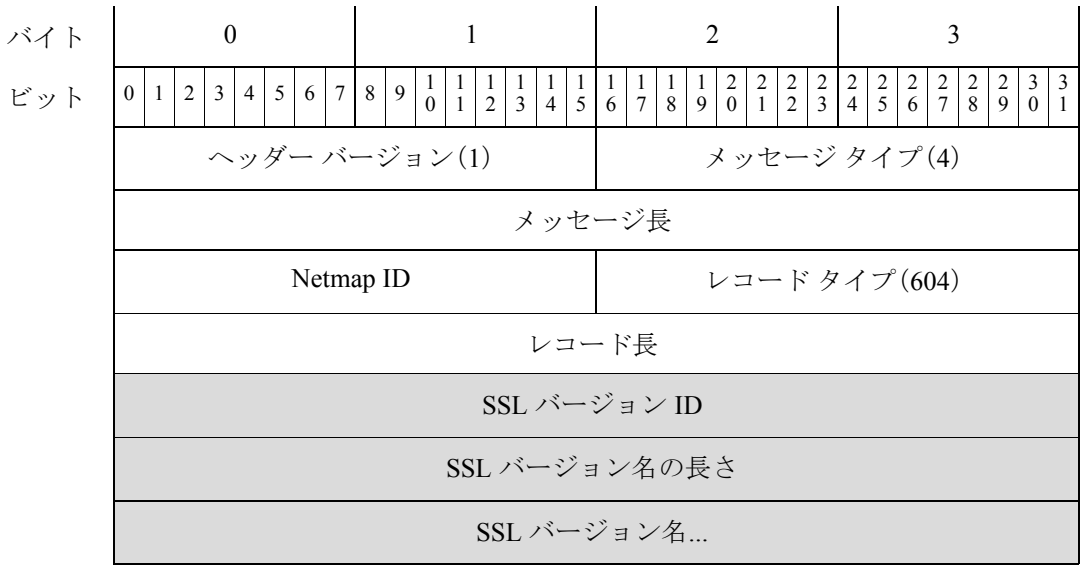
次の表は、SSL 暗号スイート レコードのフィールドについての説明です。

表 3-61　SSL 暗号スイート フィールド

フィールド	データ タイプ	説明
SSL 暗号 ID	uint32	SSL 暗号 ID 番号。
SSL 暗号スイート名の長さ	uint32	SSL 暗号スイート名に含まれるバイト数。
SSL 暗号スイート名	string	SSL 暗号スイートの記述名。

SSL バージョン

eStreamer サービスは、SSL バージョンのイベントの SSL バージョン情報を含むメタデータを送信します。形式は次のとおりです。このレコードは、SSL バージョン名に SSL バージョン ID をマッピングします。（メタデータ フラグのいずれか（要求メッセージの [要求フラグ（Request Flags）] フィールドのビット 1、14、15、または 20）が設定されていると、SSL 暗号スイートの情報が送信されます。要求フラグ（2-12 ページ） を参照してください）。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに SSL バージョン レコードを示す値 604 があることに注意してください。



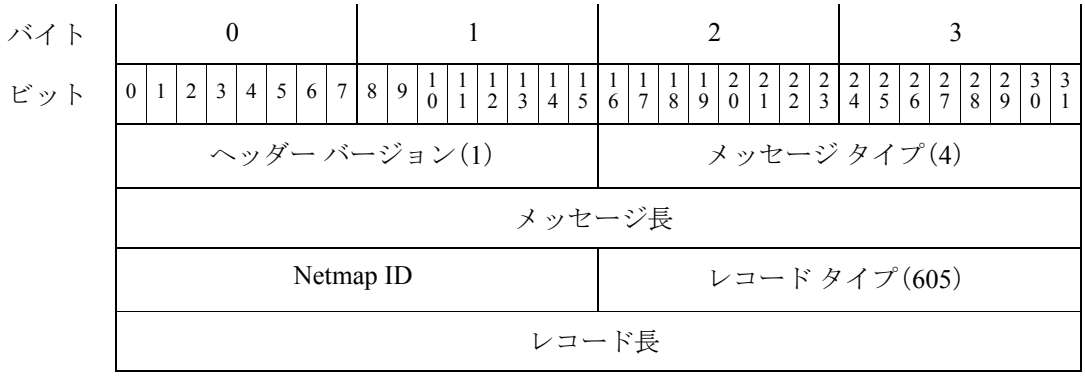
次の表は、SSL バージョン レコードのフィールドについての説明です。

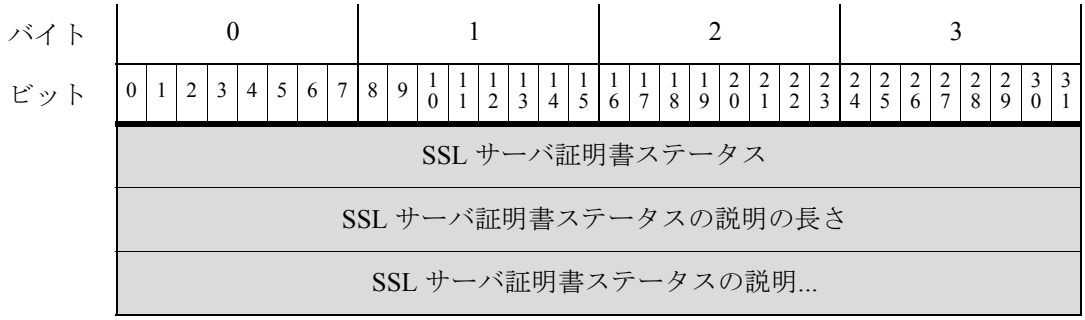
表 3-62　SSL バージョン フィールド

フィールド	データ タイプ	説明
SSL バージョン ID	uint32	SSL バージョン ID 番号。
SSL バージョン名	uint32	SSL バージョン名に含まれるバイト数。
SSL 暗号スイート名	string	SSL バージョンの記述名。

SSL サーバ証明書ステータス

eStreamer サービスは、SSL サーバ証明書ステータス情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグのいずれか(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 1、14、15、または 20)が設定されていると、SSL サーバ証明書ステータスの情報が送信されます。要求フラグ (2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに SSL サーバ証明書ステータス レコードを示す値 605 があることに注意してください。





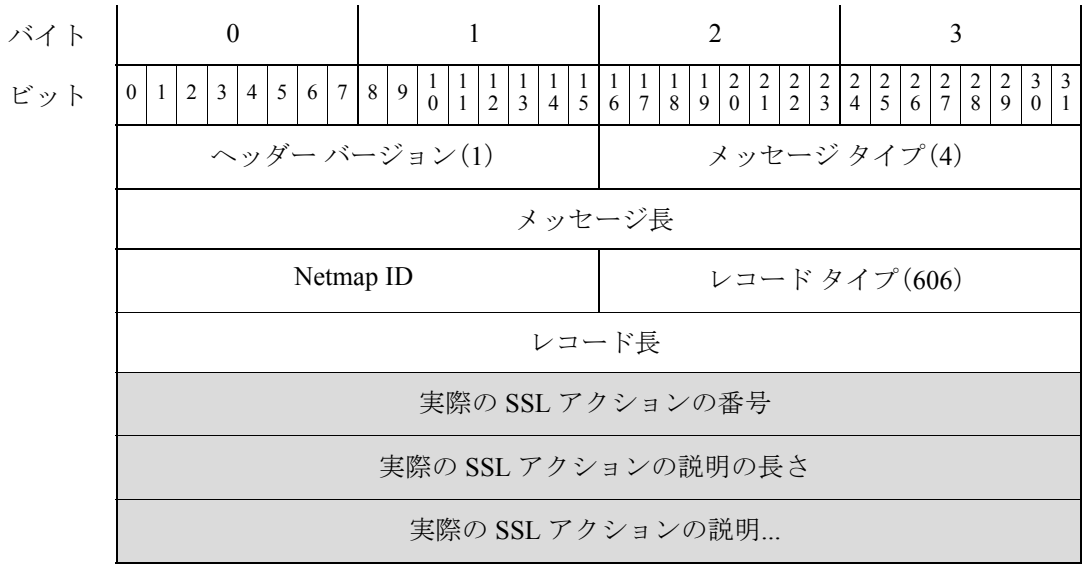
次の表は、SSL サーバ証明書ステータス レコードのフィールドについての説明です。

表 3-63　SSL サーバ証明書ステータス レコード フィールド

フィールド	データ タイプ	説明
SSL サーバ証明書ステータス	uint32	SSL サーバ証明書ステータス番号
SSL サーバ証明書ステータスの説明の長さ	uint32	SSL サーバ証明書ステータスの説明に含まれるバイト数。
SSL サーバ証明書ステータスの説明	string	SSL サーバ証明書ステータスの説明。

実際の SSL アクション

eStreamer は、実際の SSL アクションの情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグのいずれか(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 1、14、15、または 20)が設定されていると、実際の SSL アクションの情報が送信されます。要求フラグ (2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに実際の SSL アクション レコードを示す値 606 があることに注意してください。



次の表は、実際の SSL アクション レコードのフィールドについての説明です。

表 3-64　実際の SSL アクション フィールド

フィールド	データ タイプ	説明
実際の SSL アクションの番号	uint32	実際の SSL アクションを指定する番号
実際の SSL アクションの説明の長さ	uint32	実際の SSL アクションの説明に含まれるバイト数。
実際の SSL アクションの説明	string	実際の SSL アクションの説明。

予期された SSL アクション

eStreamer サービスは、予期していた SSL アクションの情報を含むメタデータを送信します。形式は次のとおりです。（メタデータ フラグのいずれか（要求メッセージの [要求フラグ（Request Flags）] フィールドのビット 1、14、15、または 20）が設定されていると、予期していた SSL アクションの情報が送信されます。要求フラグ（2-12 ページ） を参照してください）。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに予期していた SSL アクション レコードを示す値 607 があることに注意してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（607）															
レコード長																																
予期していた SSL アクションの番号																																
予期していた SSL アクションの説明の長さ																																
予期していた SSL アクションの説明...																																

次の表は、予期していた SSL アクション レコードのフィールドについての説明です。

表 3-65　実際の SSL アクション フィールド

フィールド	データ タイプ	説明
予期していた SSL アクションの番号	uint32	予期していた SSL アクションを指定する番号
予期していた SSL アクションの説明の長さ	uint32	予期していた SSL アクションの説明に含まれるバイト数。
予期していた SSL アクションの説明	string	予期していた SSL アクションの説明。

SSL フロー ステータス

eStreamer サービスは、SSL フロー ステータスの情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグのいずれか(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 1、14、15、または 20)が設定されていると、SSL フロー ステータスの情報が送信されます。要求フラグ (2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに SSL フロー ステータス レコードを示す値 608 があることに注意してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(608)															
レコード長																																
SSL フロー ステータス番号																																
SSL フロー ステータスの説明の長さ																																
SSL フロー ステータスの説明...																																

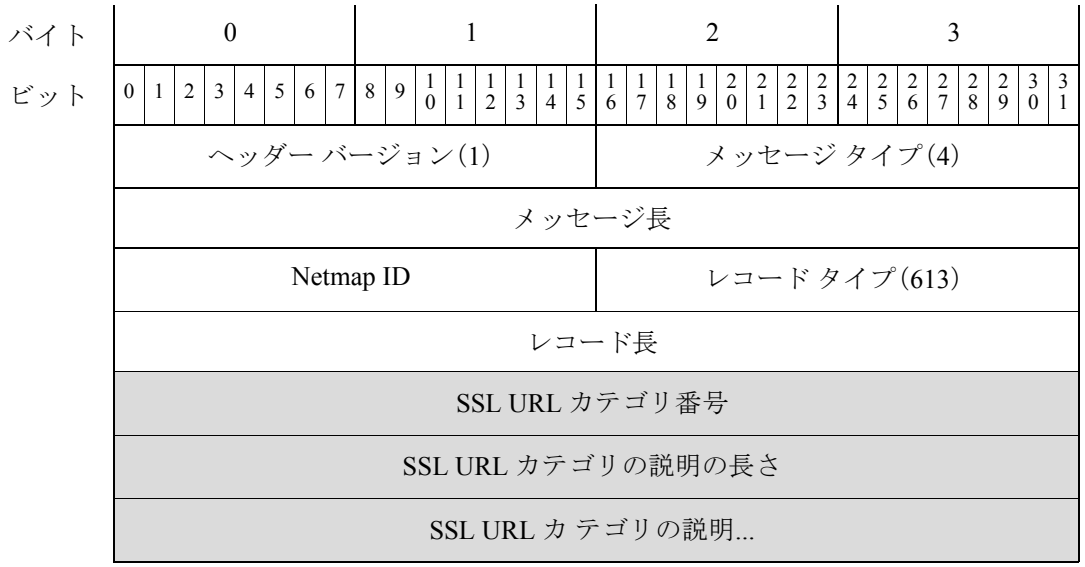
次の表は、SSL フロー ステータス レコードのフィールドについての説明です。

表 3-66　SSL フロー ステータス フィールド

フィールド	データ タイプ	説明
SSL フロー ステータス番号	uint32	SSL フロー ステータスを指定する番号
SSL フロー ステータスの説明の長さ	uint32	SSL フロー ステータスの説明に含まれるバイト数。
SSL フロー ステータスの説明	string	SSL フロー ステータスの説明。

SSL URL カテゴリ

eStreamer サービスは、SSL URL カテゴリの情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグのいずれか(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 1、14、15、または 20)が設定されていると、SSL URL カテゴリの情報が送信されます。要求フラグ(2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに SSL URL カテゴリ レコードを示す値 613 があることに注意してください。



次の表は、SSL URL カテゴリ レコードのフィールドについての説明です。

表 3-67　SSL URL カテゴリ フィールド

フィールド	データ タイプ	説明
SSL URL カテゴリ番号	uint32	SSL URL カテゴリを指定する番号
SSL URL カテゴリの説明の長さ	uint32	SSL サーバ URL カテゴリの説明に含まれるバイト数。
SSL URL カ テゴリの説明	string	SSL URL カテゴリの説明。

5.4 以上の SSL 証明書の詳細のデータ ブロック

これは、SSL 証明書に関する詳細情報を提供するデータ ブロックです。レコード タイプは 614 で、シリーズ 2 のブロック タイプ 50 です。SSL 情報を持つイベントのメタデータとして公開されます。マルウェア イベント、ファイル イベント、侵入イベント、接続イベント、および相関イベントが含まれます。

次の図に、SSL 証明書の詳細のデータ ブロックの構造を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(614)															
レコード長																																
SSL 証明書の詳細のデータ ブロック タイプ(50)																																
SSL 証明書の詳細のブロック長																																
フィンガープリント SHA ハッシュ																																
フィンガープリント SHA ハッシュ(続き)																																
フィンガープリント SHA ハッシュ(続き)																																
フィンガープリント SHA ハッシュ(続き)																																
フィンガープリント SHA ハッシュ(続き)																																
公開キーの SHA ハッシュ																																
公開キーの SHA ハッシュ(続き)																																
公開キーの SHA ハッシュ(続き)																																
公開キーの SHA ハッシュ(続き)																																
公開キーの SHA ハッシュ(続き)																																
シリアル番号																																
シリアル番号(続き)																																
シリアル番号(続き)																																
シリアル番号(続き)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	シリアル番号(続き)																															
	シリアル番号の長さ																															
サブジェクトの共通名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	サブジェクトの共通名...																															
サブジェクト組織	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	サブジェクト組織...																															
サブジェクトの組織単位	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	サブジェクトの組織単位....																															
サブジェクトの国	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	サブジェクトの国...																															
発行元の共通名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	発行元の共通名...																															
発行者組織	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	発行者組織...																															
発行者の組織単位	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	発行者の組織単位...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
発行者の国	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	発行者の国...																															
	有効な開始日																															
	有効な終了日																															

次の表は、SSL 証明書の詳細のデータ ブロックのフィールドについての説明です。

表 3-68　SSL 証明書の詳細のデータ ブロック フィールド

フィールド	データ タイプ	説明
SSL 証明書の詳細のデータ ブロック タイプの詳細	uint32	SSL 証明書の詳細のデータ ブロックを開始します。この値は常に 50 です。
SSL 証明書の詳細のデータ ブロック長	uint32	SSL 証明書の詳細のデータ ブロックの合計バイト数です。SSL 証明書の詳細のデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
フィンガープリント SHA ハッシュ	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
公開キーの SHA ハッシュ	uint8[20]	証明書に含まれる公開キーの認証に使用する SHA ハッシュ値。
シリアル番号	uint8[20]	発行元 CA によって割り当てられたシリアル番号。この番号は 20 バイトを超えない長さにする必要があります。シリアル番号の長さフィールドの指定どおりに 20 バイト未満にすることができます。
シリアル番号の長さ	uint32	シリアル番号の長さ(バイト単位)。
文字列ブロック タイプ	uint32	侵害に関連付けられたカテゴリを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとカテゴリ フィールドのバイト数が含まれます。
サブジェクトの共通名	string	SSL 証明書のサブジェクトの共通名。これは通常、証明書のサブジェクトのホストとドメイン名ですが、他の情報が含まれていることもあります。
文字列ブロック タイプ	uint32	侵害に関連付けられたイベント タイプを含む文字列データ ブロックを開始します。この値は常に 0 です。

表 3-68　SSL 証明書の詳細のデータ ブロック フィールド(続き)

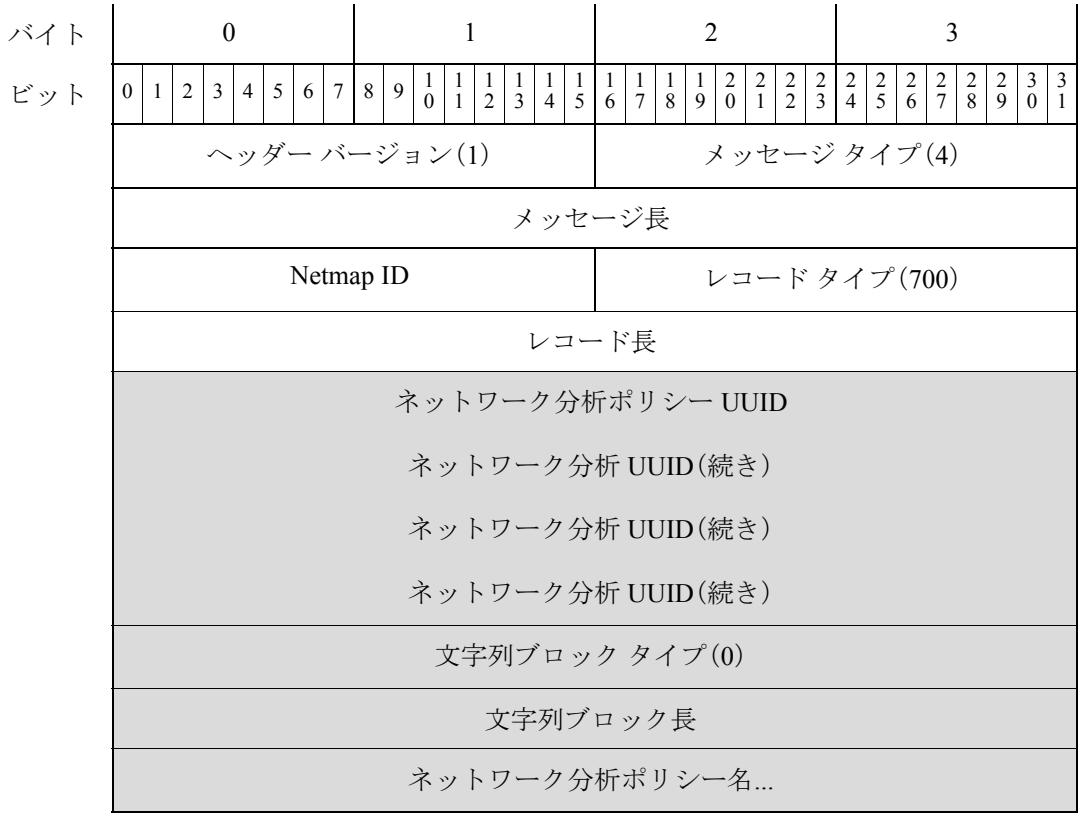
フィールド	データ タイプ	説明
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとイベント タイプ フィールドのバイト数が含まれます。
サブジェクト組織	string	証明書のサブジェクトの組織。
文字列ブロック タイプ	uint32	侵害に関連付けられたイベント タイプを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとイベント タイプ フィールドのバイト数が含まれます。
サブジェクトの組織単位	string	証明書のサブジェクトの組織単位。
文字列ブロック タイプ	uint32	侵害に関連付けられたイベント タイプを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとイベント タイプ フィールドのバイト数が含まれます。
サブジェクトの国	string	証明書のサブジェクトの国。
文字列ブロック タイプ	uint32	侵害に関連付けられたカテゴリを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとカテゴリ フィールドのバイト数が含まれます。
発行元の共通名	string	SSL 証明書の発行者の共通名。これは通常、証明書の発行者のホストとドメイン名ですが、他の情報が含まれていることもあります。
文字列ブロック タイプ	uint32	侵害に関連付けられたイベント タイプを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとイベント タイプ フィールドのバイト数が含まれます。
発行者組織	string	証明書の発行者の組織。
文字列ブロック タイプ	uint32	侵害に関連付けられたイベント タイプを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとイベント タイプ フィールドのバイト数が含まれます。
発行者の組織単位	string	証明書の発行者の組織単位。
文字列ブロック タイプ	uint32	侵害に関連付けられたイベント タイプを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとイベント タイプ フィールドのバイト数が含まれます。

表 3-68　SSL 証明書の詳細のデータ ブロック フィールド(続き)

フィールド	データ タイプ	説明
発行者の国	string	証明書の発行者の国。
有効な開始日	uint32	証明書が発行された時刻の Unix タイムスタンプ。
有効な終了日	uint32	証明書が有効でなくなる時刻の Unix タイムスタンプ。

ネットワーク分析ポリシー レコード

eStreamer サービスは、ネットワーク分析ポリシー名の情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグのいずれか(要求メッセージの [要求フラグ(Request Flags)] フィールドのビット 1、14、15、または 20)が設定されていると、ネットワーク分析ポリシー名の情報が送信されます。要求フラグ (2-12 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにネットワーク分析ポリシー名レコードを示す値 700 があることに注意してください。



次の表は、ネットワーク分析ポリシー名のレコードのフィールドについての説明です。

表 3-69　ネットワーク分析ポリシー名 レコード フィールド

フィールド	データ タイプ	説明
ネットワーク分析ポリシー UUID	uint8[16]	ネットワーク分析ポリシーの UUID
文字列ブロック タイプ	uint32	ネットワーク分析ポリシーの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ネットワーク分析ポリシー名の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとネットワーク分析ポリシー名のバイト数が含まれます。
ネットワーク分析ポリシー名	string	ネットワーク分析ポリシーの名前。

検出と接続データ構造の概要

この章では、ディスカバリ イベントと接続イベントの eStreamer メッセージに使用するデータ構造と、これらイベントのメタデータについて詳しく述べます。ディスカバリ イベント メッセージと接続イベント メッセージの違いはデータ ブロック自体の内容であり、使用する一般的なメッセージ形式とデータ ブロック シリーズは同じです。

ディスカバリ イベントには、次の 2 つのイベント サブカテゴリがあります。

- ホスト ディスカバリ イベント。これは、パケットのコンテンツから検出した、ホストで実行しているアプリケーションなど、管理対象ネットワーク上の新規ホストと変更ホストと、ホスト脆弱性を識別します。
- ログインなど、新規ユーザとユーザ アクティビティの検出を報告するユーザ イベント。

接続イベントは、監視対象のホストと他のすべてのホスト間のセッション トラフィックに関する情報を報告します。接続情報には、トランザクションの最初と最後のパケット、送信元と宛先の IP アドレス、送信元と宛先のポート、送受信したパケットとバイトの数があります。可能であれば、接続イベントでは、そのセッションに関係するクライアント アプリケーションと URL を報告します。

eStreamer サーバからのディスカバリ イベントまたは接続イベントの要求については、要求フラグ（2-12 ページ） を参照してください。

eStreamer イベント データ構造メッセージの一般的構造については、イベント データ メッセージの構成について（2-18 ページ） を参照してください。

ディスカバリ イベントと接続イベント データ構造の詳細については、この章の以下のセクションを参照してください。

- ディスカバリ イベントと接続イベントのデータ メッセージ（4-2 ページ） では、eStreamer がホスト ディスカバリ メッセージ、ユーザ メッセージ、接続メッセージに使用する構造の概要を紹介します。
- ディスカバリ イベントと接続イベントのレコード タイプ（4-2 ページ） では、ディスカバリ イベントと接続イベント レコード タイプについて説明します。
- ディスカバリ イベントのメタデータ（4-8 ページ） では、たとえば、イベント内のユーザ ID をユーザ名に変換するなど、数字データとコード化データをテキストに変換するためのコンテキスト情報を要求できるメタデータ レコードについて説明します。
- ディスカバリ イベント ヘッダー 5.2+（4-40 ページ） では、すべてのディスカバリ メッセージと接続メッセージで使用する標準イベント ヘッダーの構造と、イベント タイプ フィールドとイベント サブタイプ フィールドで発生する値について説明します。さらに、イベント タイプ フィールドとサブタイプ フィールドは、メッセージで伝えるデータ レコードの構造を定義します。

- イベント タイプ別ホスト ディスカバリ構造(4-44 ページ) では、eStreamer が各種ホスト ディスカバリ イベント タイプに使用するデータ レコードの構造について説明します。
- ホスト IOC セット メッセージ(4-61 ページ) では、eStreamer が各種ユーザ イベント タイプに使用するデータ レコードの構造について説明します。
- ディスカバリ(シリーズ1)ブロック(4-63 ページ) では、ディスカバリ イベント メッセージと接続イベント メッセージで複雑なレコードを伝えるために使用する一連のデータ ブロック構造について説明します。シリーズ 1 のデータ ブロックは、相関イベントでも使用します。
- ユーザ脆弱性データ ブロック 5.0+(4-163 ページ) では、複雑なユーザ イベント レコードを伝えるために使用するその他の シリーズ 1 ブロック構造について説明します。

ヒント　サンプル ディスカバリ イベントを扱った例については、「データ構造の例」セクション(A-1 ページ) を参照してください。

ディスカバリ イベントと接続イベントのデータ メッセージ

eStreamer は、ディスカバリ イベントと接続イベント データを同じメッセージ構造でパッケージングします。このパッケージには、以下の要素を格納します。

- オプションの netmap ID
- レコード タイプを定義するレコード ヘッダー
- イベントを識別し、その特性を表すディスカバリ イベント ヘッダー。具体的にはイベント タイプとサブタイプを識別します。詳細については、ディスカバリ イベント ヘッダー 5.2+(4-40 ページ)を参照してください。
- ブロック ヘッダーとデータ ブロックからなるデータ レコード。ディスカバリ イベントと接続イベントのデータ メッセージは、シリーズ 1 のデータ ブロックを使用します。詳細については、ホスト ディスカバリ データ ブロックと接続データ ブロック(4-64 ページ)またはユーザ脆弱性データ ブロック 5.0+(4-163 ページ)を参照してください。

ディスカバリ イベントと接続イベントのレコード タイプ

次の表は、ホスト ディスカバリ イベントと接続イベントのイベント レコード タイプと、レコード タイプ別のイベント メッセージ構造までのリンクです。このリストにはメタデータ レコード タイプもあります。レコードによっては、データの特定部分を保存するデータ ブロック 1 つだけのものがあります。これらのデータ ブロックは、ほとんどのデータ タイプを含むシリーズ 1 ブロックと、ディスカバリ データだけを含むシリーズ 2 ブロックに分かれます。次の表は、各バージョンのステータスです(現在またはレガシー)。現在のレコードは最新バージョンです。レガシー レコードは、以降のバージョンによって取って代わられていますが、eStreamer から要求することができます。

表 4-1　ディスカバリ イベントと接続イベントのレコード タイプ

レコード タイプ	含まれるブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
10	139	1	新規ホストを検出	現在（Current）	新規ホスト メッセージと最後の確認日時ホスト メッセージ(4-45 ページ)
11	103	1	新規 TCP サーバ	現在（Current）	サーバ メッセージ(4-46 ページ)
12	103	1	新規 UDP サーバ	現在（Current）	サーバ メッセージ(4-46 ページ)
13	4	1	新規ネットワーク プロトコル	現在（Current）	新規ネットワーク プロトコル メッセージ(4-47 ページ)
14	4	1	新規トランスポート プロトコル	現在（Current）	新規トランスポート プロトコル メッセージ(4-47 ページ)
15	122	1	新規クライアント アプリケーション	現在（Current）	クライアント アプリケーション メッセージ(4-48 ページ)
16	103	1	TCP サーバ情報更新	現在（Current）	サーバ メッセージ(4-46 ページ)
17	103	1	UDP サーバ情報更新	現在（Current）	サーバ メッセージ(4-46 ページ)
18	53	1	OS 情報の更新	現在（Current）	オペレーティング システム更新メッセージ(4-49 ページ)
19	該当なし	該当なし	ホスト タイムアウト	現在（Current）	IP アドレスを再利用とホスト タイムアウト/削除メッセージ(4-50 ページ)
20	該当なし	該当なし	ホスト IP アドレスを再利用	現在（Current）	IP アドレスを再利用とホスト タイムアウト/削除メッセージ(4-50 ページ)
21	該当なし	該当なし	ホストを削除。ホスト上限に到達	現在（Current）	IP アドレスを再利用とホスト タイムアウト/削除メッセージ(4-50 ページ)
22	該当なし	該当なし	ホップ数の変更	現在（Current）	ホップ変更メッセージ(4-50 ページ)
23	該当なし	該当なし	TCP ポート クローズ	現在（Current）	TCP と UDP のポート クローズ メッセージ/タイムアウト メッセージ(4-51 ページ)
24	該当なし	該当なし	UDP ポート クローズ	現在（Current）	TCP と UDP のポート クローズ メッセージ/タイムアウト メッセージ(4-51 ページ)
25	該当なし	該当なし	TCP ポート タイムアウト	現在（Current）	TCP と UDP のポート クローズ メッセージ/タイムアウト メッセージ(4-51 ページ)
26	該当なし	該当なし	UDP ポート タイムアウト	現在（Current）	TCP と UDP のポート クローズ メッセージ/タイムアウト メッセージ(4-51 ページ)
27	該当なし	該当なし	MAC 情報の変更	現在（Current）	MAC アドレス メッセージ(4-51 ページ)
28	該当なし	該当なし	ホストの追加 MAC を検出	現在（Current）	MAC アドレス メッセージ(4-51 ページ)
29	該当なし	該当なし	ホスト IP アドレスを変更	現在（Current）	IP アドレス変更メッセージ(4-48 ページ)

表 4-1　ディスカバリ イベントと接続イベントのレコード タイプ(続き)

レコード タイプ	含まれる ブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
31	該当なし	該当なし	ルータ/ブリッジとして識別したホスト	現在 (Current)	ブリッジ/ルータとして識別したホスト メッセージ(4-52 ページ)
34	14	1	VLAN タグ情報更新	現在 (Current)	VLAN タグ情報更新メッセージ(4-52 ページ)
35	122	1	クライアント アプリケーション タイムアウト	現在 (Current)	クライアント アプリケーション メッセージ(4-48 ページ)
42	35	1	NetBIOS 名変更	現在 (Current)	NetBIOS 名変更メッセージ(4-53 ページ)
44	該当なし	該当なし	ホストをドロップ。ホスト上限に到達	現在 (Current)	IP アドレスを再利用とホスト タイムアウト/削除メッセージ(4-50 ページ)
45	37	1	更新バナー	現在 (Current)	更新バナー メッセージ(4-53 ページ)
46	55	1	ホスト属性を追加	現在 (Current)	属性メッセージ(4-57 ページ)
47	55	1	ホスト属性を更新	現在 (Current)	属性メッセージ(4-57 ページ)
48	55	1	ホスト属性を削除	現在 (Current)	属性メッセージ(4-57 ページ)
51	103	1	TCP サーバ信頼度更新	レガシー	サーバ メッセージ(4-46 ページ)
52	103	1	UDP サーバ信頼度更新	レガシー	サーバ メッセージ(4-46 ページ)
53	53	1	OS 信頼度更新	レガシー	オペレーティング システム更新メッセージ(4-49 ページ)
54	該当なし	該当なし	フィンガープリント メタデータ	現在 (Current)	フィンガープリント レコード(4-8 ページ)
55	該当なし	該当なし	クライアント アプリケーション メタデータ	現在 (Current)	クライアント アプリケーション レコード(4-10 ページ)
57	該当なし	該当なし	脆弱性メタデータ	現在 (Current)	脆弱性レコード(4-10 ページ)
58	該当なし	該当なし	重要度メタデータ	現在 (Current)	重要度レコード(4-13 ページ)
59	該当なし	該当なし	ネットワーク プロトコル メタデータ	現在 (Current)	ネットワーク プロトコル レコード(4-13 ページ)
60	該当なし	該当なし	属性メタデータ	現在 (Current)	属性レコード(4-14 ページ)
61	該当なし	該当なし	スキャン タイプ メタデータ	現在 (Current)	スキャン タイプ レコード(4-15 ページ)
63	該当なし	該当なし	サーバ メタデータ	現在 (Current)	サーバ レコード(4-16 ページ)
71	144	1	接続統計情報	レガシー	接続統計データ ブロック 5.2.x(B-139 ページ)

表 4-1　ディスカバリ イベントと接続イベントのレコード タイプ(続き)

レコード タイプ	含まれる ブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
71	152	1	接続統計情報	レガシー	接続統計データ ブロック 5.3(B-155 ページ)
71	154	1	接続統計情報	レガシー	接続統計データ ブロック 5.3.1(B-162 ページ)
71	155	1	接続統計情報	レガシー	接続統計データ ブロック 5.4(B-169 ページ)
71	157	1	接続統計情報	レガシー	接続統計データ ブロック 5.4.1(B-184 ページ)
71	160	1	接続統計情報	レガシー	接続統計データ ブロック 6.0.x(B-198 ページ)
71	163	1	接続統計情報	現在 (Current)	接続統計データ ブロック 6.1+(4-122 ページ)
73	136	1	接続チャンク	現在 (Current)	接続チャンク メッセージ(4-55 ページ)
74	該当なし	該当なし	ユーザ設定 OS	現在 (Current)	ユーザ サーバ メッセージとオペレーティング システム メッセージ(4-58 ページ)
75	該当なし	該当なし	ユーザ設定サーバ	現在 (Current)	ユーザ サーバ メッセージとオペレーティング システム メッセージ(4-58 ページ)
76	83	1	ユーザ削除プロトコル	現在 (Current)	ユーザ プロトコル メッセージ(4-59 ページ)
77	60	1	ユーザ削除クライアント アプリケーション	現在 (Current)	ユーザ クライアント アプリケーション メッセージ(4-59 ページ)
78	78	1	ユーザ削除アドレス	現在 (Current)	ユーザ追加/削除ホスト メッセージ(4-56 ページ)
79	77	1	ユーザ削除サーバ	現在 (Current)	ユーザ削除サーバ メッセージ(4-56 ページ)
80	80	1	ユーザ設定の有効な脆弱性	現在 (Current)	バージョン4.6.1+ のユーザ設定脆弱性メッセージ(4-55 ページ)
81	80	1	ユーザ設定の無効な脆弱性	現在 (Current)	バージョン4.6.1+ のユーザ設定脆弱性メッセージ(4-55 ページ)
82	81	1	ユーザ設定ホスト重要度	現在 (Current)	ユーザ設定ホスト重要度メッセージ (4-57 ページ)
83	55	1	ユーザ設定属性値	現在 (Current)	属性値メッセージ(4-58 ページ)
84	82	1	ユーザ削除属性値	現在 (Current)	属性値メッセージ(4-58 ページ)
85	78	1	ユーザ追加ホスト	現在 (Current)	ユーザ追加/削除ホスト メッセージ(4-56 ページ)
86	該当なし	該当なし	ユーザ追加サーバ	現在 (Current)	ユーザ サーバ メッセージとオペレーティング システム メッセージ(4-58 ページ)

表 4-1　ディスカバリ イベントと接続イベントのレコード タイプ(続き)

レコード タイプ	含まれる ブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
87	60	1	ユーザ追加クライアント アプリケーション	現在 (Current)	ユーザ クライアント アプリケーション メッセージ(4-59 ページ)
88	83	1	ユーザ追加プロトコル	現在 (Current)	ユーザ プロトコル メッセージ (4-59 ページ)
89	142	1	ユーザ追加スキャン結果	現在 (Current)	スキャン結果を追加メッセージ (4-60 ページ)
90	該当なし	該当なし	ソース タイプ レコード	現在 (Current)	ソース タイプ レコード(4-17 ページ)
91	該当なし	該当なし	ソース アプリケーション レコード	現在 (Current)	ソース アプリケーション レコード (4-18 ページ)
92	120	1	ユーザ ドロップ変更イベント	現在 (Current)	ユーザ変更メッセージ(4-62 ページ)
93	120	1	ユーザ削除変更イベント	現在 (Current)	ユーザ変更メッセージ(4-62 ページ)
94	120	1	新規ユーザ識別イベント	現在 (Current)	ユーザ変更メッセージ(4-62 ページ)
95	121	1	ユーザ ログイン変更イベント	現在 (Current)	ユーザ情報更新メッセージ ブロック (4-62 ページ)
96	該当なし	該当なし	ソース ディテクタ レコード	現在 (Current)	ソースディテクタ レコード(4-18 ページ)
98	該当なし	該当なし	ユーザ レコード	現在 (Current)	ユーザ レコード(4-21 ページ)
101	該当なし	該当なし	新規 OS イベント	現在 (Current)	新規オペレーティング システム メッセージ(4-60 ページ)
102	94	1	アイデンティティ競合イベント	現在 (Current)	アイデンティティ競合とアイデンティティ タイムアウト システム メッセージ (4-61 ページ)
103	94	1	アイデンティティ タイムアウト イベント	現在 (Current)	アイデンティティ競合とアイデンティティ タイムアウト システム メッセージ (4-61 ページ)
106	該当なし	該当なし	サードパーティ スキャナ脆弱性レコード	現在 (Current)	サードパーティ スキャナの脆弱性レコード(4-19 ページ)
107	122	1	クライアント アプリケーション更新	現在 (Current)	クライアント アプリケーション メッセージ(4-48 ページ)
109	該当なし	該当なし	Web アプリケーション レコード	現在 (Current)	Web アプリケーション レコード (4-22 ページ)
115	該当なし	該当なし	セキュリティ ゾーン名レコード	現在 (Current)	セキュリティ ゾーン名レコード (3-32 ページ)
116	14	2	インターフェイス名レコード	現在 (Current)	インターフェイス名レコード(3-34 ページ)

表 4-1　ディスカバリ イベントと接続イベントのレコード タイプ(続き)

レコード タイプ	含まれる ブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
117	14	2	アクセス コントロール ポリシー名メタデータ	現在 (Current)	アクセス コントロール ポリシー名のレコード(3-35 ページ)
118	14	2	侵入ポリシー名レコード	現在 (Current)	侵入ポリシー名レコード(4-23 ページ)
119	14	2	アクセス コントロール ルール ID レコード	現在 (Current)	アクセス コントロール ルール ID レコードのメタデータ(3-36 ページ)
120	該当なし	該当なし	アクセス コントロール ルール アクション レコード	現在 (Current)	アクセス コントロール ルール アクション レコード メタデータ(4-24 ページ)
121	該当なし	該当なし	URL カテゴリ統計	現在 (Current)	URL カテゴリ レコード メタデータ (4-25 ページ)
122	該当なし	該当なし	URL レピュテーション メタデータ	現在 (Current)	URL レピュテーション レコード メタデータ(4-26 ページ)
124	21	2	アクセス コントロール ルール理由メタデータ	現在 (Current)	アクセス コントロール ルール理由メタデータ(4-27 ページ)
145	64	2	アクセス コントロール ポリシー メタデータ	現在 (Current)	アクセス コントロール ポリシー メタデータ(4-28 ページ)
146	64	2	プレフィルタ ポリシー メタデータ	現在 (Current)	プレフィルタ ポリシー メタデータ(4-30 ページ)
147	21	2	トンネルまたはプレフィルタ ルール メタデータ	現在 (Current)	トンネルまたはプレフィルタのルールのメタデータ(4-31 ページ)
161	39	2	5.3+ の IOC 名データ ブロック	現在 (Current)	5.3+ の IOC 名データ ブロック (4-37 ページ)
160	7	1	ホスト IOC セット メッセージ	現在 (Current)	ホスト IOC セット メッセージ (4-61 ページ)
280	22	2	セキュリティ インテリジェンス カテゴリ メタデータ	現在 (Current)	セキュリティ インテリジェンス カテゴリ メタデータ(4-33 ページ)
281	該当なし	該当なし	セキュリティ インテリジェンス送信元/宛先レコード	現在 (Current)	セキュリティ インテリジェンス送信元/宛先レコード(4-34 ページ)

ディスカバリ イベントのメタデータ

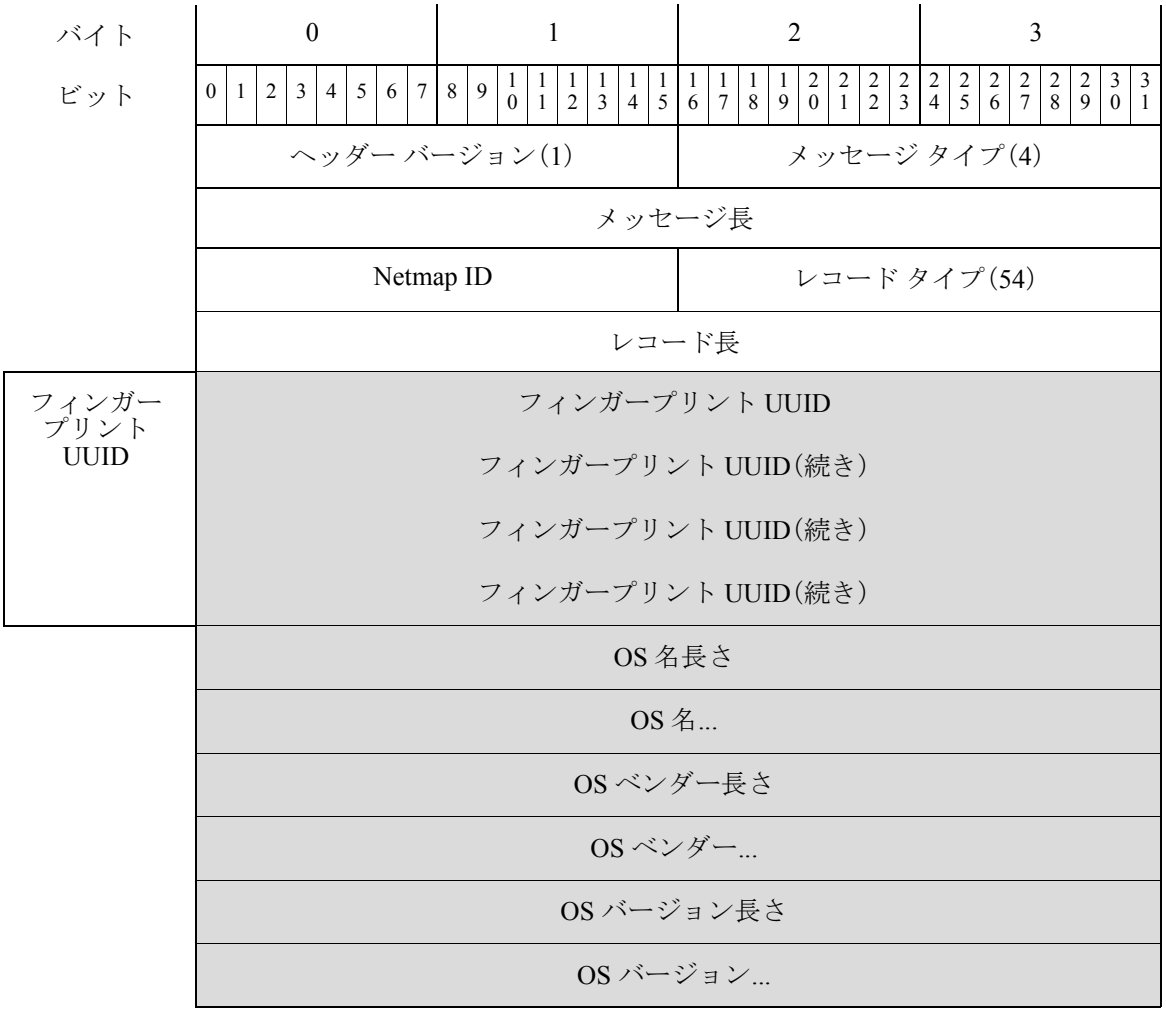
メタデータ バージョン番号でメタデータを要求します。Firepower システム のバージョンに対応するメタデータ バージョンについては、メタデータについて（2-42 ページ）を参照してください。eStreamer によるメタデータ レコードのストリーミング方法の重要な情報については、メタデータの伝送（2-42 ページ）を参照してください。

ホスト ディスカバリ レコードとユーザ イベント レコードの各種メタデータ レコード タイプの構造については、以下のページを参照してください:

侵入イベントと相関イベントのメタデータ レコードについては、侵入イベントとメタデータのレコード タイプ（3-1 ページ）を参照してください。

フィンガープリント レコード

eStreamer サービスは、次の形式のフィンガープリント レコードで、イベントのフィンガープリント メタデータを送信します。（フィンガープリント メタデータは、以下のメタデータ フラグの 1 つ（要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20）が設定されると送信されます。要求フラグ（2-12 ページ）を参照してください）。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、フィンガープリント レコードを示す 54 です。



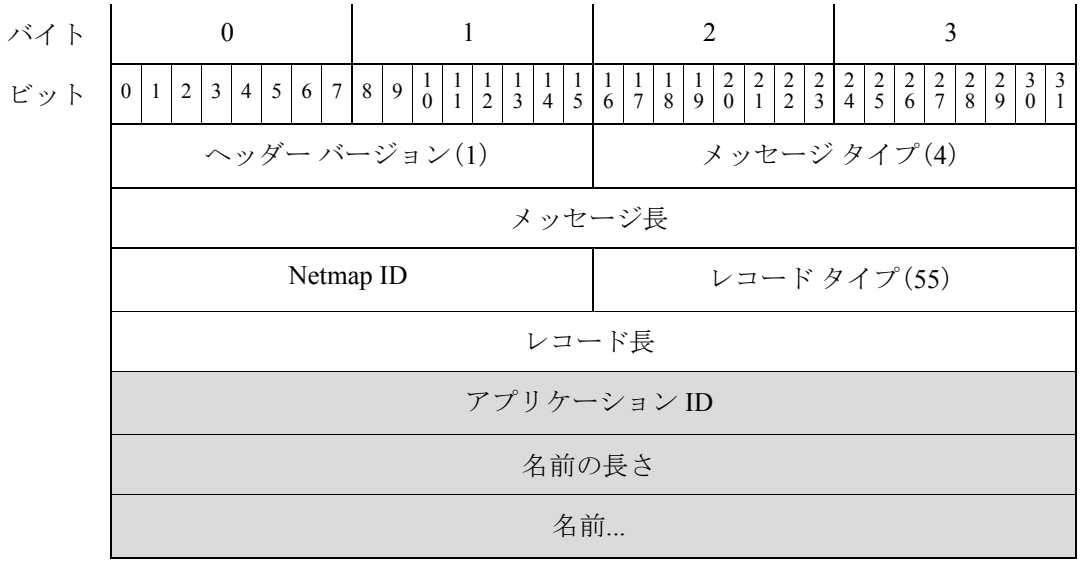
次の表では、フィンガープリント レコードのフィールドについて説明します。

表 4-2　フィンガープリント レコードのフィールド

フィールド	データ タイプ	説明
フィンガープリント UUID	uint8[16]	オペレーティング システムの一意の ID として機能するフィンガープリント ID 番号。
OS 名長さ	uint32	オペレーティング システム名のバイト数。
OS 名	string	フィンガープリントのオペレーティング システム名。
OS ベンダー長さ	uint32	オペレーティング システム ベンダー名のバイト数。
OS ベンダー	string	フィンガープリントのオペレーティング システム ベンダー名。
OS バージョン長さ	uint32	オペレーティング システム バージョンのバイト数。
OS のバージョン	string	フィンガープリントのオペレーティング システム バージョン。

クライアント アプリケーション レコード

eStreamer サービスは、次の形式のクライアント アプリケーション レコードで、イベントのクライアント アプリケーション メタデータを送信します。(クライアント アプリケーション メタデータは、以下のメタデータ フラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。要求フラグ(2-12 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、クライアント アプリケーション レコードを示す 55 です。



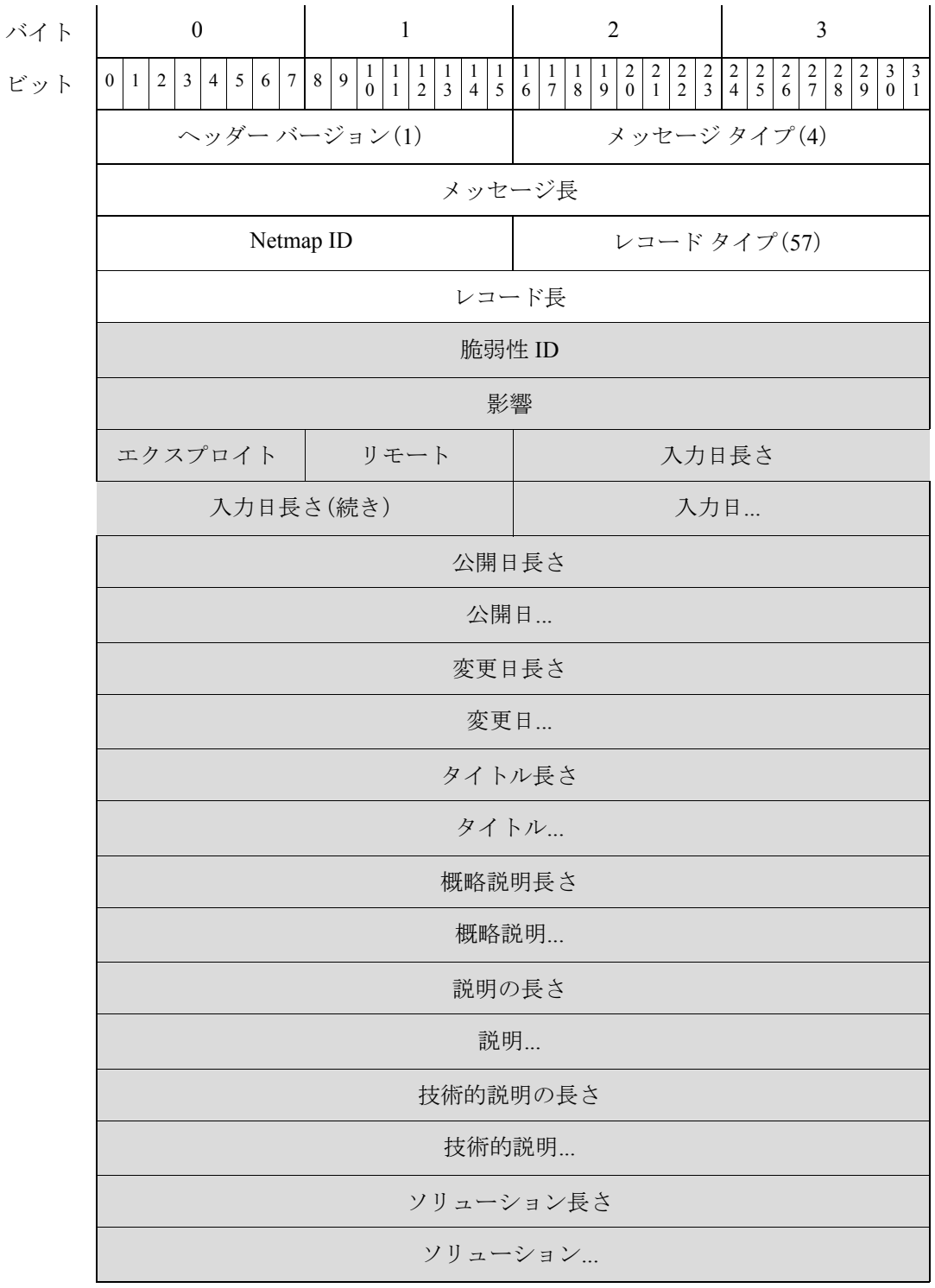
次の表では、クライアント アプリケーション レコードのフィールドについて説明します。

表 4-3　クライアント アプリケーション レコードのフィールド

フィールド	データ タイプ	説明
アプリケーション ID	uint32	クライアント アプリケーションのアプリケーション ID 番号。
名前の長さ	uint32	名前に含まれるバイト数。
名前	string	クライアント アプリケーション名。

脆弱性レコード

eStreamer サービスは、次の形式の脆弱性レコードで、イベントの脆弱性情報を格納したメタデータを送信します。(脆弱性情報は、以下のメタデータ フラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。要求フラグ(2-12 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、脆弱性レコードを示す 57 です。


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
ヘッダー バージョン(1)
メッセージ タイプ(4)
メッセージ長
Netmap ID
レコード タイプ(57)
レコード長
脆弱性 ID
影響
エクスプロイト
リモート
入力日長さ
入力日長さ(続き)
入力日...
公開日長さ
公開日...
変更日長さ
変更日...
タイトル長さ
タイトル...
概略説明長さ
概略説明...
説明の長さ
説明...
技術的説明の長さ
技術的説明...
ソリューション長さ
ソリューション...

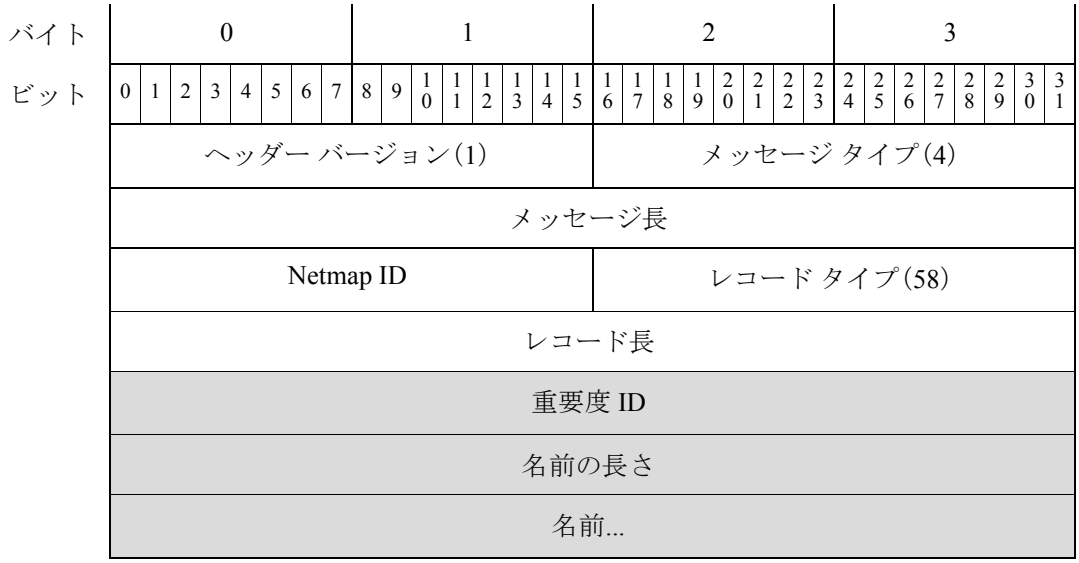
次の表では、脆弱性レコードのフィールドについて説明します。

表 4-4　脆弱性レコードのフィールド

フィールド	データ タイプ	説明
脆弱性 ID	uint32	脆弱性 ID 番号
影響	uint32	侵入データ、ホスト ディスカバリ イベント、脆弱性アセスメント間の相関に基づいて決定した影響レベルに対応した、脆弱性の影響。ここに設定可能な値の範囲は 1 ～ 10 です。最も深刻な場合で 10 です。脆弱性の影響度の値は、Bugtraq エントリの作成者が設定します。
エクスプロイト	uint8	脆弱性に既知のエクスプロイトがあるかどうかを示します。有効な値は次のとおりです。 • 0:はい • 1:いいえ
リモート	uint8	ネットワーク上でつけ込まれる余地が脆弱性にあるかどうかを示します。有効な値は次のとおりです。 • 0:はい • 1:いいえ • 空白: 不明なリモート エクスプロイトに対する脆弱性
入力日長さ	uint32	入力日付フィールド長さ。
入力日	string	脆弱性がデータベースに登録された日付。
公開日長さ	uint32	公開された日付フィールド長さ。
公開日	string	脆弱性が公開された日付。
変更日長さ	uint32	変更された日付フィールド長さ。
変更日	string	脆弱性の最終変更日(該当する場合)。
タイトル長さ	uint32	タイトル フィールド長さ。
タイトル	string	脆弱性のタイトル。
概略説明長さ	uint32	概略説明フィールド長さ。
概略説明(Short Description)	string	脆弱性の概略説明。
説明の長さ	uint32	説明フィールドの長さ。
説明	string	脆弱性に関する一般的な説明。
技術的説明の長さ	uint32	技術的説明フィールド長さ。
技術的説明	string	脆弱性に関する技術的説明。
ソリューション長さ	uint32	ソリューション フィールド長さ。
ソリューション	string	脆弱性に対するソリューション。

重要度レコード

eStreamer サービスは、次の形式の重要度レコードで、イベントのホスト重要度情報を格納したメタデータを送信します。（重要度情報は、以下のメタデータ フラグの 1 つ（要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20）が設定されると送信されます。要求フラグ（2-12 ページ） を参照してください）。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、重要度レコードを示す 58 です。



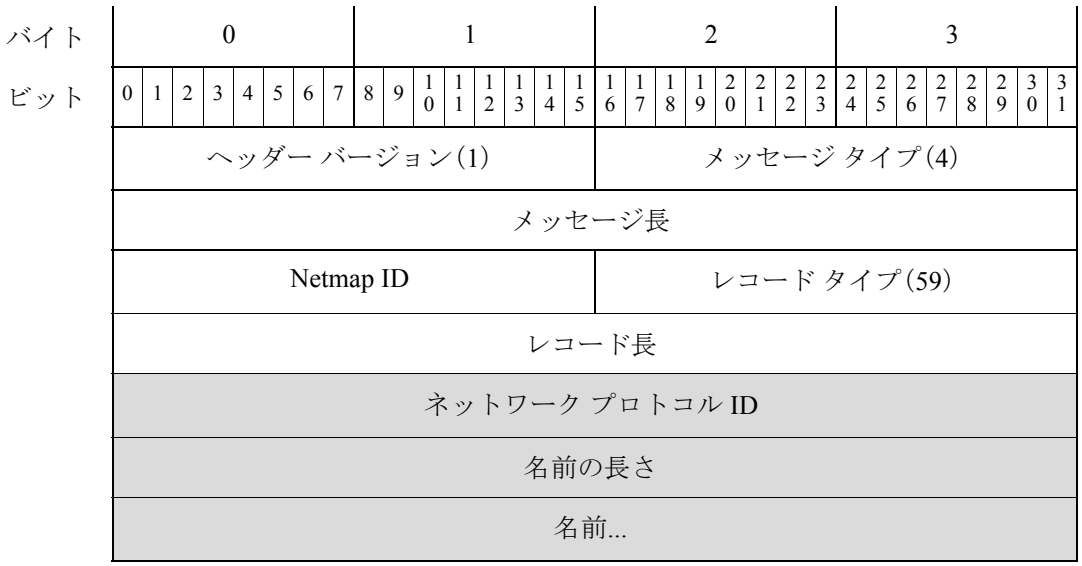
次の表では、重要度レコードのフィールドについて説明します。

表 4-5　重要度レコードのフィールド

フィールド	データ タイプ	説明
重要度 ID	uint32	重要度 ID 番号。
名前の長さ	uint32	重要度レベルのバイト数。
名前	string	重要度レベル。

ネットワーク プロトコル レコード

eStreamer サービスは、次の形式のネットワーク プロトコル レコードで、イベントのネットワーク プロトコル情報を格納したメタデータを送信します。（ネットワーク プロトコル情報は、以下のメタデータ フラグの 1 つ（要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20）が設定されると送信されます。要求フラグ（2-12 ページ） を参照してください）。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、ネットワーク プロトコル レコードを示す値 59 です。



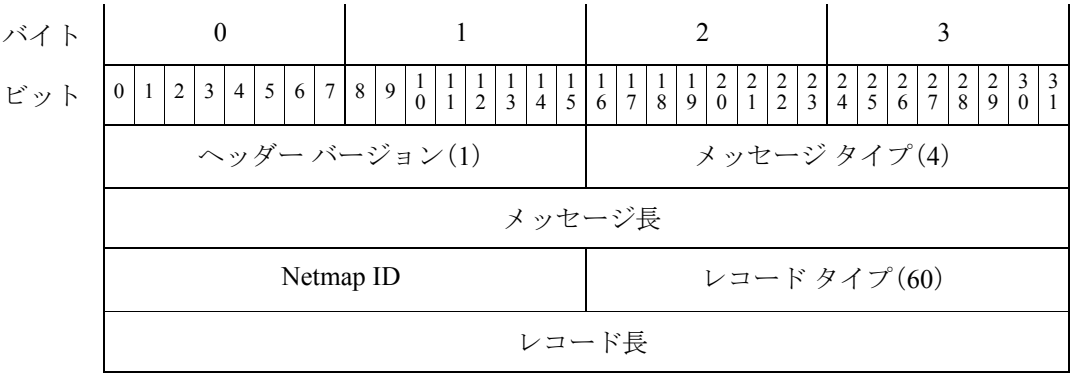
次の表では、ネットワーク プロトコル レコードのフィールドについて解説します。

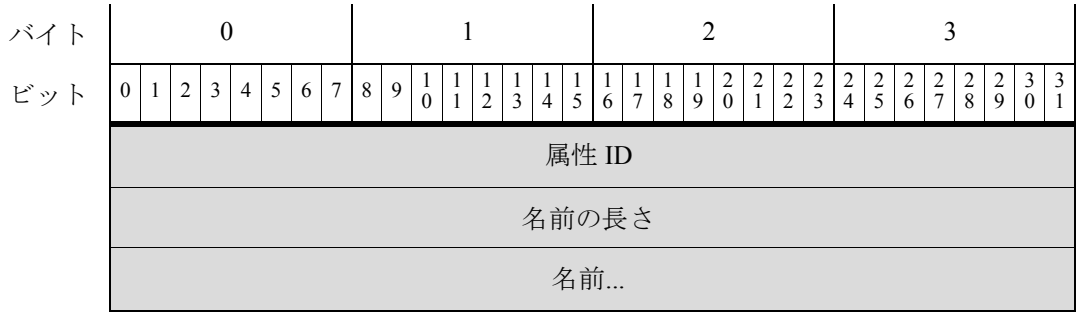
表 4-6　ネットワーク プロトコル レコードのフィールド

フィールド	データ タイプ	説明
ネットワーク プロトコル ID	uint32	ネットワーク プロトコル ID 番号。
名前の長さ	uint32	ネットワーク プロトコル名のバイト数。
名前	string	ネットワーク プロトコル名。

属性レコード

eStreamer サービスは、次の形式の属性レコードで、イベントの属性情報を格納したメタデータを送信します。(属性情報は、以下のメタデータ フラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。要求フラグ(2-12 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、属性レコードを示す 60 です。





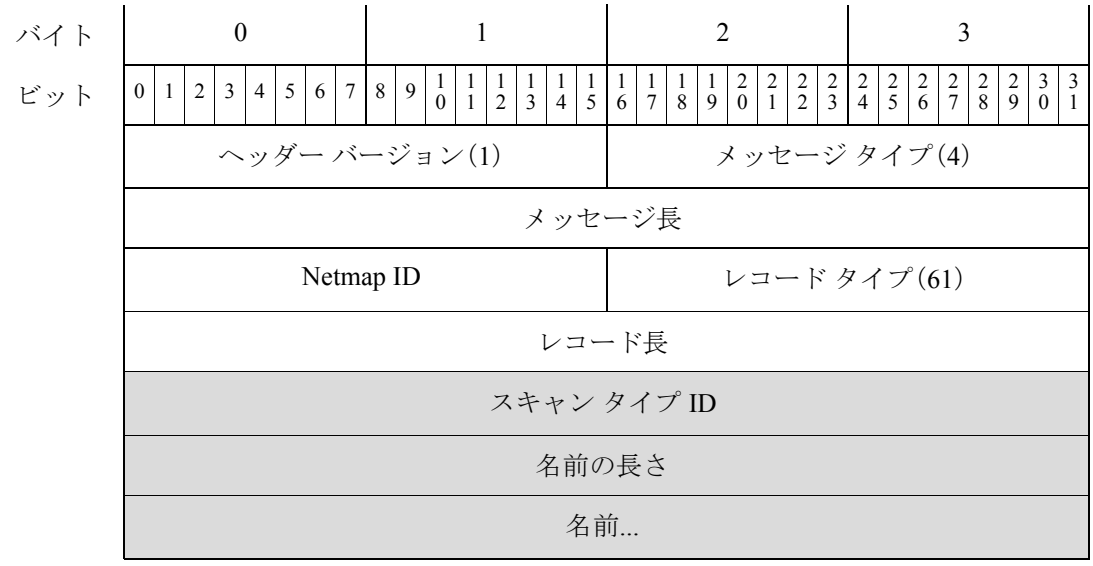
次の表では、属性レコードのフィールドについて説明します。

表 4-7　属性レコードのフィールド

フィールド	データ タイプ	説明
属性 ID	uint32	属性 ID 番号。
名前の長さ	uint32	属性名のバイト数。
名前	string	属性の名前。

スキャン タイプ レコード

eStreamer サービスは、次の形式のスキャン タイプ レコードで、イベントのスキャン タイプ情報を格納したメタデータを送信します。(スキャン タイプ情報は、以下のメタデータ フラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。要求フラグ(2-12 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、スキャン タイプ レコードを示す 61 です。



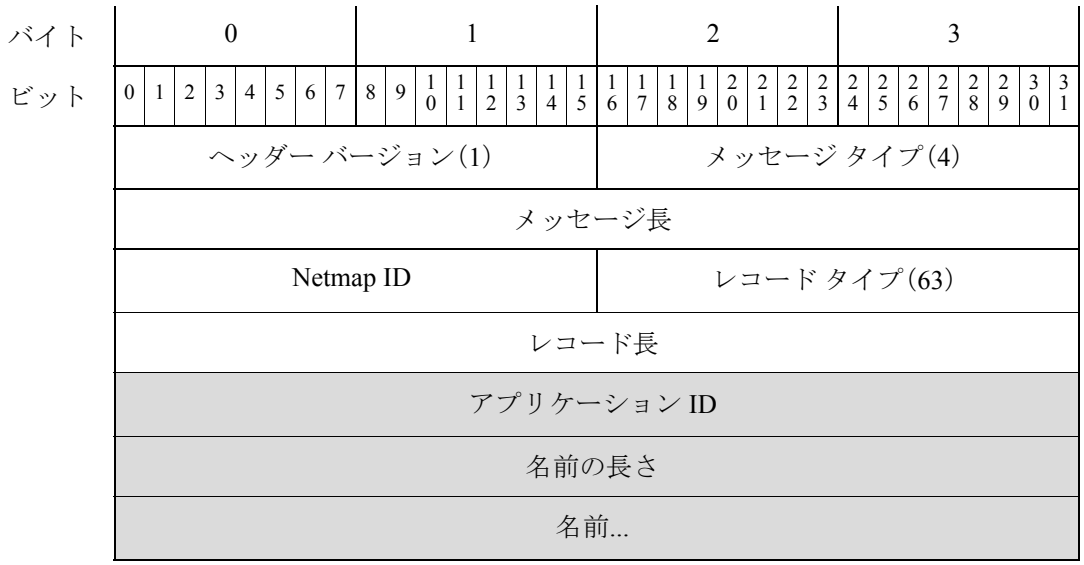
次の表では、スキャン タイプ レコードのフィールドについて説明します。

表 4-8　スキャン タイプ レコードのフィールド

フィールド	データ タイプ	説明
スキャン タイプ ID	uint32	スキャン タイプ ID 番号。
名前の長さ	uint32	スキャン タイプ名のバイト数。
名前	string	スキャン タイプ名。

サーバ レコード

eStreamer サービスは、次の形式のサーバ レコードで、イベントのサーバ情報を格納したメタデータを送信します。サーバのアプリケーション プロトコルのアプリケーション ID は、メタデータまでのクロスリファレンスを提供します。(サーバ情報は、以下のメタデータ フラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。要求フラグ(2-12 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、サーバ レコードを示す 63 です。



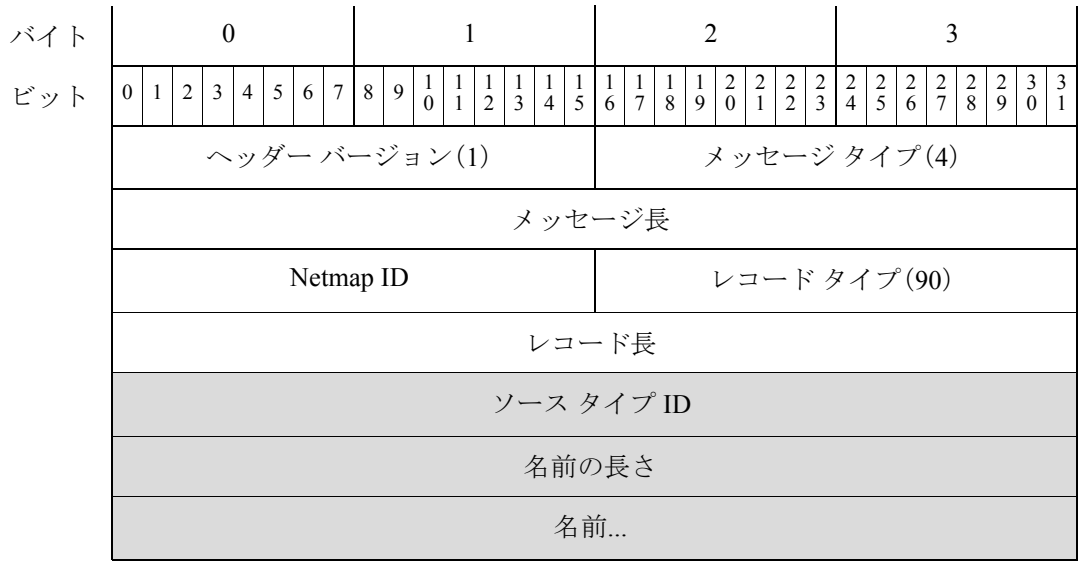
次の表では、サーバ レコードのフィールドについて説明します。

表 4-9　サーバ レコードのフィールド

フィールド	データ タイプ	説明
アプリケーション ID	uint32	アプリケーション プロトコルのアプリケーション ID 番号。
名前の長さ	uint32	サーバ名のバイト数。
名前	string	アプリケーション プロトコル名アプリケーション ID 65535 の場合、名前は unknown です。

ソース タイプ レコード

eStreamer サービスは、次の形式の送信元タイプ レコードで、イベントの送信元アプリケーションに関する情報を格納したメタデータを送信します。(送信元タイプ情報は、以下のメタデータ フラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。要求フラグ(2-12 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、送信元タイプ レコードを示す 90 です。



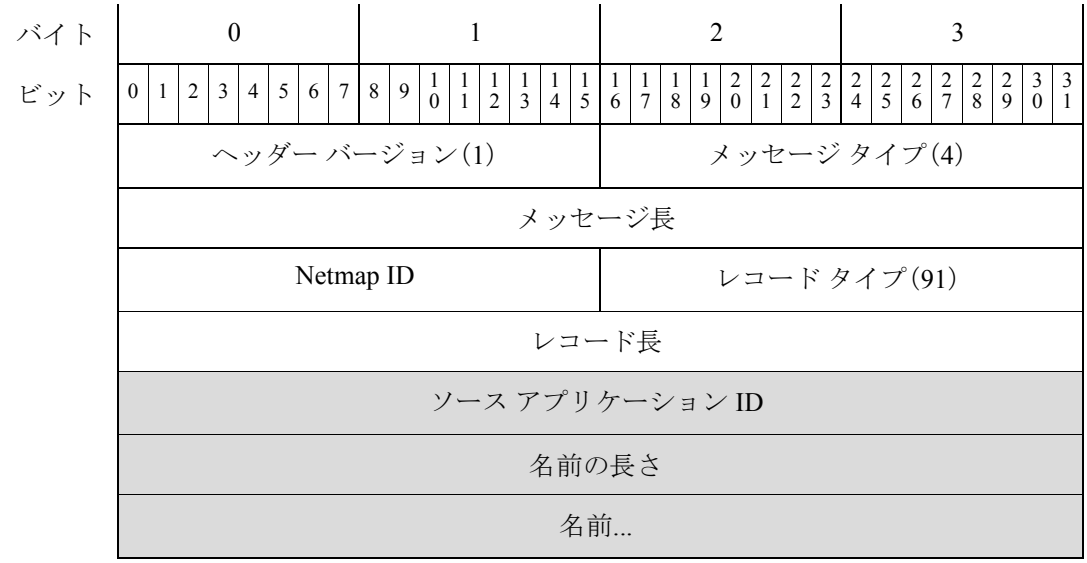
次の表では、ソース タイプ レコードのフィールドについて説明します。

表 4-10　ソース タイプ レコードのフィールド

フィールド	データ タイプ	説明
ソース タイプ ID	uint32	ソース タイプの ID 番号。
名前の長さ	uint32	送信元タイプ名のバイト数。
名前	string	ソース タイプ名。

ソース アプリケーション レコード

eStreamer サービスは、次の形式の送信元アプリケーション レコードで、ホスト ディスカバリ イベントの送信元アプリケーションに関する情報を格納したメタデータを送信します。(送信元アプリケーション情報は、以下のメタデータ フラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。要求フラグ(2-12 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、送信元アプリケーション レコードを示す 91 です。



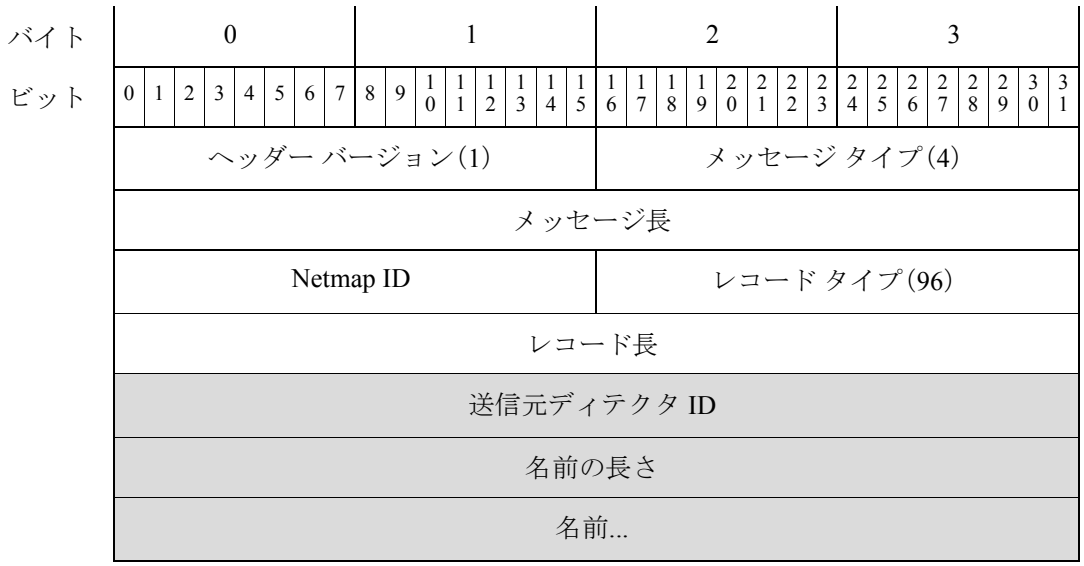
次の表では、ソース アプリケーション レコードのフィールドについて説明します。

表 4-11　送信元アプリケーション レコードのフィールド

フィールド	データ タイプ	説明
ソース アプリケーション ID	uint32	送信元アプリケーションの ID 番号。
名前の長さ	uint32	送信元アプリケーション名のバイト数。
名前	string	送信元アプリケーションの名前。

ソースディテクタ レコード

eStreamer サービスは、次の形式の送信元タイプ レコードで、ホスト ディスカバリ イベントの送信元アプリケーションに関する情報を格納したメタデータを送信します。(送信元タイプ情報は、以下のメタデータ フラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。要求フラグ(2-12 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、送信元ディテクタ レコードを示す 96 です。



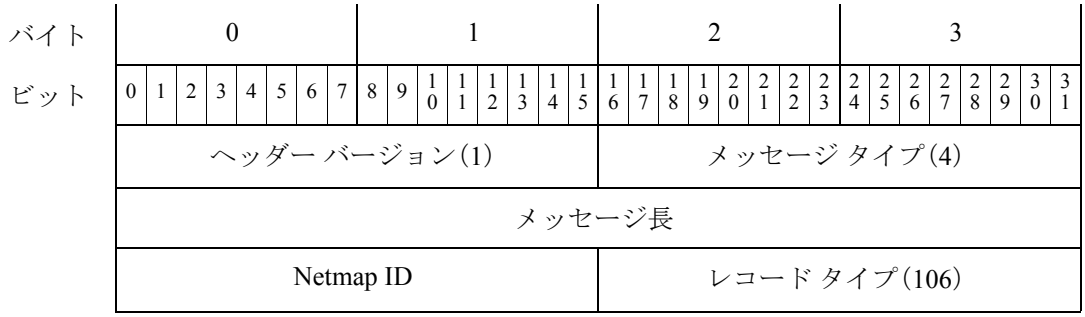
次の表では、送信元ディテクタ レコードのフィールドについて説明します。

表 4-12　送信元ディテクタ レコードのフィールド

フィールド	データ タイプ	説明
送信元ディテクタ ID	uint32	送信元ディテクタの ID 文字列。
名前の長さ	uint32	送信元タイプ名のバイト数。
名前	string	送信元ディテクタの名前。

サードパーティ スキャナの脆弱性レコード

eStreamer サービスは、次の形式のサードパーティ スキャナ脆弱性レコードで、イベントのサードパーティ脆弱性情報を格納したメタデータを送信します。(脆弱性情報は、以下のメタデータ フラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。要求フラグ(2-12 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、サードパーティ スキャナ脆弱性レコードを示す 106 です。



次の表では、脆弱性レコードのフィールドについて説明します。

表 4-13　サードパーティ スキャナ脆弱性レコードのフィールド

フィールド	データ タイプ	説明
脆弱性 ID	uint32	サードパーティ脆弱性 ID 番号。
スキャナ タイプ	uint32	サードパーティ スキャナ タイプ。
タイトル長さ	uint32	タイトル フィールド長さ。
タイトル	string	脆弱性のタイトル。
説明の長さ	uint32	説明フィールドの長さ。
説明	string	脆弱性に関する一般的な説明。
CVE ID 長さ	uint32	CVE ID フィールドの長さ。
CVE ID	string	脆弱性の Common Vulnerabilities and Exposures（CVE）ID 番号。
BugTraq ID の長さ	uint32	BugTraq ID フィールドの長さ。
BugTraq ID	string	脆弱性の BugTraq ID 番号

ユーザ レコード

eStreamer サービスは、次の形式のユーザ レコードで、システムが検出したユーザに関する情報を格納したメタデータを送信します。(バージョン 4 メタデータとポリシー イベント要求フラグ(それぞれ要求メッセージの要求フラグ フィールドのビット 20 と 22)を設定すると、ユーザ情報

が送信されます。要求フラグ (2-12 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、ユーザ レコードを示す 98 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(98)															
レコード長																																
ユーザ データ ブロック タイプ(57)																																
ユーザ データ ブロック長																																
ユーザ ID																																
プロトコル																																
文字列ブロック タイプ(0)																																
文字列ブロック長																																
ユーザ名...																																

次の表は、ユーザ レコードのフィールドについての説明です。

表 4-14　ユーザ レコードのフィールド

フィールド	データ タイプ	説明
ユーザ データ ブロック タイプ	uint32	ユーザ データ ブロックを開始します。この値は常に 57 です。ブロック タイプは、シリーズ 2 ブロックです。
ユーザ データ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
ユーザ ID	uint32	ユーザの固有識別情報。

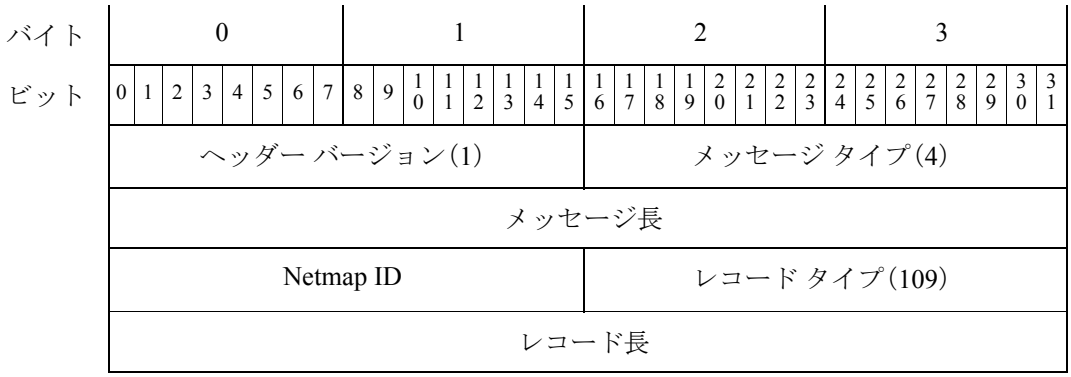
表 4-14　ユーザ レコードのフィールド(続き)

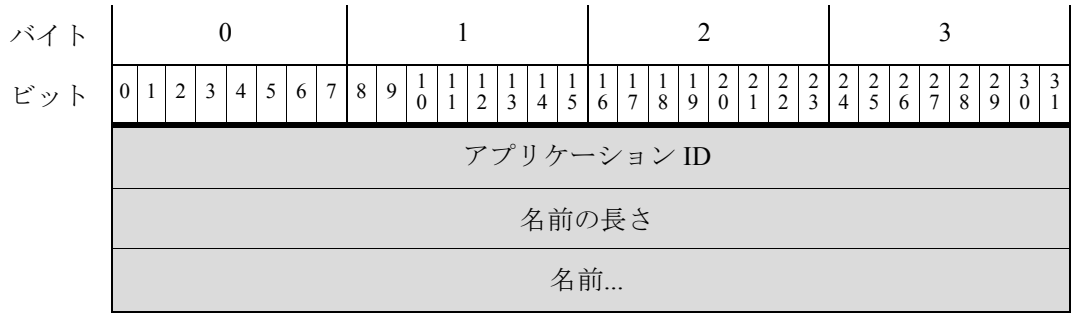
フィールド	データ タイプ	説明
プロトコル	uint32	ユーザの検出やレポートに使用するプロトコル。値は以下のとおりです。 • 165:FTP • 426:SIP • 547:AOL Instant Messenger • 683:IMAP • 710:LDAP • 767:NTP • 773:Oracle データベース • 788:POP3 • 1755:MDNS
文字列ブロック タイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトにユーザ名フィールドのバイト数を加えたユーザ名文字列データ ブロックのバイト数。
ユーザ名	string	ユーザの名前

Web アプリケーション レコード

システムは、Web サイトから送信される HTTP トラフィックの内容を検出します(該当する場合)。ホスト ディスカバリ イベント用の Web アプリケーション メタデータには、特定のタイプのコンテンツを格納できます。(WMV や QuickTime など)。

eStreamer サービスは、次の形式の Web アプリケーション レコードで、イベントの Web アプリケーション メタデータを送信します。(Web アプリケーション メタデータは、以下のメタデータ フラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。要求フラグ(2-12 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、Web アプリケーション レコードを示す 109 です。





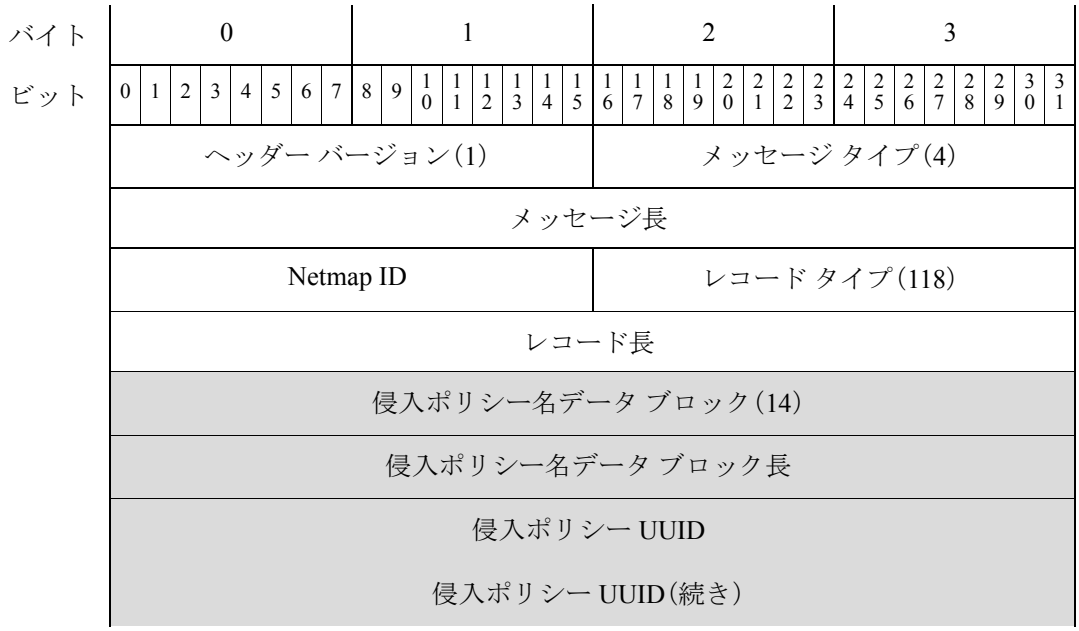
次の表では、Web アプリケーション レコードのフィールドについて説明します。

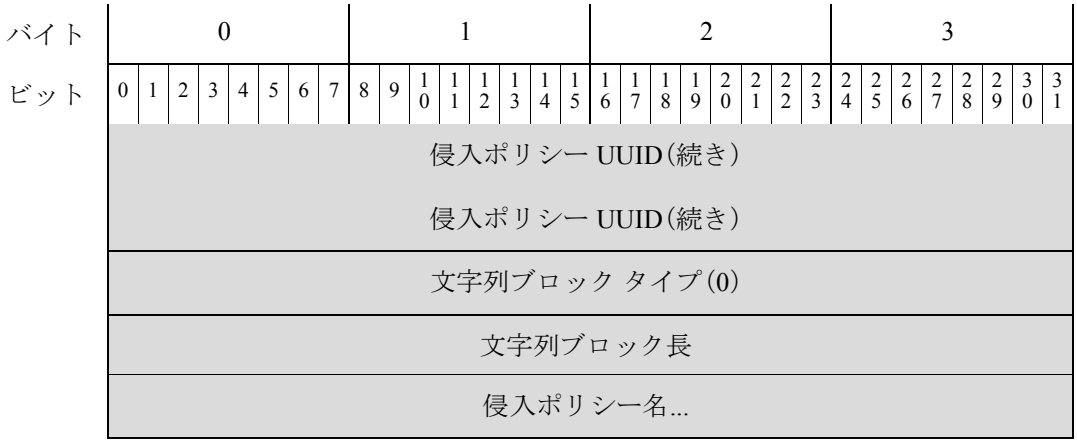
表 4-15　Web アプリケーション レコードのフィールド

フィールド	データ タイプ	説明
アプリケーション ID	uint32	Web アプリケーションのアプリケーション ID 番号。
名前の長さ	uint32	名前に含まれるバイト数。
名前	string	Web アプリケーションの内容の名前。

侵入ポリシー名レコード

eStreamer サービスは、次の形式の侵入ポリシー名レコードで、接続イベントの侵入ポリシー名情報を格納したメタデータを送信します。(侵入ポリシー名情報は、メタデータ フラグ(要求メッセージの要求フラグ フィールドのバージョン 4 メタデータ ビット 20)が設定されると送信されます。要求フラグ(2-12 ページ) を参照してください)。ちなみに、メッセージ長さフィールドの後のレコード タイプ フィールドの値は、侵入ポリシー名レコードを示す 118 です。シリーズ 2 セットのデータ ブロックのブロック タイプ 14 の UUID 文字列データ ブロックが含まれています。





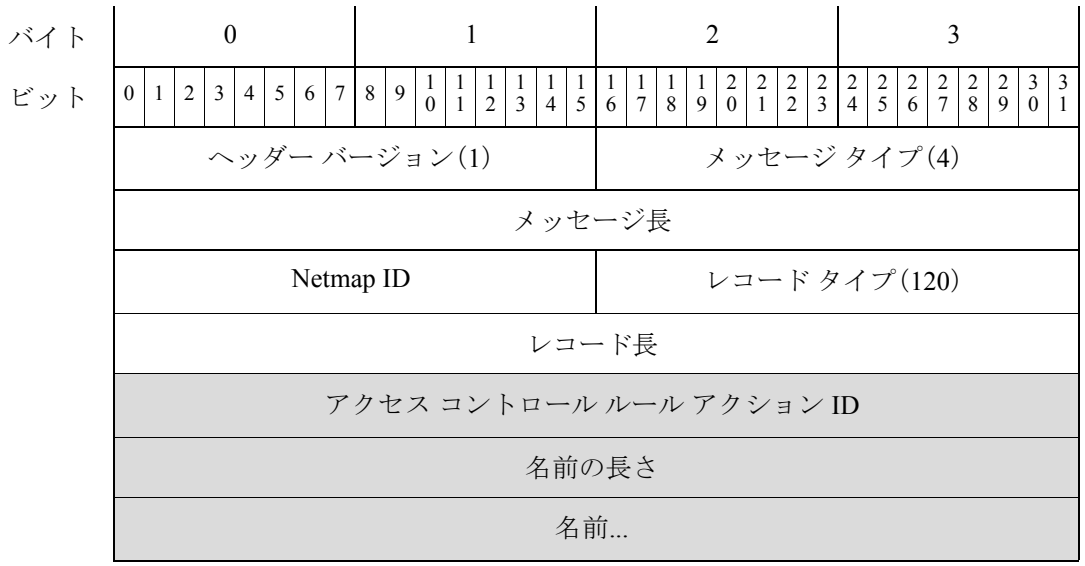
次の表では、侵入ポリシー名データ ブロックのフィールドについて説明します。

表 4-16　侵入ポリシー名データ ブロックのフィールド

フィールド	データ タイプ	説明
侵入ポリシー名データ ブロック タイプ	uint32	侵入ポリシー名データ ブロックを開始します。この値は常に 14 です。ブロック タイプは、シリーズ 2 ブロックです。
侵入ポリシー名データ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
侵入ポリシー UUID	uint8[16]	接続イベントに関連付けられた侵入ポリシーの固有識別子。
文字列ブロック タイプ	uint32	侵入ポリシーの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトに侵入ポリシー名のバイト数を加えた侵入名文字列データ ブロックのバイト数。
侵入ポリシー名	string	侵入ポリシー名。

アクセス コントロール ルール アクション レコード メタデータ

eStreamer サービスは、次の形式のアクセス コントロール ルール アクション レコードで、トリガーのかかったアクセス コントロール ルールに関連付けられたアクションを格納したメタデータを送信します。（アクセス コントロール ルール アクション情報は、バージョン 4 メタデータ フラグ（要求メッセージの要求フラグ フィールドのビット 20）が設定されると送信されます。要求フラグ（2-12 ページ） を参照してください）。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、アクセス コントロール ルール アクション レコードを示す 120 です。



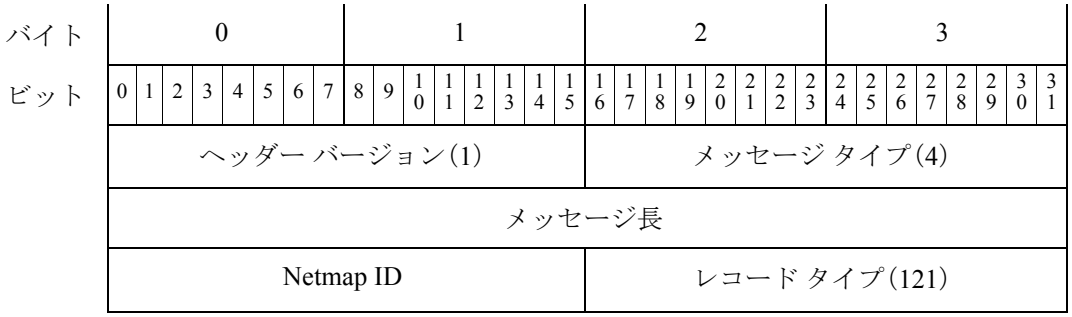
次の表では、アクセス コントロール ルール アクション レコードのフィールドについて説明します。

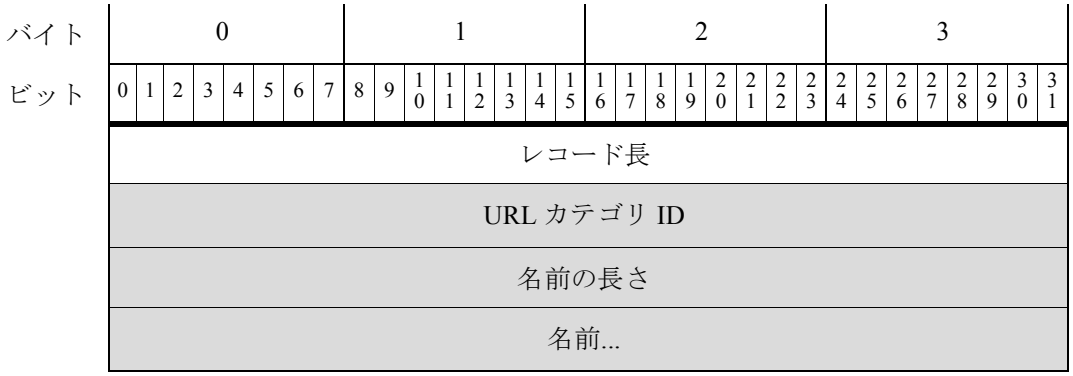
表 4-17　アクセス コントロール ルール アクション レコードのフィールド

フィールド	データ タイプ	説明
アクセス コントロール ルール アクション ID	uint32	アクセス コントロール ルール アクションの ID 番号。
名前の長さ	uint32	名前に含まれるバイト数。
名前	string	ファイアウォール ルール アクション名。

URL カテゴリ レコード メタデータ

eStreamer サービスは、次の形式の URL カテゴリ レコードで、接続ログの URL に関連付けられたカテゴリ名を格納したメタデータを送信します。(URL カテゴリ情報は、バージョン 4 メタデータ フラグ(要求メッセージの要求フラグ フィールドのビット 20)が設定されると送信されます。要求フラグ(2-12 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、URL カテゴリ レコードを示す 121 です。





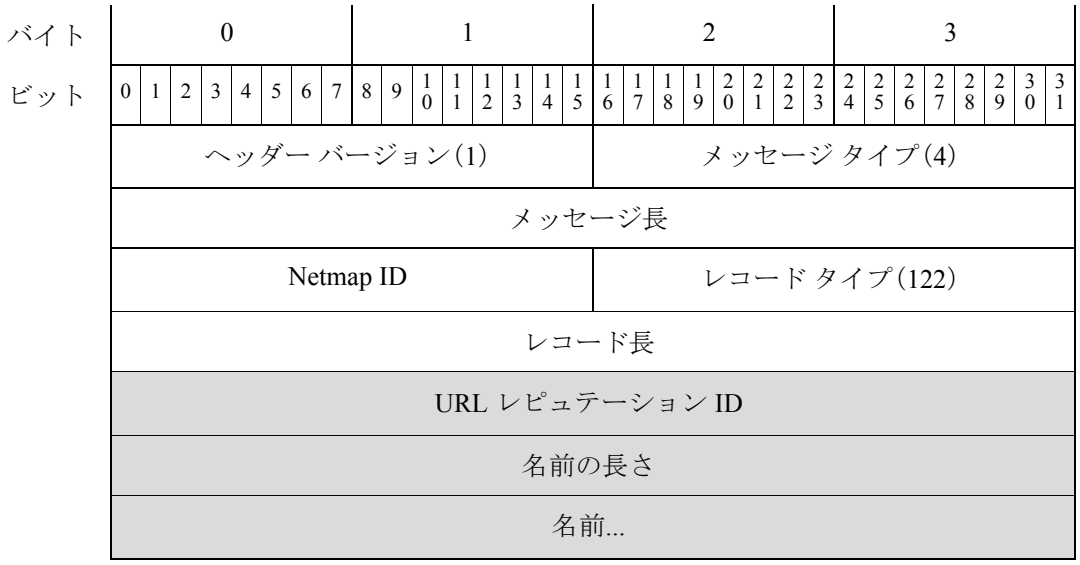
次の表では、URL カテゴリ レコードのフィールドについて説明します。

表 4-18　URL カテゴリ レコードのフィールド

フィールド	データ タイプ	説明
URL カテゴリ ID	uint32	URL カテゴリの ID 番号。
名前の長さ	uint32	名前に含まれるバイト数。
名前	string	URL カテゴリ名。

URL レピュテーション レコード メタデータ

eStreamer サービスは、次の形式の URL レピュテーション レコードで、URL に関連付けられたレピュテーション（リスク レベル）を格納したメタデータを送信します。（URL レピュテーション情報は、バージョン 4 メタデータ フラグ（要求メッセージの要求フラグ フィールドのビット 20）が設定されると送信されます。要求フラグ（2-12 ページ）を参照してください）。ちなみに、メッセージ長さフィールドの後の URL レピュテーション メタデータ レコード フィールドの値は、URL レピュテーション メタデータ レコードを示す 122 です。



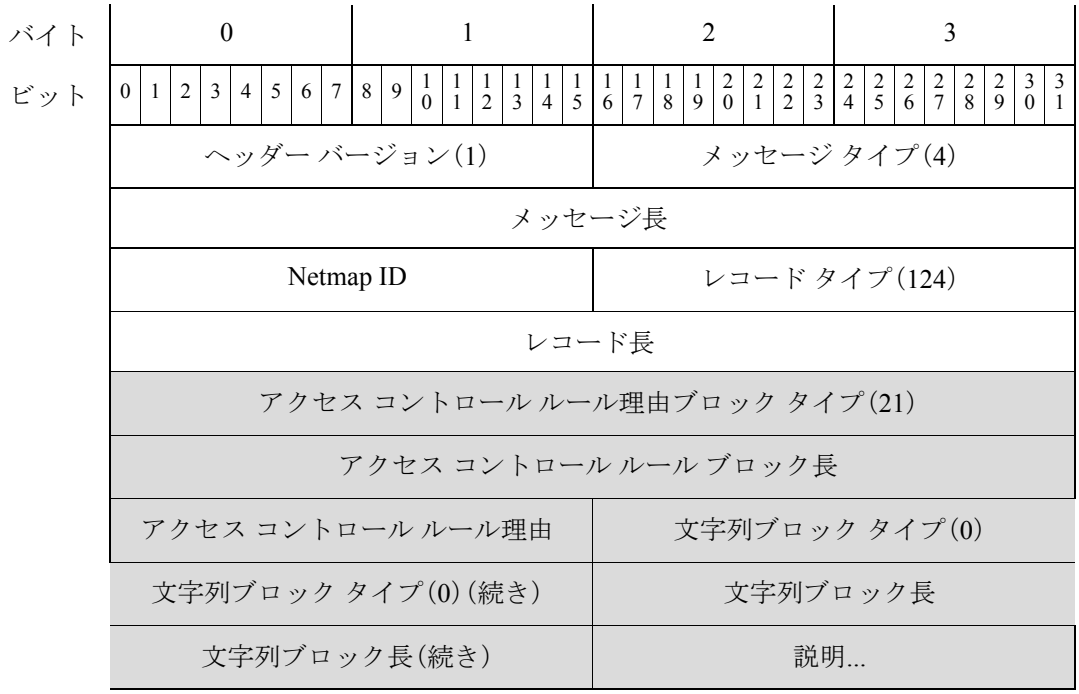
次の表では、URL レピュテーション レコードのフィールドについて説明します。

表 4-19　URL レピュテーション レコードのフィールド

フィールド	データ タイプ	説明
URL レピュテーション ID	uint32	URL レピュテーションの ID 番号。
名前の長さ	uint32	名前に含まれるバイト数。
名前	string	URL レピュテーション名。

アクセス コントロール ルール理由メタデータ

eStreamer サービスは、次の形式のアクセス コントロール ルール理由レコードで、アクセス コントロール ルールで侵入イベントまたは接続イベントにトリガーがかかった理由に関する情報を格納したメタデータを送信します。アクセス コントロール ルール理由メタデータは、バージョン 4 メタデータ フラグ（要求メッセージの要求フラグ フィールドのビット 20）が設定されると送信されます。要求フラグ（2-12 ページ）を参照してください。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、アクセス コントロール ルール理由レコードを示す 124 です。このメタデータには、アクセス コントロール ルール理由ブロックを格納します（アクセス コントロール ルール理由データ ブロック 5.1+（4-204 ページ）を参照）。アクセス コントロール ルール理由データ ブロックのブロック タイプは、シリーズ 2 のブロック タイプ 21 です。



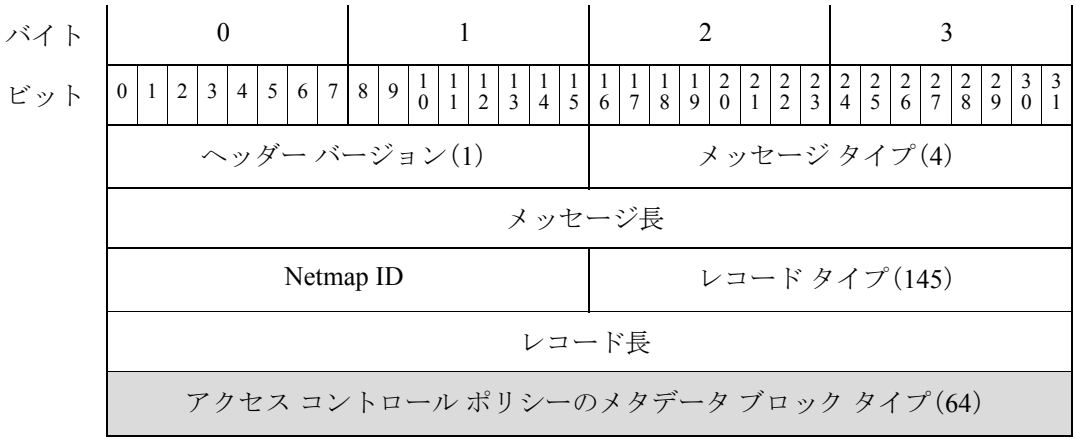
次の表では、アクセス コントロール ルール ID データ ブロックのフィールドについて説明します。

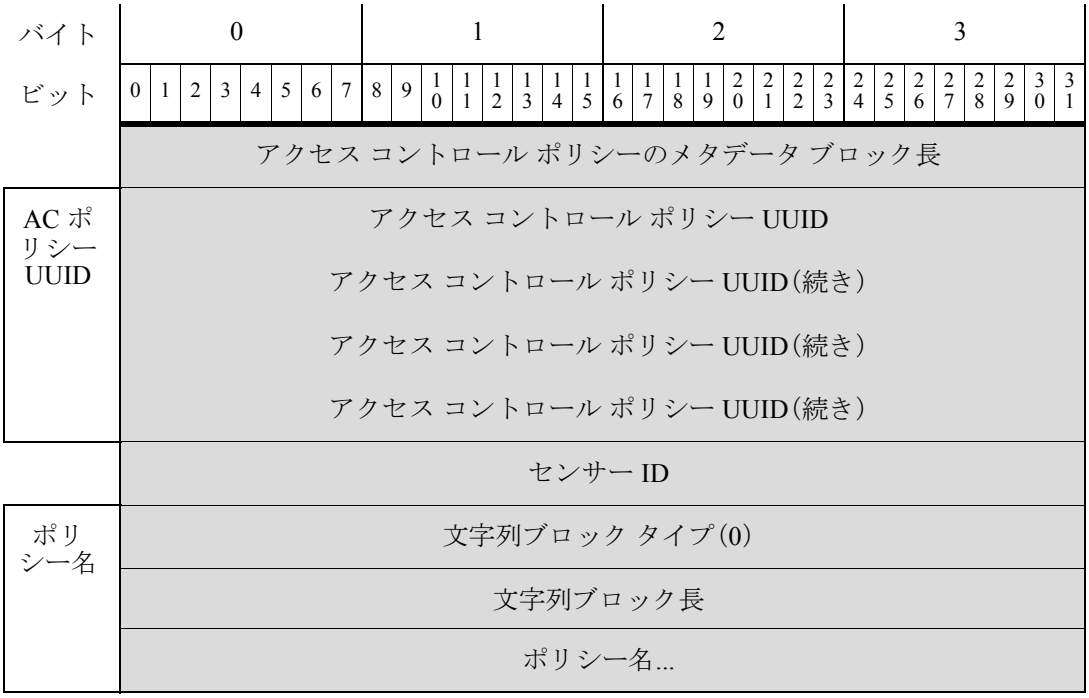
表 4-20　アクセス コントロール ルール理由メタデータのフィールド

フィールド	データ タイプ	説明
アクセス コントロール ルール理由ブロック タイプ	uint32	アクセス コントロール ルール理由ブロックを開始します。この値は常に 21 です。これはシリーズ 2 のデータ ブロックです。
アクセス コントロール ルール理由ブロック長	uint32	アクセス コントロール ルール理由ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ルール理由ブロックの合計バイト数。
アクセス コントロール ルール理由	uint16	アクセス コントロール ルールによって接続がログに記録された理由。
文字列ブロック タイプ	uint32	アクセス コントロール ルール理由に関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	アクセス コントロール ルール理由の説明。

アクセス コントロール ポリシー メタデータ

eStreamer サービスは、次の形式のアクセス コントロール ポリシー メタデータ レコードで、侵入イベントまたは接続イベントにトリガーをかけたアクセス コントロール ポリシーに関する情報を格納したメタデータを送信します。アクセス コントロール ルール ポリシー メタデータは、バージョン 4 メタデータ フラグ（要求メッセージの要求フラグ フィールドのビット 20）が設定されると送信されます。要求フラグ（2-12 ページ）を参照してください。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、アクセス コントロール ポリシー メタデータ レコードを示す 145 です。このメタデータには、アクセス コントロール ポリシー メタデータ ブロックを格納します（アクセス コントロール ポリシー メタデータ ブロック 6.0+（4-208 ページ）を参照）。アクセス コントロール ポリシー メタデータ ブロックのブロック タイプは、シリーズ 2 のブロック タイプ 64 です。





次の表では、アクセス コントロール ルール ID データ ブロックのフィールドについて説明します。

表 4-21　　アクセス コントロール ルール理由メタデータのフィールド

フィールド	データ タイプ	説明
アクセス コントロール ポリシーのメタデータ ブロック タイプ	uint32	アクセス コントロール ポリシー メタデータ ブロックを開始します。この値は常に 64 です。これはシリーズ 2 のデータ ブロックです。
アクセス コントロール ポリシーのメタデータ ブロック長	uint32	アクセス コントロール ポリシーのメタデータ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ポリシー メタデータ ブロックの合計バイト数。
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの UUID
センサー ID	uint32	アクセス コントロール ポリシーに関連付けられたセンサー ID 番号
文字列ブロック タイプ	uint32	アクセス コントロール ポリシーに関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
名前	string	アクセス コントロール ポリシーの名前。

プレフィルタ ポリシー メタデータ

eStreamer サービスは、次の形式のプレフィルタ ポリシーレコードで、侵入イベントまたは接続イベントにトリガーをかけたプレフィルタ ポリシーに関する情報を格納したメタデータを送信します。プレフィルタ ポリシー メタデータは、バージョン 4 メタデータ フラグ（要求メッセージの要求フラグ フィールドのビット 20）が設定されると送信されます。要求フラグ（2-12 ページ）を参照してください。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、プレフィルタポリシー メタデータ レコードであることを示す 146 です。このメタデータには、アクセス コントロール ポリシー メタデータ ブロックを格納します（アクセス コントロール ポリシー メタデータ ブロック 6.0+（4-208 ページ）を参照）。アクセス コントロール ポリシー メタデータ ブロックのブロック タイプは、シリーズ 2 のブロック タイプ 64 です。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		ヘッダー バージョン（1）																メッセージ タイプ（4）																
		メッセージ長																															
		Netmap ID																レコード タイプ（146）																
		レコード長																															
		アクセス コントロール ポリシーのメタデータ ブロック タイプ（64）																															
		アクセス コントロール ポリシーのメタデータ ブロック長																															
AC ポリシー UUID		アクセス コントロール ポリシー UUID																															
		アクセス コントロール ポリシー UUID（続き）																															
		アクセス コントロール ポリシー UUID（続き）																															
		アクセス コントロール ポリシー UUID（続き）																															
		センサー ID																															
ポリシー名		文字列ブロック タイプ（0）																															
		文字列ブロック長																															
		ポリシー名...																															

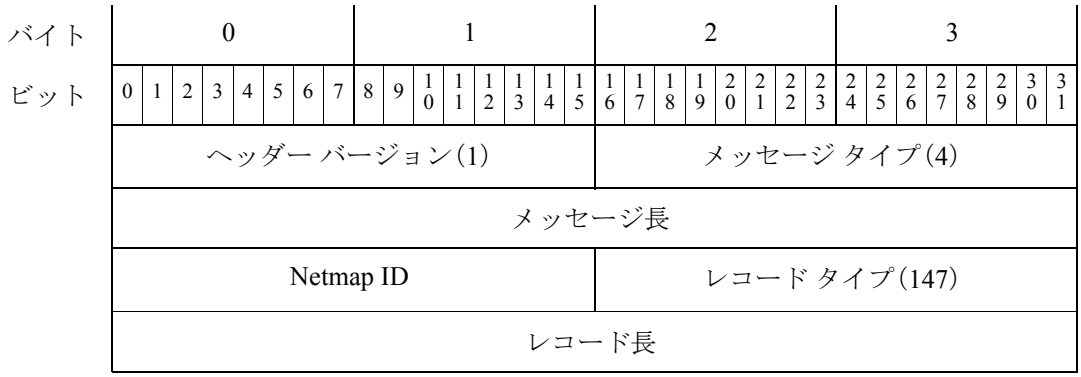
次の表では、プレフィルタ ポリシー メタデータ ブロックのフィールドについて説明します。

表 4-22　プレフィルタ ポリシー メタデータ フィールド

フィールド	データ タイプ	説明
アクセス コントロール ルール理由ブロック タイプ	uint32	アクセス コントロール ルール理由ブロックを開始します。この値は常に 64 です。これはシリーズ 2 のデータ ブロックです。
アクセス コントロール ルール理由ブロック長	uint32	アクセス コントロール ルール理由ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ルール理由ブロックの合計バイト数。
プレフィルタ ポリシー UUID	uint8[16]	プレフィルタ ポリシーの UUID
センサー ID	uint32	プレフィルタ ポリシーに関連付けられたセンサーの ID 番号
文字列ブロック タイプ	uint32	プレフィルタ ポリシーに関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
名前	string	プレフィルタ ポリシーの名前。

トンネルまたはプレフィルタのルールのメタデータ

eStreamer サービスは、次の形式のアクセス コントロール ルール理由レコードで、トンネル ルールまたはプレフィルタ ルールで侵入イベントまたは接続イベントにトリガーがかかった理由に関する情報を格納したメタデータを送信します。トンネル ルールまたはプレフィルタ ルールの理由メタデータは、バージョン 4 メタデータ フラグ（要求メッセージの要求フラグ フィールドのビット 20）が設定されると送信されます。要求フラグ（2-12 ページ）を参照してください。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、プレフィルタ ルール理由レコードであることを示す 147 です。
内容が同じなので、アクセス コントロール ルール理由ブロックを格納します（アクセス コントロール ルール データ ブロック（4-203 ページ）を参照）。アクセス コントロール ルール理由データ ブロックのブロック タイプは、シリーズ 2 のブロック タイプ 15 です。



次の表では、トンネルまたはプレフィルタ ルール理由メタデータ ブロックのフィールドについて説明します。

表 4-23　トンネルまたはプレフィルタ ルール理由メタデータ フィールド

フィールド	データ タイプ	説明
アクセス コントロール ルール ブロック タイプ	uint32	アクセス コントロール ルール ブロックを開始します。この値は常に 15 です。ちなみに、このブロックは、アクセス コントロール ルールだけでなく、トンネル ルールとプレフィルタ ルールにも使用します。
アクセス コントロール ルール ブロック長	uint32	アクセス コントロール ルール ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ルール ブロックの合計バイト数。
アクセス コントロール ルール UUID	uint8[16]	アクセス コントロール ルールの固有識別子。
アクセス コントロール ルール ID	uint32	アクセス コントロール ルールの内部 シスコ 識別子。
文字列ブロック タイプ	uint32	アクセス コントロール ルール UUID とアクセス コントロール ルール ID に関連付けられているわかりやすい名前のある文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
名前	string	わかりやすい名前。

セキュリティ インテリジェンス カテゴリ メタデータ

eStreamer サービスは、次の形式のセキュリティ インテリジェンス カテゴリ レコードで、セキュリティ インテリジェンス カテゴリに関する情報を格納したメタデータを送信します。アクセス コントロール ルール理由メタデータは、バージョン 4 メタデータ フラグ（要求メッセージの要求フラグ フィールドのビット 20）が設定されると送信されます。要求フラグ（2-12 ページ）を参照してください。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、セキュリティ インテリジェンス カテゴリ レコードを示す 280 です。これには、セキュリティ インテリジェンス カテゴリ データ ブロックを格納します（セキュリティ インテリジェンス カテゴリ データ ブロック 5.1+（4-205 ページ）を参照）。セキュリティ インテリジェンス データ ブロックのブロック タイプは、シリーズ 2 のブロック タイプ 22 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（280）															
レコード長																																
セキュリティ インテリジェンス カテゴリのブロック タイプ（22）																																
セキュリティ インテリジェンス カテゴリのブロック長																																
セキュリティ インテリジェンス リスト ID																																
アクセス コントロール ポリシー UUID																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
文字列ブロック タイプ（0）																																
文字列ブロック長																																
セキュリティ インテリジェンス リスト名...																																

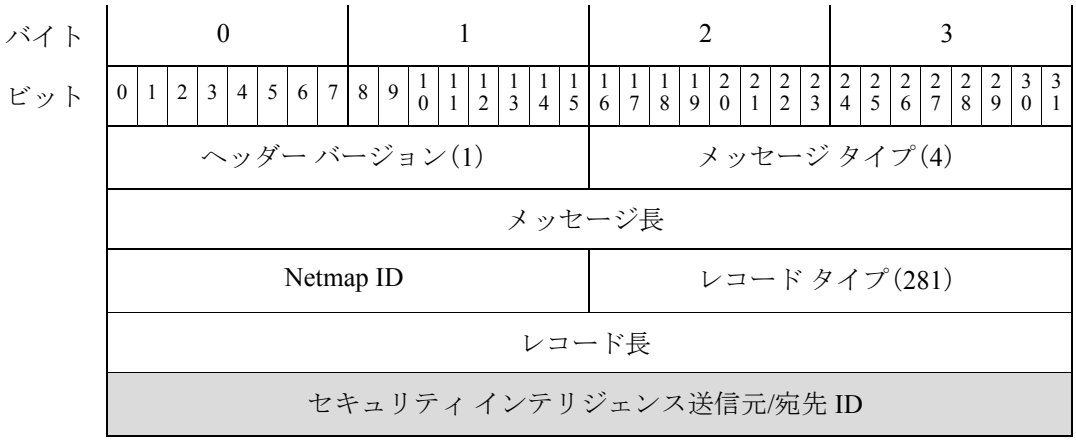
次の表では、セキュリティ インテリジェンス カテゴリ レコードのフィールドについて説明します。

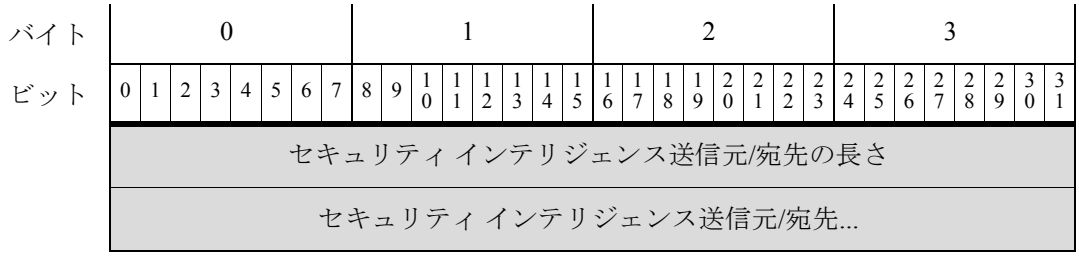
表 4-24　セキュリティ インテリジェンス カテゴリ メタデータのフィールド

フィールド	データ タイプ	説明
セキュリティ インテリジェンス カテゴリ ブロック タイプ	uint32	セキュリティ インテリジェンス カテゴリのデータ ブロックを開始します。この値は常に 22 です。これはシリーズ 2 のデータ ブロックです。
セキュリティ インテリジェンス カテゴリのブロック長	uint32	セキュリティ インテリジェンス カテゴリ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたセキュリティ インテリジェンス カテゴリ ブロックの合計バイト数。
セキュリティ インテリジェンス リスト ID	uint32	接続でトリガーがかかる IP ブラックリストまたはホワイトリストの ID。
アクセス コントロール ポリシー UUID	uint8[16]	セキュリティ インテリジェンスに設定されたアクセス コントロール ポリシーの UUID。
文字列ブロック タイプ	uint32	アクセス コントロール ルール理由に関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトにセキュリティ インテリジェンス リスト名フィールドのバイト数を加えた名前文字列データ ブロックのバイト数。
セキュリティ インテリジェンス リスト名	string	接続でトリガーがかかる IP カテゴリ ブラックリストまたはホワイトリストの名前。

セキュリティ インテリジェンス送信元/宛先レコード

eStreamer サービスは、次の形式のセキュリティ インテリジェンス送信元/宛先レコードで、セキュリティ インテリジェンスで検出した IP アドレスが、送信元 IP アドレスと宛先 IP アドレスのいずれであるかを示すメタデータを送信します。(送信元/宛先 IP 情報は、以下のメタデータ フラグの 1つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。要求フラグ(2-12 ページ) を参照してください)。ちなみに、メッセージ長 フィールドの後のレコード タイプ フィールドの値は、セキュリティ インテリジェンス送信元/宛先レコードを示す 281 です。





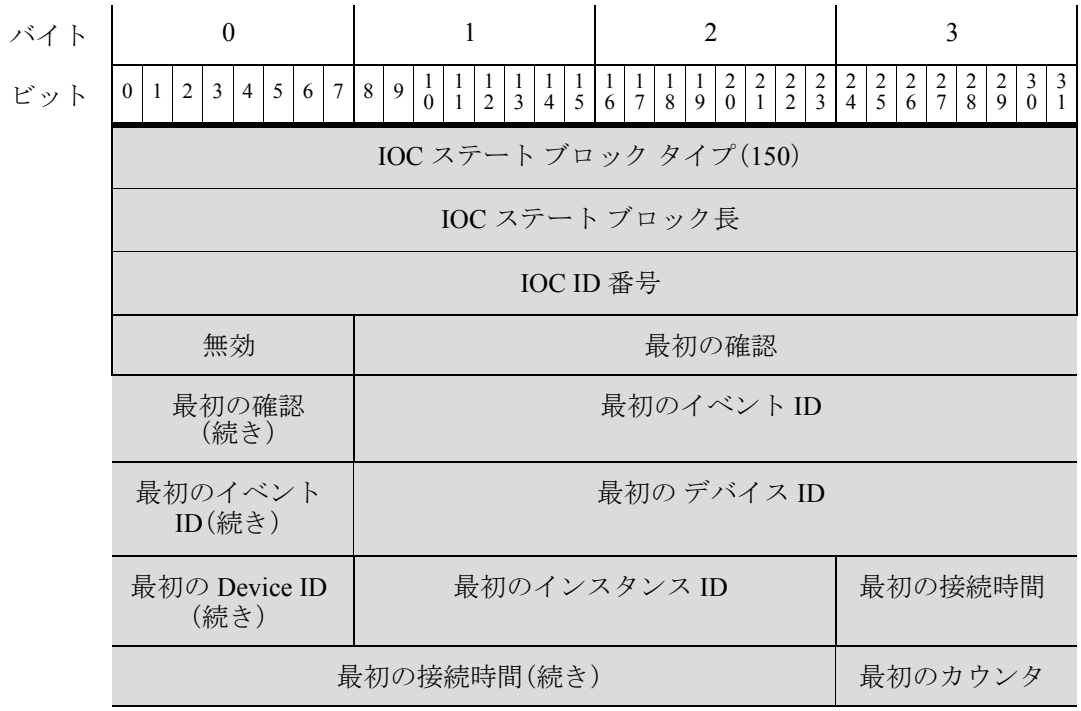
次の表では、セキュリティ インテリジェンス送信元/宛先レコードのフィールドについて説明します。

表 4-25　セキュリティ インテリジェンス送信元/宛先レコードのフィールド

フィールド	データ タイプ	説明
セキュリティ インテリジェンス送信元/宛先 ID	uint32	セキュリティ インテリジェンス送信元/宛先 ID 番号。
セキュリティ インテリジェンス送信元/宛先長さ	uint32	セキュリティ インテリジェンス送信元/宛先バイト数。
セキュリティ インテリジェンス送信元/宛先	string	検出した IP アドレスは、送信元または宛先の IP アドレスであるかどうか。

5.3+ の IOC ステート データ ブロック

IOC ステート データ ブロックは、Indication of Compromise（IOC）に関する情報を提供します。これは シリーズ 1 のブロック タイプ 150 です。このブロックに、ホスト トラッカはホスト上の侵害に関する情報を保存します。次の図は IOC ステート データ ブロックの構造です。



次の表では、IOC ステート データ ブロックのコンポーネントについて説明します。

表 4-26　IOC ステート データ ブロックのフィールド

フィールド	データ タイプ	説明
IOC ステート データ ブロック タイプ	uint32	IOC ステート データ ブロックを開始します。この値は常に 150 です。
IOC ステート データ ブロックの長さ	uint32	IOC ステート データ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えた IOC ステート データ ブロックの合計バイト数。
IOC ID 番号	uint32	侵害の固有 ID 番号。
無効	uint8	侵害がホストで無効にされているかどうかを示します: • 0:侵害は無効ではありません。 • 1:侵害が無効です。
最初の確認	uint32	この侵害の最初の検出時を示す UNIX タイムスタンプ。
最初のイベント ID	uint32	この侵害が最初に確認されたイベントの ID 番号。
最初の デバイス ID	uint32	最初に IOC を検出したセンサーの ID。
最初のインスタンス ID	uint16	最初に侵害を検出した管理対象デバイスの Snort インスタンスの数値 ID。
最初の接続時間	uint32	この侵害を最初に検出した接続の Unix タイムスタンプ。
最初のカウンタ	uint16	この侵害を最後の確認日時した接続のカウンタ。 これで、同時に発生する複数の接続を区別します。

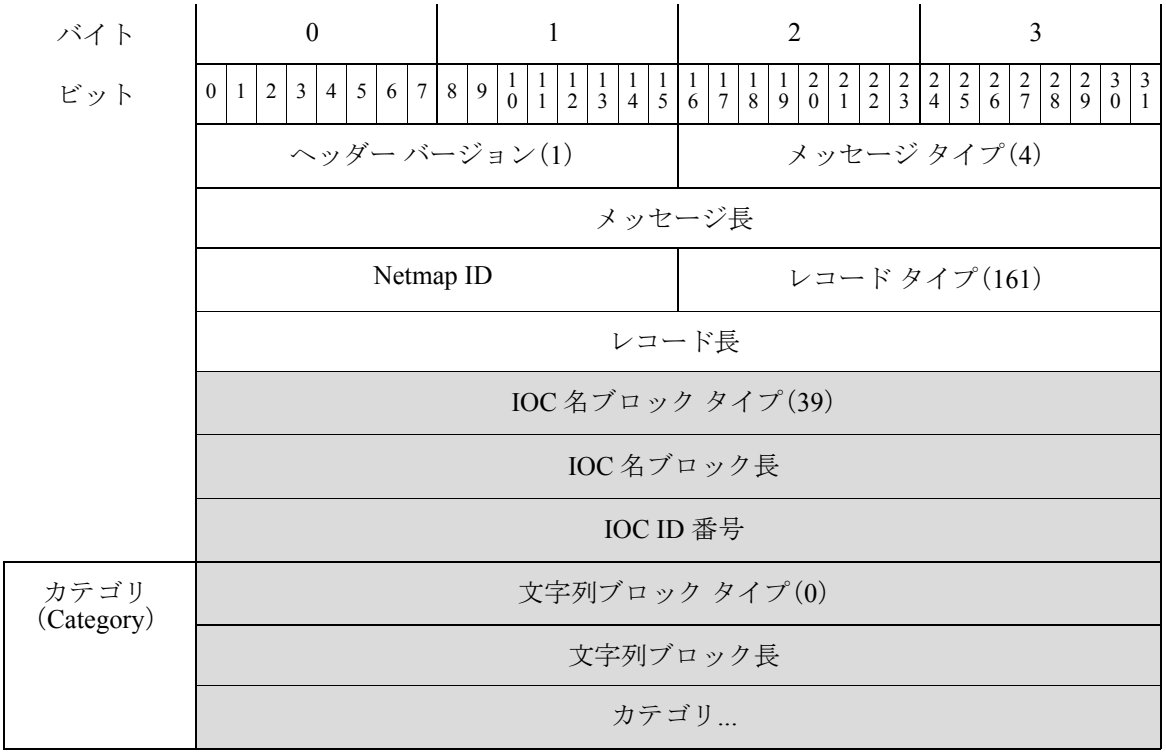
表 4-26　IOC ステート データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
最後の確認日時	uint32	この侵害の前回の検出時を示す UNIX タイムスタンプ。
前回イベント ID	uint32	この侵害を最後の確認日時したイベントの ID 番号。
前回 デバイス ID	uint32	前回 IOC を検出したセンサーの ID。
前回インスタンス ID	uint16	前回侵害を検出した管理対象デバイスの Snort インスタンスの数値 ID。
前回接続時間	uint32	この侵害を最後の確認日時した接続の Unix タイムスタンプ。
前回カウンタ	uint16	この侵害を最後の確認日時した接続のカウンタ。 これで、同時に発生する複数の接続を区別します。

5.3+ の IOC 名データ ブロック

これは Indication of Compromise（IOC）のカテゴリとイベント タイプを提供するデータ ブロックです。レコード タイプは 161 で、シリーズ 2 のブロック タイプ 39 です。これは IOC 情報があるすべてのイベントでメタデータとして適用されます。該当するイベントには、マルウェア イベント、ファイル イベント、侵入イベントがあります。

次の図は、IOC 名データ ブロックの構造です。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
イベント タイプ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	イベント タイプ...																															

次の表では、IOC データ名データ ブロックのフィールドについて説明します。

表 4-27　IOC 名データ ブロックのフィールド

フィールド	データ タイプ	説明
IOC 名データ ブロック タイプ	uint32	IOC 名データ ブロックを開始します。この値は常に 39 です。
IOC 名データ ブロック長	uint32	IOC 名データ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えた IOC 名データ ブロックの合計バイト数。
IOC ID 番号	uint32	侵害の固有 ID 番号。
文字列ブロック タイプ	uint32	侵害に関連付けられたカテゴリを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとカテゴリ フィールドのバイト数が含まれます。
カテゴリ（Category）	string	侵害のカテゴリ。有効な値は次のとおりです。 • CnC Connected • Exploit Kit • High Impact Attack • Low Impact Attack • Malware Detected • Malware Executed • Dropper Infection • Java Compromise • Word Compromise • Adobe Reader Compromise • Excel Compromise • PowerPoint Compromise • QuickTime Compromise
文字列ブロック タイプ	uint32	侵害に関連付けられたイベント タイプを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとイベント タイプ フィールドのバイト数が含まれます。

表 4-27　IOC 名データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
イベント タイプ	string	侵害のイベント タイプ。有効な値は次のとおりです。 • Adobe Reader launched shell • Dropper Infection Detected by AMP for Endpoints • Excel Compromise Detected by AMP for Endpoints • Excel launched shell • Impact 1 Intrusion Event - attempted-admin • Impact 1 Intrusion Event - attempted-user • Impact 1 Intrusion Event - successful-admin • Impact 1 Intrusion Event - successful-user • Impact 1 Intrusion Event - web-application-attack • Impact 2 Intrusion Event - attempted-admin • Impact 2 Intrusion Event - attempted-user • Impact 2 Intrusion Event - successful-admin • Impact 2 Intrusion Event - successful-user • Impact 2 Intrusion Event - web-application-attack • Intrusion Event - exploit-kit • Intrusion Event - malware-backdoor • Intrusion Event - malware-cnc • Java Compromise Detected by AMP for Endpoints • Java launched shell • PDF Compromise Detected by AMP for Endpoints • PowerPoint Compromise Detected by AMP for Endpoints • PowerPoint launched shell • QuickTime Compromise Detected by AMP for Endpoints • QuickTime launched shell • Security Intelligence Event - CnC • Security Intelligence Event - DNS CnC • Security Intelligence Event - DNS Malware • Security Intelligence Event - DNS Phishing • Security Intelligence Event - Sinkhole CnC • Security Intelligence Event - Sinkhole Malware • Security Intelligence Event - Sinkhole Phishing • Security Intelligence Event - URL CnC • Security Intelligence Event - URL Malware • Security Intelligence Event - URL Phishing • Suspected Botnet Detected by AMP for Endpoints • Threat Detected by AMP for Endpoints - Executed • Threat Detected by AMP for Endpoints - Not Executed • Threat Detected in File Transfer • Word Compromise Detected by AMP for Endpoints • Word launched shell

ディスカバリ イベント ヘッダー 5.2+

ディスカバリ イベントおよび接続イベントのメッセージには、ディスカバリ イベント ヘッダーが含まれます。これは、イベントのタイプおよびサブタイプ、イベントが発生した時刻、イベントが発生したデバイス、およびメッセージ内のイベント データの構造を伝えます。このヘッダーには、実際のホスト ディスカバリ、ユーザ、または接続イベントのデータが続きます。さまざまなイベントのタイプ/サブタイプ値に関連付けられる構造の詳細については、イベント タイプ別ホスト ディスカバリ構造（4-44 ページ）で説明します。このヘッダーは IPv6 をサポートしており、ディスカバリ イベント ヘッダー 5.0 ～ 5.1.1.x（B-93 ページ） はサポートを停止しました。

ディスカバリ イベント ヘッダーのイベント タイプ フィールドおよびイベント サブタイプ フィールドは、送信されたイベント メッセージの構造を示します。イベント データ ブロックの構造が一度判別されたら、プログラムはメッセージを適切に解析できます。

次の図の網掛けされた行は、ディスカバリ イベント ヘッダーの形式を例示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン（1）																メッセージ タイプ（4）															
	メッセージ長																															
	Netmap ID																レコード タイプ															
	レコード長																															
	eStreamer サーバ タイムスタンプ（イベント用、ビット 23 が設定されている場合のみ）																															
	将来の使用に備えて予約済み（イベントでビット 23 が設定されている場合のみ）																															
ディスカバリ イベント ヘッダー	デバイス ID																															
	レガシー IP アドレス																															
	MAC アドレス																															
	MAC アドレス（続き）																IPv6 あり								将来の使用に備えて予約済み							
	イベント秒																															
	イベント マイクロ秒																															
	イベント タイプ																															
	イベント サブタイプ																															
	ファイル番号（内部使用専用）																															
	ファイルの位置（内部使用専用）																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IPv6アドレス																															
	IPv6 アドレス（続き）																															
	IPv6 アドレス（続き）																															
	IPv6 アドレス（続き）																															

次の表は、ディスカバリ イベント ヘッダーについての説明です。

表 4-28　ディスカバリ イベント ヘッダーのフィールド

フィールド	データ型	説明
デバイス ID	uint32	ディスカバリ イベントを生成したデバイスの ID 番号。バージョン 3 および 4 のメタデータを要求すると、デバイスのメタデータを入手できます。詳細については、管理対象デバイス レコードのメタデータ（3-38 ページ）を参照してください。
レガシー IP アドレス	uint32	このフィールドは予約済みですが、設定されておりません。IPv4 アドレスは IPv6 アドレス フィールドに保存されます。詳細については、IP アドレス（1-6 ページ）を参照してください。
MAC アドレス	uint86	イベントに関連するホストの MAC アドレス。
IPv6 あり	uint8	ホストに IPv6 アドレスがあることを示すフラグ。
将来の使用に備えて予約済み	uint8	将来の使用に備えて予約済み
イベント秒	uint32	システムがイベントを生成したときの UNIX タイムスタンプ（1970 年 1 月 1 日以降の秒数）。
イベント マイクロ秒	uint32	システムがイベントを生成したときのタイムスタンプの、マイクロ秒（100 万分の 1 秒）の増分。
イベント タイプ	uint32	イベント タイプ（新規イベントは 1000、変更イベントは、1001、ユーザ入力イベントは1002、フル ホスト プロファイルは1050）。使用可能なイベント タイプの一覧の詳細については、イベント タイプ別ホスト ディスカバリ構造（4-44 ページ）を参照してください。
イベント サブタイプ	uint32	イベント サブタイプ。使用可能なイベント サブタイプの一覧の詳細については、イベント タイプ別ホスト ディスカバリ構造（4-44 ページ）を参照してください。
ファイル番号	byte[4]	シリアル ファイル番号。このフィールドは、シスコ の内部使用のためのものであり、無視してかまいません。

表 4-28　ディスカバリ イベント ヘッダーのフィールド(続き)

フィールド	データ型	説明
ファイルの位置	byte[4]	シリアル ファイル内のイベントの位置。このフィールドは、シスコ の内部使用のためのものであり、無視してかまいません。
IPv6アドレス	uin8[16]	IPv6 アドレス。このフィールドは、IPv6 フラグが設定されている場合に存在し、使用されます。

ディスカバリ イベントと接続イベントのタイプとサブタイプ

イベント タイプとイベント サブタイプ フィールド値でホストのディスカバリ メッセージまたはユーザ データ内のイベントを特定し、分類します。メッセージのデータ構造も識別します。

次の表は、ディスカバリ イベントと接続イベントのイベント タイプとイベント サブタイプです。

表 4-29　タイプ/サブタイプ別のディスカバリ イベントと接続イベント

イベント名	イベント タイプ	イベント サブタイプ
新規ホスト	1000	1
新規 TCP サーバ	1000	2
新規ネットワーク プロトコル	1000	3
新規トランスポート プロトコル	1000	4
新規 IP 対 IP トラフィック	1000	5
新規 UDP サーバ	1000	6
新規クライアント アプリケーション	1000	7
新規 OS	1000	8
IPv6 トラフィックに新しい IPv6	1000	9
ホスト IP アドレスを変更	1001	1
OS 情報の更新	1001	2
ホスト IP アドレスを再利用	1001	3
脆弱性の変更	1001	4
ホップ数の変更	1001	5
TCP サーバ情報更新	1001	6
ホスト タイムアウト	1001	7
TCP ポート クローズ	1001	8
UDP ポート クローズ	1001	9
UDP サーバ情報更新	1001	10
TCP ポート タイムアウト	1001	11
UDP ポート タイムアウト	1001	12
MAC 情報の変更	1001	13
ホストの追加 MAC を検出	1001	14

表 4-29　タイプ/サブタイプ別のディスカバリ イベントと接続イベント(続き)

イベント名	イベント タイプ	イベント サブタイプ
最終検出時のホスト	1001	15
ルータ/ブリッジとして識別したホスト	1001	16
接続統計情報	1001	17
VLAN タグ情報更新	1001	18
ホストを削除。ホスト上限に到達	1001	19
クライアント アプリケーション タイムアウト	1001	20
NetBIOS 名変更	1001	21
NetBIOS ドメイン変更	1001	22
ホストをドロップ。ホスト上限に到達	1001	23
バナー更新	1001	24
TCP サーバ信頼度更新	1001	25
UDP サーバ信頼度更新	1001	26
アイデンティティ競合	1001	29
アイデンティティ タイムアウト	1001	30
セカンダリホスト更新	1001	31
クライアント アプリケーション更新	1001	32
ユーザ設定の有効な脆弱性(レガシー)	1002	1
ユーザ設定の無効な脆弱性(レガシー)	1002	2
ユーザ削除アドレス(レガシー)	1002	3
ユーザ削除サーバ(レガシー)	1002	4
ユーザ設定ホスト重要度	1002	5
ホスト属性追加	1002	6
ホスト属性更新	1002	7
ホスト属性削除	1002	8
ホスト属性設定値(レガシー)	1002	9
ホスト属性削除値(レガシー)	1002	10
スキャン結果を追加	1002	11
ユーザ設定脆弱性資格	1002	12
ユーザポリシー制御	1002	13
プロトコルを削除	1002	14
クライアント アプリケーションを削除	1002	15
ユーザ設定オペレーティング システム	1002	16
ユーザ アカウント確認	1002	17
ユーザ アカウント更新	1002	18
ユーザ設定サーバ	1002	19

表 4-29　タイプ/サブタイプ別のディスカバリ イベントと接続イベント（続き）

イベント名	イベント タイプ	イベント サブタイプ
ユーザ削除アドレス（現在）	1002	20
ユーザ削除サーバ（現在）	1002	21
ユーザ設定の有効な脆弱性（現在）	1002	22
ユーザ設定の無効な脆弱性（現在）	1002	23
ユーザ ホスト重要度	1002	24
ホスト属性設定値（現在）	1002	25
ホスト属性削除値（現在）	1002	26
ユーザ追加ホスト	1002	27
ユーザ追加サーバ	1002	28
ユーザ追加クライアント アプリケーション	1002	29
ユーザ追加プロトコル	1002	30
アプリを再読み込み	1002	31
アカウント削除	1002	32
接続統計情報	1003	1
接続チャンク	1003	2
新規ユーザ アイデンティティ	1004	1
ユーザ ログイン	1004	2
ユーザ アイデンティティを削除	1004	3
ユーザ アイデンティティをドロップ。ユーザ上限に到達	1004	4
ホスト IOC 設定タイプ	1008	1
フル ホスト プロファイル	1050	該当なし

ヒント　各イベント タイプ/サブタイプに使用するデータ構造については、イベント タイプ別ホスト ディスカバリ構造（4-44 ページ）を参照してください。

イベント タイプ別ホスト ディスカバリ構造

eStreamer は、ディスカバリ イベント ヘッダーで指定されたイベント タイプに基づいてホスト ディスカバリ イベント メッセージを構築します。次の項では、各イベント タイプの概略構造を紹介します。

- 新規ホスト メッセージと最後の確認日時ホスト メッセージ（4-45 ページ）
- サーバ メッセージ（4-46 ページ）
- 新規ネットワーク プロトコル メッセージ（4-47 ページ）
- 新規トランスポート プロトコル メッセージ（4-47 ページ）
- クライアント アプリケーション メッセージ（4-48 ページ）

- IP アドレス変更メッセージ(4-48 ページ)
- オペレーティング システム更新メッセージ(4-49 ページ)
- IP アドレスを再利用とホスト タイムアウト/削除メッセージ(4-50 ページ)
- ホップ変更メッセージ(4-50 ページ)
- ホップ変更メッセージ(4-50 ページ)
- TCP と UDP のポート クローズ メッセージ/タイムアウト メッセージ(4-51 ページ)
- MAC アドレス メッセージ(4-51 ページ)
- ブリッジ/ルータとして識別したホスト メッセージ(4-52 ページ)
- VLAN タグ情報更新メッセージ(4-52 ページ)
- NetBIOS 名変更メッセージ(4-53 ページ)
- 更新バナー メッセージ(4-53 ページ)
- ポリシー制御の概要(4-54 ページ)
- 接続統計データ メッセージ(4-54 ページ)
- 接続チャンク メッセージ(4-55 ページ)
- バージョン4.6.1+ のユーザ設定脆弱性メッセージ(4-55 ページ)
- ユーザ追加/削除ホスト メッセージ(4-56 ページ)
- ユーザ削除サーバ メッセージ(4-56 ページ)
- ユーザ設定ホスト重要度メッセージ(4-57 ページ)
- 属性メッセージ(4-57 ページ)
- 属性値メッセージ(4-58 ページ)
- ユーザ サーバ メッセージとオペレーティング システム メッセージ(4-58 ページ)
- ユーザ プロトコル メッセージ(4-59 ページ)
- ユーザ クライアント アプリケーション メッセージ(4-59 ページ)
- スキャン結果を追加メッセージ(4-60 ページ)
- 新規オペレーティング システム メッセージ(4-60 ページ)
- アイデンティティ競合とアイデンティティ タイムアウト システム メッセージ(4-61 ページ)
- ホスト IOC セット メッセージ(4-61 ページ)

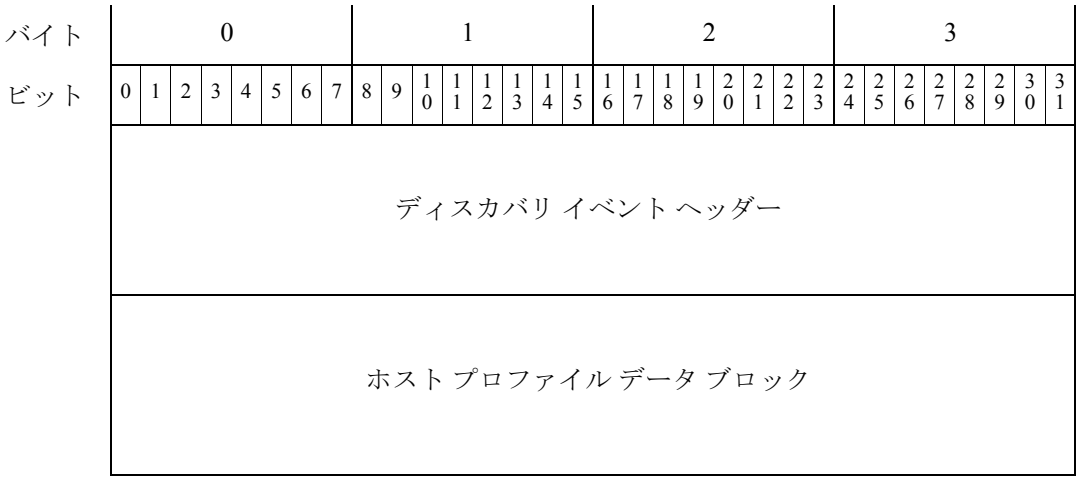
以下の項のデータ ブロック図は、ホスト ディスカバリ イベント メッセージで返る各種レコード データ ブロックです。

新規ホスト メッセージと最後の確認日時ホスト メッセージ

新規ホスト イベント メッセージと最後の確認日時ホスト イベント メッセージには、標準ディスカバリ イベント ヘッダーとホスト プロファイル データ ブロックがあります(ホスト プロファイル データブロック 5.2+(4-169 ページ) を参照)。ホスト プロファイル データ ブロックのブロック タイプは、シリーズ 1 のブロック タイプ 139 です。

なお、最後の確認日時ホスト メッセージにある情報は、ホスト上のディスカバリ検出ポリシーで設定した更新間隔内で変更されたサーバのサーバ情報のみです。つまり、最後の確認日時ホスト メッセージに含まれるのは、システムが前回情報を報告した後に変更されたサーバ ホストのみです。

(注)　ホスト プロファイル データ ブロックは、どのシステム バージョンでメッセージを作成したかによって異なります。ホスト プロファイル データ ブロックのレガシー バージョンについては、レガシー ホスト データ構造（B-268 ページ）を参照してください。



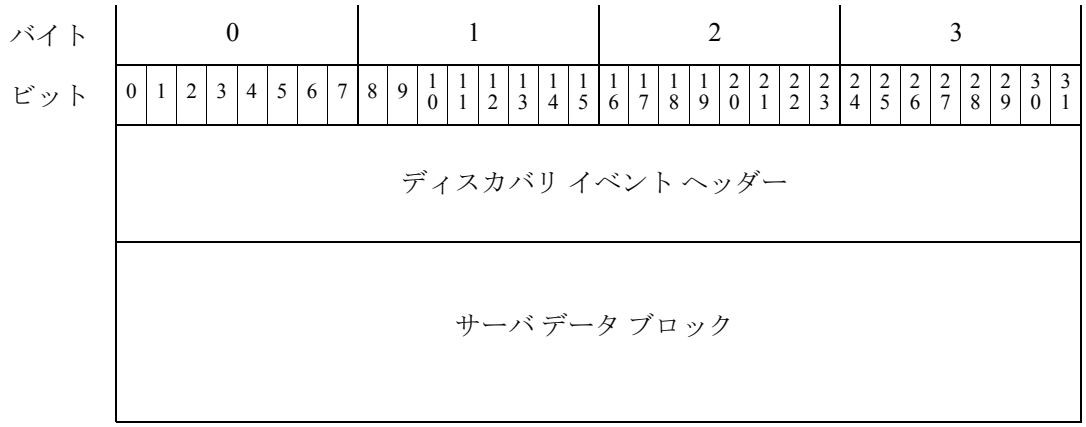
サーバ メッセージ

次の TCP サーバ イベント メッセージと UDP サーバ イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）参照）があり、サーバ データ ブロック（ホスト サーバ データ ブロック 4.10.0+（4-143 ページ）参照、シリーズ 1 のブロック タイプ 103）がそれに続きます。

- 新規 TCP サーバ
- 新規 UDP サーバ
- TCP サーバ情報更新
- UDP サーバ情報更新
- TCP サーバ信頼度更新
- UDP サーバ信頼度更新

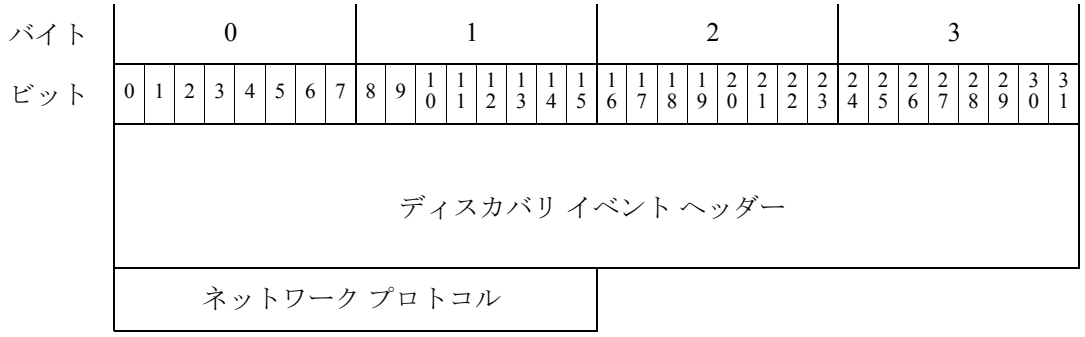
(注)　サーバ データ ブロックは、どのシステム バージョンでメッセージを作成したかによって異なります。サーバ データ ブロックのレガシー バージョンについては、レガシー データ構造の概要（B-1 ページ）を参照してください。

これらのイベントは、それぞれ次の形式を使用します:



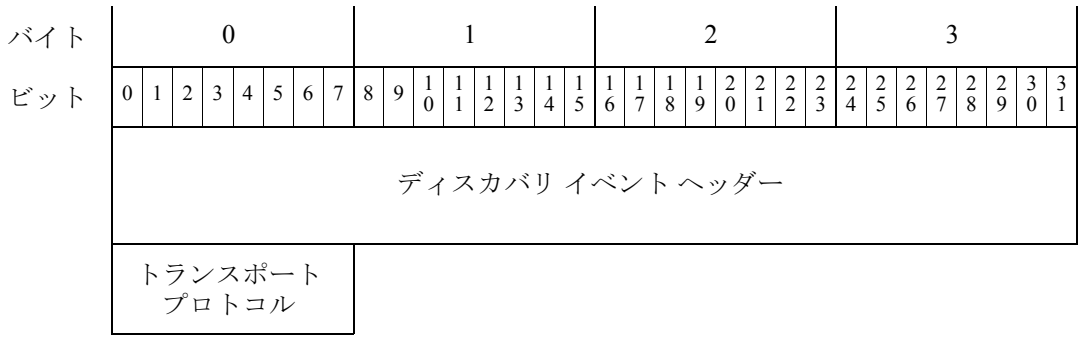
新規ネットワーク プロトコル メッセージ

新しいネットワーキング プロトコル イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ） を参照）があり、ネットワーク プロトコルの 2 バイト フィールド（次の表のプロトコル値を使用）が続きます。



新規トランスポート プロトコル メッセージ

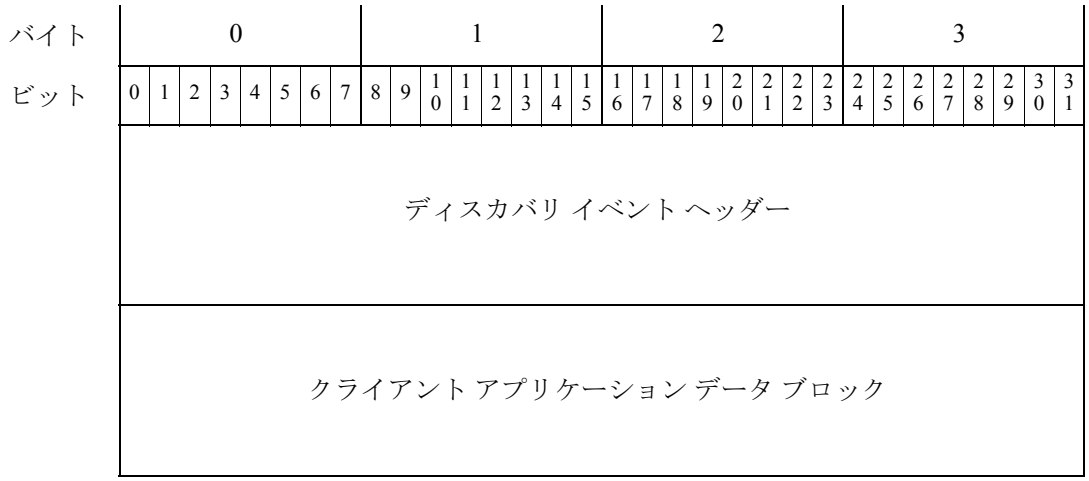
新規トランスポート プロトコルのイベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ） を参照。シリーズ 1 のブロック タイプ 4）と、トランスポート プロトコル番号の 1 バイト フィールド（次の表の値を使用）があります。



クライアント アプリケーション メッセージ

新規クライアント アプリケーション、クライアント アプリケーション アップデート、クライアント アプリケーション タイムアウト イベントは同じ形式であり、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）と、続けてクライアント アプリケーション データ ブロック（5.0+ のホスト クライアント アプリケーション データ ブロック（4-161 ページ）を参照。シリーズ 1 のブロック タイプ 122）があります。ディスカバリ イベント ヘッダーにあるレコード タイプ、イベント タイプ、イベント サブタイプは、送信されるイベントによって異なります。

（注）　クライアント アプリケーション データ ブロックは、メッセージを作成したシステム バージョンによって異なります。クライアント アプリケーション データ ブロックのレガシー バージョンについては、レガシー データ構造の概要（B-1 ページ）を参照してください。

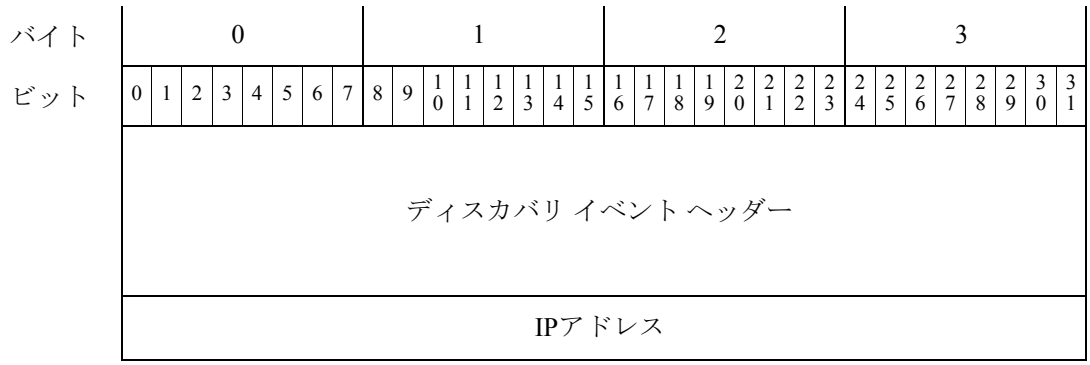


IP アドレス変更メッセージ

次のホスト ディスカバリ メッセージには、標準イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）と、2 種類の形式/構造（IP アドレスの 4 バイトと IP アドレスの 16バイト）があります。

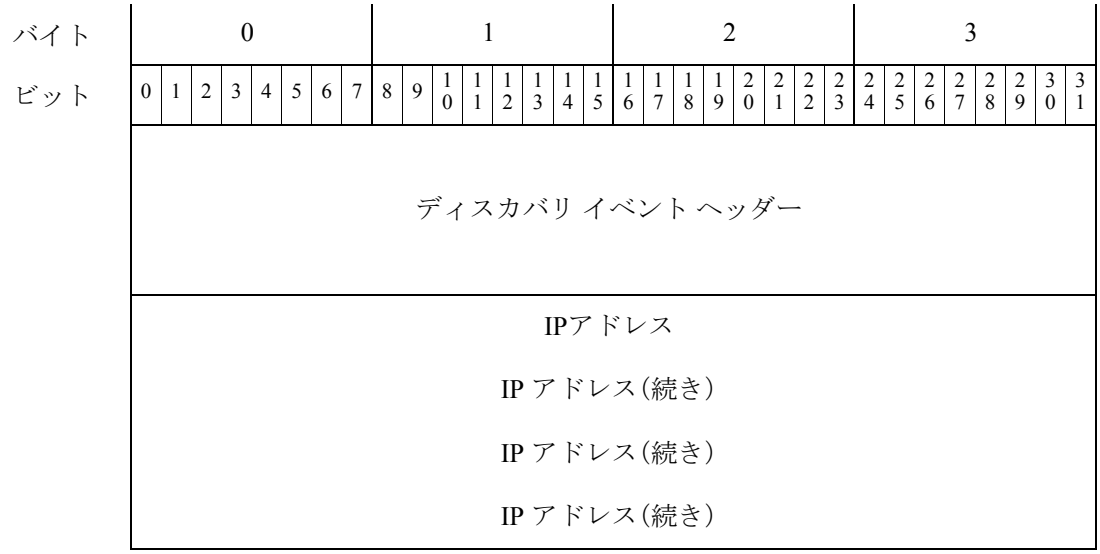
次の場合は、IP アドレスに（IP アドレス オクテット）4 バイトを使用します。

- 新規 IPv4 対 IPv4 トラフィック
- 無応答（RNA）イベント バージョンが 10 未満のとき、ホスト IP アドレスを変更



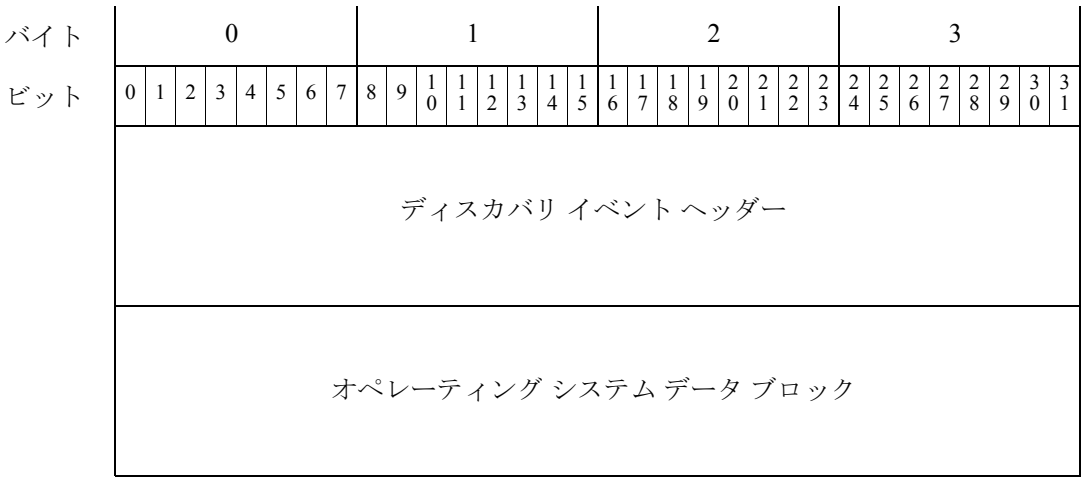
次の場合は、IP アドレスに（IP アドレス オクテット）16 バイトを使用します。

- IPv6 トラフィックに新しい IPv6
- 無応答（RNA）イベント バージョンが 10 のとき、ホスト IP アドレスを変更



オペレーティング システム更新メッセージ

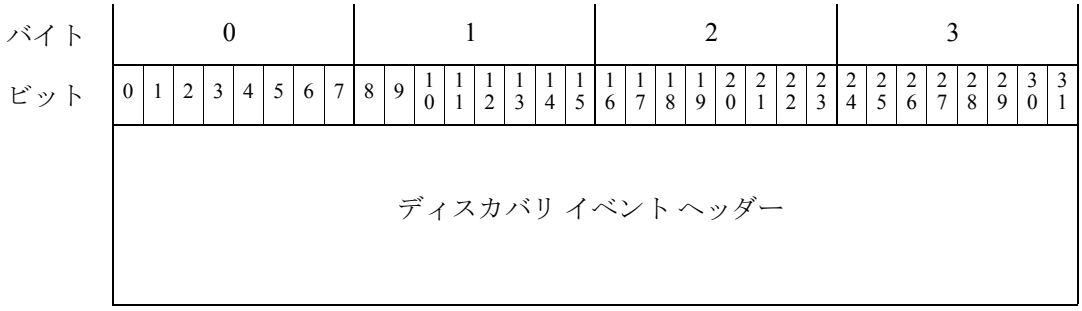
OS 情報更新イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ） を参照）があり、オペレーティング システム データ ブロック（オペレーティング システム データ ブロック 3.5+（4-88 ページ） を参照。シリーズ 1 のブロック タイプ 53）がそれに続きます。



IP アドレスを再利用とホスト タイムアウト/削除メッセージ

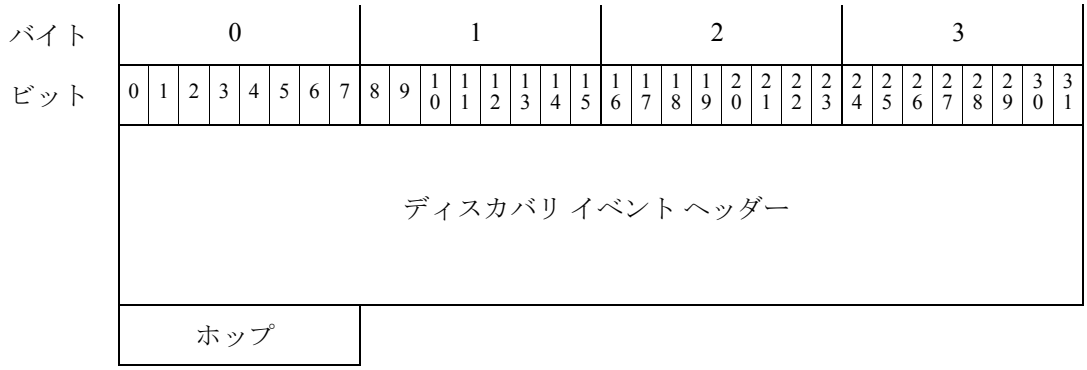
次のホスト イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）があります。他にデータはありません。

- ホスト IP アドレスを再利用
- ホスト タイムアウト
- ホストを削除。ホスト上限に到達
- ホストをドロップ。ホスト上限に到達



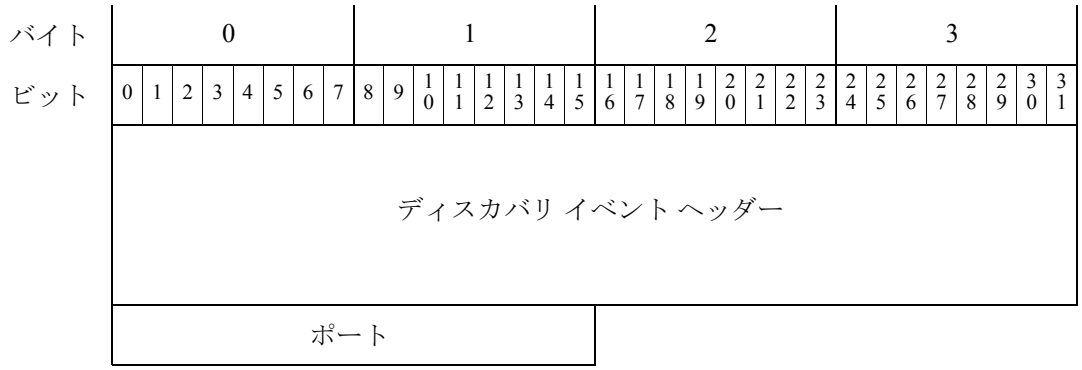
ホップ変更メッセージ

ホップ変更イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）があります。ホップ カウントの 1 バイト フィールドがそれに続きます。



TCP と UDP のポート クローズ メッセージ/タイムアウト メッセージ

TCP ポートと UDP のポート クローズ メッセージ/タイムアウト メッセージは、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）があり、ポート番号の 2 バイトがそれに続きます。

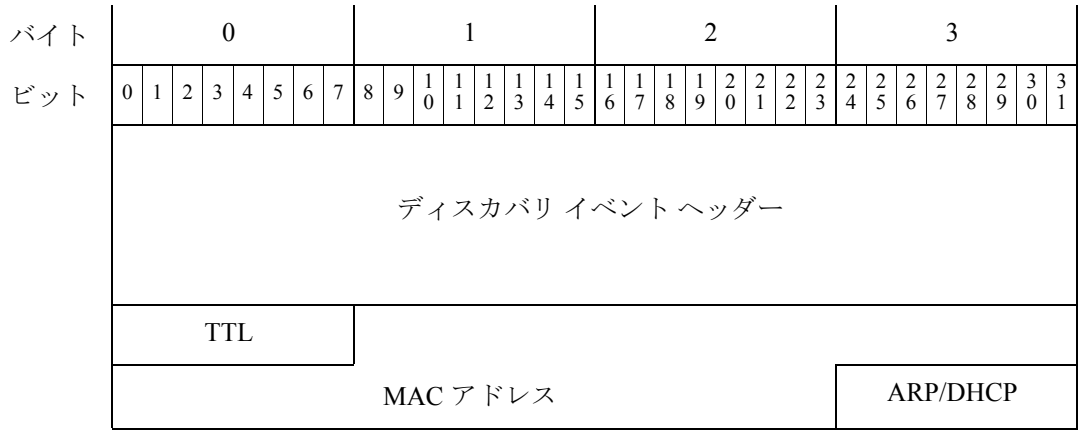


MAC アドレス メッセージ

ホストの MAC 情報変更と追加 MAC 検出メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）、TTL 値の 1 バイト、MAC アドレスの 6 バイト、ARP/DHCP トラフィックで実際の MAC アドレスとして MAC アドレスを検出したかどうかを示す 1バイトがあります。

（注）　バージョン 4.9.x を実行するシステムから MAC アドレス メッセージを受信したら、MAC アドレスのデータ ブロックの長さを確認し、それに応じて復号してください。データ ブロックの長さが 8 バイト（16 バイトとヘッダー）の場合、MAC アドレス メッセージ（4-51 ページ）を参照してください。データ ブロックの長さが 12 バイト（20 バイトとヘッダー）の場合、ホスト MAC アドレス 4.9+（4-119 ページ）を参照してください。

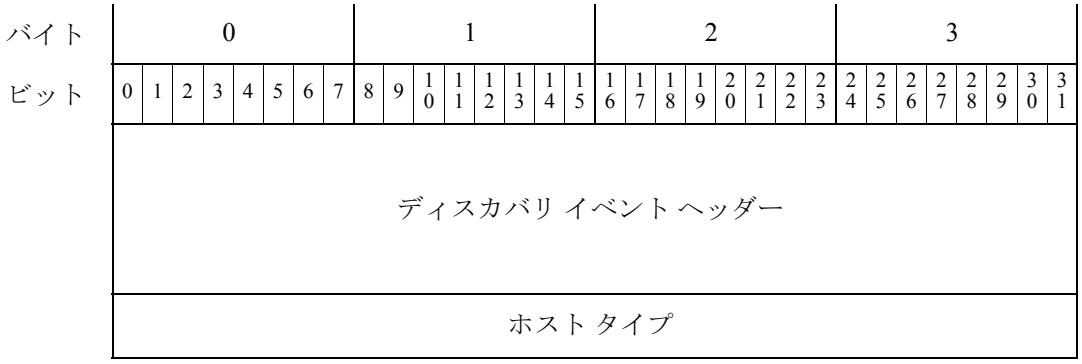
なお、MAC アドレス データ ブロック ヘッダーは、MAC 情報変更メッセージとホストに追加 MAC 検出メッセージ内では使用**しません**。



ブリッジ/ルータとして識別したホスト メッセージ

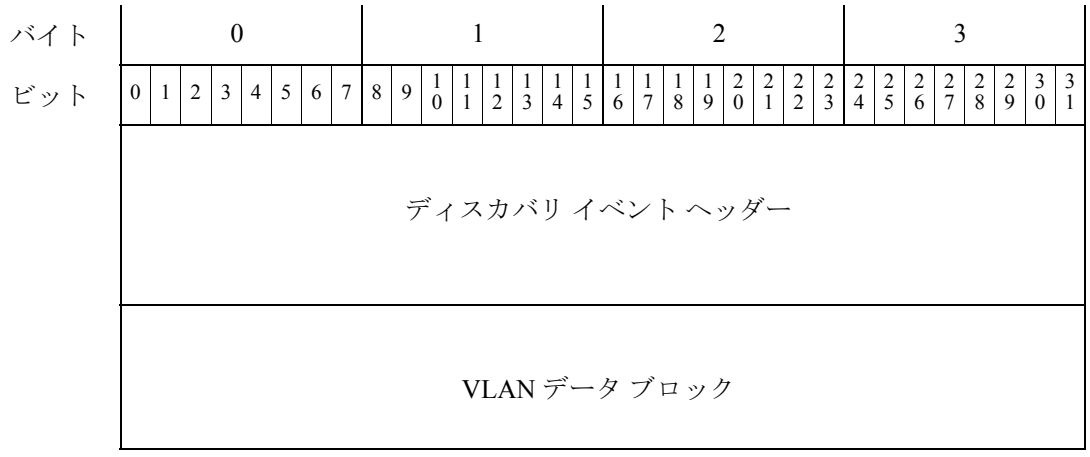
ブリッジ/ルータのイベントとして識別したホスト メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）があり、ホスト タイプと一致する値の 4 バイト フィールドが続きます。

- 0：ホスト
- 1：ルータ
- 2：ブリッジ



VLAN タグ情報更新メッセージ

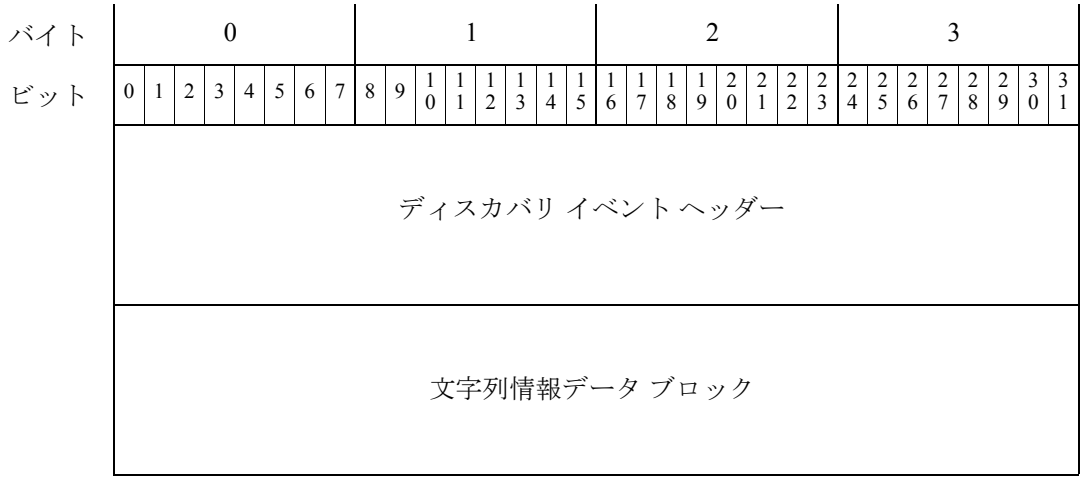
VLAN タグ情報更新イベントには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）があり、VLAN データ ブロックが続きます（VLAN データ ブロック（4-79 ページ）を参照）。VLAN データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 14 です。



NetBIOS 名変更メッセージ

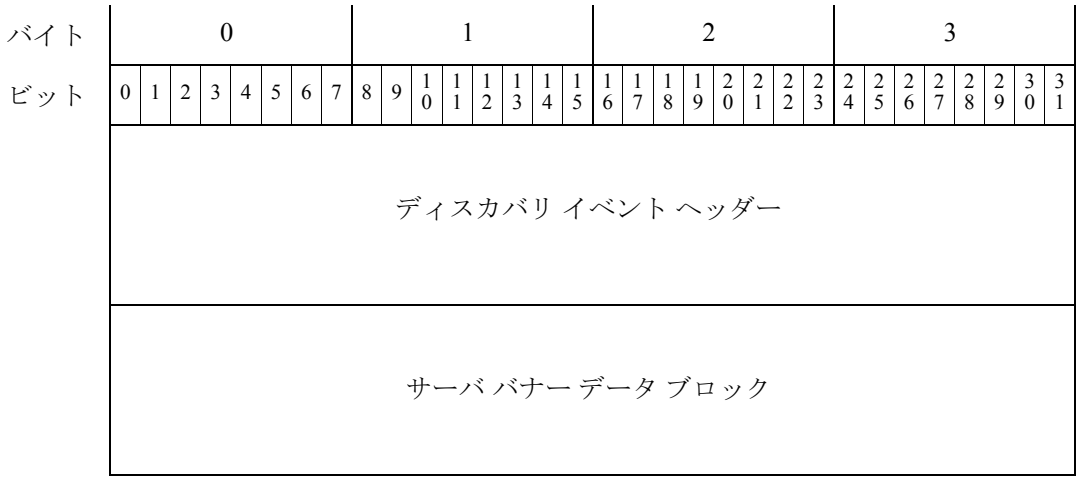
NetBIOS 名を変更イベント メッセージには、標準ディスカバリ イベント ヘッダーがあり（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）、文字列データ ブロックがそれに続きます（文字列情報データ ブロック（4-81 ページ）を参照）。文字列情報データ ブロックのブロック タイプは、シリーズ 1 のブロック タイプ 35 です。

（注）　NetBIOS ドメインを変更イベントを、Firepower システム は現在生成しません。



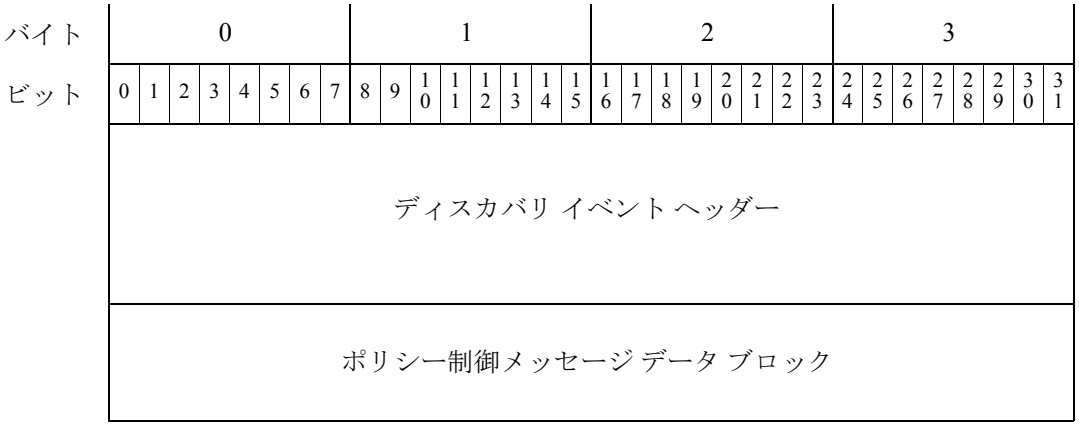
更新バナー メッセージ

更新バナー イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）があり、サーバ バナーのデータ ブロックがそれに続きます（サーバ バナー データ ブロック（4-80 ページ）を参照）。サーバ バナーのデータ ブロックのブロック タイプは、シリーズ 1 のブロック タイプ 37 です。



ポリシー制御の概要

ポリシー制御ポリシー イベントには、標準ディスカバリ イベント ヘッダーがあり（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）、ポリシー制御メッセージ データ ブロックがそれに続きます。ポリシー制御メッセージ データ ブロックの形式はシステム バージョンによって異なります。現行バージョンのポリシー制御メッセージ データ ブロック形式については、ポリシー エンジン制御メッセージ データ ブロック（4-89 ページ）を参照してください。



接続統計データ メッセージ

接続統計イベントには、標準ディスカバリ イベント ヘッダーがあり（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）、接続統計データ ブロックがそれに続きます。接続統計データ ブロックの各バージョンのドキュメントには、それを使用するシステム バージョンを格納します。バージョン 5.3.1+ の接続統計データ ブロックの形式については、次の表では、6.1+ の接続統計データ ブロックのフィールドについて説明します。（4-131 ページ）を参照してください。

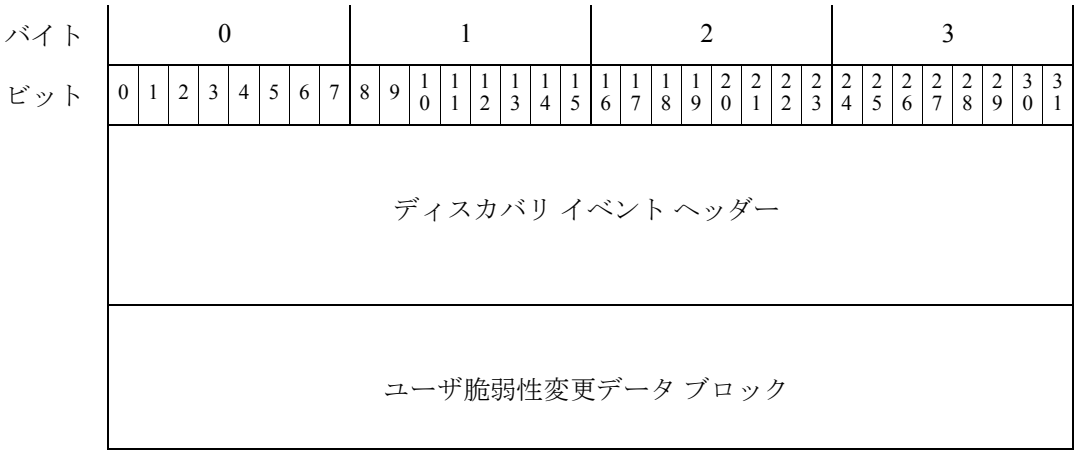
（注） 接続統計データ ブロックは、どのシステム バージョンでメッセージを作成したかによって異なります。レガシー バージョンについては、接続統計データ ブロックを参照してくださいレガシー データ構造の概要（B-1 ページ）。

接続チャンク メッセージ

接続チャンク イベントには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）があり、接続チャンク データ ブロックがそれに続きます。形式は、システム バージョンによって異なります。現行バージョンの接続チャンク データ ブロックの形式については、6.1+ の接続チャンク データ ブロック（4-103 ページ）を参照してください。接続チャンク データ ブロックのブロック タイプは、シリーズ 1 のブロック タイプ 136 です。

バージョン4.6.1+ のユーザ設定脆弱性メッセージ

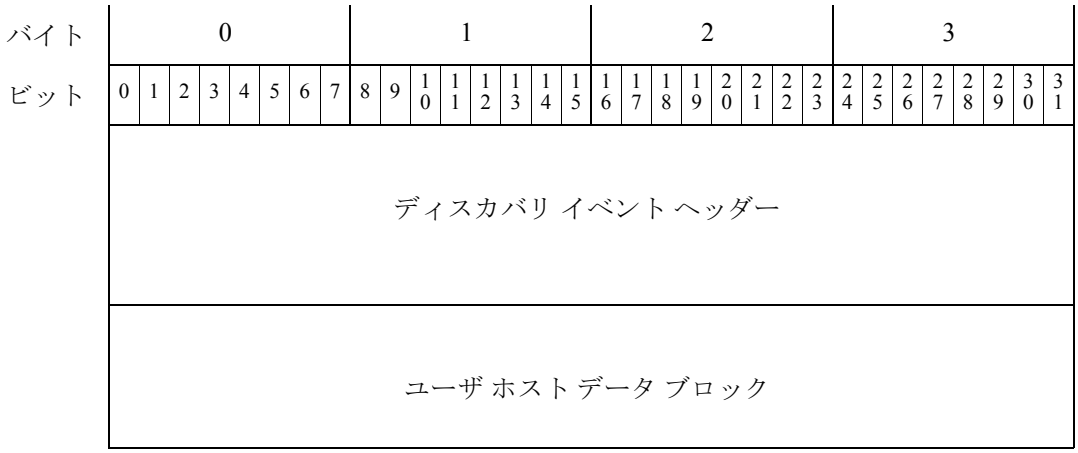
ユーザ設定の有効な脆弱性、ユーザ設定の無効な脆弱性、ユーザ脆弱性資格メッセージは、同じデータ形式を使用します。すなわち、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）にユーザ脆弱性変更データ ブロックが続きます（ユーザ脆弱性変更データ ブロック 4.7+（4-110 ページ）を参照。シリーズ 1 のブロック タイプ 80）。これらはレコード タイプ、イベント タイプ、イベント サブタイプで区別します。



ユーザ追加/削除ホスト メッセージ

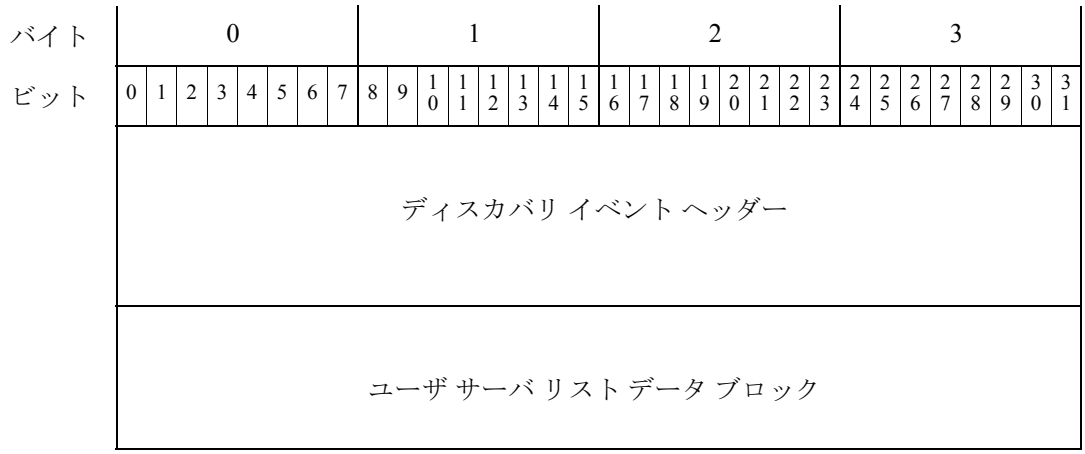
次のホスト入力イベント メッセージには、標準ディスカバリ イベント ヘッダーがあり（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）、ユーザ ホスト データ ブロックがそれに続きます（ユーザ ホスト データ ブロック 4.7+（4-108 ページ）を参照。シリーズ 1 のブロック タイプ 78）。

- ユーザ削除アドレス
- ユーザ追加ホスト



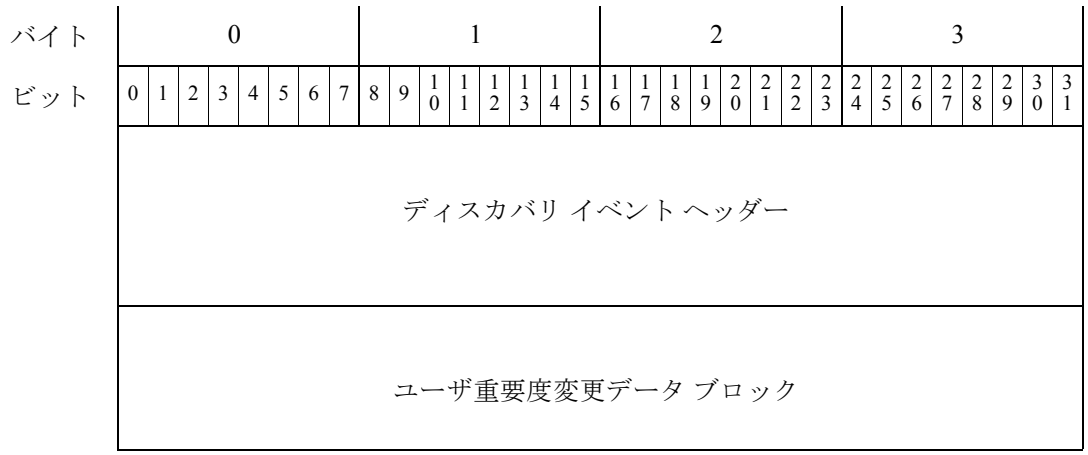
ユーザ削除サーバ メッセージ

ユーザ削除サーバ メッセージには、標準ディスカバリ イベント ヘッダーがあり（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）、ユーザ サーバ リスト データ ブロックがそれに続きます（ユーザ サーバ リスト データ ブロック（4-107 ページ）を参照）。ユーザ サーバ リスト データ ブロックはシリーズ 1 のブロック タイプ 77 です。



ユーザ設定ホスト重要度メッセージ

ユーザ設定ホスト重要度メッセージには、標準ディスカバリ イベント ヘッダーがあり（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）、ユーザ重要度変更データ ブロックがそれに続きます（ユーザ重要度変更データ ブロック 4.7+（4-111 ページ）を参照）。ユーザ重要度変更データ ブロックのブロック タイプは、シリーズ 1 ブロック タイプ 81 です。

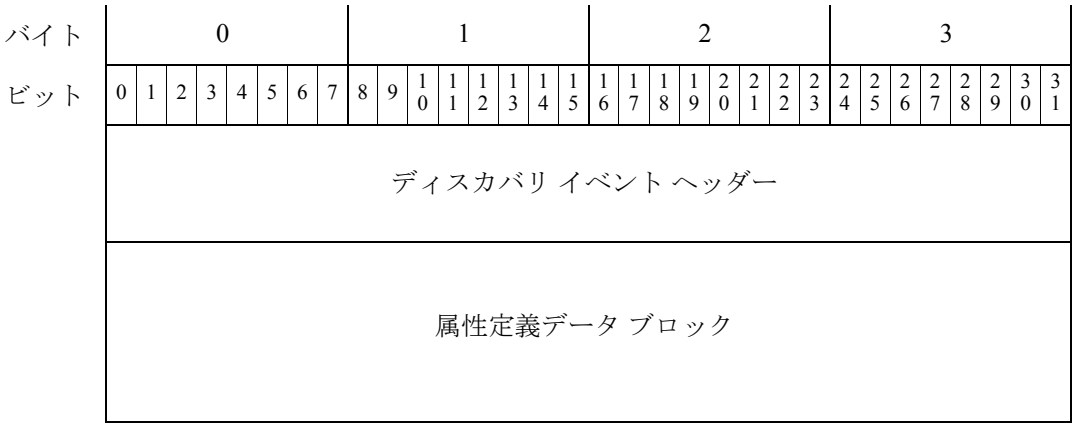


属性メッセージ

次のイベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）があり、属性定義データ ブロック（4.7+ の定義属性データ ブロック（4-90 ページ）を参照。シリーズ 1 ブロック タイプ 55）がそれに続きます。

- ホスト属性を追加
- ホスト属性を更新
- ホスト属性を削除

これらのイベントは、それぞれ次の形式を使用します:



属性値メッセージ

次のイベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ） を参照）があり、ユーザ属性値データ ブロック（ユーザ属性値データ ブロック 4.7+（4-113 ページ） を参照。シリーズ 1 ブロック タイプ 82）がそれに続きます。

- ホスト属性値を設定
- ホスト属性地を削除

これらのイベントは、それぞれ次の形式を使用します:

ユーザ サーバ メッセージとオペレーティング システム メッセージ

次のイベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ） を参照）があり、ユーザ製品データ ブロック（ユーザ製品データ ブロック 5.1+（4-177 ページ） を参照。シリーズ 1 ブロック タイプ 60）がそれに続きます。

- オペレーティング システム定義を設定
- サーバ定義を設定
- サーバの追加

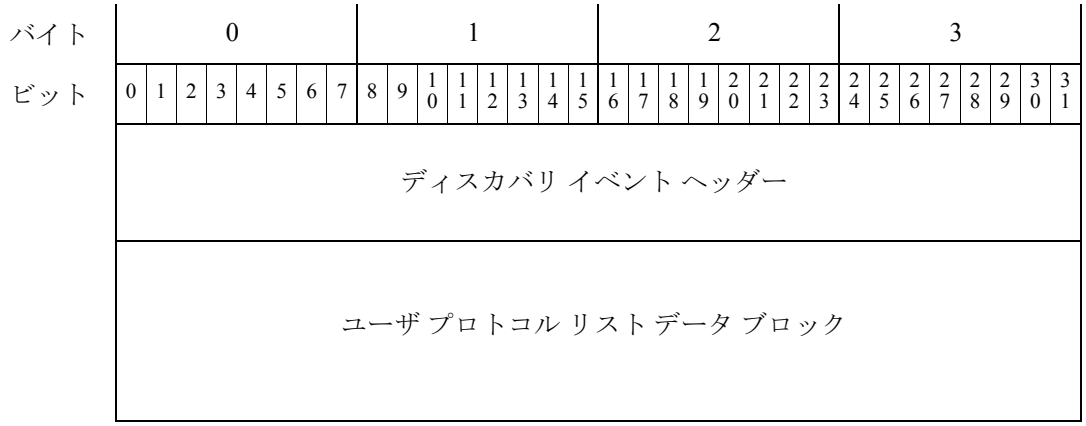
これらのイベントは、それぞれ次の形式を使用します:

ユーザ プロトコル メッセージ

次のイベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ） を参照）があり、ユーザ プロトコル リスト データ ブロック（ユーザ プロトコル リスト データ ブロック 4.7+（4-114 ページ） を参照。シリーズ 1 ブロック タイプ 83）がそれに続きます。

- プロトコルを削除
- プロトコルを追加

これらのイベントは、それぞれ次の形式を使用します:



ユーザ クライアント アプリケーション メッセージ

次のイベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ） を参照）があり、ユーザ クライアント アプリケーション リスト データ ブロック（ユーザ クライアント アプリケーション リスト データ ブロック（4-96 ページ） を参照。シリーズ 1 ブロック タイプ 60）がそれに続きます。

- クライアント アプリケーションを削除
- クライアント アプリケーションを追加

これらのイベントは、それぞれ次の形式を使用します:

スキャン結果を追加メッセージ

スキャン結果を追加イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）があり、スキャン結果データ ブロックがそれに続きます（次の表では、6.1+ の接続統計データ ブロックのフィールドについて説明します。（4-131 ページ）を参照）。スキャン結果データ ブロックのブロック タイプは、シリーズ 1 ブロック タイプ 142 です。

このイベントでは、次の形式を使用します。

新規オペレーティング システム メッセージ

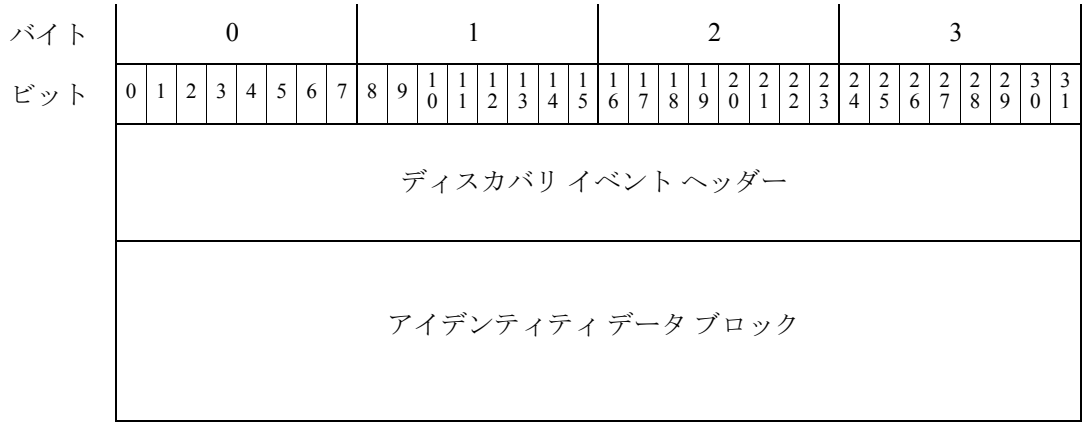
新規 OS イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ）を参照）があり、オペレーティング システム フィンガープリント データ ブロックがそれに続きます（オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照）。

このイベントでは、次の形式を使用します。

アイデンティティ競合とアイデンティティ タイムアウト システム メッセージ

アイデンティティ競合イベント メッセージとアイデンティティ タイムアウト イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ） を参照）があり、アイデンティティ データ ブロックがそれに続きます（アイデンティティ データ ブロック（4-117 ページ） を参照）。アイデンティティ データ ブロックのブロック タイプは、シリーズ 1 ブロック タイプ 94 です。これらのメッセージは、フィンガープリント送信元アイデンティティで競合またはタイムアウトが発生すると生成されます。

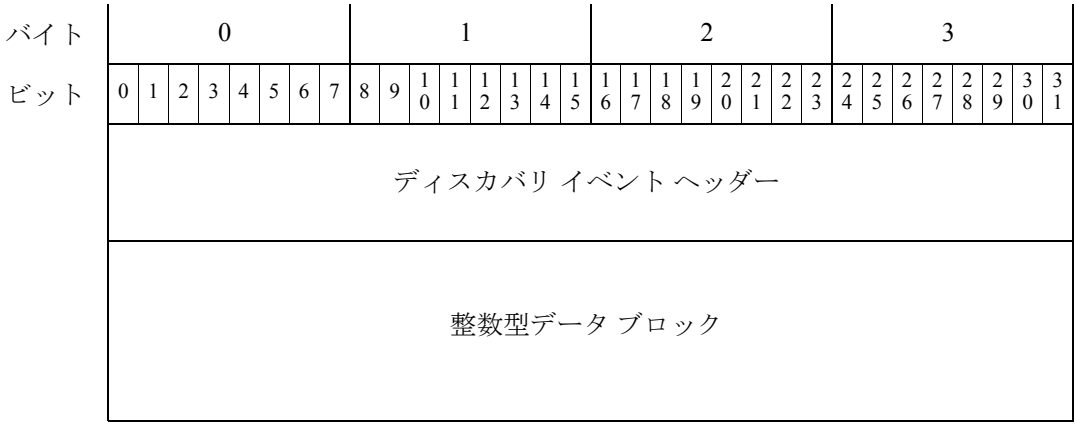
このイベントでは、次の形式を使用します。



ホスト IOC セット メッセージ

ホスト IOC セット メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-40 ページ） を参照）があり、整数型データ ブロックがそれに続きます（整数型（INT32）データ ブロック（4-79 ページ） を参照）。この整数型データ ブロックには、ホストの IOC セットの ID 番号を格納します。

このイベントでは、次の形式を使用します。



イベント タイプ別ユーザ データ構造

eStreamer は、ディスカバリ イベント ヘッダーで指定されたイベント タイプに基づいてユーザ イベント メッセージを構築します。次の項では、各イベント タイプの概略構造を紹介します。

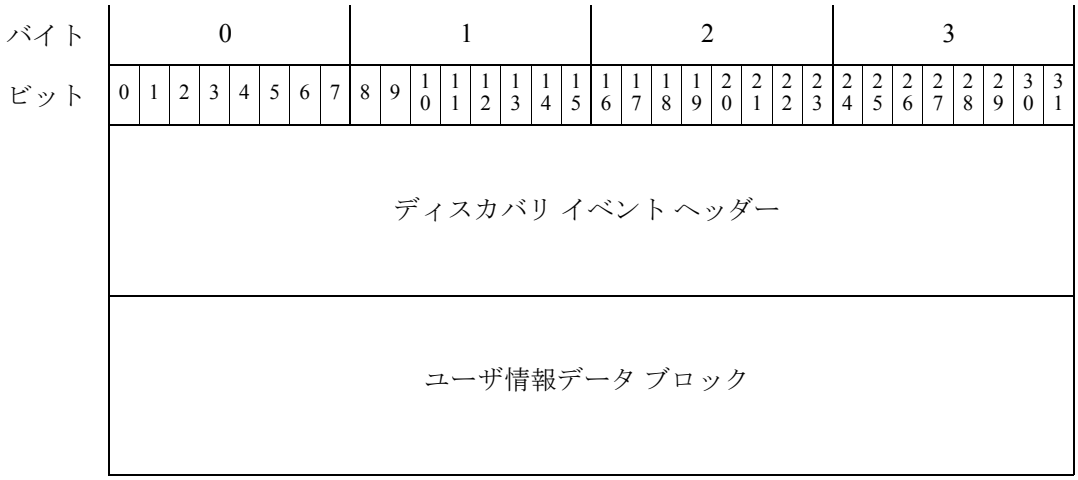
- ユーザ変更メッセージ (4-62 ページ)
- ユーザ情報更新メッセージ ブロック (4-62 ページ)

ユーザ変更メッセージ

次のイベントのどれかがシステム検出で発生すると、ユーザ変更メッセージが送信されます:

- 新規ユーザを検出しました (新規ユーザ アイデンティティ イベント — イベント タイプ 1004、サブタイプ 1)
- ユーザが削除されます (ユーザ アイデンティティを削除イベント — イベント タイプ 1004、サブタイプ3)
- ユーザがドロップされます (ユーザ アイデンティティをドロップ。ユーザ上限に到達イベント — イベント タイプ 1004、サブタイプ 4)

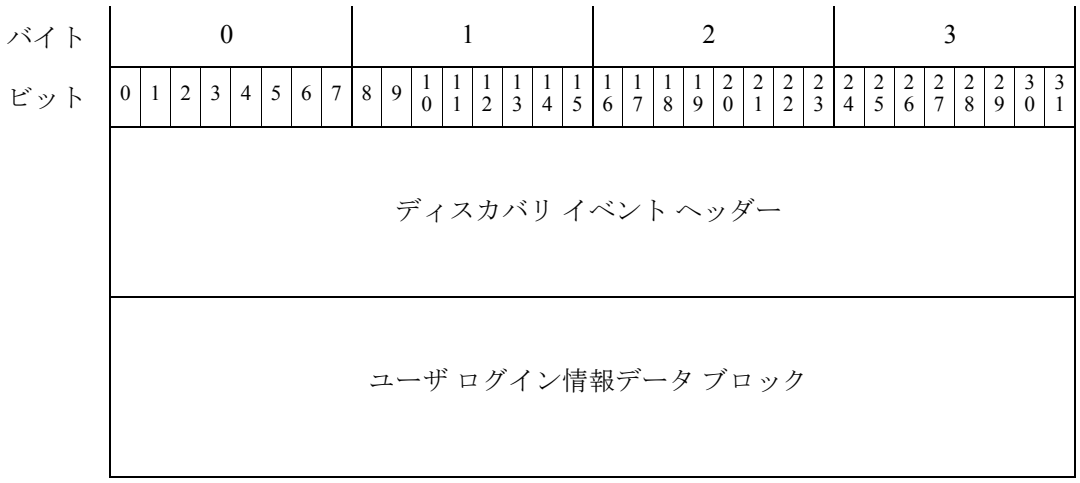
ユーザ変更イベント メッセージには、標準ディスカバリ イベント ヘッダー (ディスカバリ イベント ヘッダー 5.2+ (4-40 ページ) を参照) があり、ユーザ情報データ ブロックがそれに続きます (6.0+ の情報データ ユーザ ブロック (4-195 ページ) を参照)。ユーザ情報データ ブロックはシリーズ 1 ブロック タイプ 120 です。



ユーザ情報更新メッセージ ブロック

システムがユーザのログインの変更 (ユーザ ログイン イベント — イベント タイプ 1004、サブタイプ2) を検出すると、ユーザ情報更新メッセージが送信されます。

ユーザ情報更新イベント メッセージには標準ディスカバリ イベント ヘッダー (ディスカバリ イベント ヘッダー 5.2+ (4-40 ページ) を参照) とユーザ ログイン情報データ ブロックがあります (ユーザ ログイン情報データ ブロック 6.1+ (4-198 ページ) を参照)。ユーザ ログイン情報データ ブロックのブロック タイプは、シリーズ 1 ブロック タイプ 121 です。

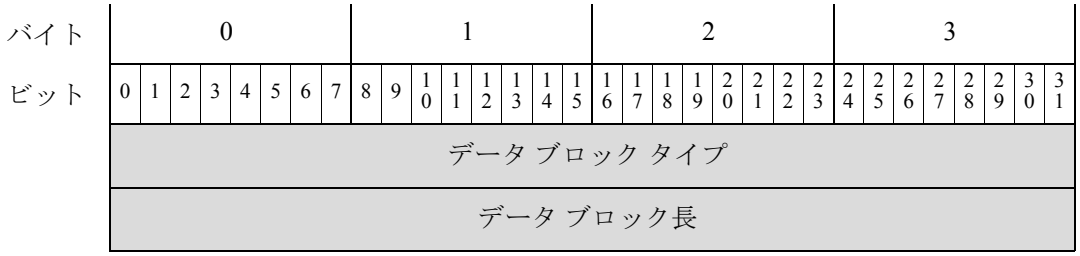


ディスカバリ（シリーズ1）ブロック

ほとんどのディスカバリ イベントと接続イベントには、シリーズ 1 グループ データ構造の 1 つ以上のデータ ブロックがあります。シリーズ 1 データ ブロック タイプは、それぞれ特定の情報タイプを伝えます。ブロック タイプ番号は、ブロックのデータにするデータに先行するデータ ブロック ヘッダーにあります。ブロック ヘッダー形式については、データ ブロック ヘッダー（2-27 ページ）を参照してください。

シリーズ 1 データ ブロック ヘッダー シリーズ

シリーズ 1 のデータ ブロック ヘッダーには、シリーズ 2 ブロック ヘッダーと同じく、ブロックのタイプ番号とブロック長を含む 2 つの 32 ビット整数フィールドがあります。



(注)　データ ブロック長フィールドには、2 つのデータ ブロック ヘッダー フィールドの 8 バイトを含むすべてのデータ ブロックでバイト数を格納します。

一部 ブロック シリーズ 1 タイプでは、ブロック ヘッダーの直後に生データが続きます。より複雑なブロック タイプでは、ヘッダーの後には標準固定長フィールドか、別のシリーズ 1 データ ブロックやブロック リストをカプセル化したシリーズ 1 プリミティブ ブロックが続きます。

シリーズ 1プリミティブ データ ブロック

シリーズ 1 とシリーズ 2 のいずれのブロックにも、1 セットのプリミティブがあり、これで可変長ブロック リストと、さらに可変長の文字列と BLOB をメッセージ内にカプセル化します。これらのプリミティブ ブロックには、前述の標準シリーズ 1 のブロック ヘッダーがあります。これらのプリミティブを使用するのは、他のシリーズ 1 データ ブロックのみです。所定のブロック タイプに任意の数値を含めることができます。プリミティブ ブロックの構造の詳細については、次の項を参照してください:

- 文字列データ ブロック (4-73 ページ)
- BLOB データ ブロック (4-74 ページ)
- リスト データ ブロック (4-75 ページ)
- 汎用リスト ブロック (4-75 ページ)

ホスト ディスカバリ データ ブロックと接続データ ブロック

ホスト ディスカバリ イベントと接続イベント ブロック タイプのリストについては、表 4-30 (4-64 ページ) を参照してください。ユーザ イベント ブロック タイプについては、表 4-85 (4-185 ページ) を参照してください。これらはすべてシリーズ 1 データ ブロックです。

次の表のエントリには、それぞれデータ ブロックを定義したサブセクションまでのリンクがあります。ブロック タイプごとに、ステータス (現在またはレガシー) が表示されます。現在のデータ ブロックが最新バージョンです。レガシー データ ブロックは、製品の旧バージョンに使用するデータ ブロックであり、eStreamer でメッセージ形式は引き続き要求できます。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ

タイプ	目次	データ ブロック ステータス	説明
0	文字列	現在 (Current)	文字列データを格納します。詳細については、文字列データ ブロック (4-73 ページ) を参照してください。
1	サブサーバ	現在 (Current)	サーバで検出したサブサーバに関する情報を格納します。詳細については、サブサーバ データ ブロック (4-76 ページ) を参照してください。
4	プロトコル	現在 (Current)	プロトコル データを格納します。詳細については、プロトコル データ ブロック (4-78 ページ) を参照してください。
7	整数型データ	現在 (Current)	整数型 (数値) データを格納します。詳細については、整数型 (INT32) データ ブロック (4-79 ページ) を参照してください。
10	BLOB	現在 (Current)	バイナリ データの生ブロックを格納し、主にバナーに使用します。詳細については、BLOB データ ブロック (4-74 ページ) を参照してください。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ(続き)

タイプ	目次	データ ブロック ステータス	説明
11	リスト	現在(Current)	その他のデータ ブロック リストを含みます。詳細については、リスト データ ブロック (4-75 ページ) を参照してください。
14	VLAN	現在(Current)	VLAN 情報を格納します。詳細については、VLAN データ ブロック (4-79 ページ) を参照してください。
20	侵入の影響アラート	現在(Current)	侵入影響アラート情報を格納します。侵入影響イベントアラートのヘッダーは、他のデータ ブロックは若干異なります。詳細については、侵入の影響アラート データ 5.3 以上 (3-18 ページ) を参照してください。
31	汎用リスト	現在(Current)	たとえば、クライアント アプリケーション ブロックなど、カプセル化する汎用リスト情報をブロック リストをホスト プロファイル ブロックに格納します。詳細については、汎用リスト ブロック (4-75 ページ) を参照してください。
35	文字列情報	現在(Current)	文字列情報を格納します。たとえば、スキャン脆弱性データ ブロックで使用すると、文字列情報データ ブロックには CVE ID 番号データが格納されます。文字列情報データ ブロック (4-81 ページ) を参照してください。
37	サーバ バナー	現在(Current)	サーバ バナー データを格納します。詳細については、サーバ バナー データ ブロック (4-80 ページ) を参照してください。
38	属性アドレス	レガシー	ホスト属性アドレスを格納します(本製品の旧バージョンを参照のこと)。サクセサ ブロックは 146 です。
39	属性リスト項目	現在(Current)	ホスト属性リスト項目値を格納します。詳細については、属性リスト項目データ ブロック (4-83 ページ) を参照してください。
42	ホスト クライアント アプリケーション	レガシー	新規クライアント アプリケーション イベントのクライアント アプリケーション情報を格納します(本製品の旧バージョンを参照のこと)。
47	フル ホスト プロファイル	レガシー	ホスト プロファイル情報一式を格納します(本製品の旧バージョンを参照のこと)。
48	属性値	現在(Current)	ホスト属性の ID 番号と値を格納します。詳細については、属性値データ ブロック (4-84 ページ) を参照してください。
51	フル サブサーバ	現在(Current)	サーバで検出したサブサーバに関する情報を格納します。フル サーバ情報ブロックとフル ホスト プロファイルで参照します。各サブサーバの脆弱性情報を格納します。詳細については、フル サブサーバ データ ブロック (4-85 ページ) を参照してください。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ(続き)

タイプ	目次	データ ブロック ステータス	説明
53	オペレーティング システム（Operating System）	現在（Current）	バージョン 3.5+ のオペレーティング システム情報を格納します。詳細については、オペレーティング システム データ ブロック 3.5+（4-88 ページ）を参照してください。
54	ポリシー エンジン制御メッセージ	現在（Current）	ユーザ ポリシー制御の変更に関する情報を格納します。詳細については、ポリシー エンジン制御メッセージ データ ブロック（4-89 ページ）を参照してください。
55	属性定義	現在（Current）	属性定義の情報を格納します。詳細については、4.7+ の定義属性データ ブロック（4-90 ページ）を参照してください。
56	接続統計情報	レガシー	4.7 ～ 4.9.0 の接続統計イベントの情報を格納します（本製品の旧バージョンを参照のこと）。
57	ユーザ プロトコル	現在（Current）	ユーザ入力のプロトコル情報を格納します。詳細については、ユーザ プロトコル データ ブロック（4-93 ページ）を参照してください。
	ユーザ クライアント アプリケーション	レガシー	ユーザ入力のクライアント アプリケーション データを格納します。詳細については、ユーザ クライアント アプリケーション データ ブロック 5.0 ～ 5.1（B-96 ページ）を参照してください。ブロック 138 に置き換わります。
60	ユーザ クライアント アプリケーション リスト	現在（Current）	ユーザ クライアント アプリケーション データ ブロックのリストを格納します。詳細については、ユーザ クライアント アプリケーション リスト データ ブロック（4-96 ページ）を参照してください。
61	IP 範囲指定	レガシー	IP アドレス範囲指定を格納します。詳細については、IP 範囲仕様データ ブロック 5.0 ～ 5.1.1.x（B-310 ページ）を参照してください。ブロック 141 に置き換わります。
	属性指定	現在（Current）	属性名と値を格納します。詳細については、属性指定データ ブロック（4-99 ページ）を参照してください。
63	MAC アドレス指定	現在（Current）	MAC アドレス範囲指定を格納します。詳細については、MAC アドレス指定データ ブロック（4-101 ページ）を参照してください。
64	IP アドレス指定	現在（Current）	IP と MAC アドレス指定ブロック リストを格納します。詳細については、アドレス指定データ ブロック（4-102 ページ）を参照してください。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ(続き)

タイプ	目次	データ ブロック ステータス	説明
65	ユーザ製品	レガシー	サードパーティ アプリケーション文字列マッピングなど、サードパーティ アプリケーションからインポートしたホスト入力データを格納します。詳細については、ユーザ製品データ ブロック 5.0.x (B-101 ページ) を参照してください。5.0 で導入したサクセサ ブロック タイプ 118 には、ブロック タイプ 65 と同じ構成があります。
66	接続チャンク	レガシー	接続チャンク情報を格納します。詳細については、接続チャンク データ ブロック 5.0 ～ 5.1 (B-146 ページ) を参照してください。5.0 で導入したサクセサ ブロック タイプ 119 には、ブロック タイプ 66 と同じ構成があります。
67	フィックス リスト	現在(Current)	ホストに適用するフィックスを格納します。詳細については、フィックス リスト データ ブロック (4-105 ページ) を参照してください。
71	汎用スキャン結果	レガシー	Nmap スキャンの結果を格納します(本製品の旧バージョンを参照のこと)。
72	スキャン結果	レガシー	サードパーティ スキャンの結果を格納します(本製品の旧バージョンを参照のこと)。
76	ユーザ サーバ	現在(Current)	ユーザ入力イベントのサーバ情報を格納します。詳細については、ユーザ サーバ データ ブロック (4-106 ページ) を参照してください。
77	ユーザ サーバ リスト	現在(Current)	ユーザ サーバ ブロックのリストを格納します。詳細については、ユーザ サーバ リスト データ ブロック (4-107 ページ) を参照してください。
78	ユーザ ホスト	現在(Current)	ユーザ ホスト入力イベントからのホスト範囲に関する情報を格納します。詳細については、ユーザ ホスト データ ブロック 4.7+ (4-108 ページ) を参照してください。
79	ユーザ脆弱性	レガシー	ホスト脆弱性に関する情報を格納します(本製品の旧バージョンを参照のこと)。バージョン 5.0 で導入したサクセサ ブロックのブロック タイプは 124 です。
80	ユーザ ホスト脆弱性の変更	現在(Current)	非アクティブ化した脆弱性のリスト、またはアクティブ化した脆弱性のリストを格納します。詳細については、ユーザ脆弱性変更データ ブロック 4.7+ (4-110 ページ) を参照してください。
81	ユーザ重要度	現在(Current)	ホストまたはホストの重要度の変更に関する情報を格納します。詳細については、ユーザ重要度変更データ ブロック 4.7+ (4-111 ページ) を参照してください。
82	ユーザ属性値	現在(Current)	ホストの属性値の変更を格納します。詳細については、ユーザ属性値データ ブロック 4.7+ (4-113 ページ) を参照してください。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ(続き)

タイプ	目次	データ ブロック ステータス	説明
83	ユーザ プロトコル リスト	現在(Current)	ホストのプロトコル リストを示します。詳細については、ユーザ プロトコル リスト データ ブロック 4.7+(4-114 ページ)を参照してください。
85	脆弱性リスト	現在(Current)	ホストに適用する脆弱性を格納します。詳細については、ホスト脆弱性データ ブロック 4.9.0+(4-116 ページ)を参照してください。
86	スキャン脆弱性	レガシー	スキャンで検出した脆弱性に関する情報を格納します(本製品の旧バージョンを参照のこと)。
87	オペレーティング システム フィンガープリント	レガシー	オペレーティング システム フィンガープリントのリストを格納します。詳細については、オペレーティング システム フィンガープリント データ ブロック 5.0 ～ 5.0.2(B-126 ページ)を参照してください。バージョン 5.1 で導入したサクセサ ブロックのブロック タイプは 130 です。
88	サーバ情報	レガシー	サーバ フィンガープリントで使用するサーバ情報を格納します(本製品の旧バージョンを参照のこと)。
89	ホスト/サーバ	レガシー	ホスト サーバ情報を格納します(本製品の旧バージョンを参照のこと)。
90	フル ホスト サーバ	レガシー	ホスト サーバ情報を格納します(本製品の旧バージョンを参照のこと)。
91	ホスト プロファイル	レガシー	ホストのプロファイル情報を格納します。詳細については、ホスト プロファイル データブロック 5.2+(4-169 ページ)を参照してください。バージョン 5.1 で導入したサクセサ ブロックのブロック タイプは 132 です。
92	フル ホスト プロファイル	レガシー	ホスト プロファイル情報一式を格納します(本製品の旧バージョンを参照のこと)。データ ブロック 47 に置き換わります。
94	アイデンティティ データ	現在(Current)	ホストのアイデンティティ データを格納します。詳細については、アイデンティティ データ ブロック(4-117 ページ)を参照してください。
95	ホスト MAC アドレス	現在(Current)	ホストの MAC アドレス情報を格納します。詳細については、ホスト MAC アドレス 4.9+(4-119 ページ)を参照してください。
96	セカンダリ ホスト更新	現在(Current)	セカンダリ セカンダリ ホストの更新(4-120 ページ) で報告された MAC アドレス情報のリストを格納します。
97	Web アプリケーション(Web Application)	レガシー	Web アプリケーション データのリストを格納します(本製品の旧バージョンを参照のこと)。バージョン 5.0 で導入したサクセサ ブロックのブロック タイプは 123 です。
98	ホスト/サーバ	レガシー	ホスト サーバ情報を格納します(本製品の旧バージョンを参照のこと)。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ(続き)

タイプ	目次	データ ブロック ステータス	説明
99	フル ホスト サーバ	レガシー	ホスト サーバ情報を格納します(本製品の旧バージョンを参照のこと)。
100	ホスト クライアント アプリケーション	レガシー	新規クライアント アプリケーション イベントのクライアント アプリケーション情報を格納します(本製品の旧バージョンを参照のこと)。バージョン 5.0 で導入したサクセサ ブロック タイプ 122 には、ブロック タイプ 100 と同じ構造があります。
101	接続統計情報	レガシー	4.9.1+ の接続統計イベントの情報を格納します(本製品の旧バージョンを参照のこと)。
102	スキャン結果	レガシー	脆弱性に関する情報を格納しており、スキャン結果を追加イベントで使用します。スキャン結果データ ブロック 5.0 ～ 5.1.1.x(B-98 ページ)を参照してください。
103	ホスト/サーバ	現在(Current)	ホスト サーバ情報を格納します。詳細については、ホスト サーバ データ ブロック 4.10.0+(4-143 ページ)を参照してください。
104	フル ホスト サーバ	現在(Current)	ホスト サーバ情報を格納します。詳細については、フル ホスト サーバ データ ブロック 4.10.0+(4-145 ページ)を参照してください。
105	サーバ情報	レガシー	サーバ フィンガープリントで使用するサーバ情報を格納します。詳細については、4.10.x、5.0 ～ 5.0.2 のサーバ情報データ ブロック(4-149 ページ)を参照してください。5.0 で導入したサクセサ ブロック タイプ 117 には、ブロック タイプ 105 と同じ構成があります。
106	フル サーバ情報	現在(Current)	ホストで検出したサーバに関する情報を格納します。詳細については、フル サーバ情報データ ブロック(4-151 ページ)を参照してください。
108	汎用スキャン結果	現在(Current)	Nmap スキャンで得た結果を格納します。詳細については、4.10.0+ の汎用スキャン結果データ ブロック(4-154 ページ)を参照してください。
109	スキャン脆弱性	現在(Current)	サードパーティ スキャンで検出した脆弱性に関する情報を格納します。4.10.0+のスキャン脆弱性データ ブロック(4-156 ページ)を参照してください。
111	フル ホスト プロファイル	レガシー	ホスト プロファイル情報一式を格納します。詳細については、フル ホスト プロファイル データ ブロック 5.0 ～ 5.0.2(B-269 ページ)を参照してください。データ ブロック 92 に置き換わります。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ(続き)

タイプ	目次	データ ブロック ステータス	説明
112	フル ホスト クライアント アプリケーション	現在(Current)	脆弱性リストとともに新規クライアント アプリケーション イベントのクライアント アプリケーション情報を格納します。詳細については、フル クライアント アプリケーション データ ブロック 5.0+(4-159 ページ)を参照してください。
115	接続統計情報	レガシー	5.0 ～ 5.0.2 の接続統計イベントの情報を格納します。詳細については、接続統計データ ブロック 5.0 ～ 5.0.2(B-128 ページ)を参照してください。バージョン 5.1 で導入したサクセサ ブロックのブロック タイプは 126 です。
117	サーバ情報	現在(Current)	サーバ フィンガープリントで使用するサーバ情報を格納します。詳細については、4.10.x、5.0 ～ 5.0.2 のサーバ情報データ ブロック(4-149 ページ)を参照してください。
118	ユーザ製品	レガシー	サードパーティ アプリケーション文字列マッピングなど、サードパーティ アプリケーションからインポートしたホスト入力データを格納します。詳細については、ユーザ製品データ ブロック 5.0.x(B-101 ページ)を参照してください。先行ブロック タイプ 65 は 5.0 で更新され、このブロック タイプと同じ構造があります。バージョン 5.1 で導入したサクセサ ブロックのブロック タイプは 132 です。
119	接続チャンク	レガシー	バージョン 4.10.1 ～ 5.1 の接続チャンク情報を格納します。詳細については、接続チャンク データ ブロック 5.0 ～ 5.1(B-146 ページ)を参照してください。サクセサ ブロックは 136 です。
122	ホスト クライアント アプリケーション	現在(Current)	バージョン 5.0 + の新規クライアント アプリケーション イベントのクライアント アプリケーション情報を格納します。詳細については、5.0+ のホスト クライアント アプリケーション データ ブロック(4-161 ページ)を参照してください。これはブロック タイプ 100 に置き換わります。
123	Web アプリケーション(Web Application)	現在(Current)	バージョン 5.0 +の Web アプリケーション データを格納します。詳細については、5.0+の Web アプリケーション データ ブロック(4-121 ページ)を参照してください。これはブロック タイプ 97 に置き換わります。
124	ユーザ脆弱性	現在(Current)	ホスト脆弱性に関する情報を格納します。ユーザ脆弱性データ ブロック 5.0+(4-163 ページ)を参照してください。これはブロック タイプ 79 に置き換わります。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ(続き)

タイプ	目次	データ ブロック ステータス	説明
125	接続統計情報	レガシー	4.10.2 の接続統計イベントの情報を格納します(本製品の旧バージョンを参照のこと)。バージョン 5.1 で導入したサクセサ ブロックのブロック タイプは 115 です。
126	接続統計情報	レガシー	5.1 の接続統計イベントの情報を格納します。詳細については、接続統計データ ブロック 5.1(B-133 ページ)を参照してください。これはブロック タイプ 115 に置き換わります。このブロック タイプはブロック タイプ 137 に置き換わります。
130	オペレーティング システム フィンガープリント	現在(Current)	オペレーティング システム フィンガープリントのリストを格納します。詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。これはブロック タイプ 87 に置き換わります。
131	モバイルデバイス情報	現在(Current)	検出したモバイル デバイスのハードウェアに関する情報を格納します。詳細については、5.1+ デバイス のモバイル情報データ ブロック(4-168 ページ)を参照してください。
132	ホスト プロファイル	レガシー	ホストのプロファイル情報を格納します。詳細については、フル ホスト プロファイル データ ブロック 5.2.x(B-290 ページ)を参照してください。これはブロック タイプ 91 に置き換わります。ブロック 139 に置き換わります。
134	ユーザ製品	現在(Current)	サードパーティ アプリケーション文字列マッピングなど、サードパーティ アプリケーションからインポートしたホスト入力データを格納します。詳細については、ユーザ製品データ ブロック 5.1+(4-177 ページ)を参照してください。これは先行ブロック タイプ 118 に置き換わります。
135	フル ホスト プロファイル	レガシー	ホスト プロファイル情報一式を格納します。詳細については、フル ホスト プロファイル データ ブロック 5.1.1(B-280 ページ)を参照してください。データ ブロック 111 に置き換わります。
136	接続チャンク	現在(Current)	接続チャンク情報を格納します。詳細については、6.1+ の接続チャンク データ ブロック(4-103 ページ)を参照してください。ブロック 119 に置き換わります。
137	接続統計情報	レガシー	5.1.1 の接続イベントの情報を格納します。詳細については、接続チャンク データ ブロック 5.0 ～ 5.1(B-146 ページ)を参照してください。これはブロック タイプ 126 に置き換わります。これはブロック タイプ 144 に置き換わります。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ(続き)

タイプ	目次	データ ブロック ステータス	説明
138	ユーザ クライアント アプリケーション	現在(Current)	ユーザ入力のクライアント アプリケーション データを格納します。詳細については、5.1.1+ のユーザ クライアント アプリケーション データ ブロック (4-94 ページ) を参照してください。これはブロック タイプに置き換わります。
139	ホスト プロファイル	現在(Current)	ホストのプロファイル情報を格納します。詳細については、ホスト プロファイル データブロック 5.2+(4-169 ページ) を参照してください。これはブロック タイプ 132 に置き換わります。
140	フル ホスト プロファイル	レガシー	ホスト プロファイル情報一式を格納します。詳細については、全ホスト プロファイル データ ブロック 5.3+(5-1 ページ) を参照してください。データ ブロック 135 に置き換わります。
141	IP 範囲指定	現在(Current)	IP アドレス範囲指定を格納します。詳細については、5.2+の IP アドレス範囲データ ブロック (4-98 ページ) を参照してください。これはブロック 61 に置き換わります。
142	スキャン結果	現在(Current)	脆弱性に関する情報を格納しており、スキャン結果を追加イベントで使用します。次の表では、6.1+ の接続統計データ ブロックのフィールドについて説明します。(4-131 ページ) を参照してください。これはブロック 102 に置き換わります。
143	ホスト名/アドレス(Host IP)	現在(Current)	ホストの IP アドレスと最後の確認日時情報を格納します。詳細については、ホスト IP アドレス データ ブロック (4-100 ページ) を参照してください。
144	接続統計情報	レガシー	5.2.x. の接続イベントの情報を格納します。詳細については、接続統計データ ブロック 5.2.x (B-139 ページ) を参照してください。これはブロック タイプ 137 に置き換わります。
146	属性アドレス	現在(Current)	5.2+ のホスト属性アドレスを格納します。詳細については、属性アドレス データ ブロック 5.2+ (4-82 ページ) を参照してください。これはブロック タイプ 38 に取って代わります。
140	フル ホスト プロファイル	現在(Current)	ホスト プロファイル情報一式を格納します。詳細については、全ホスト プロファイル データ ブロック 5.3+(5-1 ページ) を参照してください。データ ブロック 135 に置き換わります。
152	接続統計情報	レガシー	5.3+ の接続イベントの情報を格納します。詳細については、接続統計データ ブロック 5.3(B-155 ページ) を参照してください。これはブロック タイプ 144 に置き換わります。
154	接続統計情報	レガシー	5.3 の接続イベントの情報を格納します。詳細については、接続統計データ ブロック 5.3.1(B-162 ページ) を参照してください。これはブロック タイプ 152 に置き換わります。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ(続き)

タイプ	目次	データ ブロック ステータス	説明
155	接続統計情報	レガシー	5.4 の接続イベントの情報を格納します。詳細については、接続統計データ ブロック 5.4(B-169 ページ)を参照してください。これはブロック タイプ 154 に置き換わります。
157	接続統計情報	レガシー	5.4.1 の接続イベントの情報を格納します。詳細については、接続統計データ ブロック 5.4.1 (B-184 ページ)を参照してください。これはブロック タイプ 155 に置き換わります。
160	接続統計情報	現在(Current)	6.0+ の接続イベントの情報を格納します。詳細については、接続統計データ ブロック 6.1+ (4-122 ページ)を参照してください。これはブロック タイプ 157 に置き換わります。

文字列データ ブロック

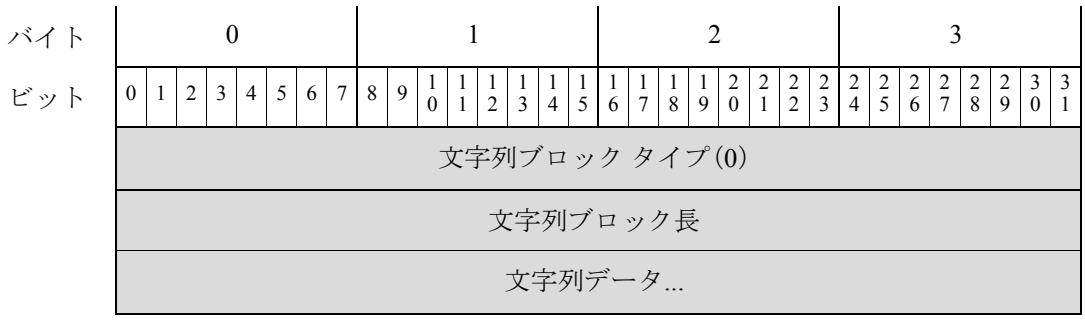
文字列データ ブロックは、シリーズ 1 ブロックの文字列データ送信に使用します。他のシリーズ 1 データ ブロックで、主に、たとえば、オペレーティング システムやサーバ名の記述に使用します。

空の文字列データ ブロック(文字列データを格納していない文字列データ ブロック)のブロック長値は 8 であり、ゼロバイトの文字列データが続きます。文字列値にコンテンツがなければ、空の文字列データ ブロックが返ります。たとえば、オペレーティング システムのベンダーが不明な場合の、オペレーティング システム データ ブロックの OS ベンダー文字列フィールドなどが該当します。

文字列データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 0 です。

(注)　このデータ ブロックで返る文字列の終端は、必ずしも NULL ではありません(最後が 0 とは限りません)。

次の図に、文字列データ ブロックの形式を示します。



次の表に、文字列データ ブロックのフィールドの説明を示します。

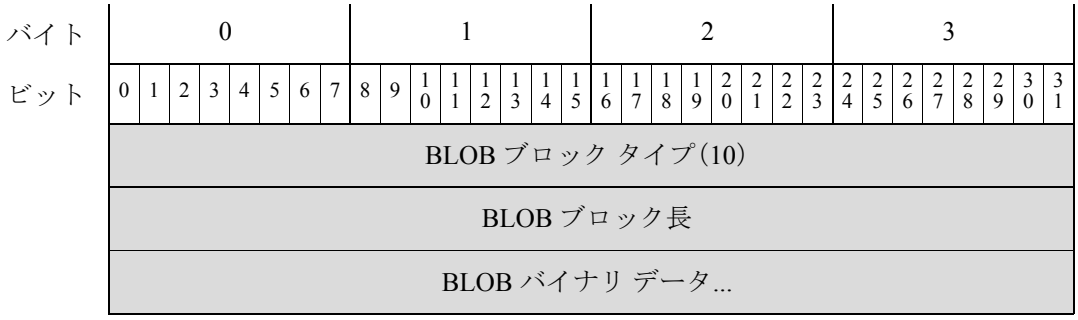
表 4-31　文字列データ ブロックのフィールド

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロック ヘッダーと文字列データを組み合わせた長さ。
文字列データ	string	文字列データが含まれています。文字列の末尾に終端文字（ヌル バイト）が含まれている場合があります。

BLOB データ ブロック

バイナリ データは BLOB データ ブロックで伝えることもできます。たとえば、システムがキャプチャしたサーバ バナーを BLOB データ ブロックで保存できます。BLOB データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 10 です。

次の図に、BLOB データ ブロックの形式を示します。



次の表に、BLOB データ ブロックのフィールドの説明を示します。

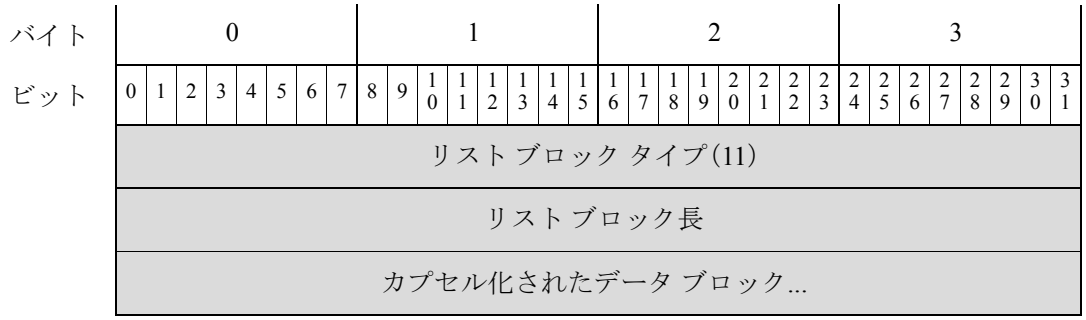
表 4-32　BLOB データ ブロック フィールド

フィールド	データ タイプ	説明
BLOB ブロック タイプ	uint32	BLOB データ ブロックを開始します。この値は常に 10 です。
BLOB ブロック長	uint32	BLOB データ ブロックのバイト数です。BLOB ブロック タイプとブロック長フィールドの 8 バイトと後続のバイナリ データの長さが含まれます。
バイナリ データ	変数	バイナリ データ（通常、サーバ バナー）を格納します。

リスト データ ブロック

リスト データ ブロックでは、シリーズ 1 データ ブロックのリストをカプセル化します。たとえば、TCP サーバのリストを送信する場合、データを含むサーバ データ ブロックはリスト データ ブロックにカプセル化されます。リスト データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 11 です。

次の図に、リスト データ ブロックの基本的な形式を示します。



次の表では、リスト データ ブロックのフィールドについて説明します。

表 4-33　リスト データ ブロックのフィールド

フィールド	データ タイプ	説明
リスト ブロック タイプ	uint32	リスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト ブロックとカプセル化されたデータのバイト数。たとえば、リストに 3 つのサブサーバ データ ブロックがある場合、その値は、サブサーバ ブロックのバイト数にリスト ブロック ヘッダーの 8 バイトを加えた値になります。
カプセル化されたデータ ブロック	変数	リスト ブロック長の最大バイト数を上限としてカプセル化したデータ ブロック。

汎用リスト ブロック

汎用リスト データ ブロックでは、シリーズ 1 データ ブロックのリストをカプセル化します。たとえば、ホスト プロファイル データ ブロックでクライアント アプリケーション情報を送信すると、クライアント アプリケーション データ ブロックのリストは、汎用リスト データ ブロックでカプセル化されます。汎用リスト データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 31 です。

次の図に、汎用リストのデータ ブロックの基本的な構造を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
汎用リスト ブロック タイプ(31)																																
汎用リスト ブロック長																																
カプセル化されたデータ ブロック...																																

次の表では、汎用リスト データ ブロックのフィールドについて説明します。

表 4-34　汎用リスト データ ブロックのフィールド

フィールド	バイト数	説明
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
カプセル化されたデータ ブロック	変数	リスト ブロック長の最大バイト数を上限としてカプセル化したデータ ブロック。

サブサーバ データ ブロック

サブサーバ データ ブロックは、個々のサブサーバに関する情報を伝えます。これは同じホスト上で別のサーバに呼び出されたサーバであり、脆弱性に関連付けられています。サブサーバ データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 1 です。

次の図は、サブサーバ データ ブロックの形式です。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	サブサーバ ブロック タイプ(1)																																
	サブサーバ ブロック長																																
サブサーバ名	文字列ブロック タイプ(0)																																
	文字列ブロック長																																
	サブサーバ名...																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ベンダー名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ベンダー名...																															
バージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	バージョン...																															

次の表では、サブサーバ データ ブロックのフィールドについて説明します。

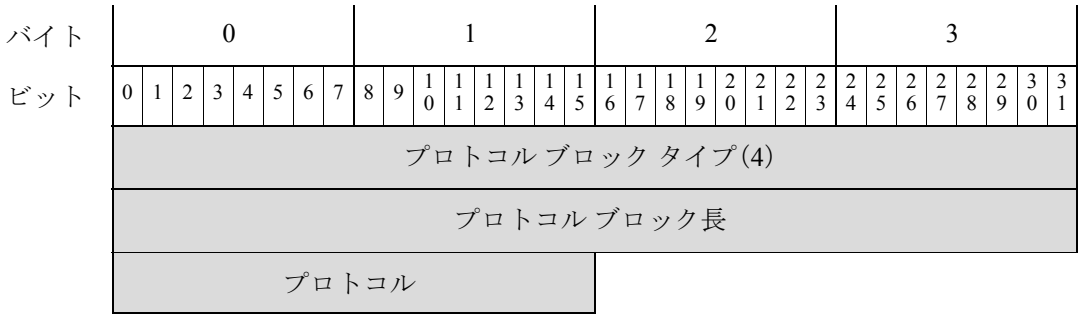
表 4-35　サブサーバ データ ブロックのフィールド

フィールド	データ タイプ	説明
サブサーバ ブロック タイプ	uint32	サブサーバ データ ブロックを開始します。この値は常に 1 です。
サブサーバ ブロック長	uint32	サブサーバ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたサブサーバ データ ブロックの合計バイト数。
文字列ブロック タイプ	uint32	サブサーバ名を格納した文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプ フィールドと長さフィールドにサブサーバ名のバイト数を加えたサブサーバ名文字列データ ブロックのバイト数。
サブサーバ名	string	サブサーバの名前。
文字列ブロック タイプ	uint32	サブサーバ ベンダーを格納した文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプ フィールドと長さフィールドにベンダー名のバイト数を加えたベンダー名文字列データ ブロックのバイト数。
ベンダー名	string	サブサーバ ベンダー名。
文字列ブロック タイプ	uint32	サブサーバ バージョンを格納した文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプ フィールドと長さフィールドにバージョンのバイト数を加えたサブサーバ バージョン文字列データ ブロックのバイト数。
バージョン	string	サブサーバ長

プロトコル データ ブロック

このプロトコル データ ブロックがプロトコルを定義します。ブロック タイプ、ブロック長、プロトコルを識別する IANA プロトコルだけのごく簡単データ ブロックです。リスト データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 4 です。

次の図は、プロトコル データ ブロックの形式です。



次の表では、プロトコル データ ブロックのフィールドについて説明します。

表 4-36　プロトコル データ ブロックのフィールド

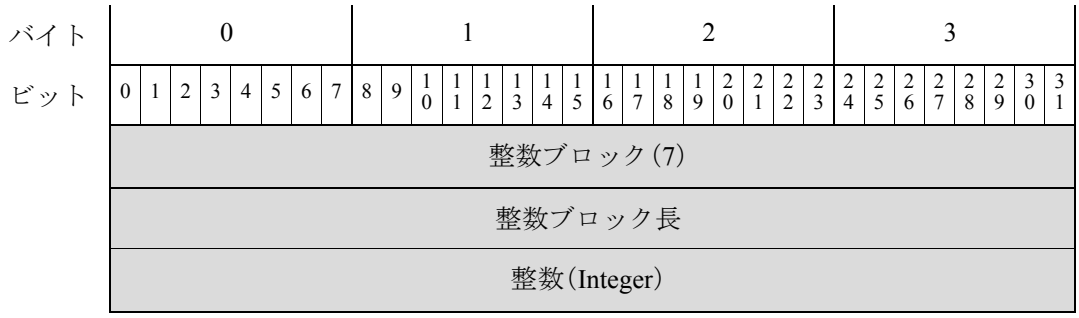
フィールド	データ タイプ	説明
プロトコル ブロック タイプ	uint32	プロトコル データ ブロックを開始します。この値は常に 4 です。
プロトコル ブロック長	uint32	プロトコル データ ブロックのバイト数。この値は常に 10 です。
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048:IP

整数型(INT32)データ ブロック

整数型(INT32)データ ブロックは、リスト データ ブロックで使用して 32 ビット整数型データを伝えます。

整数型データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 7 です。

次の図は、整数型データ ブロックの形式です。



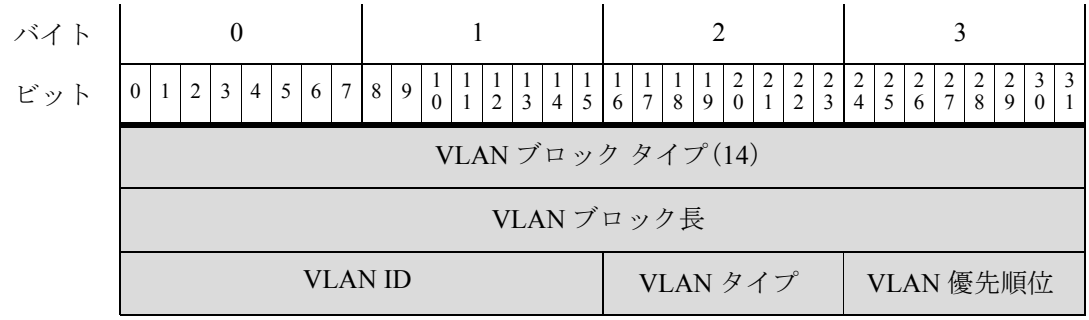
次の表では、整数型データ ブロックのフィールドについて説明します。

表 4-37　整数型データ ブロックのフィールド

フィールド	データ タイプ	説明
整数型ブロック タイプ	uint32	整数型データ ブロックを開始します。値は常に 7 です。
整数ブロック長	uint32	整数型データ ブロックのバイト数。この値は常に 12 です。
整数(Integer)	uint32	整数値を格納します。

VLAN データ ブロック

VLAN データ ブロックには、ホストの VLAN タグ情報を格納します。VLAN データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 14 です。次の図は、VLAN データ ブロックの形式です。



次の表では、VLAN データ ブロックのフィールドについて説明します。

表 4-38　VLAN データ ブロックのフィールド

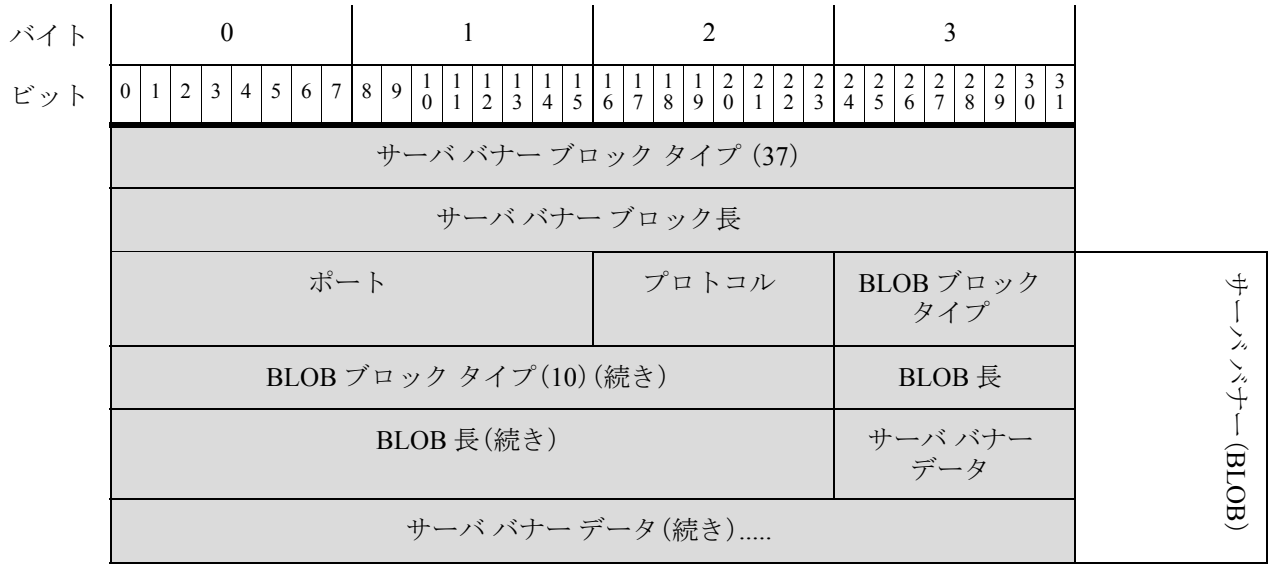
フィールド	データ タイプ	説明
VLAN ブロック タイプ	uint32	VLAN データ ブロックを開始します。この値は常に 14 です。
VLAN ブロック長	uint32	VLAN データ ブロックのバイト数。この値は常に 12 です。
VLAN ID	uint16	ホストがメンバーとして所属している VLAN を示す VLAN ID 番号を格納します。
VLAN タイプ	uint8	VLAN タグにカプセル化されたパケットのタイプ。 • 0:イーサネット • 1:トークン リング
VLAN 優先順位	uint8	VLAN タグに含まれる優先順位値。

サーバ バナー データ ブロック

サーバ バナー データ ブロックには、ホストで実行するサーバのバナーに関する情報があります。これにはサーバ ポート、プロトコル、バナー データを格納します。サーバ バナー データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 37 です。

次の図は、サーバ バナー データ ブロックの形式です。

(注)　次の図のブロック タイプ フィールドの横のアスタリスク(*)は、メッセージにシリーズ 1 データ ブロックのゼロ以上のインスタンスが含まれる可能性があることを示しています。



次の表では、サーバ バナー データ ブロックのフィールドについて説明します。

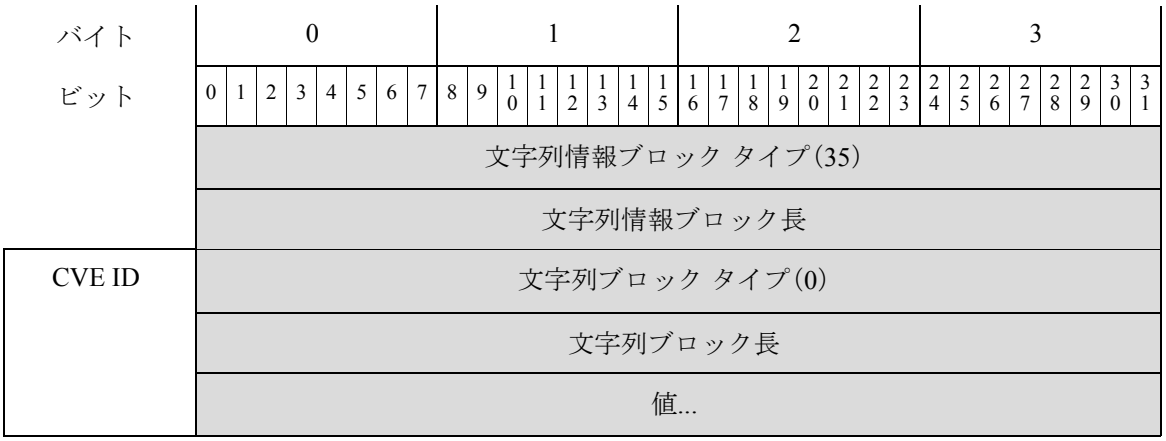
表 4-39　サーバ バナー データ ブロックのフィールド

フィールド	データ タイプ	説明
サーバ バナー ブロック タイプ	uint32	サーバ バナー データ ブロックを開始します。この値は常に 37 です。
サーバ バナー ブロック長	uint32	サーバ バナー ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたサーバ バナー データ ブロックの合計バイト数。
ポート	uint16	サーバを実行するポート番号。
プロトコル	uint8	サーバのプロトコル番号。
BLOB ブロック タイプ	uint32	サーバ バナー データを含む BLOB データ ブロックを開始します。この値は常に 10 です。
長さ（Length）	uint32	BLOB データ ブロックの合計バイト数（通常 264 バイト）。
バナー	byte[*n*]	パケットの最初の *n* バイトがサーバ イベントに関わるバイトであり、*n* は 256 以下です。

文字列情報データ ブロック

文字列情報データ ブロックには文字列データを格納します。たとえば、文字列情報データ ブロックは、スキャン脆弱性データ ブロックの Common Vulnerabilities and Exposures（CVE）識別文字列の伝達に使用します。文字列情報データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 35 です。

次の図は、文字列情報データ ブロックの形式です。



次の表では、文字列情報データ ブロックのフィールドについて説明します。

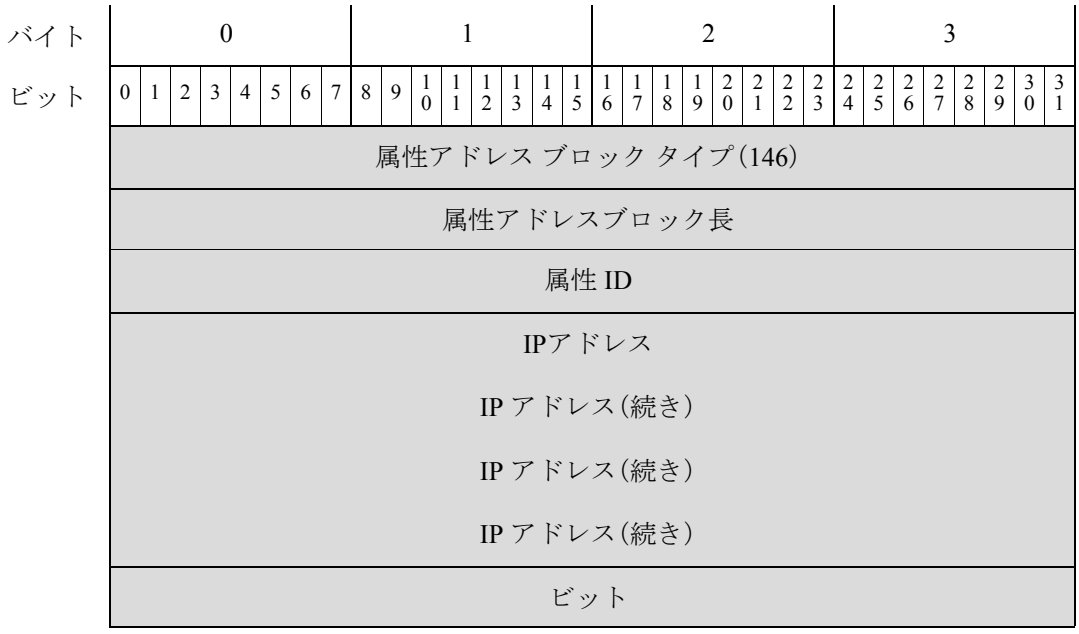
表 4-40　文字列情報データ ブロックのフィールド

フィールド	データ タイプ	説明
文字列情報ブロック タイプ	uint32	文字列情報データ ブロックを開始します。この値は常に 35 です。
文字列情報ブロック長	uint32	文字列情報データ ブロック ヘッダーと文字列情報データを組み合わせた長さ。
文字列ブロック タイプ	uint32	値を含む文字列データ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、値のバイト数を加えた値の文字列データ ブロックのバイト数。
値	string	文字列情報データ ブロックを使用した脆弱性のデータ ブロックの Common Vulnerabilities and Exposures（CVE）ID 番号の値。

属性アドレス データ ブロック 5.2+

属性アドレス ブロック データは、属性リスト項目が含まれ、属性定義データ ブロック内で使用されます。このブロック タイプは シリーズ 1 ブロック グループのブロック タイプ 146 です。

次の図は、属性アドレス ブロックの基本構造を示しています。



次の表は、属性アドレス データ ブロックのフィールドについての説明です。

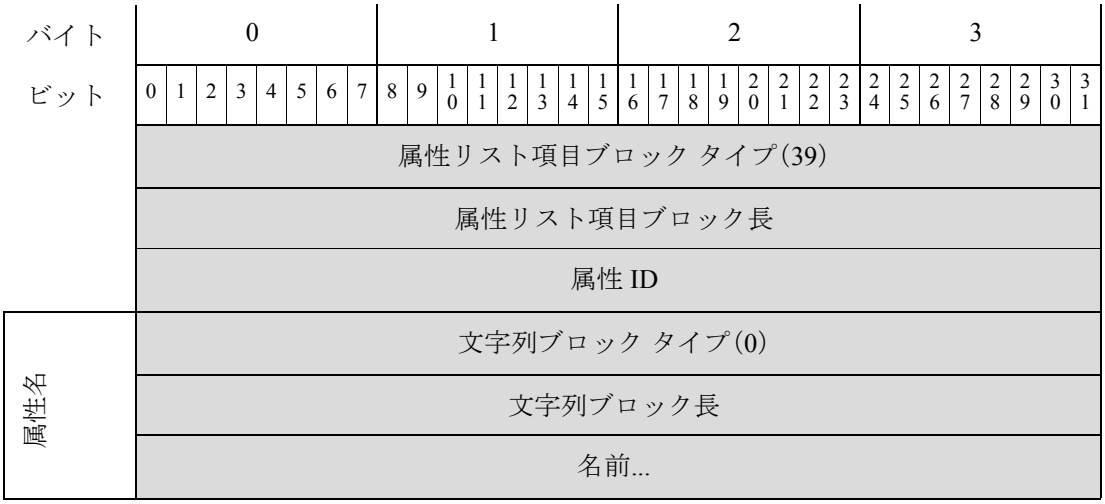
表 4-41　属性アドレス データ ブロック 5.2+ のフィールド

フィールド	データ タイプ	説明
属性アドレス ブロック タイプ	uint32	属性アドレス ブロック データを開始します。この値は常に 146 です。
属性アドレスブロック長	uint32	属性アドレス データ ブロックのバイト数（属性アドレス ブロック タイプと長さ用の 8 バイト、およびそれに続く属性アドレス データのバイト数を含む）。
属性 ID	uint32	影響を受ける属性の ID 番号（該当する場合）。
IPアドレス	uint8[16]	アドレスが自動的に割り当てられる場合は、ホストの IP アドレス。アドレスは IPv4 または IPv6 を使用できます。
ビット	uint32	IP アドレスが自動的に割り当てられた場合に、ネットマスクを計算するために使用される有効ビットが含まれます。

属性リスト項目データ ブロック

属性リスト項目データ ブロックは、属性リスト項目を格納します。属性定義データ ブロック内で使用します。このブロック タイプは シリーズ 1 ブロック グループのブロック タイプ 39 です。

次の図は、属性リスト項目データ ブロックの基本構造です。



次の表では、属性リスト項目データ ブロックのフィールドについて説明します。

表 4-42　属性リスト項目データ ブロックのフィールド

フィールド	データ タイプ	説明
属性リスト項目ブロック タイプ	uint32	属性リスト項目データ ブロックを開始します。この値は常に 39 です。
属性リスト項目ブロック長	uint32	属性リスト項目ブロック タイプと長さの 8 バイトに、後続の属性リスト項目データ バイト数を加えた属性リスト項目データ ブロックの合計バイト数。
属性 ID	uint32	影響を受ける属性の ID 番号（該当する場合）。
文字列ブロック タイプ	uint32	属性リスト項目名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、属性リスト項目名のバイト数を加えた、属性リスト項目名の文字列データ ブロックの合計バイト数。
名前	string	属性リスト項目名。

属性値データ ブロック

属性値データ ブロックは、ホスト属性の属性ID 番号と値を伝えます。イベントのホストに適用される各属性の属性値データ ブロックは、フル ホスト プロファイル データ ブロックのリストに格納します。属性値データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 48 です。

次の図は、属性値データ ブロックの形式です。

次の表では、属性値データ ブロックのコンポーネントについて説明します。

表 4-43　属性値データ ブロックのフィールド

フィールド	データ タイプ	説明
属性値 ブロック タイプ	uint32	属性値データ ブロックを開始します。この値は常に 48 です。
属性値ブロック長	uint32	属性値ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続の属性ブロック データのバイト数を加えた属性値データ ブロックの合計バイト数。
属性 ID	uint32	属性の ID 番号。
属性タイプ	uint32	影響を受ける属性のタイプ。値は以下のとおりです。 • 0:値としてのテキストによる属性。文字列データを使用します • 1:範囲の値による属性。整数型データを使用します • 2:使用可能値のリストによる属性。整数型データを使用します • 3:値としての URL による属性。文字列データを使用します • 4:値としてのバイナリ BLOB による属性。文字列データを使用します
属性整数値	uint32	属性に整数値(該当する場合)。
文字列ブロック タイプ	uint32	属性名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプ フィールドと長さフィールドに属性名のバイト数を加えた文字列データ ブロックのバイト数。
属性値	string	属性値。

フル サブサーバ データ ブロック

フル サーバ データ ブロックは、ホストで検出したサーバに関連付けられたサブサーバに関する情報を伝えます。サブサーバに関する情報には、ホスト上のサブサーバのベンダー、バージョン、関連 VDB、サードパーティ の脆弱性などがあります。サブサーバは、固有の関連脆弱性があるサーバの読み込み可能なモジュールです。フル ホスト サーバ データ ブロックには、ホストで検出した各サーバのフル サブサーバ データ ブロックが含まれます。フル ホスト サーバ データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 51 です。

(注)　次の図で、シリーズ 1 データ ブロック名の横のアスタリスク(*)は、データ ブロックの複数のインスタンスが発生する可能性があることを示します。

次の図は、フル サブサーバ データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
フル サブサーバ ブロック タイプ(51)																																
フル サブサーバ ブロック長																																
文字列ブロック タイプ(0)																																
文字列ブロック長																																
サブサーバ名文字列...																																
文字列ブロック タイプ(0)																																
文字列ブロック長																																
サブサーバ ベンダー名文字列...																																
文字列ブロック タイプ(0)																																
文字列ブロック長																																
サブサーバ バージョン文字列...																																
汎用リスト ブロック タイプ(31)																																
汎用リスト ブロック長																																
(VDB)ホスト脆弱性データ ブロック																																
汎用リスト ブロック タイプ(31)																																
汎用リスト ブロック長																																
(サードパーティ スキャン)ホスト脆弱性データ ブロック*																																

次の表では、フル サブサーバ データ ブロックのコンポーネントについて説明します。

表 4-44　フル サブサーバ データ ブロックのフィールド

フィールド	データ タイプ	説明
フル サブサーバ ブロック タイプ	uint32	フル サブサーバ ブロックを開始します。この値は常に 51 です。
フル サブサーバ ブロック長	uint32	フルサブサーバ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のフル サブサーバ ブロックのバイト数を加えたフル サブサーバ データ ブロックの合計バイト数。

表 4-44　フル サブサーバ データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	サブサーバ名を格納した文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにサブサーバ名のバイト数を加えたサブサーバ名文字列データ ブロックのバイト数。
サブサーバ名	string	サブサーバ名。
文字列ブロック タイプ	uint32	サブサーバ ベンダー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにサブサーバ名のバイト数を加えたベンダー名文字列データ ブロックのバイト数。
サブサーバ ベンダー名	string	サブサーバ ベンダーの名前。
文字列ブロック タイプ	uint32	サブサーバ バージョンを格納した文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにサブサーバ バージョンのバイト数を加えたサブサーバ バージョン文字列データ ブロックのバイト数。
サブサーバ バージョン	string	サブサーバ長
汎用リスト ブロック タイプ	uint32	VDB 脆弱性データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのホスト脆弱性データ ブロックを含む汎用リスト データ ブロックのバイト数。
VDB ホスト脆弱性ブロック*	変数	シスコ で確認されたホスト脆弱性に関する情報を格納したホスト脆弱性データブロック。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+(4-116 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	サード パーティ スキャン脆弱性データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのホスト脆弱性データ ブロックを含む汎用リスト データ ブロックのバイト数。
サードパーティ スキャン ホスト脆弱性データ ブロック*	変数	サードパーティの脆弱性のスキャナで確認されたホスト脆弱性に関する情報を格納したホスト脆弱性データブロック。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+(4-116 ページ) を参照してください。

オペレーティング システム データ ブロック 3.5+

バージョン 3.5+ のオペレーティング システム データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 53 です。このブロックには、フィンガープリント Universally Unique Identifier（UUID）を格納します。次の図は、3.5+ のオペレーティング システム データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	オペレーティング システム ブロック タイプ（53）																															
	オペレーティング システム ブロック長																															
	信頼度																															
OS フィンガープリント UUID	フィンガープリント UUID																															
	フィンガープリント UUID（続き）																															
	フィンガープリント UUID（続き）																															
	フィンガープリント UUID（続き）																															

次の表では、v3.5 オペレーティング システム データ ブロックのフィールドについて説明します。

表 4-45　オペレーティング システムのデータ ブロック 3.5+ のフィールド

フィールド	データ タイプ	説明
オペレーティング システム データ ブロック タイプ	uint32	オペレーティング システム データ ブロックを開始します。この値は常に 53 です。
オペレーティング システム データ ブロック長	uint32	オペレーティング システム データ ブロックのバイト数。この値は、常に、データ ブロック タイプ フィールドと長さ フィールドの 8 バイト、信頼度値の 4 バイト、そしてフィンガープリント UUID 値の 16 バイトからなる 28 です。
信頼度	uint32	信頼性の割合値。
フィンガープリント UUID	uint8[16]	オペレーティング システムの固有識別子として機能するフィンガープリントID 番号（オクテット）。UUID は、シスコ データベース内のオペレーティング システム名、ベンダー、およびバージョンにマップされます。

ポリシー エンジン制御メッセージ データ ブロック

ポリシー エンジン制御メッセージ データ ブロックは、ポリシー タイプの制御メッセージを伝えます。ポリシー エンジン制御メッセージ データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 54 です。

次の図は、ポリシー エンジン制御メッセージ データ ブロックの形式です。

次の表では、ポリシー エンジン制御メッセージ データ ブロックのコンポーネントについて説明します。

表 4-46　ポリシー エンジン制御メッセージ データ ブロックのフィールド

フィールド	データ タイプ	説明
ポリシー エンジン制御メッセージ ブロック タイプ	uint32	ポリシー エンジン制御メッセージ データ ブロックを開始します。この値は常に 54 です。
ポリシー エンジン制御メッセージ長さ	uint32	ポリシー エンジン制御ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のポリシー エンジン制御データのバイト数を加えたポリシー エンジン制御メッセージ データ ブロックの合計バイト数。
タイプ	uint32	イベントのポリシーのタイプを示します。
文字列ブロック タイプ	uint32	制御メッセージを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに制御メッセージのバイト数を加えた制御メッセージ文字列データ ブロックのバイト数。
制御メッセージ	uint32	ポリシー エンジンからの制御メッセージ。

4.7+ の定義属性データ ブロック

属性定義データ ブロックには、属性作成、変更、または削除イベントの更新属性定義が格納されます。属性定義データ ブロックは、ホスト属性追加イベント（イベント タイプ 1002、サブタイプ 6）、ホスト属性更新イベント（イベント タイプ 1002、サブタイプ 7）、ホスト属性削除イベント（イベント タイプ 1002、サブタイプ 8）で使用します。このブロック タイプは シリーズ 1 ブロック グループのブロック タイプ 55 です。

これらのイベントの詳細については、属性メッセージ（4-57 ページ） を参照してください。

次の図は、属性定義データ ブロックの基本構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	属性定義ブロック タイプ（55）																															
	属性定義ブロック長																															
	ソース ID																															
	UUID UUID（続き） UUID（続き） UUID（続き）																															
	ID																															
名前	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	名前...																															
	属性タイプ																															
	属性カテゴリ																															
	整数型範囲の開始値																															
	整数型範囲の終了値																															
	自動割り当て IP アドレス フラグ																															

次の表では、属性定義データ ブロックのフィールドについて説明します。

表 4-47　属性定義データ ブロックのフィールド

フィールド	データ タイプ	説明
属性定義ブロック タイプ	uint32	属性定義データ ブロックを開始します。この値は常に 55 です。
属性定義ブロック長	uint32	属性定義データ ブロック タイプと長さの 8 バイトに、後続の属性定義データのバイト数を加えた属性定義データ ブロックのバイト数。
ソース ID	uint32	属性データの送信元にマッピングするID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
UUID	uint8[16]	影響を受ける属性の固有識別子として機能する ID 番号。
属性 ID	uint32	影響を受ける属性の ID 番号(該当する場合)。
文字列ブロック タイプ	uint32	属性定義名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、属性定義名のバイト数を加えた、属性定義名の文字列データ ブロックの合計バイト数。
名前	string	属性定義名。

表 4-47　属性定義データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
属性タイプ	uint32	属性のタイプ。値は以下のとおりです。 • 0:値としてのテキストによる属性。文字列データを使用します • 1:範囲の値による属性。整数型データを使用します • 2:使用可能値のリストによる属性。整数型データを使用します • 3:値としての URL による属性。文字列データを使用します • 4:値としてのバイナリ BLOB による属性。文字列データを使用します
属性カテゴリ	uint32	属性カテゴリ
範囲の開始値	uint32	定義した属性の整数範囲内の最初の整数。
範囲の終了値	uint32	定義した属性の整数範囲の最後の整数。
自動割り当て IP アドレス フラグ	uint32	属性に基づいて IP アドレスが自動的に割り当てられるかどうかを示すフラグ。
リスト ブロック タイプ	uint32	属性リスト項目を伝える属性リスト項目データ ブロック リストで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべての属性リスト項目データ ブロックを加えた値です。 このフィールドの後にはゼロか、さらに属性リスト項目のデータ ブロックが続きます。
属性リスト項目ブロック タイプ	uint32	最初の属性リスト項目データ ブロックを開始します。このデータ ブロックには、他の属性リスト項目データ ブロックを、リスト ブロック長フィールドで定義した上限まで続けることができます。
属性リスト項目ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトに属性リスト項目のバイト数を加えた属性リスト項目文字列データ ブロックのバイト数。
属性リスト項目	変数	属性リスト項目データ ブロック (4-83 ページ) に記載の属性リスト項目データ。
リスト ブロック タイプ	uint32	ホストの IP アドレスを属性とともに伝える属性アドレス データ ブロックで構成されるリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべての属性アドレス データ ブロックを加えた値です。 このフィールドの後にはゼロか、さらに属性アドレスデータ ブロックが続きます。

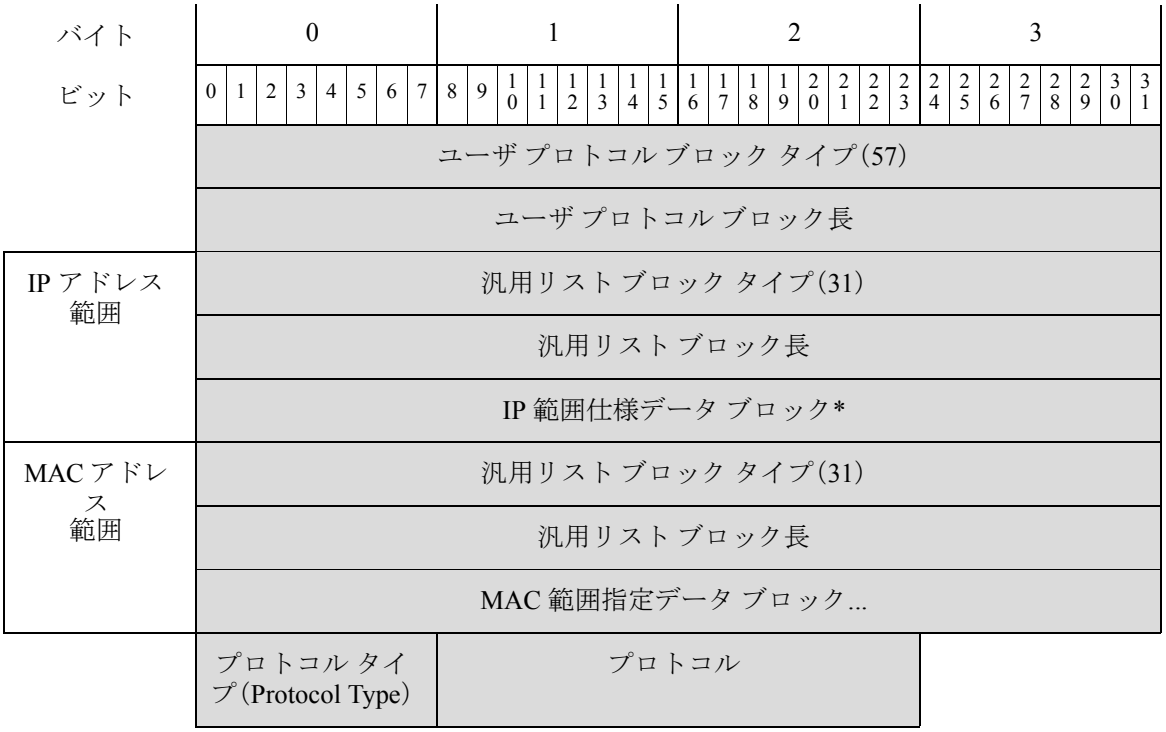
表 4-47　属性定義データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
属性アドレス ブロック タイプ	uint32	最初の属性アドレス データ ブロックを開始します。このデータ ブロックには、他の属性アドレス データ ブロックを、リスト ブロック長フィールドで定義した上限まで続けることができます。
属性アドレスブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトに属性アドレスのバイト数を加えた属性アドレス データ ブロックのバイト数。
属性アドレス	変数	属性アドレス データ ブロック 5.2+(4-82 ページ) に記載されている属性アドレス データ。

ユーザ プロトコル データ ブロック

ユーザ プロトコル データ ブロックには、追加したプロトコル、プロトコルのタイプ、ホストの IP アドレスの範囲と MAC アドレスの範囲に関する情報がプロトコルとともに格納されます。ユーザ プロトコル データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 57 です。

次の図は、ユーザ プロトコル データ ブロックの基本構造です。



次の表では、ユーザ プロトコル データ ブロックのフィールドについて説明します。

表 4-48　ユーザ プロトコル データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ プロトコル ブロック タイプ	uint32	ユーザ プロトコル データ ブロックを開始します。この値は常に 57 です。
ユーザ プロトコル ブロック長	uint32	ユーザ プロトコル ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザ プロトコル データのバイト数を加えたユーザ プロトコル データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リスト データ ブロックのバイト数。
IP 範囲仕様データ ブロック*	変数	ユーザ入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データ ブロック。このデータ ブロックの説明の詳細については、5.2+の IP アドレス範囲データ ブロック（4-98 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	MAC アドレス範囲データを伝える MAC 範囲指定データ ブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての MAC 範囲指定データ ブロックを含む汎用リスト データ ブロックのバイト数。
MAC 範囲指定データ ブロック*	変数	ユーザ入力の MAC アドレス範囲に関する情報を含む MAC 範囲指定データ ブロック。このデータ ブロックの説明の詳細については、MAC アドレス指定データ ブロック（4-101 ページ）を参照してください。
プロトコル タイプ（Protocol Type）	uint8	プロトコルのタイプを示します。プロトコルには、IP などネットワーク層プロトコルの 0、または TCP や UDP などトランスポート層プロトコルの 1 があります。
プロトコル	uint16	データ ブロックに格納されるデータのプロトコルを示します。

5.1.1+ のユーザ クライアント アプリケーション データ ブロック

ユーザ クライアント アプリケーション データ ブロックには、クライアント アプリケーション データの送信元に関する情報、データを追加したユーザの ID 番号、および IP アドレス範囲データ ブロックのリストが含まれます。バージョン 6.1 に追加されたペイロード IDは、レコードに関連付けられたアプリケーション インスタンスを指定します。ユーザ クライアント アプリケーション データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 138 です。これはブロック タイプに置き換えられます。

次の図は、ユーザ クライアント アプリケーション データ ブロックの基本構造を示しています。

次の表は、ユーザ クライアント アプリケーション データ ブロックのフィールドについての説明です。

表 4-49　ユーザ クライアント アプリケーション データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ クライアント アプリケーション ブロック タイプ	uint32	ユーザ クライアント アプリケーション データ ブロックを開始します。この値は常に 138 です。
ユーザ クライアント アプリケーション ブロック長	uint32	ユーザ クライアント アプリケーション データ ブロックのバイトの合計数(ユーザ クライアント アプリケーション ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ クライアント アプリケーション データのバイト数を含む)。
汎用リスト ブロック タイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リスト データ ブロックのバイト数。

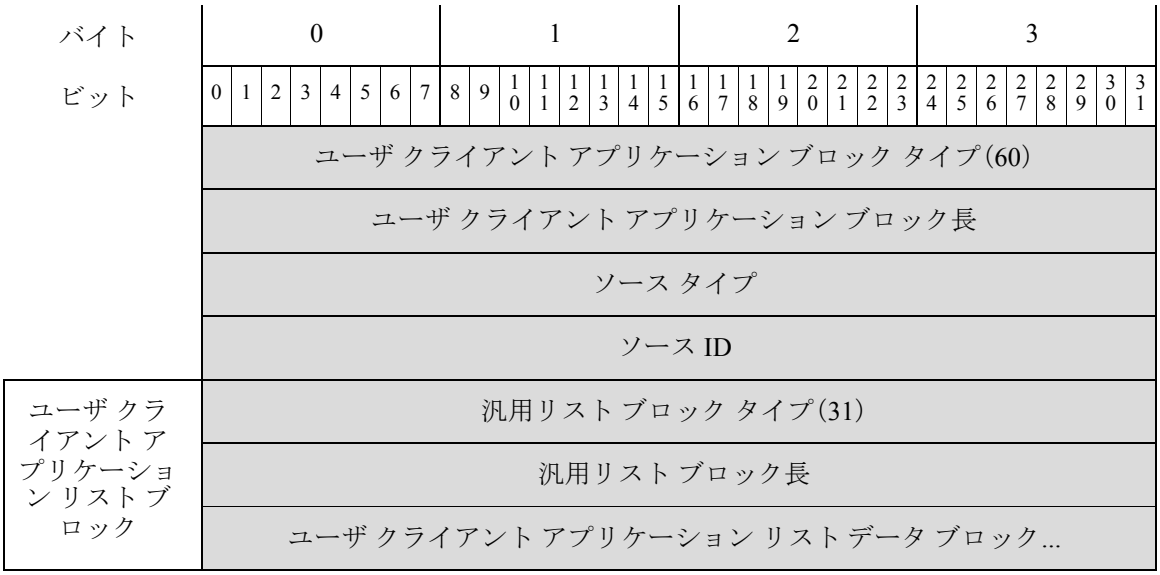
表 4-49　ユーザ クライアント アプリケーション データ ブロックのフィールド(続き)

フィールド	バイト数	説明
IP 範囲仕様データ ブロック*	変数	ユーザ入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データ ブロック。このデータ ブロックの説明の詳細については、5.2+の IP アドレス範囲データ ブロック (4-98 ページ) を参照してください。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション バージョン文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド、およびバージョンのバイト数を含む)。
バージョン	string	クライアント アプリケーション バージョン。
ペイロード タイプ (Payload Type)	uint32	このフィールドは下位互換性のために用意したものです。常に 0 です。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。

ユーザ クライアント アプリケーション リスト データ ブロック

ユーザ クライアント アプリケーション データ ブロックには、クライアント アプリケーション データの送信元に関する情報、データを追加したユーザの ID 番号、クライアント アプリケーション ブロックのリストを格納します。ユーザ クライアント アプリケーション リスト データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 60 です。

次の図は、ユーザ クライアント アプリケーション リスト データ ブロックの基本構造です。



次の表では、ユーザ クライアント アプリケーション リスト データ ブロックのフィールドについて説明します。

表 4-50　ユーザ クライアント アプリケーション リスト データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ クライアント アプリケーション リスト ブロック タイプ	uint32	ユーザ クライアント アプリケーション リスト データ ブロックを開始します。この値は常に 60 です。
ユーザ クライアント アプリケーション リスト ブロック長	uint32	ユーザ クライアント アプリケーション リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザ クライアント リスト アプリケーション データのバイト数を加えたユーザ クライアント アプリケーション リスト データ ブロックの合計バイト数。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA）がクライアント データを検出した場合、0 • ユーザがクライアント データを提供した場合、1 • サードパーティ スキャナがクライアント データを検出した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでクライアント データを提供した場合、3
ソース ID	uint32	影響を受けるクライアント アプリケーションを追加した送信元にマッピングするID 番号。送信元タイプによって、これは無応答（RNA）、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
ユーザ クライアント アプリケーション ブロック	変数	リスト ブロック長の最大バイト数を上限としてカプセル化したユーザ クライアント アプリケーション データ ブロック。ユーザ クライアント アプリケーション データ ブロックの詳細については、5.1.1+ のユーザ クライアント アプリケーション データ ブロック（4-94 ページ）を参照してください。

5.2+の IP アドレス範囲データ ブロック

5.2+ の IP アドレス範囲データ ブロックは IP アドレス範囲を伝えます。IP アドレス範囲データ ブロックは、ユーザ プロトコル、ユーザ クライアント アプリケーション、アドレス指定、ユーザ製品、ユーザ サーバ、ユーザ ホスト、ユーザ脆弱性、ユーザ重要度、ユーザ属性値データ ブロックで使用します。IP アドレス範囲データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 141 です。

次の図は、IP アドレス範囲データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IP アドレス範囲ブロック タイプ（141）																																
IP アドレス範囲ブロック長																																
IP アドレス範囲の開始																																
IP アドレス範囲の開始（続き）																																
IP アドレス範囲の開始（続き）																																
IP アドレス範囲の開始（続き）																																
IP アドレス範囲の最後																																
IP アドレス範囲の最後（続き）																																
IP アドレス範囲の最後（続き）																																
IP アドレス範囲の最後（続き）																																

次の表では、IP アドレス範囲指定データ ブロックのコンポーネントについて説明します。

表 4-51　IP アドレス範囲データ ブロックのフィールド

フィールド	データ タイプ	説明
IP アドレス範囲ブロック タイプ	uint32	IP アドレス範囲データ ブロックを開始します。この値は常に 61 です。
IP アドレス範囲ブロック長	uint32	IP アドレス範囲ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続の IP アドレス範囲データのバイト数を加えた IP アドレス範囲データ ブロックの合計バイト数。
IP アドレス範囲の開始	uint8[16]	IP アドレス範囲の開始 IP アドレス。
IP アドレス範囲の最後	uint8[16]	IP アドレス範囲の最終 IP アドレス。

属性指定データ ブロック

属性指定データ ブロックは属性名と値を伝えます。属性指定データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 62 です。

次の図は、属性指定データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	属性指定ブロック タイプ(62)																															
属性名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	属性名...																															
属性値	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	属性値...																															

次の表では、属性指定データ ブロックのコンポーネントについて説明します。

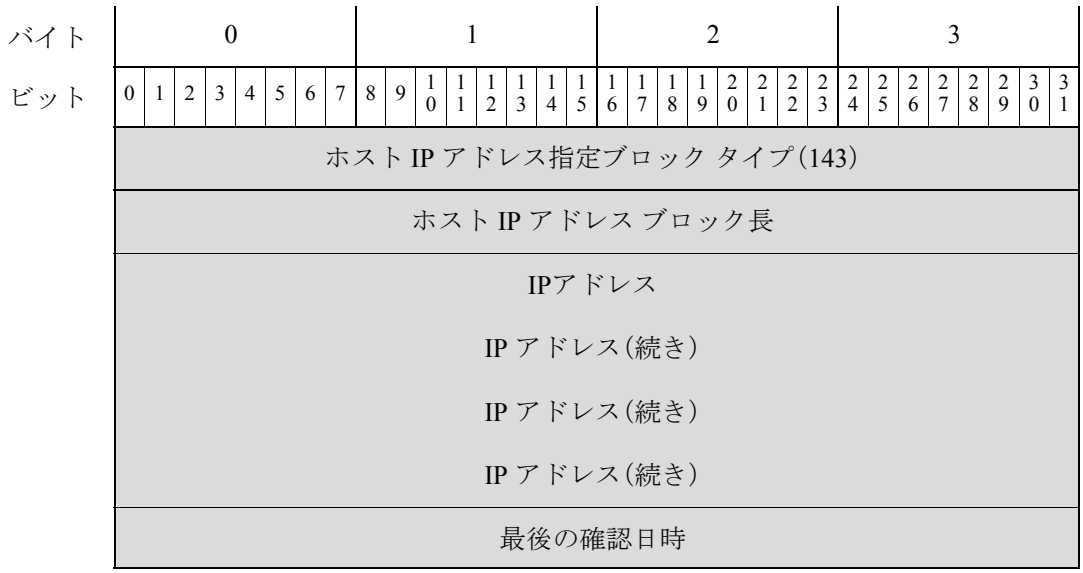
表 4-52　属性指定データ ブロックのフィールド

フィールド	データ タイプ	説明
属性指定ブロック タイプ	uint32	属性指定データ ブロックを開始します。この値は常に 62 です。
文字列ブロック タイプ	uint32	属性名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに属性名のバイト数を加えた属性名文字列データ ブロックのバイト数。
属性値	uint32	属性の値。
文字列ブロック タイプ	uint32	属性名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに属性名のバイト数を加えた属性名文字列データ ブロックのバイト数。
属性名	uint32	属性の名前。

ホスト IP アドレス データ ブロック

ホスト IP アドレス データ ブロックは個々の IP アドレスを伝えます。IP アドレスには、IPv4 アドレスと IPv6 アドレスのいずれも使用できます。ホスト IP アドレス データ ブロックは、ユーザ プロトコル、アドレス指定、ユーザ ホスト データ ブロックで使用します。ホスト IP データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 143 です。

次の図は、ホスト IP アドレス データ ブロックの形式です。



次の表では、ホスト IP アドレス データ ブロックのコンポーネントについて説明します。

表 4-53　ホスト IP アドレス データ ブロックのフィールド

フィールド	データ タイプ	説明
ホスト IP アドレス ブロック タイプ	uint32	ホスト IP アドレス データ ブロックを開始します。この値は常に 143 です。
ホスト IP ブロック長	uint32	ホスト IP ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のホスト IP アドレス データのバイト数を加えたホスト IP アドレス データ ブロックの合計バイト数。
IPアドレス	uint8[16]	IP アドレス。これには、IPv4 または IPv6 のいずれも使用できます。
最後の確認日時	uint32	IP アドレスを前回検出した時刻を表す UNIX タイムスタンプ。

MAC アドレス指定データ ブロック

MAC アドレス指定データ ブロックは個々の MAC アドレスを伝えます。MAC アドレス指定データ ブロックは、ユーザ プロトコル、アドレス指定、ユーザ ホスト データ ブロックで使用します。MAC アドレス 指定データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 63 です。

次の図は、MAC アドレス指定データ ブロックの形式です。

次の表では、MAC アドレス指定データ ブロックのコンポーネントについて説明します。

表 4-54　MAC アドレス指定データ ブロックのフィールド

フィールド	データ タイプ	説明
MAC アドレス指定ブロック タイプ	uint32	MAC アドレス指定データ ブロックを開始します。この値は常に 63 です。
MAC アドレス指定ブロック長	uint32	MAC アドレス指定ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続の MAC アドレス指定データのバイト数を加えた MAC アドレス指定データ ブロックの合計バイト数。
MAC アドレス ブロック サイズ 1 ～ 6	uint8	順に並んだ MAC アドレス ブロック。

アドレス指定データ ブロック

アドレス指定のデータ ブロックには、IP アドレス範囲指定と MAC アドレス指定のリストを格納します。アドレス指定データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 64 です。

次の図は、アドレス指定データ ブロックの基本構造です。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	アドレス指定データ ブロック タイプ(64)																																
	アドレス指定ブロック長																																
IP アドレス範囲ブロック	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
	IP アドレス範囲指定ブロック...																																
MAC アドレス ブロック	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
	MAC アドレス指定データ ブロック...																																

次の表では、アドレス指定データ ブロックのフィールドについて説明します。

表 4-55　アドレス指定データ ブロックのフィールド

フィールド	バイト数	説明
アドレス指定データブロック タイプ	uint32	アドレス指定データ ブロックを開始します。この値は常に 64 です。
アドレス指定ブロック長	uint32	アドレス指定ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のアドレス指定データのバイト数を加えたアドレス指定データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
IP アドレス範囲指定データ ブロック	変数	リスト ブロック長の最大バイト数を上限としてカプセル化した IP アドレス範囲指定データ ブロック。詳細については、5.2+の IP アドレス範囲データ ブロック(4-98 ページ)を参照してください。

表 4-55　アドレス指定データ ブロックのフィールド（続き）

フィールド	バイト数	説明
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
MAC アドレス指定データ ブロック	変数	リスト ブロック長の最大バイト数を上限としてカプセル化した MAC アドレス指定データ ブロック。詳細については、MAC アドレス指定データ ブロック（4-101 ページ）を参照してください。

6.1+ の接続チャンク データ ブロック

接続チャンク データ ブロックは、接続データを伝えます。5 分間分を集約した接続ログ データを保存します。6.1+ バージョンでは、新しいフィールドとしてオリジナル クライアント IP アドレスを導入しました。接続チャンク データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 164 です。これはブロック タイプ 136 に置き換わります。

次の図は、接続チャンク データ ブロックの形式を示しています。

次の表は、接続チャンク データ ブロックのコンポーネントについての説明です。

表 4-56　接続チャンク データ ブロックのフィールド

フィールド	データ タイプ	説明
接続チャンク ブロック タイプ	uint32	接続チャンク データ ブロックを開始します。この値は常に 164 です。
接続チャンク ブロック長	uint32	接続チャンク データ ブロックのバイト数(接続チャンク ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続チャンク データのバイト数を含む)。
イニシエータ IP アドレス	uint8(4)	この接続タイプのイニシエータの IP アドレス。このアドレスは、オリジナル クライアントとレスポンダの IP アドレスに使用して、同一の接続を識別します。
レスポンダ IP アドレス	uint8(4)	この接続タイプのレスポンダの IP アドレス。このアドレスは、イニシエータとオリジナル クライアントの IP アドレスに使用して、同一の接続を識別します。
オリジナル クライアント IP アドレス	uint8(4)	要求の送信元であるプロキシの背後にあるホストの IP アドレス。これは、イニシエータとレスポンダの IP アドレスで使用して同一の接続を確認します。
開始時刻(Start Time)	uint32	接続チャンクの開始時刻。
アプリケーション プロトコル	uint32	接続で使用されたプロトコルの ID 番号。
レスポンダ ポート	uint16	接続チャンクでレスポンダが使用したポート。
プロトコル	uint8	ユーザ情報を含むパケットのプロトコル。
接続タイプ	uint8	接続の種類。
NetFlow ディテクタ IP アドレス	uint8[4]	IP アドレス オクテットの、接続を検出した NetFlow デバイスの IP アドレス。
送信パケット数	uint64	接続チャンクで送信されたパケット数。

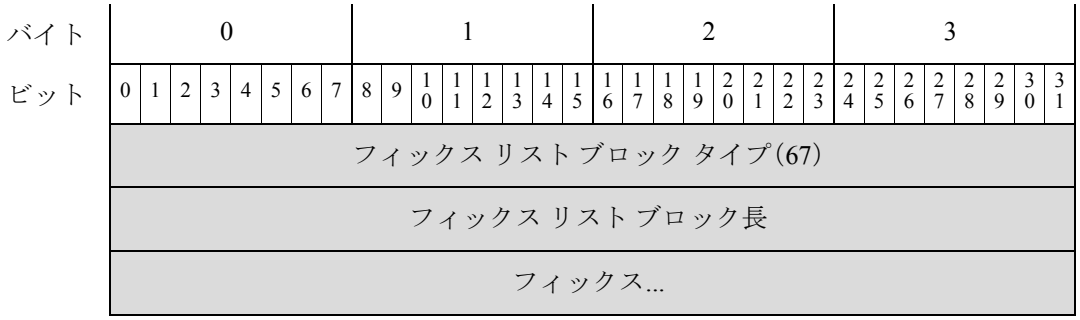
表 4-56　接続チャンク データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
受信パケット数	uint64	接続チャンクで受信されたパケット数。
送信バイト数	uint64	接続チャンクで送信されたバイト数。
受信バイト数	uint64	接続チャンクで受信されたバイト数。
接続	uint32	5 分間の接続数。

フィックス リスト データ ブロック

フィックス リスト データ ブロックはホストに適用するフィックスを伝えます。影響を受けるホストに適用される各フィックスのフィックス リストデータ ブロックは、ユーザ製品データ ブロックに格納します。フィックス リスト データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 67 です。

次の図は、フィックス リスト データ ブロックの形式です。



次の表では、フィックス リスト データ ブロックのコンポーネントについて説明します。

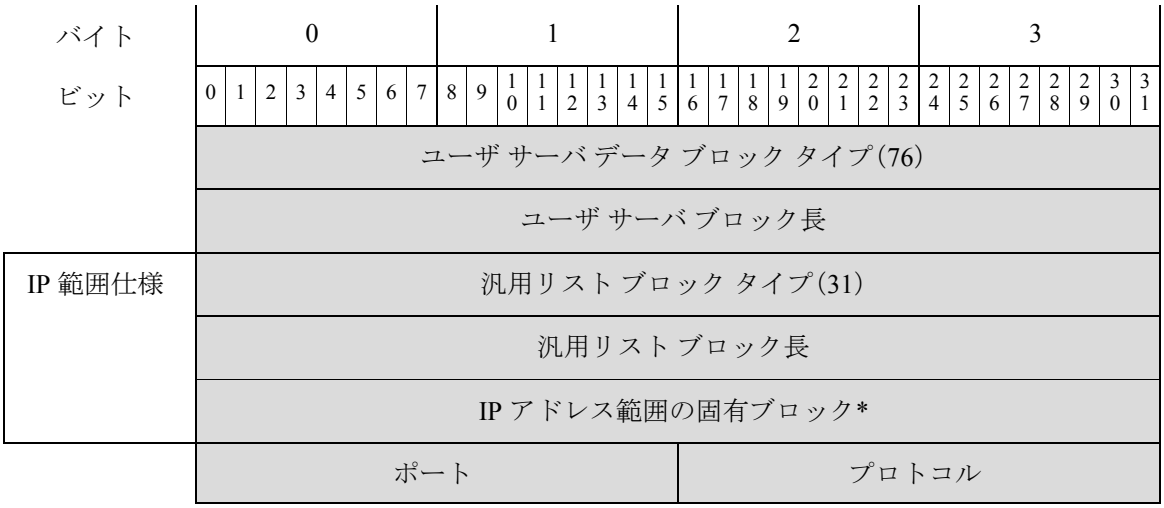
表 4-57　フィックス リスト データ ブロックのフィールド

フィールド	データ タイプ	説明
フィックス リスト ブロック タイプ	uint32	フィックス リスト データ ブロックを開始します。この値は常に 67 です。
フィックス リスト ブロック長	uint32	フィックス リスト ブロック タイプ フィールドと長さ フィールドの 8 バイトに、後続のフィックス識別データのバイト数を加えたフィックス リスト データ ブロックの合計バイト数。
フィックス ID	uint32	フィックスの ID 番号。

ユーザ サーバ データ ブロック

ユーザ サーバ データ ブロックには、ユーザ入力のサーバの詳細を格納します。ユーザ サーバ データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 76 です。

次の図は、ユーザ サーバ データ ブロックの基本構造です。



次の表では、ユーザ サーバ データ ブロックのフィールドについて説明します。

表 4-58　ユーザ サーバ データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ サーバ データ ブロック タイプ	uint32	ユーザ サーバ データ ブロックを開始します。この値は常に 76 です。
ユーザ サーバ ブロック長	uint32	ユーザ サーバ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザ サーバ データのバイト数を加えたユーザ サーバ データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
IP アドレス範囲指定データ ブロック	変数	リスト ブロック長の最大バイト数を上限としてカプセル化した IP アドレス範囲指定データ ブロック。

表 4-58　ユーザ サーバ データ ブロックのフィールド(続き)

フィールド	バイト数	説明
ポート	uint16	サーバで使用するポート。
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048:IP

ユーザ サーバ リスト データ ブロック

ユーザ サーバ リスト データ ブロックには、ユーザ入力のサーバ リスト データ ブロックを格納します。ユーザ サーバ リスト データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 77 です。次の図は、ユーザ サーバ リスト データ ブロックの基本構造です。

次の表では、ユーザ サーバ リスト データ ブロックのフィールドについて説明します。

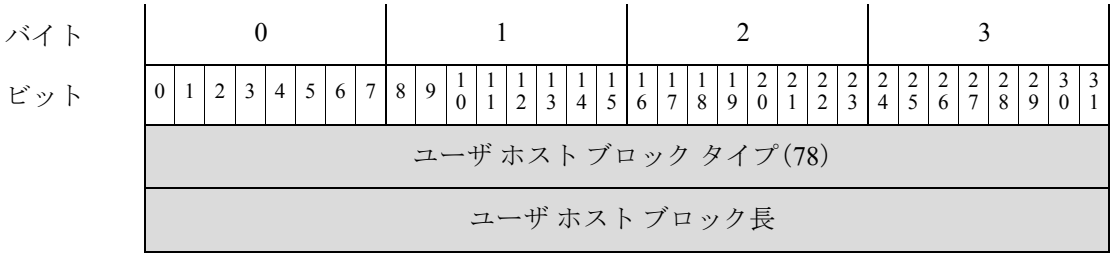
表 4-59　ユーザ サーバ リスト データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ サーバ リスト データ ブロック タイプ	uint32	ユーザ サーバ リスト データ ブロックを開始します。この値は常に 77 です。
ユーザ サーバ リスト ブロック長	uint32	ユーザ サーバ リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザ サーバ リスト データのバイト数を加えたユーザ サーバ リスト データ ブロックの合計バイト数。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA）がサーバ データを検出した場合、0 • ユーザがサーバ データを提供した場合、1 • サードパーティ スキャナがサーバ データを検出した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでサーバ データを提供した場合、3
ソース ID	uint32	サーバ データの送信元にマッピングするID 番号。送信元タイプによって、これは無応答（RNA）、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
ユーザ サーバ データ ブロック	変数	リスト ブロック長の最大バイト数を上限としてカプセル化したユーザ サーバ データ ブロック。

ユーザ ホスト データ ブロック 4.7+

ユーザ ホスト データ ブロックは、ユーザ追加/削除ホスト メッセージ（4-56 ページ）で使用し、ホスト範囲、ユーザ ホスト入力イベントから得られるユーザ アイデンティティとソース アイデンティティに関する情報を格納します。ユーザ ホスト データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 78 です。

次の図は、ユーザ ホスト データ ブロックの基本構造です。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IP 範囲	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	IP 範囲仕様データ ブロック*																															
MAC 範囲	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	MAC 範囲指定データ ブロック...																															
	ソース ID																															
	ソース タイプ																															

次の表では、ユーザ ホスト データ ブロックのフィールドについて説明します。

表 4-60　ユーザ ホスト データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ ホスト ブロック タイプ	uint32	ユーザ ホスト データ ブロックを開始します。この値は常に 78 です。
ユーザ ホスト ブロック長	uint32	ユーザ ホスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザ ホスト データのバイト数を加えたユーザ ホスト データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リスト データ ブロックのバイト数。
IP 範囲仕様データ ブロック*	変数	ユーザ入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データ ブロック。このデータ ブロックの説明の詳細については、5.2+の IP アドレス範囲データ ブロック (4-98 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	MAC アドレス範囲データを伝える MAC 範囲指定データ ブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての MAC 範囲指定データ ブロックを含む汎用リスト データ ブロックのバイト数。
MAC 範囲指定データ ブロック*	変数	ユーザ入力の MAC アドレス範囲に関する情報を含む MAC 範囲指定データ ブロック。このデータ ブロックの説明の詳細については、MAC アドレス指定データ ブロック (4-101 ページ) を参照してください。

表 4-60　ユーザ ホスト データ ブロックのフィールド(続き)

フィールド	バイト数	説明
ソース ID	uint32	ホストデータを追加または更新した送信元にマッピングする ID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答(RNA) がホスト データを検出した場合、0 • ユーザがホスト データを提供した場合、1 • サードパーティ スキャナがホスト データを検出した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでホスト データを提供した場合、3

ユーザ脆弱性変更データ ブロック 4.7+

ユーザ脆弱性変更データ ブロックには、非アクティブ化したホスト脆弱性、脆弱性を非アクティブ化したユーザ、脆弱性変更を提供した送信元に関する情報、重要度値を格納します。ユーザ脆弱性変更データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 80 です。前のユーザ脆弱性変更データ ブロックからの変更では、新規ソース タイプ フィールドが加えられ、リスト データ ブロックの代わりに、汎用リスト データ ブロックで脆弱性非アクティブ化を保存するようになりました。このデータ ブロックは、ユーザ脆弱性変更メッセージで使用します(バージョン4.6.1+ のユーザ設定脆弱性メッセージ(4-55 ページ) を参照)。

次の図は、脆弱性変更データ ブロックの基本構造です。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ脆弱性変更データ ブロック タイプ(80)																																
	ユーザ脆弱性変更ブロック長																																
	ソース ID																																
	ソース タイプ																																
Vuln Ack ブロック	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
	ユーザ脆弱性データ ブロック...*																																

次の表では、汎用リスト データ ブロックのフィールドについて説明します。

表 4-61　ユーザ脆弱性変更データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ脆弱性変更データ ブロック タイプ	uint32	ユーザ脆弱性変更データ ブロックを開始します。この値は常に 80 です。
ユーザ脆弱性変更ブロック長	uint32	ホスト脆弱性ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のホスト脆弱性データのバイト数を加えたユーザ脆弱性変更データ ブロックの合計バイト数。
ソース ID	uint32	ホスト脆弱性変更値を更新または追加した送信元にマッピングされるID 番号。送信元タイプによって、これは無応答（RNA）、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA）がホスト脆弱性データを検出した場合、0 • ユーザがホスト脆弱性データを提供した場合、1 • サードパーティ スキャナがホスト脆弱性データを検出した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでホスト脆弱性データを提供した場合、3
タイプ	uint32	脆弱性のタイプ。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
ユーザ脆弱性データ ブロック	変数	リスト ブロック長の最大バイト数を上限としてカプセル化したユーザ脆弱性データ ブロック。詳細については、ユーザ脆弱性データ ブロック 5.0+（4-163 ページ）を参照してください。

ユーザ重要度変更データ ブロック 4.7+

ユーザ重要度データ ブロックには、ホスト重要度を変更したホストの IP アドレス範囲指定リスト、重要度値を更新したユーザの ID 番号、重要度値を提供する送信元に関する情報、重要度値を格納します。ユーザ重要度データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 81 です。前のユーザ重要度データ ブロックからの変更では、新規ソース タイプ フィールドが加えられ、リスト データ ブロックの代わりに、汎用リスト データ ブロックで IP アドレスを保存するようになりました。

ユーザ設定ホスト重要度メッセージ（4-57 ページ） にあるように、ユーザ設定ホスト重要度メッセージでは、ユーザ重要度データ ブロックを使用します。

次の図は、ユーザ重要度データ ブロックの基本構造です。

次の表では、ユーザ重要度データ ブロックのフィールドについて説明します。

表 4-62　ユーザ重要度データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ重要度データ ブロック タイプ	uint32	ユーザ重要度データ ブロックを開始します。この値は常に 81 です。
ユーザ重要度ブロック長	uint32	ユーザ重要度ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザ重要度データのバイト数を加えたユーザ重要度データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
IP アドレス範囲指定データ ブロック	変数	リスト ブロック長の最大バイト数を上限としてカプセル化した IP アドレス範囲指定データ ブロック。
ソース ID	uint32	ユーザ重要度値を更新または追加した送信元にマッピングされるID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。

表 4-62　ユーザ重要度データ ブロックのフィールド(続き)

フィールド	バイト数	説明
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答(RNA) がユーザ重要度値を提供した場合、0 • ユーザがユーザ重要度値を提供した場合、1 • サードパーティ スキャナがユーザ重要度値を提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでユーザ重要度値を提供した場合、3
重要度値	uint32	ユーザの重要度値。

ユーザ属性値データ ブロック 4.7+

ユーザ属性値データ ブロックには、属性値が変更されたホストを示す IP アドレス範囲のリストが、ユーザの ID 番号、属性値、その属性値を提供した送信元に関する情報、その属性値を格納した BLOB データ ブロックとともに格納されます。ユーザ属性値データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 82 です。前のユーザ属性値データ ブロックからの変更では、新規送信元タイプ フィールドが加えられ、リスト データ ブロックの代わりに、汎用リスト データ ブロックで IP アドレスを保存するようになりました。

次の図は、ユーザ属性値データ ブロックの構造です。

次の表では、ユーザ属性値データ ブロックのフィールドについて説明します。

表 4-63　ユーザ属性値データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ属性値データ ブロック タイプ	uint32	ユーザ属性値データ ブロックを開始します。この値は常に 82 です。
ユーザ属性値ブロック長	uint32	ユーザ属性値ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザ属性ブロック データのバイト数を加えた属性値データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
IP アドレス範囲指定データ ブロック	変数	リスト ブロック長の最大バイト数を上限とした IP アドレス範囲指定データ ブロック（それぞれ開始 IP アドレスと終了 IP アドレスを含む）。
ソース ID	uint32	属性データを追加または更新した送信元にマッピングするID 番号。送信元タイプによって、これは無応答（RNA）、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA）がユーザ属性を提供した場合、0 • ユーザが属性値を提供した場合、1 • サードパーティ スキャナがユーザ属性値を提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでユーザ属性値を提供した場合、3
属性 ID	uint32	更新した属性の ID 番号（該当する場合）。
BLOB ブロック タイプ	uint32	BLOB データ ブロックを開始します。この値は常に 10 です。
BLOB ブロック長	uint32	BLOB データ ブロックのバイト数です。BLOB ブロック タイプとブロック長フィールドの 8 バイトと後続のバイナリ データの長さが含まれます。
値	変数	バイナリ形式でユーザ属性値を格納します。

ユーザ プロトコル リスト データ ブロック 4.7+

ユーザ プロトコル リスト データ ブロックには、プロトコル データの送信元に関する情報、データを追加したユーザの ID 番号、プロトコル データ ブロックのリストを格納します。ユーザ プロトコル リスト データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 83 です。ユーザ プロトコル データ ブロックの詳細については、ユーザ プロトコル データ ブロック（4-93 ページ）を参照してください。

ユーザ プロトコル メッセージ（4-59 ページ）にあるように、ユーザ プロトコル メッセージでは、ユーザ プロトコル リスト データ ブロックを使用します。

次の図は、ユーザ プロトコル リスト データ ブロックの基本構造です。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ プロトコル リスト ブロック タイプ(83)																																
	ユーザ プロトコル リスト ブロック長																																
	ソース タイプ																																
	ソース ID																																
ユーザ プロトコル ブロック	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
	ユーザ プロトコル データ ブロック...																																

次の表では、汎用リスト データ ブロックのフィールドについて説明します。

表 4-64　ユーザ プロトコル リスト データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ プロトコル リスト ブロック タイプ	uint32	ユーザ プロトコル リスト データ ブロックを開始します。この値は常に 83 です。
ユーザ プロトコル リスト ブロック長	uint32	ユーザ プロトコル リスト ブロック タイプ フィールドと長さ フィールドの 8 バイトに、後続のユーザ プロトコル リスト データのバイト数を加えたユーザ プロトコル リスト データ ブロックの合計バイト数。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答(RNA) がプロトコル データを提供した場合、0 • ユーザがプロトコル データを提供した場合、1 • サードパーティ スキャナがプロトコル データを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでプロトコル データを提供した場合、3
ソース ID	uint32	影響を受けるプロトコルの送信元にマッピングするID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。

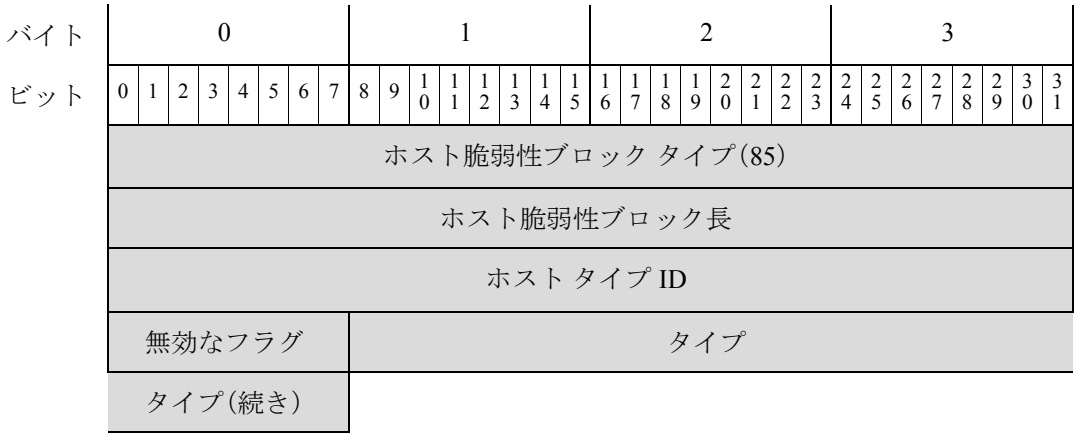
表 4-64　ユーザ プロトコル リスト データ ブロックのフィールド(続き)

フィールド	バイト数	説明
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
ユーザ プロトコル データ ブロック	変数	リスト ブロック長の最大バイト数を上限としてカプセル化されたユーザ プロトコル データ ブロック。

ホスト脆弱性データ ブロック 4.9.0+

ホスト脆弱性データ ブロックは、ホストに適用する脆弱性を伝えます。ホスト脆弱性データ ブロックごとに、1 回のイベントにおける 1 つのホストに関する 1 つの脆弱性について記述します。ホスト脆弱性データ ブロックは、フル ホスト プロファイル、フル ホスト サーバ、フル サブサーバ データ ブロックで表示されます。ホスト脆弱性データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 85 です。

次の図は、ホスト脆弱性データ ブロックの形式です。



次の表では、ホスト脆弱性データ ブロックのコンポーネントについて説明します。

表 4-65　ホスト脆弱性データ ブロックのフィールド

フィールド	データ タイプ	説明
ホスト脆弱性ブロック タイプ	uint32	ホスト脆弱性データ ブロックを開始します。この値は常に 85 です。
ホスト脆弱性ブロック長	uint32	ホスト脆弱性ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のホスト脆弱性データのバイト数を加えたホスト脆弱性データ ブロックの合計バイト数。
ホスト タイプ ID	uint32	脆弱性の ID 番号。
無効なフラグ	uint8	脆弱性がそのホストで有効であるかどうかを示す値。
タイプ	uint32	脆弱性のタイプ。

アイデンティティ データ ブロック

アイデンティティ データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 94 です。アイデンティティ データ ブロックは、オペレーティング システムやサーバ フィンガープリント送信元のアイデンティティがいつ競合するか、あるいはいつタイムアウトになるかを示すアイデンティティの競合メッセージとアイデンティティ タイムアウト メッセージで使用します。このデータ ブロックは、アクティブ送信元アイデンティティ（ユーザ、スキャナ、またはアプリケーション）と競合中であると報告されたアイデンティティを記述します。詳細については、アイデンティティ競合とアイデンティティ タイムアウト システム メッセージ（4-61 ページ）を参照してください。

次の図は、4.9+ のアイデンティティ データ ブロックの形式です。

次の表では、シスコ アイデンティティ データ ブロックのフィールドについて説明します。

表 4-66　アイデンティティ データ ブロックのフィールド

フィールド	データ タイプ	説明
アイデンティティ データ ブロック タイプ	uint32	アイデンティティ データ ブロックを開始します。この値は常に 94 です。
アイデンティティ データ ブロック長	uint32	アイデンティティ データ ブロックのバイト数。この値は常に 40 です。内訳は、データ ブロック タイプ フィールドと長さフィールド、および送信元タイプ フィールドと ID フィールドの 16 バイト、フィンガープリント UUID 値の 16バイト、ポートの 2 バイト、プロトコルの 2 バイト、そして SM ID の 4 バイトです。

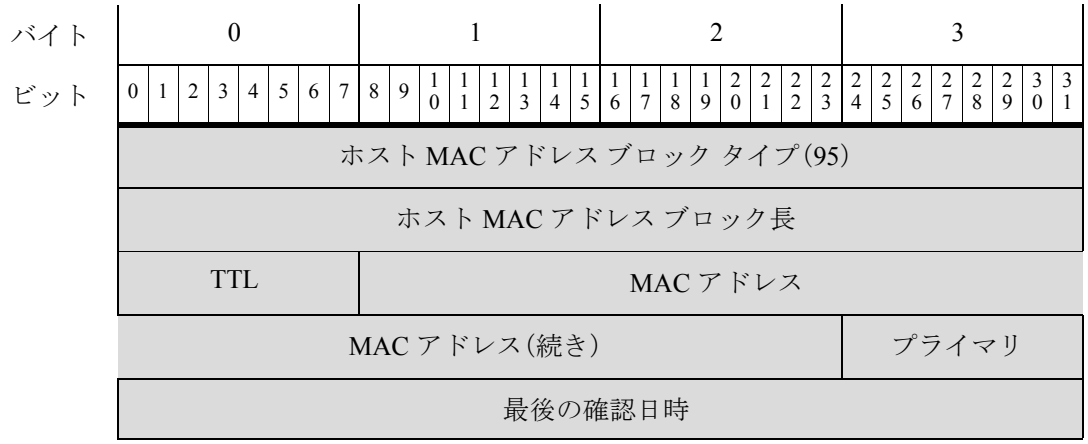
表 4-66　アイデンティティ データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
アイデンティティ データ送信元タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答(RNA) がフィンガープリント データを提供した場合、0 • ユーザがフィンガープリント データを提供した場合、1 • サードパーティ スキャナがフィンガープリント データを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでフィンガープリント データを提供した場合、3
アイデンティティ データ送信元 ID	uint32	フィンガープリント データの送信元にマッピングするID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
UUID	uint8[16]	アイデンティティがオペレーティング システム アイデンティティの場合、フィンガープリントの固有識別子として機能するオクテット形式の ID 番号。
ポート	uint16	アイデンティティがサーバ アイデンティティの場合、サーバ データを含むパケットで使用するポートを示します。
プロトコル	uint16	アイデンティティがサーバ アイデンティティの場合、ネットワーク プロトコルの IANA 番号またはサーバ データを含むパケットが使用する Ethertype を示します。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6:TCP • 7:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048:IP
サーバ マップ ID	uint32	アイデンティティがサーバ アイデンティティの場合、サーバの ID、ベンダー、バージョンの組み合わせを表すサーバ マッピング ID を示します。

ホスト MAC アドレス 4.9+

ホスト MAC アドレス データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 95 です。このブロックには、ホスト データのパケット存続時間の他、MAC アドレス、ホストのプライマリ サブネット、ホストの最後の確認日時値を格納します。

次の図は、4.9+ の MAC アドレス データ ブロックの形式です。



次の表では、ホスト MAC アドレス データ ブロックのフィールドについて説明します。

表 4-67　ホスト MAC アドレス データ ブロックのフィールド

フィールド	データ タイプ	説明
ホスト MAC アドレス データ ブロック タイプ	uint32	ホスト MAC アドレス データ ブロックを開始します。この値は常に 95 です。
ホスト MAC アドレス データ ブロック長	uint32	ホスト MAC アドレス データ ブロックのバイト数。この値は常に 20 です。内訳は、データ ブロック タイプ フィールドと長さフィールドの 8 バイト、TTL の 1 バイト、MAC アドレスの 6 バイト、プライマリ サブネットの 1 バイト、最後の確認日時値の 4 バイトです。
TTL	uint8	ホストのフィンガープリントを実行するために使用するパケットの TTL 値の違いを示します。
MAC アドレス	uint8 6	ホストの MAC アドレスを示します。
プライマリ	uint8	ホストのプライマリ サブネットを示しています。
最後の確認日時	uint32	トラフィックで前回ホストを確認した時刻を示します。

セカンダリ ホストの更新

セカンダリ ホスト更新データ ブロックには、ホストが存在する場所以外のサブネットをモニタリングするデバイスからセカンダリ ホスト更新として送信されるホストの情報を格納します。これは変更セカンダリ更新イベントで使用します(イベント タイプ 100 1、サブタイプ 31)。セカンダリ ホスト更新データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 96 です。

次の図は、セカンダリ ホスト更新データ ブロックの形式です。

次の表では、ホスト更新データ ブロックのフィールドについて説明します。

表 4-68　セカンダリ ホスト更新データ ブロックのフィールド

フィールド	データ タイプ	説明
セカンダリ ホスト更新 ブロック タイプ	uint32	セカンダリ ホスト更新データ ブロックを開始します。この値は常に 96 です。
セカンダリ ホスト更新ブロック長	uint32	セカンダリ ホスト更新ブロック タイプ フィールドと長さ フィールドの 8 バイトに、後続のホスト脆弱性データのバイト数を加えたセカンダリ ホスト更新データ ブロックの合計バイト数。
IPアドレス	uint8[4]	IP アドレスのオクテットの更新に、記載されているホストの IP アドレス。
リスト ブロック タイプ	uint32	ホスト MAC アドレス データを伝えるホスト MAC アドレス ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。

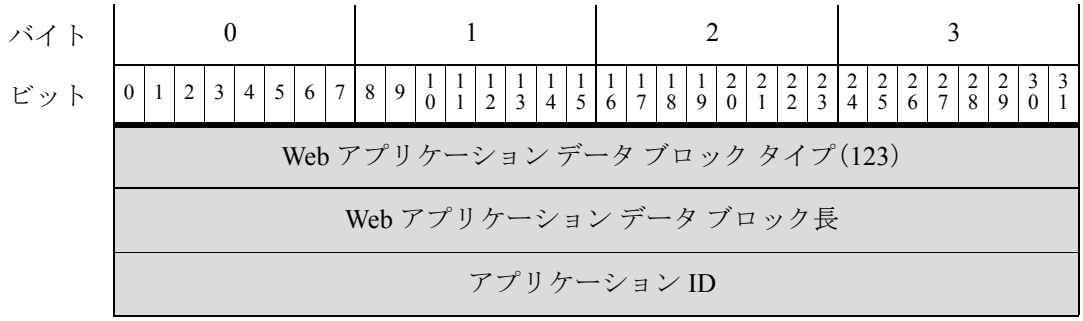
表 4-68　セカンダリ ホスト更新データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのホスト MAC アドレス データ ブロックを加えた値です。 このフィールドの後にはゼロか、さらにホスト MAC アドレス データ ブロックが続きます。
ホスト MAC アドレス ブロック タイプ	uint32	セカンダリ ホストを記述するホスト MAC アドレス データ ブロックを開始します。この値は常に 95 です。
ホスト MAC アドレス データ ブロック長	uint32	ホスト MAC アドレス データ ブロックのバイト数。この値は常に 20 です。内訳は、データ ブロック タイプ フィールドと長さフィールドの 8 バイト、TTL の 1 バイト、MAC アドレスの 6 バイト、プライマリ サブネットの 1 バイト、最後の確認日時値の 4 バイトです。
ホスト MAC アドレス データ ブロック	string	更新情報内のホスト MAC アドレス関連情報。

5.0+の Web アプリケーション データ ブロック

5.0+ の Web アプリケーション データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 123 です。このデータ ブロックは、検出した HTTP クライアント要求から得られた Web アプリケーションを記述します。

次の図は、5.0+ の Web アプリケーション データ ブロックの形式です。



次の表では、Web アプリケーション データ ブロックのフィールドについて説明します。

表 4-69　Web アプリケーション データ ブロックのフィールド

フィールド	データ タイプ	説明
Web アプリケーション データ ブロック タイプ	uint32	Web アプリケーション データ ブロックを開始します。この値は常に 123 です。
Web アプリケーション データ ブロック長	uint32	Web アプリケーション データ ブロック タイプと長さの 8 バイトに、後続の ID フィールドのバイト数を加えた Web アプリケーション データ ブロックのバイト数。
アプリケーション ID	uint32	Web アプリケーションのアプリケーション ID。

接続統計データ ブロック 6.1+

接続統計データ ブロックは、接続データ メッセージで使用されます。6.1+ の接続統計データ ブロックには、新しいフィールドが複数追加されました。ISE 統合および複数ネットワーク マップをサポートするために、フィールドが追加されました。バージョン 6.1+ の接続統計データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 163 です。これはブロック タイプ160 接続統計データ ブロック 6.0.x（B-198 ページ）に置き換わります。DNS ルックアップとセキュリティ インテリジェンスをサポートするため新しいフィールドを追加しました。

接続イベント レコードは、要求メッセージにイベント バージョン 14 とイベント コード 71 とともに拡張イベント フラグを設定して要求します。要求フラグ（2-12 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

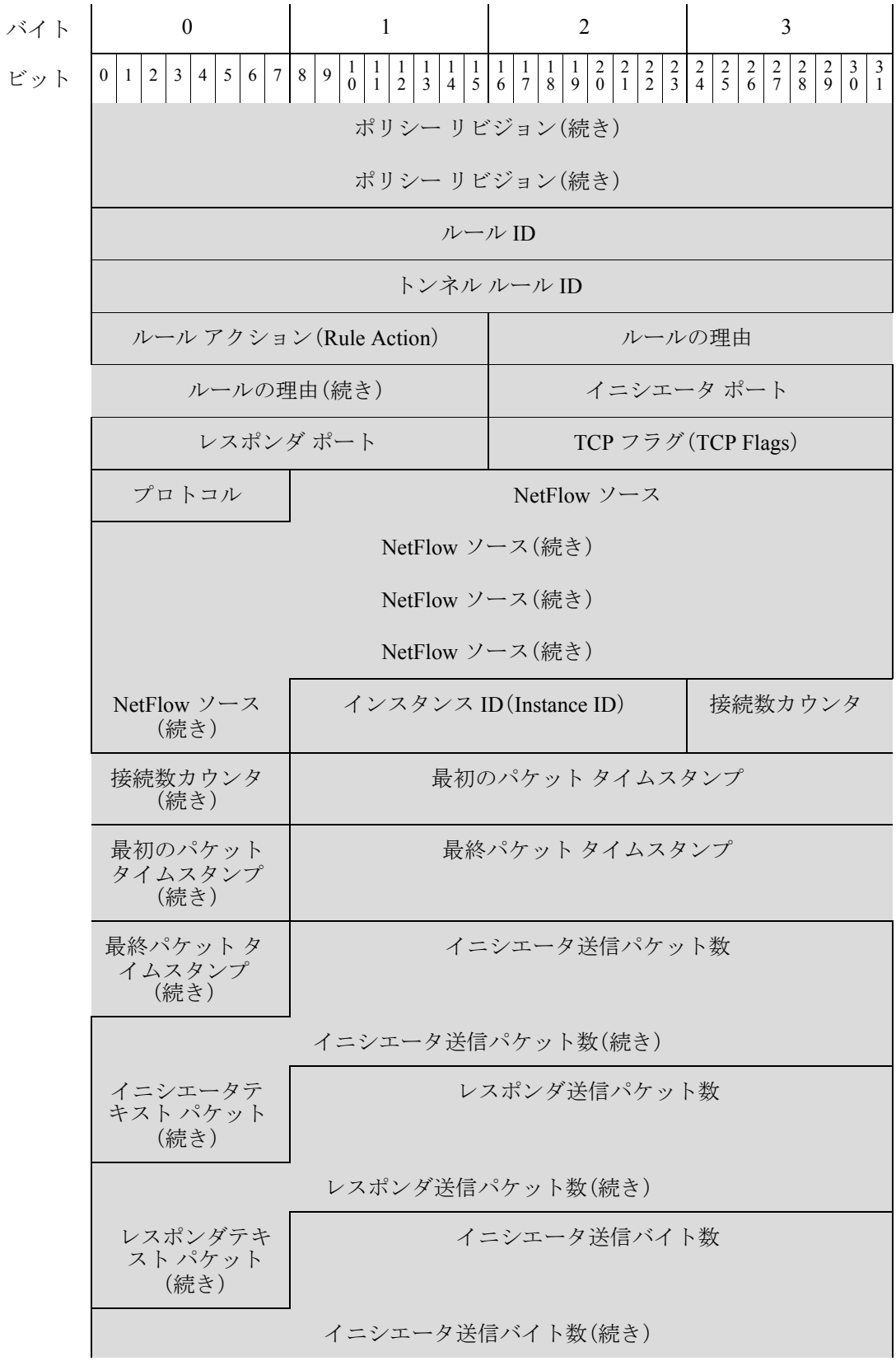
接続統計データ メッセージの詳細については、接続統計データ メッセージ（4-54 ページ）を参照してください。

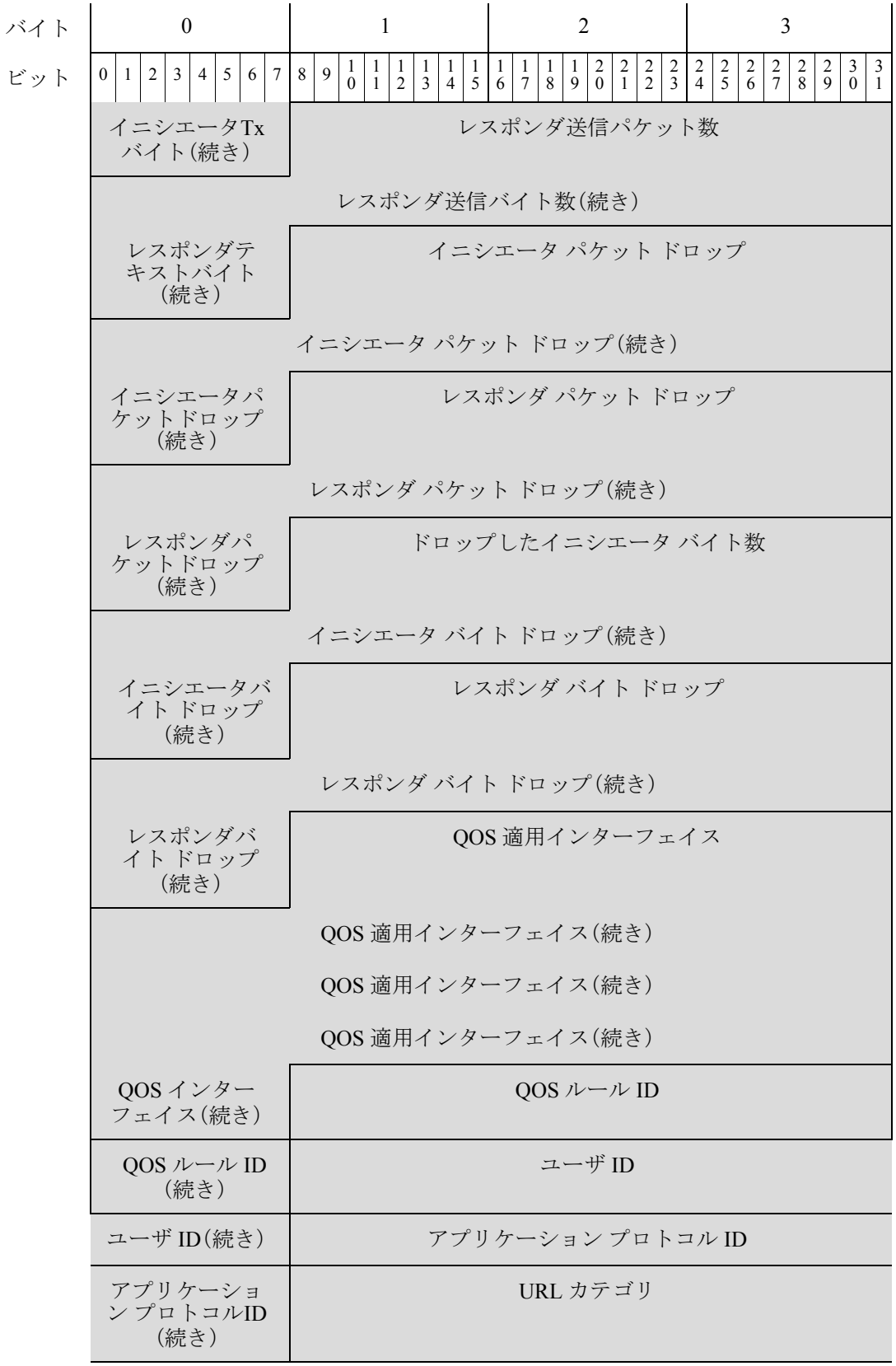
次の図は、6.1+ の接続統計データ ブロックの形式です。

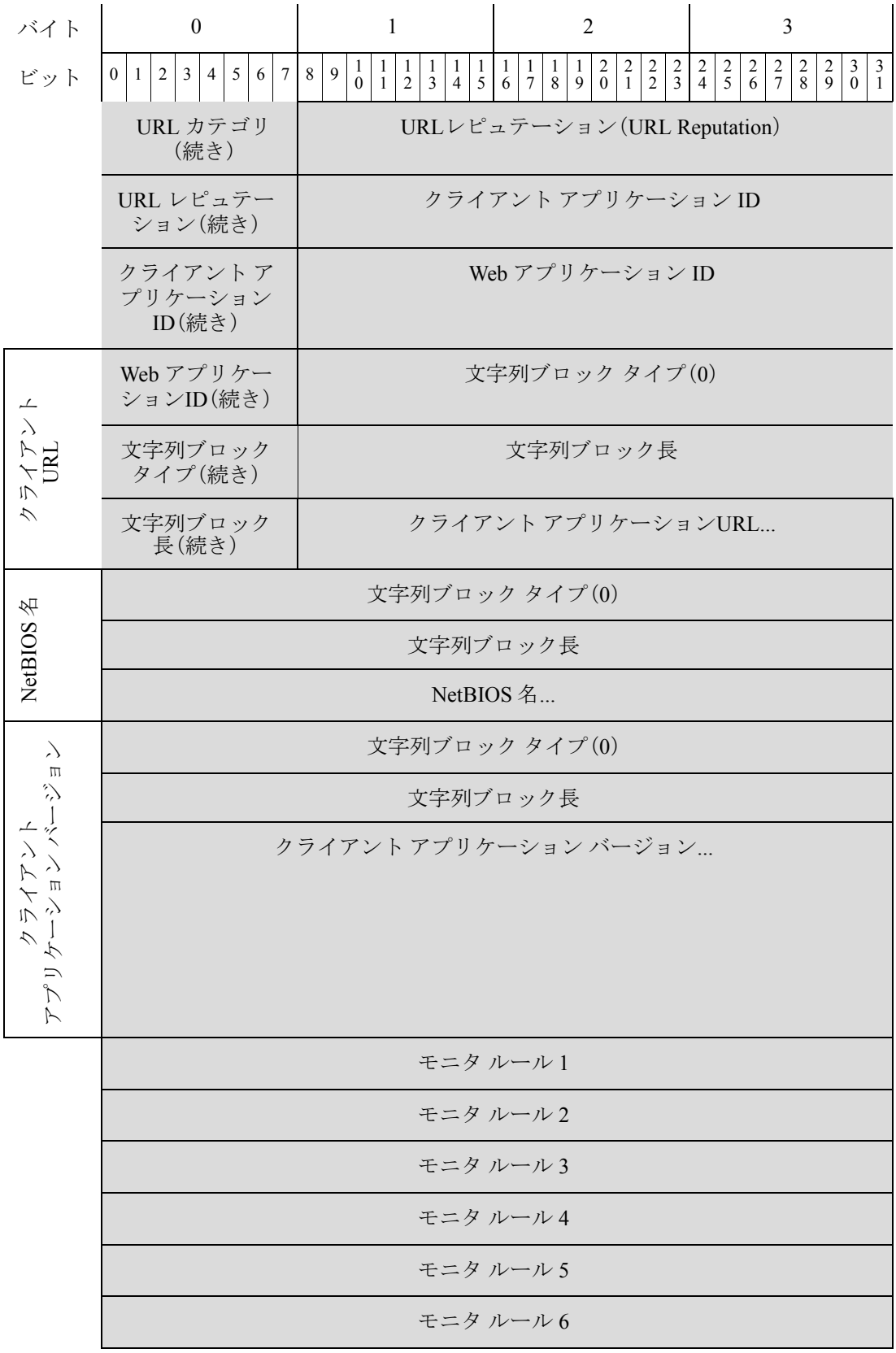
7

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続統計データ ブロック タイプ（163）																																
接続統計データ ブロック長																																
デバイスID																																
入力ゾーン 入力ゾーン（続き） 入力ゾーン（続き） 入力ゾーン（続き）																																
出力ゾーン																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出力ゾーン（続き）																																
出力ゾーン（続き）																																
出力ゾーン（続き）																																
入力インターフェイス（Ingress Interface）																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
出力インターフェイス（Egress Interface）																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
イニシエータ IP アドレス																																
イニシエータ IP アドレス（続き）																																
イニシエータ IP アドレス（続き）																																
イニシエータ IP アドレス（続き）																																
レスポンダ IP アドレス																																
レスポンダ IP アドレス（続き）																																
レスポンダ IP アドレス（続き）																																
レスポンダ IP アドレス（続き）																																
オリジナル クライアント IP アドレス																																
オリジナル クライアント IP アドレス（続き）																																
オリジナル クライアント IP アドレス（続き）																																
オリジナル クライアント IP アドレス（続き）																																
ポリシー リビジョン（Policy Revision）																																
ポリシー リビジョン（続き）																																

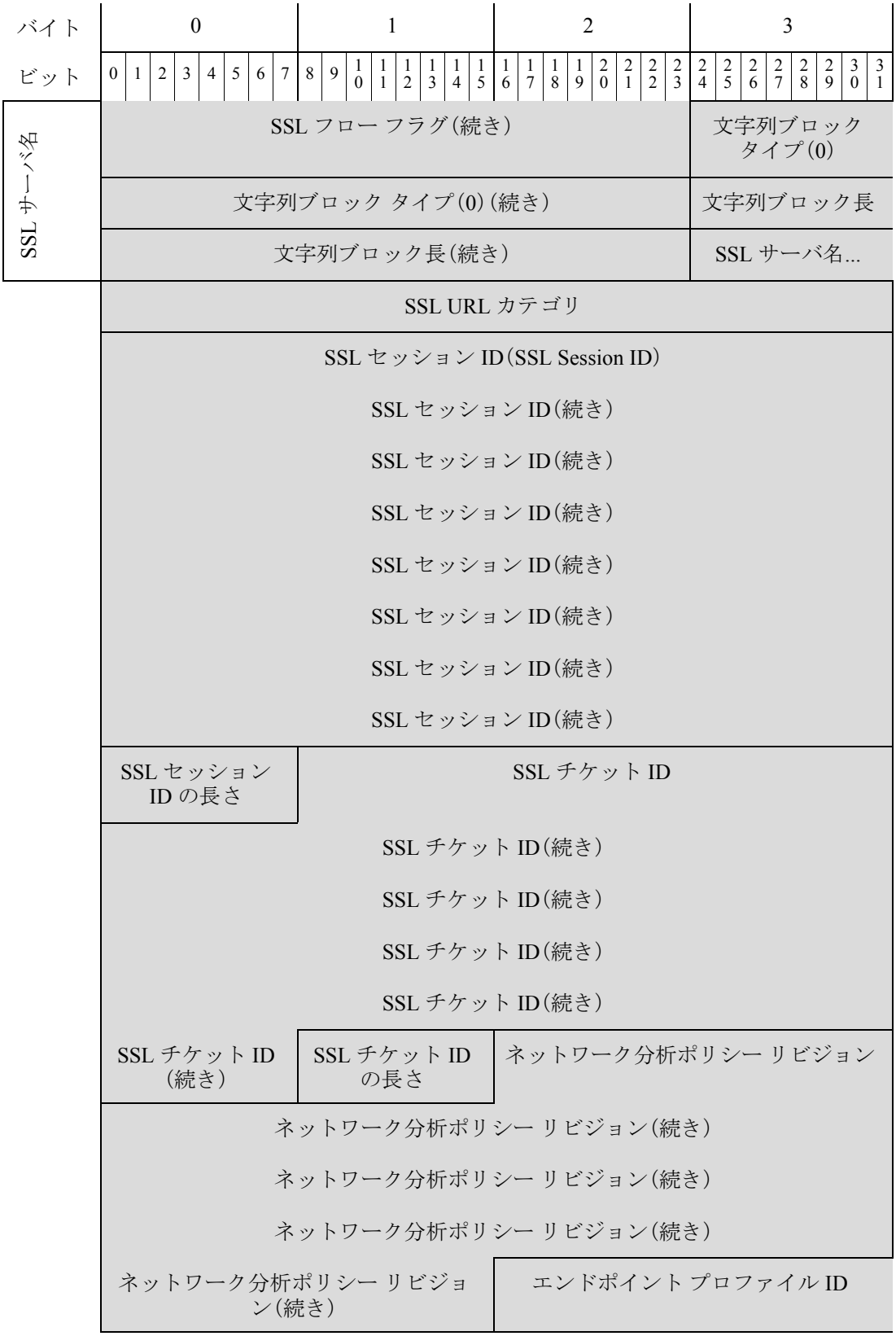

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ルール ID
トンネル ルール ID
ルール アクション(Rule Action)
ルールの理由
ルールの理由(続き)
イニシエータ ポート
レスポンダ ポート
TCP フラグ(TCP Flags)
プロトコル
NetFlow ソース
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
インスタンス ID(Instance ID)
接続数カウンタ
接続数カウンタ(続き)
最初のパケット タイムスタンプ
最初のパケット タイムスタンプ(続き)
最終パケット タイムスタンプ
最終パケット タイムスタンプ(続き)
イニシエータ送信パケット数
イニシエータ送信パケット数(続き)
イニシエータテキスト パケット(続き)
レスポンダ送信パケット数
レスポンダ送信パケット数(続き)
レスポンダテキスト パケット(続き)
イニシエータ送信バイト数
イニシエータ送信バイト数(続き)

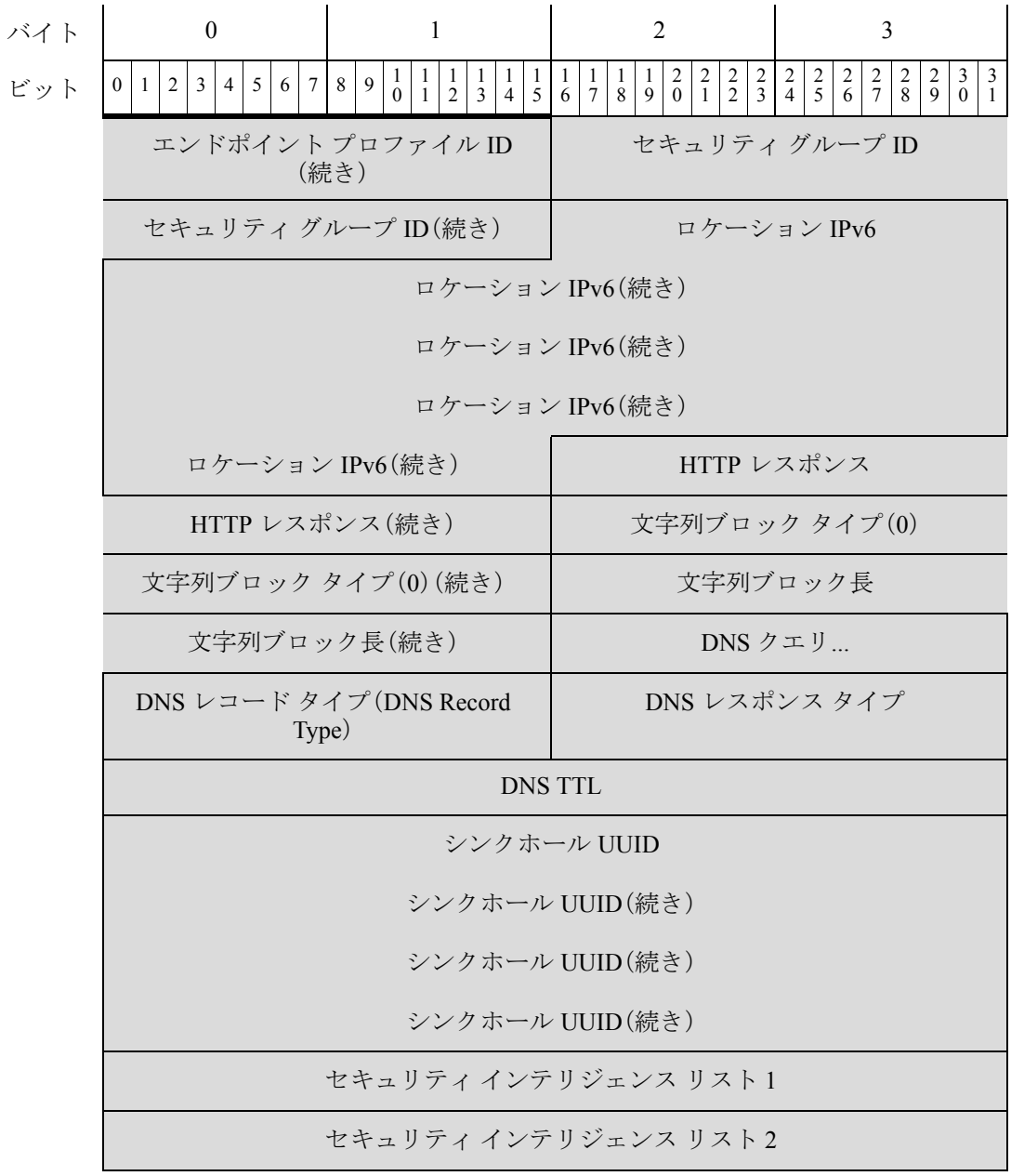

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7
8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23
24 25 26 27 28 29 30 31
イニシエータTx バイト(続き)
レスポンダ送信パケット数
レスポンダ送信バイト数(続き)
レスポンダテキストバイト(続き)
イニシエータ パケット ドロップ
イニシエータ パケット ドロップ(続き)
イニシエータパケットドロップ(続き)
レスポンダ パケット ドロップ
レスポンダ パケット ドロップ(続き)
レスポンダパケットドロップ(続き)
ドロップしたイニシエータ バイト数
イニシエータ バイト ドロップ(続き)
イニシエータバイト ドロップ(続き)
レスポンダ バイト ドロップ
レスポンダ バイト ドロップ(続き)
レスポンダバイト ドロップ(続き)
QOS 適用インターフェイス
QOS 適用インターフェイス(続き)
QOS 適用インターフェイス(続き)
QOS 適用インターフェイス(続き)
QOS インターフェイス(続き)
QOS ルール ID
QOS ルール ID(続き)
ユーザ ID
ユーザ ID(続き)
アプリケーション プロトコル ID
アプリケーション プロトコルID(続き)
URL カテゴリ


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7
8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23
24 25 26 27 28 29 30 31
URL カテゴリ（続き）
URL レピュテーション（URL Reputation）
URL レピュテーション（続き）
クライアント アプリケーション ID
クライアント アプリケーション ID（続き）
Web アプリケーション ID
クライアント URL
Web アプリケーションID（続き）
文字列ブロック タイプ（0）
文字列ブロック タイプ（続き）
文字列ブロック長
文字列ブロック長（続き）
クライアント アプリケーションURL...
NetBIOS 名
文字列ブロック タイプ（0）
文字列ブロック長
NetBIOS 名...
クライアント アプリケーション バージョン
文字列ブロック タイプ（0）
文字列ブロック長
クライアント アプリケーション バージョン...
モニタ ルール 1
モニタ ルール 2
モニタ ルール 3
モニタ ルール 4
モニタ ルール 5
モニタ ルール 6


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
モニタ ルール 7
モニタ ルール 8
秒開始送信元/宛先
秒イニシエータ層
ファイル イベント カウント
侵入イベント カウント
イニシエータの国（Initiator Country）
レスポンダの国（Responder Country）
クライアントのオリジナル国（Original Client Country）
IOC 番号
送信元自律システム
送信元自律システム（続き）
宛先自律システム
宛先自律システム
SNMP 入力
SNMP 出力
送信元 TOS
宛先 TOS
送信元マスク
宛先マスク
セキュリティ コンテキスト
セキュリティ コンテキスト
セキュリティ コンテキスト（続き）
セキュリティ コンテキスト（続き）
セキュリティ コンテキスト（続き）
VLAN ID
参照ホスト
文字列ブロック タイプ（0）
文字列ブロック長
参照ホスト...
ユーザ エージェント
文字列ブロック タイプ（0）
文字列ブロック長
ユーザ エージェント...


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
HTTP リファラ
文字列ブロック タイプ(0)
文字列ブロック長
HTTP リファラ...
SSL 証明書フィンガープリント
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL ポリシー ID
SSL ポリシー ID(続き)
SSL ポリシー ID(続き)
SSL ポリシー ID(続き)
SSL ルール ID
SSL 暗号スイート(SSL Cipher Suite)
SSL バージョン
SSL キー証明書統計
SSL キー証明書統計(続き)
実際の SSL アクション
予期された SSL アクション
予期された SSL アクション(続き)
SSL フロー ステータス
SSL フロー エラー
SSL フロー エラー(続き)
SSL フロー メッセージ
SSL フロー メッセージ(続き)
SSL フロー フラグ
SSL フロー フラグ(続き)


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL サーバ名
SSL フロー フラグ(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
SSL サーバ名...
SSL URL カテゴリ
SSL セッション ID(SSL Session ID)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID の長さ
SSL チケット ID
SSL チケット ID(続き)
SSL チケット ID(続き)
SSL チケット ID(続き)
SSL チケット ID(続き)
SSL チケット ID(続き)
SSL チケット ID の長さ
ネットワーク分析ポリシー リビジョン
ネットワーク分析ポリシー リビジョン(続き)
ネットワーク分析ポリシー リビジョン(続き)
ネットワーク分析ポリシー リビジョン(続き)
ネットワーク分析ポリシー リビジョン(続き)
エンドポイント プロファイル ID


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
エンドポイント プロファイル ID（続き）
セキュリティ グループ ID
セキュリティ グループ ID（続き）
ロケーション IPv6
ロケーション IPv6（続き）
ロケーション IPv6（続き）
ロケーション IPv6（続き）
ロケーション IPv6（続き）
HTTP レスポンス
HTTP レスポンス（続き）
文字列ブロック タイプ（0）
文字列ブロック タイプ（0）（続き）
文字列ブロック長
文字列ブロック長（続き）
DNS クエリ...
DNS レコード タイプ（DNS Record Type）
DNS レスポンス タイプ
DNS TTL
シンクホール UUID
シンクホール UUID（続き）
シンクホール UUID（続き）
シンクホール UUID（続き）
セキュリティ インテリジェンス リスト 1
セキュリティ インテリジェンス リスト 2

次の表では、6.1+ の接続統計データ ブロックのフィールドについて説明します。

表 4-70　接続統計データ ブロック 6.1+ のフィールド

フィールド	データ タイプ	説明
接続統計データ ブロック タイプ	uint32	6.1+ の接続統計データ ブロックを開始します。値は常に 163 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数（接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む）。
デバイスID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティ ゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティ ゾーン。
入力インターフェイス（Ingress Interface）	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス（Egress Interface）	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポンダ IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。
オリジナル クライアント IP アドレス	uint8[16]	要求の送信元であるプロキシの背後にあるホストの IP アドレス（オクテットの IP アドレス）。
ポリシー リビジョン（Policy Revision）	uint8[16]	トリガーされた相関イベントに関連付けられているルールのリビジョン番号（該当する場合）。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID（該当する場合）。
トンネル ルール ID	uint32	イベントにトリガーをかけたトンネル ルールの内部 ID（該当する場合）。
ルール アクション（Rule Action）	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション（allow、block など）。
ルールの理由	uint32	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポンダ ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ（TCP Flags）	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID（Instance ID）	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。

表 4-70　接続統計データ ブロック 6.1+ のフィールド(続き)

フィールド	データ タイプ	説明
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケット タイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケット タイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポンダ送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポンダ送信バイト数	uint64	応答ホストから送信バイト数。
イニシエータ パケット ドロップ	uint64	レート制限により、セッション イニシエータからドロップしたパケット数。
レスポンダ パケット ドロップ	uint64	レート制限により、セッション レスポンダからドロップしたパケット数。
ドロップしたイニシエータ バイト数	uint64	レート制限により、セッション イニシエータからドロップしたバイト数。
レスポンダ バイト ドロップ	uint64	レート制限により、セッション レスポンダからドロップしたバイト数。
QOS 適用インターフェイス	uint8[16]	レート制限された接続で、レート制限が適用されるインターフェイスの名前。
QOS ルール ID	uint32	接続に適用される QoS ルールの内部 ID 番号(該当する場合)。
ユーザ ID	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルのアプリケーション ID。
URL Category	uint32	URL カテゴリの内部 ID 番号。
URL レピュテーション(URL Reputation)	uint32	URL レピュテーションの内部 ID 番号。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロック タイプ	uint32	クライアント アプリケーション URL の文字列データ ブロックを開始します。この値は常に 0 です。

表 4-70　接続統計データ ブロック 6.1+ のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	クライアント アプリケーション URL の文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、およびクライアント アプリケーション URL 文字列のバイト数を含む)。
クライアント アプリケーション URL	string	クライアント アプリケーションがアクセスする URL(該当する場合)(`/files/index.html` など)。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に `0` です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に `0` です。
文字列ブロック長	uint32	クライアント アプリケーション バージョンの文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
クライアント アプリケーション バージョン	string	クライアント アプリケーション バージョン。
モニタ ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタ ルールの ID。
モニタ ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタ ルールの ID。
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス層	uint8	IP ブラックリストに一致した IP 層。

表 4-70　接続統計データ ブロック 6.1+ のフィールド(続き)

フィールド	データ タイプ	説明
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入イベント カウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国（Initiator Country）	uint16	開始ホストの国のコード。
レスポンダの国（Responder Country）	uint 16	応答ホストの国のコード。
クライアントのオリジナル国(Original Client Country)	uint 16	要求を開始したプロキシの背後にあるホストの国コード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。
SNMP 出力	uint16	出力インターフェイスの SNMP インデックス
送信元 TOS	uint8	着信インターフェイス用のタイプ オブ サービス バイト設定。
宛先 TOS	uint8	発信インターフェイス用のタイプ オブ サービス バイト設定。
送信元マスク	uint8	送信元アドレス プレフィックス マスク。
宛先マスク	uint8	宛先アドレス プレフィックス マスク。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
VLAN ID	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
文字列ブロック タイプ	uint32	参照ホストを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	参照ホスト文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および参照ホスト フィールドのバイト数を含む)。
参照ホスト（Referenced Host）	string	HTTP または DNS で提供されるホスト名情報。
文字列ブロック タイプ	uint32	ユーザ エージェントを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ エージェント文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ エージェント フィールドのバイト数を含む)。
ユーザ エージェント	string	セッションのユーザ エージェント ヘッダー フィールドからの情報。

表 4-70　接続統計データ ブロック 6.1+ のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	HTTP リファラを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	HTTP リファラ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および HTTP リファラ フィールドのバイト数を含む)。
HTTP リファラ(HTTP Referrer)	string	ページの発生元のサイト。これは HTTP トラフィック内の参照ヘッダー情報にあります。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
SSL ポリシー ID	uint8[16]	接続を処理した SSL ポリシーの ID 番号。
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルト アクションの ID 番号。
SSL 暗号スイート(SSL Cipher Suite)	uint16	SSL 接続で使用される暗号スイート。値は 10 進形式で保存されます。値により指定されている暗号スイートの詳細については、www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
SSL バージョン	uint8	接続の暗号化に使用された SSL または TLS プロトコル バージョン。
SSL サーバ証明書ステータス	uint16	SSL 証明書のステータス。有効な値は次のとおりです。 • 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 • 1(不明):サーバ証明書のステータスは判別できませんでした。 • 2(有効):サーバ証明書は有効です。 • 4(自己署名済み):サーバ証明書は自己署名です。 • 16(無効な発行者):サーバ証明書に無効な発行者があります。 • 32(無効な署名):サーバ証明書に無効な署名があります。 • 64(期限切れ):サーバ証明書は期限切れです。 • 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 • 256(取り消し):サーバ証明書は取り消されました。

表 4-70　接続統計データ ブロック 6.1+ のフィールド(続き)

フィールド	データ タイプ	説明
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」
予期された SSL アクション	uint16	SSL ルールに基づいて接続に対して実行する必要があるアクション。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 4-70　接続統計データ ブロック 6.1+ のフィールド(続き)

フィールド	データ タイプ	説明
SSL フロー ステータス	uint16	SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。 • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL フ ロー エ ラー	uint32	詳細な SSL エラー コード。これらの値はサポート目的で必要とされる場合があります。

表 4-70　接続統計データ ブロック 6.1+ のフィールド(続き)

フィールド	データ タイプ	説明
SSL フロー メッセージ	uint32	SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。 • 0x00000001:NSE_MT__HELLO_REQUEST • 0x00000002:NSE_MT__CLIENT_ALERT • 0x00000004:NSE_MT__SERVER_ALERT • 0x00000008:NSE_MT__CLIENT_HELLO • 0x00000010:NSE_MT__SERVER_HELLO • 0x00000020:NSE_MT__SERVER_CERTIFICATE • 0x00000040:NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080:NSE_MT__CERTIFICATE_REQUEST • 0x00000100:NSE_MT__SERVER_HELLO_DONE • 0x00000200:NSE_MT__CLIENT_CERTIFICATE • 0x00000400:NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800:NSE_MT__CERTIFICATE_VERIFY • 0x00001000: NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000:NSE_MT__CLIENT_FINISHED • 0x00004000: NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000:NSE_MT__SERVER_FINISHED • 0x00010000:NSE_MT__NEW_SESSION_TICKET • 0x00020000:NSE_MT__HANDSHAKE_OTHER • 0x00040000:NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000:NSE_MT__APP_DATA_FROM_SERVER
SSL フロー フラグ	uint64	暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。 • 0x00000001(NSE_FLOW__VALID):他のフィールドを有効にするために設定する必要があります • 0x00000002(NSE_FLOW__INITIALIZED):内部構造が処理可能です • 0x00000004(NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました
文字列ブロック タイプ	uint32	SSL サーバ名を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 4-70　接続統計データ ブロック 6.1+ のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	SSL サーバ名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および SSL サーバ名フィールドのバイト数を含む)。
SSL サーバ名	string	SSL Client Hello でサーバ名に指定された名前。
SSL URL カテゴリ	uint32	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID (SSL Session ID)	uint8[32]	クライアントとサーバがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできます。
SSL チケット ID	uint8[20]	クライアントとサーバがセッション チケットの使用に同意する場合に使用されるセッション チケットのハッシュ。
SSL チケット ID の長さ	uint8	SSL チケット ID の長さ。チケット ID は 20 バイトより長くすることはできませんが、20 バイト未満であってもかまいません。
ネットワーク分析ポリシー リビジョン	uint8[16]	接続イベントに関連付けられているネットワーク分析ポリシーのリビジョン。
エンドポイント プロファイル ID	uint32	ISE により識別される、接続エンドポイントで使用されるデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
セキュリティ グループ ID	uint32	ポリシーに基づいて ISE によりユーザに割り当てられた ID 番号。
ロケーション IPv6	uint8[16]	ISE と通信するインターフェイスの IP アドレス。IPv4 または IPv6 のアドレスを使用できます。
HTTP レスポンス	uint32	HTTP 要求の応答コード。
文字列ブロック タイプ	uint32	DNS クエリを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、および DNS クエリ文字列のバイト数を含む)。
DNS クエリ(DNS Query)	string	DNS サーバに送信されたクエリの内容。
DNS レコード タイプ(DNS Record Type)	uint16	DNS レコード タイプの数値。
DNS レスポンス タイプ	uint16	DNS 応答タイプの数値。
DNS TTL	uint32	DNS レスポンスの存続期間(秒単位)。
シンクホール UUID	uin8[16]	このシンクホール オブジェクトに関連付けられているリビジョン UUID。

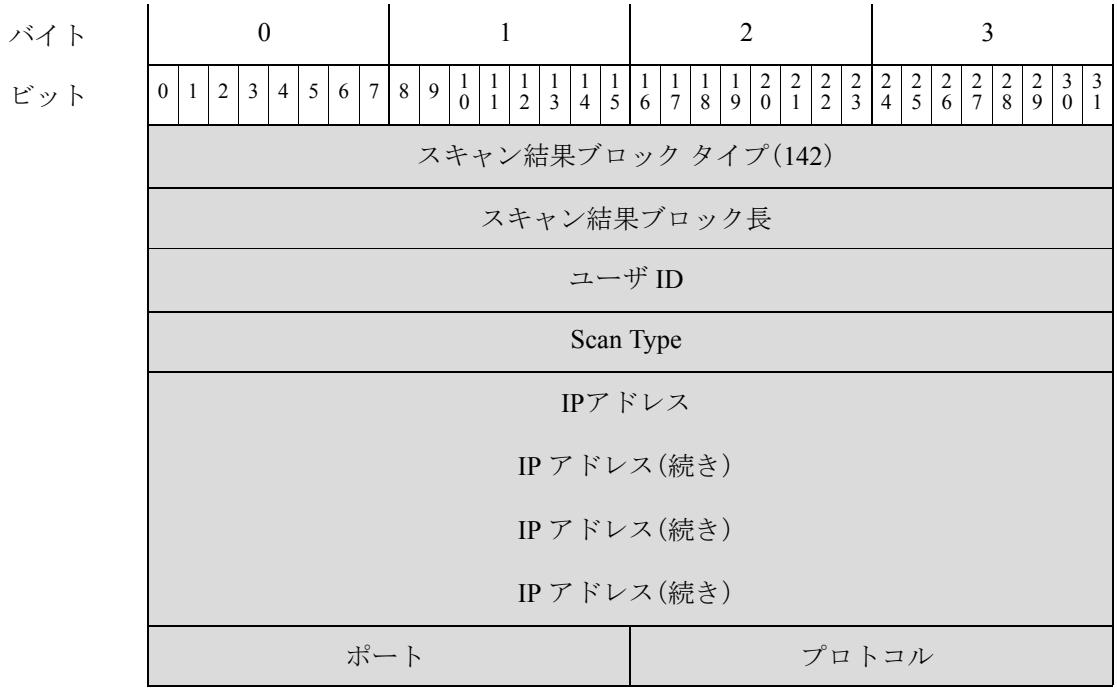
表 4-70　接続統計データ ブロック 6.1+ のフィールド(続き)

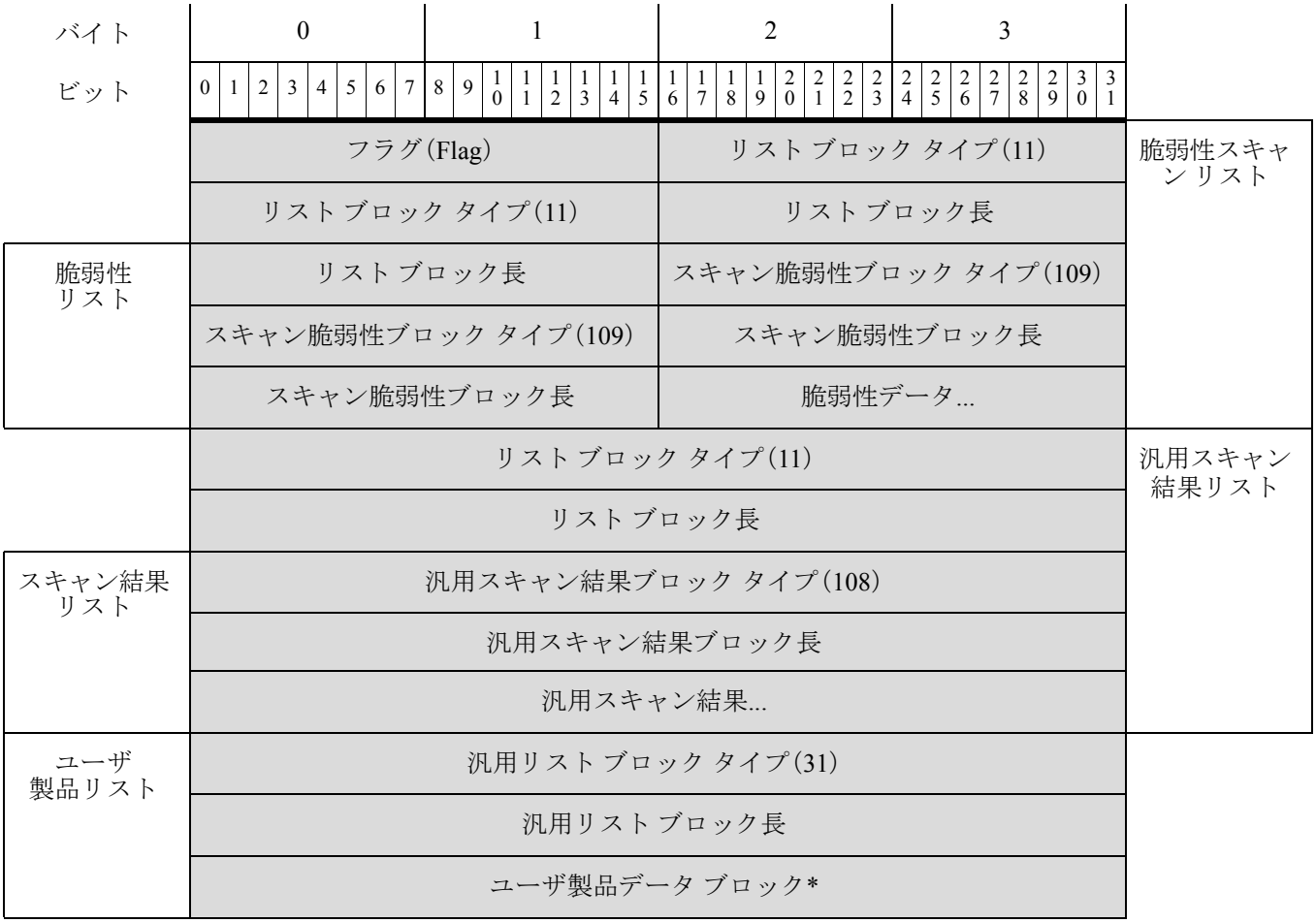
フィールド	データ タイプ	説明
セキュリティ インテリジェンス リスト 1	uint32	イベントに関連付けられているセキュリティ インテリジェンス リスト。これは、関連メタデータのセキュリティ インテリジェンス リストにマップされます。接続には、2 つのセキュリティ インテリジェンス リストが関連付けられている場合があります。
セキュリティ インテリジェンス リスト 2	uint32	イベントに関連付けられているセキュリティ インテリジェンス リスト。これは、関連メタデータのセキュリティ インテリジェンス リストにマップされます。接続には、2 つのセキュリティ インテリジェンス リストが関連付けられている場合があります。

スキャン結果データ ブロック 5.2+

スキャン結果データ ブロックは、脆弱性を説明し、スキャン結果追加イベント内で使用されます(イベント タイプ 1002、サブタイプ 11)。スキャン結果データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 142 です。これはブロック タイプ 102 に置き換わります。IP アドレス フィールドはバージョン 5.2 で 16 バイトに増えました。

次の図は、スキャン結果データ ブロックの形式を示しています。





次の表は、スキャン結果データ ブロックのフィールドについての説明です。

表 4-71　スキャン結果データ ブロックのフィールド

フィールド	データ タイプ	説明
スキャン結果ブロック タイプ	uint32	スキャン結果データ ブロックを開始します。この値は常に 142 です。
スキャン結果ブロック長	uint32	スキャン脆弱性データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン脆弱性データのバイト数を含む)。
ユーザ ID	uint32	スキャン結果をインポートしたユーザ、またはスキャン結果を生成したスキャンを実行したユーザのユーザ ID 番号が含まれます。
Scan Type	uint32	結果がシステムに追加された方法を示します。
IPアドレス	uint8[16]	IP アドレス オクテットの、結果の脆弱性によって影響を受けるホストの IP アドレス。
ポート	uint16	結果の脆弱性の影響を受ける、サブサーバで使用されるポート。

表 4-71　スキャン結果データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048:IP
フラグ(Flag)	uint16	予約済(Reserved)
リスト ブロック タイプ	uint32	トランスポート スキャン脆弱性データを伝えるスキャン脆弱性データ ブロックで構成されるリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのスキャン脆弱性データ ブロックが含まれています。 このフィールドには、ゼロ以上のスキャン脆弱性データ ブロックが続きます。
スキャン脆弱性ブロック タイプ	uint32	スキャン中に検出された脆弱性を記述するスキャン脆弱性データ ブロックを開始します。この値は常に 109 です。
スキャン脆弱性ブロック長	uint32	スキャン脆弱性データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン脆弱性データのバイト数を含む)。
脆弱性データ	string	各脆弱性に関する情報。
リスト ブロック タイプ	uint32	トランスポート スキャン脆弱性データを伝えるスキャン脆弱性データ ブロックで構成されるリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのスキャン脆弱性データ ブロックが含まれています。 このフィールドには、ゼロ以上のスキャン脆弱性データ ブロックが続きます。
汎用スキャン結果ブロック タイプ	uint32	スキャン中に検出されたサーバおよびオペレーティング システムを記述する汎用スキャン結果データ ブロックを開始します。この値は常に 108 です。
汎用スキャン結果ブロック長	uint32	汎用スキャン結果データ ブロックのバイト数(汎用スキャン結果ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン結果データのバイト数を含む)。
汎用スキャン結果データ	string	各スキャン結果に関する情報。

表 4-71　スキャン結果データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
汎用リスト ブロック タイプ	uint32	サードパーティ アプリケーションのホスト入力データを伝えるユーザ製品データ ブロックから構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのユーザ製品データ ブロックを含む)。
ユーザ製品データ ブロック*	変数	ホスト入力データを含むユーザ製品データブロック。このデータ ブロックの説明の詳細については、ユーザ製品データ ブロック 5.1+(4-177 ページ) を参照してください。

ホスト サーバ データ ブロック 4.10.0+

ホスト サーバ データ ブロックは、ホストで検出したサーバに関する情報を伝えます。ここには、検出したサーバごとにブロックとともに、サーバが実行している Web アプリケーションの Web アプリケーション データ ブロックのリストも格納します。ホスト サーバ データ ブロックは、新規と変更された TCP サーバと UDP サーバのメッセージに含まれます。詳細については、サーバ メッセージ(4-46 ページ)を参照してください。ホスト サーバ データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 103 です。

(注)　次の図で、データ ブロック名の横のアスタリスク(*)は、データ ブロックの複数のインスタンスが発生する可能性があることを示します。

次の図は、ホスト サーバ データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用リスト ブロック長																															
Web Application	Web アプリケーション ブロック タイプ(123)*																															
	Web アプリケーション ブロック長																															
	Web アプリケーション データ...																															

次の表では、ホスト サーバ データ ブロックのフィールドについて説明します。

表 4-72　ホスト サーバ データ ブロックのフィールド

フィールド	データ タイプ	説明
ホスト サーバ ブロック タイプ	uint32	ホスト サーバ データ ブロックを開始します。この値は常に 103 です。
ホスト サーバ ブロック長	uint32	ホスト サーバ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたホスト サーバ データ ブロックの合計バイト数。
ポート	uint16	サーバが実行しているポート番号。
ヒット	uint32	サーバが受信したヒット数。
前回の使用(Last Used)	uint32	システムが使用中のサーバを検出した前回時刻を表す UNIX タイムスタンプ。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リストブロックとカプセル化されたサブサーバ情報データ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
サーバ情報データ ブロック*	変数	リスト ブロック長の最大バイト数を上限としたサーバ情報データ ブロック。詳細は、4.10.x、5.0 ～ 5.0.2 のサーバ情報データ ブロック (4-149 ページ) を参照してください。
信頼度	uint32	信頼度のパーセンテージ。
汎用リスト ブロック タイプ	uint32	包括的データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	包括的ブロックとカプセル化された Web アプリケーション データ ブロックのバイト数。この数値は、カプセル化された Web アプリケーション データ ブロックすべてにバイト数と汎用リスト ブロックの 8 バイトのヘッダー フィールドを示します。
Web アプリケーション データ ブロック*	変数	リストブロック長の最大バイト数を上限としてカプセル化した Web アプリケーション データ ブロック。詳細は、5.0+の Web アプリケーション データ ブロック (4-121 ページ) を参照してください。

フル ホスト サーバ データ ブロック 4.10.0+

フル ホスト サーバ データ ブロックは、サーバ ポート、使用頻度と最新の更新、データ正確性の信頼度、シスコそのホストのサーバに関するサードパーティ脆弱性などサーバに関する情報を伝えます。フル ホスト サーバ データ ブロックには、そのサーバの各サブサーバのフル サブサーバ情報データ ブロックを格納します。各フル ホスト プロファイル データ ブロックには、ホスト上の各 TCP サーバと UDP サーバのフル ホスト サーバ データ ブロックを格納します。フル ホスト サーバ データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 104 です。

(注) 次の図で、シリーズ 1 データ ブロック名の横のアスタリスク (*) は、データ ブロックの複数のインスタンスが発生する可能性があることを示します。

次の図は、フル サーバ データ ブロックの形式です。

::

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	フル サーバ ブロック タイプ (104)																															
	フル サーバ ブロック長																															
	ポート																ヒット															
サブサーバ - シスコ	ヒット (続き)																汎用リスト ブロック タイプ (31)															
	汎用リスト ブロック タイプ (続き)																汎用リスト ブロック長															
	汎用リスト ブロック長 (続き)																フル サーバ情報データ ブロック (106)*															
サブサーバ - ユーザ	汎用リスト ブロック タイプ (31)																															
	汎用リスト ブロック長																															
	フル サーバ情報データ ブロック タイプ (106)*																															
サブサーバ - スキャナ	汎用リスト ブロック タイプ (31)																															
	汎用リスト ブロック長																															
	フル サーバ情報データ ブロック (106)*																															
サブサーバ - アプリケーション	汎用リスト ブロック タイプ (31)																															
	汎用リスト ブロック長																															
	フル サーバ情報データ ブロック (106)*																															
	信頼度																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
サーバ バナー	BLOB ブロック タイプ(10)																															
	BLOB ブロック長																															
	サーバ プローブ データ...																															
VDB 脆弱性	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	(VDB)ホスト脆弱性データ ブロック(85)*																															
サードパーティ/VDB 脆弱性	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	(サードパーティ/VDB)ホスト脆弱性データ ブロック(85)*																															
サードパーティ ホスト 脆弱性	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	(サードパーティ)ホスト脆弱性データ ブロック(85)*																															
Web アプリケーション	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	Web アプリケーション データ(123)*																															

次の表では、フル サーバ データ ブロックのコンポーネントについて説明します。

表 4-73　フル ホスト サーバ データ ブロック 4.10.0+ のフィールド

フィールド	データ タイプ	説明
フル サーバ ブロック タイプ	uint32	フル サーバ データ ブロックを開始します。この値は常に 104 です。
フル サーバ ブロック長	uint32	フル サーバ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のフル サーバ データのバイト数を加えたフル サーバ データ ブロックの合計バイト数。
ポート	uint16	サーバ ポート番号。
ヒット	uint32	サーバが受信したヒット数。
汎用リスト ブロック タイプ	uint32	検出したサブサーバ データでデータ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。

表 4-73　フル ホスト サーバ データ ブロック 4.10.0+ のフィールド(続き)

フィールド	データ タイプ	説明
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのサブサーバ情報データ ブロックを含む汎用リスト データ ブロックのバイト数。
サブサーバ情報 - シスコデータ ブロック*	変数	シスコ が検出したホスト サーバのサブサーバに関する情報を含むフル サーバ情報データ ブロック。このデータ ブロックの説明の詳細については、フル サーバ情報データ ブロック (4-151 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	ユーザが追加したサブサーバ データを伝えるサブサーバ情報データ ブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのサーバ情報データ ブロックを含む汎用リスト データ ブロックのバイト数。
サブサーバ情報 - ユーザが追加したデータ ブロック*	変数	ユーザが検出したホスト サーバのサブサーバに関する情報を含むフル サーバ情報データ ブロック。このデータ ブロックの説明の詳細については、フル サーバ情報データ ブロック (4-151 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	スキャナが追加したサブサーバ データを伝えるサブサーバ情報データ ブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのサブサーバ情報データ ブロックを含む汎用リスト データ ブロックのバイト数。
サブサーバ情報 - スキャンが追加したデータ ブロック*	変数	スキャナが検出したホスト サーバのサブサーバに関する情報を含むフル サーバ情報データ ブロック。このデータ ブロックの説明の詳細については、フル サーバ情報データ ブロック (4-151 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	アプリケーションが追加したサブサーバ データを伝えるサブサーバ情報データブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのサブサーバ情報データ ブロックを含む汎用リスト データ ブロックのバイト数。
サブサーバ情報 - アプリケーションが追加したデータ ブロック*	変数	アプリケーションが検出したホスト サーバのサブサーバに関する情報を含むフル サーバ情報データ ブロック。このデータ ブロックの説明の詳細については、フル サーバ情報データ ブロック (4-151 ページ) を参照してください。
信頼度	uint32	フル サーバ データの正しい識別における シスコ の信頼度のパーセンテージ。
BLOB ブロック タイプ	uint32	バナー データを含む BLOB データ ブロックを開始します。この値は常に 10 です。

表 4-73　フル ホスト サーバ データ ブロック 4.10.0+ のフィールド（続き）

フィールド	データ タイプ	説明
BLOB ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに、バナーのバイト数を加えた BLOB データ ブロックのバイト数。
サーバ バナー データ	byte[*n*]	パケットの最初の *n* バイトがサーバ イベントに関わるバイトであり、*n* は 256 以下です。
汎用リスト ブロック タイプ	uint32	シスコ 脆弱性データを搬送するホスト脆弱性データ ブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのホスト脆弱性データ ブロックを含む汎用リスト データ ブロックのバイト数。
（VDB）ホスト脆弱性データ ブロック*	変数	脆弱性データベース（VDB）でホスト脆弱性に関する情報を格納したホスト脆弱性データ ブロック。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+（4-116 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	サードパーティ スキャナから得られた サードパーティ ホスト脆弱性データを搬送し、VDB に登録済みの脆弱性情報を含むホスト脆弱性データ ブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのホスト脆弱性データ ブロックを含む汎用リスト データ ブロックのバイト数。
（サード パーティ/VDB）ホスト脆弱性データ ブロック*	変数	サードパーティ スキャナで得られ、脆弱性データベース（VDB）に登録されているホスト脆弱性に関する情報を格納したホスト脆弱性データ ブロック。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+（4-116 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	サードパーティ スキャナで生成したサードパーティ ホスト脆弱性データを伝えるホスト脆弱性データ ブロックで構成される汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのホスト脆弱性データ ブロックを含む汎用リスト データ ブロックのバイト数。
サードパーティ スキャン ホスト脆弱性データ ブロック*	変数	サードパーティ スキャナで識別済みでも VDB には登録されていないサードパーティ脆弱性データを含むホスト脆弱性データ ブロック。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+（4-116 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。

表 4-73　フル ホスト サーバ データ ブロック 4.10.0+ のフィールド(続き)

フィールド	データ タイプ	説明
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化された Web アプリケーション データ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
Web アプリケーション データ ブロック*	変数	リスト ブロック長の最大バイト数を上限としてカプセル化した Web アプリケーション データ ブロック。

4.10.x、5.0 ～ 5.0.2 のサーバ情報データ ブロック

サーバ情報データ ブロックは、サーバ ID、サーバ ベンダーとバージョン、送信元情報など、サーバに関する情報を伝えます。サーバ情報データ ブロックのブロック タイプは、4.10.x のシリーズ 1 ブロック グループのブロック タイプ 105 と、5.0 ～ 5.0.2 のシリーズ 1 ブロック グループのブロック タイプ 117 です。サーバ情報データ ブロックは、ホスト サーバ ブロックとフル ホスト サーバ データ ブロックのリストで搬送されます。詳細については、ホスト サーバ データ ブロック 4.10.0+(4-143 ページ) と フル ホスト サーバ データ ブロック 4.10.0+(4-145 ページ) を参照してください。

次の図は、サーバ情報データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
サブサーバ	サブサーバ ブロック タイプ(1)*																															
	サブサーバ ブロック長																															
	サブサーバ データ...																															

次の表では、サーバ情報データ ブロックのコンポーネントについて説明します。

表 4-74　サーバ情報データ ブロックのフィールド

フィールド	データ タイプ	説明
サーバ情報ブロック タイプ	uint32	サーバ情報データ ブロックを開始します。ブロック タイプは 4.10.x の場合、105、5.0+ の場合、117 です。
サーバ情報ブロック長	uint32	サーバ情報データ ブロックの合計バイト数。サーバ情報ブロック タイプ フィールドと長さフィールドの 8 バイト、サーバ ID の 4 バイト、ベンダー名ブロック タイプと長さの 8 バイト、ベンダー名にさらに 4 バイト、バージョン文字列ブロック タイプと長さに 8 バイト、バージョン文字列にさらに 4 バイト、最後に使用する送信元タイプと送信元 ID フィールドごとに 4 バイトで構成します。
アプリケーション ID	uint32	検出したサーバで実行しているアプリケーション プロトコルのアプリケーション ID。
文字列ブロック タイプ	uint32	サーバ ベンダー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにサーバ ベンダー名のバイト数を加えたベンダー名文字列データ ブロックのバイト数。
サーバ ベンダー名	string	サーバ ベンダーの名前。
文字列ブロック タイプ	uint32	サーバ バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにサーバ バージョンのバイト数を加えたサーバ バージョン文字列データ ブロックのバイト数。
サーバ バージョン	string	サーバ バージョン
前回使用時刻	uint32	トラフィックで前回サーバ情報を使用した時刻を示します。

表 4-74　サーバ情報データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答(RNA) がサーバ データを提供した場合、0 • ユーザがサーバ データを提供した場合、1 • サードパーティ スキャナがサーバ データを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでサーバ データを提供した場合、3
ソース ID	uint32	サーバ データの送信元にマッピングするID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
リスト ブロック タイプ	uint32	サブサーバ データ ブロック リストを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のカプセル化されたサブサーバ データブロックのバイト数を加えたリスト データ ブロックの合計バイト数。
サブサーバ ブロック タイプ	uint32	最初のサブサーバ データ ブロックを開始します。このデータ ブロックには、他のサブサーバ データ ブロックを、リスト ブロック長フィールドで定義した上限まで続けることができます。
サブサーバ ブロック長	uint32	サブサーバ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えた各サブサーバ データ ブロックの合計バイト数。
サブサーバ データ	変数	サブサーバ データ ブロック (4-76 ページ) に記載のサブサーバ データ。

フル サーバ情報データ ブロック

フル サーバ情報データ ブロックは、サブサーバのアプリケーション プロトコル、ベンダー、バージョン、関連サブサーバなど、ホストで検出したサーバに関する情報を伝えます。サブサーバごとに、情報は、フル サブサーバデータ ブロックに格納します(フル サブサーバ データ ブロック (4-85 ページ) を参照)。フル サーバ情報データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 106 です。

(注)　次の図で、シリーズ 1 データ ブロック名の横のアスタリスク (*) は、データ ブロックの複数のインスタンスが発生する可能性があることを示します。

次の図は、フル サーバ情報データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	フル サーバ ブロック タイプ（106）																															
	フル サーバ ブロック長																															
	アプリケーション プロトコル ID																															
ベンダー	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ベンダー名文字列...																															
バージョン	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	バージョン文字列...																															
	前回の使用（Last Used）																															
	ソース タイプ																															
	ソース ID																															
	リスト ブロック タイプ（11）																															
	リスト ブロック長																															
サブサーバ	フル サブサーバ ブロック タイプ（51）*																															
	フル サブサーバ ブロック長																															
	フル サブサーバ データ...																															

次の表では、フル サーバ情報データ ブロックのコンポーネントについて説明します。

表 4-75　フル サーバ情報データ ブロックのフィールド

フィールド	データ タイプ	説明
フル サーバ情報ブロック タイプ	uint32	フル サーバ情報データ ブロックを開始します。この値は常に 106 です。
フル サーバ情報ブロック長	uint32	フル サーバ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のフル サーバ データのバイト数を加えたフル サーバ情報データ ブロックの合計バイト数。

表 4-75　フル サーバ情報データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
アプリケーション プロトコル ID	uint32	サーバで実行しているアプリケーション プロトコルのアプリケーション ID。
文字列ブロック タイプ	uint32	アプリケーション プロトコル ベンダー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにベンダー名のバイト数を加えたベンダー名文字列データ ブロックのバイト数。
ベンダー名	string	サーバ ベンダーの名前。
文字列ブロック タイプ	uint32	アプリケーション プロトコル バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにバージョンのバイト数を加えた文字列データ ブロックのバイト数。
バージョン	string	サーバのバージョン。
前回の使用(Last Used)	uint32	システムが使用中のサーバを検出した前回時刻を表す UNIX タイムスタンプ。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答(RNA) がサーバ データを提供した場合、0 • ユーザがサーバ データを提供した場合、1 • サードパーティ スキャナがクライアント データを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでサーバ データを提供した場合、3
ソース ID	uint32	サーバ データの送信元にマッピングするID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
リスト ブロック タイプ	uint32	サブサーバ データを伝えるフル サーバ情報データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのフル サブサーバ データ ブロックを加えた値です。 このフィールドの後にはゼロか、さらにフル サブサーバ データ ブロックが続きます。
フル サブサーバ ブロック タイプ	uint32	最初のフル サブサーバ データ ブロックを開始します。このデータ ブロックには、他のフル サブサーバ データ ブロックを、リスト ブロック長フィールドで定義した上限まで続けることができます。

表 4-75　フル サーバ情報データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
フル サブサーバ ブロック長	uint32	フル サブサーバ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えた各フル サブサーバ データ ブロックの合計バイト数。
フル サブサーバ データ ブロック*	uint32	このサーバのサブサーバを含むフル サブサーバ データ ブロック。このデータ ブロックの説明の詳細については、フル サブサーバ データ ブロック (4-85 ページ) を参照してください。

4.10.0+ の汎用スキャン結果データ ブロック

汎用スキャン結果データ ブロックにはスキャン結果が格納され、次の表では、6.1+ の接続統計データ ブロックのフィールドについて説明します。(4-131 ページ) で使用します。汎用スキャン結果データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 108 です。

次の図は、汎用スキャン結果データ ブロックの基本構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用スキャン結果データ ブロック タイプ(108)																															
	汎用スキャン結果ブロック長																															
	ポート																プロトコル															
スキャン結果サブサーバ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	スキャン結果サブサーバ文字列...																															
スキャン結果値	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	スキャン結果値...																															
スキャン結果サブサーバ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	スキャン結果サブサーバ(不定様式)文字列...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
スキャン結果値	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	スキャン結果値...																															

次の表では、汎用スキャン結果データ ブロックのフィールドについて説明します。

表 4-76　汎用スキャン結果データ ブロックのフィールド

フィールド	バイト数	説明
汎用スキャン結果データ ブロック タイプ	uint32	汎用スキャン結果データ ブロックを開始します。この値は常に 108 です。
汎用スキャン結果ブロック長	uint32	汎用スキャン結果ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のスキャン結果データのバイト数を加えた汎用スキャン結果データ ブロックの合計バイト数。
ポート	uint16	結果の脆弱性による影響を受けたサーバが使用するポート。
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048:IP
文字列ブロック タイプ	uint32	サブサーバを格納した文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにサブサーバのバイト数を加えたサブサーバ文字列データ ブロックのバイト数。
スキャン結果サブサーバ	string	サブサーバ。
文字列ブロック タイプ	uint32	値を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに値のバイト数を加えた値文字列データ ブロックのバイト数。
スキャン結果値	string	スキャン結果値。
文字列ブロック タイプ	uint32	サブサーバを格納した文字列データ ブロックを開始します。この値は常に 0 です。

表 4-76　汎用スキャン結果データ ブロックのフィールド(続き)

フィールド	バイト数	説明
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにサブサーバのバイト数を加えたサブサーバ文字列データ ブロックのバイト数。
スキャン結果サブサーバ	string	サブサーバ(不定様式)。
文字列ブロック タイプ	uint32	値を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに値のバイト数を加えた値文字列データ ブロックのバイト数。
スキャン結果値	string	スキャン結果値(不定様式)。

4.10.0+のスキャン脆弱性データ ブロック

スキャン脆弱性データ ブロックは、脆弱性を記述し、スキャン結果データ ブロックで使用します。そのスキャン結果データ ブロックは、追加スキャン結果イベント(イベント タイプ 100 2、サブタイプ 11)で使用します。詳細については、次の表では、6.1+ の接続統計データ ブロックのフィールドについて説明します。(4-131 ページ)およびスキャン結果を追加メッセージ(4-60 ページ)を参照してください。スキャン脆弱性データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 109 です。

次の図は、スキャン脆弱性データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	スキャン脆弱性ブロック タイプ(109)																															
	スキャン脆弱性ブロック長																															
	ポート																プロトコル															
ID	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ID																															
名前	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	脆弱性名...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	説明...																															
名前クリーン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	脆弱性名クリーン...																															
記述クリーン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	記述クリーン...																															
Bugtraq ID	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	整数型データ ブロック(Bugtraq ID)...																															
CVE ID	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	CVE ID...																															

次の表では、スキャン脆弱性データ ブロックのフィールドについて説明します。

表 4-77　スキャン脆弱性データ ブロックのフィールド

フィールド	データ タイプ	説明
スキャン脆弱性ブロック タイプ	uint32	スキャン脆弱性データ ブロックを開始します。この値は常に 109 です。
スキャン脆弱性ブロック長	uint32	スキャン脆弱性データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン脆弱性データのバイト数を含む)。
ポート	uint16	脆弱性の影響を受けるサブサーバで使用するポート。

表 4-77　スキャン脆弱性データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048:IP
文字列ブロック タイプ	uint32	ID を含む文字列データ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、ID のバイト数を加えた ID の文字列データ ブロックのバイト数。
ID	string	脆弱性を検出したスキャン ユーティリティの指定に従って報告されたその脆弱性の ID。Qualys スキャンで検出した脆弱性の場合、たとえばこのフィールドには Qualys ID が設定されます。
文字列ブロック タイプ	uint32	脆弱性名を含むデータ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、脆弱性名のバイト数を加えた、脆弱性名の文字列データ ブロックの合計バイト数。
名前	string	脆弱性の名前。
文字列ブロック タイプ	uint32	脆弱性記述文字列データ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、脆弱性の記述のバイト数を加えた、脆弱性の記述の文字列データ ブロックの合計バイト数。
説明	string	脆弱性の記述。
文字列ブロック タイプ	uint32	脆弱性名を含むデータ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、脆弱性名のバイト数を加えた、脆弱性名の文字列データ ブロックの合計バイト数。
名前クリーン	string	脆弱性の名前(不定様式)。
文字列ブロック タイプ	uint32	脆弱性記述文字列データ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、脆弱性の記述のバイト数を加えた、脆弱性の記述の文字列データ ブロックの合計バイト数。
記述クリーン	string	脆弱性の記述(不定様式)。
リスト ブロック タイプ	uint32	Bugtraq ID 番号のリストのリスト データ ブロックを開始します。

表 4-77　スキャン脆弱性データ ブロックのフィールド（続き）

フィールド	データ タイプ	説明
リスト ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、Bugtraq ID を格納した整数型データのバイト数を加えた、Bugtraq ID 番号のリスト データ ブロックの合計バイト数。
Bugtraq ID	string	Bugtraq ID 番号のリストを形成するゼロ以上の Bugtraq（INT32）データ ブロック。これらのデータ ブロックの詳細については、整数型（INT32）データ ブロック（4-79 ページ）を参照してください。
リスト ブロック タイプ	uint32	Common Vulnerability Exposure（CVE）のリストのリスト データ ブロックを開始します。
リスト ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、CVE ID 番号のバイト数を加えた CVE ID 番号のリスト データ ブロックのバイト数。
CVE ID	string	CVE ID 番号のリストを形成するゼロ以上の文字列情報データ ブロック。これらのデータ ブロックの詳細については、文字列情報データ ブロック（4-81 ページ）を参照してください。

フル クライアント アプリケーション データ ブロック 5.0+

バージョン 5.0 + のフル ホスト クライアント アプリケーション データ ブロックは、クライアント アプリケーションと、合わせて、関連 Web アプリケーションと脆弱性の添付リストを記述します。フル ホスト クライアント アプリケーション データ ブロックは、フル ホスト プロファイル データ ブロック（111）内で使用します。このブロック タイプは シリーズ 1 ブロック グループのブロック タイプ 112 です。

次の図は、5.0+ のフル ホスト クライアント アプリケーション データ ブロックの基本構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	フル ホスト クライアント アプリケーション ブロック タイプ（112）																															
	フル ホスト クライアント アプリケーション ブロック長																															
	ヒット																															
	前回の使用（Last Used）																															
	アプリケーション ID																															
バージョン	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	バージョン...																															

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
Web アプリケーション	Web アプリケーション ブロック タイプ(123)*																																
	Web アプリケーション ブロック長																																
	Web アプリケーション データ...																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
脆弱性	脆弱性ブロック タイプ(85)*																																
	脆弱性ブロック長																																
	脆弱性データ...																																

次の表では、フル ホスト クライアント アプリケーション データ ブロックのフィールドについて説明します。

表 4-78　フル ホスト クライアント アプリケーション データ ブロック 5.0+ のフィールド

フィールド	データ タイプ	説明
フル ホスト クライアント アプリケーション ブロック タイプ	uint32	フル ホスト クライアント アプリケーション データ ブロックを開始します。この値は常に 112 です。
フル ホスト クライアント アプリケーション ブロック長	uint32	クライアント アプリケーション ブロック タイプと長さの 8 バイトに、後続のクライアント アプリケーション データのバイト数を加えたフル ホスト クライアント アプリケーション データ ブロックの合計バイト数。
ヒット	uint32	システムが使用中のクライアント アプリケーションを検出した回数。
前回の使用(Last Used)	uint32	システムが使用中のクライアントを検出した前回時刻を表す UNIX タイムスタンプ。
アプリケーション ID	uint32	検出したクライアント アプリケーションのアプリケーション ID(該当する場合)。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。

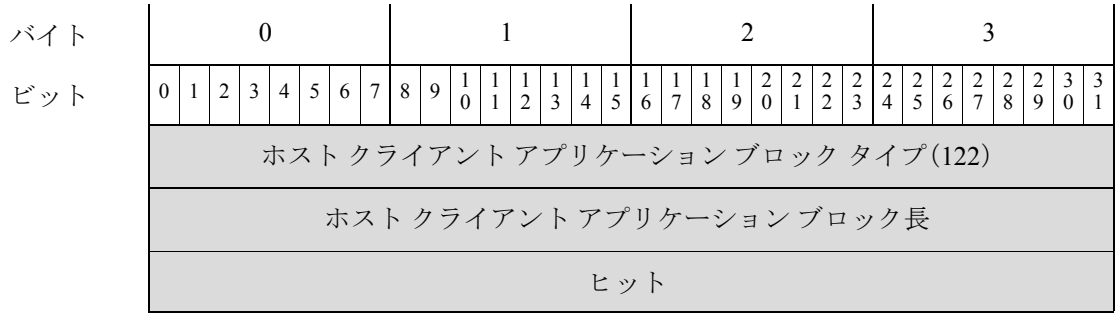
表 4-78　フル ホスト クライアント アプリケーション データ ブロック 5.0+ のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、クライアント アプリケーション バージョンのバイト数を加えたクライアント アプリケーション名の文字列データ ブロックのバイト数。
バージョン	string	クライアント アプリケーション バージョン。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化された Web アプリケーション データ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
Web アプリケーション データ ブロック	変数	汎用リスト ブロック長の最大バイト数を上限としてカプセル化した Web アプリケーション データ ブロック。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化された脆弱性データ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべての脆弱性データ ブロックのバイト数を加えた値です。
脆弱性データ ブロック	変数	汎用リスト ブロック長の最大バイト数を上限としてカプセル化した脆弱性データ ブロック。

5.0+ のホスト クライアント アプリケーション データ ブロック

5.0+ のホスト クライアント アプリケーション データ ブロックは、クライアント アプリケーションを記述し、新規クライアント アプリケーション イベント(イベント タイプ 1000、サブタイプ 7)、クライアント アプリケーション タイムアウト イベント(イベント タイプ 1001、サブタイプ 20)、クライアント アプリケーション更新イベント(イベント タイプ 1001、サブタイプ 32)で使用します。4.10.2+ のホスト クライアント アプリケーション データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 122 です。

次の図は、5.0+ のホスト クライアント アプリケーション データ ブロックの基本構造です。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	前回の使用（Last Used）																															
	ID																															
	アプリケーション プロトコル ID																															
バージョン	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	バージョン...																															
	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
Web アプリケーション	Web アプリケーション ブロック タイプ（123）*																															
	Web アプリケーション ブロック長																															
	Web アプリケーション データ...																															

次の表では、ホスト クライアント アプリケーション データ ブロックのフィールドについて説明します。

表 4-79　ホスト クライアント アプリケーション データ ブロックのフィールド

フィールド	データ タイプ	説明
クライアント アプリケーション ブロック タイプ	uint32	ホスト クライアント アプリケーション データ ブロックを開始します。この値は常に 122 です。
クライアント アプリケーション ブロック長	uint32	クライアント アプリケーション ブロック タイプと長さの 8 バイトに、後続のクライアント アプリケーション データのバイト数を加えたクライアント アプリケーション データ ブロックの合計バイト数。
ヒット	uint32	システムが使用中のクライアント アプリケーションを検出した回数。
前回の使用（Last Used）	uint32	システムが使用中のクライアントを検出した前回時刻を表す UNIX タイムスタンプ。
ID	uint32	検出したクライアント アプリケーションの ID 番号（該当する場合）。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルの内部 ID 番号（該当する場合）。

表 4-79　ホスト クライアント アプリケーション データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、クライアント アプリケーション バージョンのバイト数を加えたクライアント アプリケーション バージョンの文字列データ ブロックのバイト数。
バージョン	string	クライアント アプリケーション バージョン。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化された Web アプリケーション データ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
Web アプリケーション データ ブロック	変数	リスト ブロック長の最大バイト数を上限としてカプセル化した Web アプリケーション データ ブロック。カプセル化されたデータ ブロック(ブロック タイプ 123)については、5.0+の Web アプリケーション データ ブロック(4-121 ページ)を参照してください。

ユーザ脆弱性データ ブロック 5.0+

ユーザ脆弱性データ ブロックは、脆弱性について記述し、ユーザ脆弱性変更ブロック内で使用します。さらに、ユーザ脆弱性変更ブロックはユーザ設定有効脆弱性イベントとユーザ設定無効脆弱性イベントで使用します。5.0+ のユーザ脆弱性データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 124 です。これはブロック タイプ 79 に置き換わります。ユーザ脆弱性変更データ ブロックの詳細については、ユーザ脆弱性変更データ ブロック 4.7+(4-110 ページ)を参照してください。

次の図は、ユーザ脆弱性変更データ ブロックの形式です。

次の表では、ユーザ脆弱性データ ブロックのフィールドについて説明します。

表 4-80　ユーザ脆弱性データ ブロックのフィールド

フィールド	データ タイプ	説明
ユーザ脆弱性ブロック タイプ	uint32	ユーザ脆弱性データ ブロックを開始します。この値は常に 124 です。
ユーザ脆弱性ブロック長	uint32	ユーザ脆弱性ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザ脆弱性データのバイト数を加えたユーザ脆弱性データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リスト データ ブロックのバイト数。
IP 範囲仕様データ ブロック*	変数	ユーザ入力からの IP アドレス範囲。このデータ ブロックの説明の詳細については、5.2+の IP アドレス範囲データ ブロック（4-98 ページ）を参照してください。

表 4-80　ユーザ脆弱性データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
ポート	uint16	脆弱性の影響を受けるサーバで使用するポート。クライアント アプリケーション脆弱性の場合、値は 0 です。
プロトコル	uint16	このブロックには、フィンガープリント Universally Unique Identifier(UUID)の他、フィンガープリント タイプ、フィンガープリント送信元タイプ、フィンガープリント送信元 ID を格納します。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048:IP クライアント アプリケーション脆弱性の場合、値は 0 です。
脆弱性 ID	uint32	シスコ 脆弱性 ID。
サードパーティ脆弱性 UUID	uint8 [16]	指定する場合は、サードパーティ脆弱性の固有 ID 番号。そうでない場合、この値は0 です。
文字列ブロック タイプ	uint32	脆弱性名を含むデータ ブロックを開始します。値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、脆弱性名のバイト数を加えた、脆弱性名の文字列データ ブロックの合計バイト数。
脆弱性名	string	脆弱性名
クライアント アプリケーション ID	uint32	クライアント アプリケーションのアプリケーション ID。シングルモードの場合、この値は 0 になります。
アプリケーション プロトコル ID	uint32	クライアント アプリケーションで使用しているアプリケーション プロトコルのアプリケーション ID。シングルモードの場合、この値は 0 になります。
文字列ブロック タイプ	uint32	バージョン文字列を含む文字列データ ブロックを開始します。値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、クライアント アプリケーション バージョン文字列のバイト数を加えた文字列データ ブロックのバイト数。
バージョン	string	クライアント アプリケーション バージョン。シングルモードの場合、この値は 0 になります。

オペレーティング システム フィンガープリント データ ブロック 5.1+

オペレーティング システム フィンガープリント データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 130 です。このブロックには、フィンガープリント Universally Unique Identifier（UUID）の他、フィンガープリント タイプ、フィンガープリント送信元タイプ、フィンガープリント送信元 ID を格納します。

次の図は、5.1+ のオペレーティング システム フィンガープリント データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	オペレーティング システム フィンガープリント ブロック タイプ（130）																															
	オペレーティング システム フィンガープリント ブロック長																															
OS フィンガープリント UUID	フィンガープリント UUID フィンガープリント UUID（続き） フィンガープリント UUID（続き） フィンガープリント UUID（続き）																															
	フィンガープリント タイプ																															
	フィンガープリント ソース タイプ																															
	フィンガープリント ソース ID																															
	最後の確認日時																															
モバイル デバイス 情報	TTL 差異								汎用リスト ブロック タイプ（31）																							
	汎用リスト ブロック タイプ（続き）								汎用リスト ブロック長																							
	汎用リスト ブロック長（続き）								モバイル デバイス 情報データ ブロック*																							

次の表では、オペレーティング システムフィンガープリント データ ブロックのフィールドについて説明します。

表 4-81　オペレーティング システム フィンガープリント データ ブロックのフィールド

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント データ ブロック タイプ	uint32	オペレーティング システム データ ブロックを開始します。この値は常に 130 です。
オペレーティング システム データ ブロック長	uint32	オペレーティング システム フィンガープリント データ ブロック タイプと長さの 8 バイトに、後続のオペレーティング システム フィンガープリント データのバイト数を加えたオペレーティング システム フィンガープリント データ ブロックのバイト数。
フィンガープリント UUID	uint8[16]	オペレーティング システムの固有識別子として機能するフィンガープリントID 番号（オクテット）。フィンガープリント UUID は、脆弱性データベース（VDB）内のオペレーティング システム名、ベンダー、バージョンにマップされます。
フィンガープリント タイプ	uint32	フィンガープリントのタイプを示します。
フィンガープリント ソース タイプ	uint32	オペレーティング システム フィンガープリントを提供するソースのタイプ（ユーザやスキャナ）を示します。
フィンガープリント ソース ID	uint32	ID 番号。オペレーティング システム フィンガープリントを提供したユーザのログイン名にマップします。
最後の確認日時	uint32	トラフィックで前回フィンガープリントを確認した時刻を示します。
TTL 差異	uint8	フィンガープリントの TTL 値とホストにフィンガープリントを実行するときに使用するパケット上の TTL 値との差を示します。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
モバイル デバイス 情報データ ブロック	変数	リスト ブロック長の最大バイト数を上限としてカプセル化したモバイル デバイス 情報データ ブロック。このデータ ブロックの説明の詳細については、5.1+ デバイス のモバイル情報データ ブロック（4-168 ページ） を参照してください。

5.1+ デバイス のモバイル情報データ ブロック

次の図は、モバイル デバイス 情報データ ブロックの形式です。このデータ ブロックには、ホストを前回検出した時刻、モバイル デバイス情報、そのモバイル デバイスが改造されていないかどうかに関する情報を格納します。モバイル デバイス 情報データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 131 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	モバイル デバイス 情報ブロック タイプ(131)																															
	モバイル デバイス 情報ブロック長																															
モバイル デバイス データ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	モバイル デバイス 文字列データ...																															
	モバイル デバイス 最後の確認日時																															
	モバイル																															
	改造																															

ここでは、5.1+ で返るモバイル デバイス 情報データ ブロックを記述します。

表 4-82　モバイル デバイス 情報データ ブロック 5.1+ のフィールド

フィールド	データ タイプ	説明
モバイル デバイス 情報ブロック タイプ(131)	uint32	オペレーティング システム データ ブロックを開始します。この値は常に 131 です。
モバイル デバイス 情報ブロック長	uint32	モバイル デバイス 情報データ ブロック タイプと長さの 8 バイトに、後続のモバイル デバイス 情報データのバイト数を加えたモバイル デバイス 情報データ ブロックのバイト数。
文字列ブロック タイプ	uint32	モバイル デバイス文字列を含む文字列データ ブロックを開始します。この値は文字列データを表す 0 に設定されます。
文字列ブロック長	uint32	文字列ブロック タイプ フィールドと長さフィールドの 8 バイトに、モバイル デバイス文字列データのバイト数を加えたモバイル デバイス文字列データ ブロックのバイト数を示します。
モバイル デバイス 文字列データ	変数	検出したホストのモバイル デバイスのハードウェア情報を格納します。

表 4-82　モバイル デバイス 情報データ ブロック 5.1+ のフィールド(続き)

フィールド	データ タイプ	説明
モバイル デバイス 最後の確認日時	uint32	モバイル デバイスを最後の確認日時した時刻のタイムスタンプを格納します。
モバイル	uint32	検出したホストがモバイル デバイスであるかどうかを示す true/false フラグ。
改造	uint32	ホストが改造したモバイル デバイスであるかどうかを示す true/false フラグ。

ホスト プロファイル データブロック 5.2+

次の図は、ホスト プロファイル データ ブロックの形式を示しています。さらに、このデータ ブロックには、ホスト重要度値が含まれていませんが、VLAN プレゼンス インジケータは含まれています。さらに、このデータ ブロックは、ホストの NetBIOS 名を伝えることができます。ホスト プロファイル データ ブロックのブロック タイプは、ブロックのシリーズ 1 グループのブロック タイプ 139 です。データ ブロックは、IPv6 アドレスをサポートするようになり、クライアント アプリケーション データ ブロックを追加しました。

(注) 次の図のブロック タイプ フィールドの横のアスタリスク(*)は、メッセージにシリーズ 1 データ ブロックのゼロ以上のインスタンスが含まれる可能性があることを示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
クライアント フィンガープリント	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	クライアント フィンガープリント データ ブロック*																															
SMB フィンガープリント	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	SMB フィンガープリント データ ブロック*																															
DHCP フィンガープリント	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	DHCP フィンガープリント データ ブロック*																															
モバイル デバイス フィンガープリント	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	モバイル デバイス フィンガープリント データ ブロック*																															
IPv6 サーバ フィンガープリント	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	Ipv6 サーバ フィンガープリント データ ブロック*																															
IPv6 クライアント フィンガープリント	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	IPv6 クライアント フィンガープリント データ ブロック*																															
IPv6 DHCP フィンガープリント	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	IPv6 DHCP フィンガープリント データ ブロック*																															
ユーザ エージェント フィンガープリント	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	ユーザ エージェント フィンガープリント データ ブロック*																															

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
TCP サーバ ブロック*	リスト ブロック タイプ(11)																																TCP のリスト サーバ
	リスト ブロック長																																
	TCP サーバ データ ブロック																																
UDP サーバ ブロック*	リスト ブロック タイプ(11)																																UDP のリスト サーバ
	リスト ブロック長																																
	UDP サーバ データ ブロック																																
ネットワーク プロトコル ブロック*	リスト ブロック タイプ(11)																																ネットワーク のリスト プロトコル
	リスト ブロック長																																
	ネットワーク プロトコル データ ブロック																																
トランスポート(Transport) プロトコル ブロック*	リスト ブロック タイプ(11)																																トランスポート リスト プロトコル
	リスト ブロック長																																
	トランスポート プロトコル データ ブロック																																
MAC アドレス ブロック*	リスト ブロック タイプ(11)																																MAC のリスト アドレス
	リスト ブロック長																																
	ホスト MAC アドレス データ ブロック																																
	最終検出時のホスト																																
	ホスト タイプ																																
	モバイル								改造								VLAN の有無								VLAN ID								
クライアント アプリケーション データ	VLAN ID(続き)								VLAN タイプ								VLAN 優先順位								汎用リスト ブロック タイプ(31)								クライアント のリスト アプリケーション
	汎用リスト ブロック タイプ(31)(続き)																								汎用リスト ブロック長								
	汎用リスト ブロック長(続き)																								クライアント アプリケーション データ ブロック								

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NetBIOS 名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	NetBIOS 文字列データ...																															

次の表では、5.2+ で返るホスト プロファイル データ ブロックのフィールドについて説明します。

表 4-83　　ホスト プロファイル データブロック 5.2+ のフィールド

フィールド	データ タイプ	説明
ホスト プロファイル ブロック タイプ	uint32	5.2+ のホスト プロファイル データ ブロックを開始します。この値は常に 139 です。
ホスト プロファイル ブロック長	uint32	ホスト プロファイル データ ブロックのバイト数(ホスト プロファイル ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くホスト プロファイル データに含まれるバイト数を含む)。
IP アドレス	uint8(16)	ホストの IP アドレスこれには、IPv4 または IPv6 のいずれも使用できます。
ホップ	uint8	ホストからのデバイスまでのホップ数。
プライマリ/セカンダリ	uint8	ホストがそれを検出したデバイスのプライマリまたはセカンダリのどちらのネットワークにあるかを示します。 • 0:ホストはプライマリ ネットワークにあります。 • 1:ホストはセカンダリ ネットワークにあります。
汎用リスト ブロック タイプ	uint32	サーバ フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(サーバ フィンガープリント)データ ブロック*	変数	サーバ フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	クライアント フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。

表 4-83　ホスト プロファイル データブロック 5.2+ のフィールド(続き)

フィールド	データ タイプ	説明
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(クライアント フィンガープリント)データ ブロック*	変数	クライアント フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	SMB フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(SMB フィンガープリント)データ ブロック*	変数	SMB フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	DHCP フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(DHCP フィンガープリント)データ ブロック*	変数	DHCP フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	モバイル デバイス フィンガープリントで識別するフィンガープリント データを搬送するオペレーティング システム フィンガープリント データ ブロックで構成される汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。

表 4-83　ホスト プロファイル データブロック 5.2+ のフィールド(続き)

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント モバイル データ ブロック*	変数	モバイル デバイス フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	IPv6 サーバ フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(IPv6 サーバ)データ ブロック*	変数	IPv6 サーバ フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	IPv6 クライアント フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(IPv6 クライアント)データ ブロック*	変数	IPv6 クライアント フィンガープリントで識別したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	IPv6 DHCP フィンガープリントで識別するフィンガープリント データを搬送するオペレーティング システム フィンガープリント データ ブロックで構成される汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。

表 4-83　ホスト プロファイル データブロック 5.2+ のフィールド(続き)

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント(IPv6 DHCP フィンガープリント)データ ブロック*	変数	IPv6 DHCP フィンガープリントで識別したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	ユーザ エージェント フィンガープリントで識別するフィンガープリント データを搬送するオペレーティング システム フィンガープリント データ ブロックで構成される汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(ユーザ エージェント フィンガープリント)データ ブロック*	変数	ユーザ エージェント フィンガープリントで識別したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ) を参照してください。
リストブロック タイプ	uint32	TCP サーバ データを伝えるサーバ データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバ データ ブロックを加えた値です。 このフィールドには、ゼロ以上のサーバ データ ブロックが続きます。
TCP サーバ データ ブロック	変数	TCP サーバを記述するホスト サーバ データ ブロック。このデータ ブロックの説明の詳細については、ホスト サーバ データ ブロック 4.10.0+(4-143 ページ) を参照してください。
リストブロック タイプ	uint32	UDP サーバ データを伝えるサーバ データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバ データ ブロックを加えた値です。 このフィールドには、ゼロ以上のサーバ データ ブロックが続きます。
UDP サーバ データ ブロック	uint32	UDP サーバを記述するホスト サーバ データ ブロック。このデータ ブロックの説明の詳細については、ホスト サーバ データ ブロック 4.10.0+(4-143 ページ) を参照してください。

表 4-83　ホスト プロファイル データブロック 5.2+ のフィールド(続き)

フィールド	データ タイプ	説明
リストブロック タイプ	uint32	ネットワーク プロトコル データを伝えるプロトコル データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのプロトコル データ ブロックを加えた値です。 このフィールドには、ゼロ以上のプロトコル データ ブロックが続きます。
ネットワーク プロトコルデータ ブロック	uint32	ネットワーク プロトコルを記述するプロトコル データ ブロック。このデータ ブロックの説明の詳細については、プロトコル データ ブロック (4-78 ページ) を参照してください。
リストブロック タイプ	uint32	トランスポート プロトコル データを伝えるプロトコル データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのプロトコル データ ブロックを加えた値です。 このフィールドには、ゼロ以上のトランスポート プロトコル データ ブロックが続きます。
トランスポート プロトコル データ ブロック	uint32	トランスポート プロトコルを記述するプロトコル データ ブロック。このデータ ブロックの説明の詳細については、プロトコル データ ブロック (4-78 ページ) を参照してください。
リストブロック タイプ	uint32	MAC アドレス データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リストのバイト数(リスト ヘッダーと、カプセル化されたすべての MAC アドレス データ ブロックを含む)。
ホスト MAC アドレス データ ブロック	uint32	ホスト MAC アドレスを記述するホスト MAC アドレス データ ブロック。このデータ ブロックの説明の詳細については、ホスト MAC アドレス 4.9+ (4-119 ページ) を参照してください。
最終検出時のホスト	uint32	システムがホスト アクティビティを検出した前回時刻を表す UNIX タイムスタンプ。
ホスト タイプ	uint32	ホスト タイプを示します。表示される可能性がある値は次のとおりです。 • 0:ホスト • 1:ルータ • 2:ブリッジ • 3:NAT デバイス • 4:LB(ロード バランサ)
モバイル	uint8	検出したホストがモバイル デバイスであるかどうかを示す true/false フラグ。

表 4-83　ホスト プロファイル データブロック 5.2+ のフィールド(続き)

フィールド	データ タイプ	説明
改造	uint8	ホストが(ジェイルブレイクされていない)モバイル デバイスであるかどうかを示す true/false フラグ。
VLAN の有無	uint8	VLAN が存在するかどうかを示します。 • 0:はい • 1:いいえ
VLAN ID	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグにカプセル化されたパケットのタイプ。
VLAN 優先順位	uint8	VLAN タグに含まれる優先順位値。
文字列ブロック タイプ	uint32	ホスト クライアント アプリケーション データを含む文字列データ ブロックを開始します。この値は常に 112 です。
文字列ブロック長	uint32	文字列ブロック タイプ フィールドと長さフィールドの 8 バイトに、ホスト クライアント アプリケーション データのバイト数を加えた文字列データ ブロックのバイト数。
ホスト クライアント アプリケーション データ ブロック	変数	クライアント アプリケーション データのブロックのリスト。このデータ ブロックの説明の詳細については、フル クライアント アプリケーション データ ブロック 5.0+(4-159 ページ) を参照してください。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。

ユーザ製品データ ブロック 5.1+

ユーザ製品データ ブロックは、サードパーティ アプリケーション文字列マッピングなど、サードパーティ アプリケーションからインポートしたホスト入力データを伝えます。このデータ ブロックは次の表では、6.1+ の接続統計データ ブロックのフィールドについて説明します。(4-131 ページ) と ユーザ サーバ メッセージとオペレーティング システム メッセージ(4-58 ページ) で使用します。ユーザ製品データ ブロックのブロック タイプのブロック タイプは、4.7 ～ 4.10.1 のシリーズ 1 ブロック グループのブロック タイプ 65 と、4.10.2 ～ 5.0.x のブロック タイプ 118、そして 5.1+ のシリーズ 1 ブロック グループのブロック タイプ 134 です。ブロック タイプ 65 と 118 の構造は同じです。

(注)　次の図で、データ ブロック名の横のアスタリスク(*)は、データ ブロックの複数のインスタンスが発生する可能性があることを示します。

次の図は、ユーザ製品データ ブロックの形式を示しています。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		ユーザ製品データ ブロック タイプ（134）																															
		ユーザ製品ブロック長																															
		ソース ID																															
		ソース タイプ																															
IP アドレス範囲		汎用リスト ブロック タイプ（31）																															
		汎用リスト ブロック長																															
		IP 範囲仕様データ ブロック*																															
		ポート																プロトコル															
		ドロップ ユーザ製品																															
カスタム（Custom）ベンダー文字列		文字列ブロック タイプ（0）																															
		文字列ブロック長																															
		カスタム ベンダー文字列...																															
カスタム（Custom）製品文字列		文字列ブロック タイプ（0）																															
		文字列ブロック長																															
		カスタム製品文字列...																															
カスタム（Custom）バージョン文字列		文字列ブロック タイプ（0）																															
		文字列ブロック長																															
		カスタム バージョン文字列...																															
		ソフトウェア ID																															
		サーバ ID																															
		ベンダー ID																															
		製品 ID																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
メジャー バージョン 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	メジャー バージョン文字列...																															
マイナー バージョン 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	マイナー用バージョン文字列...																															
リビジョン 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	リビジョン文字列...																															
メジャー用 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	メジャー用バージョン文字列...																															
マイナー用 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	マイナー用バージョン文字列...																															
リビジョン用 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	リビジョン用文字列...																															
ビルド文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ビルド文字列...																															
パッチ文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	パッチ文字列...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
拡張文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	拡張文字列...																															
OS UUID	オペレーティング システム UUID																															
	オペレーティング システム UUID(続き)																															
	オペレーティング システム UUID(続き)																															
	オペレーティング システム UUID(続き)																															
デバイス 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	デバイス 文字列...																															
修正のリスト	モバイル								改造								汎用リスト ブロック タイプ(31)															
	汎用リスト ブロック タイプ(31)(続き)																汎用リスト ブロック長															
	汎用リスト ブロック長(続き)																修正リスト データ ブロック*															
	修正リスト データ ブロック*(続き)																															

次の表では、ユーザ製品データ ブロックのコンポーネントについて説明します。

表 4-84　ユーザ製品データ ブロックのフィールド

フィールド	データ タイプ	説明
ユーザ製品データ ブロック タイプ	uint32	ユーザ製品データ ブロックを開始します。5.1+ の場合、この値は 134 です。
ユーザ製品ブロック長	uint32	ユーザ製品データ ブロックのバイトの合計数(ユーザ製品ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ製品データのバイト数を含む)。
ソース ID	uint32	データをインポートした送信元にマッピングするID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。

表 4-84　ユーザ製品データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答(RNA) がデータを提供した場合、0 • ユーザがデータを提供した場合、1 • サードパーティ スキャナがデータを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでデータを提供した場合、3
汎用リスト ブロック タイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リスト データ ブロックのバイト数。
IP範囲仕様データ ブロック*	変数	ユーザ入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データ ブロック。このデータ ブロックの説明の詳細については、5.2+の IP アドレス範囲データ ブロック (4-98 ページ) を参照してください。
ポート	uint16	ユーザが指定するポート。
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048:IP
ドロップ ユーザ製品	uint32	ユーザ OS 定義がホストから削除されたかどうかを示します: • 0:いいえ • 1:はい
文字列ブロック タイプ	uint32	ユーザ入力に指定されたカスタム ベンダー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタム ベンダー文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびベンダー名のバイト数を含む)。
カスタム ベンダー名	string	ユーザ入力で指定されたカスタム ベンダー名。
文字列ブロック タイプ	uint32	ユーザ入力に指定されたカスタム製品名を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 4-84　ユーザ製品データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	カスタム製品文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、および製品名のバイト数を含む)。
カスタム製品名	string	ユーザ入力に指定されたカスタム製品名。
文字列ブロック タイプ	uint32	ユーザ入力に指定されたカスタム バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタム バージョン文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
カスタム バージョン	string	ユーザ入力に指定されたカスタム バージョン。
ソフトウェア ID	uint32	データベースのサーバまたはオペレーティング システムの特定のリビジョンの識別子。
サーバ ID	uint32	ユーザ入力に指定したホスト サーバのアプリケーション プロトコルの Firepower システム アプリケーション識別子。
ベンダー ID	uint32	サードパーティ オペレーティング システムを Firepower システム OS 定義にマッピングしたときに指定したサードパーティ オペレーティング システムのベンダーの識別子。
製品 ID	uint32	サードパーティ オペレーティング システム文字列を Firepower システム OS 定義にマッピングしたときに指定したサードパーティ オペレーティング システム文字列の製品識別文字列。
文字列ブロック タイプ	uint32	ユーザ入力のサードパーティ オペレーティング システム文字列をマップする Firepower システム オペレーティング システム定義のメジャー バージョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	メジャー文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
メジャー バージョン	string	サードパーティ OS 文字列をマップする Firepower システム オペレーティング システム定義のメジャー バージョン。
文字列ブロック タイプ	uint32	サードパーティ OS 文字列をマップする Firepower システム オペレーティング システム定義のマイナー バージョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	マイナー文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
マイナー バージョン	string	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システム定義のマイナー バージョン番号。

表 4-84　ユーザ製品データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	ユーザ入力のサードパーティ オペレーティング システム文字列をマップする Firepower システム オペレーティング システム定義のマイナー リビジョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	メジャー用文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
リビジョン	string	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システム定義のリビジョン番号。
文字列ブロック タイプ	uint32	サードパーティ オペレーティング システム文字列をマップする Firepower システム オペレーティング システム定義の最後のメジャー バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにバージョンのバイト数を加えた移行先メジャー文字列データ ブロックのバイト数。
移行先メジャー	string	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システム定義のメジャー バージョン番号の範囲の最後のバージョン番号。
文字列ブロック タイプ	uint32	サードパーティ オペレーティング システム文字列をマップする Firepower システム オペレーティング システム定義の最後のマイナー バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにバージョンのバイト数を加えたマイナー用文字列データ ブロックのバイト数。
マイナー用	string	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システム定義のマイナー バージョン番号の範囲の最後のバージョン番号。
文字列ブロック タイプ	uint32	サードパーティ OS 文字列をマップする Firepower システム オペレーティング システム定義の最後のリビジョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにリビジョン番号のバイト数を加えたリビジョン用文字列データ ブロックのバイト数。
リビジョン用	string	ユーザ入力のサードパーティの OSの文字列をマップする Firepower システム オペレーティング システム定義のリビジョン番号の範囲の最後のリビジョン番号。
文字列ブロック タイプ	uint32	サードパーティ OS 文字列をマップする Firepower システム オペレーティングシステムのビルド番号を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 4-84　ユーザ製品データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	ビルド文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびビルド番号のバイト数を含む)。
ビルド(Build)	string	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システムのビルド番号。
文字列ブロック タイプ	uint32	サードパーティ OS 文字列をマップする Firepower システム オペレーティングシステムのパッチ番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	パッチ文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびパッチ番号のバイト数を含む)。
パッチ	string	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システムのパッチ番号。
文字列ブロック タイプ	uint32	サードパーティ OS 文字列をマップする Firepower システム OS の拡張番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	拡張文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、および拡張番号のバイト数を含む)。
拡張	string	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システムの拡張番号。
UUID	uint8 [x16]	オペレーティング システム用の固有 ID 番号が含まれます。
文字列ブロック タイプ	uint32	ユーザ入力に指定されたデバイス ハードウェア情報を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ビルド文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびビルド番号のバイト数を含む)。
デバイス 文字列	string	モバイル デバイス ハードウェア情報。
モバイル	uint8	オペレーティング システムがモバイル デバイスで動作しているかどうかを示す true/false フラグ。
改造	uint8	モバイル デバイスのオペレーティング システムがジェイルブレイクされているかどうかを示す true/false フラグ。
汎用リスト ブロック タイプ	uint32	どの修正が特定の IP アドレス範囲内のホストに適用されているかに関するユーザ入力データを伝える修正リストデータ ブロックで構成される、汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべての修正リスト データ ブロックを含む)。
修正リスト データ ブロック*	変数	ホストに適用された修正に関する情報を含む修正リスト データ ブロック。このデータ ブロックの説明の詳細については、フィックス リスト データ ブロック (4-105 ページ) を参照してください。

ユーザ データ ブロック

ユーザ データ ブロックはユーザ イベント メッセージに表示されます。これらはシリーズ 1 データ ブロックのサブセットです。シリーズ 1 データ ブロックの一般的な形式については、ディスカバリ（シリーズ1）ブロック（4-63 ページ）を参照してください。

(注)　ユーザ データ ブロック ヘッダーのデータ ブロック長フィールドには、2 つのデータ ブロック ヘッダー フィールドの 8 バイトを含む、そのデータ ブロックのバイト数を格納します。

次の表は、ユーザ イベント メッセージに表示される可能性のあるユーザ データ ブロックの一覧です。一覧のデータ ブロックはデータ ブロック タイプ別に分かれています。現在のデータ ブロックは最新バージョンです。レガシー ブロックはサポート対象ですが、Firepower システム の現行バージョンによる作成対象ではありません。

表 4-85　ユーザ データ ブロック タイプ

タイプ	目次	データ ブロック カテゴリ	説明
73	ユーザ ログイン情報	レガシー	システムが検出したユーザのログイン情報の変更を格納します。詳細については、ユーザ ログイン情報 データ ブロック 6.1+（4-198 ページ）を参照してください。バージョン 5.0 で導入したサクセサ ブロック タイプは、ブロック タイプ 73 と同じ構造ですが、そのフィールド内のデータは異なります。
74	ユーザ アカウント更新メッセージ	現在（Current）	ユーザ アカウント情報の変更を格納します。詳細については、ユーザ アカウント更新メッセージ データ ブロック（4-186 ページ）を参照してください。
75	4.7 ～ 4.10.x のユーザ情報	レガシー	システムが検出したユーザの情報の変更を格納します。詳細については、6.0+ の情報データ ユーザ ブロック（4-195 ページ）を参照してください。バージョン 6.0 で導入したサクセサ ブロックのブロック タイプは 158 です。
120	5.x のユーザ情報	現在（Current）	システムが検出したユーザの情報の変更を格納します。詳細については、6.0+ の情報データ ユーザ ブロック（4-195 ページ）を参照してください。ブロック タイプ 75 に置き換わります。これはブロック タイプ 158 に更新しました。
121	ユーザ ログイン情報	レガシー	システムが検出したユーザのログイン情報の変更を格納します。詳細については、ユーザ ログイン情報 データ ブロック 5.0 ～ 5.0.2（B-109 ページ）を参照してください。プロトコル フィールドの内容であるブロック 73 とは異なります。ここには、イベントで検出したアプリケーション プロトコル ID のバージョン 5.0 +アプリケーション ID を保存します。バージョン 5.1 で導入したサクセサ ブロックのブロック タイプは 127 です。

表 4-85　ユーザ データ ブロック タイプ(続き)

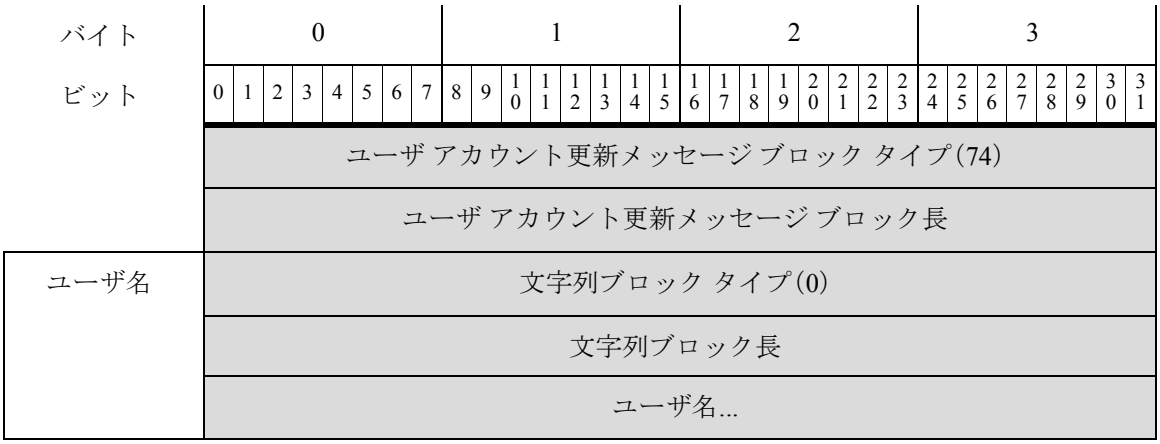
タイプ	目次	データ ブロック カテゴリ	説明
127	ユーザ ログイン情報	レガシー	システムが検出したユーザのログイン情報の変更を格納します。詳細については、ユーザ ログイン情報データ ブロック 5.1 ～ 5.4.x (B-110 ページ) を参照してください。これはブロック タイプ 121 に置き換わります。6.0 で導入したサクセサ ブロックのブロック タイプは 159 です。
150	IOC 状態	現在 (Current)	侵害に関する情報を格納します。詳細については、5.3+ の IOC ステート データ ブロック (4-35 ページ) を参照してください。
158	6.0+ のユーザ情報	現在 (Current)	システムが検出したユーザの情報の変更を格納します。詳細については、6.0+ の情報データ ユーザ ブロック (4-195 ページ) を参照してください。ブロック タイプ 120 に置き換わります。
159	ユーザ ログイン情報	現在 (Current)	システムが検出したユーザのログイン情報の変更を格納します。詳細については、ユーザ ログイン情報データ ブロック 6.1+ (4-198 ページ) を参照してください。これはブロック タイプ 127 に置き換わります。

ユーザ アカウント更新メッセージ データ ブロック

ユーザ アカウント更新メッセージ データ ブロックは、更新に関する情報をユーザのアカウント情報に伝えます。

ユーザ アカウント 更新データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 74 です。

次の図は、ユーザ アカウント更新メッセージ データ ブロックの形式です。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	名...																															
ミドルネーム イニシャル（Initials）	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ミドルネーム イニシャル...																															
姓	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	姓...																															
正式名称	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	正式名称...																															
役職（Title）	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	タイトル...																															
スタッフ ID	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	スタッフ アイデンティティ...																															
アドレス（Address）	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	住所...																															
市区町村郡（City）	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	市区町村郡...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
県	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	県...																															
国/地域	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	国/地域																															
郵便番号	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	郵便番号...																															
建物	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	建物...																															
場所	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	場所...																															
会議室（Room）	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	会議室...																															
会社	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	会社...																															
部門（Division）	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	部門...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
部署名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	部署名...																															
オフィス（Office）	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	オフィス...																															
郵便配達先	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	郵便配達先...																															
E メール	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール...																															
電話	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電話...																															
IP 電話	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	IP 電話...																															
ユーザ 1	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ 1...																															
ユーザ 2	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ 2...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ユーザ 3	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ 3...																															
ユーザ 4	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ 4...																															
電子メール エイリアス 1	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール エイリアス 1...																															
電子メール エイリアス 2	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール エイリアス 2...																															
電子メール エイリアス 3	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール エイリアス 3...																															

次の表では、ユーザ アカウント更新メッセージ データ ブロックのコンポーネントについて説明します。

表 4-86　ユーザ アカウント更新メッセージのデータ ブロックのフィールド

フィールド	データ タイプ	説明
ユーザ アカウント更新メッセージ ブロック タイプ	uint32	ユーザ アカウント更新メッセージのデータ ブロックを開始します。この値は常に 74 です。
ユーザ アカウント更新メッセージ ブロック長	uint32	ユーザ アカウント更新メッセージ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザ アカウント更新メッセージ データのバイト数を加えたユーザ アカウント更新メッセージ データ ブロックの合計バイト数。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 4-86　ユーザ アカウント更新メッセージのデータ ブロックのフィールド (続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
ユーザ名	string	ユーザのユーザ名。
文字列ブロック タイプ	uint32	ユーザの名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに名のバイト数を加えた名文字列データ ブロックのバイト数。
名	string	ユーザの名前。
文字列ブロック タイプ	uint32	ユーザのミドル ネーム イニシャルを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにミドル ネーム イニシャルのバイト数を加えたミドル ネーム イニシャル文字列データ ブロックのバイト数。
ミドル ネーム イニシャル	string	ユーザのミドル ネーム イニシャル。
文字列ブロック タイプ	uint32	ユーザの姓を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに姓のバイト数を加えた姓文字列データ ブロックのバイト数。
姓	string	ユーザの姓。
文字列ブロック タイプ	uint32	ユーザの姓名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに姓名のバイト数を加えた姓名文字列データ ブロックのバイト数。
正式名称	string	ユーザの姓名。
文字列ブロック タイプ	uint32	ユーザの役職を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに役職のバイト数を加えた役職文字列データ ブロックのバイト数。
役職(Title)	string	ユーザの役職。
文字列ブロック タイプ	uint32	ユーザのスタッフの識別子を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにスタッフ アイデンティティのバイト数を加えたスタッフ アイデンティティ文字列データ ブロックのバイト数。
スタッフ アイデンティティ	string	ユーザのスタッフ アイデンティティ。

表 4-86　ユーザ アカウント更新メッセージのデータ ブロックのフィールド（続き）

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	ユーザのアドレスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにアドレスのバイト数を加えたアドレス文字列データ ブロックのバイト数。
アドレス（Address）	string	ユーザの住所。
文字列ブロック タイプ	uint32	ユーザの住所から得た市町村郡を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに市町村郡のバイト数を加えた市町村郡文字列データ ブロックのバイト数。
市区町村郡（City）	string	ユーザの住所から得た市町村郡。
文字列ブロック タイプ	uint32	ユーザの住所から得た県を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに県のバイト数を加えた県文字列データ ブロックのバイト数。
県	string	ユーザの県。
文字列ブロック タイプ	uint32	ユーザの住所から得た国または地域を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに国または地域のバイト数を加えた国または地域文字列データ ブロックのバイト数。
国/地域	string	ユーザの住所から得た国または地域。
文字列ブロック タイプ	uint32	ユーザの住所から得た郵便番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに郵便番号のバイト数を加えた郵便番号文字列データ ブロックのバイト数。
郵便番号	string	ユーザの住所から得た郵便番号。
文字列ブロック タイプ	uint32	ユーザの住所から得た建物を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに建物名のバイト数を加えた建物文字列データ ブロックのバイト数。
建物	string	ユーザの住所から得た建物。
文字列ブロック タイプ	uint32	ユーザの住所から得た場所を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに場所名のバイト数を加えた場所文字列データ ブロックのバイト数。
場所	string	ユーザの住所から得た場所。

表 4-86　ユーザ アカウント更新メッセージのデータ ブロックのフィールド（続き）

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	ユーザの住所から得たルームを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにルームのバイト数を加えたルーム文字列データ ブロックのバイト数。
会議室（Room）	string	ユーザの住所から得たルーム。
文字列ブロック タイプ	uint32	ユーザの住所から得た会社を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに会社名のバイト数を加えた会社文字列データ ブロックのバイト数。
会社	string	ユーザの住所から得た会社。
文字列ブロック タイプ	uint32	ユーザの住所から得た部門を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに部門名のバイト数を加えた部門文字列データ ブロックのバイト数。
部門（Division）	string	ユーザの住所から得た部門。
文字列ブロック タイプ	uint32	ユーザの住所から得た部署を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	部署文字列データ ブロックのバイト数（ブロック タイプと長さのフィールド用の 8 バイト、および部署のバイト数を含む）。
部署名（Department）	string	ユーザの住所から得た部署。
文字列ブロック タイプ	uint32	ユーザの住所から得たオフィスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにオフィスのバイト数を加えたオフィス文字列データ ブロックのバイト数。
オフィス（Office）	string	ユーザの住所から得たオフィス。
文字列ブロック タイプ	uint32	ユーザの住所から得た郵便配達先を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに郵便配達先のバイト数を加えた郵便配達先文字列データ ブロックのバイト数。
郵便配達先	string	ユーザの住所から得た郵便配達先。
文字列ブロック タイプ	uint32	ユーザの電子メールアドレスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メール アドレスのバイト数を加えた電子メール アドレス文字列データ ブロックのバイト数。

表 4-86　ユーザ アカウント更新メッセージのデータ ブロックのフィールド (続き)

フィールド	データ タイプ	説明
E メール	string	ユーザの電子メール アドレス。
文字列ブロック タイプ	uint32	ユーザの電話番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電話番号のバイト数を加えた電話番号文字列データ ブロックのバイト数。
電話	string	ユーザの電話番号。
文字列ブロック タイプ	uint32	ユーザのインターネット電話番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにインターネット電話番号のバイト数を加えたインターネット電話番号文字列データ ブロックのバイト数。
インターネット電話	string	ユーザのインターネット電話番号。
文字列ブロック タイプ	uint32	ユーザの代替ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにユーザ名のバイト数を加えたユーザ文字列データ ブロックのバイト数。
ユーザ 1	string	ユーザの代替ユーザ名。
文字列ブロック タイプ	uint32	ユーザの代替ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにユーザ名のバイト数を加えたユーザ文字列データ ブロックのバイト数。
ユーザ 2	string	ユーザの代替ユーザ名。
文字列ブロック タイプ	uint32	ユーザの代替ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにユーザ名のバイト数を加えたユーザ文字列データ ブロックのバイト数。
ユーザ 3	string	ユーザの代替ユーザ名。
文字列ブロック タイプ	uint32	ユーザの代替ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにユーザ名のバイト数を加えたユーザ文字列データ ブロックのバイト数。
ユーザ 4	string	ユーザの代替ユーザ名。
文字列ブロック タイプ	uint32	ユーザの電子メール エイリアスを含む文字列データ ブロックを開始します。この値は常に 0 です。

表 4-86　ユーザ アカウント更新メッセージのデータ ブロックのフィールド（続き）

フィールド	データ タイプ	説明
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メール エイリアスのバイト数を加えた電子メール エイリアス文字列データ ブロックのバイト数。
電子メール エイリアス 1	string	ユーザの電子メール アドレス。
文字列ブロック タイプ	uint32	ユーザの電子メール エイリアスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メール エイリアスのバイト数を加えた電子メール エイリアス文字列データ ブロックのバイト数。
電子メール エイリアス 2	string	ユーザの電子メール アドレス。
文字列ブロック タイプ	uint32	ユーザの電子メール エイリアスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メール エイリアスのバイト数を加えた電子メール エイリアス文字列データ ブロックのバイト数。
電子メール エイリアス 3	string	ユーザの電子メール アドレス。

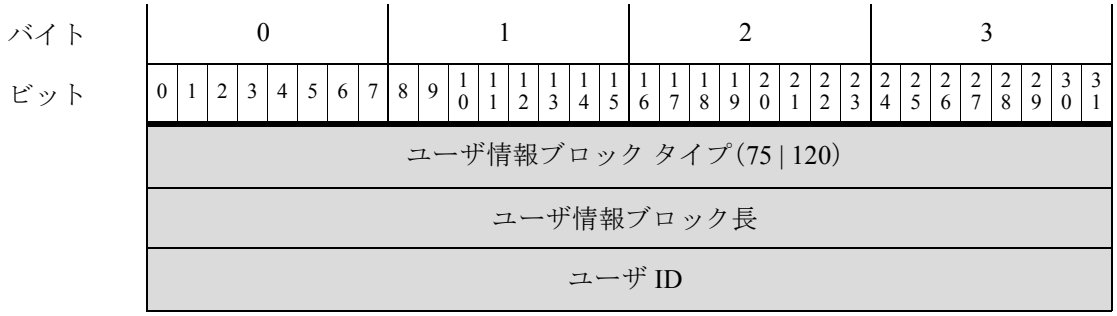
6.0+ の情報データ ユーザ ブロック

ユーザ情報データ ブロックはユーザ変更メッセージで使用され、検出、削除、またはドロップされたユーザの情報を伝えます。詳細については、ユーザ変更メッセージ（4-62 ページ）を参照してください。

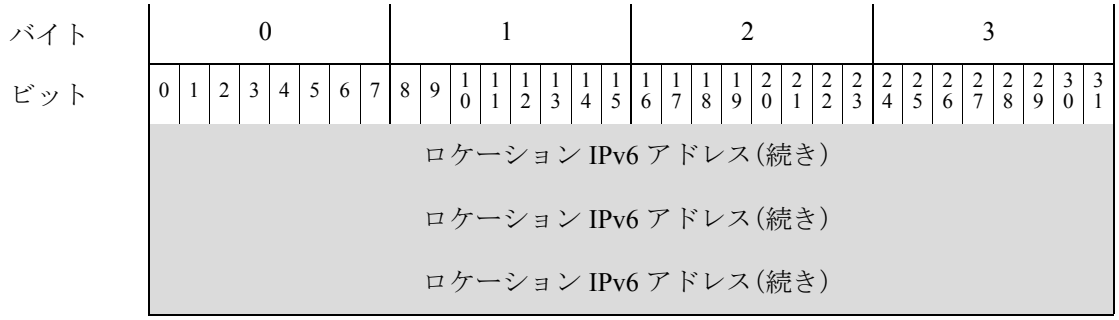
ユーザ情報データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 158 です。ユーザ重要度データ ブロックには、新しいエンドポイント プロファイル フィールド、セキュリティ インテリジェンスフィールド、IPv6 フィールドがあります。

ユーザ情報データ ブロックのブロック タイプは、4.7 ～ 4.10.x のシリーズ 1 ブロック グループのブロック タイプ 75 と、5.x のシリーズ 1 ブロック グループのブロック タイプ 120 です。詳細については、ユーザ情報データ ブロック 5.x（B-116 ページ）を参照してください。

次の図は、ユーザ情報データ ブロックの形式です。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ユーザ名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ名...																															
	レルム ID																															
	プロトコル																															
名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	名...																															
姓	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	姓...																															
E メール	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール...																															
部署名（Department）	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	部署名...																															
電話	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電話...																															
	エンドポイント プロファイル ID																															
	セキュリティ グループ ID																															
	ロケーション IPv6 アドレス																															



次の表は、ユーザ情報データ ブロックのコンポーネントについての説明です。

表 4-87　ユーザ情報データ ブロックのフィールド

フィールド	データ タイプ	説明
ユーザ情報ブロック タイプ	uint32	ユーザ情報データ ブロックを開始します。この値は 158 です。
ユーザ情報ブロック長	uint32	ユーザ情報データ ブロックのバイトの合計数（ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ情報データのバイト数を含む）。
ユーザ ID	uint32	ユーザの ID 番号。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数（ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む）。
ユーザ名	string	ユーザのユーザ名。
レルム ID	uint32	アイデンティティ レルムに対応する整数 ID。
プロトコル	uint32	ユーザ情報を含むパケットのプロトコル。
文字列ブロック タイプ	uint32	ユーザの名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名文字列データ ブロックのバイト数（ブロック タイプと長さのフィールド用の 8 バイト、および名のバイト数を含む）。
名	string	ユーザの名前。
文字列ブロック タイプ	uint32	ユーザの姓を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	姓文字列データ ブロックのバイト数（ブロック タイプと長さのフィールド用の 8 バイト、および姓のバイト数を含む）。
姓	string	ユーザの姓。
文字列ブロック タイプ	uint32	ユーザの電子メールアドレスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メール アドレスのバイト数を加えた電子メール アドレス文字列データ ブロックのバイト数。

表 4-87　ユーザ情報データ ブロックのフィールド(続き)

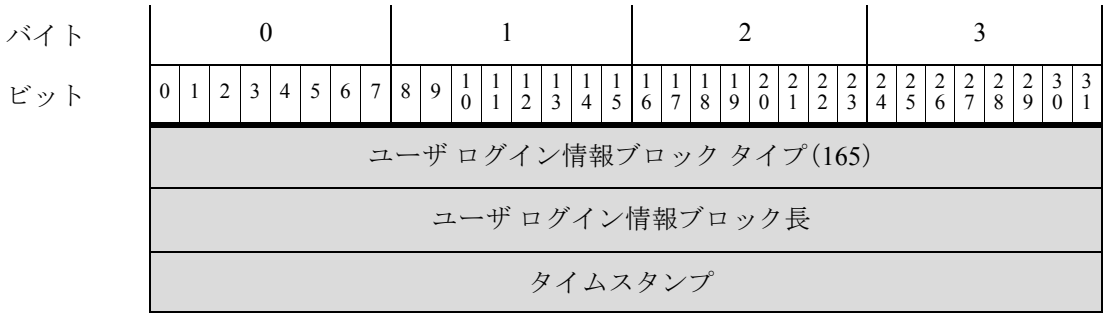
フィールド	データ タイプ	説明
E メール	string	ユーザの電子メール アドレス。
文字列ブロック タイプ	uint32	ユーザの部署を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	部署文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、および部署のバイト数を含む)。
部署名(Department)	string	ユーザの部署名。
文字列ブロック タイプ	uint32	ユーザの電話番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電話番号のバイト数を加えた電話番号文字列データ ブロックのバイト数。
電話	string	ユーザの電話番号。
エンドポイント プロファイル ID	uint32	接続エンドポイントが使用するデバイスのタイプの ID 番号。この番号は防御センターごとに固有であり、メタデータで解決します。
セキュリティ グループ ID	uint32	ネットワーク トラフィック グループの ID 番号。
ロケーション IPv6 アドレス	uint16[8]	ISE と通信するインターフェイスの IP アドレス。IPv4 または IPv6 のアドレスを使用できます。

ユーザ ログイン情報データ ブロック 6.1+

ユーザ ログイン情報データ ブロックは、ユーザ情報更新メッセージで使用され、検出されたユーザのログイン情報の変更を伝えます。詳細については、ユーザ情報更新メッセージ ブロック (4-62 ページ)を参照してください。

ユーザ ログイン情報データ ブロックのブロック タイプは、バージョン 6.1+ のシリーズ 1 ブロック グループのブロック タイプ 165 です。ここには新しいポート フィールドとトンネリング フィールドがあります。これはブロック タイプ 159 に置き換わります。詳細については、ユーザ ログイン情報データ ブロック 6.0.x (B-112 ページ)を参照してください。

次の図は、ユーザ ログイン情報データ ブロックの形式を示しています。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IPv4 アドレス																															
ユーザ名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ名...																															
ドメイン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ドメイン...																															
	ユーザ ID																															
	レルム ID																															
	エンドポイント プロファイル ID																															
	セキュリティ グループ ID																															
	アプリケーション ID																															
	プロトコル																															
	ポート																範囲の開始															
	開始ポート																終了ポート															
E メール	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール...																															
	IPv6アドレス IPv6 アドレス(続き) IPv6 アドレス(続き) IPv6 アドレス(続き)																															
	ロケーション IPv6 アドレス ロケーション IPv6 アドレス(続き) ロケーション IPv6 アドレス(続き)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ロケーション IPv6 アドレス(続き)																															
レポート基準	ログイン タイプ								承認タイプ								文字列ブロック タイプ(0)															
	文字列ブロック タイプ(0)(続き)																文字列ブロック長															
	文字列ブロック長(続き)																レポート基準...															

次の表は、ユーザ ログイン情報データ ブロックのコンポーネントについての説明です。

表 4-88　ユーザ ログイン情報データ ブロックのフィールド

フィールド	データ タイプ	説明
ユーザ ログイン情報ブロック タイプ	uint32	ユーザ ログイン情報データ ブロックを開始します。バージョン 6.1+ の場合、この値は 165 です。
ユーザ ログイン情報ブロック長	uint32	ユーザ ログイン情報データ ブロックのバイトの合計数(ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ ログイン情報データのバイト数を含む)。
タイムスタンプ	uint32	イベントのタイムスタンプ。
IPv4 アドレス	uint32	このフィールドは予約済みですが、設定されておりません。IPv4 アドレスは IPv6 アドレス フィールドに保存されます。詳細については、IP アドレス (1-6 ページ) を参照してください。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
ユーザ名	string	ユーザのユーザ名。
文字列ブロック タイプ	uint32	ドメインを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにドメインのバイト数を加えたユーザ名文字列データ ブロックのバイト数。
ドメイン	string	ユーザがログインしているドメイン。
ユーザ ID	uint32	ユーザの ID 番号。
レルム ID	uint32	アイデンティティ レルムに対応する整数 ID。
エンドポイント プロファイル ID	uint32	接続エンドポイントが使用するデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。

表 4-88　ユーザ ログイン情報データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
セキュリティ グループ ID	uint32	ネットワーク トラフィック グループの ID 番号。
アプリケーション ID	uint32	ログイン情報の取得元の、接続に使用されたアプリケーション プロトコルのアプリケーション ID。
プロトコル	uint32	ユーザの検出やレポートに使用するプロトコル。値は以下のとおりです。 • 165:FTP • 426:SIP • 547:AOL Instant Messenger • 683:IMAP • 710:LDAP • 767:NTP • 773:Oracle データベース • 788:POP3 • 1755:MDNS
ポート	uint16	ユーザを検出したポート番号。
範囲の開始	uint16	TS エージェントが使用するポート範囲の開始ポート
開始ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の開始ポート。
終了ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の最終ポート。
文字列ブロック タイプ	uint32	ユーザの電子メールアドレスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メール アドレスのバイト数を加えた電子メール アドレス文字列データ ブロックのバイト数。
E メール	string	ユーザの電子メール アドレス。
IPv6アドレス	uint8[16]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IPv6 アドレス。
ロケーション IPv6 アドレス	uint8[16]	ユーザがログインした最新の IP アドレス。IPv4 または IPv6 のどちらかのアドレスになります。
ログイン タイプ	uint8	検出されたユーザ ログインのタイプ。
認証タイプ（Authentication Type）	uint8	ユーザが使用する認証のタイプ。値は次のとおりです。 • 0:認証は不要 • 1:パッシブ認証、AD エージェント、または ISE セッション • 2:キャプティブ ポータルの正常な認証 • 3:キャプティブ ポータルのゲスト認証 • 4:キャプティブ ポータルの失敗認証

表 4-88　ユーザ ログイン情報データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	レポート基準値を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	レポート基準文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびレポート基準フィールドのバイト数を含む)。
レポート基準	string	ログインをレポートする Active Directory サーバの名前。

ディスカバリ/接続イベント シリーズ 2 データ ブロック

次の表では、データ ブロック ステータス フィールドは、ブロックが現在(最新バージョン)とレガ シー(旧バージョンで使用したもので、現在も eStreamer で要求可能)のいずれであるかを示します。

表 4-89　ディスカバリ /接続イベント シリーズ 2 ブロック タイプ

タイプ	目次	データ ブロック ステータス	説明
15	アクセス コントロール ルール(Access Control Rule)	現在(Current)	アクセス コントロール ルールのメタデータ メッセージが、ポリシー UUID 値とルール ID 値を記述文字列にマップするときに使用します。アクセス コントロール ルール データ ブロック (4-203 ページ)を参照してください。
21	アクセス コントロール ルール理由	現在(Current)	アクセス コントロール ルールのメタデータ メッセージが、アクセス コントロール ルール理由を記述文字列にマップするときに使用します。アクセス コントロール ルール理由データ ブロック 5.1+(4-204 ページ)を参照してください。
22	セキュリティ インテリジェンスのカテゴリ(Security Intelligence Category)	現在(Current)	セキュリティ インテリジェンス情報の保存に使用します。セキュリティ インテリジェンス カテゴリ データ ブロック 5.1+(4-205 ページ)を参照してください。
57	ユーザ データ(User Data)	現在(Current)	ユーザ レコード メタデータ メッセージが、ユーザを検出したユーザ ID 番号、プロトコル、そしてユーザ名を提供するために使用します。ユーザ データ ブロック (4-206 ページ)を参照してください。

アクセス コントロール ルール データ ブロック

eStreamer サービスは、アクセス コントロール ルールのメタデータ メッセージでアクセス コントロール ルール データ ブロックを使用し、ポリシー UUID とルール ID を組み合わせて、記述文字列にマップします。アクセス コントロール ルール データ ブロックのブロック タイプは、シリーズ 2 ブロック グループのブロック タイプ 15 です。

次の図は、アクセス コントロール ルール データ ブロックの構造です。

次の表では、アクセス コントロール ルール データ ブロックのフィールドについて説明します。

表 4-90　アクセス コントロール ルール データ ブロックのフィールド

フィールド	データ タイプ	説明
アクセス コントロール ルール ブロック タイプ	uint32	アクセス コントロール ルール ブロックを開始します。この値は常に 15 です。
アクセス コントロール ルール ブロック長	uint32	アクセス コントロール ルール ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ルール ブロックの合計バイト数。
アクセス コントロール ルール UUID	uint8[16]	アクセス コントロール ルールの固有識別子。
アクセス コントロール ルール ID	uint32	アクセス コントロール ルールの内部 シスコ 識別子。

表 4-90　アクセス コントロール ルール データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	アクセス コントロール ルール UUID とアクセス コントロール ルール ID に関連付けられているわかりやすい名前のある文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
名前	string	わかりやすい名前。

アクセス コントロール ルール理由データ ブロック 5.1+

eStreamer サービスでは、アクセス コントロール ルール理由データ ブロックをアクセス コントロール ルール理由メタデータ メッセージで使用して、アクセス制御原因を記述文字列にマッピングします。アクセス コントロール ルール理由データ ブロックのブロック タイプは、シリーズ 2 ブロック グループのブロック タイプ 21 です。

次の図は、アクセス コントロール ルール理由データ ブロックの構造です。

次の表では、アクセス コントロール ルール理由データ ブロックのフィールドについて説明します。

表 4-91　アクセス コントロール ルール理由データ ブロックのフィールド

フィールド	データ タイプ	説明
アクセス コントロール ルール理由ブロック タイプ	uint32	アクセス コントロール ルール理由ブロックを開始します。この値は常に 21 です。
アクセス コントロール ルール理由ブロック長	uint32	アクセス コントロール ルール理由ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ルール理由ブロックの合計バイト数。

表 4-91　アクセス コントロール ルール理由データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
アクセス コントロール ルール理由	uint16	アクセス コントロール ルールによって接続がログに記録された理由。
文字列ブロック タイプ	uint32	アクセス コントロール ルール理由に関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	アクセス コントロール ルール理由の説明。

セキュリティ インテリジェンス カテゴリ データ ブロック 5.1+

eStreamer サービスは、アクセス コントロール ルール メタデータ メッセージのセキュリティ インテリジェンス カテゴリ データ ブロックで、セキュリティ インテリジェンス情報をストリーミングします。セキュリティ インテリジェンス カテゴリ データ ブロックのブロック タイプは、シリーズ 2 ブロック グループのブロック タイプ 22 です。

次の図は、セキュリティ インテリジェンス カテゴリ データ ブロックの構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	セキュリティ インテリジェンス カテゴリのブロック タイプ(22)																															
	セキュリティ インテリジェンス カテゴリのブロック長																															
	セキュリティ インテリジェンス リスト ID																															
AC ポリシー UUID	アクセス コントロール ポリシー UUID																															
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
ルール名（Rule Name）	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	セキュリティ インテリジェンス リスト名...																															

次の表では、セキュリティ インテリジェンス カテゴリ データ ブロックのフィールドについて説明します。

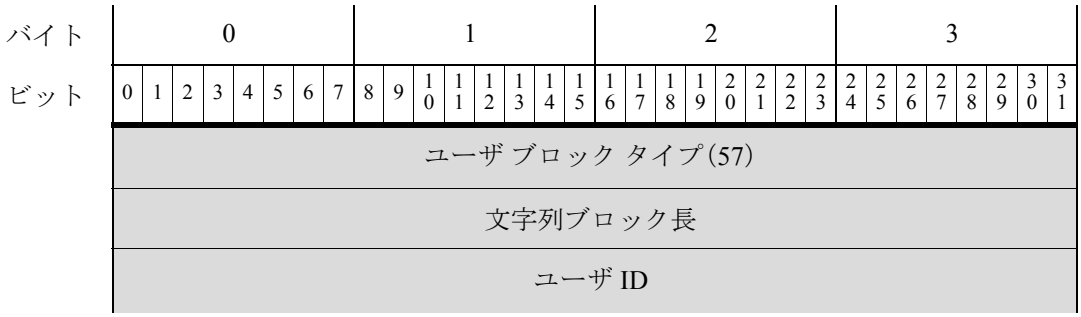
表 4-92　セキュリティ インテリジェンス カテゴリ データ ブロックのフィールド

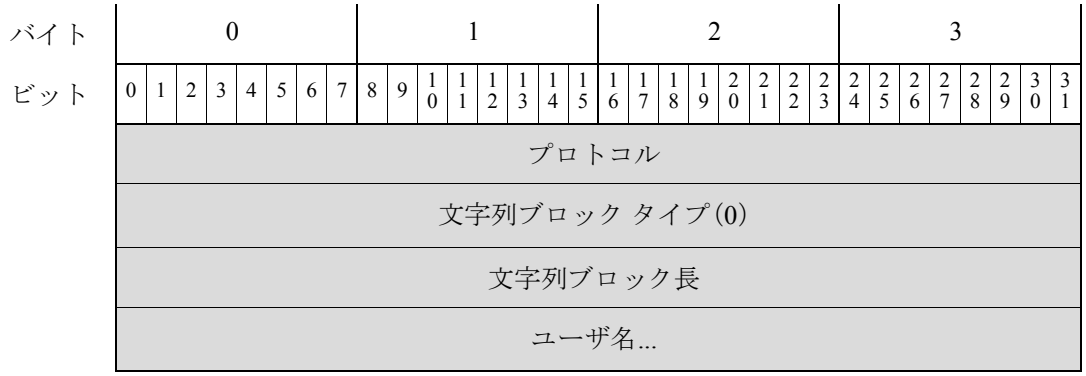
フィールド	データ タイプ	説明
セキュリティ インテリジェンス カテゴリ ブロック タイプ	uint32	セキュリティ インテリジェンス カテゴリのデータ ブロックを開始します。この値は常に 22 です。
セキュリティ インテリジェンス カテゴリのブロック長	uint32	セキュリティ インテリジェンス カテゴリ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたセキュリティ インテリジェンス カテゴリ ブロックの合計バイト数。
セキュリティ インテリジェンス リスト ID	uint32	接続でトリガーがかかる IP ブラックリストまたはホワイトリストの ID。
アクセスコントロール ポリシー UUID	uint8[16]	セキュリティ インテリジェンスに設定されたアクセス コントロール ポリシーの UUID。
文字列ブロック タイプ	uint32	アクセス コントロール ルール理由に関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトにセキュリティ インテリジェンス リスト名フィールドのバイト数を加えた名前文字列データ ブロックのバイト数。
セキュリティ インテリジェンス リスト名	string	接続でトリガーがかかるセキュリティ インテリジェンス カテゴリ IP カテゴリ ブラックリストまたはホワイトリストの名前。

ユーザ データ ブロック

eStreamer サービスは、ユーザ レコード メタデータ メッセージのユーザデータ ブロックで、ユーザ ID 番号、ユーザを検出したプロトコル、そしてユーザ名を提供します。ユーザ データ ブロックのブロック タイプは、シリーズ 2 ブロック グループのブロック タイプ 57 です。

次の図は、ユーザ データ ブロックの構造です。





次の表では、ユーザ データ ブロックのフィールドについて説明します。

表 4-93　ユーザ データ ブロックのフィールド

フィールド	データ タイプ	説明
ユーザ ブロック タイプ	uint32	ユーザ ブロックを開始します。この値は常に 57 です。
文字列ブロック長	uint32	ユーザ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータのバイト数を加えたユーザ ブロックの合計バイト数。
ユーザ ID	uint32	ユーザの固有識別情報。
プロトコル	uint32	ユーザの検出やレポートに使用するプロトコル。値は以下のとおりです。 • 165:FTP • 426:SIP • 547:AOL Instant Messenger • 683:IMAP • 710:LDAP • 767:NTP • 773:Oracle データベース • 788:POP3 • 1755:MDNS
文字列ブロック タイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトにユーザ名フィールドのバイト数を加えたユーザ名文字列データ ブロックのバイト数。
ユーザ名	string	ユーザの名前

アクセス コントロール ポリシー メタデータ ブロック 6.0+

eStreamer サービスはアクセス制御ポリシー メタデータ メッセージのアクセス制御ポリシー メタデータ データ ブロックでアクセス制御情報を提供します。アクセス コントロール ルール ポリシー メタデータ ブロックのブロック タイプは、シリーズ 2 ブロック グループのブロック タイプ 64 です。

次の図は、アクセス コントロール ポリシー メタデータ ブロックの構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	アクセス コントロール ポリシーのメタデータ ブロック タイプ(64)																															
	アクセス コントロール ポリシーのメタデータ ブロック長																															
AC ポリシー UUID	アクセス コントロール ポリシー UUID																															
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
	センサー ID																															
ポリシー名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ポリシー名...																															

次の表では、アクセス コントロール ルール理由データ ブロックのフィールドについて説明します。

表 4-94　アクセス コントロール ルール理由データ ブロックのフィールド

フィールド	データ タイプ	説明
アクセス コントロール ポリシーのメタデータ ブロック タイプ	uint32	アクセス コントロール ポリシー メタデータ ブロックを開始します。この値は常に 64 です。
アクセス コントロール ポリシーのメタデータ ブロック長	uint32	アクセス コントロール ポリシーのメタデータ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ポリシー メタデータ ブロックの合計バイト数。
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの UUID

表 4-94　アクセス コントロール ルール理由データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
センサー ID	uint32	アクセス コントロール ポリシーに関連付けられたセンサー ID 番号
文字列ブロック タイプ	uint32	アクセス コントロール ポリシーに関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
名前	string	アクセス コントロール ポリシーの名前。

ホスト データ構造の概要

この章では、1 つのホストについて記述しているデータ セットを伝送する全ホスト プロファイル データ ブロックの形式について説明します。eStreamer サーバはホスト データの要求に応じてこれらのブロックを作成し、送信します。クライアント要求手順、メッセージ構造、配信方法に関する詳細は、ホスト データおよびマルチ ホスト データ メッセージの形式（2-31 ページ）を参照してください。

eStreamer では、シリーズ 1 データ ブロック構造を使用して、これらの全ホスト プロファイル ブロックをパッケージ化します。シリーズ 1 ブロックの一般的な構造については、シリーズ 1 データ ブロック ヘッダー シリーズ（4-63 ページ）を参照してください。全ホスト プロファイル データ ブロックには、検出と接続データ構造の概要（4-1 ページ）で定義されているサブセクションにそれぞれ記述されているいくつかのカプセル化されたブロックを含みます。

現行および従来の全ホスト プロファイル データ ブロックに関する詳細は、次のセクションを参照してください:

- 全ホスト プロファイル データ ブロック 5.3+（5-1 ページ）では、現行の全ホスト プロファイル データ ブロック構造について説明します。
- フル ホスト プロファイル データ ブロック 5.0 ～ 5.0.2（B-269 ページ）では、バージョン 5.0 ～ 5.0.2 の従来の全ホスト プロファイル データ ブロック構造について説明します。

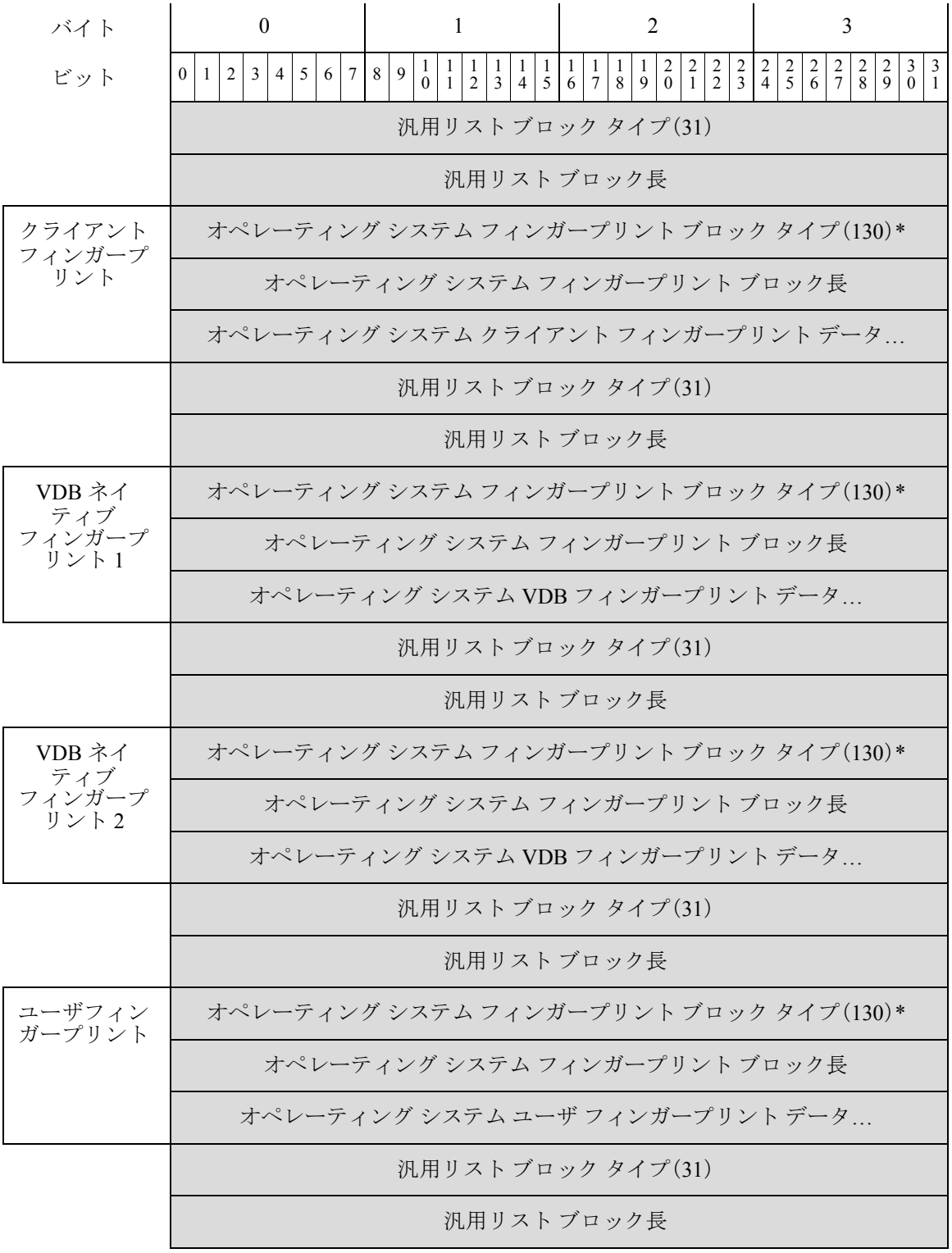
全ホスト プロファイル データ ブロック 5.3+

全ホスト プロファイル データ ブロック バージョン 5.3+ には、1 つのホストについて記述する全データ セットが含まれています。このデータ セットの形式を次の図に示し、次表で説明します。図には、リスト データ ブロックを除き、カプセル化データ ブロック フィールドを提示していない点にご注意ください。これらのカプセル化データ ブロックは、検出と接続データ構造の概要（4-1 ページ）で別途説明します。全ホスト プロファイル データ ブロックのブロック タイプ値は 149 です。これは、ブロック タイプが 140 であった以前のバージョンの代替となります。

（注） 次の図において、ブロック名の横にあるアスタリスク（*）は、データ ブロックのインスタンスが複数発生する可能性があることを示しています。

次の図は、全ホスト プロファイル データ ブロック 5.3+ の形式を示しています。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		全ホスト プロファイル データ ブロック(149)																															
		データ ブロック長																															
		ホスト ID(Host ID)																															
		ホスト ID(続き)																															
		ホスト ID(続き)																															
		ホスト ID(続き)																															
IP アドレス		リスト ブロック タイプ(11)																															
		リスト ブロック長																															
		IP アドレス データ ブロック(143)*																															
		ホップ								汎用リスト ブロック タイプ(31)																							
		汎用リスト ブロック タイプ(続き)								汎用リスト ブロック長																							
OS から取得したフィンガープリント		汎用リスト ブロック長(続き)								オペレーティング システム フィンガープリント ブロック タイプ(130)*																							
		OS フィンガープリント ブロック タイプ(130)*(続き)								オペレーティング システム フィンガープリント ブロック長																							
		OS フィンガープリント ブロック長(続き)								オペレーティング システムから取得したフィンガープリント データ…																							
		汎用リスト ブロック タイプ(31)																															
		汎用リスト ブロック長																															
サーバ フィンガープリント		オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
		オペレーティング システム フィンガープリント ブロック長																															
		オペレーティング システム サーバ フィンガープリント データ																															


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
汎用リスト ブロック タイプ(31)
汎用リスト ブロック長
クライアント フィンガープリント
オペレーティング システム フィンガープリント ブロック タイプ(130)*
オペレーティング システム フィンガープリント ブロック長
オペレーティング システム クライアント フィンガープリント データ…
汎用リスト ブロック タイプ(31)
汎用リスト ブロック長
VDB ネイティブ フィンガープリント 1
オペレーティング システム フィンガープリント ブロック タイプ(130)*
オペレーティング システム フィンガープリント ブロック長
オペレーティング システム VDB フィンガープリント データ…
汎用リスト ブロック タイプ(31)
汎用リスト ブロック長
VDB ネイティブ フィンガープリント 2
オペレーティング システム フィンガープリント ブロック タイプ(130)*
オペレーティング システム フィンガープリント ブロック長
オペレーティング システム VDB フィンガープリント データ…
汎用リスト ブロック タイプ(31)
汎用リスト ブロック長
ユーザフィンガープリント
オペレーティング システム フィンガープリント ブロック タイプ(130)*
オペレーティング システム フィンガープリント ブロック長
オペレーティング システム ユーザ フィンガープリント データ…
汎用リスト ブロック タイプ(31)
汎用リスト ブロック長

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
スキャン（Scan）フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム スキャン フィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
アプリケーション フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム アプリケーション フィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
競合フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム競合フィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
モバイル フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム モバイル フィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
IPv6 サーバ フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム IPv6 サーバ フィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用リスト ブロック長																															
Ipv6 クライアント フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム Ipv6 クライアント フィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
IPv6 DHCP フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム IPv6 DHCP フィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
ユーザ エージェント フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム ユーザ エージェント フィンガープリント データ…																															
(TCP)全サーバ データ	リスト ブロック タイプ(11)…																															
	リスト ブロック長…																															
	(TCP)全サーバ データ ブロック(104)*																															
(UDP)全サーバ データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	(UDP)全サーバ データ ブロック(104)*																															
ネットワーク プロトコル データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	(ネットワーク)プロトコル データ ブロック(4)*																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
トランスポート プロトコル データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	(トランスポート)プロトコル データ ブロック(4)*																															
MAC アドレス データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	ホスト MAC アドレス データ ブロック(95)*																															
	Last Seen																															
	ホスト タイプ																															
	ビジネス上の重要度																VLAN ID															
	VLAN タイプ								VLAN プライオリティ								汎用リスト ブロック タイプ(31)															
ホスト クライアント データ	汎用リスト ブロック タイプ(続き)																汎用リスト ブロック長															
	汎用リスト ブロック長(続き)																全ホスト クライアント アプリケーション データ ブロック(112)*															
NetBIOS 名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	NetBIOS 名文字列																															
注記 データ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	Notes 文字列....																															
(VDB)ホスト Vulns	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	(VDB)ホスト脆弱性データ ブロック(85)*																															
(サード パーティ /VDB) Host Vulns	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	(サードパーティ/VDB)ホスト脆弱性データ ブロック(85)*																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
サードパーティ スキャン Host Vulns	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	(サードパーティ スキャン)元の Vuln ID によるホスト脆弱性データ ブロック(85)*																															
属性値データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	属性値データ ブロック*																															
	モバイル								Jailbroken								汎用リスト ブロック タイプ(31)															
IOC ステート	汎用リスト ブロック タイプ(続き)																汎用リスト ブロック長															
	汎用リスト ブロック長(続き)																IOC ステート データ ブロック(150)*															

次の表では、5.3+ レコード用の全ホスト プロファイルのコンポーネントについて説明します。

表 5-1　全ホスト プロファイル レコード 5.3+ フィールド

フィールド	データ タイプ	説明
ホスト ID(Host ID)	uint8[16]	ホストの一意の ID 番号。これは UUID です。
リスト ブロック タイプ	uint32	TCP サービス データを伝送する IP アドレス データ ブロックを含むリスト データ ブロックを表示します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値には、リスト ブロック タイプ フィールド、リスト ブロック長フィールド、すべてのカプセル化 IP アドレス データ ブロック長から成る 8 バイトを含みます。
[IPアドレス(IP Address)]	変数	ホストの IP アドレスおよび各 IP アドレスが最後に表示されたときの IP アドレス。このデータ ブロックの詳細については、ホスト IP アドレス データ ブロック (4-100 ページ) を参照してください。
ホップ	uint8	ホストからデバイスへのネットワーク ホップ数。
汎用リスト ブロック タイプ	uint32	ホストの既存のフィンガープリントから取得したフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。

表 5-1　全ホスト プロファイル レコード 5.3+ フィールド(続き)

フィールド	データ タイプ	説明
オペレーティング システムから取得したフィンガープリント データ ブロック*	変数	ホストの既存のフィンガープリントから取得したホストでのオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	サーバ フィンガープリントを使用して特定されたフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント(サーバ フィンガープリント)データ ブロック*	変数	サーバ フィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	クライアント フィンガープリントを使用して特定したフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント(クライアント フィンガープリント)データ ブロック*	変数	クライアント フィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。

表 5-1　全ホスト プロファイル レコード 5.3+ フィールド（続き）

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント（VDB）ネイティブ フィンガープリント 1）データ ブロック*	変数	シスコ脆弱性データベース（VDB）のフィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント（VDB）ネイティブ フィンガープリント 2）データ ブロック*	変数	シスコ脆弱性データベース（VDB）のフィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	ユーザが追加したフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント（ユーザ フィンガープリント）データ ブロック*	変数	ユーザが追加したホストのオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	脆弱性スキャナによって追加されたフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。

表 5-1　全ホスト プロファイル レコード 5.3+ フィールド(続き)

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント(スキャン フィンガープリント)データ ブロック*	変数	脆弱性スキャナによって追加されたホストのオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	アプリケーションによって追加されたフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント(アプリケーション フィンガープリント)データ ブロック*	変数	アプリケーションによって追加されたホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	フィンガープリント競合解決から選択したフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント(競合フィンガープリント)データ ブロック*	変数	フィンガープリント競合解決から選択したホストのオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	モバイル デバイス フィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント(モバイル)データ ブロック*	変数	モバイル デバイス ホストのオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。

表 5-1　全ホスト プロファイル レコード 5.3+ フィールド(続き)

フィールド	データ タイプ	説明
汎用リスト ブロック タイプ	uint32	IPv6 サーバ フィンガープリントを使用して特定されたフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント (IPv6 サーバ フィンガープリント) データ ブロック*	変数	IPv6 サーバ フィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	IPv6 クライアント フィンガープリントを使用して特定されたフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント (IPv6 クライアント フィンガープリント)データ ブロック*	変数	IPv6 クライアント フィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	IPv6 DHCP フィンガープリントを使用して特定されたフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント (IPv6 DHCP)データ ブロック*	変数	IPv6 DHCP フィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	ユーザ エージェントのフィンガープリントを使用して特定したフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に31 です。

表 5-1　全ホスト プロファイル レコード 5.3+ フィールド(続き)

フィールド	データ タイプ	説明
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント(ユーザ エージェント)データ ブロック*	変数	ユーザ エージェントのフィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+ (4-166 ページ)を参照してください。
リスト ブロック タイプ	uint32	TCP サービス データを伝送する全サーバ データ ブロックを含むリスト データ ブロックを表示します。この値は常に11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値には、リスト ブロック タイプ フィールド、リスト ブロック長フィールド、すべてのカプセル化全サーバ データ ブロック長から成る 8 バイトを含みます。
(TCP)全サーバ データ ブロック*	変数	ホストで TCP サービスに関するデータを伝送する全サーバ データ ブロックのリスト。このデータ ブロックの詳細については、フル ホスト サーバ データ ブロック 4.10.0+(4-145 ページ)を参照してください。
リスト ブロック タイプ	uint32	UDP サービス データを伝送する全サーバ データ ブロックを含むリスト データ ブロックを表示します。この値は常に11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値には、リスト ブロック タイプ フィールド、リスト ブロック長フィールド、すべてのカプセル化全サーバ データ ブロック長から成る 8 バイトを含みます。
(UDP)全サーバ データ ブロック*	変数	ホストで UDP サブサービスに関するデータを伝送する全サーバ データ ブロックのリスト。このデータ ブロックの詳細については、フル ホスト サーバ データ ブロック 4.10.0+(4-145 ページ)を参照してください。
リスト ブロック タイプ	uint32	ネットワーク プロトコル データを伝送するプロトコル データ ブロックを含むリスト データ ブロックを表示します。この値は常に11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値には、リスト ブロック タイプ フィールド、リスト ブロック長フィールド、すべてのカプセル化プロトコル データ ブロック長から成る 8 バイトを含みます。
(ネットワーク)プロトコル データ ブロック*	変数	ホストでネットワーク プロトコルに関するデータを伝送するプロトコル データ ブロックのリスト。このデータ ブロックの詳細については、プロトコル データ ブロック(4-78 ページ)を参照してください。
リスト ブロック タイプ	uint32	トランスポート プロトコル データを伝送するプロトコル データ ブロックを含むリスト データ ブロックを表示します。この値は常に11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値には、リスト ブロック タイプ フィールド、リスト ブロック長フィールド、すべてのカプセル化プロトコル データ ブロック長から成る 8 バイトを含みます。

表 5-1　全ホスト プロファイル レコード 5.3+ フィールド（続き）

フィールド	データ タイプ	説明
（トランスポート）プロトコル データ ブロック*	変数	ホストでトランスポート プロトコルに関するデータを伝送するプロトコル データ ブロックのリスト。このデータ ブロックの詳細については、プロトコル データ ブロック（4-78 ページ）を参照してください。
リスト ブロック タイプ	uint32	ホスト MAC アドレス データ ブロックを含むリスト データ ブロックを表示します。この値は常に 11 です。
リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化ホスト MAC アドレス データ ブロックを含むリストのバイト数。
ホスト MAC アドレス データ ブロック*	変数	ホスト MAC アドレス データ ブロックのリスト。このデータ ブロックの詳細については、ホスト MAC アドレス 4.9+（4-119 ページ）を参照してください。
Last Seen	uint32	システムがホストのアクティビティを検出した最後の時間を示す UNIX タイムスタンプ。
ホスト タイプ	uint32	ホストのタイプを示します。次の値を指定します。 • 0 — ホスト • 1 — ルータ • 2 — ブリッジ • 3 — NAT（ネットワーク アドレス変換デバイス） • 4 — LB（ロード バランサー）
ビジネス上の重要度	uint16	ビジネスに対するホストの重要度を示します。
VLAN ID	uint16	ホストがいずれの VLAN メンバーであるかを示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグ内でカプセル化されるパケットのタイプ。
VLAN プライオリティ	uint8	VLAN タグに含まれるプライオリティ値。
汎用リスト ブロック タイプ	uint32	クライアント アプリケーション データを伝送するホスト脆弱性データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化クライアント アプリケーション データ ブロックを含む汎用リスト データ ブロック内のバイト数。
全ホスト クライアント アプリケーション データ ブロック*	変数	クライアント アプリケーション データ ブロックのリスト。このデータ ブロックの詳細については、フル クライアント アプリケーション データ ブロック 5.0+（4-159 ページ）を参照してください。
文字列ブロック タイプ	uint32	ホストの NetBIOS 名の文字列データ ブロックを表示します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプ フィールドおよび文字列ブロック長フィールドの 8 バイトを含む文字列データ ブロック内のバイト数と NetBIOS 名文字列のバイト数。

表 5-1　全ホスト プロファイル レコード 5.3+ フィールド(続き)

フィールド	データ タイプ	説明
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	ホストの注記の文字列データ ブロックを表示します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプ フィールドおよび文字列ブロック長フィールドの 8 バイトを含む注記文字列データ ブロックのバイト数および注記文字列のバイト数。
注記	string	ホストの注記ホスト属性の内容を含みます。
汎用リスト ブロック タイプ	uint32	VDB 脆弱性データを伝送するホスト脆弱性データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化データ ブロックを含む汎用リスト データ ブロック内のバイト数。
(VDB)ホスト脆弱性データ ブロック*	変数	シスコ脆弱性データベース(VDB)で特定された脆弱性に関するホスト脆弱性データ ブロックのリスト。このデータ ブロックの詳細については、ホスト脆弱性データ ブロック 4.9.0+ (4-116 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	サードパーティ スキャン脆弱性データを伝送するホスト脆弱性データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化データ ブロックを含む汎用リスト データ ブロック内のバイト数。
(サードパーティ /VDB)ホスト脆弱性データ ブロック*	変数	サードパーティのスキャナから送信され、シスコ脆弱性データベース(VDB)でカタログされているホストの脆弱性に関する情報を含むホスト脆弱性データ ブロック。このデータ ブロックの詳細については、ホスト脆弱性データ ブロック 4.9.0+ (4-116 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	サードパーティ スキャン脆弱性データを伝送するホスト脆弱性データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化データ ブロックを含む汎用リスト データ ブロック内のバイト数。
(サードパーティ スキャン)ホスト脆弱性データ ブロック*	変数	サードパーティのスキャナから送信されたホスト脆弱性データ ブロック。これらのデータ ブロックのホスト脆弱性 ID は、サードパーティのスキャナ ID であり、シスコによって検出された ID ではない点にご注意ください。このデータ ブロックの詳細については、ホスト脆弱性データ ブロック 4.9.0+(4-116 ページ) を参照してください。
リスト ブロック タイプ	uint32	属性データを伝送する属性値データ ブロックを含むリスト データ ブロックを表示します。この値は常に 11 です。
リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化データ ブロックを含むリスト データ ブロック内のバイト数。

表 5-1　全ホスト プロファイル レコード 5.3+ フィールド（続き）

フィールド	データ タイプ	説明
属性値データ ブロック*	変数	属性値データ ブロックのリスト。このリストのデータ ブロックの詳細については、属性値データ ブロック (4-84 ページ) を参照してください。
モバイル	uint8	オペレーティング システムがモバイル デバイスで動作しているかどうかを示す true/false フラグ。
Jailbroken	uint8	モバイル デバイスのオペレーティング システムがジェイルブレイクされているかどうかを示す true/false フラグ。
汎用リスト ブロック タイプ	uint32	IOC ステート データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化 IOC ステート データ ブロックを含む汎用リスト データ ブロック内のバイト数。
IOC ステート データ ブロック*	変数	ホストの侵害に関する情報を含む IOC ステート データ ブロック。このデータ ブロックの詳細については、5.3+ の IOC ステート データ ブロック (4-35 ページ) を参照してください。

eStreamer の設定

クライアント アプリケーションを作成したら、ユーザはそれを eStreamer サーバに接続し、eStreamer サービスを開始して、データのやりとりを始めることができます。

(注) *eStreamer* サーバとは、eStreamer サービスが実行されている Management Center または管理対象デバイス(バージョン 4.9 以降)です。

eStreamer とクライアントのインタラクションを管理するには、次のタスクを実行します。

1. eStreamer サーバ上で eStreamer を有効にします。

   eStreamer サーバへのアクセス許可、クライアントの追加、および認証された接続を確立するための認証クレデンシャルの生成の詳細については、「eStreamer サーバでの eStreamer の設定(6-1 ページ)」を参照してください。

2. 必要に応じて、手動で eStreamer サービス(eStreamer)を実行します。サービスのステータスを停止、開始、および表示できます。また、コマンドライン オプションを使用して、クライアント/サーバ通信をデバッグできます。

   詳細については、eStreamer サービスの管理(6-4 ページ)を参照してください。

3. オプションとして、eStreamer 参照クライアントを使用して接続またはデータ ストリームをトラブルシューティングするには、クライアントの実行を予定しているコンピュータで参照クライアントを設定します。

   eStreamer 参照クライアントの設定(6-6 ページ)を参照してください。

eStreamer サーバでの eStreamer の設定

License: 任意(Any)

eStreamer サーバとして使用する Management Center または管理対象デバイスが、クライアント アプリケーションへのイベントのストリームを開始する前に、クライアントにイベントを送信するように eStreamer サーバを設定し、クライアントに関する情報を指定して、通信を確立するときに使用する認証クレデンシャルを生成する必要があります。これらのタスクはすべて、Management Center または管理対象デバイスのユーザ インターフェイスから実行できます。

詳細については、次の各項を参照してください。

- eStreamer イベント タイプの設定(6-2 ページ)
- eStreamer クライアントの認証の追加(6-3 ページ)

eStreamer イベント タイプの設定

License: 任意（Any）

eStreamer サーバはどのタイプのイベントを要求するクライアント アプリケーションに送信できるかを制御できます。

管理対象デバイスまたは Management Center で使用可能なイベント タイプは、以下のとおりです。

- 侵入イベント
- 侵入イベント パケット データ
- 侵入イベント追加データ

次のものを含む Management Center で使用可能なイベントのタイプ:

- 検出イベント（これも、接続イベントを有効にします）
- 相関およびホワイトリスト イベント
- 影響フラグ アラート
- ユーザ アクティビティ イベント
- マルウェア イベント
- ファイル イベント

スタック構成 3D9900 ペアのプライマリとセカンダリは、それらが別の管理対象デバイスであるかのように、Management Center に侵入イベントを報告することに注意してください。3D9900 スタックのプライマリで eStreamer クライアントとの通信を設定する場合は、セカンダリでもクライアントを設定する必要があります。クライアント設定は複製されません。同様に、クライアントを削除する場合は、両方で削除します。スタック構成で 3D9900 を管理する Management Center に eStreamer クライアントを設定する場合は、同じイベントが両方によって報告されても、両方の管理対象デバイスから受信するすべてのイベントは Management Center が報告することに注意してください。

高可用性の構成の Management Center で eStreamer クライアントを設定する場合は、クライアントの設定は、プライマリの Management Center からセカンダリの Management Center に複製されません。

eStreamer によってキャプチャされるイベントのタイプを設定する方法:

Access: [管理（Admin）]

手順 1　[システム（System）] > [ローカル（Local）] > [登録（Registration）] を選択します。

手順 2　[eStreamer] をクリックします。

[eStreamer] ページには、[eStreamer イベント設定（eStreamer Event Configuration）] メニューが表示されます。

手順 3　eStreamer でキャプチャし、要求するクライアントに転送するイベントのタイプの横にあるチェックボックスを選択します。チェックボックスが現在オフにされている場合は、データはキャプチャされていないことに注意してください。チェックボックスをオフにしても、すでにキャプチャされたデータは削除されません。

Management Center または管理対象デバイスで、次のいずれかまたはすべてを選択できます。

- [侵入イベント（Intrusion Events）]: 管理対象デバイスによって生成された侵入イベントを送信します。

- [侵入イベント パケット データ（Intrusion Event Packet Data）]：侵入イベントに関連付けられたパケットを送信します。
- [侵入イベント追加データ（Intrusion Event Extra Data）]：HTTP プロキシまたはロード バランサ経由で Web サーバに接続しているクライアントの発信元 IP アドレスに関連付けられている URL など、侵入イベントに関連付けられた追加データを送信します。

Management Center で、次のいずれかまたはすべてを選択できます。

- [検出イベント（Discovery Events）]：ホスト検出イベントを送信します。
- [相関イベント（Correlation Events）]：相関イベントおよびホワイトリスト イベントを送信します。
- [影響フラグ アラート（Impact Flag Alerts）]：Management Center によって生成される影響アラートを送信します。
- [ユーザ アクティビティ イベント（User Activity Events）]：ユーザ イベントを送信します。
- [侵入イベント追加データ（Intrusion Event Extra Data）]：HTTP プロキシまたはロード バランサ経由で Web サーバに接続しているクライアントの発信元 IP アドレスに関連付けられている URL など、侵入イベントの追加データを送信します。

（注） これは、eStreamer サーバが送信できるイベントを制御することに注意してください。クライアント アプリケーションは、ユーザが受信する必要のあるイベントのタイプを明確に要求する必要があります。詳細については、要求フラグ（2-12 ページ）を参照してください。

手順 4　[保存（Save）] をクリックします。

設定が保存され、選択したイベントが、要求時に、eStreamer クライアントに転送されます。

eStreamer クライアントの認証の追加

License: 任意（Any）

eStreamer がクライアントにイベントを送信する前に、eStreamer サーバのピア データベースにクライアントを追加しておく必要があります。また、eStreamer サーバによって生成された認証証明書をクライアントにコピーする必要もあります。

eStreamer クライアントを追加する方法：

Access: [管理（Admin）]

手順 1　[ロ ーカル（Local）] > [登録（Registration）] [eStreamer] > を選択し ます。

[eStreamer] ページが表示されます。

手順 2　[クライアントの作成（Create Client）] をクリックします。

[クライアントの作成（Create Client）] ページが表示されます。

手順 3　[ホスト名（Hostname）] フィールドに、eStreamer クライアントを実行しているホストのホスト名または IP アドレスを入力します。

(注)　ホスト名を使用する場合は、ホスト入力サーバはホストを IP アドレスに解決できる**必要**があります。DNS 解決を設定していない場合、最初に設定するか、IP アドレスを使用する必要があります。

手順 4　証明書ファイルを暗号化するには、[パスワード(Password)] フィールドにパスワードを入力します。

手順 5　[保存(Save)] をクリックします。

eStreamer サーバはクライアント コンピュータから Management Center 上のポート 8302 へのアクセスを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。新しいクライアントが [eStreamer クライアント(eStreamer Client)] の下に表示された状態で、[eStreamer クライアント(eStreamer Client)] ページが再表示されます。

手順 6　証明書ファイルの横にあるダウンロード アイコン( )をクリックします。

手順 7　SSL 認証のためにクライアント コンピュータが使用するディレクトリに証明書ファイルを保存します。

これで、クライアントは Management Center に接続できるようになりました。

ヒント　クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン( )をクリックします。Management Center でホスト入力サービスを再開する必要はありません。アクセスはただちに取り消されます。

eStreamer サービスの管理

License: 任意(Any)

eStreamer サービスはユーザ インターフェイスから管理できます。ただし、サービスを開始/停止する場合は、コマンドラインも使用できます。以降のセクションで eStreamer のコマンド ライン オプションについて説明します。

- eStreamer サービスの開始および停止(6-4 ページ)では、eStreamer サービスを開始および停止する方法を説明しています。
- eStreamer サービスのオプション(6-5 ページ)では、eStreamer サービスで使用可能なコマンドライン オプションとそれらを使用する方法について説明しています。

eStreamer サービスの開始および停止

License: 任意(Any)

eStreamer サービスは、サービスを開始、停止、リロード、および再開できる `manage_estreamer.pl` スクリプトを使用して管理できます。

ヒント　また、eStreamer の初期化スクリプトにコマンド ライン オプションを追加することもできます。詳細については、eStreamer サービスのオプション(6-5 ページ)を参照してください。

次の表で、Management Center または管理対象デバイスで使用可能な manage_estreamer.pl スクリプトのオプションについて説明します。

表 6-1　eStreamer 管理オプション

オプション	説明	選択するオプション番号
enable	サービスを開始します。	3
disable	サービスを停止します。	2
restart	サービスを再開します。	4
status	サービスが実行されているかどうかを示します。	1

eStreamer サービスのオプション

License: 任意（Any）

eStreamer には、サービスをトラブルシューティングすることを可能にする多くのサービス オプションが含まれています。次の表に記載されているオプションは、eStreamer サービスとともに使用できます。

表 6-2　eStreamer サービスのオプション

オプション	説明
--debug	デバッグ レベル ロギングで eStreamer を実行します。エラーは syslog に保存され（--nodaemon とともに使用される際）、画面に表示されます。
--nodaemon	フォアグラウンド プロセスとして eStreamer を実行します。エラーは画面上に表示されます。
--nohostcheck	ホスト名の確認を無効化して eStreamer を実行します。つまり、クライアント ホスト名がクライアント証明書の subjectAltName:dNSName エントリに含まれているホスト名と一致しない場合も、アクセスは依然として許可されます。nohostcheck オプションは、ネットワーク DNS および NAT の設定が、正常なホスト名の確認を防げる場合に役立ちます。その他のセキュリティの確認はすべて実行されることに注意してください。 ⚠ **注意**　このオプションを有効にすると、システムのセキュリティにマイナスに影響する可能性があります。

最初に eStreamer サービスを停止し、次に必要なオプションでサービスを実行し、最後にサービスを再開して、上記のオプションを使用します。たとえば、eStreamer の機能をデバッグするには、デバッグ モードでの eStreamer サービスの実行（6-6 ページ）に記載されている手順に従うことができます。

デバッグ モードでの eStreamer サービスの実行

License: 任意（Any）

デバッグ モードで eStreamer サービスを実行すると、サービスによって生成される各ステータス メッセージを端末画面に表示できます。デバッグを実行するには、次の手順を使用します。

デバッグ モードでの eStreamer サービスの実行:

Access: [管理（Admin）]

手順 1　Management Center または管理対象デバイスに SSH を使用してログインします。

手順 2　`manage_estreamer.pl` を使用して、オプション `2` を選択し、eStreamer サービスを停止します。

手順 3　`./usr/local/sf/bin/sfestreamer --nodaemon --debug` を使用して、デバッグ モードで eStreamer サービスを再開します。

サービスのステータス メッセージが端末画面に表示されます。

手順 4　デバッグを終了したら、`manage_estreamer.pl` を使用し、オプション `4` を選択して通常モードでサービスを再開します。

eStreamer 参照クライアントの設定

eStreamer SDK とともに提供される*参照クライアント*とは、eStreamer API の使用方法を示すために含まれているサンプル クライアント スクリプトおよび Perl モジュールのセットです。これらを実行して eStreamer の出力に習熟したり、これらを使用してカスタム設計クライアントのインストールの問題をデバッグしたりできます。

参照クライアントのセットアップの詳細については、以降の各項を参照してください。

- eStreamer Perl 参照クライアントの設定（6-6 ページ）
- eStreamer Perl 参照クライアントの実行（6-12 ページ）

eStreamer Perl 参照クライアントの設定

eStreamer Perl 参照クライアントを使用するには、まず環境と要件に合うようにサンプル スクリプトを設定する必要があります。

詳細については、次の項を参照してください。

- eStreamer Perl 参照クライアントについて（6-7 ページ）
- eStreamer 参照クライアントの通信の設定（6-7 ページ）
- Perl 参照クライアントのための一般的な前提条件のロード（6-8 ページ）
- Perl SNMP 参照クライアントのための前提条件のロード（6-8 ページ）
- テスト スクリプトで要求されるデータについて（6-8 ページ）
- テスト スクリプトで要求されるデータ タイプの変更（6-10 ページ）
- Perl 参照クライアントのための証明書の作成（6-11 ページ）

eStreamer Perl 参照クライアントについて

eStreamer Perl 参照クライアントを含む `eStreamer SDK.zip` パッケージは、シスコ サポート サイトからダウンロードできます。`eStreamer SDK.zip` パッケージには次のファイルが含まれています。

- `SF_CUSTOM_ALERT.MIB`

  この MIB ファイルは、SNMP トラップを設定するために `snmp.pm` ファイルによって使用されます。
- `SFRecords.pm`

  この Perl モジュールには、検出メッセージのレコード ブロックの定義が含まれています。
- `SFStreamer.pm`

  この Perl モジュールには、Perl クライアントが呼び出す関数が含まれています。
- `SFPkcs12.pm`

  この Perl モジュールはクライアント証明書を解析し、クライアントが eStreamer サーバに接続できるようにします。
- `SFRNABlocks.pm`

  この Perl モジュールには、検出データのブロックの定義が含まれています。
- `ssl_test.pl`

  この Perl スクリプトは、SSL 接続を介した侵入イベント要求をテストするために使用できます。
- `OutputPlugins/csv.pm`

  この Perl モジュールは、侵入イベントをカンマ区切り値の（CSV）の形式に出力します。
- `OutputPlugins/print.pm`

  この Perl モジュールは、人間が解読可能な形式でイベントを出力します。
- `OutputPlugins/snmp.pm`

  この Perl モジュールは、特定の SNMP サーバにイベントを送信します。
- `OutputPlugins/pcap.pm`

  この Perl モジュールは、パケット キャプチャを pcap ファイルとして保存します。
- `OutputPlugins/syslog.pm`

  この Perl モジュールは、ローカルの syslog サーバにイベントを送信します。

eStreamer 参照クライアントの通信の設定

参照クライアントは、データ通信にセキュア ソケット レイヤ（SSL）を使用します。クライアントとして使用する予定のコンピュータに OpenSSL をインストールし、環境に合わせて適切に設定する必要があります。

（注）　Linux のオペレーティング システムの初期インストールの場合は、このダウンロードの一部として `libssl-dev` コンポーネントをインストールする必要があります。

クライアントでの SSL の設定:

手順 1　OpenSSL を http://openssl.org/source/ からダウンロードします。

手順 2　`/Usr/local/src` にソースを展開します。

手順 3　Configure スクリプトを実行して、ソースを設定します。

手順 4　コンパイル対象のソースに Make を実行し、インストールします。

Perl 参照クライアントのための一般的な前提条件のロード

eStreamer Perl 参照クライアントを実行する前に、クライアント コンピュータに IO::Socket::SSL Perl モジュールをインストールする必要があります。モジュールは手動でインストールすることも、cpan を使用してインストールすることもできます。

（注）　クライアント コンピュータに Net::SSLeay モジュールがインストールされていない場合は、そのモジュールも同様にインストールします。Net::SSLeay は OpenSSL との通信に必要です。

eStreamer サーバへの SSL 接続をサポートするためには、OpenSSL もインストールし、設定する必要があります。詳細については、eStreamer 参照クライアントの通信の設定（6-7 ページ）を参照してください。

Perl SNMP 参照クライアントのための前提条件のロード

Perl 参照クライアントの eStreamer SNMP モジュールを実行する前に、クライアント コンピュータのクライアント オペレーティング システムで使用可能な最新の net-snmp Perl モジュールをインストールする必要があります。

Perl 参照クライアントのダウンロードと展開

eStreamer Perl 参照クライアントを含む EventStreamerSDK.zip ファイルは、シスコ サポート サイトからダウンロードできます。

クライアントを実行する予定の Linux オペレーティング システムを実行しているコンピュータで zip ファイルを展開します。

テスト スクリプトで要求されるデータについて

デフォルトで、参照クライアントで ssl_test -o 設定を使用する際は、次の表に示すようにデータを要求します。

表 6-3　出力プラグインで作成されるデフォルト要求

構文	プラグインの呼び出し	送信内容	要求するデータ
./ssl_test.pl *eStreamerServerName* -h HostIPAddresses	該当なし	ホスト要求、メッセージ タイプ 5、ビット 11 で 1 に設定	ホスト データ（ホスト データおよびマルチ ホスト データ メッセージの形式（2-31 ページ）を参照してください。）
./ssl_test.pl *eStreamerServerName* -d "Global \ domain \ subdomain"	該当なし	指定されたドメインまたはサブドメインに対するイベント ストリーム要求。	指定されたドメインに対するイベント情報のストリーム（ドメイン ストリーミング要求メッセージの形式（2-36 ページ）を参照してください。）

表 6-3　出力プラグインで作成されるデフォルト要求（続き）

構文	プラグインの呼び出し	送信内容	要求するデータ
`./ssl_test.pl` *eStreamerServerName* `-o print -f` *TextFile*	OutputPlugins/print.pm	イベント ストリーム要求、メッセージ タイプ 2、ビット 2 および 20 ～ 24 を 1 に設定	イベント データ（イベント ストリーム要求メッセージの形式（2-11 ページ）、相関ポリシー レコード（3-25 ページ）、相関ルール レコード（3-27 ページ）、ディスカバリ イベントのメタデータ（4-8 ページ）、イベント タイプ別ホスト ディスカバリ構造（4-44 ページ）、およびホスト IOC セット メッセージ（4-61 ページ）を参照してください。） eStreamer は、ビット 2 がイベント ストリーム要求に設定されているため、タイプ 1 の侵入イベントを送信します。
`./ssl_test.pl` *eStreamerServerName* `-o pcap -f` *TargetPCAPFile*	OutputPlugins/pcap.pm	イベント ストリーム要求、メッセージ タイプ 2、ビット 0 および 23 を 1 に設定	パケット データ（イベント データ メッセージの形式（2-18 ページ）およびパケット レコード 4.8.0.2 以上（3-6 ページ）を参照してください。） eStreamer は、ビット 0 がイベント ストリーム要求に設定されているため、パケットデータのみを送信します。
`./ssl_test.pl` *eStreamerServerName* `-o csv -f` *CSVFile*	OutputPlugins/csv.pm	イベント ストリーム要求、メッセージ タイプ 2、ビット 2 および 23 を 1 に設定	侵入イベント データ（イベント データ メッセージの形式（2-18 ページ）および侵入イベント レコード 6.0 以上（3-8 ページ）を参照してください。） eStreamer は、ビット 2 がイベント ストリーム要求に設定されているため、タイプ 1 の侵入イベントを送信します。
`./ssl_test.pl` *eStreamerServerName* `-o snmp -f` *SNMPServer*	OutputPlugins/snmp.pm	イベント ストリーム要求、メッセージ タイプ 2、ビット 2、20、および 23 を 1 に設定	侵入イベント データ（イベント データ メッセージの形式（2-18 ページ）および侵入イベント レコード 6.0 以上（3-8 ページ）を参照してください。） eStreamer は、ビット 2 がイベント ストリーム要求に設定されているため、タイプ 1 の侵入イベントを送信します。
`./ssl_test.pl` *eStreamerServerName* `-o syslog`	OutputPlugins/syslog.pm	イベント ストリーム要求、メッセージ タイプ 2、ビット 2、20、および 23 を 1 に設定	侵入イベント データ（イベント データ メッセージの形式（2-18 ページ）および侵入イベント レコード 6.0 以上（3-8 ページ）を参照してください。） eStreamer は、ビット 2 がイベント ストリーム要求に設定されているため、タイプ 1 の侵入イベントを送信します。

テスト スクリプトで要求されるデータ タイプの変更

SFStreamer.pm Perl モジュールは、データを要求する際に、サンプル スクリプトで使用できる複数の要求フラグの変数を定義します。次の表では、イベント ストリーム要求メッセージで、各要求フラグを設定するために呼び出す要求フラグの変数を示しています。出力モジュールのいずれかを使用してさまざまなデータを要求する場合は、モジュールの $FLAG の設定を編集できます。

要求フラグ、お客様が要求するデータ、各フラグに対応する製品バージョンの詳細については、要求フラグ (2-12 ページ) を参照してください。

表 6-4　サンプル スクリプトで使用される要求フラグ変数

変数	設定する要求フラグ	要求するデータ
$FLAG_PKTS	0	パケット データ
$FLAG_METADATA	1	バージョン 1 のメタデータ
$FLAG_IDS	2	タイプ 1 の侵入イベント
$FLAG_RNA	3	バージョン 1 の検出イベント
$FLAG_POLICY_EVENTS	4	バージョン 1 の相関イベント
$FLAG_IMPACT_ALERTS	5	侵入の影響アラート
$FLAG_IDS_IMPACT_FLAG	6	タイプ 7 の侵入イベント
$FLAG_RNA_EVENTS_2	7	バージョン 2 の検出イベント
$FLAG_RNA_FLOW	8	バージョン 1 の接続データ
$FLAG_POLICY_EVENTS_2	9	バージョン 2 の相関イベント
$FLAG_RNA_EVENTS_3	10	バージョン 3 の検出イベント
$FLAG_HOST_ONLY	11	$FLAG_HOST_SINGLE (1 台のホスト用) または $FLAG_HOST_MULTI (複数のホスト用) とともに送信される場合は、イベント データのないホスト データのみ
$FLAG_RNA_FLOW_3	12	バージョン 3 の接続データ
$FLAG_POLICY_EVENTS_3	13	バージョン 3 の相関イベント
$FLAG_METADATA_2	18	バージョン 2 のメタデータ
$FLAG_METADATA_3	15	バージョン 3 のメタデータ
$FLAG_RNA_EVENTS_4	17	バージョン 4 の検出イベント
$FLAG_RNA_FLOW_4	18	バージョン 4 の接続データ
$FLAG_POLICY_EVENTS_4	19	バージョン 4 の相関イベント
$FLAG_METADATA_4	20	バージョン 4 のメタデータ
$FLAG_RUA	21	ユーザ アクティビティ イベント
$FLAG_POLICY_EVENTS_5	22	バージョン 5 の相関イベント
$FLAGS_SEND_ARCHIVE_TIMESTAMP	23	タイムスタンプを含む拡張されたイベント ヘッダーは、eStreamer サーバでの処理のためにイベントがアーカイブされたときに適用されます
$FLAG_RNA_EVENTS_5	24	バージョン 5 の検出イベント
$FLAG_RNA_EVENTS_6	25	バージョン 6 の検出イベント

表 6-4　サンプル スクリプトで使用される要求フラグ変数（続き）

変数	設定する要求フラグ	要求するデータ
$FLAG_RNA_FLOW_5	26	バージョン 5 の接続データ
$FLAG_EXTRA_DATA	27	侵入イベント追加データ レコード
$FLAG_RNA_EVENTS_7	36	バージョン 7 の検出イベント
$FLAG_POLICY_EVENTS_6	29	バージョン 6 の相関イベント
$FLAG_DETAIL_REQUEST	30	eStreamer に対する拡張された要求

注意　バージョン 5.x より前は、すべてのイベント タイプでは、参照クライアントは `detection engine ID` フィールドを `sensor ID` としてラベル付けしています。

Perl 参照クライアントのための証明書の作成

License: 任意（Any）

Perl 参照クライアントを使用する前に、Management Center または管理対象デバイスで、クライアントを実行するコンピュータ用に証明書を作成する必要があります。次に、証明書ファイルをクライアント コンピュータにダウンロードし、それを使用して証明書（`server.crt`）および RSA キー ファイル（`server.key`）を作成します。

Perl 参照クライアントのための証明書の作成:

Access: [管理（Admin）]

手順 1　[運用（Operations）] > [設定（Configuration）] > [eStreamer] を選択します。

[eStreamer] ページが表示されます。

手順 2　[クライアントの作成（Create Client）] をクリックします。

[クライアントの作成（Create Client）] ページが表示されます。

手順 3　[ホスト名（Hostname）] フィールドに、eStreamer クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注）　ホスト名を使用する場合は、ホスト入力サーバはホストを IP アドレスに解決できる**必要**があります。DNS 解決を設定していない場合、最初に設定するか、IP アドレスを使用する必要があります。

手順 4　証明書ファイルを暗号化するには、[パスワード（Password）] フィールドにパスワードを入力します。

手順 5　[保存（Save）] をクリックします。

eStreamer サーバはクライアント コンピュータから Management Center 上のポート 8302 へのアクセスを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。新しいクライアントが [eStreamer クライアント（eStreamer Client）] の下に表示された状態で、[eStreamer クライアント（eStreamer Client）] ページが再表示されます。

手順 6　証明書ファイルの横にあるダウンロード アイコン（ ）をクリックします。

手順 7　SSL 認証のためにクライアント コンピュータが使用するディレクトリに証明書ファイルを保存します。

これで、クライアントは Management Center に接続できるようになりました。

ヒント　クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン( )をクリックします。Management Center でホスト入力サービスを再開する必要はありません。アクセスはただちに取り消されます。

eStreamer Perl 参照クライアントの実行

eStreamer Perl 参照クライアント スクリプトは、Linux カーネルを備えた 64 ビットのオペレーティング システムで使用するように設計されていますが、クライアント マシンがeStreamer Perl 参照クライアントの設定（6-6 ページ）で定義されている前提条件を満たしていれば、任意の POSIX ベースの 64 ビットのオペレーティング システムでも機能します。

詳細については、次の項を参照してください。

- ホストの要求を使用した SSL 上のクライアント接続のテスト（6-12 ページ）
- 参照クライアントを使用した PCAP のキャプチャ（6-13 ページ）
- 参照クライアントを使用した CSV レコードのキャプチャ（6-13 ページ）
- 参照のクライアントを使用した SNMP サーバへのレコードの送信（6-13 ページ）
- 参照クライアントを使用した Syslog へのイベントのロギング（6-13 ページ）
- IPv6 アドレスへの接続（6-14 ページ）

ホストの要求を使用した SSL 上のクライアント接続のテスト

`Ssl_test.pl` スクリプトを使用すると、eStreamer サーバおよび eStreamer クライアント間で接続をテストできます。`ssl_test.pl` スクリプトはどのレコード タイプも処理し、STDOUT または指定する出力プラグインにこれを出力します。出力オプションを使用せずに `-h` オプションを使用すると、指定したホストのホスト データが端末にストリームされます。

（注）　STDOUT へ raw パケット データを出力すると端末を干渉するため、出力プラグインへの方向付けをせずに、このスクリプトを使用してパケット データをストリームすることはできません。

次の構文と、`ssl_test.pl` スクリプトを使用して、標準的な出力にホスト データを送信します。

```
./ssl_test.pl eStreamer ServerIPAddress -h HostIPAddresses
```

たとえば、10.10.0.4 の IP アドレスの eStreamer サーバへの接続を介した 10.0.0.0/8 サブネット上のホストのホスト データの受信をテストするには、次の構文を使用します。

```
./ssl_test.pl 10.10.0.4 -h 10.0.0.0/8
```

参照クライアントを使用した PCAP のキャプチャ

ストリームされたパケット データを PCAP ファイルでキャプチャし、クライアントが受信するデータの構造を確認する場合に、参照クライアントを使用できます。-o pcap 出力オプションを使用する際は、-f を使用してターゲット ファイルを指定する必要があることに注意してください。

ssl_test.pl スクリプトを使用して、ストリームされたパケット データを PCAP ファイルでキャプチャするには、次の構文を使用します。

```
./ssl_test.pl eStreamer ServerIPAddress -o pcap -f ResultingPCAPFile
```

たとえば、10.10.0.4 の IP アドレスの eStreamer サーバからストリームされたイベントを使用して、test.pcap という名前の PCAP ファイルを作成するには、次の構文を使用します。

```
./ssl_test.pl 10.10.0.4 -o pcap -f test.pcap
```

参照クライアントを使用した CSV レコードのキャプチャ

ストリームされた侵入イベント データを CSV ファイルでキャプチャし、クライアントが受信するデータの構造を確認する場合も、参照クライアントを使用できます。

次の構文を使用して streamer_csv.pl スクリプトを実行します。

```
./ssl_test.pl eStreamer ServerIPAddress -o csv -f ResultingCSVFile
```

たとえば、10.10.0.4 の IP アドレスの eStreamer サーバからストリームされたイベントを使用して、test.csv という名前の CSV ファイルを作成するには、次の構文を使用します。

```
./ssl_test.pl 10.10.0.4 -o csv -f test.csv
```

参照のクライアントを使用した SNMP サーバへのレコードの送信

侵入イベント データを SNMP サーバにストリームする場合も、参照クライアントを使用できます。-f オプションを使用して、イベントを受信する SNMP トラップ サーバの名前を示します。この出力方法では、パスに snmptrapd という名前のバイナリが必用であるため、UNIX のようなシステムでのみ機能することに注意してください。

SNMP サーバに侵入イベントを送信するには、次の構文を使用します。

```
./ssl_test.pl eStreamer ServerIPAddress -o snmp
   -f SNMPServerName
```

たとえば、10.10.0.4 の IP アドレスの eStreamer サーバからストリームされたイベントを使用して、10.10.0.3 で SNMP サーバにイベントを送信するには、次の構文を使用します。

```
./ssl_test.pl 10.10.0.4 -o snmp -f 10.10.0.3
```

参照クライアントを使用した Syslog へのイベントのロギング

クライアントのローカル syslog サーバに侵入イベントをストリームする場合も、参照クライアントを使用できます。

Syslog にイベントを送信するには、次の構文を使用します。

```
./ssl_test.pl eStreamer ServerIPAddress -o syslog
```

たとえば、10.10.0.4 の IP アドレスの eStreamer サーバからストリームされたイベントを記録するには、次の構文を使用します。

```
./ssl_test.pl 10.10.0.4 -o syslog
```

IPv6 アドレスへの接続

プライマリ管理インターフェイスを介して IPv6 アドレスの Management Center に接続する場合も、参照クライアントを使用できます。クライアントのマシンには Socket6 および IO::Socket::INET6 Perl モジュールがインストールしてある必要があり、`-ipv6` オプションまたは短縮形式の `-i` を使用します。

ssl_test.pl スクリプトを使用して IPv6 アドレスを指定するには、次の構文を使用します。

```
./ssl_test.pl -ipv6 eStreamer ServerIPAddress
```

または

```
./ssl_test.pl -i eStreamer ServerIPAddress
```

たとえば、IPv6 アドレス `2001:470:e09c:20:7c1e:5248:1bf7:2ea0` を使用して Management Center に接続するには、次の構文を使用します。

```
./ssl_test.pl -ipv6 2001:470:e09c:20:7c1e:5248:1bf7:2ea0
```

データ構造の例

この付録には、一部の侵入、相関、ディスカバリの各イベントのデータ構造の例が記載されています。それぞれの例は、各ビットがどのように設定されているかを明確に示すため、2 進数形式で表示されます。

詳細については、次の各項を参照してください。

- 侵入イベントのデータ構造の例
- ディスカバリ データ構造の例（A-18 ページ）

侵入イベントのデータ構造の例

このセクションには、侵入イベントについて eStreamer で送信される可能性があるデータ構造の例が記載されています。ここでは、次の例を示します。

- Management Center 5.4+ の侵入イベントの例（A-1 ページ）
- 侵入影響アラートの例（A-7 ページ）
- パケット レコードの例（A-9 ページ）
- 分類レコードの例（A-10 ページ）
- 優先度レコードの例（A-12 ページ）
- ルール メッセージ レコードの例（A-12 ページ）
- バージョン 5.1+ ユーザ イベントの例（A-15 ページ）

Management Center 5.4+ の侵入イベントの例

次の図に、イベント レコードの例を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1	1	0

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
3	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
5	0	1	0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0
11	0	1	0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	1	1	1	0	0	1	1	1	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	1	1	1	1	0	1	1	1	0	1	1	1	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	1	1	1	0	0	0	1	0	0	0	0	1	0	1
20	1	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	1	0	0	1	0	0	0	0
21	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	1	0	1	0	1	0	0	0	0	0	0	1	1	0	0	1	1	1	0	1	0	0	1	1	0	1	1	1	1	1	1	0
	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	0	0
	1	0	1	0	0	1	0	0	1	0	0	0	0	1	0	1	1	1	0	1	0	0	0	0	0	1	1	1	0	0	0	1
	1	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	1	0	0	0	1	0	0	1	1	0	1	0	0	0	1	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	1	1
27	0	1	1	1	0	1	1	1	0	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	1	0	1	0	0	1	0	0
36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	1	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
30	1	1	0	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	1	0
	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	0	0
	1	0	1	0	0	1	0	1	1	1	1	1	0	1	1	0	1	0	1	1	0	0	1	1	0	0	0	0	1	0	0	1
	0	1	0	0	0	0	0	1	1	0	0	1	0	1	1	1	1	0	0	1	1	1	1	1	0	0	0	1	0	1	0	0
31	0	1	1	0	1	0	0	1	0	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	0	0	0	1	1	0	1	0
	1	1	1	1	1	1	1	0	0	0	1	1	1	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	1	0	1	0	0	0	1	0	1	0	0	1	0	0	0	0	1	0	1	0	0	1	1	0	0	1	1	0	1
	1	0	1	0	1	0	1	1	0	0	0	1	0	1	0	0	1	1	0	0	1	1	1	1	1	0	0	1	1	1	0	0
32	0	1	1	0	1	0	0	1	0	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	0	0	0	1	1	0	1	0
	1	1	1	1	1	1	1	0	0	0	1	1	1	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	1	0	1	0	0	0	1	0	1	0	0	1	0	0	0	0	1	0	1	0	0	1	1	0	0	1	1	0	1
	1	0	1	0	1	0	1	1	0	0	0	1	0	1	0	0	1	1	0	0	1	1	1	1	1	0	0	1	1	1	0	0
33	0	0	1	0	1	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	0	0	1	1	0	0	1	1	0	0	0	0
	1	1	1	1	1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	1
	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	0	0	1	0	0	0	1	1	0	1	0	0	1	0	0	1	1

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
34	0	0	1	0	1	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	0	0	1	1	0	0	1	1	0	0	0	0
	1	1	1	1	1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	1
	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	0	0	1	0	0	0	1	1	0	1	0	0	1	0	0	1	1
35	0	1	0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1
36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1	0	0	0	0	1	1	0
37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
38	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
54	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0																

上記の例では、次のイベント情報を確認できます。

番号	説明
1	この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ(つまり、メッセージ タイプ 4)であることを示しています。
2	この行は、後続のメッセージの長さが 294 バイトであることを示しています。
3	この先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーであることを示すフラグです。後続の 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプション フィールドです。行の残りの部分は、レコード タイプの値 400 を示し、侵入イベント レコードを表しています。
4	この行は、後続のイベント レコードの長さが 278 バイトであることを示しています。
5	この行は、イベントの保存時のタイムスタンプです。この場合、2014 年 7 月 2 日(水)の 16 時 11 分 27 秒に保存されています。
6	この行は、将来使用するために予約されており、ゼロが入っています。
7	この行は、ブロック タイプが 45 であることを示しています。これは、バージョン 5.4+ の侵入イベント レコードのブロック タイプです。
8	この行は、データ ブロックの長さが 278 バイトであることを示しています。
9	この行は、イベントがセンサー番号 5 から収集されることを示しています。
10	この行は、イベント ID 番号が 65580 であることを示しています。
11	この行は、イベントが 1404317489 秒で発生したことを示しています。
12	この行は、イベントが 46542 マイクロ秒で発生したことを示しています。
13	この行は、ルール ID 番号が 4 であることを示しています。
18	この行は、イベントがジェネレータ ID 番号 119(ルール エンジン)で検出されたことを示しています。
15	この行は、ルールのリビジョン番号が 1 であることを示しています。
16	この行は、分類 ID 番号が 1 であることを示しています。
17	この行は、優先度 ID 番号が 3 であることを示しています。
18	この行は、送信元 IP アドレスが 10.5.61.220 であることを示しています。このフィールドには IPv4 アドレスと IPv6 アドレスのいずれかが含まれる可能性があることに注意してください。
19	この行は、宛先 IP アドレスが 10.5.56.133 であることを示しています。このフィールドには IPv4 アドレスと IPv6 アドレスのいずれかが含まれる可能性があることに注意してください。
20	この行の最初の 2 バイトは送信元ポート番号が 33018 であることを示し、2 番目の 2 バイトは宛先ポート番号が 8080 であることを示しています。

番号	説明
21	この行の最初のバイトは、TCP(6)がイベントで使用されているプロトコルであることを示しています。2 番目のバイトは影響フラグであり、2 番目のビットが 1 であるため、イベントがレッド(脆弱)であることを示します。また、送信元または宛先ホストはシステムによってモニタされているネットワーク内にあること、送信元または宛先ホストがネットワーク マップにあること、送信元または宛先ホストがイベント発生ポートでサーバを実行していることを示します。さらに、2 番目と 3 番目のフラグが 1 であるため、これがオレンジ(脆弱の可能性あり)のイベントであることを示しています。この行の 3 番目のバイトは影響フラグです。2 であるため、イベントがオレンジ(脆弱の可能性あり)であることを示しています。最後のバイトはイベントがブロックされなかったことを示しています。
22	この行には、MPLS ラベルが含まれます(存在する場合)。
23	この行の最初の 2 バイトは VLAN ID が 0 であることを示しています。最後の 2 バイトは、予約されており、0 に設定されています。
24	この行には、侵入ポリシーの一意の ID 番号が含まれます。
25	この行には、ユーザの内部 ID 番号が含まれます。該当のユーザが存在しないため、すべてゼロになっています。
26	この行には Web アプリケーションの内部 ID 番号が含まれ、この場合は 847 となっています。
27	この行にはクライアント アプリケーションの内部 ID 番号が含まれ、この場合は 2000000676 となっています。
36	この行にはアプリケーション プロトコルの内部 ID 番号が含まれ、この場合は 676 となっています。
29	この行には、アクセス制御ルールの一意の ID が含まれ、この場合は 1 となっています。
30	この行には、アクセス制御ポリシーの一意の ID が含まれます。
31	この行には、入力インターフェイスの一意の ID が含まれます。
32	この行には、出力インターフェイスの一意の ID が含まれます。このイベントはブロックされています。
33	この行には、入力セキュリティ ゾーンの一意の ID が含まれます。
34	この行には、出力セキュリティ ゾーンの一意の ID が含まれます。
35	この行には、侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプが含まれます。
36	この行の最初の 2 バイトは、接続イベントが生成された管理対象デバイスの Snort インスタンスの数値 ID を示します。残りの 2 バイトは、同じ秒の間に発生する接続イベントを区別するために使用される値を示します。
37	この行の最初の 2 バイトは、送信元ホストの国のコードを示します。残りの 2 バイトは、宛先ホストの国のコードを示します。
38	この行の最初の 2 バイトには、このイベントに関連付けられている侵害の ID 番号が含まれます。残りの 2 バイトには、トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号の最初の部分が含まれます。
39	この行には、トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号の残りの部分が含まれます。
40	この行の最初の 2 バイトには、トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の最後の 2 バイトが含まれます。SSL が使用された場合、2 番目の 2 バイトには、SSL サーバ証明書の SHA1 ハッシュの最初の部分が含まれます。

番号	説明
41	SSL が使用された場合、この行には、SSL サーバ証明書の SHA1 ハッシュの残りの部分が含まれます。
54	この行の最初の 2 バイトには、SSL サーバ証明書の SHA1 ハッシュの最後の 2 バイトが含まれます。2 番目の 2 バイトには、実際に実行された SSL アクションが含まれます。この接続では SSL が使用されなかったため、0 になっています。
43	この行の最初の 2 バイトには、SSL フロー ステータスが含まれます。この接続では SSL が使用されなかったため、0 になっています。2 番目の 2 バイトには、このイベントに関連付けられているネットワーク分析ポリシーの UUID の最初の 2 バイトが含まれます。
44	この行には、このイベントに関連付けられているネットワーク分析ポリシーの UUID の残りの部分が含まれます。

侵入影響アラートの例

次の図に、侵入影響アラート レコードの例を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	1	0	0	0	1	0	1	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
9	0	1	0	0	0	0	0	0	1	1	0	0	1	1	0	1	1	0	1	1	0	1	1	1	1	0	0	1	0	1	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
11	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0
15	0	1	0	1	0	1	1	0	0	1	1	1	0	1	0	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1	0
	0	1	1	0	0	1	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	0
	0	1	1	0	1	1	0	0	0	1	1	0	0	1	0	1																

上記の例では、次の情報を確認できます。

番号	説明
1	この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ（メッセージ タイプ 4）であることを示しています。
2	この行は、後続のメッセージの長さが 58 バイトであることを示しています。
3	この行の先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーではないことを示すフラグです。後続の 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプション フィールドです。行の残りの部分は、レコード タイプの値 9 を示し、影響アラート レコードを表しています。
4	この行は、後続のデータの長さが 50 バイトであることを示しています。
5	この行には値 20 が含まれており、侵入影響アラート データ ブロックが後に続いていることを示しています。
6	この行は、影響アラート ブロック ヘッダーを含む影響アラート ブロックの長さを示し、この場合は 50 バイトです。
7	この行は、イベント ID 番号が 201256 であることを示しています。
8	この行は、イベントがデバイス番号 2 から収集されることを示しています。
9	この行は、イベントが 1087223700 秒で発生したことを示しています。
10	この行は、イベントに関連付けられている影響レベルが 1（赤、脆弱）であることを示しています。
11	この行は、違反イベントに関連付けられている IP アドレスが 172.16.1.22 であることを示しています。
12	この行は、違反に関連付けられている宛先 IP アドレスがないことを示しています（値は 0 に設定）。
13	この行は、文字列ブロックの長さとテキスト文字列を含む文字列ブロックが続くことを示します。この場合、テキスト文字列は影響名です。文字列ブロックの詳細については、文字列データ ブロック (3-62 ページ) を参照してください。
18	この行は、文字列ブロック インジケータを含めた文字列ブロックのトータル長が 18 バイトであることを示しています。これには、影響の説明の 10 バイトと文字列ヘッダーの 8 バイトが含まれています。
15	この行は、影響の説明が「Vulnerable（脆弱）」であることを示しています。

パケット レコードの例

次の図に、パケット レコードの例を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	1	1	0	1	
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	1	0	1
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1	0	1	1	0	1	1	0	0	1	1
7	0	0	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	0	1	1	1	0	0	1	0
8	0	0	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	0	1	1	1	0	1	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	1	0	0	1	1	1	0	1
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	0	1
12	0	0	1	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0
	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	1	1	0	1	0	0	0	1	0	0	0	0

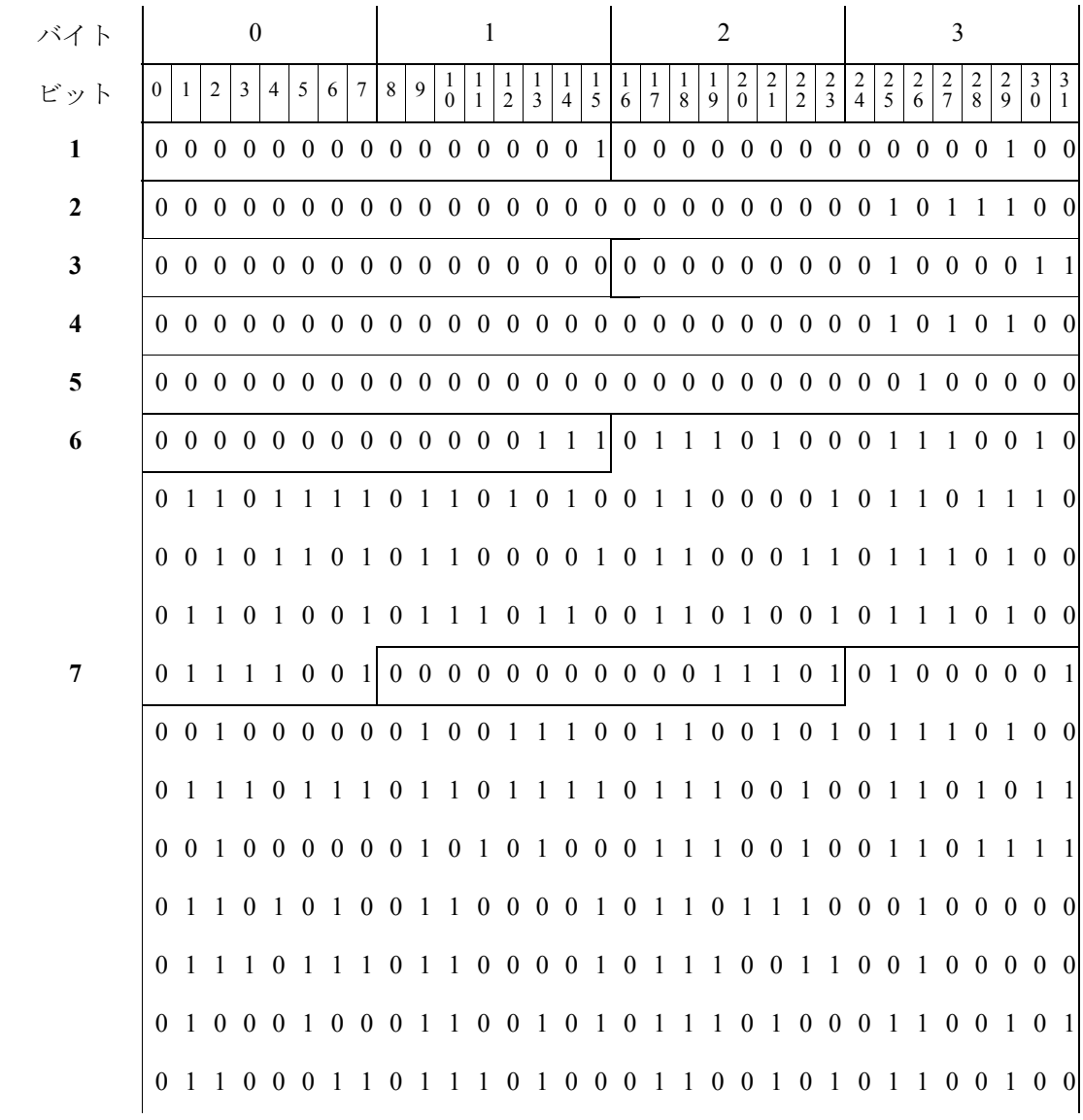
上記の例では、次のパケット情報を確認できます。

番号	説明
1	この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ(メッセージ タイプ 4)であることを示しています。
2	この行は、後続のメッセージの長さが 989 バイトであることを示しています。
3	この行の先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーではないことを示すフラグです。後続の 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプション フィールドです。行の残りの部分は、レコード タイプの値 2 を示し、パケット レコードを表します。
4	この行は、後続のパケット レコードの長さが 981 バイトであることを示しています。
5	この行は、イベントがデバイス番号 3 から収集されることを示しています。
6	この行は、イベント ID 番号が 195430 であることを示しています。
7	この行は、イベントが 10572378 秒で発生したことを示しています。

番号	説明
8	この行は、パケットが 10572380 秒で収集されたことを示しています。
9	この行は、パケットが 254365 マイクロ秒で収集されたことを示しています。
10	この行は、リンク タイプが 1(イーサネット層)であることを示しています。
11	この行は、後続のパケット データの長さが 953 バイトであることを示しています。
12	この行と次の行は、実際のペイロード データを示します。実際のデータは 953 バイトであり、この例では切り捨てられていることに注意してください。

分類レコードの例

次の図に、分類レコードの例を示します。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
8	1	0	0	1	1	1	0	1	1	1	0	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	1	0	1	0	0	0
	1	1	0	0	1	0	1	1	1	0	1	0	0	0	1	0	0	0	0	1	0	0	0	1	1	1	0	1	1	0	0	1
	1	0	0	0	1	0	0	1	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
	0	1	0	1	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

上記の例では、次のイベント情報を確認できます。

番号	説明
1	行の最初の 2 バイトは、標準ヘッダー値 `1` を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ（メッセージ タイプ 4）であることを示しています。
2	この行は、後続のメッセージの長さが `92` バイトであることを示しています。
3	この行の先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーではないことを示すフラグです。後続の 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプション フィールドです。行の残りの部分は、レコード タイプの値 `67` を示し、分類レコードを表します。
4	この行は、後続の分類レコードの長さが `84` バイトであることを示しています。
5	この行は、分類 ID が `35` であることを示しています。
6	この行の最初の 2 バイトは、後続の分類名の長さが `15` バイトであることを示しています。2 番目の 2 バイトは、分類名自体で始まり、この場合は「trojan-activity（トロイの木馬アクティビティ）」です。
7	この行の先頭バイトは、行 6 で説明している分類名の続きです。この行の最初の 2 バイトは、後続の説明の長さが `29` バイトであることを示しています。残りのバイトは、分類の説明で始まり、この場合は「`A Network Trojan was Detected.`（ネットワークでトロイの木馬が検出されました。）」です。
8	この行は、分類の一意の ID としての役割を果たす分類 ID 番号を示します。
9	この行は、分類のリビジョンの一意の ID としての役割を果たす分類リビジョン ID 番号を示し、この場合、分類のリビジョンがないため、Null です。

優先度レコードの例

次に、優先度レコードの例を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	0	0	0	0	1	1	0	1	0	0	1
	0	1	1	0	0	1	1	1	0	1	1	0	1	0	0	0																

上記の例では、次のイベント情報を確認できます。

番号	説明
1	この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ（メッセージ タイプ 4）であることを示しています。
2	この行は、後続のメッセージが 16 バイトであることを示しています。
3	この行は、レコード タイプの値 4 を示し、優先度レコードを表します。
4	この行は、後続の優先度レコードの長さが 8 バイトであることを示しています。
5	この行は、優先度 ID が 1 であることを示しています。
6	この行の最初の 2 バイトは、優先度名に 4 バイトが含まれていることを示しています。2 番目の 2 バイトと次の行の 2 バイトは、優先度名自体（「high（高）」）を示しています。

ルール メッセージ レコードの例

次に、ルール メッセージ レコードの例を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	1	1	0	1	0	0	1	0	1
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	1	1	0	1	0	0	1	0	1
9	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1
	0	0	1	0	0	1	1	1	0	0	1	1	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	1	1	1	1	1
	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	1	0	0	1
	1	0	0	0	0	1	0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	0	0	1	1	1	1	0	0	0	1	1
10	0	1	1	0	1	1	0	1	1	1	0	1	0	0	1	0	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1
	0	0	1	0	1	0	1	0	1	0	1	0	0	1	0	1	0	0	1	0	0	1	1	0	0	0	0	1	1	1	1	1
	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	1	0	0	1
	1	0	0	0	0	1	0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	0	0	1	1	1	1	0	0	0	1	1
11	0	1	1	0	1	1	0	1	1	1	0	1	0	0	1	0	0	1	0	0	0	0	0	1	0	1	0	1	0	0	0	0
	0	1	0	1	0	0	0	0	0	0	1	0	1	1	0	1	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	1
	0	1	0	1	0	1	0	0	0	1	0	0	0	1	0	1	0	1	0	0	0	0	1	1	0	1	0	1	0	1	0	0
	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	1	1	1	0	0	1	0	1	0	0	1	1
	0	0	1	0	0	0	0	0	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	1	1	1	0	0	0	1
	0	1	1	1	0	1	0	1	0	1	1	0	0	1	0	1	0	1	1	1	0	0	1	1	0	1	1	1	0	1	0	0
	0	0	1	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	1	1	1	1	0	1	1	1	0	0	1	0
	0	0	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	1	1	0	1	1	1	1	0	1	1	1	0	1	0	0
	0	1	1	0	0	1	0	1	0	1	1	0	1	1	1	0	0	1	1	1	0	1	0	0	0	1	1	0	1	0	0	1
	0	1	1	0	0	0	0	0	1	0	1	1	0	1	1	0	0	0	0	1	0	0	0	0	0	1	1	0	1	1	0	1
	0	1	1	0	0	0	0	1	0	1	1	0	1	1	0	0	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	1
	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0	0	1	1

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	1	1	0	0	0	0	1	0	1	1	0	0	1	1	0	0	1	1	0	0	1	0	1	0	1	0	0	0	1	1	1
	0	1	1	1	0	1	0	1	0	1	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	0
	0	0	1	0	0	0	0	0	0	1	1	1	0	1	0	0	0	1	1	0	0	1	1	1	0	0	1	0	0	0	0	0
	0	1	1	0	0	1	0	0	0	1	1	0	1	1	1	1	0	1	1	0	1	1	0	1	0	1	1	0	0	0	0	1
	0	1	1	0	1	0	0	1	0	1	1	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1
	0	0	1	1	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	1	0	1	1	1	0	0	1	1	0	0	0	1	1
	0	1	1	0	1	1	1	0																								

上記の例では、次のイベント情報を確認できます。

番号	説明
1	この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ(つまり、メッセージ タイプ 4)であることを示しています。
2	この行は、後続のメッセージが 129 バイトであることを示しています。
3	この行の先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーではないことを示すフラグです。後続の 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプション フィールドです。行の残りの部分は、レコード タイプの値 66 を示し、ルール メッセージ レコードを表します。
4	この行は、後続のルール メッセージ レコードの長さが 121 バイトであることを示しています。
5	この行は、ジェネレータ ID 番号が 1(ルール エンジン)であることを示しています。
6	この行は、ルール ID 番号が 28069 であることを示しています。
7	この行は、ルールのリビジョン番号が 1 であることを示しています。
8	この行は、Firepower システム に渡されたルール ID 番号が 28069 であることを示しています。
9	この行の最初の 2 バイトは、ルール テキスト名に 71 バイトが含まれていることを示しています。2 番目の 2 バイトは、ルールの一意の ID 番号で始まります。
10	この行の最初の 2 バイトは、ルールの一意の ID 番号で終わります。次の 2 バイトは、ルールのリビジョンの一意の ID 番号で始まります。
11	この行の最初の 2 バイトは、ルールのリビジョンの一意の ID 番号で終わります。2 番目の 2 バイトは、ルール メッセージ自体のテキストで始まります。送信されたルール メッセージのフルテキストは「APP-DETECT DNS request for potential malware SafeGuard to domain 360.cn(domain 360.cn に対する潜在的なマルウェア SafeGuard に関する APP-DETECT DNS 要求)」です。

バージョン 5.1+ ユーザ イベントの例

次の図に、ユーザ イベント レコードの例を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	1
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	1
5	0	1	0	1	0	0	1	1	0	0	1	1	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	0	1	0	0	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
11	0	1	0	1	0	0	1	0	1	1	1	0	1	1	1	1	1	1	1	1	0	0	0	1	0	1	1	1	0	0	1	1
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	0	0	1	0	0	1	1	1	1
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
15	0	1	1	1	0	0	1	1	1	1	1	1	0	0	0	1	1	1	1	0	1	1	1	1	0	1	0	1	0	0	1	0
16	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	1	0	1	1	1	1	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1
20	0	1	0	1	0	0	1	0	1	1	1	0	1	1	1	1	1	1	1	1	0	0	0	1	0	1	1	1	0	0	1	1

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
24	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	1
	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	0
	0	0	1	1	0	1	0	0	0	0	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	1	0	0	0	1
	0	0	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1	0	1
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	1	0	1	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	1	0	1	1	1	1	0	0	0
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0																								

上記の例では、次の情報を確認できます。

番号	説明
1	この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ(つまり、メッセージ タイプ 4)であることを示しています。
2	この行は、後続のメッセージの長さが 153 バイトであることを示しています。
3	この先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーであることを示すフラグです。後続の 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプション フィールドです。行の残りの部分は、レコード タイプの値 95 を示し、ユーザ情報更新メッセージを表します。

番号	説明
4	この行は、後続のデータの長さが 137 バイトであることを示しています。
5	この行には、アーカイブのタイムスタンプが含まれます。23 ビットが設定されたため、含まれています。タイムスタンプが UNIX タイムスタンプである場合は、1970 年 1 月 1 日以降の秒数として保存されます。このタイムスタンプは 1,391,789,354 であり、2014 年 2 月 3 日（月）の 19 時 43 分 49 秒を表しています。
6	この行にはゼロが含まれており、将来使用するために予約されています。
7	この行は、検出エンジン ID 番号が 3 であることを示しています。
8	この行は、レガシー IP（IPv4）アドレス用です。事前に設定されていないため、すべてゼロになっており、IPv4 アドレスは IPv6 フィールドに保存されます。
9	この行には、イベントに関連付けられている MAC アドレスが含まれます。MAC アドレスがないため、ゼロが含まれています。
10	この行の前半は、MAC アドレスの残りの部分であり、ゼロです。次のバイトは、IPv6 アドレスが存在することを示しています。この行の最後のバイトは将来使用するために予約されており、ゼロが含まれています。
11	この行には、システムがイベントを生成した時刻の UNIX タイムスタンプ（1970 年 1 月 1 日以降の秒数）が含まれます。
12	この行には、システムがイベントを生成した時刻をマイクロ秒（100 万分の 1 秒）単位で表した値が含まれます。
13	この行には、イベント タイプが含まれます。ユーザ変更メッセージを示す値 1004 が含まれています。
18	この行には、イベント サブタイプが含まれます。ユーザ ログイン イベントを示す値 2 が含まれています。
15	この行には、シリアル ファイル番号が含まれます。このフィールドは、内部使用向けであり、無視してかまいません。
16	この行には、シリアル ファイル内のイベントの位置が含まれます。このフィールドは、内部使用向けであり、無視してかまいません。
17	この行には、IPv6 アドレスが含まれます。このフィールドは、IPv6 フラグが設定されている場合に存在し、使用されます。ただし、この場合は IPv4 アドレス 10.4.15.120 が含まれています。
18	この行は、ブロック タイプ 127 で示されるユーザ ログイン情報データ ブロックで始まります。
19	この行は、後続のブロックの長さが 81 バイトであることを示しています。
20	この行は、ユーザ ログインのタイムスタンプが 1,391,456,7 であることを示しています。これは、2014 年 10 月 3 日（月）の 19 時 43 分 47 秒（GMT）に生成されたことを意味します。
21	この行は、レガシー IP（IPv4）アドレス用です。事前に設定されていないため、すべてゼロになっており、IPv4 アドレスは IPv6 フィールドに保存されます。
22	この行は、文字列ブロックの長さとテキスト文字列を含む文字列ブロックが続くことを示します。この場合、テキスト文字列はユーザ名です。文字列ブロックの詳細については、文字列データ ブロック（3-62 ページ）を参照してください。
23	この行は、文字列ブロック内のデータの長さが 16 バイトであることを示しています。
24	この行は、ユーザ名が「301@10.4.11.175」であることを示しています。
25	この行は、ユーザの ID 番号を示します。

番号	説明
26	この行は、ログイン情報の取得元の接続で使用されているアプリケーション プロトコルのアプリケーション ID を示します。
27	この行は、文字列ブロックの長さとテキスト文字列を含む文字列ブロックが続くことを示します。この場合、テキスト文字列は電子メール アドレスです。文字列ブロックの詳細については、文字列データ ブロック（3-62 ページ）を参照してください。
36	この行は、文字列ブロック内のデータの長さが 0 バイトであることを示しています。なぜならば、このユーザに関連付けられている電子メールアドレスがないためです。
29	この行には、ユーザのログインが検出されたホストの IP アドレスが含まれます。
30	先頭バイトには、ログイン タイプが含まれます。この行の残りの部分は、文字列ブロックの長さとテキスト文字列を含む文字列ブロックが続くことを示します。この場合、テキスト文字列は、ログインを報告した Active Directory サーバの名前です。文字列ブロックの詳細については、文字列データ ブロック（3-62 ページ）を参照してください。
31	この行の先頭バイトで、文字列データ ブロックの開始が完了します。この行の残りの部分は、文字列ブロック内のデータの長さが 0 バイトであることを示しています。なぜならば、このログインに関連付けられている Active Directory サーバがないためです。

ディスカバリ データ構造の例

このセクションでは、ディスカバリ イベントに関して eStreamer で送信されることがあるデータ構造の例を紹介します。ここでは、次の例を示します。

- 新しいネットワーキング プロトコル メッセージの例（A-18 ページ）
- 新しい TCP サーバ メッセージの例（A-20 ページ）

新しいネットワーキング プロトコル メッセージの例

次の図に、3.0+ の新しいネットワーク プロトコル メッセージの例を示します。

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
ヘッダー バージョン 1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	イベント メッセージ (4) を含む標準メッセージ ヘッダーの開始
メッセージ長（49 バイト）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
新しいネットワーク プロトコル メッセージ（13）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	
メッセージ長（41 バイト）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	0	0	
検出エンジン ID（2）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	
IP（192.168.1.10）	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0	
MAC アドレス（なし）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	予約バイト（0）
UNIX 秒（1047242787）	0	0	1	1	1	1	1	0	0	1	1	0	1	0	1	1	1	0	1	0	1	0	0	0	0	0	1	0	0	0	1	1	
UNIX ミリ秒（973208）	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0	0	
予約バイト（0）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	0	0	イベント タイプ 1000 — 新規
イベント サブタイプ 4 - 新しい転送プロトコル	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	
ファイル番号	0	1	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	0	0	1	1	1	0	1	0	0	0	1	
ファイルの位置	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	標準メッセージ ヘッダーの終了
プロトコル（6—TCP）	0	0	0	0	0	1	1	0																									

新しい TCP サーバ メッセージの例

次の図に、3.0+ の新しい TCP サーバ メッセージの例を示します。

バイト	0	1	2	3	
ビット	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31	
ヘッダー バージョン 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0	0 0 0 0 0 1 0 0	イベント メッセージ (4) を含む標準メッセージ ヘッダーの開始
メッセージ長（256 バイト）	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0	
新しい TCP サーバ メッセージ（11）	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 1 0 1 1	
メッセージ長（248 バイト）	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	1 1 1 1 1 0 0 0	
検出エンジン ID（2）	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 0	
IP（192.168.1.10）	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 1 0 1 0	
MAC アドレス（なし）	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	
	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	予約バイト（0）
UNIX 秒（1047242787）	0 0 1 1 1 1 1 0	0 1 1 0 1 0 1 1	1 0 1 0 1 0 0 0	0 0 1 0 0 0 1 1	
UNIX ミリ秒（973208）	0 0 0 0 0 0 0 0	0 0 0 0 1 1 1 0	1 1 0 1 1 0 0 1	1 0 0 1 1 0 0 0	
予約バイト(0)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 1	1 1 1 0 1 0 0 0	イベント タイプ 1000 — 新規
イベント サブタイプ 2 - 新しいホスト	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 0	
ファイル番号	0 1 0 0 0 0 0 0	0 1 0 0 0 1 1 1	1 0 0 0 1 0 0 1	1 1 0 1 0 0 0 1	
ファイルの位置	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	1 1 0 0 0 0 0 0	標準メッセージ ヘッダーの終了

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
サーバブロック ヘッダー(12)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	サーバ データ ブロックの開始
サーバ長(208 バイト)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	
サーバ ポート (80)	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	ヒット
ヒット(1)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブロック ヘッダー
文字列ブロック ヘッダー(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブロック長
文字列ブロック長(13 バイト)	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	1	1	0	1	0	0	0	0	1	1	1	0	1	0	
サーバ名 (https)	0	1	1	1	0	1	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブロック ヘッダー
文字列ブロック ヘッダー(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブロック長
文字列ブロック長(15 バイト)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	
	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1	1	0	1	1	0	1	0	0	0	
サーバ ベンダー (Apache + Null バイト)	0	1	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブロック ヘッダー
文字列ブロック ヘッダー(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブロック長
文字列長(8 - 製品なし)	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブロック ヘッダー
文字列ブロック ヘッダー(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブロック長
文字列ブロック長(22 バイト)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	1	1	0	0	0	1	0	0	1	0	1	1	1	0	

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
バージョン - 1.3.26（UNIX）	0	0	1	1	0	0	1	1	0	0	1	0	1	1	1	0	0	0	1	1	0	0	1	0	0	0	1	1	0	1	1	0	
	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	1	0	1	0	1	0	1	1	0	1	1	1	0	
	0	1	1	0	1	0	0	1	0	1	1	1	1	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	
リストブロック ヘッダー（11）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	サブサーバ リストの開始
リスト ブロック サイズ（94 バイト）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	0	
サブサーバ ヘッダー（1）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		サブサーバ ブロックの開始
サブサーバ長（46 バイト）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0		
文字列ブロック ヘッダー（0）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
文字列長（16 バイト）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0		
サブサーバ名 - mod_ssl	0	1	1	0	1	1	0	1	0	1	1	0	1	1	1	1	0	1	1	0	0	1	0	0	0	1	0	1	1	1	1	1		
	0	1	1	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0		
文字列ブロック ヘッダー（0）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
文字列ブロック長（8 バイト）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		（サブタイプ ベンダーなし）
文字列ブロック ヘッダー（0）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
文字列ブロック長（14 バイト）	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0		
サブサーバ バージョン - 2.8.9 + Null 文字	0	0	1	1	0	0	1	0	0	0	1	0	1	1	1	0	0	0	1	1	1	0	0	0	0	0	1	0	1	1	1	0		サブサーバ ブロックの終了
	0	0	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		サブサーバ ブロックの開始

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
サブサーバ ヘッダー(1)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	サブサーバ長
サブサーバ長(48 バイト)	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブロック ヘッダー
文字列ブロック ヘッダー(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブロック サイズ
文字列ブロック サイズ(16 バイト)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	1	1	1	1	0	1	1	1	0	0	0	0	
サブサーバ名 - OpenSSL	0	1	1	0	0	1	0	1	0	1	1	0	1	1	1	0	0	1	0	1	0	0	1	1	0	1	0	1	0	0	1	1	
	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブロック ヘッダー
文字列ブロック ヘッダー(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列データ長
文字列長(8 - ベンダーなし)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブロック ヘッダー
文字列ブロック ヘッダー(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブロック長
文字列ブロック長(16 バイト)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	1	0	1	1	1	1	0	
サブサーバ バージョン - 0.9.6.d + Null 文字	0	0	1	1	1	0	0	1	0	0	1	0	1	1	1	0	0	0	1	1	0	1	1	0	0	0	1	0	1	1	1	0	サブサーバ ブロックの終了
	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	信頼性(%)
信頼性(%) (100)	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	1	前回の使用
前回の使用 (1047242787)	1	0	1	0	1	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	BLOB データ ブロック
BLOB データ ブロック(10)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	BLOB データ長
BLOB データ長 (22 バイト)	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	1	0	0	1	0	0	0	0	1	0	1	0	1	0	0	

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
サーバ バナー（HTTP/1.1 414 要求）- 短縮されたサーバ バナー（例えば、通常は 256 バイト）	0	1	0	1	0	1	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	1	1	1	0	0	1	1	0	0	0	1	
	0	0	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	1	0	1	0	0	
	0	0	1	1	0	0	0	1	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	0	1	0	
	0	1	1	0	0	1	0	1	0	1	1	1	0	0	0	1	0	1	1	1	0	1	0	1	0	1	1	0	0	1	0	1	サーバ データ ブロックの終了

レガシー データ構造の概要

この付録には、旧バージョンの Firepower システム 製品の eStreamer によってサポートされるデータ構造に関する情報を記載しています。

クライアントが、旧バージョン形式でデータを要求するようにビットが設定されているイベント ストリーム要求を使用する場合、この付録の情報を使用して、受け取るデータ メッセージのデータ構造を識別できます。

バージョン 5.0 より前は、検出エンジンに個別に ID が割り当てられていたことに注意してください。バージョン 5.0 では、デバイスに ID が割り当てられます。この点は、バージョンに基づいてデータ構造に反映されます。

(注) この付録では、Firepower システム のバージョン 4.9 以降からのデータ構造のみを説明します。以前のデータ構造バージョンによる構造向けの資料が必要な場合は、Cisco カスタマー サポートにお問い合わせください。

詳細については、次の各項を参照してください。

レガシー侵入データ構造

侵入イベント(IPv4)レコード 5.0.x ～ 5.1

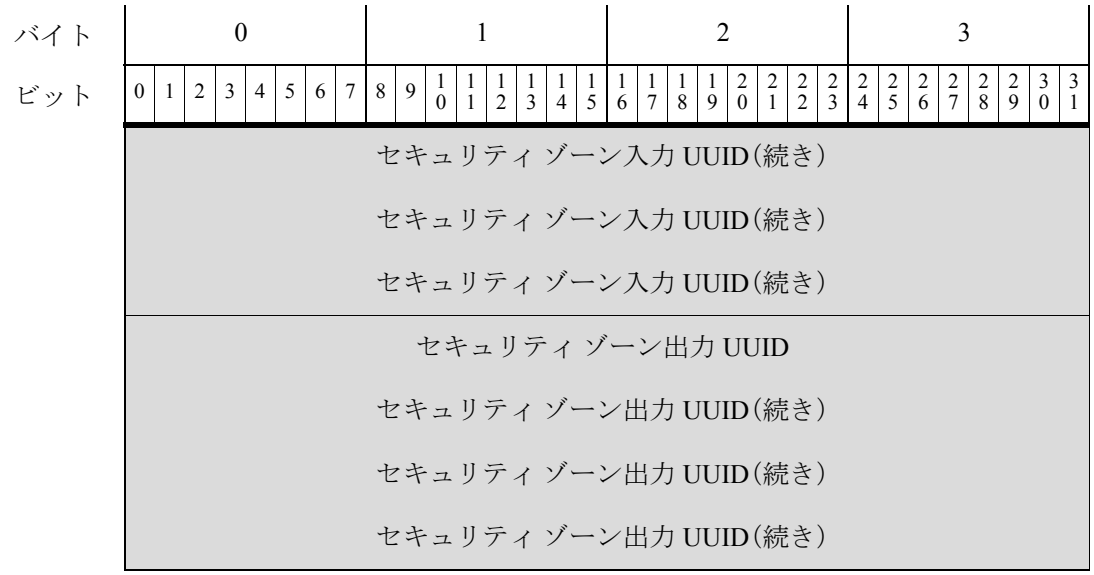
侵入イベント(IPv4)レコードのフィールドは、次の図では網掛けされています。レコードの種類は 207 です。

侵入イベント レコードは、要求メッセージに侵入イベント フラグまたは拡張要求フラグを設定して要求します。要求フラグ(2-12 ページ)および拡張要求の送信(2-4 ページ)を参照してください。

バージョン 5.0.x ～ 5.1 の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(207)															
レコード長																																
eStreamer サーバ タイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																																
将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																																
デバイス ID																																
イベント ID.																																
イベント秒																																
イベント マイクロ秒																																
ルール ID(シグネチャ ID)																																
ジェネレータ ID																																
ルール リビジョン																																
分類 ID																																
プライオリティ ID																																
送信元 IPv4 アドレス																																
宛先 IPv4 アドレス																																
送信元ポート																	接続先ポー ト															
IP プロトコル ID									影響フラグ								影響								ブロック							

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MPLSラベル																																
VLAN ID																	パッド															
ポリシー UUID ポリシー UUID（続き） ポリシー UUID（続き） ポリシー UUID（続き）																																
ユーザID																																
Web アプリケーション ID																																
クライアント アプリケーション ID																																
アプリケーション プロトコル ID																																
アクセス コントロール ルール ID																																
アクセス コントロール ポリシー UUID アクセス コントロール ポリシー UUID（続き） アクセス コントロール ポリシー UUID（続き） アクセス コントロール ポリシー UUID（続き）																																
インターフェイス入力 UUID インターフェイス入力 UUID（続き） インターフェイス入力 UUID（続き） インターフェイス入力 UUID（続き）																																
インターフェイス出力 UUID インターフェイス出力 UUID（続き） インターフェイス出力 UUID（続き） インターフェイス出力 UUID（続き）																																
セキュリティ ゾーン入力 UUID																																



次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 B-1　　侵入イベント（IPv4）レコードのフィールド

フィールド	データ タイプ	説明
デバイス ID	unit32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ（3-38 ページ）を参照してください。
イベント ID	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
イベント マイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒（100 万分の 1 秒）単位の増分。
ルール ID（シグネチャ ID）	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IPv4 アドレス	uint8[4]	アドレス オクテットの、イベントで使用される送信元 IPv4 アドレス。
宛先 IPv4 アドレス	uint8[4]	アドレス オクテットの、イベントで使用される宛先 IPv4 アドレス。

表 B-1　侵入イベント(IPv4)レコードのフィールド(続き)

フィールド	データ タイプ	説明
送信元ポート	uint16	イベント プロトコル タイプが TCP または UDP の場合は送信元ポート番号。
接続先ポート	uint16	イベント プロトコル タイプが TCP または UDP の場合は宛先ポート番号。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 • 0:IP • 1:ICMP • 6:TCP • 17:UDP

表 B-1　侵入イベント(IPv4)レコードのフィールド(続き)

フィールド	データ タイプ	説明
影響フラグ	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。 次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • (0、不明):00X00000 • 赤(1、脆弱):xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx • オレンジ(2、潜在的に脆弱):00X00111 • 黄(3、現在は脆弱でない):00X00011 • 青(4、不明なターゲット):00X00001
影響	uint8	イベントの影響フラグ値。値は次のとおりです。 • 1:レッド(脆弱) • 2:オレンジ(脆弱の可能性あり) • 3:イエロー(現在は脆弱でない) • 4:ブルー(不明なターゲット) • 5:グレー(不明なインパクト)

表 B-1　侵入イベント(IPv4)レコードのフィールド(続き)

フィールド	データ タイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 • 0:ブロックされていない • 1:ブロックされた • 2:ブロックされた可能性がある(設定では許可されていない)
MPLSラベル	uint32	MPLS ラベル。
VLAN ID	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルの内部 ID 番号(該当する場合)。
アクセス コントロール ルール ID	uint32	アクセス コントロール ルールの固有識別子として機能するルール ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティ ゾーン UUID	uint8[16]	入力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティ ゾーン UUID	uint8[16]	出力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。

侵入イベント(IPv6)レコード 5.0.x ～ 5.1

侵入イベント(IPv6)レコードのフィールドは、次の図では網掛けされています。レコードの種類は 208 です。

侵入イベント レコードは、要求メッセージに侵入イベント フラグまたは拡張要求フラグを設定して要求します。要求フラグ(2-12 ページ)および拡張要求の送信(2-4 ページ)を参照してください。

バージョン 5.0.x ～ 5.1 の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(208)															
レコード長																																
eStreamer サーバ タイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																																
将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																																
デバイス ID																																
イベント ID																																
イベント秒																																
イベント マイクロ秒																																
ルール ID(シグネチャ ID)																																
ジェネレータ ID																																
ルール リビジョン																																
分類 ID																																
プライオリティ ID																																
送信元 IPv6 アドレス 送信元 IPv6 アドレス(続き) 送信元 IPv6 アドレス(続き) 送信元 IPv6 アドレス(続き)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
宛先 IPv6 アドレス																																
宛先 IPv6 アドレス（続き）																																
宛先 IPv6 アドレス（続き）																																
宛先 IPv6 アドレス（続き）																																
送信元ポート/ICMP タイプ																	宛先ポート/ICMP コード															
IP プロトコル ID									影響フラグ								影響								ブロック							
MPLSラベル																																
VLAN ID																	パッド															
ポリシー UUID																																
ポリシー UUID（続き）																																
ポリシー UUID（続き）																																
ポリシー UUID（続き）																																
ユーザ ID																																
Web アプリケーション ID																																
クライアント アプリケーション ID																																
アプリケーション プロトコル ID																																
アクセス コントロール ルール ID																																
アクセス コントロール ポリシー UUID																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
インターフェイス入力 UUID																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
インターフェイス入力 UUID（続き）																																
インターフェイス出力 UUID																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
セキュリティ ゾーン入力 UUID																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン出力 UUID																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																

次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 B-2　侵入イベント（IPv6）レコードのフィールド

フィールド	データ タイプ	説明
デバイス ID	unit32	検出デバイスの ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ (3-38 ページ) を参照してください。
イベント ID	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
イベント マイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒（100 万分の 1 秒）単位の増分。
ルール ID（シグネチャ ID）	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。

表 B-2　侵入イベント(IPv6)レコードのフィールド(続き)

フィールド	データ タイプ	説明
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IPv6 アドレス	uint8[16]	アドレス オクテットの、イベントで使用される送信元 IPv6 アドレス。
宛先 IPv6 アドレス	uint8[16]	アドレス オクテットの、イベントで使用される宛先 IPv6 アドレス。
送信元ポート/ICMP タイプ	uint16	イベント プロトコル タイプが TCP または UDP の場合は送信元ポート番号。プロトコル タイプが ICMP である場合、これは ICMP タイプを示します。
宛先ポート/ICMP コード	uint16	イベント プロトコル タイプが TCP または UDP の場合は宛先ポート番号。プロトコル タイプが ICMP である場合、これは ICMP コードを示します。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 • 0:IP • 1:ICMP • 6:TCP • 17:UDP

表 B-2　侵入イベント(IPv6)レコードのフィールド(続き)

フィールド	データ タイプ	説明
影響フラグ	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。 次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • (0、不明):00X00000 • 赤(1、脆弱):xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx • オレンジ(2、潜在的に脆弱):00X00111 • 黄(3、現在は脆弱でない):00X00011 • 青(4、不明なターゲット):00X00001
影響	uint8	イベントの影響フラグ値。値は次のとおりです。 • 1:レッド(脆弱) • 2:オレンジ(脆弱の可能性あり) • 3:イエロー(現在は脆弱でない) • 4:ブルー(不明なターゲット) • 5:グレー(不明なインパクト)

表 B-2　侵入イベント(IPv6)レコードのフィールド(続き)

フィールド	データ タイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 • 0:ブロックされていない • 1:ブロックされた • 2:ブロックされた可能性がある(設定では許可されていない)
MPLS ラベル	uint32	MPLS ラベル。(4.9+ のイベントにのみ適用。)
VLAN ID	uint16	パケットの発信元の VLAN の ID を示します。(4.9+ のイベントにのみ適用。)
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルの内部 ID 番号(該当する場合)。
アクセス コントロール ルール ID	uint32	アクセス コントロール ルールの固有識別子として機能するルール ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティ ゾーン UUID	uint8[16]	入力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティ ゾーン UUID	uint8[16]	出力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。

侵入イベント レコード 5.2.x

侵入イベント レコードのフィールドは、次の図で網掛けされています。レコード タイプは 400 であり、ブロック タイプはシリーズ 2 セットのデータ ブロックの 34 です。

eStreamer からの 5.2.x 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベント タイプ コード 12 およびバージョン 5 を要求します（拡張要求の送信の詳細については、拡張要求の送信（2-4 ページ）を参照してください）。

バージョン 5.2.x の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。接続の秒、接続インスタンス、および接続数カウンタは、侵入イベントに関連付けられた接続イベントの、1 つの固有識別子を形成します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（400）															
レコード長																																
eStreamer サーバ タイムスタンプ（イベント用、ビット 23 が設定されている場合のみ）																																
将来の使用に備えて予約済み（イベントでビット 23 が設定されている場合のみ）																																
ブロック タイプ（34）																																
ブロック長																																
デバイス ID																																
イベント ID																																
イベント秒																																
イベント マイクロ秒																																
ルール ID（シグネチャ ID）																																
ジェネレータ ID																																
ルール リビジョン																																
分類 ID																																
プライオリティ ID																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
送信元 IP アドレス																																
送信元 IP アドレス（続き）																																
送信元 IP アドレス（続き）																																
送信元 IP アドレス（続き）																																
宛先IPアドレス																																
宛先 IP アドレス（続き）																																
宛先 IP アドレス（続き）																																
宛先 IP アドレス（続き）																																
送信元ポートまたは ICMP タイプ																	送信先ポートまたは ICMP コード														
IP プロトコル ID									影響フラグ								影響								ブロック							
MPLSラベル																																
VLAN ID																	パッド															
ポリシー UUID																																
ポリシー UUID（続き）																																
ポリシー UUID（続き）																																
ポリシー UUID（続き）																																
ユーザ ID																																
Web アプリケーション ID																																
クライアント アプリケーション ID																																
アプリケーション プロトコル ID																																
アクセス コントロール ルール ID																																
アクセス コントロール ポリシー UUID																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
インターフェイス入力 UUID																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																
インターフェイス出力 UUID																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
セキュリティ ゾーン入力 UUID																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン出力 UUID																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
接続タイムスタンプ																																
接続インスタンス ID																	接続数カウンタ															
送信元の国																	宛先の国															

次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 B-3　侵入イベント レコード 5.2.x のフィールド

フィールド	データ タイプ	説明
ブロック タイプ	unint32	侵入イベント データ ブロックを開始します。この値は常に 34 です。
ブロック長	unint32	侵入イベント データ ブロックのバイトの合計数（侵入イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む）。
デバイス ID	unit32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ (3-38 ページ) を参照してください。
イベント ID	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
イベント マイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒（100 万分の 1 秒）単位の増分。
ルール ID（シグネチャ ID）	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポートまたは ICMP タイプ	uint16	イベント プロトコル タイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
送信先ポートまたは ICMP コード	uint16	イベント プロトコル タイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 • 0：IP • 1：ICMP • 6：TCP • 17：UDP

表 B-3　侵入イベント レコード5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
影響フラグ	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) 次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • (0、不明):00X00000 • 赤(1、脆弱):xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx(バージョン 5.0+ のみ) • オレンジ(2、潜在的に脆弱):00X0011X • 黄(3、現在は脆弱でない):00X0001X • 青(4、不明なターゲット):00X00001
影響	uint8	イベントの影響フラグ値。値は次のとおりです。 • 1:レッド(脆弱) • 2:オレンジ(脆弱の可能性あり) • 3:イエロー(現在は脆弱でない) • 4:ブルー(不明なターゲット) • 5:グレー(不明なインパクト)

表 B-3　侵入イベント レコード 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 • 0:ブロックされていない • 1:ブロックされた • 2:ブロックされた可能性がある(設定では許可されていない)
MPLSラベル	uint32	MPLS ラベル。
VLAN ID	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルの内部 ID 番号(該当する場合)。
アクセス コントロール ルール ID	uint32	アクセス コントロール ルールの固有識別子として機能するルール ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティ ゾーン UUID	uint8[16]	入力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティ ゾーン UUID	uint8[16]	出力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。

表 B-3　侵入イベント レコード 5.2.x のフィールド（続き）

フィールド	データ タイプ	説明
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。

侵入イベント レコード 5.3

侵入イベント レコードのフィールドは、次の図で網掛けされています。レコード タイプは 400 であり、ブロック タイプはデータ ブロックのシリーズ 2 セットの 41 です。

eStreamer からの 5.3 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベント タイプ コード 12 およびバージョン 6 を要求します（拡張要求の送信の詳細については、拡張要求の送信（2-4 ページ）を参照してください）。

バージョン 5.3 の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。接続の秒、接続インスタンス、および接続数カウンタは、侵入イベントに関連付けられた接続イベントの、1 つの固有識別子を形成します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（400）															
レコード長																																
eStreamer サーバ タイムスタンプ（イベント用、ビット 23 が設定されている場合のみ）																																
将来の使用に備えて予約済み（イベントでビット 23 が設定されている場合のみ）																																
ブロック タイプ（41）																																
ブロック長																																
デバイス ID																																
イベント ID																																
イベント秒																																
イベント マイクロ秒																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ルール ID（シグネチャ ID）																																
ジェネレータ ID																																
ルール リビジョン																																
分類 ID																																
プライオリティ ID																																
送信元 IP アドレス 送信元 IP アドレス（続き） 送信元 IP アドレス（続き） 送信元 IP アドレス（続き）																																
宛先IPアドレス 宛先 IP アドレス（続き） 宛先 IP アドレス（続き） 宛先 IP アドレス（続き）																																
送信元ポートまたは ICMP タイプ																	送信先ポートまたは ICMP コード														
IP プロトコル ID									影響フラグ								影響								ブロック							
MPLSラベル																																
VLAN ID																	パッド															
ポリシー UUID ポリシー UUID（続き） ポリシー UUID（続き） ポリシー UUID（続き）																																
ユーザ ID																																
Web アプリケーション ID																																
クライアント アプリケーション ID																																
アプリケーション プロトコル ID																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
アクセス コントロール ルール ID																																
アクセス コントロール ポリシー UUID																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
インターフェイス入力 UUID																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																
インターフェイス出力 UUID																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
セキュリティ ゾーン入力 UUID																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン出力 UUID																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
接続タイムスタンプ																																
接続インスタンス ID																	接続数カウンタ															
送信元の国																	宛先の国															
IOC 番号																																

次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 B-4　侵入イベント レコード 5.3 のフィールド

フィールド	データ タイプ	説明
ブロック タイプ	unint32	侵入イベント データ ブロックを開始します。この値は常に 34 です。
ブロック長	unint32	侵入イベント データ ブロックのバイトの合計数（侵入イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む）。
デバイス ID	unit32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ (3-38 ページ) を参照してください。
イベント ID	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
イベント マイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒（100 万分の 1 秒）単位の増分。
ルール ID（シグネチャ ID）	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポートまたは ICMP タイプ	uint16	イベント プロトコル タイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
送信先ポートまたは ICMP コード	uint16	イベント プロトコル タイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 • 0：IP • 1：ICMP • 6：TCP • 17：UDP

表 B-4　侵入イベント レコード 5.3 のフィールド(続き)

フィールド	データ タイプ	説明
影響フラグ	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) 次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • (0、不明):00X00000 • 赤(1、脆弱):xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx(バージョン 5.0+ のみ) • オレンジ(2、潜在的に脆弱):00X0011X • 黄(3、現在は脆弱でない):00X0001X • 青(4、不明なターゲット):00X00001
影響	uint8	イベントの影響フラグ値。値は次のとおりです。 • 1:レッド(脆弱) • 2:オレンジ(脆弱の可能性あり) • 3:イエロー(現在は脆弱でない) • 4:ブルー(不明なターゲット) • 5:グレー(不明なインパクト)

表 B-4　侵入イベント レコード 5.3 のフィールド（続き）

フィールド	データ タイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 • 0:ブロックされていない • 1:ブロックされた • 2:ブロックされた可能性がある（設定では許可されていない）
MPLSラベル	uint32	MPLS ラベル。
VLAN ID	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID	uint32	ユーザの内部 ID 番号（該当する場合）。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号（該当する場合）。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号（該当する場合）。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルの内部 ID 番号（該当する場合）。
アクセス コントロール ルール ID	uint32	アクセス コントロール ルールの固有識別子として機能するルール ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティ ゾーン UUID	uint8[16]	入力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティ ゾーン UUID	uint8[16]	出力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ（1970 年 1 月 1 日からの経過秒数）。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。

表 B-4　侵入イベント レコード 5.3 のフィールド（続き）

フィールド	データ タイプ	説明
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。

侵入イベント レコード 5.1.1.x

侵入イベント レコードのフィールドは、次の図で網掛けされています。レコード タイプは 400 で、ブロック タイプは 25 です。

eStreamer からの 5.1.1 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベント タイプ コード 12 およびバージョン 4 を要求します（拡張要求の送信の詳細については、拡張要求の送信（2-4 ページ）を参照してください）。

バージョン 5.1.1.x の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。接続の秒、接続インスタンス、および接続数カウンタは、侵入イベントに関連付けられた接続イベントの、1 つの固有識別子を形成します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（400）															
レコード長																																
eStreamer サーバ タイムスタンプ（イベント用、ビット 23 が設定されている場合のみ）																																
将来の使用に備えて予約済み（イベントでビット 23 が設定されている場合のみ）																																
ブロック タイプ（25）																																
ブロック長																																
デバイス ID																																
イベント ID																																
イベント秒																																
イベント マイクロ秒																																
ルール ID（シグネチャ ID）																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ジェネレータ ID																																
ルール リビジョン																																
分類 ID																																
プライオリティ ID																																
送信元 IP アドレス 送信元 IP アドレス（続き） 送信元 IP アドレス（続き） 送信元 IP アドレス（続き）																																
宛先IPアドレス 宛先 IP アドレス（続き） 宛先 IP アドレス（続き） 宛先 IP アドレス（続き）																																
送信元ポート/ICMP タイプ																	宛先ポート/ICMP コード														
IP プロトコル ID									影響フラグ								影響								ブロック							
MPLSラベル																																
VLAN ID																	パッド															
ポリシー UUID ポリシー UUID（続き） ポリシー UUID（続き） ポリシー UUID（続き）																																
ユーザ ID																																
Web アプリケーション ID																																
クライアント アプリケーション ID																																
アプリケーション プロトコル ID																																
アクセス コントロール ルール ID																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
アクセス コントロール ポリシー UUID																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
インターフェイス入力 UUID																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																
インターフェイス出力 UUID																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
セキュリティ ゾーン入力 UUID																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン出力 UUID																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
接続タイムスタンプ																																
接続インスタンス ID																	接続数カウンタ															

次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 B-5　侵入イベント レコード 5.1.1 のフィールド

フィールド	データ タイプ	説明
ブロック タイプ	unint32	侵入イベント データ ブロックを開始します。この値は常に 25 です。
ブロック長	unint32	侵入イベント データ ブロックのバイトの合計数（侵入イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む）。
デバイス ID	unit32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ (3-38 ページ) を参照してください。
イベント ID	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
イベント マイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒（100 万分の 1 秒）単位の増分。
ルール ID（シグネチャ ID）	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポート /ICMP タイプ	uint16	イベント プロトコル タイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
宛先ポート /ICMP コード	uint16	イベント プロトコル タイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 • 0：IP • 1：ICMP • 6：TCP • 17：UDP

表 B-5　侵入イベント レコード 5.1.1 のフィールド(続き)

フィールド	データ タイプ	説明
影響フラグ	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。 次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • (0、不明):00X00000 • 赤(1、脆弱):xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx • オレンジ(2、潜在的に脆弱):00X00111 • 黄(3、現在は脆弱でない):00X00011 • 青(4、不明なターゲット):00X00001
影響	uint8	イベントの影響フラグ値。値は次のとおりです。 • 1:レッド(脆弱) • 2:オレンジ(脆弱の可能性あり) • 3:イエロー(現在は脆弱でない) • 4:ブルー(不明なターゲット) • 5:グレー(不明なインパクト)

表 B-5　侵入イベント レコード 5.1.1 のフィールド(続き)

フィールド	データ タイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 • 0:ブロックされていない • 1:ブロックされた • 2:ブロックされた可能性がある(設定では許可されていない)
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルの内部 ID 番号(該当する場合)。
アクセス コントロール ルール ID	uint32	アクセス コントロール ルールの固有識別子として機能するルール ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティ ゾーン UUID	uint8[16]	入力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティ ゾーン UUID	uint8[16]	出力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。

侵入イベント レコード 5.3.1

侵入イベント レコードのフィールドは、次の図で網掛けされています。レコード タイプは 400 であり、ブロック タイプはシリーズ 2 セットのデータ ブロックの 42 です。

eStreamer からの 5.3.1 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベント タイプ コード 12 およびバージョン 7 を要求します（拡張要求の送信の詳細については、拡張要求の送信（2-4 ページ）を参照してください）。

バージョン 5.3.1 の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。接続の秒、接続インスタンス、および接続数カウンタは、侵入イベントに関連付けられた接続イベントの、1 つの固有識別子を形成します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（400）															
レコード長																																
eStreamer サーバ タイムスタンプ（イベント用、ビット 23 が設定されている場合のみ）																																
将来の使用に備えて予約済み（イベントでビット 23 が設定されている場合のみ）																																
ブロック タイプ（42）																																
ブロック長																																
デバイスID																																
イベント ID																																
イベント秒																																
イベント マイクロ秒																																
ルール ID（シグネチャ ID）																																
ジェネレータ ID																																
ルール リビジョン																																
分類 ID																																
プライオリティ ID																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
送信元 IP アドレス																																
送信元 IP アドレス（続き）																																
送信元 IP アドレス（続き）																																
送信元 IP アドレス（続き）																																
宛先 IP アドレス																																
宛先 IP アドレス（続き）																																
宛先 IP アドレス（続き）																																
宛先 IP アドレス（続き）																																
送信元ポートまたは ICMP タイプ																	送信先ポートまたは ICMP コード														
IP プロトコル ID									影響フラグ								影響								ブロック							
MPLS ラベル																																
VLAN ID																	パッド															
ポリシー UUID																																
ポリシー UUID（続き）																																
ポリシー UUID（続き）																																
ポリシー UUID（続き）																																
ユーザ ID																																
Web アプリケーション ID																																
クライアント アプリケーション ID																																
アプリケーション プロトコル ID																																
アクセス コントロール ルール ID																																
アクセス コントロール ポリシー UUID																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
インターフェイス入力 UUID																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																
インターフェイス出力 UUID																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
セキュリティ ゾーン入力 UUID																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン出力 UUID																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
接続タイムスタンプ																																
接続インスタンス ID																	接続数カウンタ															
送信元の国																	宛先の国															
IOC 番号																	セキュリティ コンテキスト															
セキュリティ コンテキスト（続き）																																
セキュリティ コンテキスト（続き）																																
セキュリティ コンテキスト（続き）																																
セキュリティ コンテキスト（続き）																																

次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 B-6　　侵入イベント レコード 5.3.1 のフィールド

フィールド	データ タイプ	説明
ブロック タイプ	unint32	侵入イベント データ ブロックを開始します。この値は常に 42 です。
ブロック長	unint32	侵入イベント データ ブロックのバイトの合計数（侵入イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む）。
デバイスID	unit32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ (3-38 ページ) を参照してください。
イベント ID	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
イベント マイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒（100 万分の 1 秒）単位の増分。
ルール ID（シグネチャ ID）	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポートまたは ICMP タイプ	uint16	イベント プロトコル タイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
送信先ポートまたは ICMP コード	uint16	イベント プロトコル タイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 • 0：IP • 1：ICMP • 6：TCP • 17：UDP

表 B-6　侵入イベント レコード 5.3.1 のフィールド(続き)

フィールド	データ タイプ	説明
影響フラグ	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) 次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • (0、不明):`00X00000` • 赤(1、脆弱):`xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx`(バージョン 5.0+ のみ) • オレンジ(2、潜在的に脆弱):`00X0011X` • 黄(3、現在は脆弱でない):`00X0001X` • 青(4、不明なターゲット):`00X00001`
影響	uint8	イベントの影響フラグ値。値は次のとおりです。 • `1`:レッド(脆弱) • `2`:オレンジ(脆弱の可能性あり) • `3`:イエロー(現在は脆弱でない) • `4`:ブルー(不明なターゲット) • `5`:グレー(不明なインパクト)

表 B-6　侵入イベント レコード 5.3.1 のフィールド(続き)

フィールド	データ タイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 • 0:ブロックされていない • 1:ブロックされた • 2:ブロックされた可能性がある(設定では許可されていない)
MPLSラベル	uint32	MPLS ラベル。
VLAN ID	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルの内部 ID 番号(該当する場合)。
アクセス コントロール ルール ID	uint32	アクセス コントロール ルールの固有識別子として機能するルール ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティ ゾーン UUID	uint8[16]	入力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティ ゾーン UUID	uint8[16]	出力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
送信元の国	uint16	送信元ホストの国のコード。

表 B-6　侵入イベント レコード 5.3.1 のフィールド（続き）

フィールド	データ タイプ	説明
宛先の国	uint 16	宛先ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト（仮想ファイアウォール）の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

侵入イベント レコード 5.4.x

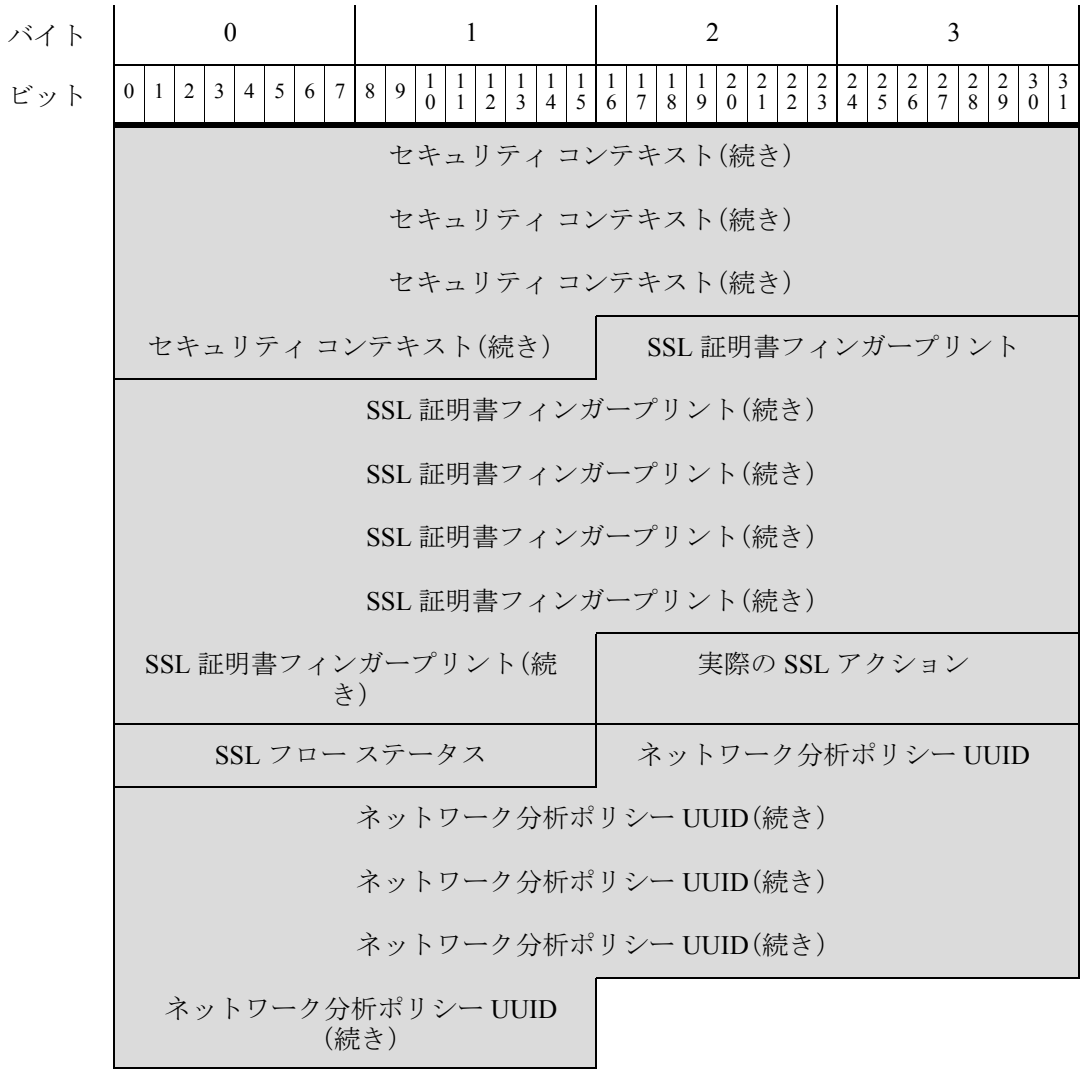
侵入イベント レコードのフィールドは、次の図で網掛けされています。レコード タイプは 400 であり、ブロック タイプはシリーズ 2 セットのデータ ブロックの 45 です。これはブロック タイプ 42 に取って代わり、ブロック タイプ 60 により取って代わられます。SSL サポート用およびネットワーク分析ポリシー用のフィールドが追加されました。

eStreamer からの 5.4.x 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベント タイプ コード 12 およびバージョン 8 を要求します（拡張要求の送信の詳細については、拡張要求の送信（2-4 ページ）を参照してください）。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

ルール ID（シグネチャ ID）			
ジェネレータ ID			
ルール リビジョン			
分類 ID			
プライオリティ ID			
送信元 IP アドレス 送信元 IP アドレス（続き） 送信元 IP アドレス（続き） 送信元 IP アドレス（続き）			
宛先 IP アドレス 宛先 IP アドレス（続き） 宛先 IP アドレス（続き） 宛先 IP アドレス（続き）			
送信元ポートまたは ICMP タイプ		送信先ポートまたは ICMP コード	
IP プロトコル ID	影響フラグ	影響	ブロック
MPLS ラベル			
VLAN ID		パッド	
ポリシー UUID ポリシー UUID（続き） ポリシー UUID（続き） ポリシー UUID（続き）			
ユーザ ID			
Web アプリケーション ID			
クライアント アプリケーション ID			
アプリケーション プロトコル ID			

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
アクセス コントロール ルール ID																																
アクセス コントロール ポリシー UUID																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
インターフェイス入力 UUID																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																
インターフェイス出力 UUID																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
セキュリティ ゾーン入力 UUID																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン出力 UUID																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
接続タイムスタンプ																																
接続インスタンス ID																	接続数カウンタ															
送信元の国																	宛先の国															
IOC 番号																	セキュリティ コンテキスト															



次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 B-7　侵入イベント レコード 5.4.x のフィールド

フィールド	データ タイプ	説明
ブロック タイプ	unint32	侵入イベント データ ブロックを開始します。この値は常に 45 です。
ブロック長	unint32	侵入イベント データ ブロックのバイトの合計数(侵入イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイスID	unit32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ (3-38 ページ) を参照してください。
イベント ID	uint32	イベント ID 番号。

表 B-7　侵入イベント レコード5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
イベント秒	uint32	イベント検出の UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
イベント マイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒(100 万分の 1 秒)単位の増分。
ルール ID(シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポートまたは ICMP タイプ	uint16	イベント プロトコル タイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
送信先ポートまたは ICMP コード	uint16	イベント プロトコル タイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 • 0:IP • 1:ICMP • 6:TCP • 17:UDP

表 B-7　侵入イベント レコード5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
影響フラグ	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) 次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • グレー(0、不明):`00X00000` • 赤(1、脆弱):`XXXX1XXX`, `XXX1XXXX`, `X1XXXXXX`, `1XXXXXXX`(バージョン 5.0+ のみ) • オレンジ(2、潜在的に脆弱):`00X0011X` • 黄(3、現在は脆弱でない):`00X0001X` • 青(4、不明なターゲット):`00X00001`
影響	uint8	イベントの影響フラグ値。値は次のとおりです。 • `1`:レッド(脆弱) • `2`:オレンジ(脆弱の可能性あり) • `3`:イエロー(現在は脆弱でない) • `4`:ブルー(不明なターゲット) • `5`:グレー(不明なインパクト)

表 B-7　侵入イベント レコード5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 • 0:ブロックされていない • 1:ブロックされた • 2:ブロックされた可能性がある(設定では許可されていない)
MPLSラベル	uint32	MPLS ラベル。
VLAN ID	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルの内部 ID 番号(該当する場合)。
アクセス コントロール ルール ID	uint32	アクセス コントロール ルールの固有識別子として機能するルール ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティ ゾーン UUID	uint8[16]	入力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティ ゾーン UUID	uint8[16]	出力セキュリティ ゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
送信元の国	uint16	送信元ホストの国のコード。

表 B-7　侵入イベント レコード5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
宛先の国	uint 16	宛先ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティ コンテキスト	uint8[16]	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書 フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 B-7　侵入イベント レコード 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
SSL フロー ステータス	uint16	SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。 • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
ネットワーク分析ポリシー UUID	uint8[16]	侵入イベントを作成したネットワーク分析ポリシーの UUID。

侵入影響アラート データ

侵入影響アラート イベントには、影響イベントに関する情報が含まれます。これは、侵入イベントがシステム ネットワーク マップ データと比較され、影響が判別されているときに送信されます。これはレコード タイプ 9 の標準レコード ヘッダーを使用し、シリーズ 1 グループのブロックの、データ ブロック タイプが 20 である侵入影響アラート データ ブロックが続きます。（影響アラート データ ブロック タイプは、シリーズ 1 データ ブロックです。シリーズ 1 データ ブロックの詳細については、ディスカバリ（シリーズ1）ブロック（4-63 ページ）を参照してください。）

要求メッセージのフラグ フィールドにビット 5 を設定することで、eStreamer が侵入の影響イベントを送信するように要求できます。要求メッセージの詳細については、イベント ストリーム要求メッセージの形式（2-11 ページ）を参照してください。これらのアラートのバージョン 1 は、IPv4 のみを処理します。5.3 で導入されたバージョン 2 は、IPv4 に加えて IPv6 イベントを処理します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン（1）																メッセージ タイプ（4）															
	メッセージ長																															
	Netmap ID																レコード タイプ（9）															
	レコード長																															
	侵入影響アラート ブロック タイプ（20）																															
	侵入影響アラート ブロック長																															
	イベント ID																															
	デバイス ID																															
	イベント秒																															
	影響																															
	送信元 IP アドレス																															
	宛先 IP アドレス																															
影響説明	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	説明...																															

次の表は、影響イベントの各データ フィールドについての説明です。

表 B-8　影響イベント データ フィールド

フィールド	データ タイプ	説明
侵入影響アラート ブロック タイプ	uint32	侵入影響アラート データ ブロックが続くことを示します。このフィールドの値は、常に 20 です。侵入イベントとメタデータのレコード タイプ(3-1 ページ)を参照してください。
侵入影響アラート ブロック長	uint32	侵入の影響アラートのブロック タイプの長さを示します。後続のすべてのデータ、および侵入の影響アラートのブロック タイプと長さの 8 バイトを含みます。
イベント ID	uint32	イベント ID 番号を表示します。
デバイス ID	uint32	管理対象デバイス ID 番号を表示します。
イベント秒	uint32	イベントが検出された秒(1970 年 1 月 1 日からの経過秒数)を示します。

表 B-8　影響イベント データ フィールド(続き)

フィールド	データ タイプ	説明
影響	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) 次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • (0、不明):00X00000 • 赤(1、脆弱):XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX (バージョン 5.0+ のみ) • オレンジ(2、潜在的に脆弱):00X0011X • 黄(3、現在は脆弱でない):00X0001X • 青(4、不明なターゲット):00X00001
送信元 IP アドレス	uint8[4]	IP アドレス オクテットの、影響イベントに関連付けられているホストの IP アドレス。
宛先IPアドレス	uint8[4]	IP アドレス オクテットの、影響イベントに関連付けられている宛先 IP アドレスの IP アドレス(該当する場合)。宛先 IP アドレスがない場合、この値は 0 です。

表 B-8　影響イベント データ フィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	影響名を含む文字列データのブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、文字列データ ブロック (4-73 ページ) を参照してください。
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数。これには文字列ブロック タイプ用の 4 バイト、文字列ブロック長用の 4 バイト、および説明のバイト数が含まれます。
説明	string	影響イベントについての説明。

レガシー マルウェア イベントのデータ構造

マルウェア イベントのデータ ブロック 5.1

eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 16 です。マルウェア イベント レコードの一部としてイベントを要求するには、イベント バージョン 1 およびイベント コード 101 の要求メッセージ内に、マルウェア イベント フラグ(要求フラグ フィールドのビット 30)を設定します。

次の図は、マルウェア イベント データ ブロックの構造を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
マルウェア イベント ブロック タイプ(16)																																
マルウェア イベントのブロック長																																
エージェント UUID エージェント UUID(続き) エージェント UUID(続き)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	エージェント UUID（続き）																															
	クラウド UUID クラウド UUID（続き） クラウド UUID（続き） クラウド UUID（続き）																															
	タイムスタンプ																															
	イベント タイプ ID																															
	イベント サブタイプ ID								ホスト IP アドレス																							
検出名	ホスト IP アドレス（続き）								ディテクタ ID								文字列ブロック タイプ（0）															
	文字列ブロック タイプ（0）（続き）																文字列ブロック長															
	文字列ブロック長（続き）																検出名...															
ユーザ	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル名...																															
ファイル パス	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル パス...																															
ファイル SHA ハッシュ	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイル サイズ																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ファイル タイプ								ファイルのタイムスタンプ																							
親ファイル名前	ファイルのタイムスタンプ（続き）								文字列ブロック タイプ(0)																							
	文字列ブロック タイプ(0)（続き）								文字列ブロック長																							
	文字列ブロック長（続き）								親ファイル名...																							
親ファイル SHA ハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル SHA ハッシュ...																															
イベント説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	イベントの説明...																															

次の表は、マルウェア イベント データ ブロックのフィールドについての説明です。

表 B-9　　マルウェア イベント データ ブロックのフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 16 です。
マルウェア イベントのブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする AMP for Endpoints エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェア イベントの発生元であるマルウェア認識ネットワークの、内部の固有 ID。
タイムスタンプ	uint32	マルウェア イベント生成時のタイムスタンプ。
イベント タイプ ID	uint32	マルウェア イベント タイプの内部 ID。
イベント サブタイプ ID	uint8	マルウェア検出につながったアクションの内部 ID。
ホスト IP アドレス	uint32	マルウェア イベントに関連付けられているホスト IP アドレス。

表 B-9　マルウェア イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。
文字列ブロック タイプ	uint32	検出名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	検出名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロック タイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ フィールドのバイト数を含む)。
ユーザ	string	Cisco Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイル パスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル パス文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル パス フィールドのバイト数を含む)。
ファイル パス	string	検出または検疫されたファイルのファイル パス。ファイル名は含まれません。
文字列ブロック タイプ	uint32	ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル SHA ハッシュ フィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値。
ファイル サイズ	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイル タイプ	uint8	検出または検疫されたファイルのファイル タイプ。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成タイムスタンプ。

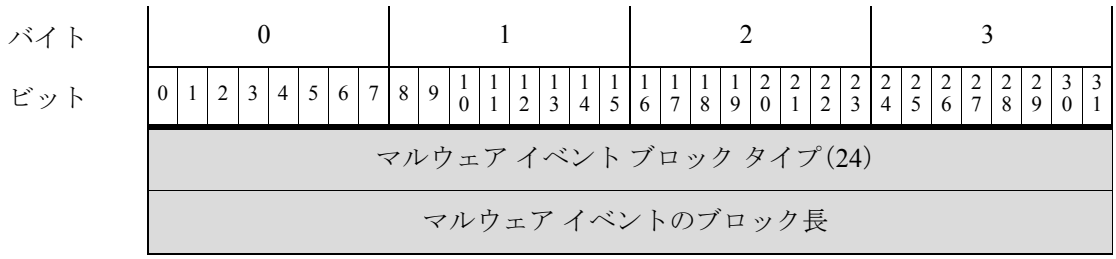
表 B-9　　マルウェア イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	親ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロック タイプ	uint32	親ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル SHA ハッシュ フィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロック タイプ	uint32	イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベント タイプに関連付けられている追加イベント情報。

マルウェア イベント データ ブロック 5.1.1.x

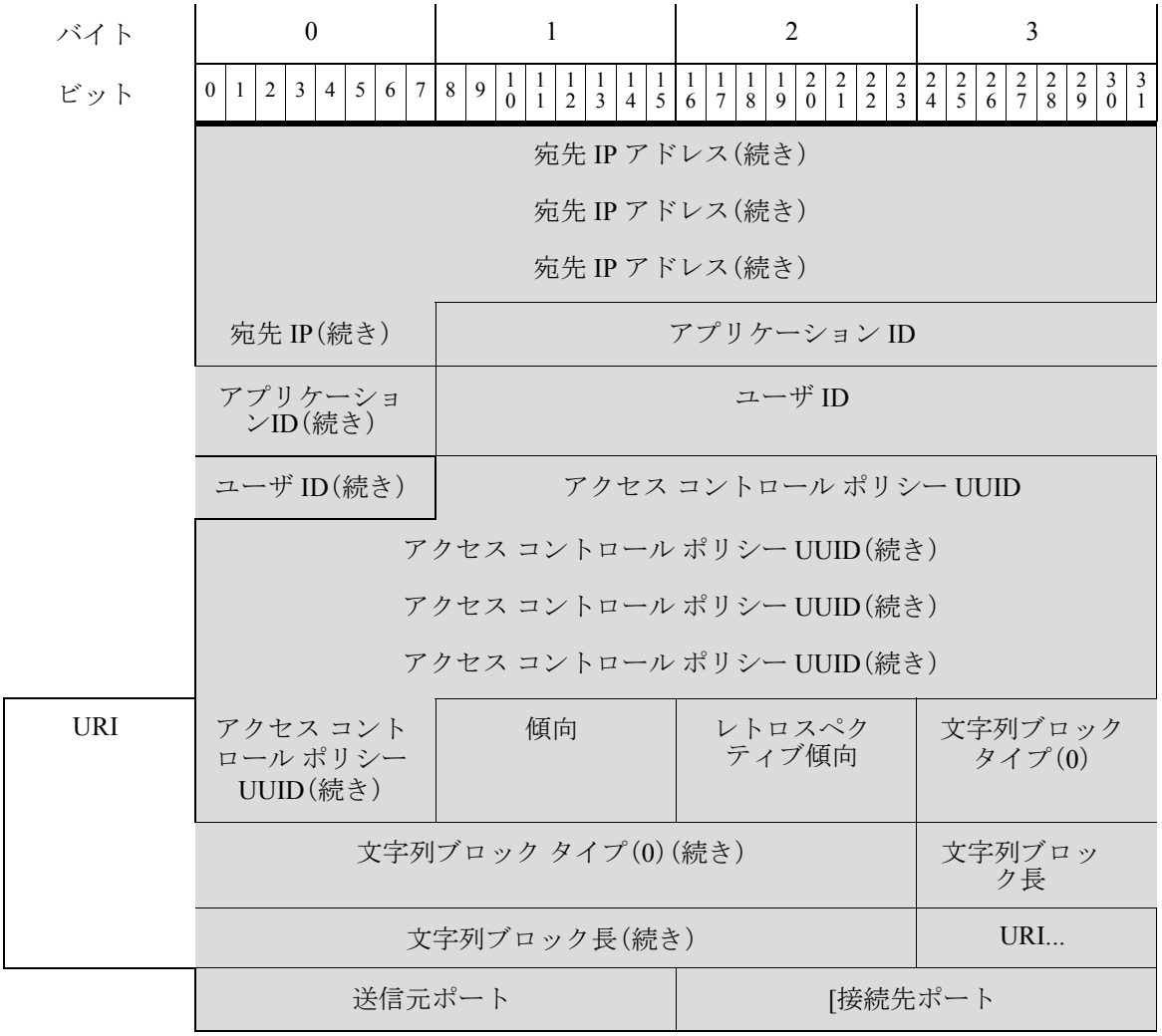
eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 24 です。マルウェア イベント レコードの一部として、イベント バージョン 2 およびイベント コード 101 の要求メッセージ内にマルウェア イベント フラグ(要求フラグ フィールドのビット 30)を設定して、イベントを要求します。

次の図は、マルウェア イベント データ ブロックの構造を示しています。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	エージェント UUID																															
	エージェント UUID（続き）																															
	エージェント UUID（続き）																															
	エージェント UUID（続き）																															
	クラウド UUID																															
	クラウド UUID（続き）																															
	クラウド UUID（続き）																															
	クラウド UUID（続き）																															
	マルウェア イベント タイムスタンプ																															
	イベント タイプ ID																															
	イベント サブタイプ ID								ホスト IP アドレス																							
検出名	ホスト IP アドレス（続き）								ディテクタ ID								文字列ブロック タイプ（0）															
	文字列ブロック タイプ（0）（続き）																文字列ブロック長															
	文字列ブロック長（続き）																検出名...															
ユーザ	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル名...																															
ファイル パス	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル パス...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイル SHAハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイル サイズ																															
	ファイル タイプ								ファイルのタイムスタンプ																							
親ファイル名.	ファイルのタイムスタンプ(続き)								文字列ブロック タイプ(0)																							
	文字列ブロック タイプ(0)(続き)								文字列ブロック長																							
	文字列ブロック長(続き)								親ファイル名...																							
親ファイル SHA ハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル SHA ハッシュ...																															
イベント説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	イベントの説明...																															
	デバイス ID																															
	接続インスタンス																接続数カウンタ															
	接続イベント タイムスタンプ																															
	方向								送信元 IP アドレス																							
	送信元 IP アドレス(続き)																															
	送信元 IP アドレス(続き)																															
	送信元 IP アドレス(続き)																															
	送信元 IP(続き)								宛先IPアドレス																							



次の表は、マルウェア イベント データ ブロックのフィールドについての説明です。

表 B-10　　マルウェア イベント データ ブロック 5.1.1.x のフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 24 です。
マルウェア イベントのブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする AMP for Endpoints エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェア イベントの発生元であるマルウェア認識ネットワークの、内部の固有 ID。
マルウェア イベント タイムスタンプ	uint32	マルウェア イベント生成時のタイムスタンプ。

表 B-10　マルウェア イベント データ ブロック 5.1.1.x のフィールド(続き)

フィールド	データ タイプ	説明
イベント タイプ ID	uint32	マルウェア イベント タイプの内部 ID。
イベント サブタイプ ID	uint8	マルウェア検出につながったアクションの内部 ID。
ホスト IP アドレス	uint32	マルウェア イベントに関連付けられているホスト IP アドレス。
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。
文字列ブロック タイプ	uint32	検出名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	検出名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロック タイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ フィールドのバイト数を含む)。
ユーザ	string	Cisco Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイル パスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル パス文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル パス フィールドのバイト数を含む)。
ファイル パス	string	検出または検疫されたファイルのファイル パス。ファイル名は含まれません。
文字列ブロック タイプ	uint32	ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル SHA ハッシュ フィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値のレンダリングされた文字列。

表 B-10　マルウェア イベント データ ブロック 5.1.1.x のフィールド(続き)

フィールド	データ タイプ	説明
ファイル サイズ	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイル タイプ	uint8	検出または検疫されたファイルのファイル タイプ。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
文字列ブロック タイプ	uint32	親ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロック タイプ	uint32	親ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル SHA ハッシュ フィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロック タイプ	uint32	イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベント タイプに関連付けられている追加イベント情報。
デバイス ID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または IDS イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続イベント タイムスタンプ	uint32	接続イベントのタイムスタンプ。
方向	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示します。次のいずれかの値になります。 • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。

表 B-10　マルウェア イベント データ ブロック 5.1.1.x のフィールド(続き)

フィールド	データ タイプ	説明
アプリケーション ID	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する ID 番号。
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4(CACHE_MISS):ソフトウェアは Cisco クラウドに特性を確認する要求を送信できませんでした。 • 5(NO_CLOUD_RESP):Cisco クラウド サービスが要求に応答しませんでした。
レトロスペクティブ特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロック タイプ	uint32	URI を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。

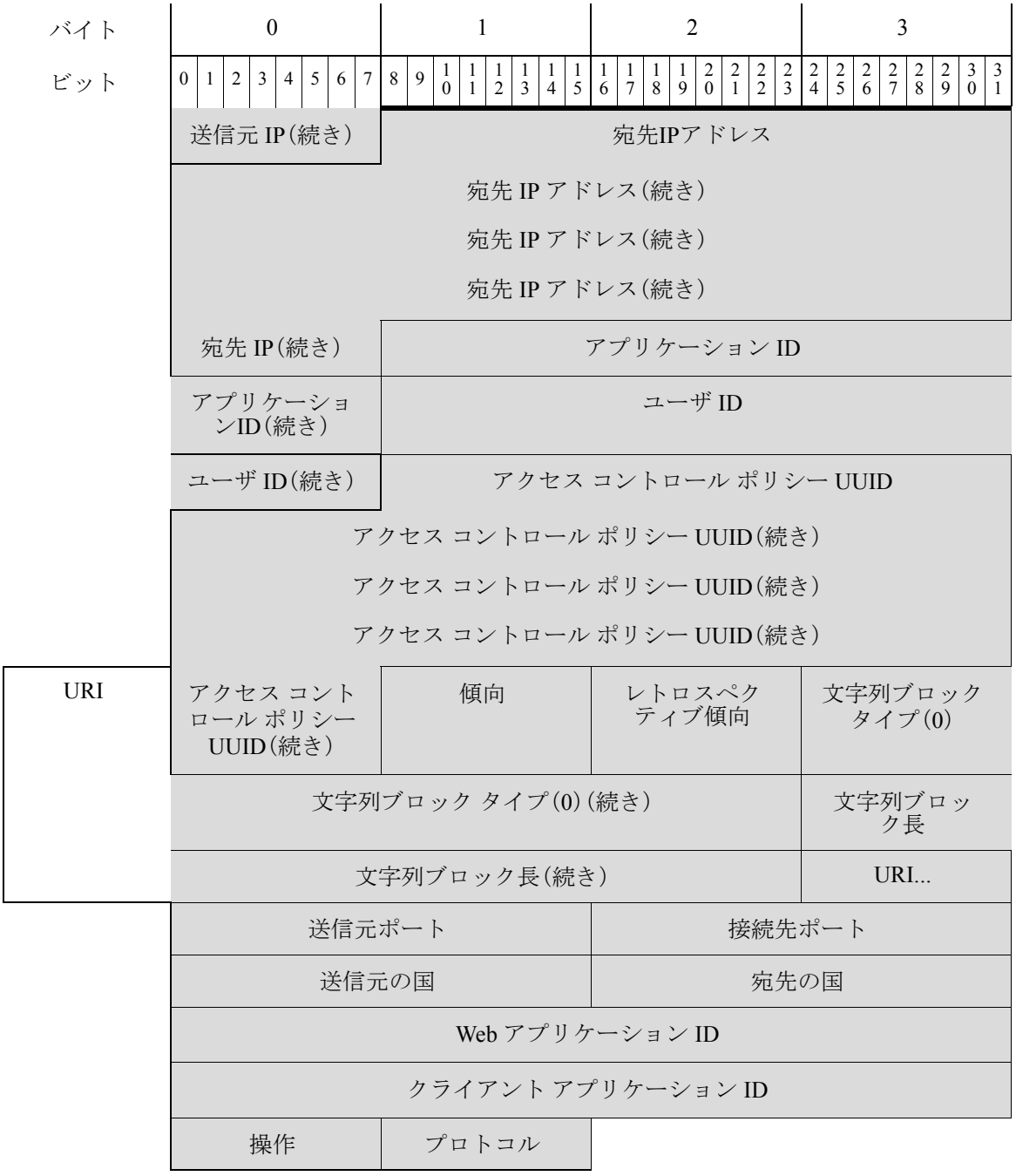
マルウェア イベント データ ブロック 5.2.x

eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 33 です。マルウェア イベント レコードの一部として、イベント バージョン 3 およびイベント コード 101 の要求メッセージ内にマルウェア イベント フラグ(要求フラグ フィールドのビット 30)を設定して、イベントを要求します。

次の図は、マルウェア イベント データ ブロックの構造を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	マルウェア イベントのブロック タイプ（33）																															
	マルウェア イベントのブロック長																															
	エージェント UUID エージェント UUID（続き） エージェント UUID（続き） エージェント UUID（続き）																															
	クラウド UUID クラウド UUID（続き） クラウド UUID（続き） クラウド UUID（続き）																															
	マルウェア イベント タイムスタンプ																															
	イベント タイプ ID																															
検出名	イベント サブタイプ ID								ディテクタ ID								文字列ブロック タイプ（0）															
	文字列ブロック タイプ（0）（続き）																文字列ブロック長															
	文字列ブロック長（続き）																検出名...															
ユーザ	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル名...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイル パス	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル パス...																															
ファイル SHA ハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイル サイズ																															
	ファイル タイプ																															
	ファイルのタイムスタンプ																															
親ファイル名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル名...																															
親ファイル SHA ハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル SHA ハッシュ...																															
イベント 説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	イベントの説明...																															
	デバイス ID																															
	接続インスタンス																接続数カウンタ															
	接続イベント タイムスタンプ																															
	方向								送信元 IP アドレス																							
	送信元 IP アドレス(続き)																															
	送信元 IP アドレス(続き)																															
	送信元 IP アドレス(続き)																															


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
送信元 IP(続き)
宛先IPアドレス
宛先 IP アドレス(続き)
宛先 IP アドレス(続き)
宛先 IP アドレス(続き)
宛先 IP(続き)
アプリケーション ID
アプリケーションID(続き)
ユーザ ID
ユーザ ID(続き)
アクセス コントロール ポリシー UUID
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
URI
アクセス コントロール ポリシー UUID(続き)
傾向
レトロスペクティブ傾向
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
URI...
送信元ポート
接続先ポート
送信元の国
宛先の国
Web アプリケーション ID
クライアント アプリケーション ID
操作
プロトコル

次の表は、マルウェア イベント データ ブロックのフィールドについての説明です。

表 B-11　　マルウェア イベント データ ブロック 5.2.x のフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 33 です。
マルウェア イベントのブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする AMP for Endpoints エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェア イベントの発生元であるマルウェア認識ネットワークの、内部の固有 ID。
マルウェア イベント タイムスタンプ	uint32	マルウェア イベント生成時のタイムスタンプ。
イベント タイプ ID	uint32	マルウェア イベント タイプの内部 ID。
イベント サブタイプ ID	uint8	マルウェア検出につながったアクションの内部 ID。
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。
文字列ブロック タイプ	uint32	検出名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	検出名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロック タイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ フィールドのバイト数を含む)。
ユーザ	string	Cisco Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイル パスを含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-11　マルウェア イベント データ ブロック 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	ファイル パス文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル パス フィールドのバイト数を含む)。
ファイル パス	string	検出または検疫されたファイルのファイル パス。ファイル名は含まれません。
文字列ブロック タイプ	uint32	ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル SHA ハッシュ フィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値のレンダリングされた文字列。
ファイル サイズ	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイル タイプ	uint8	検出または検疫されたファイルのファイル タイプ。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
文字列ブロック タイプ	uint32	親ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロック タイプ	uint32	親ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル SHA ハッシュ フィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロック タイプ	uint32	イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベント タイプに関連付けられている追加イベント情報。
デバイス ID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または IDS イベントとイベントをリンクするために使用されます。

表 B-11　マルウェア イベント データ ブロック 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続イベント タイムスタンプ	uint32	接続イベントのタイムスタンプ。
方向	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示します。次のいずれかの値になります。 • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する ID 番号。
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(NEUTRAL):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4(CACHE_MISS):ソフトウェアから Cisco クラウドに対して、特性を確認する要求を送信できなかったか、または Cisco クラウド サービスが要求に応答しませんでした。
レトロスペクティブ特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロック タイプ	uint32	URI を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。

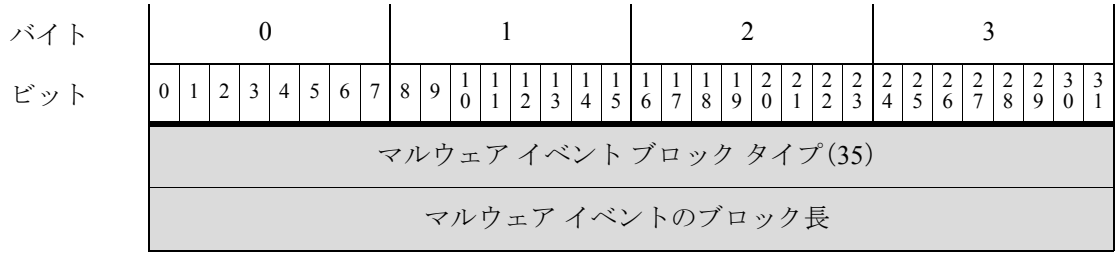
表 B-11　マルウェア イベント データ ブロック 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
接続先ポート	uint16	接続の宛先のポート番号。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。

マルウェア イベントのデータ ブロック 5.3

eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 35 です。マルウェア イベント レコードの一部として、イベント バージョン 4 およびイベント コード 101 の要求メッセージ内にマルウェア イベント フラグ(要求フラグ フィールドのビット 30)を設定して、イベントを要求します。

次の図は、マルウェア イベント データ ブロックの構造を示しています。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	エージェント UUID																															
	エージェント UUID（続き）																															
	エージェント UUID（続き）																															
	エージェント UUID（続き）																															
	クラウド UUID																															
	クラウド UUID（続き）																															
	クラウド UUID（続き）																															
	クラウド UUID（続き）																															
	マルウェア イベント タイムスタンプ																															
	イベント タイプ ID																															
	イベント サブタイプ ID																															
検出名	ディテクタ ID								文字列ブロック タイプ（0）																							
	文字列ブロック タイプ（0）（続き）								文字列ブロック長																							
	文字列ブロック長（続き）								検出名...																							
ユーザ	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル名...																															
ファイル パス	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル パス...																															


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
ファイル SHAハッシュ
文字列ブロック タイプ(0)
文字列ブロック長
ファイル SHA ハッシュ...
ファイル サイズ
ファイル タイプ
ファイルのタイムスタンプ
親ファイル名
文字列ブロック タイプ(0)
文字列ブロック長
親ファイル名...
親ファイル SHA ハッシュ
文字列ブロック タイプ(0)
文字列ブロック長
親ファイル SHA ハッシュ...
イベント説明
文字列ブロック タイプ(0)
文字列ブロック長
イベントの説明...
デバイス ID
接続インスタンス
接続数カウンタ
接続イベント タイムスタンプ
方向
送信元 IP アドレス
送信元 IP アドレス(続き)
送信元 IP アドレス(続き)
送信元 IP アドレス(続き)
送信元 IP(続き)
宛先IPアドレス


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
宛先 IP アドレス(続き)
宛先 IP アドレス(続き)
宛先 IP アドレス(続き)
宛先 IP(続き)
アプリケーション ID
アプリケーション ID(続き)
ユーザ ID
ユーザ ID(続き)
アクセス コントロール ポリシー UUID
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
URI
アクセス コントロール ポリシー UUID(続き)
傾向
レトロスペクティブ傾向
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
URI...
送信元ポート
[接続先ポート
送信元の国
宛先の国
Web アプリケーション ID
クライアント アプリケーション ID
操作
プロトコル
脅威スコア
IOC 番号
IOC 番号(続き)

次の表は、マルウェア イベント データ ブロックのフィールドについての説明です。

表 B-12　　マルウェア イベント データ ブロック 5.3 のフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 35 です。
マルウェア イベントのブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする AMP for Endpoints エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェア イベントの発生元であるマルウェア認識ネットワークの、内部の固有 ID。
マルウェア イベント タイムスタンプ	uint32	マルウェア イベント生成時のタイムスタンプ。
イベント タイプ ID	uint32	マルウェア イベント タイプの内部 ID。
イベント サブタイプ ID	uint32	マルウェア検出につながったアクションの内部 ID。
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。
文字列ブロック タイプ	uint32	検出名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	検出名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロック タイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ フィールドのバイト数を含む)。
ユーザ	string	Cisco Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイル パスを含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-12　マルウェア イベント データ ブロック 5.3 のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	ファイル パス文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル パス フィールドのバイト数を含む)。
ファイル パス	string	検出または検疫されたファイルのファイル パス。ファイル名は含まれません。
文字列ブロック タイプ	uint32	ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル SHA ハッシュ フィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値のレンダリングされた文字列。
ファイル サイズ	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイル タイプ	uint8	検出または検疫されたファイルのファイル タイプ。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、AMP for Endpoints ファイル タイプのメタデータ (3-44 ページ) を参照してください。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
文字列ブロック タイプ	uint32	親ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロック タイプ	uint32	親ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル SHA ハッシュ フィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロック タイプ	uint32	イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベント タイプに関連付けられている追加イベント情報。
デバイス ID	uint32	イベントを生成したデバイスの ID。

表 B-12　マルウェア イベント データ ブロック 5.3 のフィールド(続き)

フィールド	データ タイプ	説明
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または IDS イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続イベント タイムスタンプ	uint32	接続イベントのタイムスタンプ。
方向	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示します。次のいずれかの値になります。 • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する ID 番号。
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4(UNAVAILABLE):ソフトウェアから Cisco クラウドに対して、特性を確認する要求を送信できなかったか、または Cisco クラウド サービスが要求に応答しませんでした。 • 5(CUSTOM SIGNATURE):ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
レトロスペクティブ特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。

表 B-12　マルウェア イベント データ ブロック 5.3 のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	URI を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ～ 100)。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。

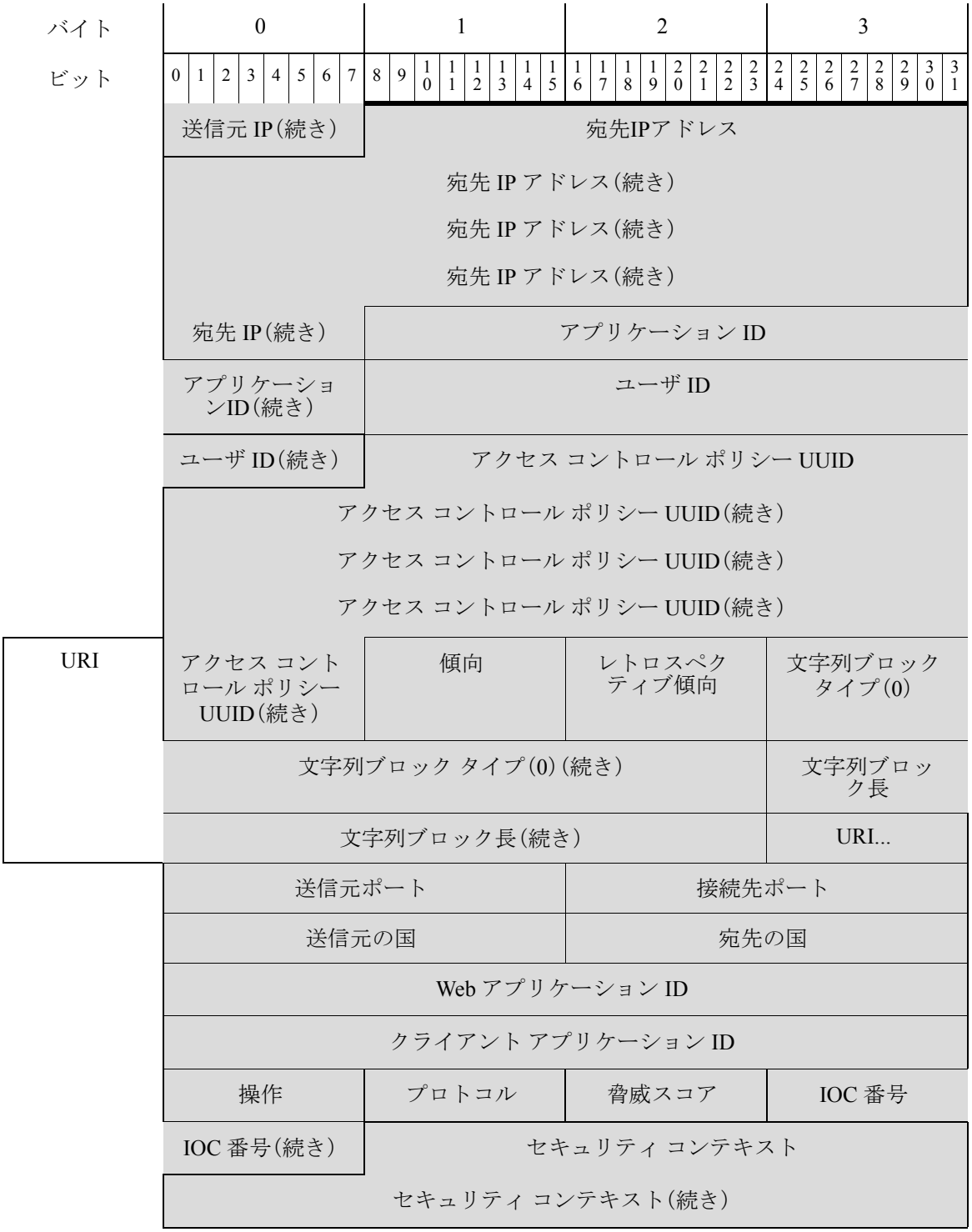
マルウェア イベント データ ブロック 5.3.1

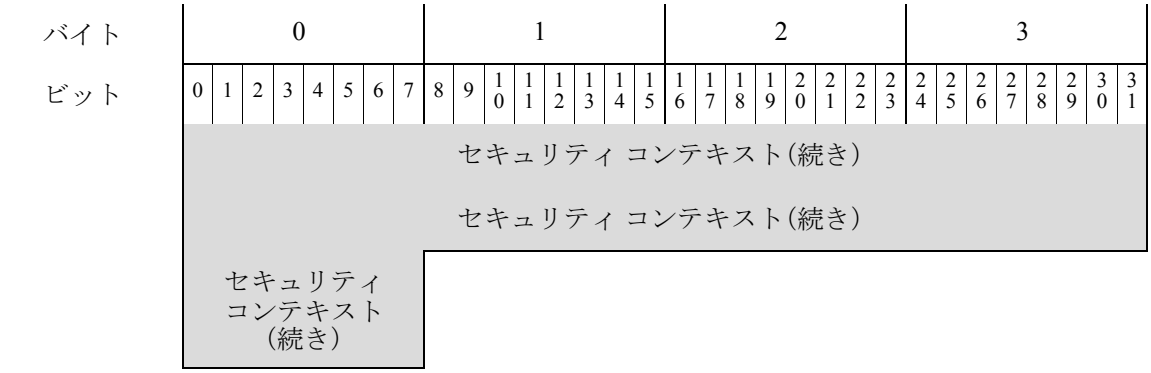
eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 44 です。これはブロック 35 に取って代わります。マルウェア イベント レコードの一部として、イベント バージョン 5 およびイベント コード 101 の要求メッセージ内にマルウェア イベント フラグ(要求フラグ フィールドのビット 30)を設定して、イベントを要求します。

次の図は、マルウェア イベント データ ブロックの構造を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	マルウェア イベント ブロック タイプ(44)																															
	マルウェア イベントのブロック長																															
	エージェント UUID エージェント UUID(続き) エージェント UUID(続き) エージェント UUID(続き)																															
	クラウド UUID クラウド UUID(続き) クラウド UUID(続き) クラウド UUID(続き)																															
	マルウェア イベント タイムスタンプ																															
	イベント タイプ ID																															
	イベント サブタイプ ID																															
検出名	ディテクタ ID								文字列ブロック タイプ(0)																							
	文字列ブロック タイプ(0)(続き)								文字列ブロック長																							
	文字列ブロック長(続き)								検出名...																							
ユーザ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル名...																															

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイル パス		文字列ブロック タイプ(0)																															
		文字列ブロック長																															
		ファイル パス...																															
ファイル SHAハッシュ		文字列ブロック タイプ(0)																															
		文字列ブロック長																															
		ファイル SHA ハッシュ...																															
		ファイル サイズ																															
		ファイル タイプ																															
		ファイルのタイムスタンプ																															
親ファイル 名		文字列ブロック タイプ(0)																															
		文字列ブロック長																															
		親ファイル名...																															
親ファイル SHA ハッシュ		文字列ブロック タイプ(0)																															
		文字列ブロック長																															
		親ファイル SHA ハッシュ...																															
イベント 説明		文字列ブロック タイプ(0)																															
		文字列ブロック長																															
		イベントの説明...																															
		デバイスID																															
		接続インスタンス																接続数カウンタ															
		接続イベント タイムスタンプ																															
		方向								送信元 IP アドレス																							
		送信元 IP アドレス(続き)																															
		送信元 IP アドレス(続き)																															
		送信元 IP アドレス(続き)																															


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
送信元 IP(続き)
宛先IPアドレス
宛先 IP アドレス(続き)
宛先 IP アドレス(続き)
宛先 IP アドレス(続き)
宛先 IP(続き)
アプリケーション ID
アプリケーションID(続き)
ユーザ ID
ユーザ ID(続き)
アクセス コントロール ポリシー UUID
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
URI
アクセス コントロール ポリシー UUID(続き)
傾向
レトロスペクティブ傾向
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
URI...
送信元ポート
接続先ポート
送信元の国
宛先の国
Web アプリケーション ID
クライアント アプリケーション ID
操作
プロトコル
脅威スコア
IOC 番号
IOC 番号(続き)
セキュリティ コンテキスト
セキュリティ コンテキスト(続き)



次の表は、マルウェア イベント データ ブロックのフィールドについての説明です。

表 B-13　　マルウェア イベント データ ブロック 5.3.1 のフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 44 です。
マルウェア イベントのブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする AMP for Endpoints エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェア イベントの発生元 Cisco Advanced Malware Protection cloud の、内部の固有 ID。
マルウェア イベント タイムスタンプ	uint32	マルウェア イベント生成時のタイムスタンプ。
イベント タイプ ID	uint32	マルウェア イベント タイプの内部 ID。
イベント サブタイプ ID	uint32	マルウェア検出につながったアクションの内部 ID。
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。
文字列ブロック タイプ	uint32	検出名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	検出名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロック タイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ フィールドのバイト数を含む)。

表 B-13　マルウェア イベント データ ブロック 5.3.1 のフィールド(続き)

フィールド	データ タイプ	説明
ユーザ	string	Cisco Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイル パスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル パス文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル パス フィールドのバイト数を含む)。
ファイル パス	string	検出または検疫されたファイルのファイル パス。ファイル名は含まれません。
文字列ブロック タイプ	uint32	ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル SHA ハッシュ フィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値のレンダリングされた文字列。
ファイル サイズ	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイル タイプ	uint8	検出または検疫されたファイルのファイル タイプ。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、AMP for Endpoints ファイル タイプのメタデータ (3-44 ページ) を参照してください。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
文字列ブロック タイプ	uint32	親ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロック タイプ	uint32	親ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-13　マルウェア イベント データ ブロック 5.3.1 のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル SHA ハッシュ フィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロック タイプ	uint32	イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベント タイプに関連付けられている追加イベント情報。
デバイスID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または IDS イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続イベント タイムスタンプ	uint32	接続イベントのタイムスタンプ。
方向	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示します。次のいずれかの値になります。 • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する ID 番号。

表 B-13　マルウェア イベント データ ブロック 5.3.1 のフィールド(続き)

フィールド	データ タイプ	説明
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4(UNAVAILABLE):ソフトウェアから Cisco クラウドに対して、特性を確認する要求を送信できなかったか、または Cisco クラウド サービスが要求に応答しませんでした。 • 5(CUSTOM SIGNATURE):ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
レトロスペクティブ特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロック タイプ	uint32	URI を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト

表 B-13　マルウェア イベント データ ブロック 5.3.1 のフィールド(続き)

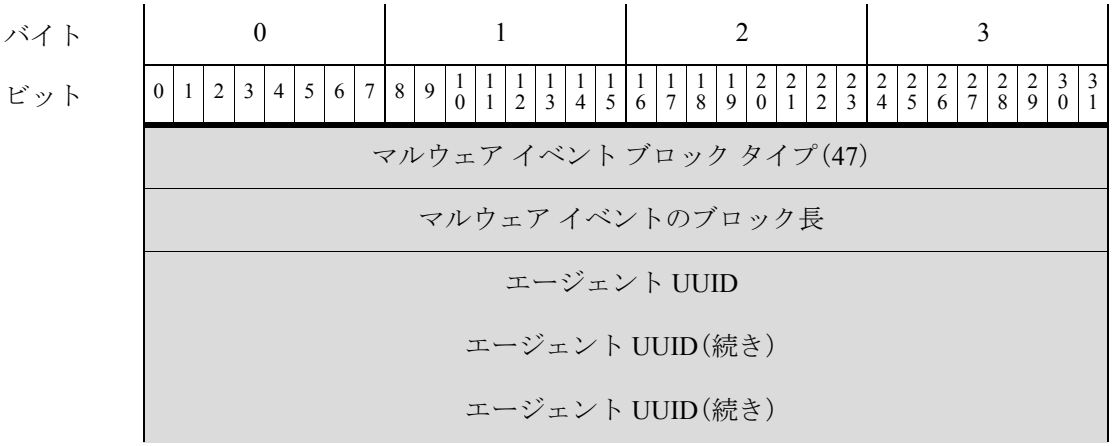
フィールド	データ タイプ	説明
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ～ 100)。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

マルウェア イベント データ ブロック 5.4.x

eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 47 です。これはブロック 44 に取って代わり、ブロックによって取って代わられます。SSL とファイル アーカイブ サポート用のフィールドが追加されました。

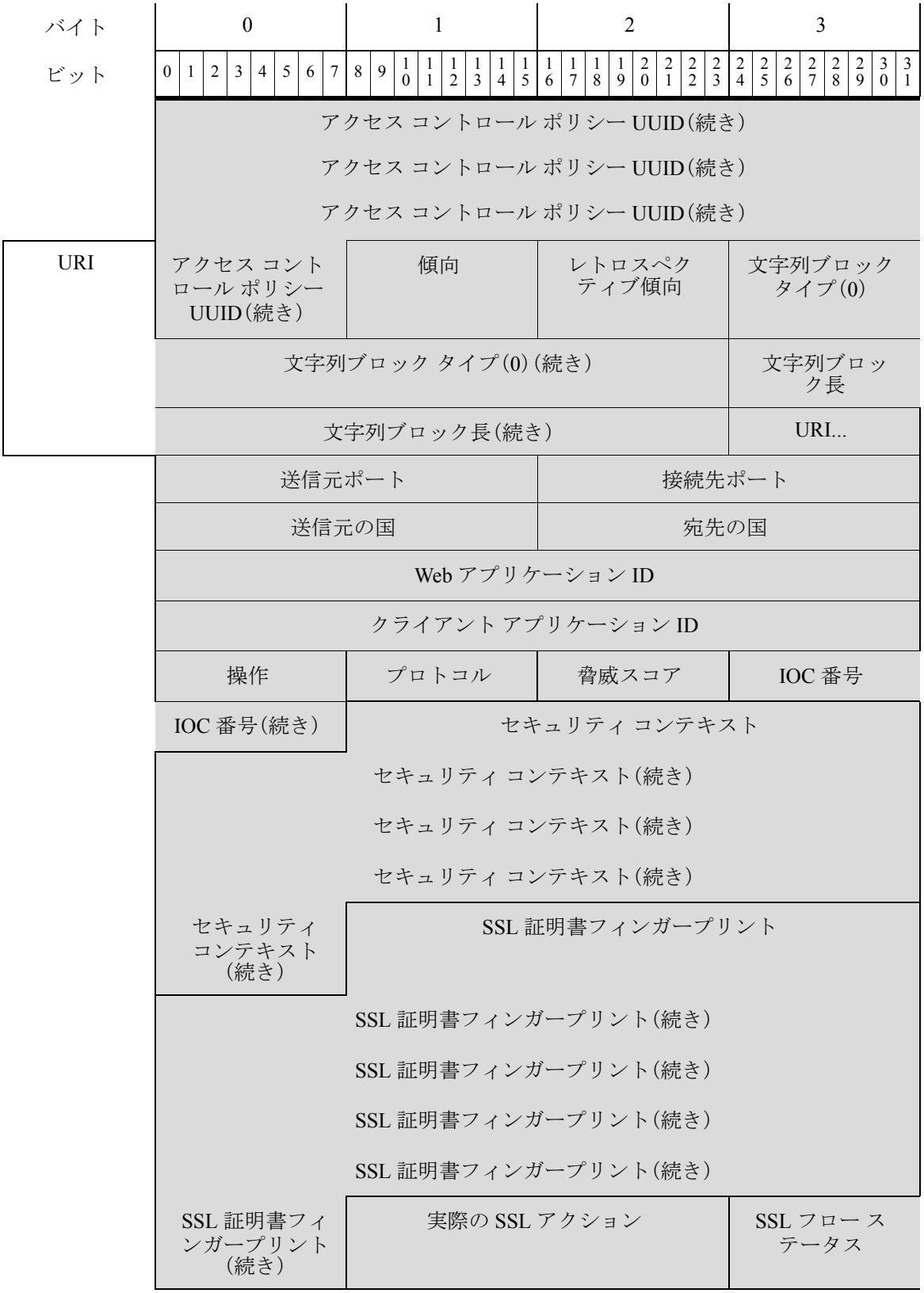
マルウェア イベント レコードの一部としてイベントを要求するには、イベント バージョン 6 およびイベント コード 101 の要求メッセージ内に、マルウェア イベント フラグ(要求フラグ フィールドのビット 30)を設定します。

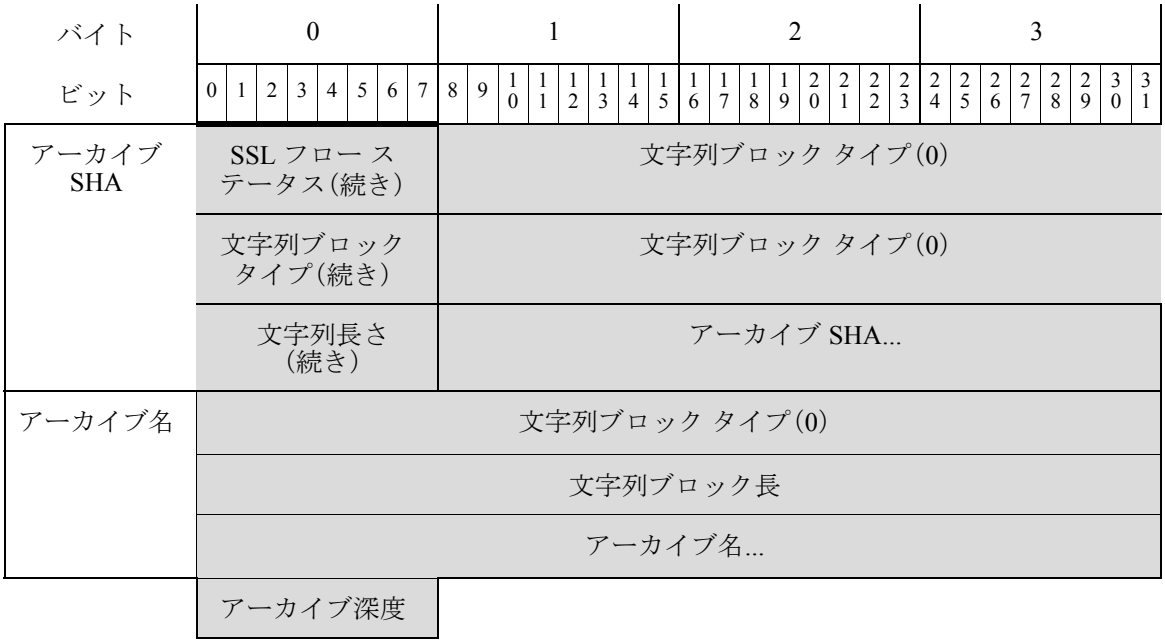
次の図は、マルウェア イベント データ ブロックの構造を示しています。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	エージェント UUID（続き）																															
	クラウド UUID クラウド UUID（続き） クラウド UUID（続き） クラウド UUID（続き）																															
	マルウェア イベント タイムスタンプ																															
	イベント タイプ ID																															
	イベント サブタイプ ID																															
検出名	ディテクタ ID								文字列ブロック タイプ（0）																							
	文字列ブロック タイプ（0）（続き）								文字列ブロック長																							
	文字列ブロック長（続き）								検出名...																							
ユーザ	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル名...																															
ファイル パス	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル パス...																															
ファイル SHAハッシュ	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイル サイズ																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ファイル タイプ																															
	ファイルのタイムスタンプ																															
親ファイル名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル名...																															
親ファイル SHA ハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル SHA ハッシュ...																															
イベント説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	イベントの説明...																															
	デバイスID																															
	接続インスタンス																接続数カウンタ															
	接続イベント タイムスタンプ																															
	方向								送信元 IP アドレス																							
	送信元 IP アドレス(続き)																															
	送信元 IP アドレス(続き)																															
	送信元 IP アドレス(続き)																															
	送信元 IP(続き)								宛先IPアドレス																							
	宛先 IP アドレス(続き)																															
	宛先 IP アドレス(続き)																															
	宛先 IP アドレス(続き)																															
	宛先 IP(続き)								アプリケーション ID																							
	アプリケーションID(続き)								ユーザ ID																							
	ユーザ ID(続き)								アクセス コントロール ポリシー UUID																							


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
URI
アクセス コントロール ポリシー UUID(続き)
傾向
レトロスペクティブ傾向
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
URI...
送信元ポート
接続先ポート
送信元の国
宛先の国
Web アプリケーション ID
クライアント アプリケーション ID
操作
プロトコル
脅威スコア
IOC 番号
IOC 番号(続き)
セキュリティ コンテキスト
セキュリティ コンテキスト(続き)
セキュリティ コンテキスト(続き)
セキュリティ コンテキスト(続き)
セキュリティ コンテキスト(続き)
SSL 証明書フィンガープリント
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
実際の SSL アクション
SSL フロー ステータス



次の表は、マルウェア イベント データ ブロックのフィールドについての説明です。

表 B-14　　マルウェア イベント データ ブロック 5.4.x のフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 47 です。
マルウェア イベントのブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする AMP for Endpoints エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェア イベントの発生元 Cisco Advanced Malware Protection cloud の、内部の固有 ID。
マルウェア イベント タイムスタンプ	uint32	マルウェア イベント生成時のタイムスタンプ。
イベント タイプ ID	uint32	マルウェア イベント タイプの内部 ID。
イベント サブタイプ ID	uint32	マルウェア検出につながったアクションの内部 ID。
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。
文字列ブロック タイプ	uint32	検出名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	検出名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。

表 B-14　マルウェア イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ フィールドのバイト数を含む)。
ユーザ	string	Cisco Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイル パスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル パス文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル パス フィールドのバイト数を含む)。
ファイル パス	string	検出または検疫されたファイルのファイル パス。ファイル名は含まれません。
文字列ブロック タイプ	uint32	ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル SHA ハッシュ フィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値のレンダリングされた文字列。
ファイル サイズ	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイル タイプ	uint8	検出または検疫されたファイルのファイル タイプ。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、AMP for Endpoints ファイル タイプのメタデータ (3-44 ページ) を参照してください。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
文字列ブロック タイプ	uint32	親ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。

表 B-14　マルウェア イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロック タイプ	uint32	親ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル SHA ハッシュ フィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロック タイプ	uint32	イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベント タイプに関連付けられている追加イベント情報。
デバイスID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または IDS イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続イベント タイムスタンプ	uint32	接続イベントのタイムスタンプ。
方向	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示します。次のいずれかの値になります。 • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する ID 番号。

表 B-14　マルウェア イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4(UNAVAILABLE):ソフトウェアから Cisco クラウドに対して、特性を確認する要求を送信できなかったか、または Cisco クラウド サービスが要求に応答しませんでした。 • 5(CUSTOM SIGNATURE):ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
レトロスペクティブ特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロック タイプ	uint32	URI を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。

表 B-14　マルウェア イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト • 6:クラウド ルックアップのタイムアウト • 7:カスタム検出 • 8:カスタム検出ブロック • 9:アーカイブ ブロック(深度超過) • 10:アーカイブ ブロック(暗号化されている) • 11:アーカイブ ブロック(調査エラー)
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ～ 100)。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。

表 B-14　マルウェア イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 B-14　マルウェア イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
SSL フロー ステータス	uint16	SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。 • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
文字列ブロック タイプ	uint32	アーカイブ SHA を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-14　マルウェア イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	アーカイブ SHA 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および侵入ポリシー名のバイト数を含む)。
アーカイブ SHA	string	ファイルが含まれる親アーカイブの SHA1 ハッシュ。
文字列ブロック タイプ	uint32	アーカイブ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	アーカイブ名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびアーカイブ名のバイト数を含む)。
アーカイブ名	string	親アーカイブの名前。
アーカイブ深度	uint8	ファイルがネストされている層の数。たとえば、テキスト ファイルが zip アーカイブ内にある場合、この値は 1 になります。

レガシー ディスカバリ データ構造

レガシー ディスカバリ イベント ヘッダー

ディスカバリ イベント ヘッダー 5.0 ～ 5.1.1.x

ディスカバリ イベントおよび接続イベントのメッセージには、ディスカバリ イベント ヘッダーが含まれます。これは、イベントのタイプおよびサブタイプ、イベントが発生した時刻、イベントが発生したデバイス、およびメッセージ内のイベント データの構造を伝えます。このヘッダーには、実際のホスト ディスカバリ、ユーザ、または接続イベントのデータが続きます。さまざまなイベントのタイプ/サブタイプ値に関連付けられる構造の詳細については、イベント タイプ別ホスト ディスカバリ構造(4-44 ページ)で説明します。

ディスカバリ イベント ヘッダーのイベント タイプ フィールドおよびイベント サブタイプ フィールドは、送信されたイベント メッセージの構造を示します。イベント データ ブロックの構造が一度判別されたら、プログラムはメッセージを適切に解析できます。

次の図の網掛けされた行は、ディスカバリ イベント ヘッダーの形式を例示しています。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		ヘッダー バージョン(1)																メッセージ タイプ(4)																
		メッセージ長																															
		Netmap ID																レコード タイプ															
		レコード長																															
		eStreamer サーバ タイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
		将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
ディスカバリ イベント ヘッダー		デバイス ID																															
		IPアドレス																															
		MAC アドレス																															
		MAC アドレス(続き)																将来の使用に備えて予約済み															
		イベント秒																															
		イベント マイクロ秒																															
		予約済み(内部使用)								イベント タイプ																							
		イベント サブタイプ																															
		ファイル番号(内部使用専用)																															
		ファイルの位置(内部使用専用)																															

次の表は、ディスカバリ イベント ヘッダーについての説明です。

表 B-15　ディスカバリ イベント ヘッダーのフィールド

フィールド	データ型	説明
デバイス ID	uint32	ディスカバリ イベントを生成したデバイスの ID 番号。バージョン 3 および 4 のメタデータを要求すると、デバイスのメタデータを入手できます。詳細については、管理対象 デバイス レコードのメタデータ (3-38 ページ) を参照してください。
IPアドレス	uint32	イベントに関連するホストの IP アドレス。
MAC アドレス	uint86	イベントに関連するホストの MAC アドレス。
将来の使用に備えて予約済み	byte[2]	0 に設定された値による 2 バイトのパディング。
イベント秒	uint32	システムがイベントを生成したときの UNIX タイムスタンプ (1970 年 1 月 1 日以降の秒数)。
イベント マイクロ秒	uint32	システムがイベントを生成したときのタイムスタンプの、マイクロ秒 (100 万分の 1 秒) の増分。
予約済み (内部使用)	バイト	Cisco の内部データであり、無視してかまいません。
イベント タイプ	uint32	イベントのタイプ (新規イベントの場合は 1000、変更イベントの場合は 1001、ユーザ入力イベントの場合は 1002、フル ホスト プロファイルの場合は 1050)。使用可能なイベント タイプの一覧の詳細については、イベント タイプ別ホスト ディスカバリ構造 (4-44 ページ) を参照してください。
イベント サブタイプ	uint32	イベント サブタイプ。使用可能なイベント サブタイプの一覧の詳細については、イベント タイプ別ホスト ディスカバリ構造 (4-44 ページ) を参照してください。
ファイル番号	byte[4]	シリアル ファイル番号。このフィールドは、Cisco の内部使用のためのものであり、無視してかまいません。
ファイルの位置	byte[4]	シリアル ファイル内のイベントの位置。このフィールドは、Cisco の内部使用のためのものであり、無視してかまいません。

レガシー サーバ データ ブロック

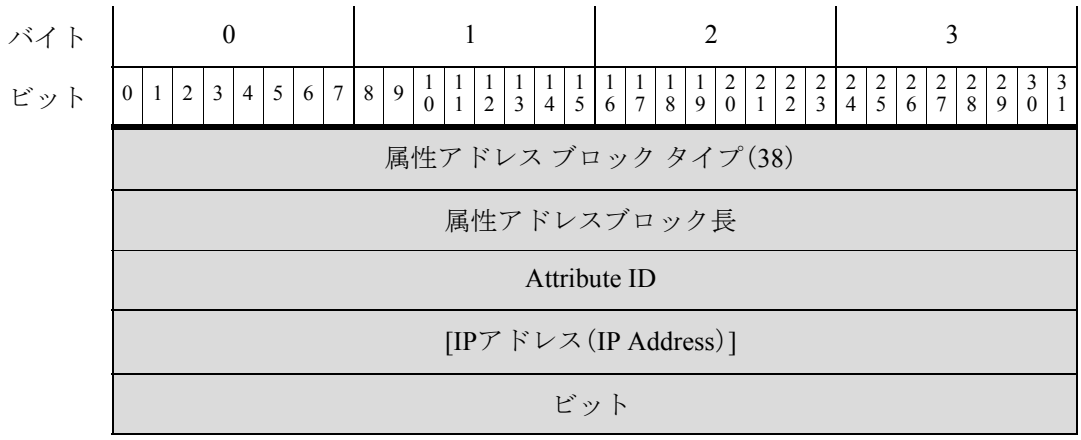
詳細については、次の項を参照してください。

- 属性アドレス データ ブロック 5.0 ～ 5.1.1.x (B-95 ページ)

属性アドレス データ ブロック 5.0 ～ 5.1.1.x

属性アドレス ブロック データは、属性リスト項目が含まれ、属性定義データ ブロック内で使用されます。これはブロック タイプ 38 です。

次の図は、属性アドレス ブロックの基本構造を示しています。



次の表は、属性アドレス データ ブロックのフィールドについての説明です。

表 B-16　　属性アドレス データ ブロックのフィールド

フィールド	データ タイプ	説明
属性アドレス ブロック タイプ	uint32	属性アドレス ブロック データを開始します。この値は常に 38 です。
属性アドレスブロック長	uint32	属性アドレス データ ブロックのバイト数(属性アドレス ブロック タイプと長さ用の 8 バイト、およびそれに続く属性アドレス データのバイト数を含む)。
属性 ID	uint32	影響を受ける属性の ID 番号(該当する場合)。
IPアドレス	uint8[4]	IP アドレス オクテットの、ホストの IP アドレス(アドレスが自動的に割り当てられた場合)。
ビット	uint32	IP アドレスが自動的に割り当てられた場合に、ネットマスクを計算するために使用される有効ビットが含まれます。

レガシー クライアント アプリケーション データ ブロック

詳細については、次の項を参照してください。

- ユーザ クライアント アプリケーション データ ブロック 5.0 ～ 5.1(B-96 ページ)

ユーザ クライアント アプリケーション データ ブロック 5.0 ～ 5.1

ユーザ クライアント アプリケーション データ ブロックには、クライアント アプリケーション データの送信元に関する情報、データを追加したユーザの ID 番号、および IP アドレス範囲データ ブロックのリストが含まれます。ユーザ クライアント アプリケーション データ ブロックのブロック タイプは 59 です。

次の図は、ユーザ クライアント アプリケーション データ ブロックの基本構造を示しています。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ クライアント アプリケーション ブロック タイプ(59)																																
	ユーザ クライアント アプリケーション ブロック長																																
IPアドレス範囲	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
	IP 範囲仕様データ ブロック*																																
	アプリケーション プロトコル ID																																
	クライアント アプリケーション ID																																
バージョン	文字列ブロック タイプ(0)																																
	文字列ブロック長																																
	バージョン...																																

次の表は、ユーザ クライアント アプリケーション データ ブロックのフィールドについての説明です。

表 B-17　ユーザ クライアント アプリケーション データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ クライアント アプリケーション ブロック タイプ	uint32	ユーザ クライアント アプリケーション データ ブロックを開始します。この値は常にです。
ユーザ クライアント アプリケーション ブロック長	uint32	ユーザ クライアント アプリケーション データ ブロックのバイトの合計数(ユーザ クライアント アプリケーション ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ クライアント アプリケーション データのバイト数を含む)。
汎用リスト ブロック タイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リスト データ ブロックのバイト数。
IP範囲仕様データ ブロック*	変数	ユーザ入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データ ブロック。このデータ ブロックの説明の詳細については、表 4-58ユーザ サーバ データ ブロックのフィールド(4-106 ページ)を参照してください。

表 B-17　ユーザ クライアント アプリケーション データ ブロックのフィールド(続き)

フィールド	バイト数	説明
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション バージョン文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド、およびバージョンのバイト数を含む)。
バージョン	string	クライアント アプリケーション バージョン。

レガシー スキャン結果データ ブロック

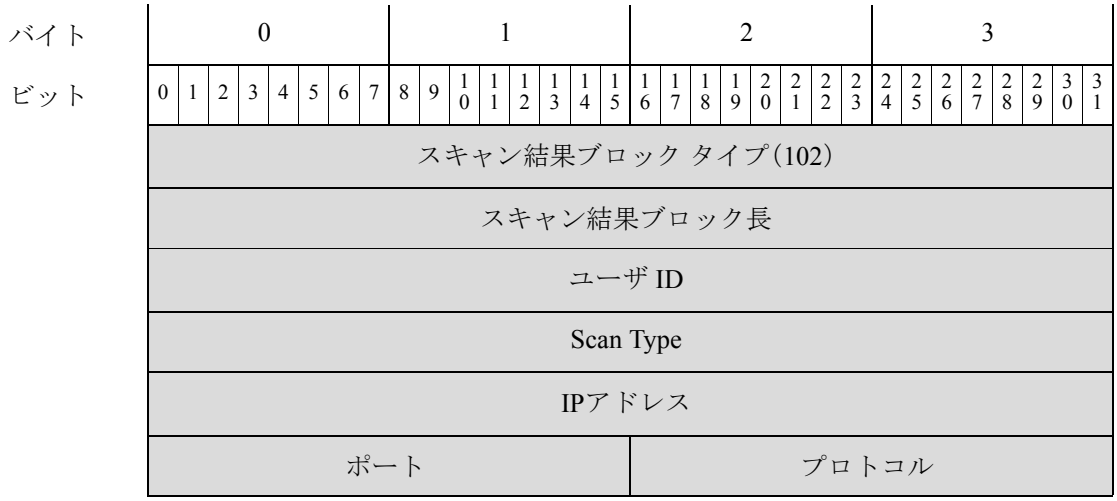
詳細については、次の項を参照してください。

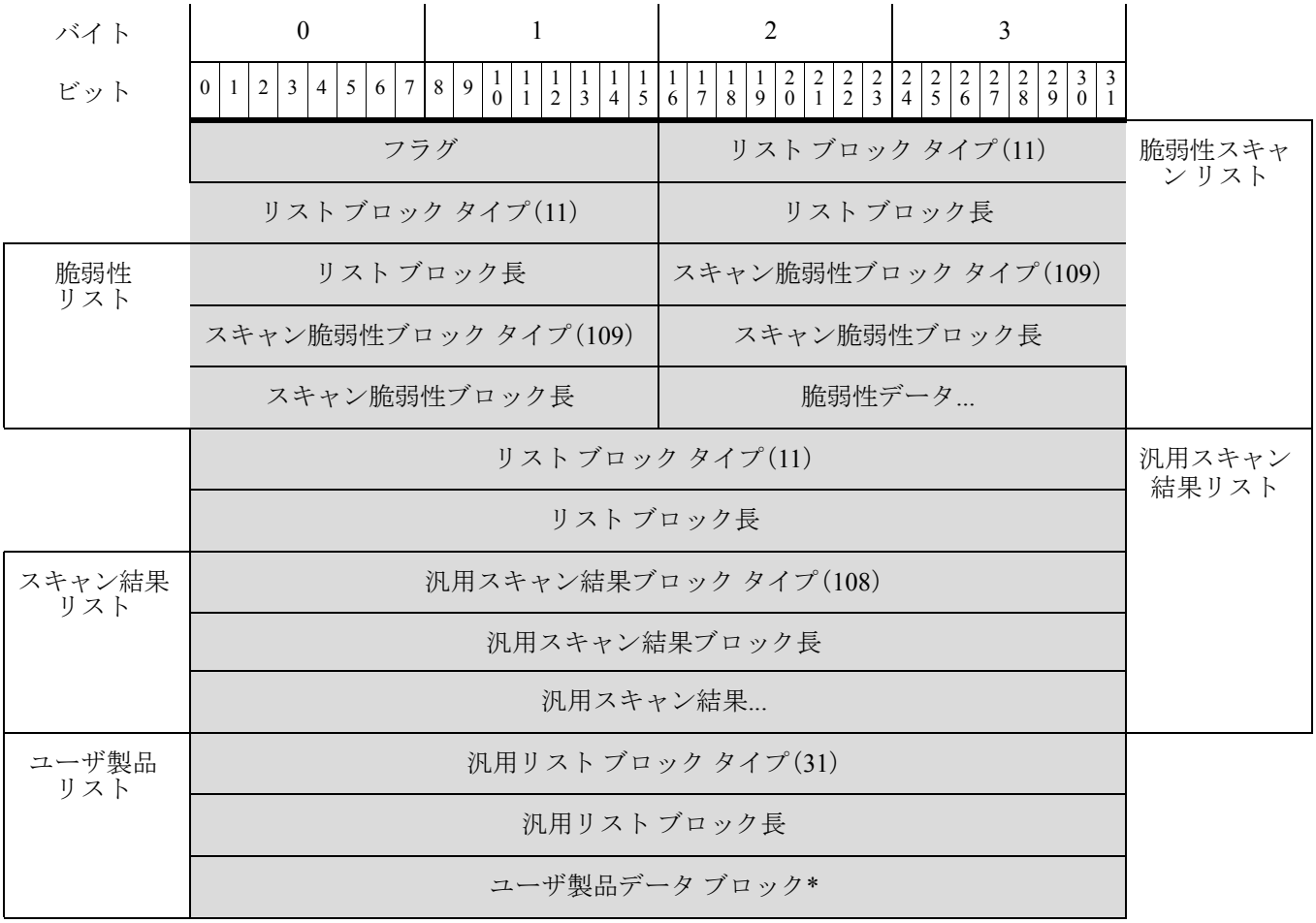
- スキャン結果データ ブロック 5.0 ～ 5.1.1.x(B-98 ページ)
- ユーザ製品データ ブロック 5.0.x(B-101 ページ)
- ユーザ情報データ ブロック 5.x(B-115 ページ)

スキャン結果データ ブロック 5.0 ～ 5.1.1.x

スキャン結果データ ブロックは、脆弱性を説明し、スキャン結果追加イベント内で使用されます(イベント タイプ 1002、サブタイプ 11)。スキャン結果データ ブロックのブロック タイプは 102 です。

次の図は、スキャン結果データ ブロックの形式を示しています。





次の表は、スキャン結果データ ブロックのフィールドについての説明です。

表 B-18　　スキャン結果データ ブロックのフィールド

フィールド	データ タイプ	説明
スキャン結果ブロック タイプ	uint32	スキャン結果データ ブロックを開始します。この値は常に 102 です。
スキャン結果ブロック長	uint32	スキャン脆弱性データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン脆弱性データのバイト数を含む)。
ユーザ ID	uint32	スキャン結果をインポートしたユーザ、またはスキャン結果を生成したスキャンを実行したユーザのユーザ ID 番号が含まれます。
スキャン タイプ	uint32	結果がシステムに追加された方法を示します。
IPアドレス	uint32	IP アドレス オクテットの、結果の脆弱性によって影響を受けるホストの IP アドレス。
ポート	uint16	結果の脆弱性の影響を受ける、サブサーバで使用されるポート。

表 B-18　スキャン結果データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
プロトコル	uint16	IANA プロトコル番号。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP
フラグ	uint16	予約済
リスト ブロック タイプ	uint32	トランスポート スキャン脆弱性データを伝えるスキャン脆弱性データ ブロックで構成されるリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのスキャン脆弱性データ ブロックが含まれています。 このフィールドには、ゼロ以上のスキャン脆弱性データ ブロックが続きます。
スキャン脆弱性ブロック タイプ	uint32	スキャン中に検出された脆弱性を記述するスキャン脆弱性データ ブロックを開始します。この値は常に 109 です。
スキャン脆弱性ブロック長	uint32	スキャン脆弱性データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン脆弱性データのバイト数を含む)。
脆弱性データ	string	各脆弱性に関する情報。
リスト ブロック タイプ	uint32	トランスポート スキャン脆弱性データを伝えるスキャン脆弱性データ ブロックで構成されるリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのスキャン脆弱性データ ブロックが含まれています。 このフィールドには、ゼロ以上のスキャン脆弱性データ ブロックが続きます。
汎用スキャン結果ブロック タイプ	uint32	スキャン中に検出されたサーバおよびオペレーティング システムを記述する汎用スキャン結果データ ブロックを開始します。この値は常に 108 です。
汎用スキャン結果ブロック長	uint32	汎用スキャン結果データ ブロックのバイト数(汎用スキャン結果ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン結果データのバイト数を含む)。
汎用スキャン結果データ	string	各スキャン結果に関する情報。
汎用リスト ブロック タイプ	uint32	サード パーティ アプリケーションからのホスト入力データを伝えるユーザ製品データ ブロックを構成する、汎用リスト データ ブロックを開始します。この値は常に 31 です。

表 B-18　スキャン結果データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのユーザ製品データ ブロックを含む)。
ユーザ製品データ ブロック*	変数	ホスト入力データを含むユーザ製品データ ブロック。このデータ ブロックの説明の詳細については、ユーザ製品データ ブロック 5.1+(4-177 ページ)を参照してください。

ユーザ製品データ ブロック 5.0.x

ユーザ製品データ ブロックは、サード パーティ アプリケーション文字列マッピングを含む、サード パーティ アプリケーションからインポートされたホスト入力データを伝えます。このデータ ブロックは、次の表では、6.1+ の接続統計データ ブロックのフィールドについて説明します。(4-131 ページ)で使用されます。ユーザ製品データ ブロックは、4.10.x の場合はブロック タイプ 65、5.0 ～ 5.0.x の場合はブロック タイプ 118 です。それぞれのブロック タイプは同じ構造を持ちます。

(注)　次の図で、データ ブロック名の横のアスタリスク(*)は、データ ブロックの複数のインスタンスが発生する可能性があることを示します。

次の図は、ユーザ製品データ ブロックの形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
カスタムベンダー文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	カスタム ベンダー文字列...																															
カスタム製品文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	カスタム製品文字列...																															
カスタムバージョン文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	カスタム バージョン文字列...																															
	ソフトウェア ID																															
	サーバ ID																															
	ベンダー ID																															
	製品 ID																															
メジャーバージョン文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	メジャー バージョン文字列...																															
マイナーバージョン文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	マイナー バージョン文字列...																															
リビジョン文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	リビジョン文字列…																															
移行先メジャー文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	移行先メジャー バージョン文字列...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
マイナー用文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	マイナー用バージョン文字列...																															
リビジョン用文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	リビジョン用文字列…																															
ビルド文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ビルド文字列…																															
パッチ文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	パッチ文字列…																															
内線番号文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	拡張文字列…																															
OS UUID	オペレーティング システム UUID																															
	オペレーティング システム UUID(続き)																															
	オペレーティング システム UUID(続き)																															
	オペレーティング システム UUID(続き)																															
修正のリスト	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	修正リスト データ ブロック*																															

次の表は、ユーザ製品データ ブロックのコンポーネントについての説明です。

表 B-19　ユーザ製品データ ブロック 4.10.x、5.0 ～ 5.0.x のフィールド

フィールド	データ タイプ	説明
ユーザ製品データ ブロック タイプ	uint32	ユーザ製品データ ブロックを開始します。この値はバージョン 4.10.x の場合は 65、バージョン 5.0 ～ 5.0.x の場合は 118 です。
ユーザ製品ブロック長	uint32	ユーザ製品データ ブロックのバイトの合計数(ユーザ製品ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ製品データのバイト数を含む)。
ソース ID	uint32	データをインポートした送信元の ID 番号。
ソース タイプ	uint32	データ提供ソースのソース タイプ。
汎用リスト ブロック タイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リスト データ ブロックのバイト数。
IP 範囲仕様データ ブロック*	変数	ユーザ入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データ ブロック。このデータ ブロックの説明の詳細については、5.2+の IP アドレス範囲データ ブロック (4-98 ページ) を参照してください。
ポート	uint16	ユーザが指定したポート。
プロトコル	uint16	ユーザが指定した IANA プロトコル数。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP
ドロップ ユーザ製品	uint32	ユーザ OS 定義がホストから削除されたかどうかを次のように示します。 • 0:いいえ • 1:はい
文字列ブロック タイプ	uint32	ユーザ入力で指定されたカスタム ベンダー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタム ベンダー文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびベンダー名のバイト数を含む)。
カスタム ベンダー名	string	ユーザ入力で指定されたカスタム ベンダー名。
文字列ブロック タイプ	uint32	ユーザ入力で指定されたカスタム製品名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタム製品文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、および製品名のバイト数を含む)。

表 B-19　ユーザ製品データ ブロック 4.10.x、5.0 ～ 5.0.x のフィールド(続き)

フィールド	データ タイプ	説明
カスタム製品名	string	ユーザ入力で指定されたカスタム製品名。
文字列ブロック タイプ	uint32	ユーザ入力で指定されたカスタム バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタム バージョン文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
カスタム バージョン	string	ユーザ入力で指定されたカスタム バージョン。
ソフトウェア ID	uint32	Cisco データベースの特定のリビジョンのサーバまたはオペレーティング システムの ID。
サーバ ID	uint32	ユーザ入力で指定されたホスト サーバ上のアプリケーション プロトコルの Cisco アプリケーション ID。
ベンダー ID	uint32	サード パーティ オペレーティング システムが Cisco 3D オペレーティング システム定義にマップされるときに指定される、サード パーティ オペレーティング システムのベンダーの ID。
製品 ID	uint32	サード パーティ オペレーティング システム文字列が Cisco 3D オペレーティング システム定義にマップされるときに指定される、サードパーティ オペレーティング システム文字列の製品 ID 文字列。
文字列ブロック タイプ	uint32	ユーザ入力内のサード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システム定義のメジャー バージョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	メジャー文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
メジャー バージョン	string	サード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システム定義のメジャー バージョン。
文字列ブロック タイプ	uint32	サード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システム定義のマイナー バージョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	マイナー文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
マイナー バージョン	string	ユーザ入力内のサード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システム定義のマイナー バージョン。
文字列ブロック タイプ	uint32	ユーザ入力内のサード パーティ オペレーティング システム文字列がマップされる Cisco オペレーティング システム定義のリビジョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-19　ユーザ製品データ ブロック 4.10.x、5.0 ～ 5.0.x のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	リビジョン文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびリビジョン番号のバイト数を含む)。
リビジョン	string	ユーザ入力内のサード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システム定義のリビジョン番号。
文字列ブロック タイプ	uint32	サード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システム定義の最終メジャー バージョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	メジャー用文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
移行先メジャー	string	ユーザ入力内のサード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システム定義のメジャー バージョン番号の範囲内にある、最終バージョン番号。
文字列ブロック タイプ	uint32	サード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システム定義の最終マイナー バージョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	マイナー用文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
マイナー用	string	ユーザ入力内のサード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システム定義のマイナー バージョン番号の範囲内にある、最終バージョン番号。
文字列ブロック タイプ	uint32	サード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システム定義の最終リビジョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	リビジョン用文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびリビジョン番号のバイト数を含む)。
リビジョン用	string	ユーザ入力内のサード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システム定義のリビジョン番号の範囲内にある、最終リビジョン番号。
文字列ブロック タイプ	uint32	サード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システムのビルド番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ビルド文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびビルド番号のバイト数を含む)。

表 B-19　ユーザ製品データ ブロック 4.10.x、5.0 ～ 5.0.x のフィールド(続き)

フィールド	データ タイプ	説明
ビルド	string	ユーザ入力内のサード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システムのビルド番号。
文字列ブロック タイプ	uint32	サード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システムのパッチ番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	パッチ文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびパッチ番号のバイト数を含む)。
パッチ	string	ユーザ入力内のサード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システムのパッチ番号。
文字列ブロック タイプ	uint32	サード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システムの拡張番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	拡張文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、および拡張番号のバイト数を含む)。
内線番号	string	ユーザ入力内のサード パーティ オペレーティング システム文字列がマップされる Cisco 3D オペレーティング システムの拡張番号。
UUID	uint8 [x16]	オペレーティング システム用の固有 ID 番号が含まれます。
汎用リスト ブロック タイプ	uint32	どの修正が特定の IP アドレス範囲内のホストに適用されているかに関するユーザ入力データを伝える修正リスト データ ブロックで構成される、汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべての修正リスト データ ブロックを含む)。
修正リスト データ ブロック*	変数	ホストに適用された修正に関する情報を含む修正リスト データ ブロック。このデータ ブロックの説明の詳細については、フィックス リスト データ ブロック(4-105 ページ)を参照してください。

レガシー ユーザ ログイン データ ブロック

詳細については、次の各項を参照してください。

- ユーザ ログイン情報データ ブロック 5.0 ～ 5.0.2(B-108 ページ)
- ユーザ ログイン情報データ ブロック 5.1 ～ 5.4.x(B-109 ページ)
- ユーザ ログイン情報データ ブロック 6.0.x(B-111 ページ)
- ユーザ情報データ ブロック 5.x(B-115 ページ)

ユーザ ログイン情報データ ブロック 5.0 ～ 5.0.2

ユーザ ログイン情報データ ブロックは、ユーザ情報更新メッセージで使用され、検出されたユーザのログイン情報の変更を伝えます。詳細については、ユーザ情報更新メッセージ ブロック (4-62 ページ)を参照してください。

ユーザ ログイン情報データ ブロックは、バージョン 5.0 ～ 5.0.2 の場合は、ブロック タイプ 121 です。

次の図は、ユーザ ログイン情報データ ブロックの形式を示しています。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ ログイン情報ブロック タイプ(121)																																
	ユーザ ログイン情報ブロック長																																
	タ イ ム ス タ ンプ																																
	IPアドレス																																
ユーザ名	文字列ブロック タイプ(0)																																
	文字列ブロック長																																
	ユーザ名...																																
	ユーザ ID																																
	アプリケーション ID																																
E メール	文字列ブロック タイプ(0)																																
	文字列ブロック長																																
	電子メール...																																

次の表は、ユーザ ログイン情報データ ブロックのコンポーネントについての説明です。

表 B-20　　ユーザ ログイン情報データ ブロック 5.0 ～ 5.0.2 のフィールド

フィールド	データ タイプ	説明
ユーザ ログイン情報ブロック タイプ	uint32	ユーザ ログイン情報データ ブロックを開始します。この値は、バージョン 5.0 ～ 5.0.2 の場合は 121 です。
ユーザ ログイン情報ブロック長	uint32	ユーザ ログイン情報データ ブロックのバイトの合計数(ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ ログイン情報データのバイト数を含む)。

表 B-20　ユーザ ログイン情報データ ブロック 5.0 ～ 5.0.2 のフィールド(続き)

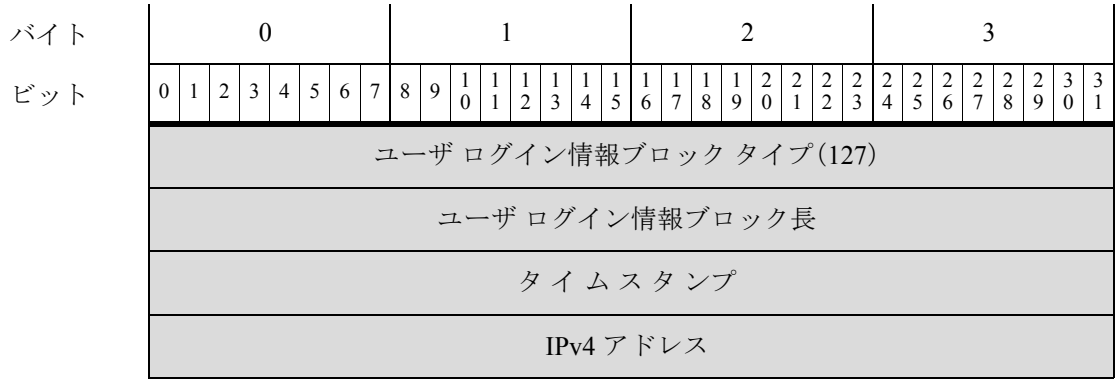
フィールド	データ タイプ	説明
タイムスタンプ	uint32	イベントのタイムスタンプ。
IPアドレス	uint8[4]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IP アドレス。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
ユーザ名	string	ユーザのユーザ名。
ユーザ ID	uint32	ユーザの ID 番号。
アプリケーション ID	uint32	ログイン情報の取得元の、接続に使用されたアプリケーション プロトコルのアプリケーション ID。
文字列ブロック タイプ	uint32	ユーザの電子メールアドレスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メール アドレスのバイト数を加えた電子メール アドレス文字列データ ブロックのバイト数。
E メール	string	ユーザの電子メール アドレス。

ユーザ ログイン情報データ ブロック 5.1 ～ 5.4.x

ユーザ ログイン情報データ ブロックは、ユーザ情報更新メッセージで使用され、検出されたユーザのログイン情報の変更を伝えます。詳細については、ユーザ アカウント更新メッセージ データ ブロック (4-186 ページ) を参照してください。

ユーザ ログイン情報データ ブロックは、バージョン 4.7 ～ 4.10.x の場合はブロック タイプ 73、バージョン 5.0 ～ 5.0.2 の場合はシリーズ 1 グループのブロックのブロック タイプ 121、バージョン 5.1 ～ 5.4.x の場合はシリーズ 1 グループのブロックのデータ タイプ 127 です。

次の図は、ユーザ ログイン情報データ ブロックの形式を示しています。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ユーザ名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ名...																															
	ユーザ ID																															
	アプリケーション ID																															
E メール	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール...																															
	IPv6アドレス IPv6 アドレス(続き) IPv6 アドレス(続き) IPv6 アドレス(続き)																															
レポート基準	ログイン タイプ								文字列ブロック タイプ(0)																							
	文字列ブロック タイプ(0)(続き)								文字列ブロック長																							
	文字列ブロック長								レポート基準...																							

次の表は、ユーザ ログイン情報データ ブロックのコンポーネントについての説明です。

表 B-21　　ユーザ ログイン情報データ ブロックのフィールド

フィールド	データ タイプ	説明
ユーザ ログイン情報ブロック タイプ	uint32	ユーザ ログイン情報データ ブロックを開始します。この値は、バージョン 5.1+ の場合は 127 です。
ユーザ ログイン情報ブロック長	uint32	ユーザ ログイン情報データ ブロックのバイトの合計数(ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ ログイン情報データのバイト数を含む)。
タイムスタンプ	uint32	イベントのタイムスタンプ。

表 B-21　ユーザ ログイン情報データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
IPv4 アドレス	uint32	このフィールドは予約済みですが、設定されておりません。IPv4 アドレスは IPv6 アドレス フィールドに保存されます。詳細については、IP アドレス(1-6 ページ)を参照してください。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
ユーザ名	string	ユーザのユーザ名。
ユーザ ID	uint32	ユーザの ID 番号。
アプリケーション ID	uint32	ログイン情報の取得元の、接続に使用されたアプリケーション プロトコルのアプリケーション ID。
文字列ブロック タイプ	uint32	ユーザの電子メールアドレスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メール アドレスのバイト数を加えた電子メール アドレス文字列データ ブロックのバイト数。
E メール	string	ユーザの電子メール アドレス。
IPv6アドレス	uint8[16]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IPv6 アドレス。
ログイン タイプ	uint8	検出されたユーザ ログインのタイプ。
文字列ブロック タイプ	uint32	レポート基準値を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	レポート基準文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびレポート基準フィールドのバイト数を含む)。
レポート基準	string	ログインをレポートする Active Directory サーバの名前。

ユーザ ログイン情報データ ブロック 6.0.x

ユーザ ログイン情報データ ブロックは、ユーザ情報更新メッセージで使用され、検出されたユーザのログイン情報の変更を伝えます。詳細については、ユーザ アカウント更新メッセージ データ ブロック(4-186 ページ)を参照してください。

ユーザ ログイン情報データ ブロックは、バージョン 6.0.x の場合は、ブロック タイプ 159 です。これには新しい ISE 統合エンドポイント プロファイル、セキュリティ インテリジェンスのフィールドがあります。

ユーザ ログイン情報データ ブロックは、バージョン 4.7 ～ 4.10.x の場合はブロック タイプ 73、バージョン 5.0 ～ 5.0.2 の場合はシリーズ 1 グループのブロックのブロック タイプ 121、バージョン 5.1+ の場合はシリーズ 1 グループのブロックのデータ タイプ 127 です。詳細については、ユーザ ログイン情報データ ブロック 5.1 ～ 5.4.x(B-109 ページ)を参照してください。

次の図は、ユーザ ログイン情報データ ブロックの形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ ログイン情報ブロック タイプ(159)																															
	ユーザ ログイン情報ブロック長																															
	タ イ ム ス タ ンプ																															
	IPv4 アドレス																															
ユーザ名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ名...																															
ドメイン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ドメイン...																															
	ユーザ ID																															
	レルム ID																															
	エンドポイント プロファイル ID																															
	セキュリティ グループ ID																															
	アプリケーション ID																															
	プロトコル																															
E メール	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール...																															
	IPv6アドレス IPv6 アドレス(続き) IPv6 アドレス(続き) IPv6 アドレス(続き)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ロケーション IPv6 アドレス ロケーション IPv6 アドレス（続き） ロケーション IPv6 アドレス（続き） ロケーション IPv6 アドレス（続き）																															
レポート基準	ログイン タイプ								承認タイプ								文字列ブロック タイプ（0）															
	文字列ブロック タイプ（0）（続き）																文字列ブロック長															
	文字列ブロック長（続き）																レポート基準...															

次の表は、ユーザ ログイン情報データ ブロックのコンポーネントについての説明です。

表 B-22　　ユーザ ログイン情報データ ブロックのフィールド

フィールド	データ タイプ	説明
ユーザ ログイン情報ブロック タイプ	uint32	ユーザ ログイン情報データ ブロックを開始します。この値は、バージョン 6.0.x の場合は 159 です。
ユーザ ログイン情報ブロック長	uint32	ユーザ ログイン情報データ ブロックのバイトの合計数（ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ ログイン情報データのバイト数を含む）。
タイムスタンプ	uint32	イベントのタイムスタンプ。
IPv4 アドレス	uint32	このフィールドは予約済みですが、設定されておりません。IPv4 アドレスは IPv6 アドレス フィールドに保存されます。詳細については、IP アドレス（1-6 ページ）を参照してください。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数（ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む）。
ユーザ名	string	ユーザのユーザ名。
文字列ブロック タイプ	uint32	ドメインを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにドメインのバイト数を加えたユーザ名文字列データ ブロックのバイト数。
ドメイン	string	ユーザがログインしているドメイン。
ユーザ ID	uint32	ユーザの ID 番号。

表 B-22　ユーザ ログイン情報データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
レルム ID	uint32	アイデンティティ レルムに対応する整数 ID。
エンドポイント プロファイル ID	uint32	接続エンドポイントが使用するデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
セキュリティ グループ ID	uint32	ネットワーク トラフィック グループの ID 番号。
アプリケーション ID	uint32	ログイン情報の取得元の、接続に使用されたアプリケーション プロトコルのアプリケーション ID。
プロトコル	uint32	ユーザの検出やレポートに使用するプロトコル。値は以下のとおりです。 • 165?FTP • 426?SIP • 547?AOL Instant Messenger • 683:IMAP • 710:LDAP • 767?NTP • 773:Oracle データベース • 788:POP3 • 1755:MDNS
文字列ブロック タイプ	uint32	ユーザの電子メールアドレスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メール アドレスのバイト数を加えた電子メール アドレス文字列データ ブロックのバイト数。
E メール	string	ユーザの電子メール アドレス。
IPv6アドレス	uint8[16]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IPv6 アドレス。
ロケーション IPv6 アドレス	uint8[16]	ユーザがログインした最新の IP アドレス。IPv4 または IPv6 のどちらかのアドレスになります。
ログイン タイプ	uint8	検出されたユーザ ログインのタイプ。
認証タイプ	uint8	ユーザが使用する認証のタイプ。値は次のとおりです。 • 0:認証は不要 • 1:パッシブ認証、AD エージェント、または ISE セッション • 2:キャプティブ ポータルの正常な認証 • 3:キャプティブ ポータルのゲスト認証 • 4:キャプティブ ポータルの失敗認証
文字列ブロック タイプ	uint32	レポート基準値を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-22　ユーザ ログイン情報データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	レポート基準文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびレポート基準フィールドのバイト数を含む)。
レポート基準	string	ログインをレポートする Active Directory サーバの名前。

ユーザ情報データ ブロック 5.x

ユーザ情報データ ブロックはユーザ変更メッセージで使用され、検出、削除、またはドロップされたユーザの情報を伝えます。詳細については、ユーザ変更メッセージ(4-62 ページ)を参照してください。

ユーザ情報データ ブロックのブロック タイプは、4.7 ～ 4.10.x のシリーズ 1 ブロック グループのブロック タイプ 75 と、5.x のシリーズ 1 ブロック グループのブロック タイプ 120 です。構成は、ブロック タイプ 75 と 120 で同じです。

次の図は、ユーザ情報データ ブロックの形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ情報ブロック タイプ(75 | 120)																															
	ユーザ情報ブロック長																															
	ユーザ ID																															
ユーザ名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ名...																															
	プロトコル																															
名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	名...																															
姓	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	姓...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
E メール	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール...																															
部署名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	部署名...																															
電話	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電話...																															

次の表は、ユーザ情報データ ブロックのコンポーネントについての説明です。

表 B-23　　ユーザ情報データ ブロックのフィールド

フィールド	データ タイプ	説明
ユーザ情報ブロック タイプ	uint32	ユーザ情報データ ブロックを開始します。この値は、バージョン 4.7 ～ 4.10.x の場合は 75、5.0+ の場合は 120 です。
ユーザ情報ブロック長	uint32	ユーザ情報データ ブロックのバイトの合計数(ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ情報データのバイト数を含む)。
ユーザ ID	uint32	ユーザの ID 番号。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
ユーザ名	string	ユーザのユーザ名。
プロトコル	uint32	ユーザ情報を含むパケットのプロトコル。
文字列ブロック タイプ	uint32	ユーザの名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、および名のバイト数を含む)。
名	string	ユーザの名前。
文字列ブロック タイプ	uint32	ユーザの姓を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-23　ユーザ情報データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	姓文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、および姓のバイト数を含む)。
姓	string	ユーザの姓。
文字列ブロック タイプ	uint32	ユーザの電子メールアドレスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メール アドレスのバイト数を加えた電子メール アドレス文字列データ ブロックのバイト数。
E メール	string	ユーザの電子メール アドレス。
文字列ブロック タイプ	uint32	ユーザの部署を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	部署文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、および部署のバイト数を含む)。
部署名	string	ユーザの部署名。
文字列ブロック タイプ	uint32	ユーザの電話番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電話番号のバイト数を加えた電話番号文字列データ ブロックのバイト数。
電話	string	ユーザの電話番号。

レガシー ホスト プロファイル データ ブロック

詳細については、次の各項を参照してください。

- ホスト プロファイル データ ブロック 5.0 ～ 5.0.2(B-117 ページ)

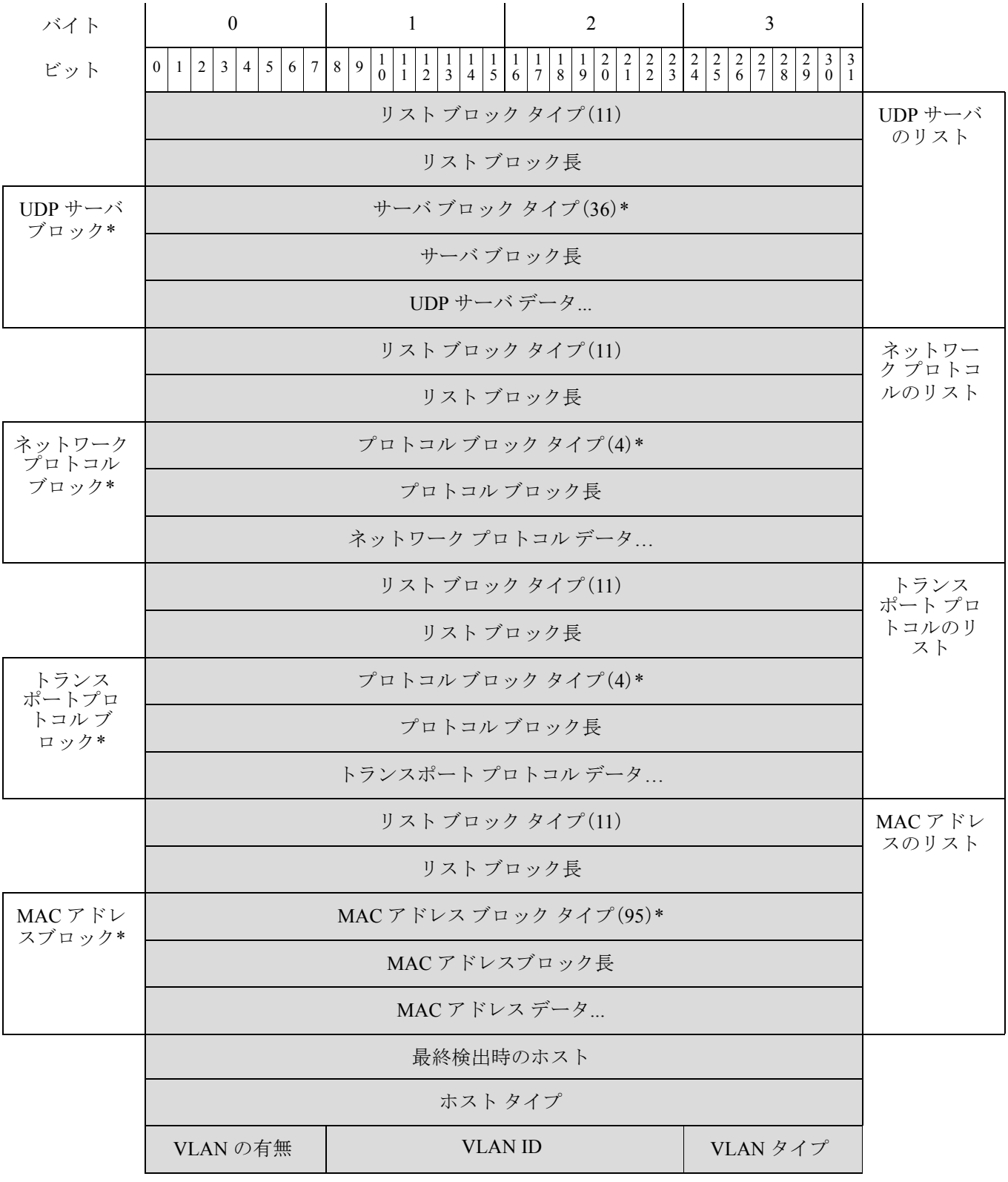
ホスト プロファイル データ ブロック 5.0 ～ 5.0.2

次の図は、ホスト プロファイル データ ブロックのバージョン 5.0 ～ 5.0.2 の形式を示しています。さらに、ホスト プロファイル データ ブロックには、ホスト重要度値が含まれていませんが、VLAN のプレゼンス インジケータは含まれています。さらに、ホスト プロファイル データ ブロックは、ホストの NetBIOS 名を伝えることができます。ホスト プロファイル データ ブロックのブロック タイプは 91 です。

(注)　次の図のブロック タイプ フィールドの横のアスタリスク(*)は、メッセージにシリーズ 1 データ ブロックのゼロ以上のインスタンスが含まれる可能性があることを示しています。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ホスト プロファイル ブロック タイプ(91)																																
	ホスト プロファイル ブロック長																																
	IPアドレス																																
サーバ フィンガープリント	ホップ									プライマリ/セカンダリ								汎用リスト ブロック タイプ(31)															
	汎用リスト ブロック タイプ(続き)																	汎用リスト ブロック長															
	汎用リスト ブロック長(続き)																	サーバ フィンガープリント データ ブロック*															
クライアント フィンガープリント	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
	クライアント フィンガープリント データ ブロック*																																
SMB フィンガープリント	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
	SMB フィンガープリント データ ブロック*																																
DHCP フィンガープリント	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
	DHCP フィンガープリント データ ブロック*																																
	リスト ブロック タイプ(11)																																
	リスト ブロック長																																
TCP サーバ ブロック*	サーバ ブロック タイプ(36)																																
	サーバ ブロック長																																
	TCP サーバ データ...																																

TCP サーバのリスト


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
リスト ブロック タイプ(11)
リスト ブロック長
UDP サーバ ブロック*
サーバ ブロック タイプ(36)*
サーバ ブロック長
UDP サーバ データ...
UDP サーバのリスト
リスト ブロック タイプ(11)
リスト ブロック長
ネットワーク プロトコル ブロック*
プロトコル ブロック タイプ(4)*
プロトコル ブロック長
ネットワーク プロトコル データ…
ネットワーク プロトコルのリスト
リスト ブロック タイプ(11)
リスト ブロック長
トランスポートプロトコル ブロック*
プロトコル ブロック タイプ(4)*
プロトコル ブロック長
トランスポート プロトコル データ…
トランスポート プロトコルのリスト
リスト ブロック タイプ(11)
リスト ブロック長
MAC アドレスブロック*
MAC アドレス ブロック タイプ(95)*
MAC アドレスブロック長
MAC アドレス データ...
MAC アドレスのリスト
最終検出時のホスト
ホスト タイプ
VLAN の有無
VLAN ID
VLAN タイプ

次の表は、バージョン 4.9 ～ 5.0.2 により返されるホスト プロファイル データ ブロックのフィールドについての説明です。

表 B-24　　ホスト プロファイル データ ブロック 5.0 ～ 5.0.2 のフィールド

フィールド	データ タイプ	説明
ホスト プロファイル ブロック タイプ	uint32	ホスト プロファイル データ ブロック 4.9 ～ 5.0.2 を開始します。このデータ ブロックのブロック タイプは 91 です。
ホスト プロファイル ブロック長	uint32	ホスト プロファイル データ ブロックのバイト数(ホスト プロファイル ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くホスト プロファイル データに含まれるバイト数を含む)。
IPアドレス	uint8[4]	IP アドレス オクテットの、プロファイルに記述されているホストの IP アドレス。
ホップ	uint8	ホストからのデバイスまでのホップ数。
プライマリ/セカンダリ	uint8	ホストがそれを検出したデバイスのプライマリまたはセカンダリのどちらのネットワークにあるかを示します。 • 0:ホストはプライマリ ネットワークにあります。 • 1:ホストはセカンダリ ネットワークにあります。

表 B-24　ホスト プロファイル データ ブロック 5.0 ～ 5.0.2 のフィールド(続き)

フィールド	データ タイプ	説明
汎用リスト ブロック タイプ	uint32	サーバ フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(サーバ フィンガープリント)データ ブロック*	変数	サーバ フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.0 ～ 5.0.2 (B-125 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	クライアント フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(クライアント フィンガープリント)データ ブロック*	変数	クライアント フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.0 ～ 5.0.2 (B-125 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	SMB フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(SMB フィンガープリント)データ ブロック*	変数	SMB フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.0 ～ 5.0.2 (B-125 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	DHCP フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。

表 B-24　ホスト プロファイル データ ブロック 5.0 ～ 5.0.2 のフィールド(続き)

フィールド	データ タイプ	説明
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(DHCP フィンガープリント)データ ブロック*	変数	DHCP フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.0 ～ 5.0.2 (B-125 ページ)を参照してください。
リスト ブロック タイプ	uint32	TCP サーバ データを伝えるサーバ データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのサーバ データ ブロックが含まれています。 このフィールドには、ゼロ以上のサーバ データ ブロックが続きます。
サーバ ブロック タイプ	uint32	サーバ データ ブロックを開始します。この値は常に 89 です。
サーバ ブロック長	uint32	サーバ データ ブロックのバイト数(サーバ ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く TCP サーバ データのバイト数を含む)。
TCP サーバ データ	変数	TCP サーバを記述するデータ フィールド(旧バージョンの製品で説明)。
リスト ブロック タイプ	uint32	UDP サーバ データを伝えるサーバ データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのサーバ データ ブロックが含まれています。 このフィールドには、ゼロ以上のサーバ データ ブロックが続きます。
サーバ ブロック タイプ	uint32	UDP サーバを記述するサーバ データ ブロックを開始します。この値は常に 89 です。
サーバ ブロック長	uint32	サーバ データ ブロックのバイト数(サーバ ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く UDP サーバ データのバイト数を含む)。
UDP サーバ データ	変数	UDP サーバを記述するデータ フィールド(旧バージョンの製品で説明)。
リスト ブロック タイプ	uint32	ネットワーク プロトコル データを伝えるプロトコル データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。

表 B-24　ホスト プロファイル データ ブロック 5.0 ～ 5.0.2 のフィールド(続き)

フィールド	データ タイプ	説明
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのプロトコル データ ブロックが含まれています。 このフィールドには、ゼロ以上のプロトコル データ ブロックが続きます。
プロトコル ブロック タイプ	uint32	ネットワーク プロトコルを記述するプロトコル データ ブロックを開始します。この値は常に 4 です。
プロトコル ブロック長	uint32	プロトコル データ ブロックのバイト数(プロトコル ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くプロトコル データのバイト数を含む)。
ネットワーク プロトコル データ	uint16	ネットワーク プロトコル数が含まれるデータ フィールド(プロトコル データ ブロック (4-78 ページ) で説明)。
リスト ブロック タイプ	uint32	トランスポート プロトコル データを伝えるプロトコル データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのプロトコル データ ブロックが含まれています。 このフィールドには、ゼロ以上のトランスポート プロトコル データ ブロックが続きます。
プロトコル ブロック タイプ	uint32	トランスポート プロトコルを記述するプロトコル データ ブロックを開始します。この値は常に 4 です。
プロトコル ブロック長	uint32	プロトコル データ ブロックのバイト数(プロトコル ブロック タイプと長さ用の 8 バイト、およびそれに続くプロトコル データのバイト数を含む)。
トランスポート プロトコル データ	変数	トランスポート プロトコル数が含まれるデータ フィールド (プロトコル データ ブロック (4-78 ページ) で説明)。
リスト ブロック タイプ	uint32	MAC アドレス データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リストのバイト数(リスト ヘッダーと、カプセル化されたすべての MAC アドレス データ ブロックを含む)。
ホスト MAC アドレス ブロック タイプ	uint32	ホスト MAC アドレス データ ブロックを開始します。この値は常に 95 です。
ホスト MAC アドレス ブロック長	uint32	ホスト MAC アドレス データ ブロックのバイト数(ホスト MAC アドレス ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くホスト MAC アドレス データのバイト数を含む)。
ホスト MAC アドレス データ	変数	ホスト MAC アドレス データ フィールド(ホスト MAC アドレス 4.9+ (4-119 ページ) で説明)。
最終検出時のホスト	uint32	システムがホストのアクティビティを検出した最終時刻を表す UNIX タイムスタンプ。

表 B-24　ホスト プロファイル データ ブロック 5.0 ～ 5.0.2 のフィールド(続き)

フィールド	データ タイプ	説明
ホスト タイプ	uint32	ホストのタイプを示します。表示される可能性がある値は次のとおりです。 • 0:ホスト • 1:ルータ • 2:ブリッジ • 3:NAT デバイス • 4:LB(ロード バランサ)
VLAN の有無	uint8	VLAN が存在するかどうかを示します。 • 0:はい • 1:いいえ
VLAN ID	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグにカプセル化されたパケットのタイプ。
VLAN 優先順位	uint8	VLAN タグに含まれる優先順位値。
汎用リスト ブロック タイプ	uint32	クライアント アプリケーション データを伝えるクライアント アプリケーション データ ブロックで構成される汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのクライアント アプリケーション データ ブロックを含む)。
クライアント アプリケーション ブロック タイプ	uint32	クライアント アプリケーション ブロックを開始します。この値は常に 5 です。
クライアント アプリケーション ブロック長	uint32	クライアント アプリケーション ブロックのバイト数(クライアント アプリケーション ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くクライアント アプリケーション データのバイト数を含む)。
クライアント アプリケーション データ	変数	クライアント アプリケーションを記述するクライアント アプリケーション データ フィールド(5.0+ のホスト クライアント アプリケーション データ ブロック (4-161 ページ) で説明)。
文字列ブロック タイプ	uint32	NetBIOS 名の文字列データ ブロックを開始します。この値は文字列データを示す 0 に設定されます。
文字列ブロック長	uint32	NetBIOS 名データ ブロックのバイト数を示します(文字列ブロック タイプと長さのフィールド用の 8 バイト、および NetBIOS 名のバイト数を含む)。
NetBIOS 文字列データ	変数	ホスト プロファイルに記述されているホストの NetBIOS 名が含まれます。

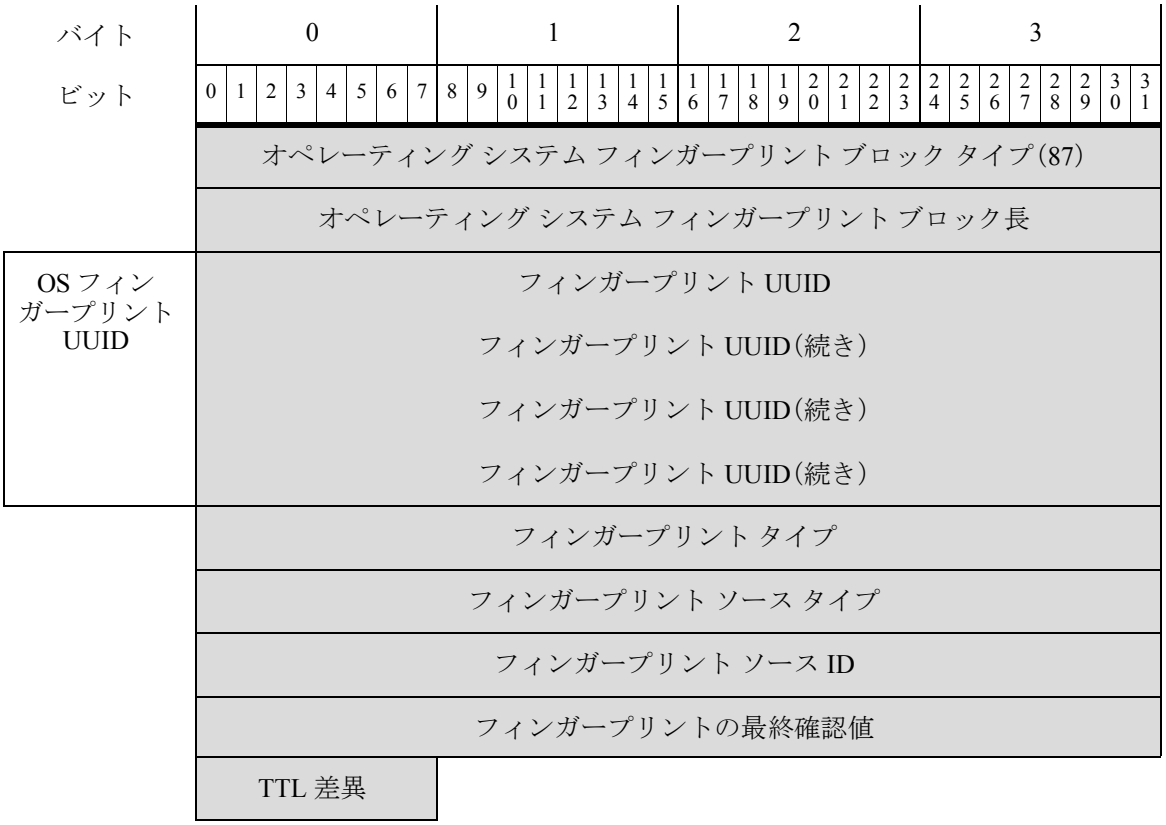
レガシー OS フィンガープリント データ ブロック

詳細については、次の各項を参照してください。

- オペレーティング システム フィンガープリント データ ブロック 5.0 ～ 5.0.2（B-125 ページ）

オペレーティング システム フィンガープリント データ ブロック 5.0 ～ 5.0.2

オペレーティング システム フィンガープリント データ ブロックのブロック タイプは 87 です。このブロックには、フィンガープリント Universally Unique Identifier（UUID）の他、フィンガープリント タイプ、フィンガープリント送信元タイプ、フィンガープリント送信元 ID を格納します。次の図は、オペレーティング システム フィンガープリント データ ブロックのバージョン 5.0 ～ 5.0.2 の形式を示しています。



次の表は、オペレーティング システム フィンガープリント データ ブロックのフィールドについての説明です。

表 B-25　オペレーティング システム フィンガープリント データ ブロックのフィールド

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント データ ブロック タイプ	uint32	オペレーティング システム データ ブロックを開始します。この値は常に 87 です。
オペレーティング システム データ ブロック長	uint32	オペレーティング システム フィンガープリント データ ブロックのバイト数。この値は常に 41 です。データ ブロック タイプと長さのフィールド用の 8 バイト、フィンガープリント UUID 値用の 16 バイト、フィンガープリントのタイプ用の 4 バイト、フィンガープリント ソースのタイプ用の 4 バイト、フィンガープリント ソース ID 用の 4 バイト、最終確認値用の 4 バイト、および TTL 差異用の 1 バイトです。
フィンガープリント UUID	uint8[16]	オペレーティング システムの固有識別子として機能するフィンガープリントID 番号（オクテット）。フィンガープリント UUID は、脆弱性データベース（VDB）内のオペレーティング システム名、ベンダー、およびバージョンにマップされます。
フィンガープリント タイプ	uint32	フィンガープリントのタイプを示します。
フィンガープリント ソース タイプ	uint32	オペレーティング システム フィンガープリントを提供した送信元のタイプ（ユーザまたはスキャナなど）を示します。
フィンガープリント ソース ID	uint32	オペレーティング システム フィンガープリントを提供した送信元の ID を示します。
最後の確認日時	uint32	トラフィック内でフィンガープリントが最後に検出された時を示します。
TTL 差異	uint8	フィンガープリントの TTL 値と、ホストのフィンガープリント取得に使用したパケットに表示される TTL 値との間の差異を示します。

レガシー接続データ構造

詳細については、次の項を参照してください。

接続統計データ ブロック 5.0 ～ 5.0.2

接続統計データ ブロックは、接続データ メッセージで使用されます。接続統計データ ブロック バージョン 5.0 ～ 5.0.2 のブロック タイプは 115 です。

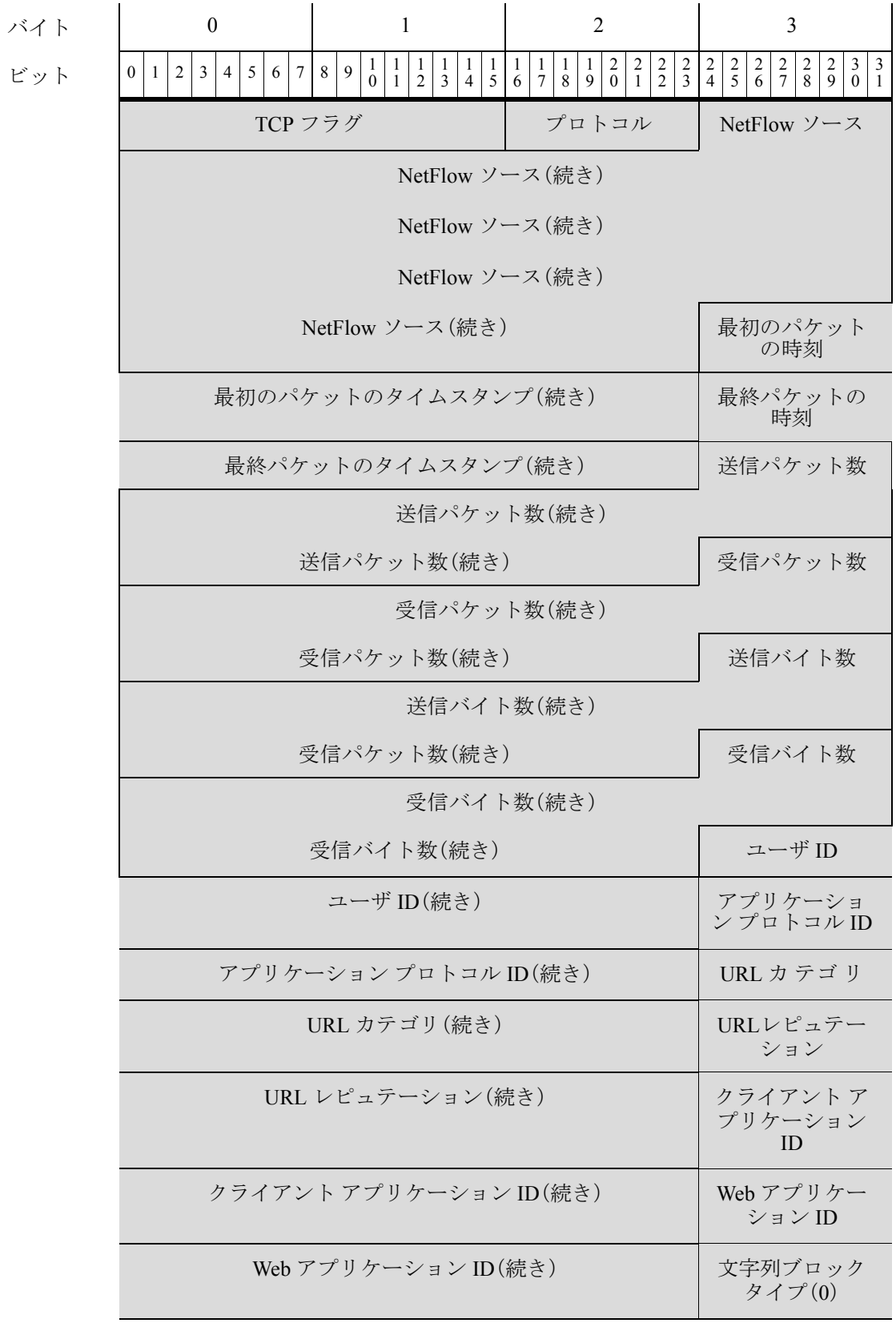
接続統計データ メッセージの詳細については、接続統計データ メッセージ（4-54 ページ）を参照してください。

次の図は、接続統計データ ブロック 5.0 ～ 5.0.2 の形式を示しています。

::

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続データ ブロック タイプ（115）																																
接続データ ブロック長																																
デバイス ID																																
入力ゾーン 入力ゾーン（続き） 入力ゾーン（続き） 入力ゾーン（続き）																																
出力ゾーン 出力ゾーン（続き）																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出力ゾーン(続き)																																
出力ゾーン(続き)																																
入力インターフェイス																																
入力インターフェイス(続き)																																
入力インターフェイス(続き)																																
入力インターフェイス(続き)																																
出力インターフェイス																																
出力インターフェイス(続き)																																
出力インターフェイス(続き)																																
出力インターフェイス(続き)																																
イニシエータ IP アドレス																																
イニシエータ IP アドレス(続き)																																
イニシエータ IP アドレス(続き)																																
イニシエータ IP アドレス(続き)																																
レスポンダ IP アドレス																																
レスポンダ IP アドレス(続き)																																
レスポンダ IP アドレス(続き)																																
レスポンダ IP アドレス(続き)																																
ポリシー リビジョン																																
ポリシー リビジョン(続き)																																
ポリシー リビジョン(続き)																																
ポリシー リビジョン(続き)																																
ルール ID																																
ルール アクション																																
イニシエータ ポート																	レスポンダ ポート															


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
TCP フラグ
プロトコル
NetFlow ソース
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
最初のパケットの時刻
最初のパケットのタイムスタンプ(続き)
最終パケットの時刻
最終パケットのタイムスタンプ(続き)
送信パケット数
送信パケット数(続き)
送信パケット数(続き)
受信パケット数
受信パケット数(続き)
受信パケット数(続き)
送信バイト数
送信バイト数(続き)
受信パケット数(続き)
受信バイト数
受信バイト数(続き)
受信バイト数(続き)
ユーザ ID
ユーザ ID(続き)
アプリケーション プロトコル ID
アプリケーション プロトコル ID(続き)
URL カテゴリ
URL カテゴリ(続き)
URL レピュテーション
URL レピュテーション(続き)
クライアント アプリケーション ID
クライアント アプリケーション ID(続き)
Web アプリケーション ID
Web アプリケーション ID(続き)
文字列ブロック タイプ(0)

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
クライアント アプリケーション URL	文字列ブロック タイプ(続き)																								文字列ブロック長							
	文字列ブロック長(続き)																								クライアント アプリケーション URL...							
NetBIOS 名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	NetBIOS 名...																															
クライアント アプリケーション バージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	クライアント アプリケーション バージョン...																															

次の表は、接続統計データ ブロック 5.0 ～ 5.0.2 のフィールドについての説明です。

表 B-26　　接続統計データ ブロック 5.0 ～ 5.0.2 のフィールド

フィールド	データ タイプ	説明
接続統計データ ブロック タイプ	uint32	接続統計データ ブロック 5.0 ～ 5.0.2 を開始します。値は常に 115 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティ ゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティ ゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポンダ IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた相関イベントに関連付けられているルールのリビジョン番号(該当する場合)。

表 B-26　接続統計データ ブロック 5.0 ～ 5.0.2 のフィールド(続き)

フィールド	データ タイプ	説明
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アクション	uint32	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポンダ ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス
最初のパケット タイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケット タイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
送信パケット数	uint64	開始ホストからの送信パケット数。
受信パケット数	uint64	応答ホストが送信したパケット数。
送信バイト数	uint64	開始ホストからの送信バイト数。
受信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URLレピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロック タイプ	uint32	クライアント アプリケーション URL の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション URL の文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、およびクライアント アプリケーション URL 文字列のバイト数を含む)。

表 B-26　接続統計データ ブロック 5.0 ～ 5.0.2 のフィールド(続き)

フィールド	データ タイプ	説明
クライアント アプリケーション URL	string	クライアント アプリケーションがアクセスする URL(該当する場合)(`/files/index.html` など)。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション バージョンの文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
クライアント アプリケーション バージョン	string	クライアント アプリケーション バージョン。

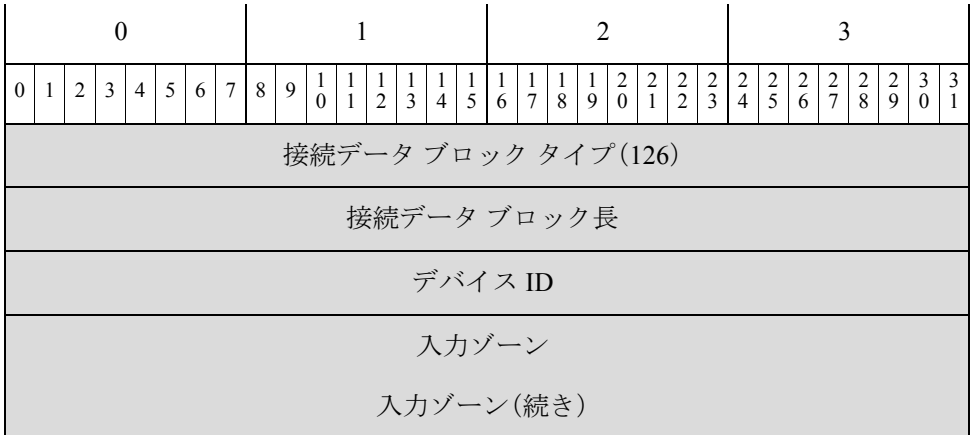
接続統計データ ブロック 5.1

接続統計データ ブロックは、接続データ メッセージで使用されます。バージョン 5.0.2 と 5.1 の間に加えられた接続データ ブロックの変更には、5.1 で導入された設定パラメータ(ルール アクション理由、モニタ ルール、セキュリティ インテリジェンス送信元/宛先、セキュリティ インテリジェンス レイヤ)が指定される新規フィールドの追加が含まれます。接続統計データ ブロック バージョン 5.1 のブロック タイプは 126 です。

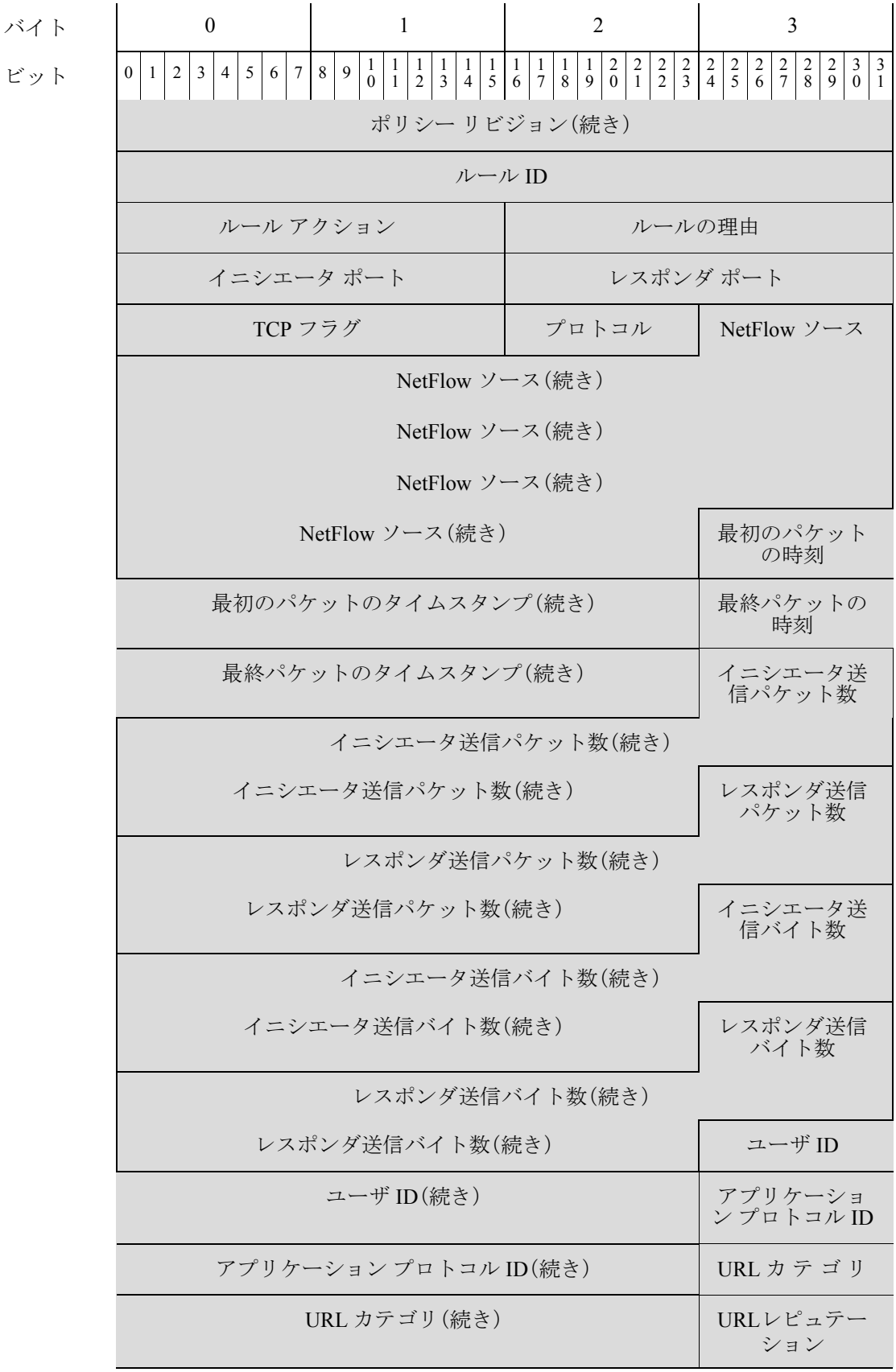
接続統計データ メッセージの詳細については、接続統計データ メッセージ(4-54 ページ)を参照してください。

次の図は、接続統計データ ブロック 5.1 の形式を示しています。

::



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
入力ゾーン（続き）																																
入力ゾーン（続き）																																
出力ゾーン																																
出力ゾーン（続き）																																
出力ゾーン（続き）																																
出力ゾーン（続き）																																
入力インターフェイス																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
出力インターフェイス																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
イニシエータ IP アドレス																																
イニシエータ IP アドレス（続き）																																
イニシエータ IP アドレス（続き）																																
イニシエータ IP アドレス（続き）																																
レスポンダ IP アドレス																																
レスポンダ IP アドレス（続き）																																
レスポンダ IP アドレス（続き）																																
レスポンダ IP アドレス（続き）																																
ポリシー リビジョン																																
ポリシー リビジョン（続き）																																
ポリシー リビジョン（続き）																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
ポリシー リビジョン(続き)
ルール ID
ルール アクション
ルールの理由
イニシエータ ポート
レスポンダ ポート
TCP フラグ
プロトコル
NetFlow ソース
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
最初のパケットの時刻
最初のパケットのタイムスタンプ(続き)
最終パケットの時刻
最終パケットのタイムスタンプ(続き)
イニシエータ送信パケット数
イニシエータ送信パケット数(続き)
イニシエータ送信パケット数(続き)
レスポンダ送信パケット数
レスポンダ送信パケット数(続き)
レスポンダ送信パケット数(続き)
イニシエータ送信バイト数
イニシエータ送信バイト数(続き)
イニシエータ送信バイト数(続き)
レスポンダ送信バイト数
レスポンダ送信バイト数(続き)
レスポンダ送信バイト数(続き)
ユーザ ID
ユーザ ID(続き)
アプリケーション プロトコル ID
アプリケーション プロトコル ID(続き)
URL カテゴリ
URL カテゴリ(続き)
URL レピュテーション

次の表は、接続統計データ ブロック 5.1 のフィールドについての説明です。

表 B-27　接続統計データ ブロック 5.1 のフィールド

フィールド	データ タイプ	説明
接続統計データ ブロック タイプ	uint32	接続統計データ ブロック 5.1 を開始します。値は常に 126 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティ ゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティ ゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポンダ IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた相関イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アクション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポンダ ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
最初のパケット タイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケット タイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポンダ送信パケット数	uint64	応答ホストが送信したパケット数。

表 B-27　接続統計データ ブロック 5.1 のフィールド(続き)

フィールド	データ タイプ	説明
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポンダ送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URLレピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロック タイプ	uint32	クライアント アプリケーション URL の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション URL の文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、およびクライアント アプリケーション URL 文字列のバイト数を含む)。
クライアント アプリケーション URL	string	クライアント アプリケーションがアクセスする URL(該当する場合) (`/files/index.html` など)。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション バージョンの文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
クライアント アプリケーション バージョン	string	クライアント アプリケーション バージョン。
モニタ ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタ ルールの ID。

表 B-27　接続統計データ ブロック 5.1 のフィールド（続き）

フィールド	データ タイプ	説明
モニタ ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタ ルールの ID。
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス層	uint8	IP ブラックリストに一致した IP 層。

接続統計データ ブロック 5.2.x

接続統計データ ブロックは、接続データ メッセージで使用されます。バージョン 5.1.1 と 5.2 の間に加えられた接続データ ブロックの変更には、地理位置情報をサポートするための新規フィールドの追加が含まれます。バージョン 5.2.x の接続統計データ ブロックは、シリーズ 1 グループのブロックの、ブロック タイプ 144 です。これにより、ブロック タイプ 137（接続統計データ ブロック 5.1.1.x（B-148 ページ））は廃止されます。

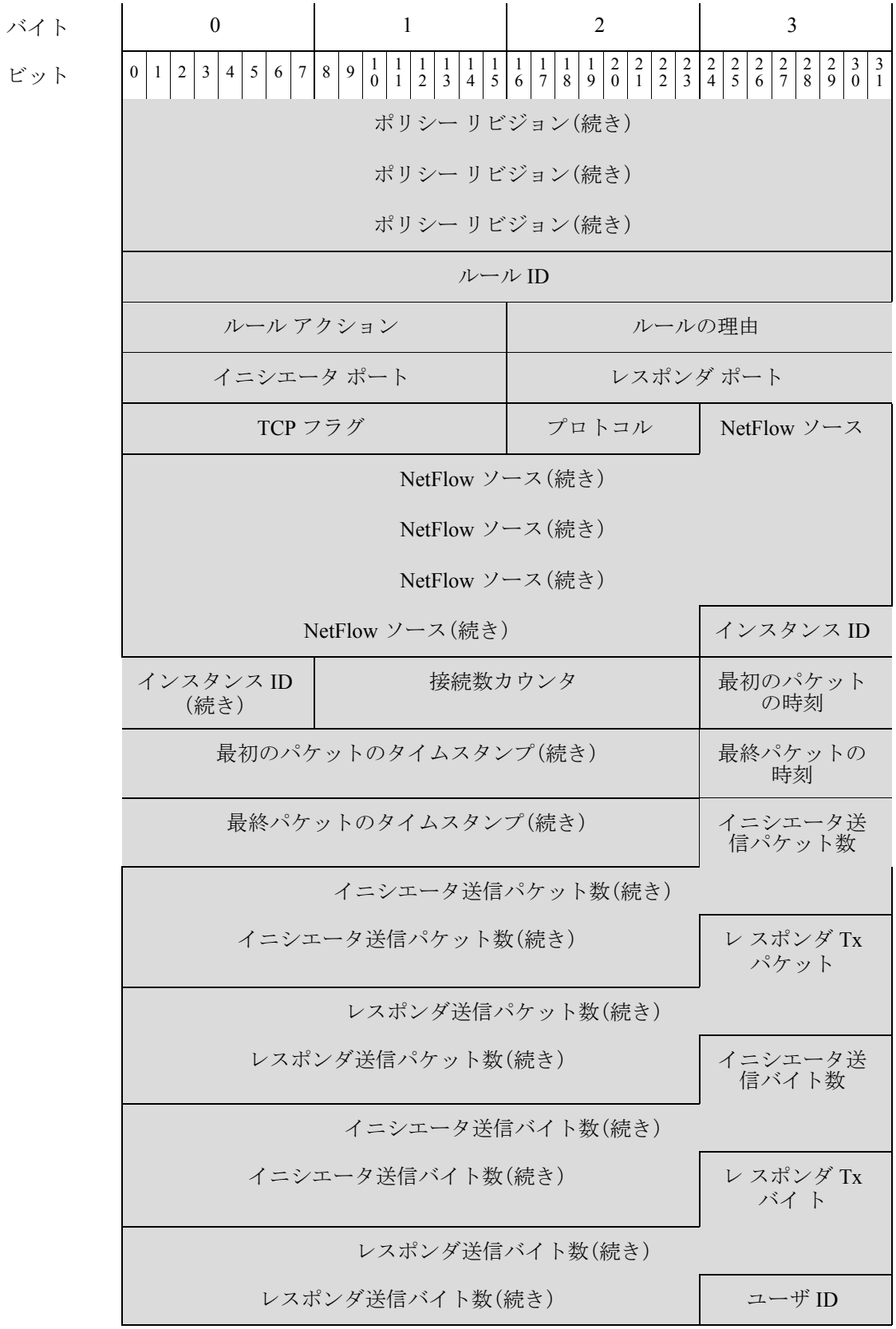
接続統計データ メッセージの詳細については、接続統計データ メッセージ（4-54 ページ）を参照してください。

次の図は、接続統計データ ブロック 5.2.x の形式を示しています。

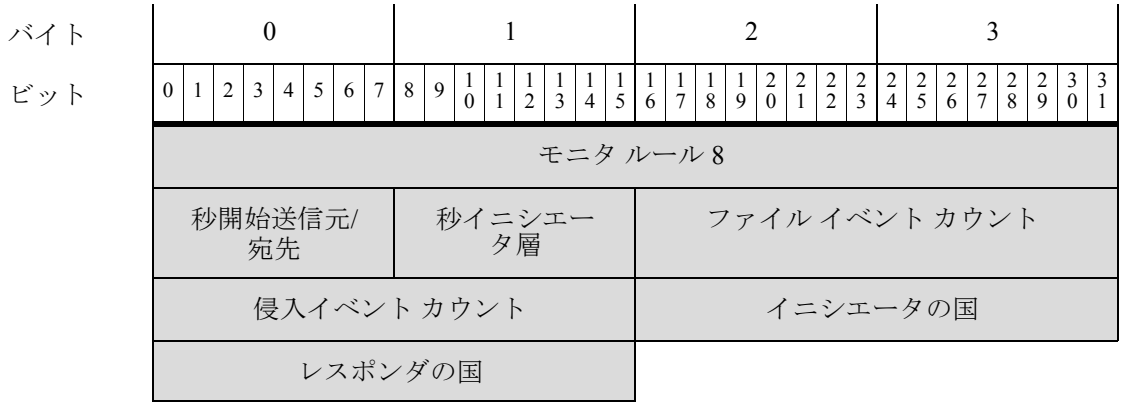
::

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続データ ブロック タイプ（144）																																
接続データ ブロック長																																
デバイス ID																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
入力ゾーン																																
入力ゾーン（続き）																																
入力ゾーン（続き）																																
入力ゾーン（続き）																																
出力ゾーン																																
出力ゾーン（続き）																																
出力ゾーン（続き）																																
出力ゾーン（続き）																																
入力インターフェイス																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
出力インターフェイス																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
イニシエータ IP アドレス																																
イニシエータ IP アドレス（続き）																																
イニシエータ IP アドレス（続き）																																
イニシエータ IP アドレス（続き）																																
レスポンダ IP アドレス																																
レスポンダ IP アドレス（続き）																																
レスポンダ IP アドレス（続き）																																
レスポンダ IP アドレス（続き）																																
ポリシー リビジョン																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ルール ID
ルール アクション
ルールの理由
イニシエータ ポート
レスポンダ ポート
TCP フラグ
プロトコル
NetFlow ソース
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
インスタンス ID
インスタンス ID(続き)
接続数カウンタ
最初のパケットの時刻
最初のパケットのタイムスタンプ(続き)
最終パケットの時刻
最終パケットのタイムスタンプ(続き)
イニシエータ送信パケット数
イニシエータ送信パケット数(続き)
イニシエータ送信パケット数(続き)
レスポンダ Tx パケット
レスポンダ送信パケット数(続き)
レスポンダ送信パケット数(続き)
イニシエータ送信バイト数
イニシエータ送信バイト数(続き)
イニシエータ送信バイト数(続き)
レスポンダ Tx バイト
レスポンダ送信バイト数(続き)
レスポンダ送信バイト数(続き)
ユーザ ID

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		ユーザ ID(続き)																								アプリケーション プロトコルID							
		アプリケーション プロトコル ID(続き)																								URL カ テ ゴ リ							
		URL カテゴリ(続き)																								URLレピュテーション							
		URL レピュテーション(続き)																								クライアント アプリケーション ID							
		クライアント アプリケーション ID(続き)																								Web アプリケーション ID							
クライアント URL		Web アプリケーション ID(続き)																								文字列ブロック タイプ(0)							
		文字列ブロック タイプ(続き)																								文字列ブロック長							
		文字列ブロック長(続き)																								クライアント アプリケーション URL...							
NetBIOS 名		文字列ブロック タイプ(0)																															
		文字列ブロック長																															
		NetBIOS 名...																															
クライアント アプリケーション バージョン		文字列ブロック タイプ(0)																															
		文字列ブロック長																															
		クライアント アプリケーション バージョン...																															
		モニタ ルール 1																															
		モニタ ルール 2																															
		モニタ ルール 3																															
		モニタ ルール 4																															
		モニタ ルール 5																															
		モニタ ルール 6																															
		モニタ ルール 7																															



次の表は、接続統計データ ブロック 5.2.x のフィールドについての説明です。

表 B-28　　接続統計データ ブロック 5.2.x のフィールド

フィールド	データ タイプ	説明
接続統計データ ブロック タイプ	uint32	接続統計データ ブロック 5.2.x を開始します。値は常に 144 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティ ゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティ ゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポンダ IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた相関イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アクション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポンダ ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。

表 B-28　接続統計データ ブロック 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケット タイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケット タイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポンダ送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポンダ送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルのアプリケーション ID。
URL Category	uint32	URL カテゴリの内部 ID 番号。
URLレピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロック タイプ	uint32	クライアント アプリケーション URL の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション URL の文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、およびクライアント アプリケーション URL 文字列のバイト数を含む)。
クライアント アプリケーション URL	string	クライアント アプリケーションがアクセスする URL(該当する場合) (`/files/index.html` など)。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。

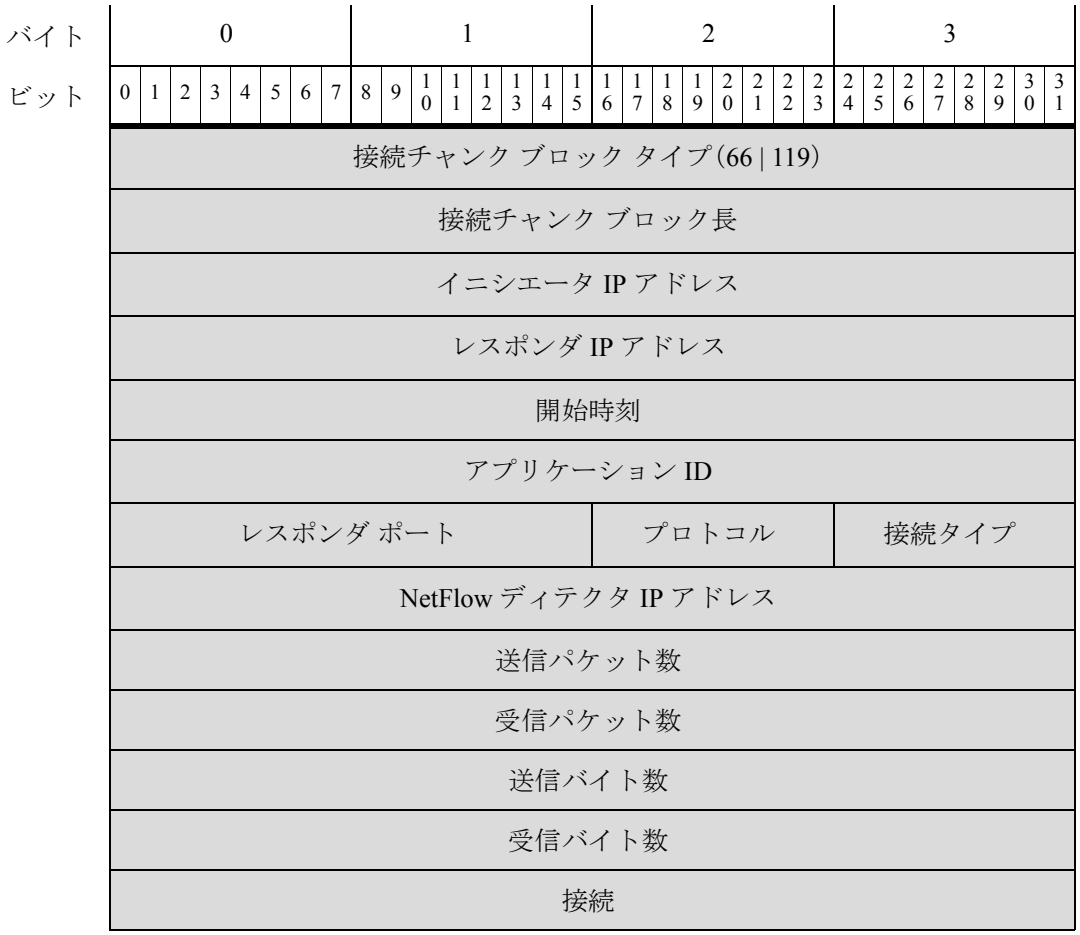
表 B-28　接続統計データ ブロック 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション バージョンの文字列データ ブロックのバイト数(文字列ブロック タイプと長さ フィールド用の 8 バイト、およびバージョンのバイト数を含む)。
クライアント アプリケーション バージョン	string	クライアント アプリケーション バージョン。
モニタ ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタ ルールの ID。
モニタ ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタ ルールの ID。
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入イベント カウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポンダの国	uint16	応答ホストの国のコード。

接続チャンク データ ブロック 5.0 ～ 5.1

接続チャンク データ ブロックは、NetFlow デバイスによって検出された接続データを伝えます。接続チャンク データ ブロックのブロック タイプは、4.10.1 よりも前のバージョンの場合は 66 です。バージョン 5.0 ～ 5.1 の場合、ブロック タイプは 119 です。

次の図は、接続チャンク データ ブロックの形式を示しています。



次の表は、接続チャンク データ ブロックのコンポーネントについての説明です。

表 B-29　　接続チャンク データ ブロックのフィールド

フィールド	データ タイプ	説明
接続チャンク ブロック タイプ	uint32	接続チャンク データ ブロックを開始します。この値は、バージョン 4.10.1 以前の場合は 66、バージョン 5.0 の場合は 119 です。
接続チャンク ブロック長	uint32	接続チャンク データ ブロックのバイト数（接続チャンク ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続チャンク データのバイト数を含む）。

表 B-29　接続チャンク データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
イニシエータ IP アドレス	uint8[4]	IP アドレス オクテットの、接続を開始したホストの IP アドレス。
レスポンダ IP アドレス	uint8[4]	IP アドレス オクテットの、接続で応答するホストの IP アドレス。
開始時刻	uint32	接続チャンクの開始時刻。
アプリケーション ID	uint32	接続で使用されるアプリケーション プロトコルのアプリケーション ID 番号。
レスポンダ ポート	uint16	接続チャンクでレスポンダが使用したポート。
プロトコル	uint8	ユーザ情報を含むパケットのプロトコル。
接続タイプ	uint8	接続の種類。
送信元 デバイス IP アドレス	uint8[4]	IP アドレス オクテットの、接続を検出した NetFlow デバイスの IP アドレス。
送信パケット数	uint32	接続チャンクで送信されたパケット数。
受信パケット数	uint32	接続チャンクで受信されたパケット数。
送信バイト数	uint32	接続チャンクで送信されたバイト数。
受信バイト数	uint32	接続チャンクで受信されたバイト数。
接続	uint32	接続チャンクで行われたセッション数。

接続チャンク データ ブロック 5.1.1 ～ 6.0.x

接続チャンク データ ブロックは、接続データを伝えます。5 分間分を集約した接続ログ データを保存します。接続チャンク データ ブロックのブロック タイプは、シリーズ 1 グループの 136 です。これはブロック タイプ 119 に取って代わります。

次の図は、接続チャンク データ ブロックの形式を示しています。

次の表は、接続チャンク データ ブロックのコンポーネントについての説明です。

表 B-30　　接続チャンク データ ブロックのフィールド

フィールド	データ タイプ	説明
接続チャンク ブロック タイプ	uint32	接続チャンク データ ブロックを開始します。この値は常に 136 です。
接続チャンク ブロック長	uint32	接続チャンク データ ブロックのバイト数(接続チャンク ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続チャンク データのバイト数を含む)。
イニシエータ IP アドレス	uint8(4)	この接続タイプのイニシエータの IP アドレス。これはレスポンダ IP アドレスとともに、複数の同じ接続を見分けるために使用されます。
レスポンダ IP アドレス	uint8(4)	この接続タイプのレスポンダの IP アドレス。これはイニシエータ IP アドレスとともに、複数の同じ接続を見分けるために使用されます。
開始時刻	uint32	接続チャンクの開始時刻。
アプリケーション プロトコル	uint32	接続で使用されたプロトコルの ID 番号。
レスポンダ ポート	uint16	接続チャンクでレスポンダが使用したポート。
プロトコル	uint8	ユーザ情報を含むパケットのプロトコル。

表 B-30　接続チャンク データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
接続タイプ	uint8	接続の種類:
NetFlow ディテクタ IP アドレス	uint8[4]	IP アドレス オクテットの、接続を検出した NetFlow デバイスの IP アドレス。
送信パケット数	uint64	接続チャンクで送信されたパケット数。
受信パケット数	uint64	接続チャンクで受信されたパケット数。
送信バイト数	uint64	接続チャンクで送信されたバイト数。
受信バイト数	uint64	接続チャンクで受信されたバイト数。
接続	uint32	5 分間の接続数。

接続統計データ ブロック 5.1.1.x

接続統計データ ブロックは、接続データ メッセージで使用されます。バージョン 5.1 と 5.1.1 の間に加えられた接続データ ブロックの変更には、関連する侵入イベントを識別するための新規フィールドの追加が含まれます。接続統計データ ブロック バージョン 5.1.1.x のブロック タイプは 137 です。これにより、ブロック タイプ 126(接続統計データ ブロック 5.1(B-132 ページ))は廃止されます。

接続統計データ メッセージの詳細については、接続統計データ メッセージ(4-54 ページ)を参照してください。

次の図は、接続統計データ ブロック 5.1.1 の形式を示しています。

::

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続データ ブロック タイプ(137)																																
接続データ ブロック長																																
デバイス ID																																
入力ゾーン																																
入力ゾーン(続き)																																
入力ゾーン(続き)																																
入力ゾーン(続き)																																
出力ゾーン																																
出力ゾーン(続き)																																
出力ゾーン(続き)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出力ゾーン(続き)																																
入力インターフェイス																																
入力インターフェイス(続き)																																
入力インターフェイス(続き)																																
入力インターフェイス(続き)																																
出力インターフェイス																																
出力インターフェイス(続き)																																
出力インターフェイス(続き)																																
出力インターフェイス(続き)																																
イニシエータ IP アドレス																																
イニシエータ IP アドレス(続き)																																
イニシエータ IP アドレス(続き)																																
イニシエータ IP アドレス(続き)																																
レスポンダ IP アドレス																																
レスポンダ IP アドレス(続き)																																
レスポンダ IP アドレス(続き)																																
レスポンダ IP アドレス(続き)																																
ポリシー リビジョン																																
ポリシー リビジョン(続き)																																
ポリシー リビジョン(続き)																																
ポリシー リビジョン(続き)																																
ルール ID																																
ルール アクション																	ルールの理由															
イニシエータ ポート																	レスポンダ ポート															
TCP フラグ																	プロトコル								NetFlow ソース							

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NetFlow ソース（続き）																																
NetFlow ソース（続き）																																
NetFlow ソース（続き）																																
NetFlow ソース（続き）																									インスタンス ID							
インスタンス ID（続き）									接続数カウンタ																最初のパケットの時刻							
最初のパケットのタイムスタンプ（続き）																									最終パケットの時刻							
最終パケットのタイムスタンプ（続き）																									イニシエータ送信パケット数							
イニシエータ送信パケット数（続き）																																
イニシエータ送信パケット数（続き）																									レスポンダ Tx パケット							
レスポンダ送信パケット数（続き）																																
レスポンダ送信パケット数（続き）																									イニシエータ送信バイト数							
イニシエータ送信バイト数（続き）																																
イニシエータ送信バイト数（続き）																									レスポンダ Tx バイト							
レスポンダ送信バイト数（続き）																																
レスポンダ送信バイト数（続き）																									ユーザ ID							
ユーザ ID（続き）																									アプリケーション プロトコルID							
アプリケーション プロトコル ID（続き）																									URL カテゴリ							
URL カテゴリ（続き）																									URLレピュテーション							
URL レピュテーション（続き）																									クライアント アプリケーション ID							
クライアント アプリケーション ID（続き）																									Web アプリケーション ID							

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
クライアント URL	Web アプリケーション ID（続き）																								文字列ブロック タイプ（0）							
	文字列ブロック タイプ（続き）																								文字列ブロック長							
	文字列ブロック長（続き）																								クライアント アプリケーション URL...							
NetBIOS 名	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	NetBIOS 名...																															
クライアント アプリケーション バージョン	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	クライアント アプリケーション バージョン...																															
	モニタ ルール 1																															
	モニタ ルール 2																															
	モニタ ルール 3																															
	モニタ ルール 4																															
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/宛先								秒イニシエータ層								ファイル イベント カウント															
	侵入イベント カウント																															

次の表は、接続統計データ ブロック 5.1.1.x のフィールドについての説明です。

表 B-31　接続統計データ ブロック 5.1.1.x のフィールド

フィールド	データ タイプ	説明
接続統計データ ブロック タイプ	uint32	接続統計データ ブロック 5.1.1.x を開始します。値は常に 137 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティ ゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティ ゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポンダ IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた相関イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アクション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポンダ ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケット タイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。

表 B-31　接続統計データ ブロック 5.1.1.x のフィールド(続き)

フィールド	データ タイプ	説明
最終パケット タイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポンダ送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポンダ送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URLレピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロック タイプ	uint32	クライアント アプリケーション URL の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション URL の文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、およびクライアント アプリケーション URL 文字列のバイト数を含む)。
クライアント アプリケーション URL	string	クライアント アプリケーションがアクセスする URL(該当する場合) (/files/index.html など)。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション バージョンの文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。

表 B-31　接続統計データ ブロック 5.1.1.x のフィールド(続き)

フィールド	データ タイプ	説明
クライアント アプリケーション バージョン	string	クライアント アプリケーション バージョン。
モニタ ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタ ルールの ID。
モニタ ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタ ルールの ID。
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入イベント カウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。

接続統計データ ブロック 5.3

接続統計データ ブロックは、接続データ メッセージで使用されます。バージョン 5.2.x と 5.3 の間に加えられた接続データ ブロックの変更には、NetFlow 情報用の新規フィールドの追加が含まれます。バージョン 5.3 の接続統計データ ブロックは、シリーズ 1 グループのブロックの、ブロック タイプ 152 です。これにより、ブロック タイプ 144（接続統計データ ブロック 5.2.x（B-138 ページ））は廃止されます。

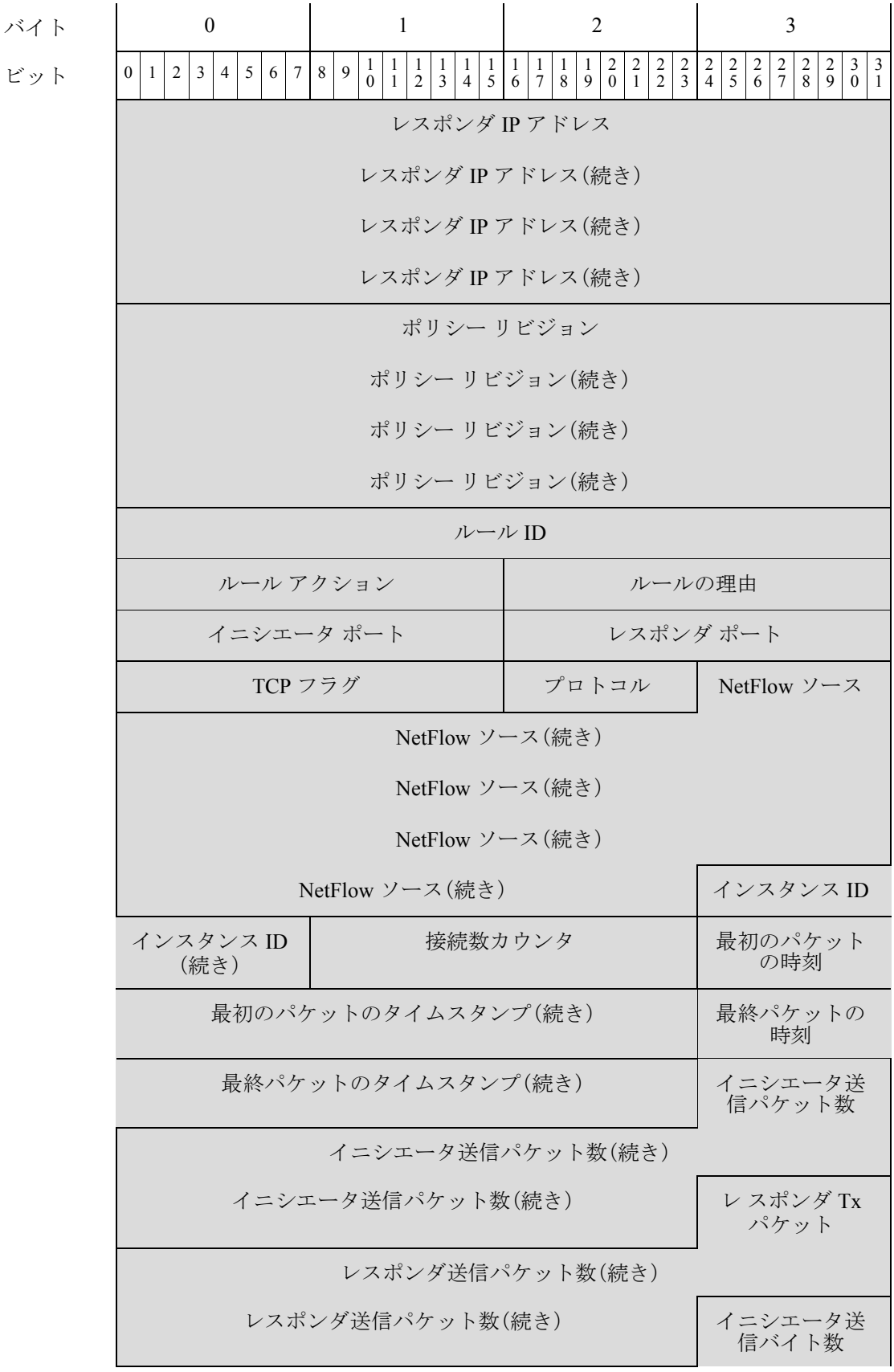
接続イベント レコードを要求するには、イベント バージョン 10 およびイベント コード 71 の要求メッセージ内に、拡張イベント フラグ（要求フラグ フィールドのビット 30）を設定します。要求フラグ（2-12 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

接続統計データ メッセージの詳細については、接続統計データ メッセージ（4-54 ページ）を参照してください。

次の図は、接続統計データ ブロック 5.3+の形式を示しています。

::

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続データ ブロック タイプ（152）																																
接続データ ブロック長																																
デバイス ID																																
入力ゾーン																																
入力ゾーン（続き）																																
入力ゾーン（続き）																																
入力ゾーン（続き）																																
出力ゾーン																																
出力ゾーン（続き）																																
出力ゾーン（続き）																																
出力ゾーン（続き）																																
入力インターフェイス																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
出力インターフェイス																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
イニシエータ IP アドレス																																
イニシエータ IP アドレス（続き）																																
イニシエータ IP アドレス（続き）																																
イニシエータ IP アドレス（続き）																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
レスポンダ IP アドレス
レスポンダ IP アドレス(続き)
レスポンダ IP アドレス(続き)
レスポンダ IP アドレス(続き)
ポリシー リビジョン
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ルール ID
ルール アクション
ルールの理由
イニシエータ ポート
レスポンダ ポート
TCP フラグ
プロトコル
NetFlow ソース
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
インスタンス ID
インスタンス ID(続き)
接続数カウンタ
最初のパケットの時刻
最初のパケットのタイムスタンプ(続き)
最終パケットの時刻
最終パケットのタイムスタンプ(続き)
イニシエータ送信パケット数
イニシエータ送信パケット数(続き)
イニシエータ送信パケット数(続き)
レ スポンダ Tx パケット
レスポンダ送信パケット数(続き)
レスポンダ送信パケット数(続き)
イニシエータ送信バイト数

	バイト 0								バイト 1								バイト 2								バイト 3							
	ビット 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	イニシエータ送信バイト数(続き)																															
	イニシエータ送信バイト数(続き)																								レスポンダ Tx バイト							
	レスポンダ送信バイト数(続き)																															
	レスポンダ送信バイト数(続き)																								ユーザ ID							
	ユーザ ID(続き)																								アプリケーション プロトコルID							
	アプリケーション プロトコル ID(続き)																								URL カテゴリ							
	URL カテゴリ(続き)																								URLレピュテーション							
	URL レピュテーション(続き)																								クライアント アプリケーション ID							
	クライアント アプリケーション ID(続き)																								Web アプリケーション ID							
クライアント URL	Web アプリケーション ID(続き)																								文字列ブロック タイプ(0)							
	文字列ブロック タイプ(続き)																								文字列ブロック長							
	文字列ブロック長(続き)																								クライアント アプリケーション URL...							
NetBIOS 名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	NetBIOS 名...																															
クライアント アプリケーション バージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	クライアント アプリケーション バージョン...																															
	モニタ ルール 1																															
	モニタ ルール 2																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
モニタ ルール 3																																
モニタ ルール 4																																
モニタ ルール 5																																
モニタ ルール 6																																
モニタ ルール 7																																
モニタ ルール 8																																
秒開始送信元/宛先									秒イニシエータ層								ファイル イベント カウント															
侵入イベント カウント																									イニシエータの国							
レスポンダの国																									IOC 番号							
送信元自律システム																																
宛先自律システム																																
SNMP 入力																									SNMP 出力							
送信元 TOS									宛先 TOS								送信元マスク								宛先マスク							

次の表は、接続統計データ ブロック 5.3 のフィールドについての説明です。

表 B-32　　接続統計データ ブロック 5.3+のフィールド

フィールド	データ タイプ	説明
接続統計データ ブロック タイプ	uint32	接続統計データ ブロック 5.3 を開始します。値は常に 152 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティ ゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティ ゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。

表 B-32　接続統計データ ブロック 5.3+のフィールド(続き)

フィールド	データ タイプ	説明
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポンダ IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた相関イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アクション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポンダ ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケット タイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケット タイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポンダ送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポンダ送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。

表 B-32　接続統計データ ブロック 5.3+のフィールド(続き)

フィールド	データ タイプ	説明
URLレピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロック タイプ	uint32	クライアント アプリケーション URL の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション URL の文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、およびクライアント アプリケーション URL 文字列のバイト数を含む)。
クライアント アプリケーション URL	string	クライアント アプリケーションがアクセスする URL(該当する場合) (`/files/index.html` など)。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション バージョンの文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
クライアント アプリケーション バージョン	string	クライアント アプリケーション バージョン。
モニタ ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタ ルールの ID。
モニタ ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタ ルールの ID。
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。

表 B-32　接続統計データ ブロック 5.3+のフィールド(続き)

フィールド	データ タイプ	説明
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入イベント カウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポンダの国	uint 16	応答ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。
SNMP 出力	uint16	出力インターフェイスの SNMP インデックス
送信元 TOS	uint8	着信インターフェイス用のタイプ オブ サービス バイト設定。
宛先 TOS	uint8	発信インターフェイス用のタイプ オブ サービス バイト設定。
送信元マスク	uint8	送信元アドレス プレフィックス マスク。
宛先マスク	uint8	宛先アドレス プレフィックス マスク。

接続統計データ ブロック 5.3.1

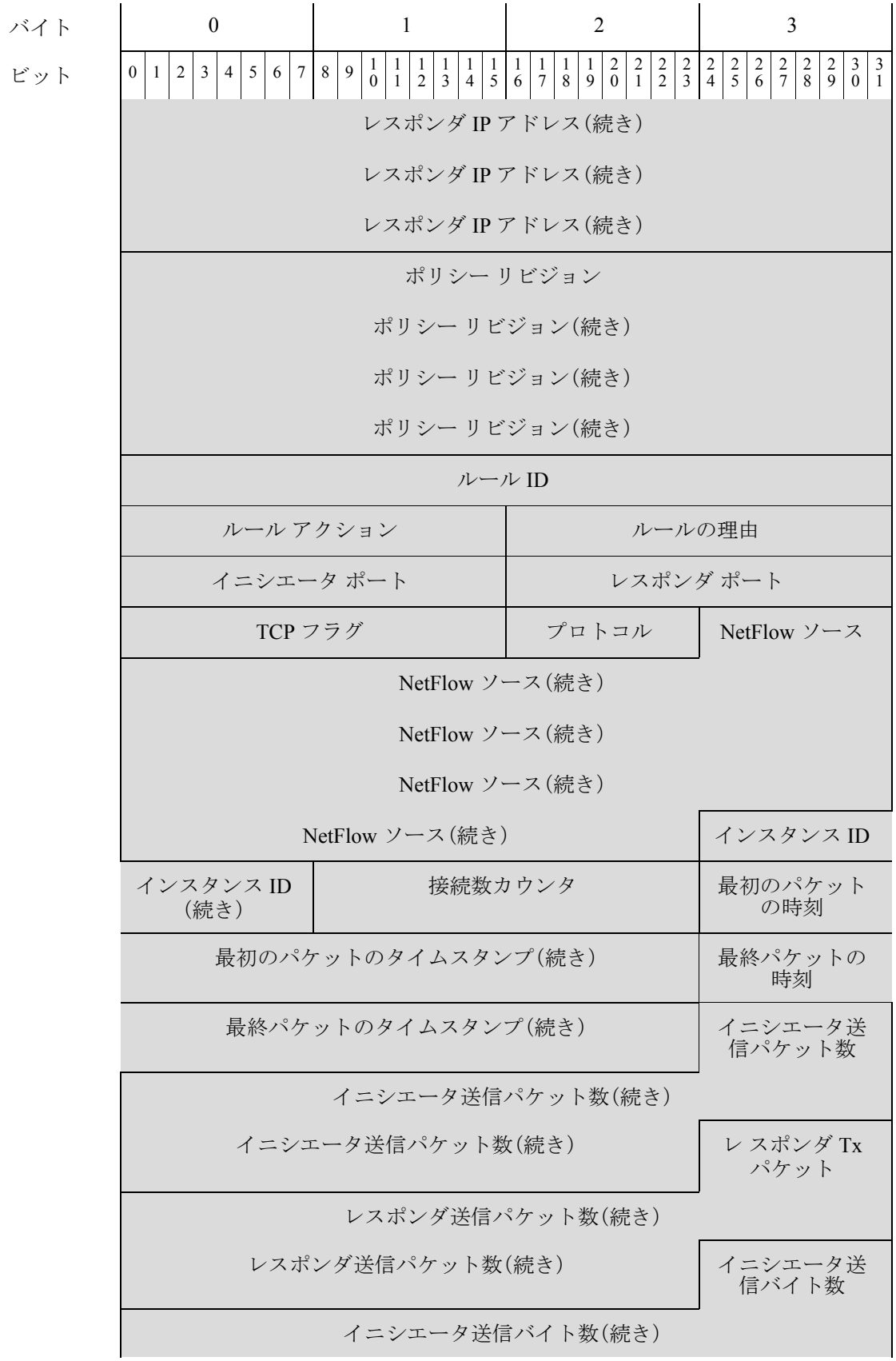
接続統計データ ブロックは、接続データ メッセージで使用されます。バージョン 5.3 と 5.3.1 との間で加えられた接続データ ブロックの唯一の変更は、セキュリティ コンテキスト フィールドの追加です。バージョン 5.3.1 の接続統計データ ブロックは、シリーズ 1 グループのブロックの、ブロック タイプ 154 です。これにより、ブロック タイプ 152(接続統計データ ブロック 5.3(B-154 ページ))は廃止されます。

接続イベント レコードを要求するには、イベント バージョン 11 およびイベント コード 71 の要求メッセージ内に、拡張イベント フラグ(要求フラグ フィールドのビット 30)を設定します。要求フラグ(2-12 ページ)を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。接続統計データ メッセージの詳細については、接続統計データ メッセージ(4-54 ページ)を参照してください。

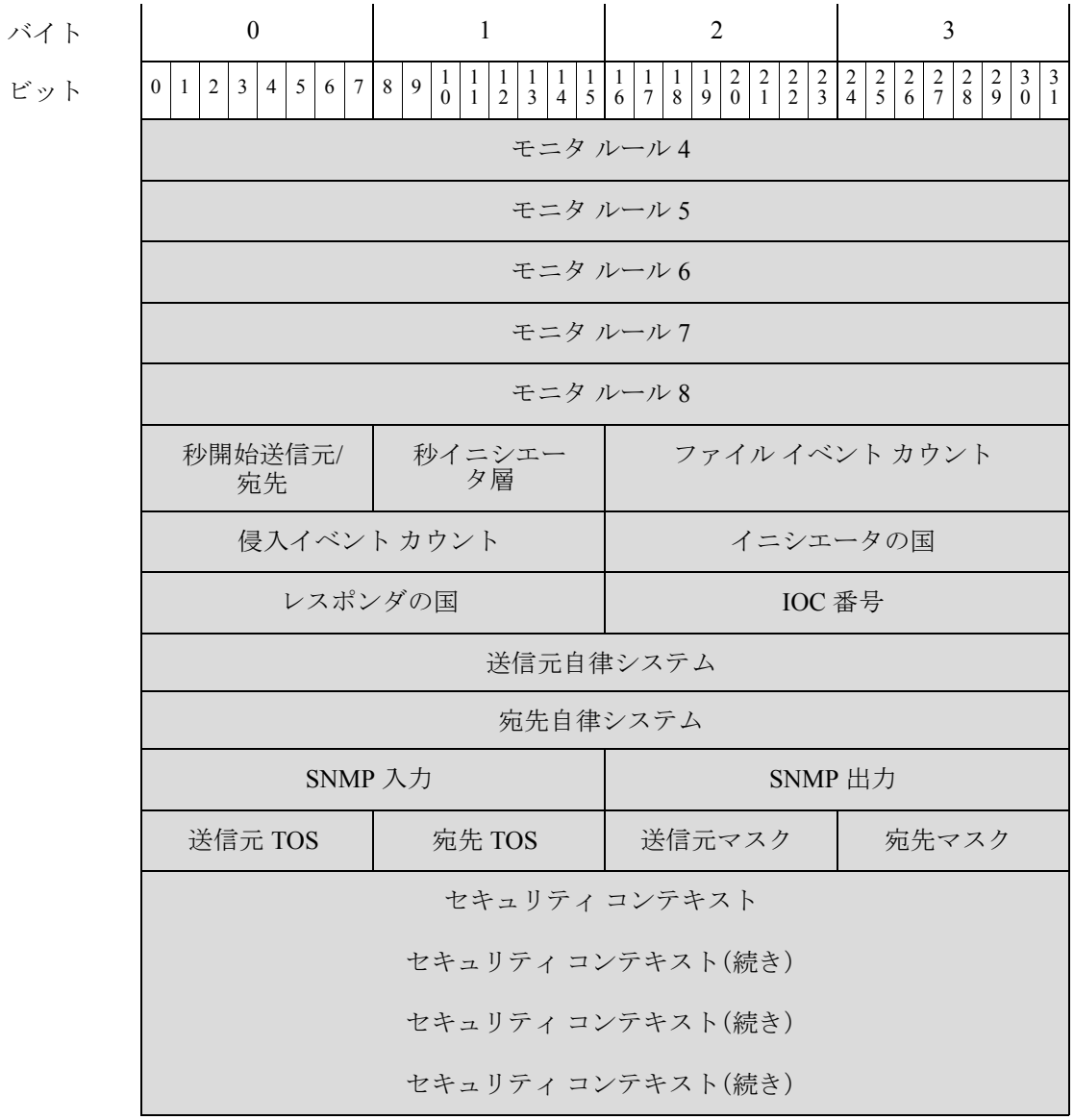
次の図は、接続統計データ ブロック 5.3.1 の形式を示しています。

::

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続データ ブロック タイプ（154）																																
接続データ ブロック長																																
デバイスID																																
入力ゾーン 入力ゾーン（続き） 入力ゾーン（続き） 入力ゾーン（続き）																																
出力ゾーン 出力ゾーン（続き） 出力ゾーン（続き） 出力ゾーン（続き）																																
入力インターフェイス 入力インターフェイス（続き） 入力インターフェイス（続き） 入力インターフェイス（続き）																																
出力インターフェイス 出力インターフェイス（続き） 出力インターフェイス（続き） 出力インターフェイス（続き）																																
イニシエータ IP アドレス イニシエータ IP アドレス（続き） イニシエータ IP アドレス（続き） イニシエータ IP アドレス（続き）																																
レスポンダ IP アドレス																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
レスポンダ IP アドレス(続き)
レスポンダ IP アドレス(続き)
レスポンダ IP アドレス(続き)
ポリシー リビジョン
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ルール ID
ルール アクション
ルールの理由
イニシエータ ポート
レスポンダ ポート
TCP フラグ
プロトコル
NetFlow ソース
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
インスタンス ID
インスタンス ID(続き)
接続数カウンタ
最初のパケットの時刻
最初のパケットのタイムスタンプ(続き)
最終パケットの時刻
最終パケットのタイムスタンプ(続き)
イニシエータ送信パケット数
イニシエータ送信パケット数(続き)
イニシエータ送信パケット数(続き)
レスポンダ Tx パケット
レスポンダ送信パケット数(続き)
レスポンダ送信パケット数(続き)
イニシエータ送信バイト数
イニシエータ送信バイト数(続き)

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		イニシエータ送信バイト数(続き)																								レスポンダ Tx バイト							
		レスポンダ送信バイト数(続き)																															
		レスポンダ送信バイト数(続き)																								ユーザ ID							
		ユーザ ID(続き)																								アプリケーション プロトコルID							
		アプリケーション プロトコル ID(続き)																								URL カテゴリ							
		URL カテゴリ(続き)																								URL レピュテーション							
		URL レピュテーション(続き)																								クライアント アプリケーション ID							
		クライアント アプリケーション ID(続き)																								Web アプリケーション ID							
	クライアント URL	Web アプリケーション ID(続き)																								文字列ブロック タイプ(0)							
		文字列ブロック タイプ(続き)																								文字列ブロック長							
		文字列ブロック長(続き)																								クライアント アプリケーション URL...							
	NetBIOS 名	文字列ブロック タイプ(0)																															
		文字列ブロック長																															
		NetBIOS 名...																															
	クライアント アプリケーション バージョン	文字列ブロック タイプ(0)																															
		文字列ブロック長																															
		クライアント アプリケーション バージョン...																															
		モニタ ルール 1																															
		モニタ ルール 2																															
		モニタ ルール 3																															



次の表は、接続統計データ ブロック 5.3.1 のフィールドについての説明です。

表 B-33　　接続統計データ ブロック 5.3.1 のフィールド

フィールド	データ タイプ	説明
接続統計データ ブロック タイプ	uint32	接続統計データ ブロック 5.3.1+ を開始します。値は常に 154 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイスID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティ ゾーン。

表 B-33　接続統計データ ブロック 5.3.1 のフィールド(続き)

フィールド	データ タイプ	説明
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティ ゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポンダ IP アドレス	uint8[16]	IPアドレス オクテットの、開始ホストに応答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた相関イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アクション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポンダ ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケット タイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケット タイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポンダ送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポンダ送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。

表 B-33　接続統計データ ブロック 5.3.1 のフィールド(続き)

フィールド	データ タイプ	説明
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URLレピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロック タイプ	uint32	クライアント アプリケーション URL の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション URL の文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、およびクライアント アプリケーション URL 文字列のバイト数を含む)。
クライアント アプリケーション URL	string	クライアント アプリケーションがアクセスする URL(該当する場合) (/files/index.html など)。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション バージョンの文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
クライアント アプリケーション バージョン	string	クライアント アプリケーション バージョン。
モニタ ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタ ルールの ID。
モニタ ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタ ルールの ID。
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。

表 B-33　接続統計データ ブロック 5.3.1 のフィールド(続き)

フィールド	データ タイプ	説明
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入イベント カウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポンダの国	uint 16	応答ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。
SNMP 出力	uint16	出力インターフェイスの SNMP インデックス
送信元 TOS	uint8	着信インターフェイス用のタイプ オブ サービス バイト設定。
宛先 TOS	uint8	発信インターフェイス用のタイプ オブ サービス バイト設定。
送信元マスク	uint8	送信元アドレス プレフィックス マスク。
宛先マスク	uint8	宛先アドレス プレフィックス マスク。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

接続統計データ ブロック 5.4

接続統計データ ブロックは、接続データ メッセージで使用されます。接続統計データ ブロック 5.4 には、いくつかの新しいフィールドが追加されました。SSL 接続、HTTP リダイレクション、およびネットワーク分析ポリシーをサポートするためのフィールドが追加されています。バージョン 5.4 の接続統計データ ブロックは、シリーズ 1 グループのブロックの、ブロック タイプ 155 です。これにより、ブロック タイプ 154(接続統計データ ブロック 5.3.1(B-161 ページ))は廃止されます。

接続イベント レコードを要求するには、イベント バージョン 12 およびイベント コード 71 の要求メッセージ内に、拡張イベント フラグ（要求フラグ フィールドのビット 30）を設定します。要求フラグ（2-12 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

接続統計データ メッセージの詳細については、接続統計データ メッセージ（4-54 ページ）を参照してください。

次の図は、接続統計データ ブロック 5.4 の形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続データ ブロック タイプ（155）																																
接続データ ブロック長																																
デバイスID																																
入力ゾーン																																
入力ゾーン（続き）																																
入力ゾーン（続き）																																
入力ゾーン（続き）																																
出力ゾーン																																
出力ゾーン（続き）																																
出力ゾーン（続き）																																
出力ゾーン（続き）																																
入力インターフェイス																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
出力インターフェイス																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
イニシエータ IP アドレス																																
イニシエータ IP アドレス（続き）																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
イニシエータ IP アドレス(続き)
イニシエータ IP アドレス(続き)
レスポンダ IP アドレス
レスポンダ IP アドレス(続き)
レスポンダ IP アドレス(続き)
レスポンダ IP アドレス(続き)
ポリシー リビジョン
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ルール ID
ルール アクション
ルールの理由
イニシエータ ポート
レスポンダ ポート
TCP フラグ
プロトコル
NetFlow ソース
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
インスタンス ID
インスタンス ID (続き)
接続数カウンタ
最初のパケットの時刻
最初のパケットのタイムスタンプ(続き)
最終パケットの時刻
最終パケットのタイムスタンプ(続き)
イニシエータ送信パケット数
イニシエータ送信パケット数(続き)
イニシエータ送信パケット数(続き)
レ スポンダ Tx パケット


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
レスポンダ送信パケット数(続き)
レスポンダ送信パケット数(続き)
イニシエータ送信バイト数
イニシエータ送信バイト数(続き)
イニシエータ送信バイト数(続き)
レスポンダ Tx バイト
レスポンダ送信バイト数(続き)
レスポンダ送信バイト数(続き)
ユーザ ID
ユーザ ID(続き)
アプリケーション プロトコルID
アプリケーション プロトコル ID(続き)
URL カテゴリ
URL カテゴリ(続き)
URL レピュテーション
URL レピュテーション(続き)
クライアント アプリケーション ID
クライアント アプリケーション ID(続き)
Web アプリケーション ID
クライアント URL
Web アプリケーション ID(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(続き)
文字列ブロック長
文字列ブロック長(続き)
クライアント アプリケーション URL...
NetBIOS 名
文字列ブロック タイプ(0)
文字列ブロック長
NetBIOS 名...

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
クライアント アプリケーション バージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	クライアント アプリケーション バージョン...																															
	モニタ ルール 1																															
	モニタ ルール 2																															
	モニタ ルール 3																															
	モニタ ルール 4																															
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/宛先								秒イニシエータ層								ファイル イベント カウント															
	侵入イベント カウント																イニシエータの国															
	レスポンダの国																IOC 番号															
	送信元自律システム																															
	宛先自律システム																															
	SNMP 入力																SNMP 出力															
	送信元 TOS								宛先 TOS								送信元マスク								宛先マスク							
	セキュリティ コンテキスト セキュリティ コンテキスト(続き) セキュリティ コンテキスト(続き)																															


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
セキュリティ コンテキスト(続き)
参照ホスト
VLAN ID
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
参照ホスト...
ユーザ エージェント
文字列ブロック タイプ(0)
文字列ブロック長
ユーザ エージェント...
HTTP リファラ
文字列ブロック タイプ(0)
文字列ブロック長
HTTP リファラ...
SSL 証明書フィンガープリント
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL ポリシー ID
SSL ポリシー ID(続き)
SSL ポリシー ID(続き)
SSL ポリシー ID(続き)
SSL ルール ID
SSL 暗号スイート
SSL バージョン
SSL キー証明書統計
SSL キー証明書統計(続き)
実際の SSL アクション
予期された SSL アクション


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
予期された SSL アクション(続き)
SSL フロー ステータス
SSL フロー エラー
SSL フロー エラー(続き)
SSL フロー メッセージ
SSL フロー メッセージ(続き)
SSL フロー フラグ
SSL フロー フラグ(続き)
SSL フロー フラグ(続き)
文字列ブロック タイプ(0)
SSL サーバ名
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
SSL サーバ名...
SSL URL カテゴリ
SSL セッション ID
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID の長さ
SSL チケット ID
SSL チケット ID(続き)
SSL チケット ID(続き)
SSL チケット ID(続き)
SSL チケット ID(続き)

次の表は、接続統計データ ブロック 5.4+のフィールドについての説明です。

表 B-34　　接続統計データ ブロック 5.4+のフィールド

フィールド	データ タイプ	説明
接続統計データ ブロック タイプ	uint32	接続統計データ ブロック 5.4+を開始します。値は常に 155 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイスID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティ ゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティ ゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポンダ IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた相関イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アクション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。

表 B-34　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポンダ ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケット タイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケット タイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポンダ送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポンダ送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URL レピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロック タイプ	uint32	クライアント アプリケーション URL の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション URL の文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、およびクライアント アプリケーション URL 文字列のバイト数を含む)。

表 B-34　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
クライアント アプリケーション URL	string	クライアント アプリケーションがアクセスする URL(該当する場合)(`/files/index.html` など)。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に `0` です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に `0` です。
文字列ブロック長	uint32	クライアント アプリケーション バージョンの文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
クライアント アプリケーション バージョン	string	クライアント アプリケーション バージョン。
モニタ ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタ ルールの ID。
モニタ ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタ ルールの ID。
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入イベント カウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。

表 B-34　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
イニシエータの国	uint16	開始ホストの国のコード。
レスポンダの国	uint 16	応答ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。
SNMP 出力	uint16	出力インターフェイスの SNMP インデックス
送信元 TOS	uint8	着信インターフェイス用のタイプ オブ サービス バイト設定。
宛先 TOS	uint8	発信インターフェイス用のタイプ オブ サービス バイト設定。
送信元マスク	uint8	送信元アドレス プレフィックス マスク。
宛先マスク	uint8	宛先アドレス プレフィックス マスク。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
VLAN ID	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
文字列ブロック タイプ	uint32	参照ホストを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	参照ホスト文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および参照ホスト フィールドのバイト数を含む)。
参照ホスト	string	HTTP または DNS で提供されるホスト名情報。
文字列ブロック タイプ	uint32	ユーザ エージェントを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ エージェント文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ エージェント フィールドのバイト数を含む)。
ユーザ エージェント	string	セッションのユーザ エージェント ヘッダー フィールドからの情報。
文字列ブロック タイプ	uint32	HTTP リファラを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	HTTP リファラ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および HTTP リファラ フィールドのバイト数を含む)。
HTTP リファラ	string	ページの発生元のサイト。これは HTTP トラフィック内の参照ヘッダー情報にあります。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
SSL ポリシー ID	uint8[16]	接続を処理した SSL ポリシーの ID 番号。

表 B-34　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルト アクションの ID 番号。
SSL 暗号スイート	uint16	SSL 接続で使用される暗号スイート。値は 10 進形式で保存されます。値により指定されている暗号スイートの詳細については、www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
SSL バージョン	uint8	接続の暗号化に使用された SSL または TLS プロトコル バージョン。
SSL サーバ証明書ステータス	uint16	SSL 証明書のステータス。有効な値は次のとおりです。 • 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 • 1(不明):サーバ証明書のステータスは判別できませんでした。 • 2(有効):サーバ証明書は有効です。 • 4(自己署名済み):サーバ証明書は自己署名です。 • 16(無効な発行者):サーバ証明書に無効な発行者があります。 • 32(無効な署名):サーバ証明書に無効な署名があります。 • 64(期限切れ):サーバ証明書は期限切れです。 • 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 • 256(取り消し):サーバ証明書は取り消されました。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 B-34　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
予期された SSL アクション	uint16	SSL ルールに基づいて接続に対して実行する必要があるアクション。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 B-34　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
SSL フロー ステータス	uint16	SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。 • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL フロー エラー	uint32	詳細な SSL エラー コード。これらの値はサポート目的で必要とされる場合があります。

表 B-34　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
SSL フロー メッセージ	uint32	SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。 • 0x00000001:NSE_MT__HELLO_REQUEST • 0x00000002:NSE_MT__CLIENT_ALERT • 0x00000004:NSE_MT__SERVER_ALERT • 0x00000008:NSE_MT__CLIENT_HELLO • 0x00000010:NSE_MT__SERVER_HELLO • 0x00000020:NSE_MT__SERVER_CERTIFICATE • 0x00000040:NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080:NSE_MT__CERTIFICATE_REQUEST • 0x00000100:NSE_MT__SERVER_HELLO_DONE • 0x00000200:NSE_MT__CLIENT_CERTIFICATE • 0x00000400:NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800:NSE_MT__CERTIFICATE_VERIFY • 0x00001000: NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000:NSE_MT__CLIENT_FINISHED • 0x00004000: NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000:NSE_MT__SERVER_FINISHED • 0x00010000:NSE_MT__NEW_SESSION_TICKET • 0x00020000:NSE_MT__HANDSHAKE_OTHER • 0x00040000:NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000:NSE_MT__APP_DATA_FROM_SERVER
SSL フロー フラグ	uint64	暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。 • 0x00000001(NSE_FLOW__VALID):他のフィールドを有効にするために設定する必要があります • 0x00000002(NSE_FLOW__INITIALIZED):内部構造が処理可能です • 0x00000004(NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました
文字列ブロック タイプ	uint32	SSL サーバ名を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-34　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	SSL サーバ名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および SSL サーバ名フィールドのバイト数を含む)。
SSL サーバ名	string	SSL Client Hello でサーバ名に指定された名前。
SSL URL カテゴリ	uint32	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできます。
SSL チケット ID	uint8[20]	クライアントとサーバがセッション チケットの使用に同意する場合に使用されるセッション チケットのハッシュ。
SSL チケット ID の長さ	uint8	SSL チケット ID の長さ。チケット ID は 20 バイトより長くすることはできませんが、20 バイト未満であってもかまいません。
ネットワーク分析ポリシー リビジョン	uint8[16]	接続イベントに関連付けられているネットワーク分析ポリシーのリビジョン。

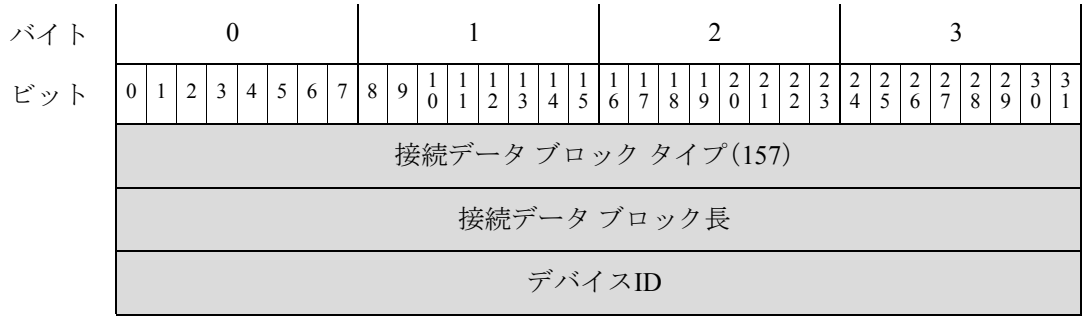
接続統計データ ブロック 5.4.1

接続統計データ ブロックは、接続データ メッセージで使用されます。接続統計データ ブロック 5.4 には、いくつかの新しいフィールドが追加されました。SSL 接続、HTTP リダイレクション、およびネットワーク分析ポリシーをサポートするためのフィールドが追加されています。バージョン 5.4+ の接続統計データ ブロックは、シリーズ 1 グループのブロックの、ブロック タイプ 157 です。これにより、ブロック タイプ 155(接続統計データ ブロック 5.3.1(B-161 ページ))は廃止されます。

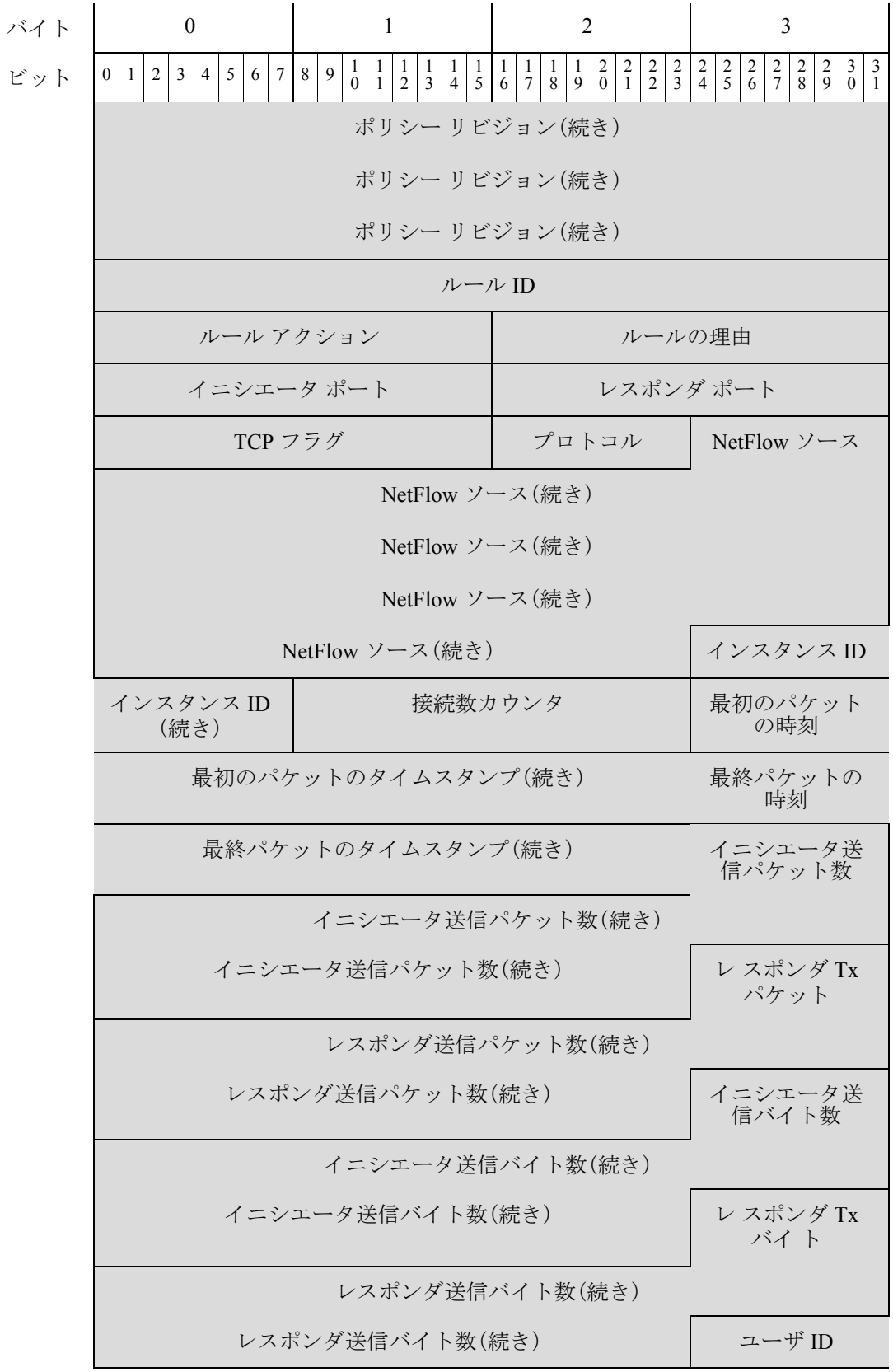
接続イベント レコードを要求するには、イベント バージョン 12 およびイベント コード 71 の要求メッセージ内に、拡張イベント フラグ(要求フラグ フィールドのビット 30)を設定します。要求フラグ(2-12 ページ)を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

接続統計データ メッセージの詳細については、接続統計データ メッセージ(4-54 ページ)を参照してください。

次の図は、接続統計データ ブロック 5.4+の形式を示しています。



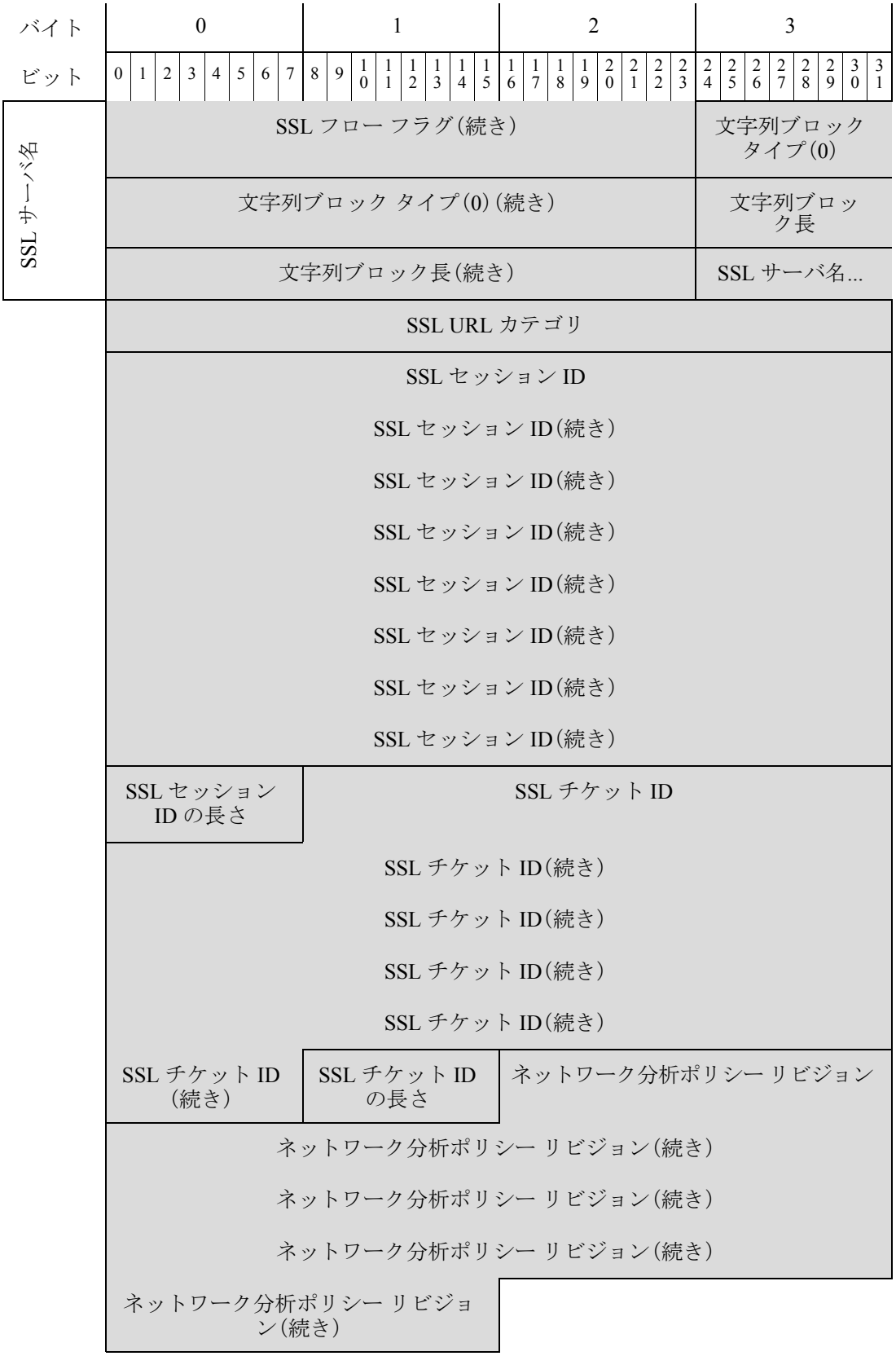
バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
入力ゾーン																																
入力ゾーン（続き）																																
入力ゾーン（続き）																																
入力ゾーン（続き）																																
出力ゾーン																																
出力ゾーン（続き）																																
出力ゾーン（続き）																																
出力ゾーン（続き）																																
入力インターフェイス																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
出力インターフェイス																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
イニシエータ IP アドレス																																
イニシエータ IP アドレス（続き）																																
イニシエータ IP アドレス（続き）																																
イニシエータ IP アドレス（続き）																																
レスポンダ IP アドレス																																
レスポンダ IP アドレス（続き）																																
レスポンダ IP アドレス（続き）																																
レスポンダ IP アドレス（続き）																																
ポリシー リビジョン																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ルール ID
ルール アクション
ルールの理由
イニシエータ ポート
レスポンダ ポート
TCP フラグ
プロトコル
NetFlow ソース
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
インスタンス ID
インスタンス ID(続き)
接続数カウンタ
最初のパケットの時刻
最初のパケットのタイムスタンプ(続き)
最終パケットの時刻
最終パケットのタイムスタンプ(続き)
イニシエータ送信パケット数
イニシエータ送信パケット数(続き)
イニシエータ送信パケット数(続き)
レ スポンダ Tx パケット
レスポンダ送信パケット数(続き)
レスポンダ送信パケット数(続き)
イニシエータ送信バイト数
イニシエータ送信バイト数(続き)
イニシエータ送信バイト数(続き)
レ スポンダ Tx バイ ト
レスポンダ送信バイト数(続き)
レスポンダ送信バイト数(続き)
ユーザ ID


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
ユーザ ID(続き)
アプリケーション プロトコルID
アプリケーション プロトコル ID(続き)
URL カテゴリ
URL カテゴリ(続き)
URLレピュテーション
URL レピュテーション(続き)
クライアント アプリケーション ID
クライアント アプリケーション ID(続き)
Web アプリケーション ID
クライアント URL
Web アプリケーション ID(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(続き)
文字列ブロック長
文字列ブロック長(続き)
クライアント アプリケーション URL...
NetBIOS 名
文字列ブロック タイプ(0)
文字列ブロック長
NetBIOS 名...
クライアント アプリケーション バージョン
文字列ブロック タイプ(0)
文字列ブロック長
クライアント アプリケーション バージョン...
モニタ ルール 1
モニタ ルール 2
モニタ ルール 3

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	モニタ ルール 4																															
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/宛先								秒イニシエータ層								ファイル イベント カウント															
	侵入イベント カウント																イニシエータの国															
	レスポンダの国																IOC 番号															
	送信元自律システム																															
	宛先自律システム																															
	SNMP 入力																SNMP 出力															
	送信元 TOS								宛先 TOS								送信元マスク								宛先マスク							
	セキュリティ コンテキスト セキュリティ コンテキスト(続き) セキュリティ コンテキスト(続き) セキュリティ コンテキスト(続き)																															
参照ホスト	VLAN ID																文字列ブロック タイプ(0)															
	文字列ブロック タイプ(0)(続き)																文字列ブロック長															
	文字列ブロック長(続き)																参照ホスト...															
ユーザ エージェント	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ エージェント...																															


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
HTTP リファラ
文字列ブロック タイプ(0)
文字列ブロック長
HTTP リファラ...
SSL 証明書フィンガープリント
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL ポリシー ID
SSL ポリシー ID(続き)
SSL ポリシー ID(続き)
SSL ポリシー ID(続き)
SSL ルール ID
SSL 暗号スイート
SSL バージョン
SSL キー証明書統計
SSL キー証明書統計(続き)
実際の SSL アクション
予期された SSL アクション
予期された SSL アクション(続き)
SSL フロー ステータス
SSL フロー エラー
SSL フロー エラー(続き)
SSL フロー メッセージ
SSL フロー メッセージ(続き)
SSL フロー フラグ
SSL フロー フラグ(続き)


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL サーバ名
SSL フロー フラグ(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
SSL サーバ名...
SSL URL カテゴリ
SSL セッション ID
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID の長さ
SSL チケット ID
SSL チケット ID(続き)
SSL チケット ID(続き)
SSL チケット ID(続き)
SSL チケット ID(続き)
SSL チケット ID(続き)
SSL チケット ID の長さ
ネットワーク分析ポリシー リビジョン
ネットワーク分析ポリシー リビジョン(続き)
ネットワーク分析ポリシー リビジョン(続き)
ネットワーク分析ポリシー リビジョン(続き)
ネットワーク分析ポリシー リビジョン(続き)

次の表は、接続統計データ ブロック 5.4+のフィールドについての説明です。

表 B-35　接続統計データ ブロック 5.4+のフィールド

フィールド	データ タイプ	説明
接続統計データ ブロック タイプ	uint32	接続統計データ ブロック 5.4+を開始します。値は常に 157 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイスID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティ ゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティ ゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポンダ IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた相関イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アクション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポンダ ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケット タイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケット タイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。

表 B-35　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポンダ送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポンダ送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URLレピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロック タイプ	uint32	クライアント アプリケーション URL の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション URL の文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、およびクライアント アプリケーション URL 文字列のバイト数を含む)。
クライアント アプリケーション URL	string	クライアント アプリケーションがアクセスする URL(該当する場合) (`/files/index.html` など)。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション バージョンの文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
クライアント アプリケーション バージョン	string	クライアント アプリケーション バージョン。

表 B-35　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
モニタ ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタ ルールの ID。
モニタ ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタ ルールの ID。
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入イベント カウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポンダの国	uint 16	応答ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。
SNMP 出力	uint16	出力インターフェイスの SNMP インデックス
送信元 TOS	uint8	着信インターフェイス用のタイプ オブ サービス バイト設定。
宛先 TOS	uint8	発信インターフェイス用のタイプ オブ サービス バイト設定。
送信元マスク	uint8	送信元アドレス プレフィックス マスク。
宛先マスク	uint8	宛先アドレス プレフィックス マスク。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

表 B-35　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
VLAN ID	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
文字列ブロック タイプ	uint32	参照ホストを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	参照ホスト文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および参照ホスト フィールドのバイト数を含む)。
参照ホスト	string	HTTP または DNS で提供されるホスト名情報。
文字列ブロック タイプ	uint32	ユーザ エージェントを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ エージェント文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ エージェント フィールドのバイト数を含む)。
ユーザ エージェント	string	セッションのユーザ エージェント ヘッダー フィールドからの情報。
文字列ブロック タイプ	uint32	HTTP リファラを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	HTTP リファラ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および HTTP リファラ フィールドのバイト数を含む)。
HTTP リファラ	string	ページの発生元のサイト。これは HTTP トラフィック内の参照ヘッダー情報にあります。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
SSL ポリシー ID	uint8[16]	接続を処理した SSL ポリシーの ID 番号。
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルト アクションの ID 番号。
SSL 暗号スイート	uint16	SSL 接続で使用される暗号スイート。値は 10 進形式で保存されます。値により指定されている暗号スイートの詳細については、`www.iana.org/assignments/tls-parameters/tls-parameters.xhtml` を参照してください。
SSL バージョン	uint8	接続の暗号化に使用された SSL または TLS プロトコル バージョン。

表 B-35　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
SSL サーバ証明書ステータス	uint16	SSL 証明書のステータス。有効な値は次のとおりです。 • 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 • 1(不明):サーバ証明書のステータスは判別できませんでした。 • 2(有効):サーバ証明書は有効です。 • 4(自己署名済み):サーバ証明書は自己署名です。 • 16(無効な発行者):サーバ証明書に無効な発行者があります。 • 32(無効な署名):サーバ証明書に無効な署名があります。 • 64(期限切れ):サーバ証明書は期限切れです。 • 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 • 256(取り消し):サーバ証明書は取り消されました。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」
予期された SSL アクション	uint16	SSL ルールに基づいて接続に対して実行する必要があるアクション。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 B-35　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
SSL フロー ステータス	uint16	SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。 • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL フロー エラー	uint32	詳細な SSL エラー コード。これらの値はサポート目的で必要とされる場合があります。

表 B-35　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
SSL フロー メッセージ	uint32	SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。 • 0x00000001:NSE_MT__HELLO_REQUEST • 0x00000002:NSE_MT__CLIENT_ALERT • 0x00000004:NSE_MT__SERVER_ALERT • 0x00000008:NSE_MT__CLIENT_HELLO • 0x00000010:NSE_MT__SERVER_HELLO • 0x00000020:NSE_MT__SERVER_CERTIFICATE • 0x00000040:NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080:NSE_MT__CERTIFICATE_REQUEST • 0x00000100:NSE_MT__SERVER_HELLO_DONE • 0x00000200:NSE_MT__CLIENT_CERTIFICATE • 0x00000400:NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800:NSE_MT__CERTIFICATE_VERIFY • 0x00001000: NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000:NSE_MT__CLIENT_FINISHED • 0x00004000: NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000:NSE_MT__SERVER_FINISHED • 0x00010000:NSE_MT__NEW_SESSION_TICKET • 0x00020000:NSE_MT__HANDSHAKE_OTHER • 0x00040000:NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000:NSE_MT__APP_DATA_FROM_SERVER
SSL フロー フラグ	uint64	暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。 • 0x00000001(NSE_FLOW__VALID):他のフィールドを有効にするために設定する必要があります • 0x00000002(NSE_FLOW__INITIALIZED):内部構造が処理可能です • 0x00000004(NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました
文字列ブロック タイプ	uint32	SSL サーバ名を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-35　接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	SSL サーバ名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および SSL サーバ名フィールドのバイト数を含む)。
SSL サーバ名	string	SSL Client Hello でサーバ名に指定された名前。
SSL URL カテゴリ	uint32	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできます。
SSL チケット ID	uint8[20]	クライアントとサーバがセッション チケットの使用に同意する場合に使用されるセッション チケットのハッシュ。
SSL チケット ID の長さ	uint8	SSL チケット ID の長さ。チケット ID は 20 バイトより長くすることはできませんが、20 バイト未満であってもかまいません。
ネットワーク分析ポリシー リビジョン	uint8[16]	接続イベントに関連付けられているネットワーク分析ポリシーのリビジョン。

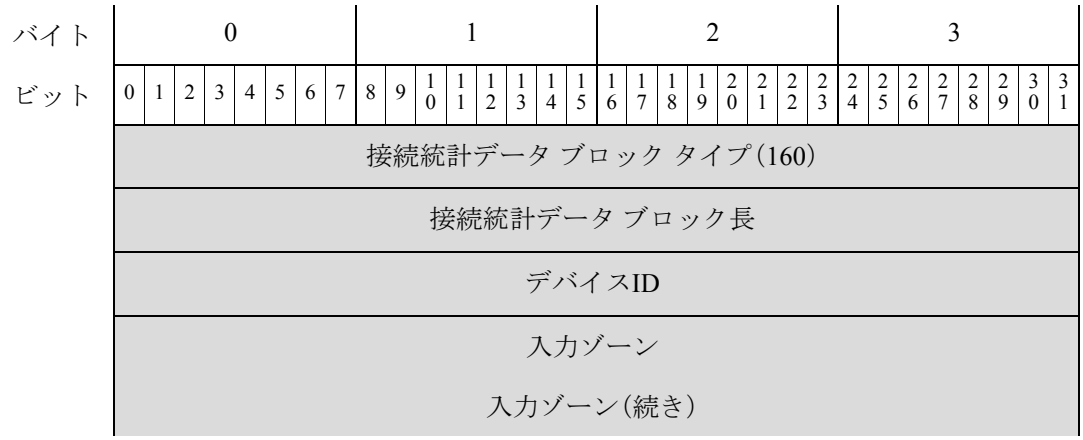
接続統計データ ブロック 6.0.x

接続統計データ ブロックは、接続データ メッセージで使用されます。接続統計データ ブロック 6.0 には、いくつかの新しいフィールドが追加されました。ISE 統合および複数ネットワーク マップをサポートするために、フィールドが追加されました。バージョン 6.0.x の接続統計データ ブロックは、シリーズ 1 グループのブロックの、ブロック タイプ 160 です。これはブロック タイプ 157(接続統計データ ブロック 5.4.1(B-183 ページ))に取って代わります。DNS ルックアップとセキュリティ インテリジェンスをサポートするため新しいフィールドを追加しました。

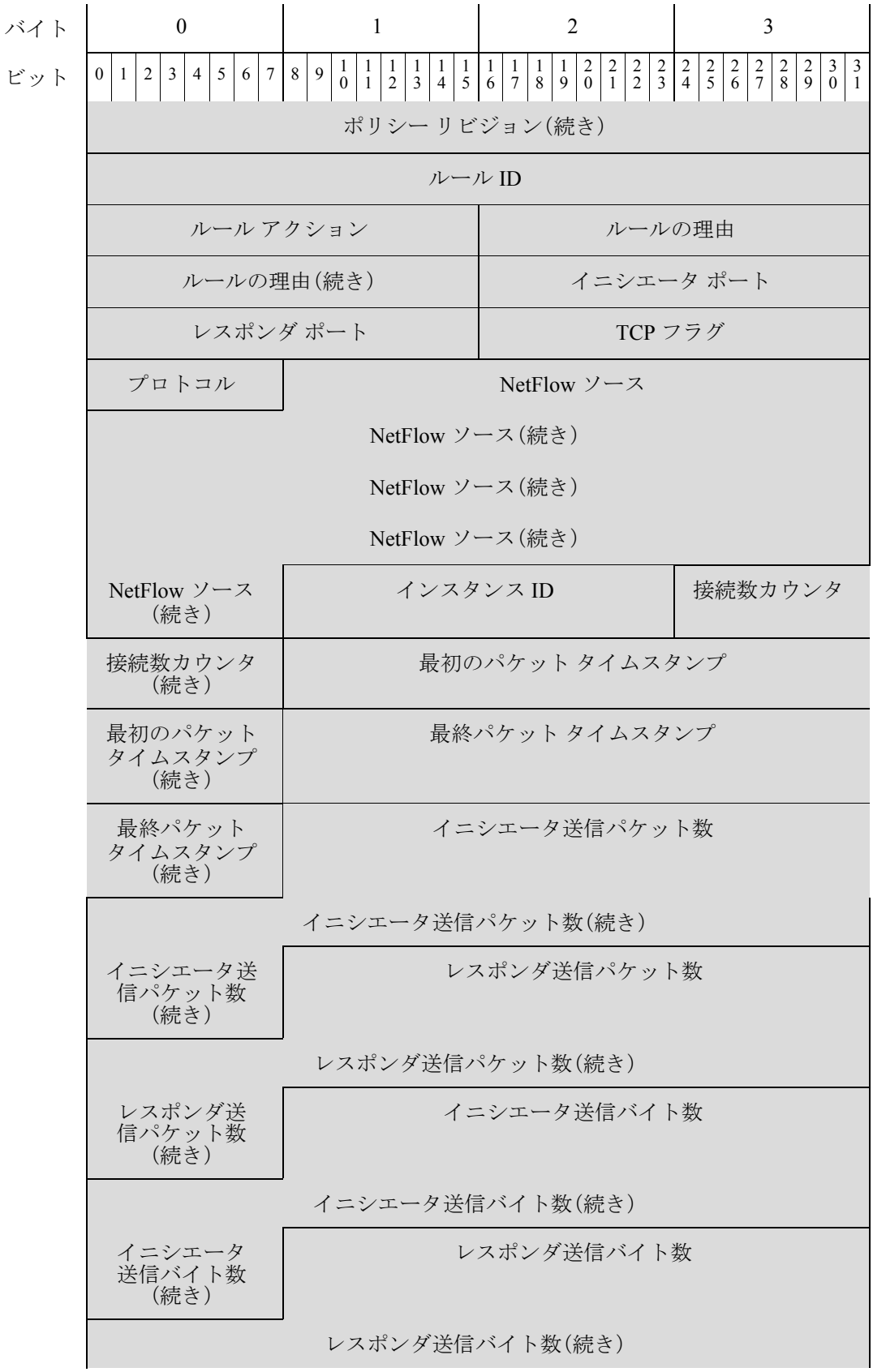
接続イベント レコードは、要求メッセージにイベント バージョン 14 とイベント コード 71 とともに拡張イベント フラグを設定して要求します。要求フラグ(2-12 ページ)を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

次の図は、接続統計データ ブロック 6.0.x の形式を示しています。

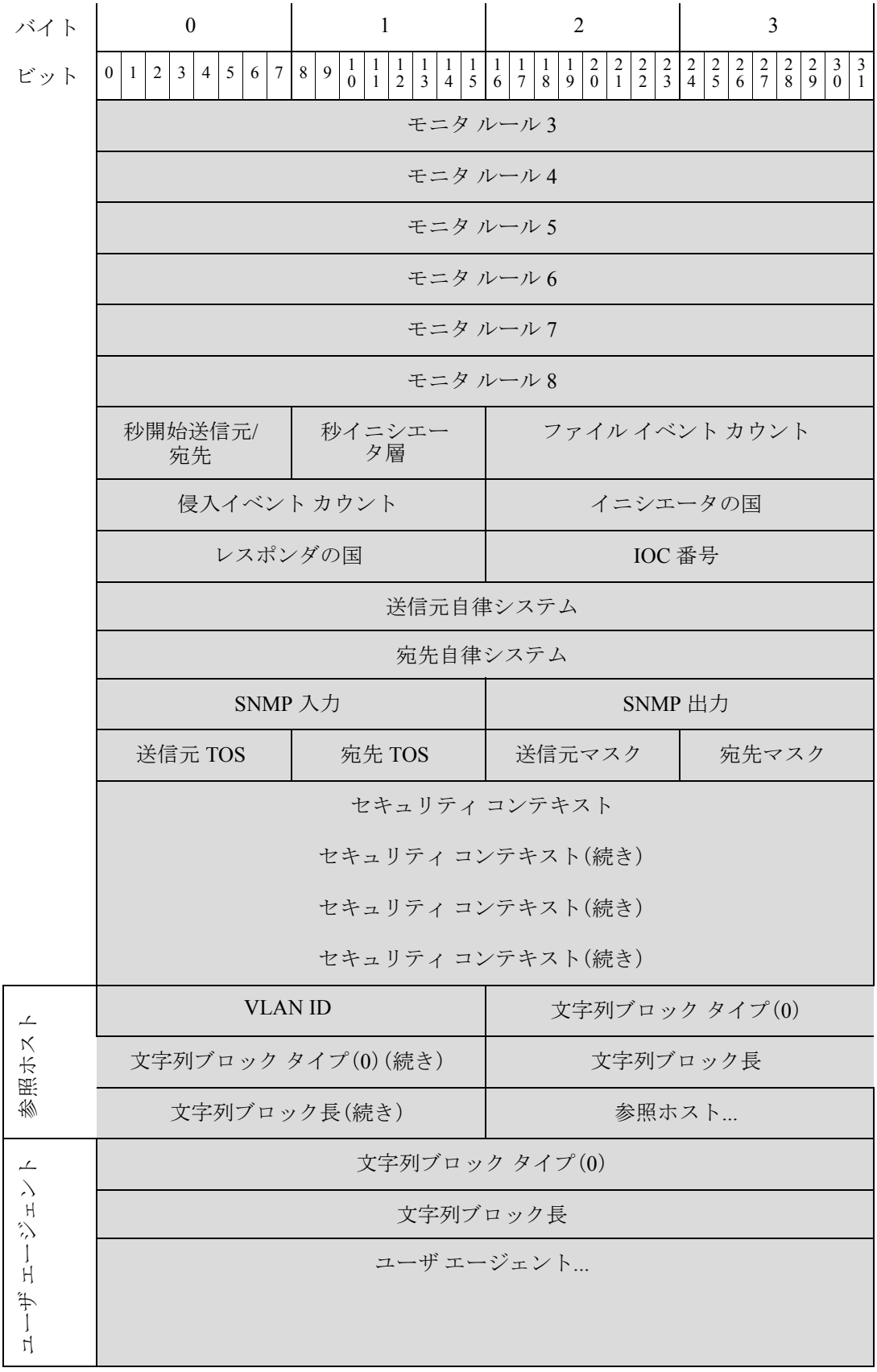
7



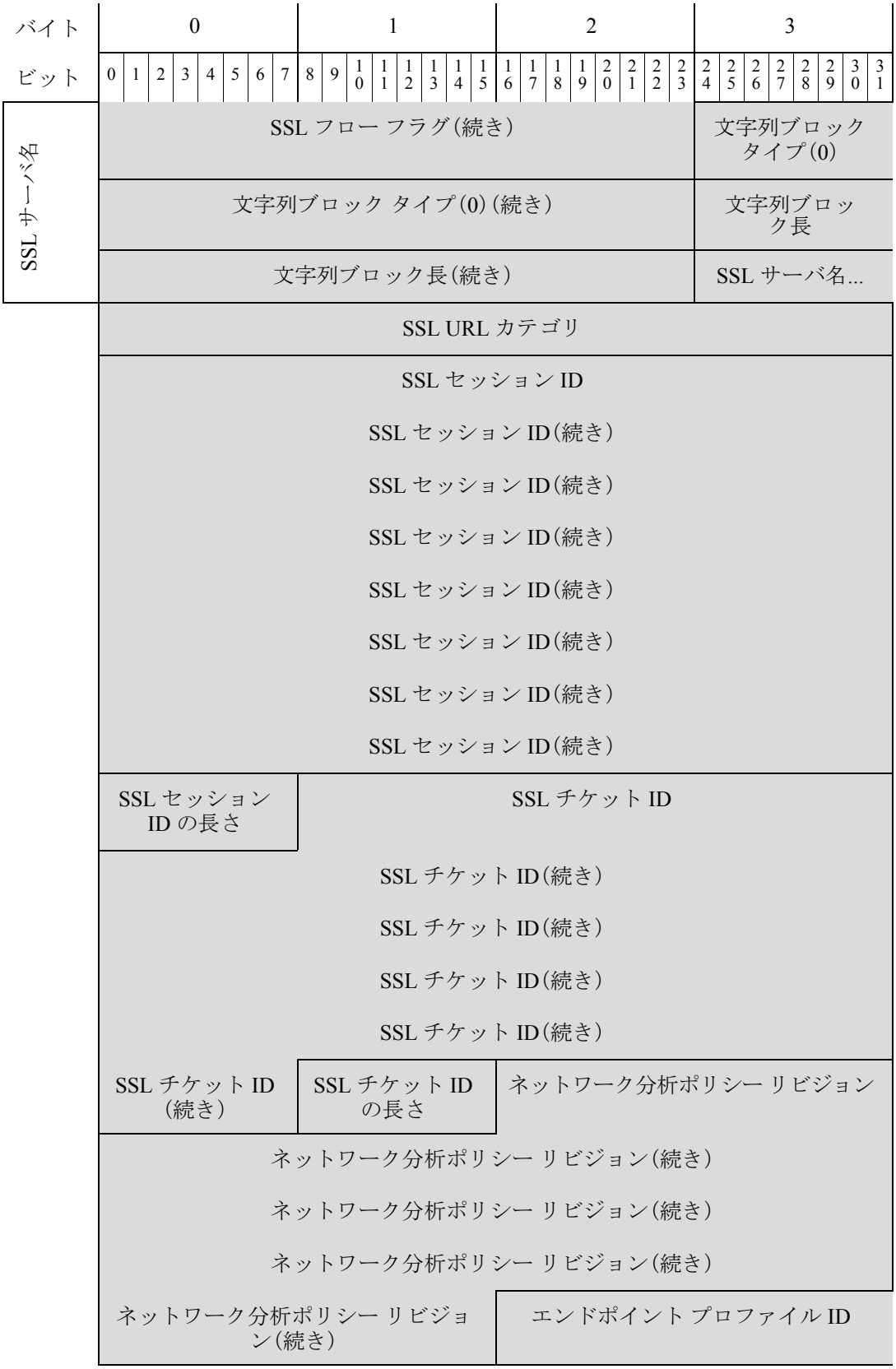
バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
入力ゾーン(続き)																																
入力ゾーン(続き)																																
出力ゾーン																																
出力ゾーン(続き)																																
出力ゾーン(続き)																																
出力ゾーン(続き)																																
入力インターフェイス																																
入力インターフェイス(続き)																																
入力インターフェイス(続き)																																
入力インターフェイス(続き)																																
出力インターフェイス																																
出力インターフェイス(続き)																																
出力インターフェイス(続き)																																
出力インターフェイス(続き)																																
イニシエータ IP アドレス																																
イニシエータ IP アドレス(続き)																																
イニシエータ IP アドレス(続き)																																
イニシエータ IP アドレス(続き)																																
レスポンダ IP アドレス																																
レスポンダ IP アドレス(続き)																																
レスポンダ IP アドレス(続き)																																
レスポンダ IP アドレス(続き)																																
ポリシー リビジョン																																
ポリシー リビジョン(続き)																																
ポリシー リビジョン(続き)																																

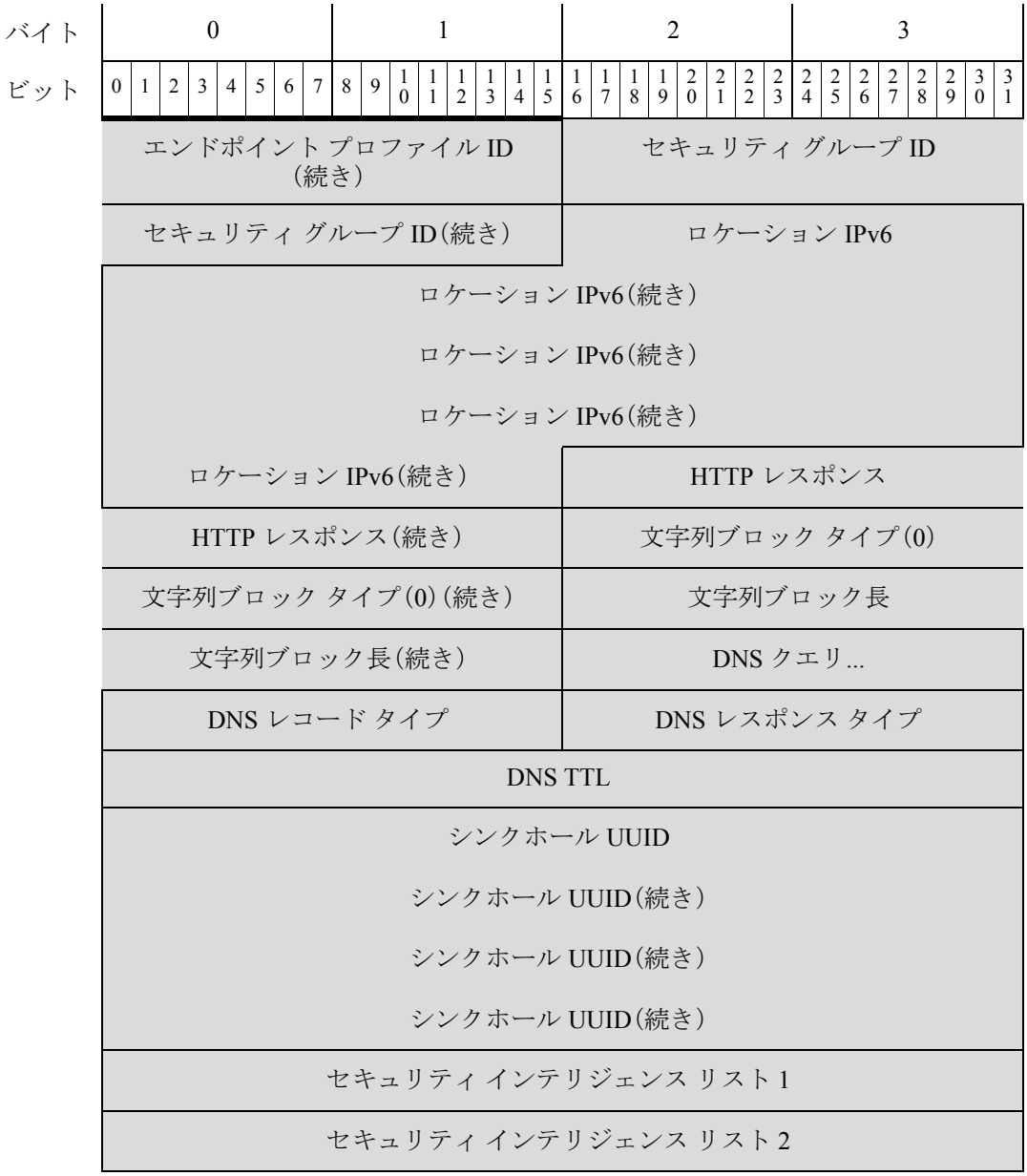

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
ポリシー リビジョン(続き)
ルール ID
ルール アクション
ルールの理由
ルールの理由(続き)
イニシエータ ポート
レスポンダ ポート
TCP フラグ
プロトコル
NetFlow ソース
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
インスタンス ID
接続数カウンタ
接続数カウンタ(続き)
最初のパケット タイムスタンプ
最初のパケット タイムスタンプ(続き)
最終パケット タイムスタンプ
最終パケット タイムスタンプ(続き)
イニシエータ送信パケット数
イニシエータ送信パケット数(続き)
レスポンダ送信パケット数
レスポンダ送信パケット数(続き)
レスポンダ送信パケット数(続き)
イニシエータ送信バイト数
イニシエータ送信バイト数(続き)
イニシエータ送信バイト数(続き)
レスポンダ送信バイト数
レスポンダ送信バイト数(続き)


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7
8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23
24 25 26 27 28 29 30 31
レスポンダ送信バイト数(続き)
ユーザ ID
ユーザ ID(続き)
アプリケーション プロトコル ID
アプリケーション プロトコル ID(続き)
URL カテゴリ
URL カテゴリ(続き)
URLレピュテーション
URL レピュテーション(続き)
クライアント アプリケーション ID
クライアント アプリケーション ID(続き)
Web アプリケーション ID
クライアント URL
Web アプリケーション ID(続き)
Stringブロック タイプ(0)
文字列ブロック タイプ(続き)
文字列ブロック長
文字列ブロック長(続き)
クライアント アプリケーションURL...
NetBIOS 名
文字列ブロック タイプ(0)
文字列ブロック長
NetBIOS 名...
クライアント アプリケーション バージョン
文字列ブロック タイプ(0)
文字列ブロック長
クライアント アプリケーション バージョン...
モニタ ルール 1
モニタ ルール 2


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
モニタ ルール 3
モニタ ルール 4
モニタ ルール 5
モニタ ルール 6
モニタ ルール 7
モニタ ルール 8
秒開始送信元/宛先
秒イニシエータ層
ファイル イベント カウント
侵入イベント カウント
イニシエータの国
レスポンダの国
IOC 番号
送信元自律システム
宛先自律システム
SNMP 入力
SNMP 出力
送信元 TOS
宛先 TOS
送信元マスク
宛先マスク
セキュリティ コンテキスト
セキュリティ コンテキスト(続き)
セキュリティ コンテキスト(続き)
セキュリティ コンテキスト(続き)
参照ホスト
VLAN ID
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
参照ホスト...
ユーザ エージェント
文字列ブロック タイプ(0)
文字列ブロック長
ユーザ エージェント...


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
HTTP リファラ
文字列ブロック タイプ(0)
文字列ブロック長
HTTP リファラ...
SSL 証明書フィンガープリント
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL ポリシー ID
SSL ポリシー ID(続き)
SSL ポリシー ID(続き)
SSL ポリシー ID(続き)
SSL ルール ID
SSL 暗号スイート
SSL バージョン
SSL キー証明書統計
SSL キー証明書統計(続き)
実際の SSL アクション
予期された SSL アクション
予期された SSL アクション(続き)
SSL フロー ステータス
SSL フロー エラー
SSL フロー エラー(続き)
SSL フロー メッセージ
SSL フロー メッセージ(続き)
SSL フロー フラグ
SSL フロー フラグ(続き)


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL サーバ名
SSL フロー フラグ(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
SSL サーバ名...
SSL URL カテゴリ
SSL セッション ID
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID の長さ
SSL チケット ID
SSL チケット ID(続き)
SSL チケット ID(続き)
SSL チケット ID(続き)
SSL チケット ID(続き)
SSL チケット ID (続き)
SSL チケット ID の長さ
ネットワーク分析ポリシー リビジョン
ネットワーク分析ポリシー リビジョン(続き)
ネットワーク分析ポリシー リビジョン(続き)
ネットワーク分析ポリシー リビジョン(続き)
ネットワーク分析ポリシー リビジョン(続き)
エンドポイント プロファイル ID



次の表は、接続統計データ ブロック 6.0.x のフィールドについての説明です。

表 B-36　　接続統計データ ブロック 6.0.x のフィールド

フィールド	データ タイプ	説明
接続統計データ ブロック タイプ	uint32	接続統計データ ブロック 6.0+を開始します。値は常に 160 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数（接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む）。

表 B-36　接続統計データ ブロック 6.0.x のフィールド(続き)

フィールド	データ タイプ	説明
デバイスID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティ ゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティ ゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポンダ IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた相関イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アクション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint32	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポンダ ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケット タイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケット タイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポンダ送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。

表 B-36　接続統計データ ブロック 6.0.x のフィールド(続き)

フィールド	データ タイプ	説明
レスポンダ送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URL レピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロック タイプ	uint32	クライアント アプリケーション URL の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション URL の文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、およびクライアント アプリケーション URL 文字列のバイト数を含む)。
クライアント アプリケーション URL	string	クライアント アプリケーションがアクセスする URL(該当する場合) (`/files/index.html` など)。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション バージョンの文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
クライアント アプリケーション バージョン	string	クライアント アプリケーション バージョン。
モニタ ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタ ルールの ID。
モニタ ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタ ルールの ID。
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。

表 B-36　接続統計データ ブロック 6.0.x のフィールド(続き)

フィールド	データ タイプ	説明
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入イベント カウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポンダの国	uint 16	応答ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。
SNMP 出力	uint16	出力インターフェイスの SNMP インデックス
送信元 TOS	uint8	着信インターフェイス用のタイプ オブ サービス バイト設定。
宛先 TOS	uint8	発信インターフェイス用のタイプ オブ サービス バイト設定。
送信元マスク	uint8	送信元アドレス プレフィックス マスク。
宛先マスク	uint8	宛先アドレス プレフィックス マスク。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
VLAN ID	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
文字列ブロック タイプ	uint32	参照ホストを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	参照ホスト文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および参照ホスト フィールドのバイト数を含む)。

表 B-36　接続統計データ ブロック 6.0.x のフィールド(続き)

フィールド	データ タイプ	説明
参照ホスト	string	HTTP または DNS で提供されるホスト名情報。
文字列ブロック タイプ	uint32	ユーザ エージェントを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ エージェント文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ エージェント フィールドのバイト数を含む)。
ユーザ エージェント	string	セッションのユーザ エージェント ヘッダー フィールドからの情報。
文字列ブロック タイプ	uint32	HTTP リファラを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	HTTP リファラ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および HTTP リファラ フィールドのバイト数を含む)。
HTTP リファラ	string	ページの発生元のサイト。これは HTTP トラフィック内の参照ヘッダー情報にあります。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
SSL ポリシー ID	uint8[16]	接続を処理した SSL ポリシーの ID 番号。
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルト アクションの ID 番号。
SSL 暗号スイート	uint16	SSL 接続で使用される暗号スイート。値は 10 進形式で保存されます。値により指定されている暗号スイートの詳細については、www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
SSL バージョン	uint8	接続の暗号化に使用された SSL または TLS プロトコル バージョン。

表 B-36　接続統計データ ブロック 6.0.x のフィールド(続き)

フィールド	データ タイプ	説明
SSL サーバ証明書ステータス	uint16	SSL 証明書のステータス。有効な値は次のとおりです。 • 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 • 1(不明):サーバ証明書のステータスは判別できませんでした。 • 2(有効):サーバ証明書は有効です。 • 4(自己署名済み):サーバ証明書は自己署名です。 • 16(無効な発行者):サーバ証明書に無効な発行者があります。 • 32(無効な署名):サーバ証明書に無効な署名があります。 • 64(期限切れ):サーバ証明書は期限切れです。 • 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 • 256(取り消し):サーバ証明書は取り消されました。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」
予期された SSL アクション	uint16	SSL ルールに基づいて接続に対して実行する必要があるアクション。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 B-36　接続統計データ ブロック 6.0.x のフィールド(続き)

フィールド	データ タイプ	説明
SSL フロー ステータス	uint16	SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。 • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL フロー エラー	uint32	詳細な SSL エラー コード。これらの値はサポート目的で必要とされる場合があります。

表 B-36　接続統計データ ブロック 6.0.x のフィールド(続き)

フィールド	データ タイプ	説明
SSL フロー メッセージ	uint32	SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。 • 0x00000001:NSE_MT__HELLO_REQUEST • 0x00000002:NSE_MT__CLIENT_ALERT • 0x00000004:NSE_MT__SERVER_ALERT • 0x00000008:NSE_MT__CLIENT_HELLO • 0x00000010:NSE_MT__SERVER_HELLO • 0x00000020:NSE_MT__SERVER_CERTIFICATE • 0x00000040:NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080:NSE_MT__CERTIFICATE_REQUEST • 0x00000100:NSE_MT__SERVER_HELLO_DONE • 0x00000200:NSE_MT__CLIENT_CERTIFICATE • 0x00000400:NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800:NSE_MT__CERTIFICATE_VERIFY • 0x00001000: NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000:NSE_MT__CLIENT_FINISHED • 0x00004000: NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000:NSE_MT__SERVER_FINISHED • 0x00010000:NSE_MT__NEW_SESSION_TICKET • 0x00020000:NSE_MT__HANDSHAKE_OTHER • 0x00040000:NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000:NSE_MT__APP_DATA_FROM_SERVER
SSL フロー フラグ	uint64	暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。 • 0x00000001(NSE_FLOW__VALID):他のフィールドを有効にするために設定する必要があります • 0x00000002(NSE_FLOW__INITIALIZED):内部構造が処理可能です • 0x00000004(NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました
文字列ブロック タイプ	uint32	SSL サーバ名を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-36　接続統計データ ブロック 6.0.x のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	SSL サーバ名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および SSL サーバ名フィールドのバイト数を含む)。
SSL サーバ名	string	SSL Client Hello でサーバ名に指定された名前。
SSL URL カテゴリ	uint32	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできます。
SSL チケット ID	uint8[20]	クライアントとサーバがセッション チケットの使用に同意する場合に使用されるセッション チケットのハッシュ。
SSL チケット ID の長さ	uint8	SSL チケット ID の長さ。チケット ID は 20 バイトより長くすることはできませんが、20 バイト未満であってもかまいません。
ネットワーク分析ポリシー リビジョン	uint8[16]	接続イベントに関連付けられているネットワーク分析ポリシーのリビジョン。
エンドポイント プロファイル ID	uint32	ISE により識別される、接続エンドポイントで使用されるデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
セキュリティ グループ ID	uint32	ポリシーに基づいて ISE によりユーザに割り当てられた ID 番号。
ロケーション IPv6	uint8[16]	ISE と通信するインターフェイスの IP アドレス。IPv4 または IPv6 のアドレスを使用できます。
HTTP レスポンス	uint32	HTTP 要求の応答コード。
文字列ブロック タイプ	uint32	DNS クエリを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、および DNS クエリ文字列のバイト数を含む)。
DNS クエリ	string	DNS サーバに送信されたクエリの内容。
DNS レコード タイプ	uint16	DNS レコード タイプの数値。

表 B-36　接続統計データ ブロック 6.0.x のフィールド(続き)

フィールド	データ タイプ	説明
DNS レスポンス タイプ	uint16	0(NoError):エラーなし 1(FormErr):フォーマット エラー 2(ServFail):サーバ障害 3(NXDomain):存在していないドメイン 4(NotImp):未実装 5(Refused):クエリ拒否 6(YXDomain):名前が存在してはならない状況で存在している 7(YXRRSet):RR セットが存在してはならない状況で存在している 8(NXRRSet):存在しているべき RR セットが存在していない 9(NotAuth):未承認 10(NotZone):名前がゾーンに含まれていない 16(BADSIG):TSIG 署名失敗 17(BADKEY):キーが認識されない 18(BADTIME):時間範囲外の署名 19(BADMODE):不適切な TKEY モード 20(BADNAME):重複するキー名 21(BADALG):サポートされていないアルゴリズム 22(BADTRUNC):不適切な切り捨て 3841(NXDOMAIN):ファイアウォールからの NXDOMAIN 応答 3842(SINKHOLE):ファイアウォールからのシンクホール応答
DNS TTL	uint32	DNS レスポンスの存続期間(秒単位)。
シンクホール UUID	uin8[16]	このシンクホール オブジェクトに関連付けられているリビジョン UUID。
セキュリティ インテリジェンス リスト 1	uint32	イベントに関連付けられているセキュリティ インテリジェンス リスト。これは、関連メタデータのセキュリティ インテリジェンス リストにマップされます。接続には、2 つのセキュリティ インテリジェンス リストが関連付けられている場合があります。
セキュリティ インテリジェンス リスト 2	uint32	イベントに関連付けられているセキュリティ インテリジェンス リスト。これは、関連メタデータのセキュリティ インテリジェンス リストにマップされます。接続には、2 つのセキュリティ インテリジェンス リストが関連付けられている場合があります。

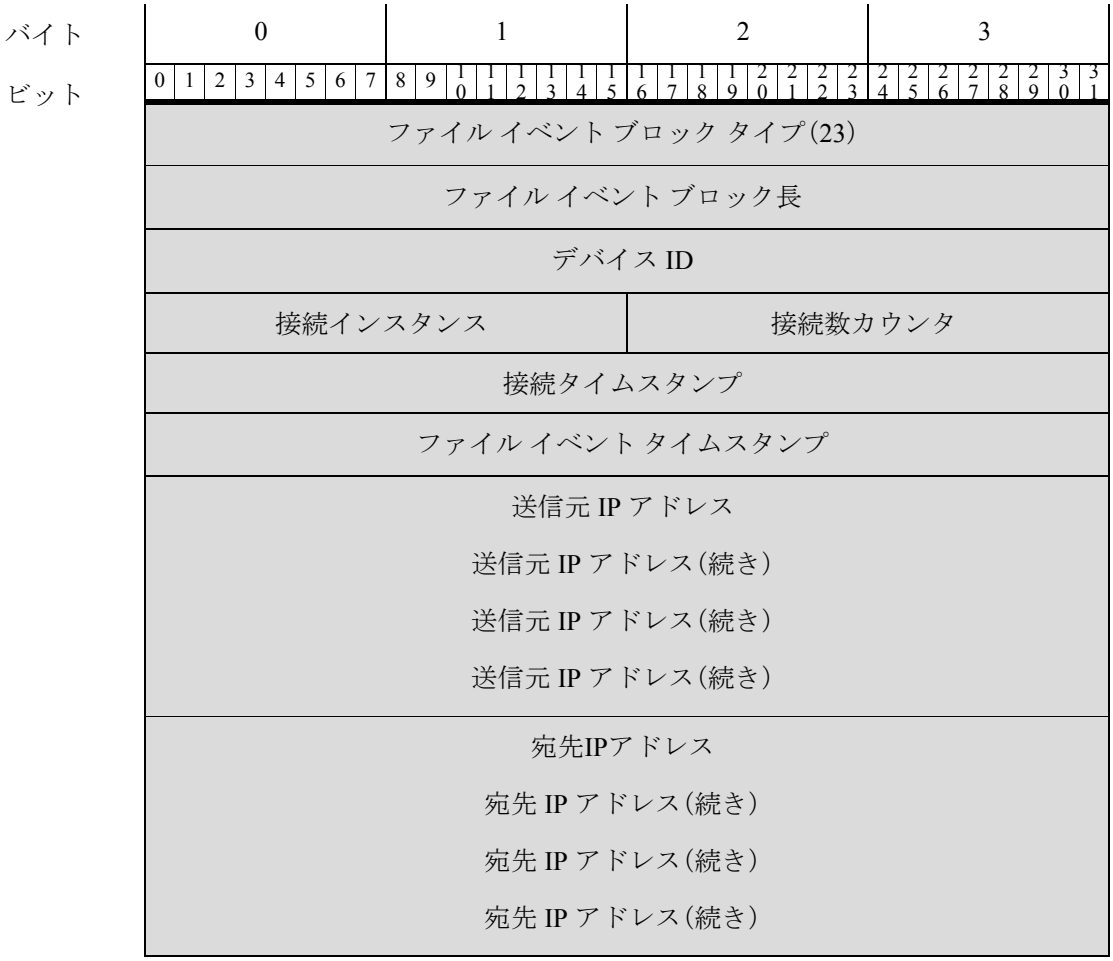
レガシー ファイル イベントのデータ構造

続くいくつかのトピックでは、他のレガシー ファイル イベント データの構造について説明します。

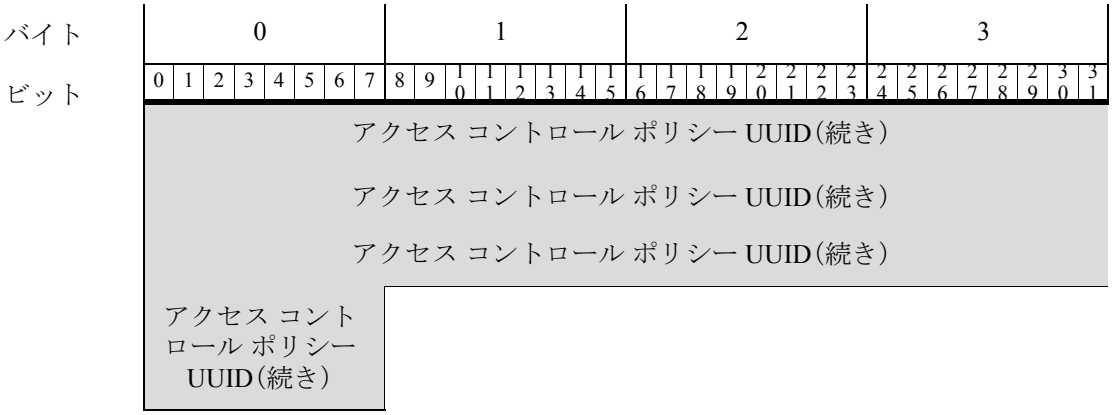
ファイル イベント 5.1.1.x

ファイル イベントには、ネットワークを介して送信されるファイルに関する情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントのブロック タイプは、シリーズ 2 グループのブロックの、ブロック タイプ 23 です。

次の図は、ファイル イベント データ ブロックの構造を示しています。




バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
傾向
操作
SHA ハッシュ
SHA ハッシュ(続き)
SHA ハッシュ(続き)
SHA ハッシュ(続き)
SHA ハッシュ(続き)
SHA ハッシュ(続き)
SHA ハッシュ(続き)
SHA ハッシュ(続き)
ファイル タイプ ID
ファイル名
ファイル タイプ ID(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
ファイル名...
ファイル サイズ
ファイル サイズ(続き)
方向
アプリケーション ID
アプリケーション ID(続き)
ユーザ ID
URI
ユーザ ID(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
URI...
シグネチャ
文字列ブロック タイプ(0)
文字列ブロック長
署名...
送信元ポート
接続先ポート
プロトコル
アクセス コントロール ポリシー UUID



次の表は、ファイル イベント データ ブロックのフィールドについての説明です。

表 B-37　　ファイル イベント データ ブロックのフィールド

フィールド	データ タイプ	説明
ファイル イベント ブロック タイプ	uint32	ファイル イベント データ ブロックを開始します。この値は常に 23 です。
ファイル イベント ブロック長	uint32	ファイル イベント ブロックのバイトの合計数(ファイル イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または侵入イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続タイムスタンプ	uint32	関連する接続イベントの UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
ファイル イベント タイムスタンプ	uint32	ファイル タイプが識別されてファイル イベントが生成されたときの UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。

表 B-37　ファイル イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4(CACHE_MISS):ソフトウェアは Cisco クラウドに特性を確認する要求を送信できませんでした。 • 5(NO_CLOUD_RESP):Cisco クラウド サービスが要求に応答しませんでした。
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
ファイル タイプ ID	uint32	ファイル タイプにマップされている ID 番号。
ファイル名	string	ファイルの名前。
ファイル サイズ	uint64	ファイルのサイズ(バイト単位)。
方向	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示す値。次のいずれかの値になります。 • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
アプリケーション ID	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
URI	string	接続の Uniform Resource Identifier(URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。

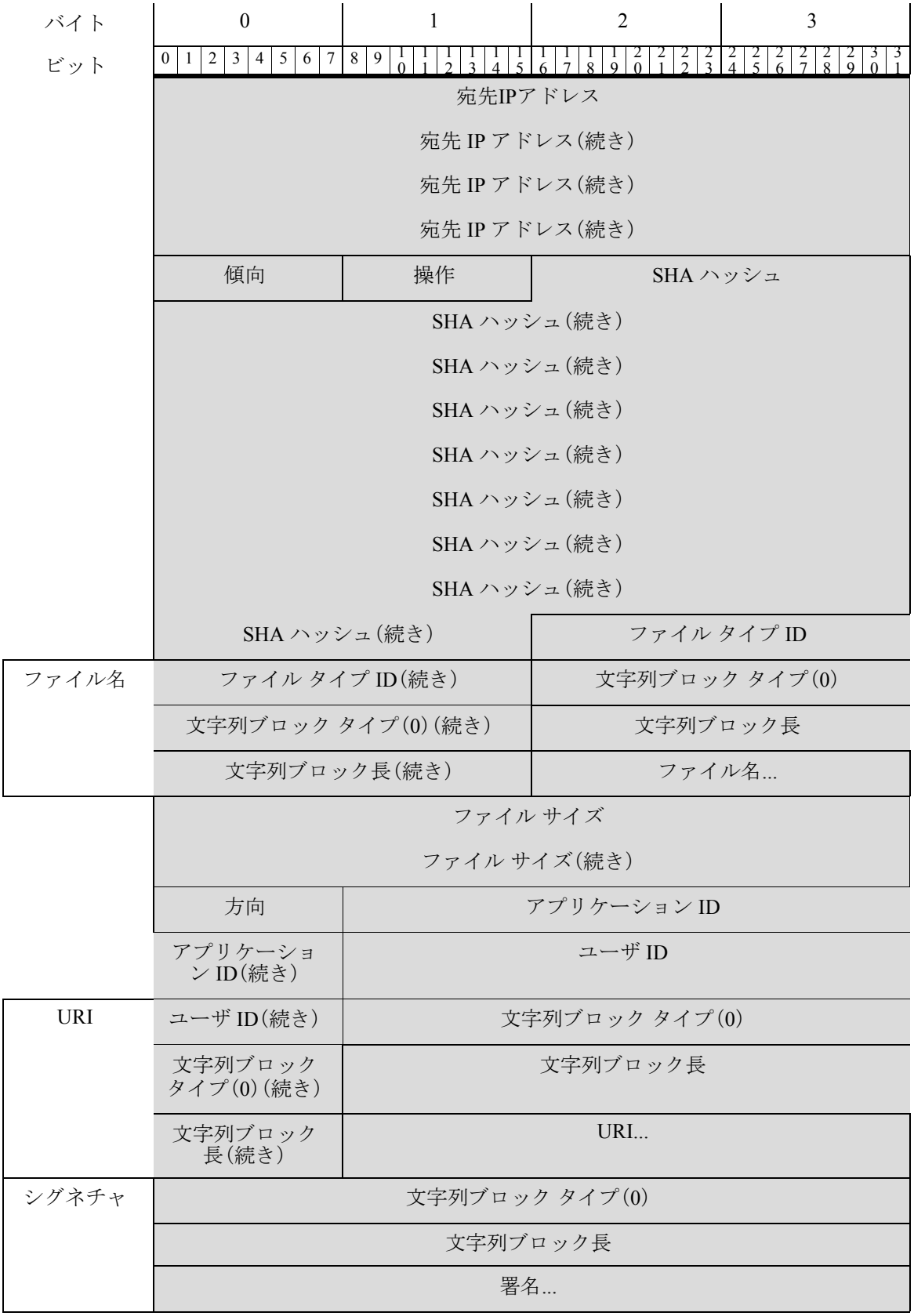
表 B-37　　ファイル イベント データ ブロックのフィールド(続き)

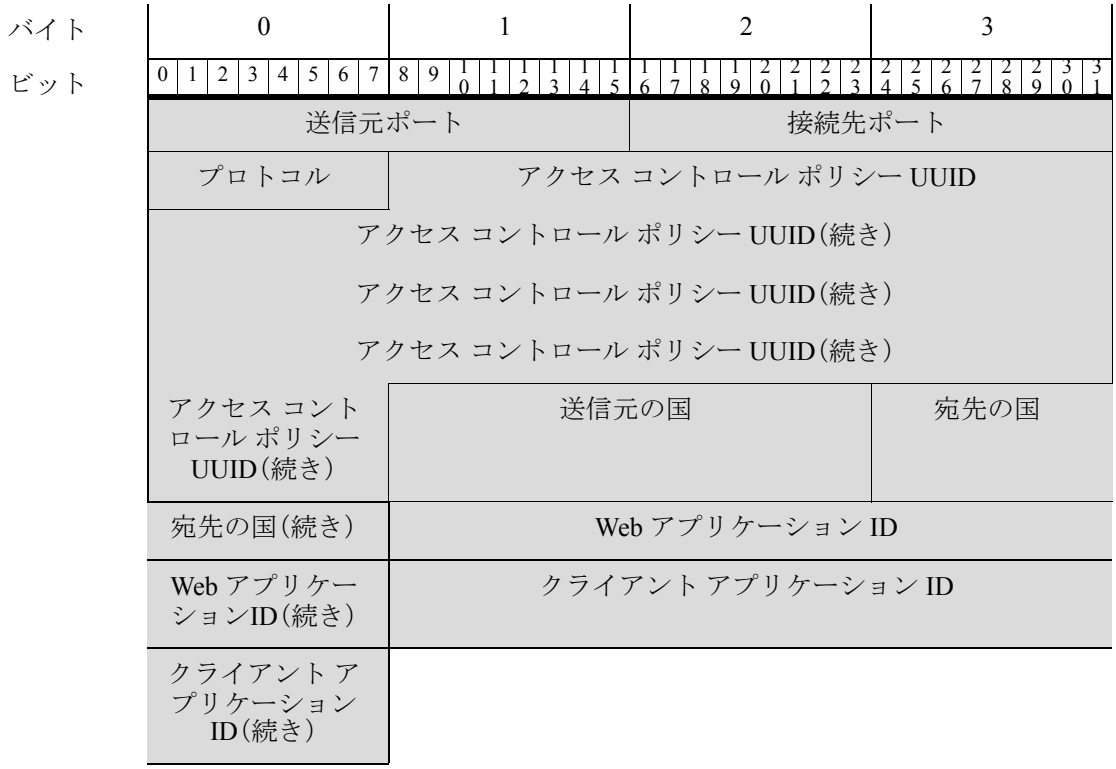
フィールド	データ タイプ	説明
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。

ファイル イベント 5.2.x

ファイル イベントには、ネットワークを介して送信されるファイルに関する情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントのブロック タイプは、シリーズ 2 グループのブロックの、ブロック タイプ 32 です。これはブロック タイプ 23 に取って代わります。送信元と宛先の国、およびクライアントと Web アプリケーション インスタンスを追跡するために、新しいフィールドが追加されました。

次の図は、ファイル イベント データ ブロックの構造を示しています。


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
宛先IPアドレス
宛先 IP アドレス(続き)
宛先 IP アドレス(続き)
宛先 IP アドレス(続き)
傾向
操作
SHA ハッシュ
SHA ハッシュ(続き)
SHA ハッシュ(続き)
SHA ハッシュ(続き)
SHA ハッシュ(続き)
SHA ハッシュ(続き)
SHA ハッシュ(続き)
SHA ハッシュ(続き)
SHA ハッシュ(続き)
ファイル タイプ ID
ファイル名
ファイル タイプ ID(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
ファイル名...
ファイル サイズ
ファイル サイズ(続き)
方向
アプリケーション ID
アプリケーション ID(続き)
ユーザ ID
URI
ユーザ ID(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
URI...
シグネチャ
文字列ブロック タイプ(0)
文字列ブロック長
署名...



次の表は、ファイル イベント データ ブロックのフィールドについての説明です。

表 B-38　　ファイル イベント データ ブロックのフィールド

フィールド	データ タイプ	説明
ファイルイベント ブロック タイプ	uint32	ファイル イベント データ ブロックを開始します。この値は常に 23 です。
ファイルイベント ブロック長	uint32	ファイル イベント ブロックのバイトの合計数(ファイル イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または侵入イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続タイムスタンプ	uint32	関連する接続イベントの UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
ファイルイベント タイムスタンプ	uint32	ファイル タイプが識別されてファイル イベントが生成されたときの UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。

表 B-38　ファイル イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(NEUTRAL):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4(CACHE_MISS):ソフトウェアから Cisco クラウドに対して、特性を確認する要求を送信できなかったか、または Cisco クラウド サービスが要求に応答しませんでした。
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
ファイル タイプ ID	uint32	ファイル タイプにマップされている ID 番号。
ファイル名	string	ファイルの名前。
ファイル サイズ	uint64	ファイルのサイズ(バイト単位)。
方向	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示す値。次のいずれかの値になります。 • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
アプリケーション ID	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
URI	string	接続の Uniform Resource Identifier(URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。

表 B-38　ファイル イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。

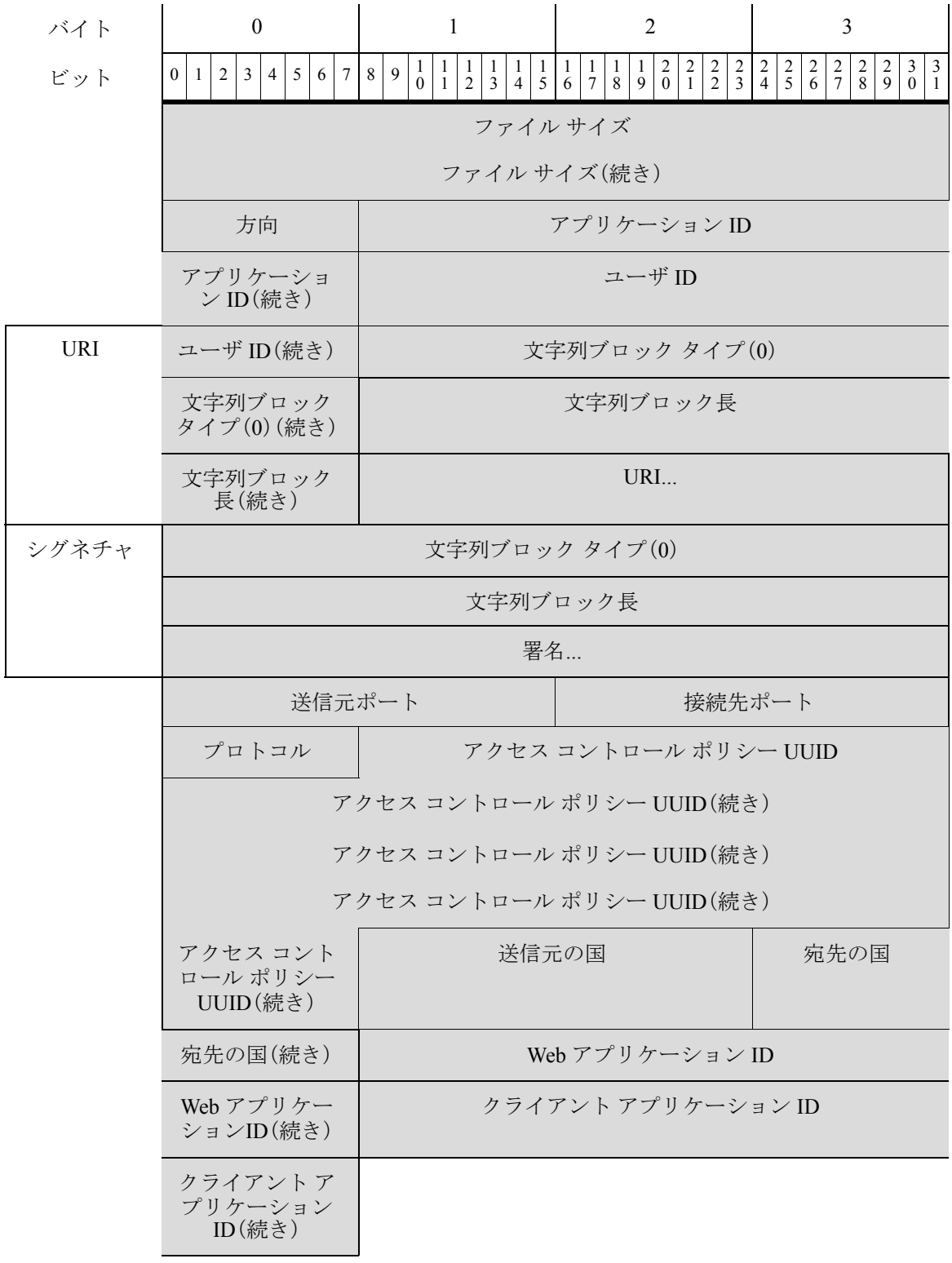
ファイル イベント 5.3

ファイル イベントには、ネットワークを介して送信されるファイルに関する情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントのブロック タイプは、シリーズ 2 グループのブロックの、ブロック タイプ 38 です。これはブロック タイプ 32 に取って代わります。新しいフィールドは、ダイナミック ファイル分析とファイル ストレージを追跡するために追加されました。

ファイル イベント レコードを要求するには、イベント バージョン 3 およびイベント コード 111 の要求メッセージ内に、ファイル イベント フラグ(要求フラグ フィールドのビット 30)を設定します。要求フラグ(2-12 ページ)を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

次の図は、ファイル イベント データ ブロックの構造を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続タイムスタンプ																																
ファイル イベント タイムスタンプ																																
送信元 IP アドレス 送信元 IP アドレス(続き) 送信元 IP アドレス(続き) 送信元 IP アドレス(続き)																																
宛先IPアドレス 宛先 IP アドレス(続き) 宛先 IP アドレス(続き) 宛先 IP アドレス(続き)																																
傾向									SPERO 解析結果								ファイル ストレージ ステータス								ファイル分析ステータス							
アーカイブ ファイル ステータス									脅威スコア								操作								SHA ハッシュ							
SHA ハッシュ(続き) SHA ハッシュ(続き) SHA ハッシュ(続き) SHA ハッシュ(続き) SHA ハッシュ(続き) SHA ハッシュ(続き) SHA ハッシュ(続き)																																
SHA ハッシュ(続き)																									ファイル タイプ ID							
ファイル名	ファイル タイプ ID(続き)																								文字列ブロック タイプ(0)							
	文字列ブロック タイプ(0)(続き)																								文字列ブロック長							
	文字列ブロック長(続き)																								ファイル名...							


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
ファイル サイズ
ファイル サイズ(続き)
方向
アプリケーション ID
アプリケーション ID(続き)
ユーザ ID
URI
ユーザ ID(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
URI...
シグネチャ
文字列ブロック タイプ(0)
文字列ブロック長
署名...
送信元ポート
接続先ポート
プロトコル
アクセス コントロール ポリシー UUID
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
送信元の国
宛先の国
宛先の国(続き)
Web アプリケーション ID
Web アプリケーションID(続き)
クライアント アプリケーション ID
クライアント アプリケーション ID(続き)

次の表は、ファイル イベント データ ブロックのフィールドについての説明です。

表 B-39　ファイル イベント データ ブロックのフィールド

フィールド	データ タイプ	説明
ファイル イベント ブロック タイプ	uint32	ファイル イベント データ ブロックを開始します。この値は常に 23 です。
ファイル イベント ブロック長	uint32	ファイル イベント ブロックのバイトの合計数(ファイル イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または侵入イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続タイムスタンプ	uint32	関連する接続イベントの UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
ファイル イベント タイムスタンプ	uint32	ファイル タイプが識別されてファイル イベントが生成されたときの UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4(UNAVAILABLE):ソフトウェアから Cisco クラウドに対して、特性を確認する要求を送信できなかったか、または Cisco クラウド サービスが要求に応答しませんでした。 • 5(CUSTOM SIGNATURE):ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
SPERO 解析結果	uint8	SPERO 署名がファイル分析で使用されたかどうかを示します。値が 1、2、または 3 であれば、SPERO 分析は使用されました。それ以外の値であれば、SPERO 分析は使用されませんでした。

表 B-39　ファイル イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
ファイル ストレージ ステータス	uint8	ファイルの保存ステータス。値は以下のとおりです。 • 1:ファイルが保存されました • 2:ファイルが保存されました • 3:ファイルを保存できません • 4:ファイルを保存できません • 5:ファイルを保存できません • 6:ファイルを保存できません • 7:ファイルを保存できません • 8:ファイル サイズが大きすぎます • 9:ファイル サイズが小さすぎます • 10:ファイルを保存できません • 11:ファイルは保存されておらず、解析結果を入手できません

表 B-39　ファイル イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
ファイル分析ステータス	uint8	ファイルが動的分析のために送信されているかどうかを示します。値は以下のとおりです。 • 0:ファイルが分析のために送信されていません • 1:分析のために送信されました • 2:分析のために送信されました • 4:分析のために送信されました • 5:送信に失敗しました • 6:送信に失敗しました • 7:送信に失敗しました • 8:送信に失敗しました • 9:ファイル サイズが小さすぎます • 10:ファイル サイズが大きすぎます • 11:分析のために送信されました • 12:分析が完了しました • 13:失敗(ネットワークの問題) • 14:失敗(レート制限) • 15:失敗(ファイルが大きすぎます) • 16:失敗(ファイルの読み取りエラー) • 17:失敗(内部ライブラリ エラー) • 19:ファイルは送信されておらず、解析結果を入手できません • 20:失敗(ファイルを実行できません) • 21:失敗(分析タイムアウト) • 22:分析のために送信されました • 23:サポートされていないファイル
アーカイブ ファイル ステータス	uint8	この値は常に 0 です。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ～ 100)。
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。

表 B-39　ファイル イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
ファイル タイプ ID	uint32	ファイル タイプにマップされている ID 番号。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、AMP for Endpoints ファイル タイプのメタデータ (3-44 ページ) を参照してください。
ファイル名	string	ファイルの名前。
ファイル サイズ	uint64	ファイルのサイズ(バイト単位)。
方向	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示す値。次のいずれかの値になります。 • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
アプリケーション ID	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
URI	string	接続の Uniform Resource Identifier(URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。

ファイル イベント 5.3.1

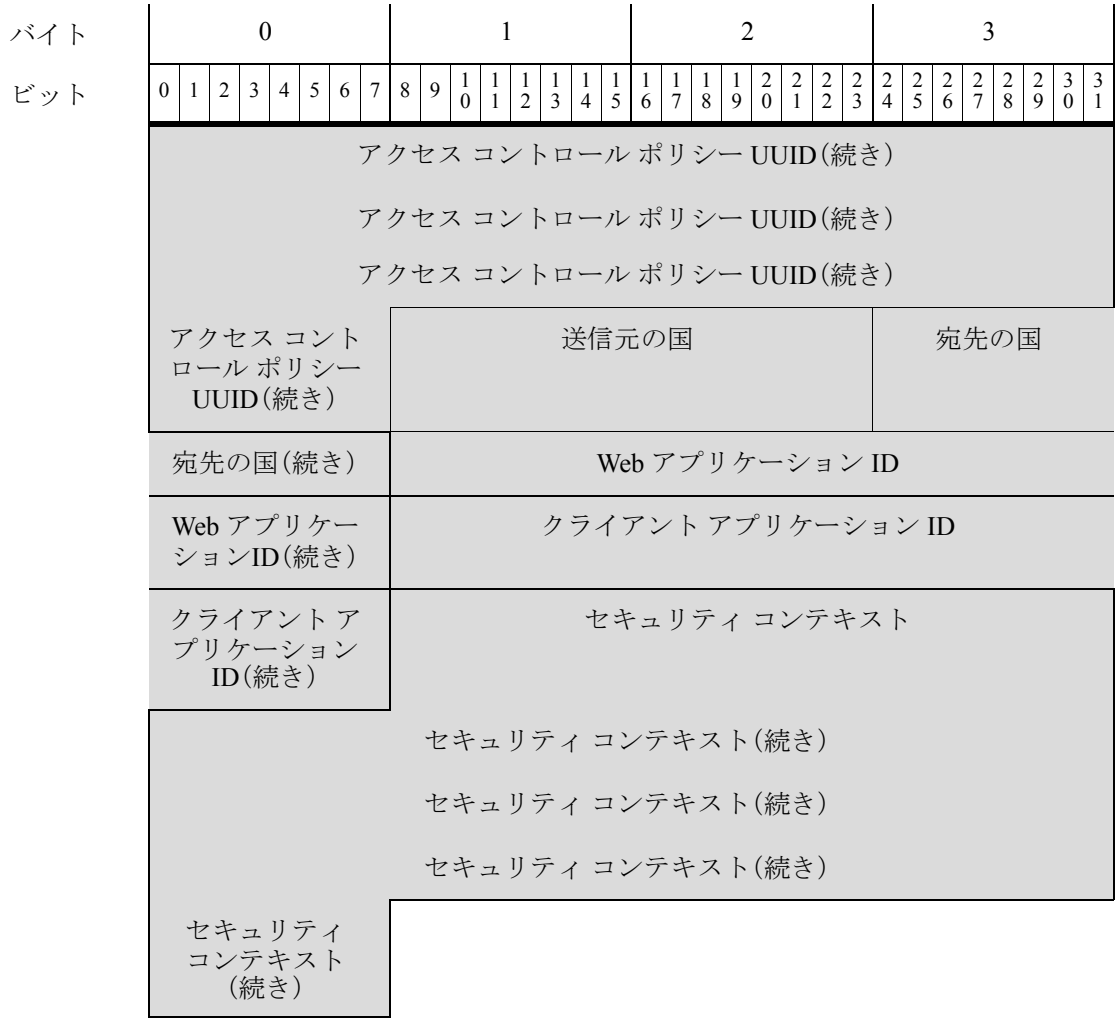
ファイル イベントには、ネットワークを介して送信されるファイルに関する情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントのブロック タイプは、シリーズ 2 グループのブロックの、ブロック タイプ 43 です。これはブロック タイプ 38 に取って代わります。セキュリティ コンテキスト フィールドが追加されました。

ファイル イベント レコードを要求するには、イベント バージョン 4 およびイベント コード 111 の要求メッセージ内に、ファイル イベント フラグ（要求フラグ フィールドのビット 30）を設定します。要求フラグ（2-12 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

次の図は、ファイル イベント データ ブロックの構造を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイル イベント ブロック タイプ（43）																																
ファイル イベント ブロック長																																
デバイスID																																
接続インスタンス																	接続数カウンタ															
接続タイムスタンプ																																
ファイル イベント タイムスタンプ																																
送信元 IP アドレス 送信元 IP アドレス（続き） 送信元 IP アドレス（続き） 送信元 IP アドレス（続き）																																
宛先IPアドレス 宛先 IP アドレス（続き） 宛先 IP アドレス（続き） 宛先 IP アドレス（続き）																																
傾向									SPERO 解析結果								ファイル ストレージ ステータス								ファイル分析ステータス							
アーカイブ ファイル ステータス									脅威スコア								操作								SHA ハッシュ							

	0	1	2	3
ビット	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
	SHA ハッシュ（続き）			
	SHA ハッシュ（続き）			
	SHA ハッシュ（続き）			
	SHA ハッシュ（続き）			
	SHA ハッシュ（続き）			
	SHA ハッシュ（続き）			
	SHA ハッシュ（続き）			
	SHA ハッシュ（続き）			ファイル タイプ ID
ファイル名	ファイル タイプ ID（続き）			文字列ブロック タイプ（0）
	文字列ブロック タイプ（0）（続き）			文字列ブロック長
	文字列ブロック長（続き）			ファイル名...
	ファイル サイズ			
	ファイル サイズ（続き）			
	方向	アプリケーション ID		
	アプリケーション ID（続き）	ユーザ ID		
URI	ユーザ ID（続き）	文字列ブロック タイプ（0）		
	文字列ブロック タイプ（0）（続き）	文字列ブロック長		
	文字列ブロック長（続き）	URI...		
シグネチャ	文字列ブロック タイプ（0）			
	文字列ブロック長			
	署名...			
	送信元ポート		接続先ポート	
	プロトコル	アクセス コントロール ポリシー UUID		



次の表は、ファイル イベント データ ブロックのフィールドについての説明です。

表 B-40　　ファイル イベント データ ブロックのフィールド

フィールド	データ タイプ	説明
ファイル イベント ブロック タイプ	uint32	ファイル イベント データ ブロックを開始します。この値は常に 43 です。
ファイル イベント ブロック長	uint32	ファイル イベント ブロックのバイトの合計数(ファイル イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイスID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または侵入イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。

表 B-40　ファイル イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
接続タイムスタンプ	uint32	関連する接続イベントの UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
ファイル イベント タイムスタンプ	uint32	ファイル タイプが識別されてファイル イベントが生成されたときの UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4(UNAVAILABLE):ソフトウェアから Cisco クラウドに対して、特性を確認する要求を送信できなかったか、または Cisco クラウド サービスが要求に応答しませんでした。 • 5(CUSTOM SIGNATURE):ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
SPERO 解析結果	uint8	SPERO 署名がファイル分析で使用されたかどうかを示します。値が 1、2、または 3 であれば、SPERO 分析は使用されました。それ以外の値であれば、SPERO 分析は使用されませんでした。
ファイル ストレージ ステータス	uint8	ファイルの保存ステータス。値は以下のとおりです。 • 1:ファイルが保存されました • 2:ファイルが保存されました • 3:ファイルを保存できません • 4:ファイルを保存できません • 5:ファイルを保存できません • 6:ファイルを保存できません • 7:ファイルを保存できません • 8:ファイル サイズが大きすぎます • 9:ファイル サイズが小さすぎます • 10:ファイルを保存できません • 11:ファイルは保存されておらず、解析結果を入手できません

表 B-40　ファイル イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
ファイル分析ステータス	uint8	ファイルが動的分析のために送信されているかどうかを示します。値は以下のとおりです。 • 0:ファイルが分析のために送信されていません • 1:分析のために送信されました • 2:分析のために送信されました • 4:分析のために送信されました • 5:送信に失敗しました • 6:送信に失敗しました • 7:送信に失敗しました • 8:送信に失敗しました • 9:ファイル サイズが小さすぎます • 10:ファイル サイズが大きすぎます • 11:分析のために送信されました • 12:分析が完了しました • 13:失敗(ネットワークの問題) • 14:失敗(レート制限) • 15:失敗(ファイルが大きすぎます) • 16:失敗(ファイルの読み取りエラー) • 17:失敗(内部ライブラリ エラー) • 19:ファイルは送信されておらず、解析結果を入手できません • 20:失敗(ファイルを実行できません) • 21:失敗(分析タイムアウト) • 22:分析のために送信されました • 23:サポートされていないファイル • 23(ファイル送信によるファイル キャパシティの処理):分析のためにファイルをサンドボックスに送信できなかったので、ファイル キャパシティが処理されました(センサーに保存) • 25(ファイル送信サーバ制限超過によるキャパシティの処理):サーバの速度制限が原因でファイル キャパシティが処理されました • 26(通信障害):クラウド接続失敗が原因でファイル キャパシティが処理されました • 27(未送信):設定が原因でファイルは送信されていません。 • 28(事前分類の一致なし):事前分類でファイル内に埋め込みオブジェクトまたは疑わしいオブジェクトが検出されなかったため、ファイルはダイナミック分析用に送信されませんでした • 29(Transmit Sent Sandbox Private Cloud):ダイナミック分析のためにファイルがプライベート クラウドに送信されました。 • 30(送信ボックスはプライベート クラウドに未送信):ファイルは分析のためにプライベート クラウドに送信されませんでした

表 B-40　ファイル イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
アーカイブ ファイル ステータス	uint8	この値は常に 0 です。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ～ 100)。
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
ファイル タイプ ID	uint32	ファイル タイプにマップされている ID 番号。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、AMP for Endpoints ファイル タイプのメタデータ (3-44 ページ) を参照してください。
ファイル名	string	ファイルの名前。
ファイル サイズ	uint64	ファイルのサイズ(バイト単位)。
方向	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示す値。次のいずれかの値になります。 • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
アプリケーション ID	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
URI	string	接続の Uniform Resource Identifier(URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。

表 B-40　ファイル イベント データ ブロックのフィールド(続き)

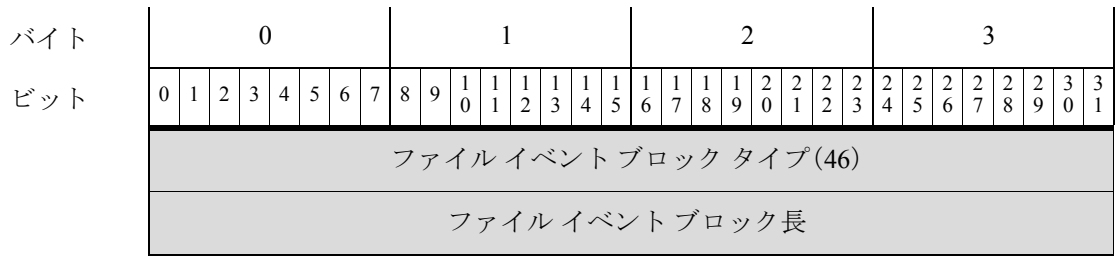
フィールド	データ タイプ	説明
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

ファイル イベント 5.4.x

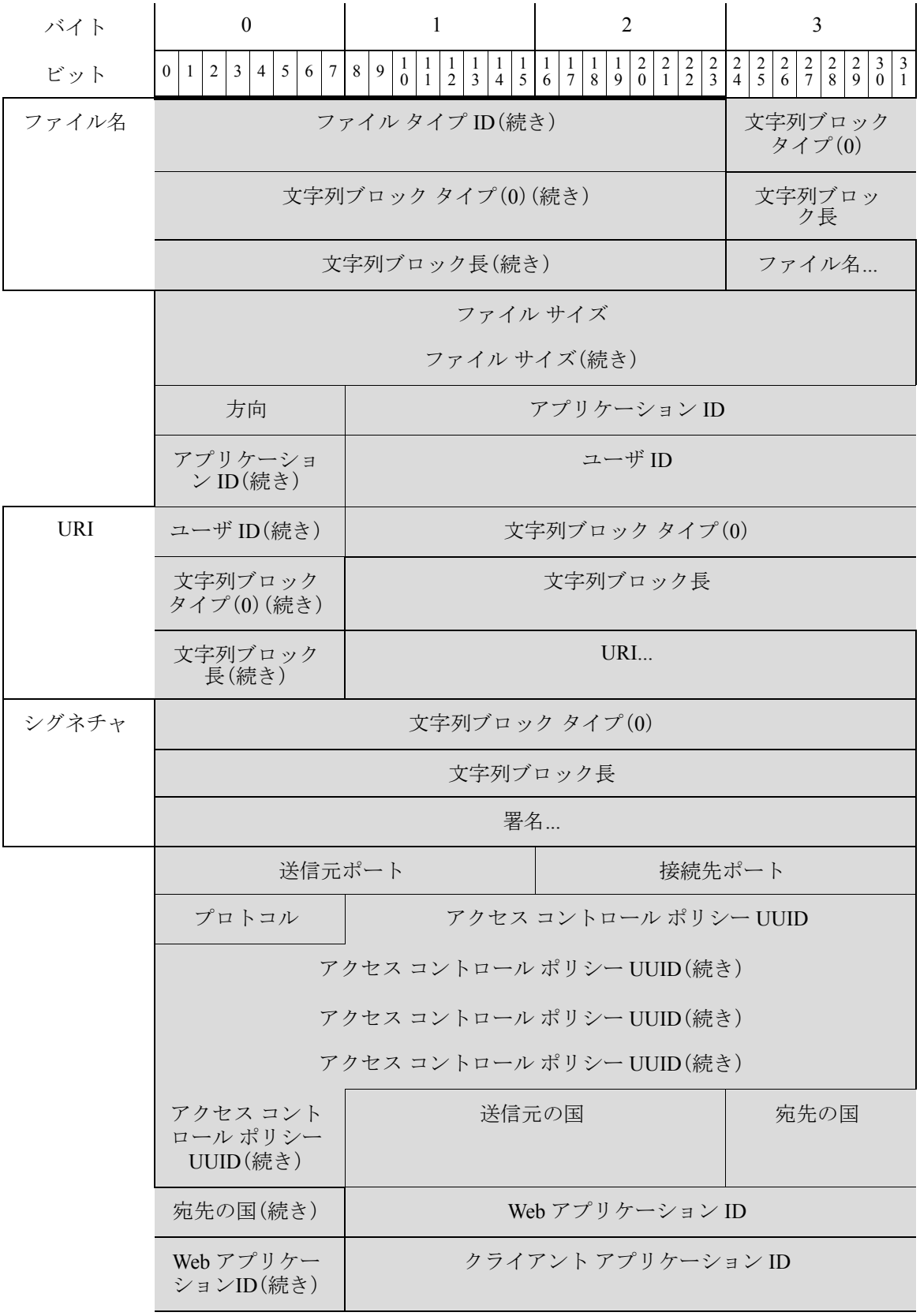
ファイル イベントには、ネットワークを介して送信されるファイルに関する情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントのブロック タイプは、シリーズ 2 グループのブロックの、ブロック タイプ 46 です。これはブロック タイプ 43 に取って代わります。SSL とファイル アーカイブ サポート用のフィールドが追加されました。

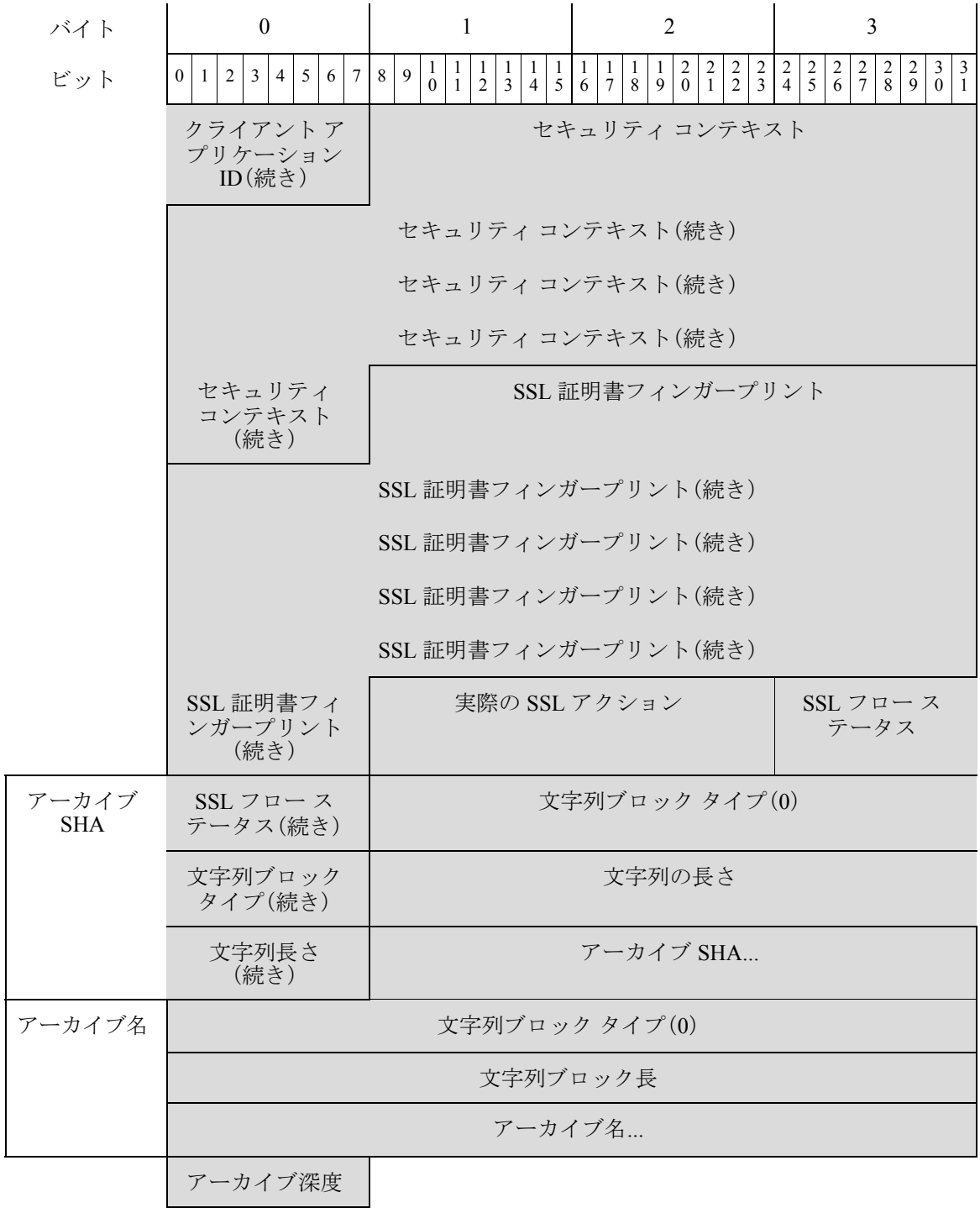
ファイル イベント レコードを要求するには、イベント バージョン 5 およびイベント コード 111 の要求メッセージ内に、ファイル イベント フラグ(要求フラグ フィールドのビット 30)を設定します。要求フラグ(2-12 ページ)を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

次の図は、ファイル イベント データ ブロックの構造を示しています。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
デバイスID																																
接続インスタンス																	接続数カウンタ															
接続タイムスタンプ																																
ファイル イベント タイムスタンプ																																
送信元 IP アドレス 送信元 IP アドレス（続き） 送信元 IP アドレス（続き） 送信元 IP アドレス（続き）																																
宛先IPアドレス 宛先 IP アドレス（続き） 宛先 IP アドレス（続き） 宛先 IP アドレス（続き）																																
傾向									SPERO 解析結果								ファイル ストレージ ステータス								ファイル分析ステータス							
アーカイブ ファイル ステータス									脅威スコア								操作								SHA ハッシュ							
SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き）																																
SHA ハッシュ（続き）																									ファイル タイプ ID							


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
ファイル名
ファイル タイプ ID(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
ファイル名...
ファイル サイズ
ファイル サイズ(続き)
方向
アプリケーション ID
アプリケーション ID(続き)
ユーザ ID
URI
ユーザ ID(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
URI...
シグネチャ
文字列ブロック タイプ(0)
文字列ブロック長
署名...
送信元ポート
接続先ポート
プロトコル
アクセス コントロール ポリシー UUID
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
送信元の国
宛先の国
宛先の国(続き)
Web アプリケーション ID
Web アプリケーションID(続き)
クライアント アプリケーション ID


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
クライアント アプリケーション ID(続き)
セキュリティ コンテキスト
セキュリティ コンテキスト(続き)
セキュリティ コンテキスト(続き)
セキュリティ コンテキスト(続き)
セキュリティ コンテキスト(続き)
SSL 証明書フィンガープリント
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
実際の SSL アクション
SSL フロー ステータス
アーカイブ SHA
SSL フロー ステータス(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(続き)
文字列の長さ
文字列長さ(続き)
アーカイブ SHA...
アーカイブ名
文字列ブロック タイプ(0)
文字列ブロック長
アーカイブ名...
アーカイブ深度

次の表は、ファイル イベント データ ブロックのフィールドについての説明です。

表 B-41　ファイル イベント データ ブロック 5.4.x のフィールド

フィールド	データ タイプ	説明
ファイル イベント ブロック タイプ	uint32	ファイル イベント データ ブロックを開始します。この値は常に 46 です。
ファイル イベント ブロック長	uint32	ファイル イベント ブロックのバイトの合計数（ファイル イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む）。
デバイスID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または侵入イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続タイムスタンプ	uint32	関連する接続イベントの UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
ファイル イベント タイムスタンプ	uint32	ファイル タイプが識別されてファイル イベントが生成されたときの UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先IPアドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1（CLEAN）：ファイルはクリーンであり、マルウェアは含まれていません。 • 2（UNKNOWN）：ファイルにマルウェアが含まれているかどうかは不明です。 • 3（MALWARE）：ファイルにはマルウェアが含まれています。 • 4（UNAVAILABLE）：ソフトウェアから Cisco クラウドに対して、特性を確認する要求を送信できなかったか、または Cisco クラウド サービスが要求に応答しませんでした。 • 5（CUSTOM SIGNATURE）：ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
SPERO 解析結果	uint8	SPERO 署名がファイル分析で使用されたかどうかを示します。値が 1、2、または 3 であれば、SPERO 分析は使用されました。それ以外の値であれば、SPERO 分析は使用されませんでした。

表 B-41　ファイル イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
ファイル ストレージ ステータス	uint8	ファイルの保存ステータス。値は以下のとおりです。 • 1:ファイルが保存されました • 2:ファイルが保存されました • 3:ファイルを保存できません • 4:ファイルを保存できません • 5:ファイルを保存できません • 6:ファイルを保存できません • 7:ファイルを保存できません • 8:ファイル サイズが大きすぎます • 9:ファイル サイズが小さすぎます • 10:ファイルを保存できません • 11:ファイルは保存されておらず、解析結果を入手できません

表 B-41　ファイル イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
ファイル分析ステータス	uint8	ファイルが動的分析のために送信されているかどうかを示します。値は以下のとおりです。 • 0:ファイルが分析のために送信されていません • 1:分析のために送信されました • 2:分析のために送信されました • 4:分析のために送信されました • 5:送信に失敗しました • 6:送信に失敗しました • 7:送信に失敗しました • 8:送信に失敗しました • 9:ファイル サイズが小さすぎます • 10:ファイル サイズが大きすぎます • 11:分析のために送信されました • 12:分析が完了しました • 13:失敗(ネットワークの問題) • 14:失敗(レート制限) • 15:失敗(ファイルが大きすぎます) • 16:失敗(ファイルの読み取りエラー) • 17:失敗(内部ライブラリ エラー) • 19:ファイルは送信されておらず、解析結果を入手できません • 20:失敗(ファイルを実行できません) • 21:失敗(分析タイムアウト) • 22:分析のために送信されました • 23:サポートされていないファイル

表 B-41　ファイル イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
アーカイブ ファイル ステータス	uint8	調査中のアーカイブのステータス。次のいずれかの値になります。 • 0(N/A):ファイルがアーカイブとして検査されていません。 • 1:保留中。アーカイブは調査中です • 2:取得済み。調査が問題なく正常に実行されました • 3:失敗。システムのリソース不足のため調査に失敗しました。 • 4:深度の超過。調査は正常に実行されましたが、アーカイブがネストされた調査の深度を超過しました • 5:暗号化。部分的に正常に実行されましたが、アーカイブが暗号化されているか、暗号化されたアーカイブが含まれています • 6:調査できませんでした。部分的に正常に実行されましたが、ファイル形式が不正であるか破損しています
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ～ 100)。
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト • 6:クラウド ルックアップのタイムアウト • 7:カスタム検出 • 8:カスタム検出ブロック • 9:アーカイブ ブロック(深度超過) • 10:アーカイブ ブロック(暗号化されている) • 11:アーカイブ ブロック(調査エラー)
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
ファイル タイプ ID	uint32	ファイル タイプにマップされている ID 番号。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、AMP for Endpoints ファイル タイプのメタデータ (3-44 ページ) を参照してください。
ファイル名	string	ファイルの名前。

表 B-41　ファイル イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
ファイル サイズ	uint64	ファイルのサイズ(バイト単位)。
方向	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示す値。次のいずれかの値になります。 • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
アプリケーション ID	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
URI	string	接続の Uniform Resource Identifier(URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。

表 B-41　ファイル イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 B-41　ファイル イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
SSL フロー ステータス	uint16	SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。 • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
文字列ブロック タイプ	uint32	アーカイブ SHA を含む文字列データ ブロックを開始します。この値は常に 0 です。

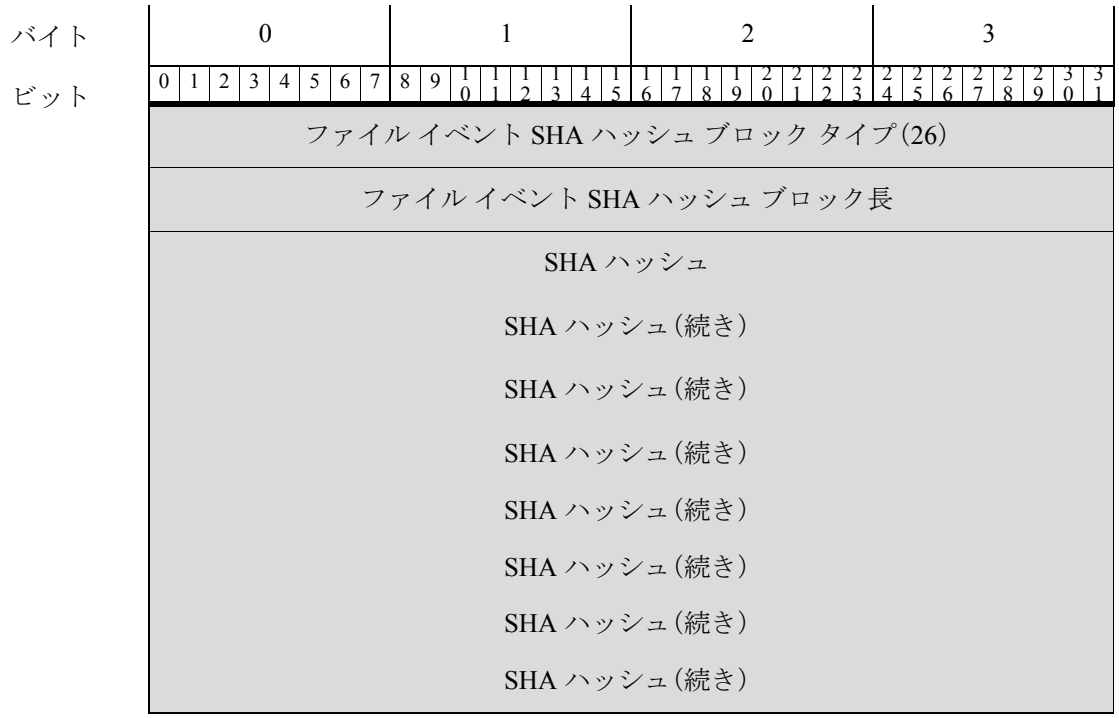
表 B-41　ファイル イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	アーカイブ SHA 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および侵入ポリシー名のバイト数を含む)。
アーカイブ SHA	string	ファイルが含まれる親アーカイブの SHA1 ハッシュ。
文字列ブロック タイプ	uint32	アーカイブ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	アーカイブ名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびアーカイブ名のバイト数を含む)。
アーカイブ名	string	親アーカイブの名前。
アーカイブ深度	uint8	ファイルがネストされている層の数。たとえば、テキスト ファイルが zip アーカイブ内にある場合、この値は 1 になります。

ファイル イベント SHA ハッシュ 5.1.1 ～ 5.2.x

eStreamer サービスは、ファイルの SHA ハッシュとそのファイル名とのマッピングのメタデータを含む、ファイル イベント SHA ハッシュ データ ブロックを使用します。ブロック タイプは、シリーズ 2 リストのデータ ブロックの 26 です。これは、ファイル ログ イベントが拡張要求(イベント コード 111)で要求されており、ビット 20 が設定されているかまたはメタデータがイベント バージョン 4 およびイベント コード 21 で要求されていれば、要求することができます。

次の図は、ファイル イベント ハッシュ データ ブロックの構造を示しています。



ファイル名	文字列ブロック タイプ(0)
	文字列ブロック長
	ファイル名または解析結果...

次の表は、ファイル イベント SHA ハッシュ データ ブロックのフィールドについての説明です。

表 B-42　ファイル イベント SHA ハッシュ データ ブロック 5.1.1 ～ 5.2.x のフィールド

フィールド	データ タイプ	説明
ファイル イベント SHA ハッシュ ブロック タイプ	uint32	ファイル イベント SHA ハッシュ ブロックを開始します。この値は常に 26 です。
ファイル イベント SHA ハッシュ ブロック長	uint32	ファイル イベント SHA ハッシュ ブロックのバイトの合計数(ファイル イベント SHA ハッシュ ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
文字列ブロック タイプ	uint32	ファイルに関連付けられている記述名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
ファイル名または解析結果	string	ファイルの記述名または解析結果。ファイルがクリーンである場合、この値は Clean です。ファイルの解析結果が不明の場合、この値は Neutral です。ファイルにマルウェアが含まれている場合、ファイル名が示されます。

レガシー相関イベントのデータ構造

続くいくつかのトピックでは、他のレガシー相関(コンプライアンス)データの構造について説明します。

- 相関イベント 5.0 ～ 5.0.2(B-247 ページ)
- 相関イベント 5.1 ～ 5.3.x(B-256 ページ)

相関イベント 5.0 ～ 5.0.2

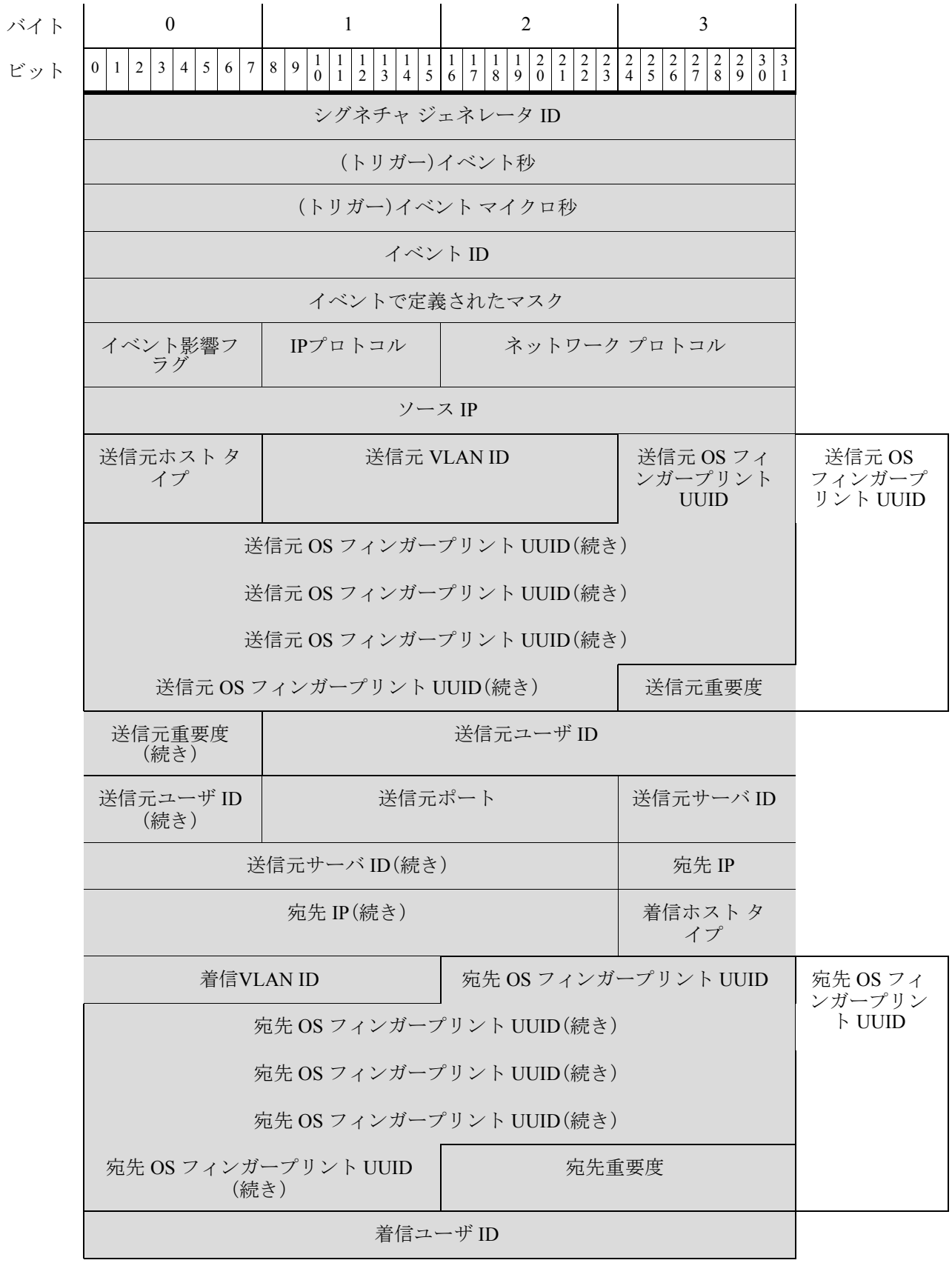
相関イベント(5.0 よりも前のバージョンではコンプライアンス イベントと呼ばれていた)には、相関ポリシー違反に関する情報が含まれます。このメッセージは、標準 eStreamer メッセージ ヘッダーを使用し、レコード タイプ 112 を指定し、それに相関データ ブロック タイプ 116 が続きます。データ ブロック タイプ 116 は、関連するセキュリティ ゾーンとインターフェイスに関する追加情報が含まれるという点で、その先行するもの(ブロック タイプ 107)とは異なります。

eStreamer からの 5.0 相関イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベント タイプ コード 31 およびバージョン 7 を要求します（拡張要求の送信の詳細については、拡張要求の送信（2-4 ページ）を参照してください）。オプションで、最初のイベント ストリーム要求メッセージのフラグ フィールドでビット 23 を有効にして、拡張イベント ヘッダーを含めることができます。また、フラグ フィールドでビット 20 を有効にして、ユーザ メタデータを含めることもできます。

レコード構造には、シリーズ 1 のブロックである、文字列ブロック タイプが含まれることに注目してください。シリーズ 1 ブロックの詳細については、ディスカバリ（シリーズ1）ブロック（4-63 ページ）を参照してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（112）															
レコード長																																
eStreamer サーバ タイムスタンプ（イベント用、ビット 23 が設定されている場合のみ）																																
将来の使用に備えて予約済み（イベントでビット 23 が設定されている場合のみ）																																
相関ブロック タイプ（116）																																
相関ブロック長																																
デバイス ID																																
（相関）イベント秒																																
イベント ID																																
ポリシー ID																																
ルール ID																																
プライオリティ																																
文字列ブロック タイプ（0）																																
文字列ブロック長																																
説明...																									イベント タイプ							
イベント デバイス ID																																
シグネチャ ID																																

イベント説明


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
シグネチャ ジェネレータ ID
(トリガー)イベント秒
(トリガー)イベント マイクロ秒
イベント ID
イベントで定義されたマスク
イベント影響フラグ
IPプロトコル
ネットワーク プロトコル
ソース IP
送信元ホスト タイプ
送信元 VLAN ID
送信元 OS フィンガープリント UUID
送信元 OS フィンガープリント UUID
送信元 OS フィンガープリント UUID(続き)
送信元 OS フィンガープリント UUID(続き)
送信元 OS フィンガープリント UUID(続き)
送信元 OS フィンガープリント UUID(続き)
送信元重要度
送信元重要度(続き)
送信元ユーザ ID
送信元ユーザ ID(続き)
送信元ポート
送信元サーバ ID
送信元サーバ ID(続き)
宛先 IP
宛先 IP(続き)
着信ホスト タイプ
着信VLAN ID
宛先 OS フィンガープリント UUID
宛先 OS フィンガープリント UUID
宛先 OS フィンガープリント UUID(続き)
宛先 OS フィンガープリント UUID(続き)
宛先 OS フィンガープリント UUID(続き)
宛先 OS フィンガープリント UUID(続き)
宛先重要度
着信ユーザ ID

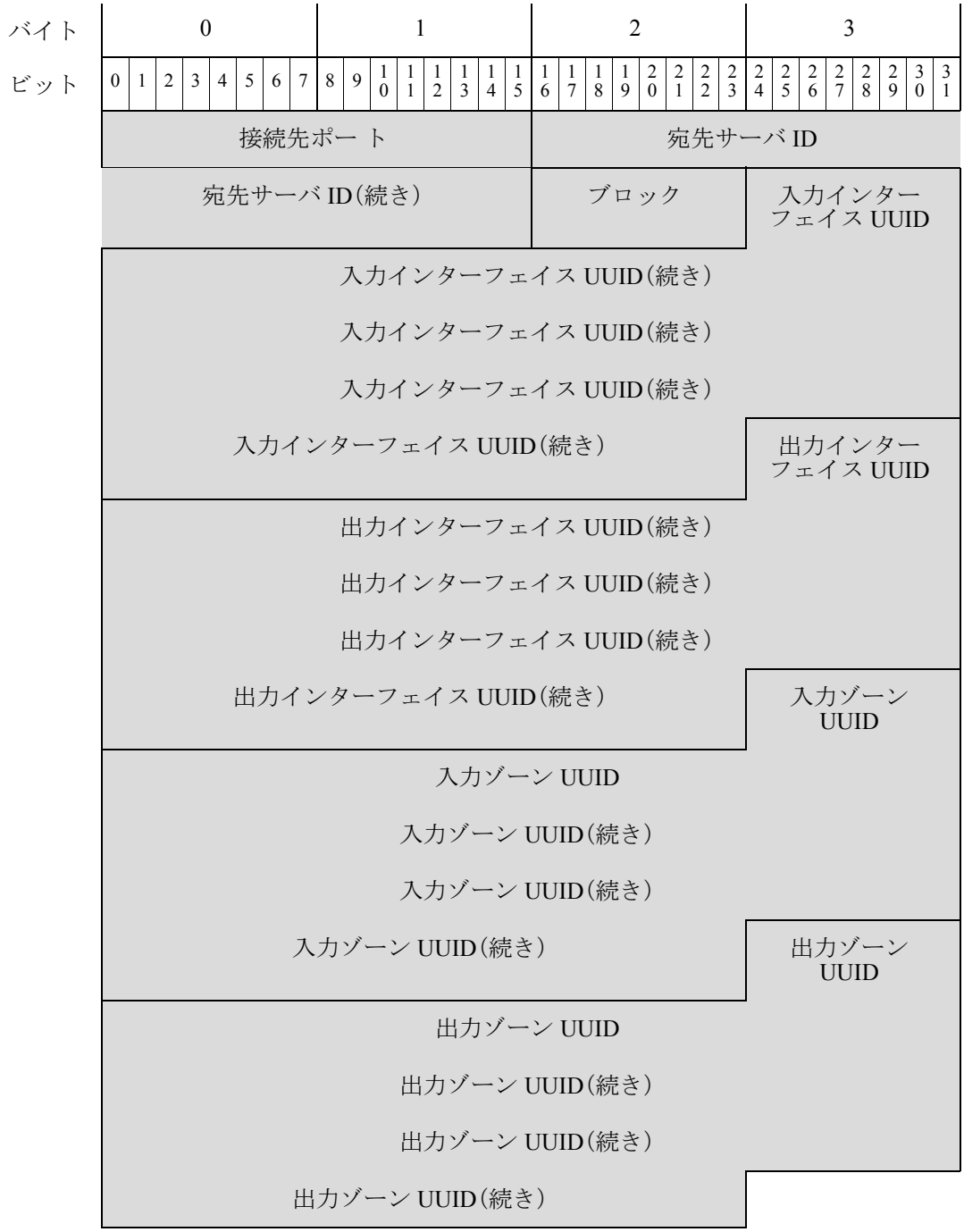

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
接続先ポー ト
宛先サーバ ID
宛先サーバ ID(続き)
ブロック
入力インターフェイス UUID
入力インターフェイス UUID(続き)
入力インターフェイス UUID(続き)
入力インターフェイス UUID(続き)
入力インターフェイス UUID(続き)
出力インターフェイス UUID
出力インターフェイス UUID(続き)
出力インターフェイス UUID(続き)
出力インターフェイス UUID(続き)
出力インターフェイス UUID(続き)
入力ゾーン UUID
入力ゾーン UUID
入力ゾーン UUID(続き)
入力ゾーン UUID(続き)
入力ゾーン UUID(続き)
出力ゾーン UUID
出力ゾーン UUID
出力ゾーン UUID(続き)
出力ゾーン UUID(続き)
出力ゾーン UUID(続き)
出力ゾーン UUID(続き)

表 B-43　相関イベント データ 5.0 ～ 5.0.2 のフィールド

フィールド	データ タイプ	説明
相関ブロック タイプ	uint32	相関イベント データ ブロックが続くことを示します。このフィールドの値は、常に 107 です。ディスカバリ（シリーズ1）ブロック（4-63 ページ）を参照してください。
相関ブロック長	uint32	相関データ ブロック長（相関ブロック タイプと長さの 8 バイト、およびそれに続く相関データを含む）。
デバイス ID	uint32	相関イベントを生成した管理対象デバイスまたは Defense Center の内部 ID 番号。値 0 は Defense Center を示します。バージョン 3 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ（3-38 ページ）を参照してください。
（相関）イベント秒	uint32	相関イベントが生成された時刻を示す UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
イベント ID	uint32	相関イベント ID 番号。
ポリシー ID	uint32	違反された相関ポリシーの ID 番号。データベースからのポリシー ID 番号を入手する方法の詳細については、サーバ レコード（4-16 ページ）を参照してください。
ルール ID	uint32	トリガーしてポリシー違反となった相関ルールの ID 番号。データベースからポリシー ID 番号を取得する方法の詳細については、サーバ レコード（4-16 ページ）を参照してください。
プライオリティ	uint32	イベントに割り当てられた優先順位。これは、0 ～ 5 の整数値です。
文字列ブロック タイプ	uint32	相関違反イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、文字列データ ブロック（4-73 ページ）を参照してください。
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数（文字列のブロック タイプのための 4 バイト、文字列ブロック長のための 4 バイト、説明のバイト数を含む）。
説明	string	相関イベントについての説明。
イベント タイプ	uint8	相関イベントが、侵入、ホスト検出、またはユーザ イベントによってトリガーされたかどうかを示します。 • 1：侵入 • 2：ホストのディスカバリ • 3：ユーザ
イベント デバイス ID	uint32	相関イベントをトリガーしたイベントを生成したデバイスの ID 番号。バージョン 3 メタデータを要求するとデバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ（3-38 ページ）を参照してください。
シグネチャ ID	uint32	イベントが侵入イベントであった場合、イベントに対応するルール ID 番号を示します。そうでない場合、この値は 0 になります。

表 B-43　相関イベント データ 5.0 ～ 5.0.2 のフィールド（続き）

フィールド	データ タイプ	説明
シグネチャ ジェネレータ ID	uint32	イベントが侵入イベントであった場合、イベントを生成した Firepower システム プリプロセッサまたはルール エンジンの ID 番号を示します。
（トリガー）イベント秒	uint32	相関ポリシー ルールをトリガーしたイベントの時刻を示す UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
（トリガー）イベント マイクロ秒	uint32	イベントが検出されたタイムスタンプの、マイクロ秒（100 万分の 1 秒）の増分。
イベント ID	uint32	デバイスによって生成されたイベントの ID 番号。
イベントで定義されたマスク	bits[32]	このフィールドに設定されたビットは、メッセージ内の続くどのフィールドが有効であるかを示します。各ビット値のリストの詳細については、表 B-44（B-255 ページ）を参照してください。

表 B-43　相関イベント データ 5.0 ～ 5.0.2 のフィールド(続き)

フィールド	データ タイプ	説明
イベント影響フラグ	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40:このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます(ビット 6)。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。 次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • (0、不明):00X00000 • 赤(1、脆弱):xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx • オレンジ(2、潜在的に脆弱):00X00111 • 黄(3、現在は脆弱でない):00X00011 • 青(4、不明なターゲット):00X00001
IPプロトコル	uint8	イベントに関連付けられている IP プロトコルの ID(該当する場合)。
ネットワーク プロトコル	uint16	イベントに関連付けられているネットワーク プロトコル(該当する場合)。
ソース IP	uint8[4]	IP アドレス オクテットの、イベントの送信元ホストの IP アドレス。
送信元ホスト タイプ	uint8	送信元ホストのタイプ: • 0:ホスト • 1:ルータ • 2:ブリッジ

表 B-43　相関イベント データ 5.0 ～ 5.0.2 のフィールド（続き）

フィールド	データ タイプ	説明
送信元 VLAN ID	uint16	送信元ホストの VLAN ID 番号（該当する場合）。
送信元 OS フィンガープリント UUID	uint8[16]	送信元ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID。 フィンガープリント ID にマップする値の取得の詳細については、サーバ レコード（4-16 ページ）を参照してください。
送信元重要度	uint16	送信元ホストの、ユーザ定義の重要度値： • 0：なし • 1：低 • 2：中 • 3：高
送信元ユーザ ID	uint32	システムにより識別される、送信元ホストにログインしたユーザの ID 番号。
送信元ポート	uint16	イベントの送信元ポート。
送信元サーバ ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
宛先IPアドレス	uint8[4]	ポリシー違反に関連付けられた宛先ホストの IP アドレス（該当する場合）。宛先 IP アドレスがない場合、この値は 0 になります。
宛先ホスト タイプ	uint8	宛先ホストのタイプ： • 0：ホスト • 1：ルータ • 2：ブリッジ
宛先 VLAN ID	uint16	宛先ホストの VLAN ID 番号（該当する場合）。
宛先 OS フィンガープリント UUID	uint8[16]	宛先ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID 番号。 フィンガープリント ID にマップする値の取得の詳細については、サーバ レコード（4-16 ページ）を参照してください。
宛先重要度	uint16	宛先ホストの、ユーザ定義の重要度値： • 0：なし • 1：低 • 2：中 • 3：高
宛先ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
接続先ポート	uint16	イベントの宛先ポート。
宛先サービス ID	uint32	送信元ホスト上で実行するサーバの ID 番号。

表 B-43　相関イベント データ 5.0 ～ 5.0.2 のフィールド(続き)

フィールド	データ タイプ	説明
ブロック	uint8	侵入イベントをトリガーしたパケットの処理を示す値。 • 0:侵入イベントがドロップされていない • 1:侵入イベントがドロップされている(展開がインライン型、スイッチ型、またはルーティング型である場合はドロップ) • 2:侵入ポリシーが、インライン型、スイッチ型、またはルーティング型展開のデバイスに適用されている場合は、イベントをトリガーしたパケットがドロップされている可能性がある。
入力インターフェイス UUID	uint8[16]	相関イベントに関連付けられている入力インターフェイスの固有識別子として機能するインターフェイス ID。
出力インターフェイス UUID	uint8[16]	相関イベントに関連付けられている出力インターフェイスの固有識別子として機能するインターフェイス ID。
入力ゾーン UUID	uint8[16]	相関イベントに関連付けられている入力セキュリティ ゾーンの固有識別子として機能するゾーン ID。
出力ゾーン UUID	uint8[16]	相関イベントに関連付けられている出力セキュリティ ゾーンの固有識別子として機能するゾーン ID。

次の表は、各イベント定義マスク値についての説明です。

表 B-44　イベントで定義された値

説明	マスク値
イベント影響フラグ	0x00000001
IPプロトコル	0x00000002
ネットワーク プロトコル	0x00000004
ソース IP	0x00000008
送信元ホスト タイプ	0x00000010
送信元 VLAN ID	0x00000020
送信元フィンガープリント ID	0x00000040
送信元重要度	0x00000080
送信元ポート	0x00000100
送信元サーバ	0x00000200
宛先 IP	0x00000400
宛先ホスト タイプ	0x00000800
宛先 VLAN ID	0x00001000
宛先フィンガープリント ID	0x00002000
宛先重要度	0x00004000
接続先ポート	0x00008000

表 B-44　　イベントで定義された値（続き）

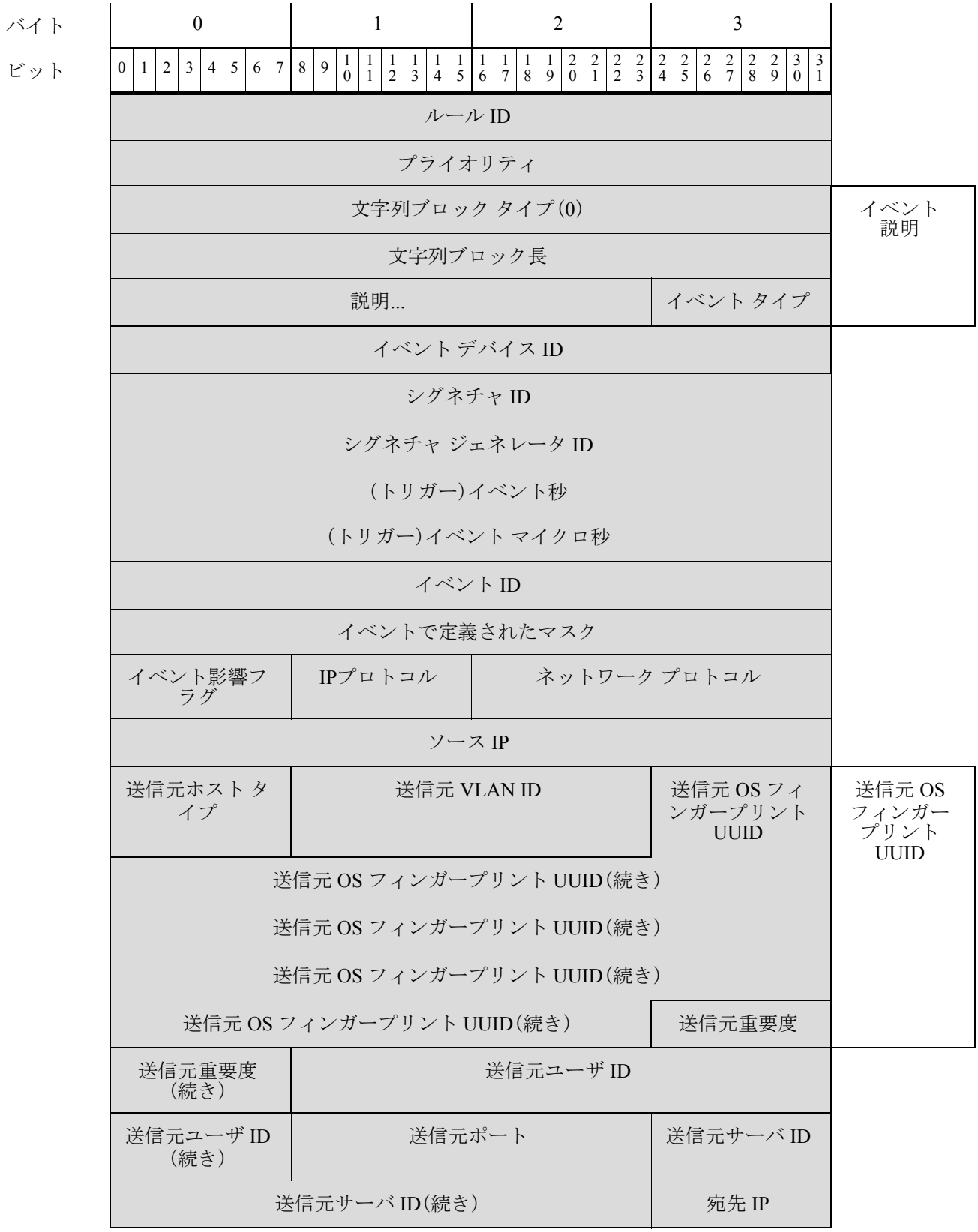
説明	マスク値
宛先サーバ	0x00010000
送信元ユーザ	0x00020000
宛先ユーザ	0x00040000

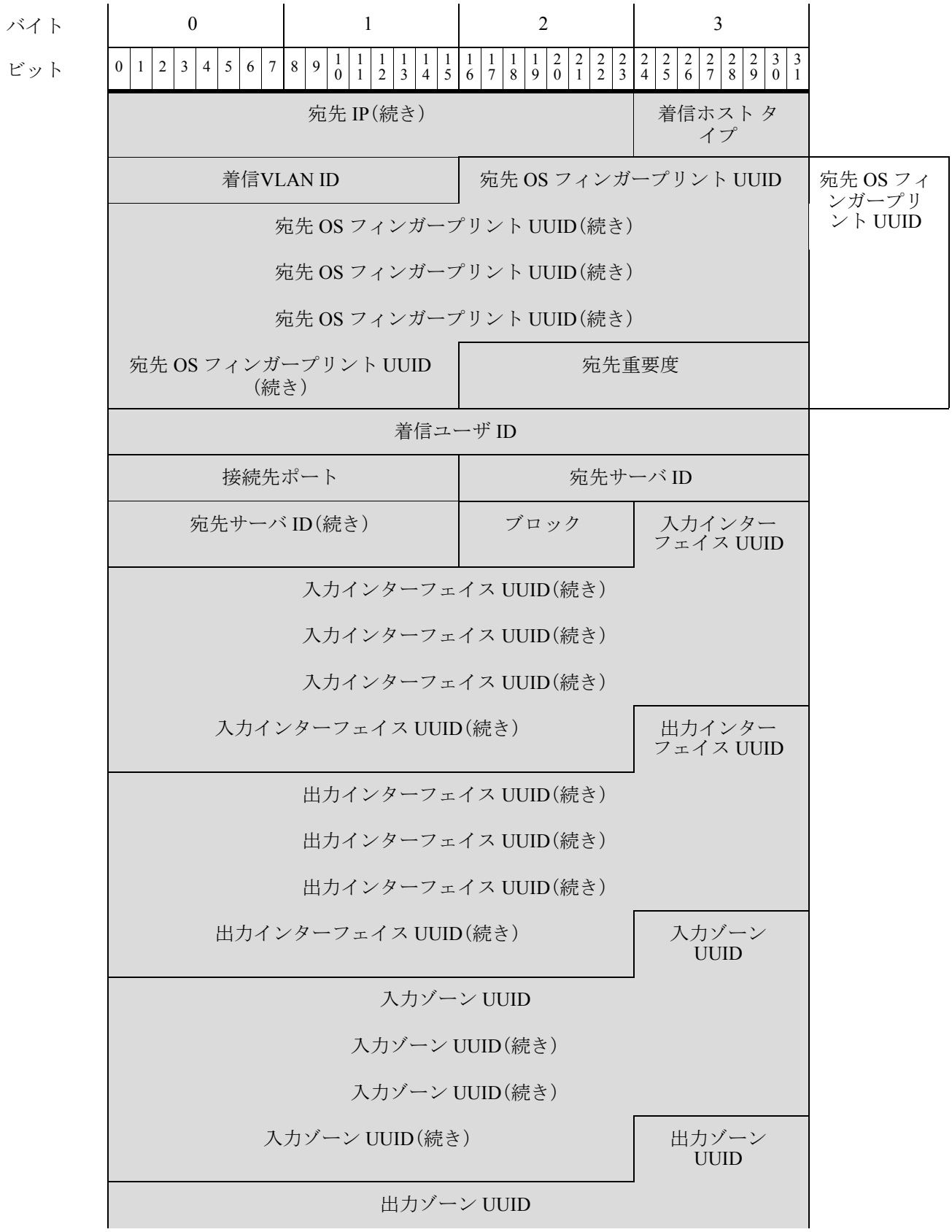
相関イベント 5.1 ～ 5.3.x

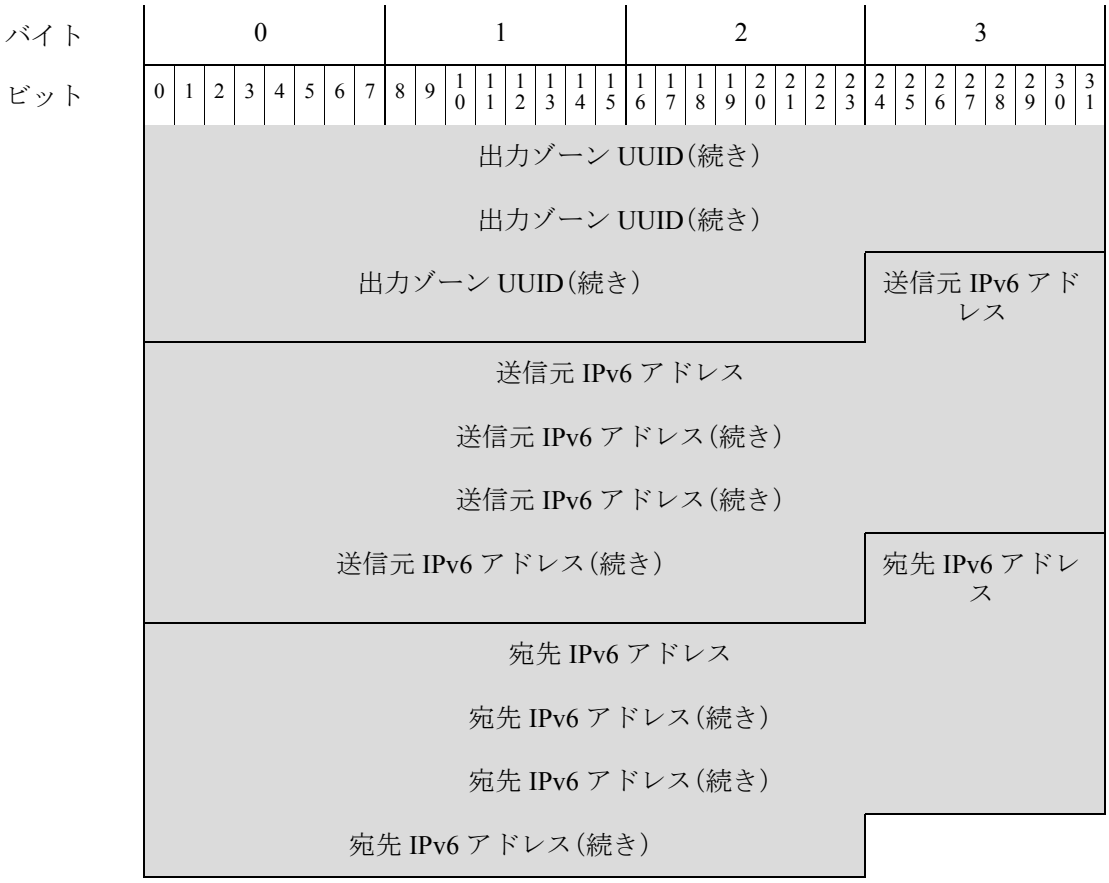
相関イベント（5.0 よりも前のバージョンではコンプライアンス イベントと呼ばれていた）には、相関ポリシー違反に関する情報が含まれます。このメッセージは、標準 eStreamer メッセージ ヘッダーを使用し、レコード タイプ 112 を指定し、それにシリーズ 1 セットのデータ ブロックの相関データ ブロック タイプ 128 が続きます。データ ブロック タイプ 128 は、IPv6 サポートが含まれるという点で、その先行するもの（ブロック タイプ 116）とは異なります。

eStreamer からの 5.1 ～ 5.3.x の相関イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベント タイプ コード 31 およびバージョン 8 を要求します（拡張要求の送信の詳細については、拡張要求の送信（2-4 ページ）を参照してください）。オプションで、最初のイベント ストリーム要求メッセージのフラグ フィールドでビット 23 を有効にして、拡張イベント ヘッダーを含めることができます。また、フラグ フィールドでビット 20 を有効にして、ユーザ メタデータを含めることもできます。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（112）															
レコード長																																
eStreamer サーバ タイムスタンプ（イベント用、ビット 23 が設定されている場合のみ）																																
将来の使用に備えて予約済み（イベントでビット 23 が設定されている場合のみ）																																
相関ブロック タイプ（128）																																
相関ブロック長																																
デバイスID																																
（相関）イベント秒																																
イベント ID																																
ポリシー ID																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
ルール ID
プライオリティ
文字列ブロック タイプ(0)
文字列ブロック長
説明...
イベント タイプ
イベント説明
イベント デバイス ID
シグネチャ ID
シグネチャ ジェネレータ ID
(トリガー)イベント秒
(トリガー)イベント マイクロ秒
イベント ID
イベントで定義されたマスク
イベント影響フラグ
IPプロトコル
ネットワーク プロトコル
ソース IP
送信元ホスト タイプ
送信元 VLAN ID
送信元 OS フィンガープリント UUID
送信元 OS フィンガープリント UUID(続き)
送信元 OS フィンガープリント UUID(続き)
送信元 OS フィンガープリント UUID(続き)
送信元 OS フィンガープリント UUID(続き)
送信元重要度
送信元 OS フィンガープリント UUID
送信元重要度(続き)
送信元ユーザ ID
送信元ユーザ ID(続き)
送信元ポート
送信元サーバ ID
送信元サーバ ID(続き)
宛先 IP


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
宛先 IP(続き)
着信ホスト タイプ
着信VLAN ID
宛先 OS フィンガープリント UUID
宛先 OS フィンガープリント UUID
宛先 OS フィンガープリント UUID(続き)
宛先 OS フィンガープリント UUID(続き)
宛先 OS フィンガープリント UUID(続き)
宛先 OS フィンガープリント UUID(続き)
宛先重要度
着信ユーザ ID
接続先ポート
宛先サーバ ID
宛先サーバ ID(続き)
ブロック
入力インターフェイス UUID
入力インターフェイス UUID(続き)
入力インターフェイス UUID(続き)
入力インターフェイス UUID(続き)
入力インターフェイス UUID(続き)
出力インターフェイス UUID
出力インターフェイス UUID(続き)
出力インターフェイス UUID(続き)
出力インターフェイス UUID(続き)
出力インターフェイス UUID(続き)
入力ゾーン UUID
入力ゾーン UUID
入力ゾーン UUID(続き)
入力ゾーン UUID(続き)
入力ゾーン UUID(続き)
出力ゾーン UUID
出力ゾーン UUID



レコード構造には、シリーズ 1 のブロックである、文字列ブロック タイプが含まれることに注目してください。シリーズ 1 ブロックの詳細については、ディスカバリ（シリーズ1）ブロック（4-63 ページ）を参照してください。

表 B-45　相関イベント データ 5.1 ～ 5.3.x のフィールド

フィールド	データ タイプ	説明
相関ブロック タイプ	uint32	相関イベント データ ブロックが続くことを示します。このフィールドの値は、常に 128 です。ディスカバリ（シリーズ1）ブロック（4-63 ページ）を参照してください。
相関ブロック長	uint32	相関データ ブロック長（相関ブロック タイプと長さの 8 バイト、およびそれに続く相関データを含む）。
デバイスID	uint32	相関イベントを生成した管理対象デバイスまたは Defense Center の内部 ID 番号。値 0 は Defense Center を示します。バージョン 3 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ（3-38 ページ）を参照してください。
（相関）イベント秒	uint32	相関イベントが生成された時刻を示す UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
イベント ID	uint32	相関イベント ID 番号。

表 B-45　相関イベント データ 5.1 ～ 5.3.x のフィールド（続き）

フィールド	データ タイプ	説明
ポリシー ID	uint32	違反された相関ポリシーの ID 番号。データベースからのポリシー ID 番号を入手する方法の詳細については、サーバ レコード (4-16 ページ) を参照してください。
ルール ID	uint32	トリガーしてポリシー違反となった相関ルールの ID 番号。データベースからのポリシー ID 番号を入手する方法の詳細については、サーバ レコード (4-16 ページ) を参照してください。
プライオリティ	uint32	イベントに割り当てられた優先順位。これは、0 ～ 5 の整数値です。
文字列ブロック タイプ	uint32	相関違反イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、文字列データ ブロック (4-73 ページ) を参照してください。
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数（文字列のブロック タイプのための 4 バイト、文字列ブロック長のための 4 バイト、説明のバイト数を含む）。
説明	string	相関イベントについての説明。
イベント タイプ	uint8	相関イベントが、侵入、ホスト検出、またはユーザ イベントによってトリガーされたかどうかを示します。 • 1：侵入 • 2：ホストのディスカバリ • 3：ユーザ
イベント デバイス ID	uint32	相関イベントをトリガーしたイベントを生成したデバイスの ID 番号。バージョン 3 メタデータを要求するとデバイス名を入手できます。詳細については、管理対象 デバイス レコードのメタデータ (3-38 ページ) を参照してください。
シグネチャ ID	uint32	イベントが侵入イベントであった場合、イベントに対応するルール ID 番号を示します。そうでない場合、この値は 0 になります。
シグネチャ ジェネレータ ID	uint32	イベントが侵入イベントであった場合、イベントを生成した Firepower システム プリプロセッサまたはルール エンジンの ID 番号を示します。
（トリガー）イベント秒	uint32	相関ポリシー ルールをトリガーしたイベントの時刻を示す UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
（トリガー）イベント マイクロ秒	uint32	イベントが検出されたタイムスタンプの、マイクロ秒（100 万分の 1 秒）の増分。
イベント ID	uint32	Cisco デバイスによって生成されたイベントの ID 番号。
イベントで定義されたマスク	bits[32]	このフィールドに設定されたビットは、メッセージ内の続くどのフィールドが有効であるかを示します。各ビット値のリストの詳細については、表 B-44 (B-255 ページ) を参照してください。

表 B-45　相関イベント データ 5.1 ～ 5.3.x のフィールド(続き)

フィールド	データ タイプ	説明
イベント影響フラグ	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) 次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • (0、不明):`00X00000` • 赤(1、脆弱):`XXXX1XXX`, `XXX1XXXX`, `X1XXXXXX`, `1XXXXXXX`(バージョン 5.0+ のみ) • オレンジ(2、潜在的に脆弱):`00X0011X` • 黄(3、現在は脆弱でない):`00X0001X` • 青(4、不明なターゲット):`00X00001`
IPプロトコル	uint8	イベントに関連付けられている IP プロトコルの ID(該当する場合)。
ネットワーク プロトコル	uint16	イベントに関連付けられているネットワーク プロトコル(該当する場合)。
送信元 IP アドレス	uint8[4]	このフィールドは予約済みですが、設定されておりません。送信元 IPv4 アドレスは、送信元 IPv6 アドレス フィールドに保存されます。詳細については、IP アドレス(1-6 ページ)を参照してください。

表 B-45　相関イベント データ 5.1 ～ 5.3.x のフィールド（続き）

フィールド	データ タイプ	説明
送信元ホスト タイプ	uint8	送信元ホストのタイプ: • 0:ホスト • 1:ルータ • 2:ブリッジ
送信元 VLAN ID	uint16	送信元ホストの VLAN ID 番号（該当する場合）。
送信元 OS フィンガープリント UUID	uint8[16]	送信元ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID。 フィンガープリント ID にマップする値の取得の詳細については、サーバ レコード（4-16 ページ）を参照してください。
送信元重要度	uint16	送信元ホストの、ユーザ定義の重要度値: • 0:なし • 1:低 • 2:中 • 3:高
送信元ユーザ ID	uint32	システムにより識別される、送信元ホストにログインしたユーザの ID 番号。
送信元ポート	uint16	イベントの送信元ポート。
送信元サーバ ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
宛先IPアドレス	uint8[4]	このフィールドは予約済みですが、設定されておりません。宛先 IPv4 アドレスは、宛先 IPv6 アドレス フィールドに保存されます。詳細については、IP アドレス（1-6 ページ）を参照してください。
宛先ホスト タイプ	uint8	宛先ホストのタイプ: • 0:ホスト • 1:ルータ • 2:ブリッジ
宛先 VLAN ID	uint16	宛先ホストの VLAN ID 番号（該当する場合）。
宛先 OS フィンガープリント UUID	uint8[16]	宛先ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID 番号。 フィンガープリント ID にマップする値の取得の詳細については、サーバ レコード（4-16 ページ）を参照してください。
宛先重要度	uint16	宛先ホストの、ユーザ定義の重要度値: • 0:なし • 1:低 • 2:中 • 3:高

表 B-45　相関イベント データ 5.1 ～ 5.3.x のフィールド（続き）

フィールド	データ タイプ	説明
宛先ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
接続先ポート	uint16	イベントの宛先ポート。
宛先サービス ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
ブロック	uint8	侵入イベントをトリガーしたパケットの処理を示す値。 • 0：侵入イベントがドロップされていない • 1：侵入イベントがドロップされている（展開がインライン型、スイッチ型、またはルーティング型である場合はドロップ） • 2：侵入ポリシーが、インライン型、スイッチ型、またはルーティング型展開のデバイスに適用されている場合は、イベントをトリガーしたパケットがドロップされている可能性がある。
入力インターフェイス UUID	uint8[16]	相関イベントに関連付けられている入力インターフェイスの固有識別子として機能するインターフェイス ID。
出力インターフェイス UUID	uint8[16]	相関イベントに関連付けられている出力インターフェイスの固有識別子として機能するインターフェイス ID。
入力ゾーン UUID	uint8[16]	相関イベントに関連付けられている入力セキュリティ ゾーンの固有識別子として機能するゾーン ID。
出力ゾーン UUID	uint8[16]	相関イベントに関連付けられている出力セキュリティ ゾーンの固有識別子として機能するゾーン ID。
送信元 IPv6 アドレス	uint8[16]	IPv6 アドレス オクテットの、イベントの送信元ホストの IP アドレス。
宛先 IPv6 アドレス	uint8[16]	IPv6 アドレス オクテットの、イベントの宛先ホストの IP アドレス。

レガシー ホスト データ構造

これらの構造を要求するには、ホスト要求メッセージを使用する必要があります。レガシー構造を要求するには、古い形式のホスト要求メッセージを使用する必要があります。詳細については、ホスト要求メッセージの形式（2-27 ページ）を参照してください。

続くいくつかのトピックでは、ホスト プロファイルとフル ホスト プロファイルの両方の構造を含む、レガシー ホスト データ構造について説明します。

フル ホスト プロファイル データ ブロック 5.0 ～ 5.0.2

フル ホスト プロファイル データ ブロック バージョン 5.0 ～ 5.0.2 には、1 つのホストを記述するフルセットのデータが含まれています。このデータ セットの形式を次の図に示し、次表で説明します。図には、リスト データ ブロックを除き、カプセル化データ ブロック フィールドを提示していない点にご注意ください。これらのカプセル化データ ブロックは、検出と接続データ構造の概要（4-1 ページ）で別途説明します。フル ホスト プロファイル データ ブロックのブロック タイプ値は、111 です。

（注） 次の図において、ブロック名の横にあるアスタリスク（*）は、データ ブロックのインスタンスが複数発生する可能性があることを示しています。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	フル ホスト プロファイル データ ブロック（111）																																
	データ ブロック長																																
	[IPアドレス																																
	ホップ									汎用リスト ブロック タイプ（31）																							
	汎用リスト ブロック タイプ（続き）									汎用リスト ブロック長																							
OS 派生フィンガープリント	汎用リスト ブロック長（続き）									オペレーティング システム フィンガープリント ブロック タイプ（130）*																							
	OS フィンガープリント ブロック タイプ（130）*（続き）									オペレーティング システム フィンガープリント ブロック長																							
	OS フィンガープリント ブロック長（続き）									オペレーティング システム派生のフィンガープリント データ…																							
	汎用リスト ブロック タイプ（31）																																
	汎用リスト ブロック長																																
サーバ フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ（130）*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム サーバのフィンガープリント データ…																																

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
クライアント フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム クライアントのフィンガープリント データ…																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
VDB ネイティブ フィンガープリント 1	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム VDB のフィンガープリント データ…																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
VDB ネイティブ フィンガープリント 2	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム VDB のフィンガープリント データ…																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
ユーザ フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム ユーザのフィンガープリント データ…																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
スキャン フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム スキャンのフィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
アプリケーション フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム アプリケーションのフィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
競合 フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム競合のフィンガープリント データ…																															
(TCP)フル サーバ データ	リスト ブロック タイプ(11)…																															
	リスト ブロック長...																															
	(TCP)フル サーバ データ ブロック(104)*																															
(UDP)フル サーバ データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	(UDP)フル サーバ データ ブロック(104)*																															
ネットワーク プロトコル データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	(ネットワーク)プロトコル データ ブロック(4)*																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
トランスポートプロトコルデータ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	(トランスポート)プロトコル データ ブロック(4)*																															
MAC アドレス データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	ホスト MAC アドレス データ ブロック(95)*																															
	最後の確認日時																															
	ホスト タイプ																															
	ビジネス上の重要度																VLAN ID															
	VLAN タイプ								VLAN 優先順位								汎用リスト ブロック タイプ(31)															
ホスト クライアント データ	汎用リスト ブロック タイプ(続き)																汎用リスト ブロック長															
	汎用リスト ブロック長(続き)																フル ホスト クライアント アプリケーション データ ブロック(112)*															
NetBIOS 名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	NetBIOS 名前文字列...																															
注記 データ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	注記文字列...																															
(VDB)ホスト Vuln	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	(VDB)ホスト脆弱性データ ブロック(85)*																															
(サード パーティ/VDB)ホスト Vuln	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	(サードパーティ/VDB)ホスト脆弱性データ ブロック(85)*																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
サード パーティ スキャン ホスト Vuln	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	元の Vuln ID を持つ(サード パーティ スキャン)ホスト脆弱性データ ブロック(85)*																															
属性値 データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	属性値データ ブロック*																															

次の表は、フル ホスト プロファイル 5.0 ～ 5.0.2 レコードのコンポーネントについての説明です。

表 B-46　　フル ホスト プロファイル レコード 5.0 ～ 5.0.2 のフィールド

フィールド	データ タイプ	説明
IPアドレス	uint8[4]	IP アドレス オクテットの、ホストの IP アドレス。
ホップ	uint8	ホストからのデバイスまでのネットワーク ホップ数。
汎用リスト ブロック タイプ	uint32	ホストの既存のフィンガープリントから派生したフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム派生のフィンガープリント データ ブロック*	変数	ホストの既存のフィンガープリントから派生したホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	サーバ フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。

表 B-46　フル ホスト プロファイル レコード 5.0 ～ 5.0.2 のフィールド（続き）

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント（サーバ フィンガープリント）データ ブロック*	変数	サーバ フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	クライアント フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。
オペレーティング システム フィンガープリント（クライアント フィンガープリント）データ ブロック*	変数	クライアント フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	Cisco VDB フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。
オペレーティング システム フィンガープリント（VDB）ネイティブ フィンガープリント（1）データ ブロック*	変数	Cisco 脆弱性データベース（VDB）のフィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	Cisco VDB フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。

表 B-46　フル ホスト プロファイル レコード 5.0 ～ 5.0.2 のフィールド(続き)

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント(VDB)ネイティブ フィンガープリント(2)データ ブロック*	変数	Cisco 脆弱性データベース(VDB)のフィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	ユーザによって追加されたフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(ユーザ フィンガープリント)データ ブロック*	変数	ユーザによって追加されたホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	脆弱性スキャナによって追加されたフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(スキャン フィンガープリント)データ ブロック*	変数	脆弱性スキャナによって追加されたホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	アプリケーションによって追加されたフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。

表 B-46　フル ホスト プロファイル レコード 5.0 ～ 5.0.2 のフィールド（続き）

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント（アプリケーション フィンガープリント）データ ブロック*	変数	アプリケーションによって追加されたホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	フィンガープリント競合解決により選択されたフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。
オペレーティング システム フィンガープリント（競合フィンガープリント）データ ブロック*	変数	フィンガープリント競合解決により選択されたホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
リストブロック タイプ	uint32	TCP サービス データを伝えるフル サーバ データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのフル サーバ データ ブロック長が含まれています。
（TCP）フル サーバ データ ブロック*	変数	ホスト上の TCP サービスに関するデータを伝えるフル サーバ データ ブロックのリスト。このデータ ブロックの説明の詳細については、フル ホスト サーバ データ ブロック 4.10.0+（4-145 ページ）を参照してください。
リストブロック タイプ	uint32	UDP サービス データを伝えるフル サーバ データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのフル サーバ データ ブロック長が含まれています。
（UDP）フル サーバ データ ブロック*	変数	ホスト上の UDP サブサーバに関するデータを伝えるフル サーバ データ ブロックのリスト。このデータ ブロックの説明の詳細については、フル ホスト サーバ データ ブロック 4.10.0+（4-145 ページ）を参照してください。
リストブロック タイプ	uint32	ネットワーク プロトコル データを伝えるプロトコル データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。

表 B-46　フル ホスト プロファイル レコード 5.0 ～ 5.0.2 のフィールド(続き)

フィールド	データ タイプ	説明
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのプロトコル データ ブロック長が含まれています。
(ネットワーク)プロトコル データ ブロック*	変数	ホスト上のネットワーク プロトコルに関するデータを伝えるプロトコル データ ブロックのリスト。このデータ ブロックの説明の詳細については、プロトコル データ ブロック (4-78 ページ) を参照してください。
リストブロック タイプ	uint32	トランスポート プロトコル データを伝えるプロトコル データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのプロトコル データ ブロック長が含まれています。
(転送)プロトコル データ ブロック*	変数	ホスト上のトランスポート プロトコルに関するデータを伝えるプロトコル データ ブロックのリスト。このデータ ブロックの説明の詳細については、プロトコル データ ブロック (4-78 ページ) を参照してください。
リストブロック タイプ	uint32	ホスト MAC アドレス データ ブロックを含むリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リストのバイト数(リスト ヘッダーと、カプセル化されたすべてのホスト MAC アドレス データ ブロックを含む)。
ホスト MAC アドレス データ ブロック*	変数	ホスト MAC アドレス データ ブロックのリスト。このデータ ブロックの説明の詳細については、ホスト MAC アドレス 4.9+ (4-119 ページ) を参照してください。
最後の確認日時	uint32	システムがホストのアクティビティを検出した最終時刻を表す UNIX タイムスタンプ。
ホスト タイプ	uint32	ホストのタイプを示します。次の値を指定します。 • 0:ホスト • 1:ルータ • 2:ブリッジ • 3:NAT(ネットワーク アドレス変換デバイス) • 4:LB(ロード バランサ)
ビジネス上の重要度	uint16	ビジネスに対するホストの重要度を示します。
VLAN ID	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグにカプセル化されたパケットのタイプ。
VLAN 優先順位	uint8	VLAN タグに含まれる優先順位値。
汎用リスト ブロック タイプ	uint32	クライアント アプリケーション データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。

表 B-46　フル ホスト プロファイル レコード 5.0 ～ 5.0.2 のフィールド（続き）

フィールド	データ タイプ	説明
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのクライアント アプリケーション データ ブロックを含む）。
フル ホスト クライアント アプリケーション データ ブロック*	変数	クライアント アプリケーション データのブロックのリスト。このデータ ブロックの説明の詳細については、フル クライアント アプリケーション データ ブロック 5.0+（4-159 ページ）を参照してください。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数（文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む）。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	ホスト注記の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	注記文字列データ ブロックのバイト数（文字列ブロック タイプと長さのフィールド用の 8 バイト、および注記文字列のバイト数を含む）。
注記	string	ホストの注記ホスト属性の内容が含まれます。
汎用リスト ブロック タイプ	uint32	VDB 脆弱性データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのデータ ブロックを含む）。
（VDB）ホスト脆弱性データ ブロック*	変数	Cisco 脆弱性データベース（VDB）で識別される脆弱性の、ホスト脆弱性データ ブロックのリスト。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+（4-116 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	サード パーティ スキャン脆弱性データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのデータ ブロックを含む）。
（サード パーティ/VDB）ホスト脆弱性データ ブロック*	変数	サード パーティ スキャナから送信され、Cisco 脆弱性データベース（VDB）でカタログされているホスト脆弱性に関する情報が含まれている、ホスト脆弱性データ ブロック。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+（4-116 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	サード パーティ スキャン脆弱性データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのデータ ブロックを含む）。

表 B-46　フル ホスト プロファイル レコード 5.0 ～ 5.0.2 のフィールド(続き)

フィールド	データ タイプ	説明
(サードパーティ スキャン)ホスト脆弱性データ ブロック*	変数	サード パーティ スキャナから送信されたホスト脆弱性データ ブロック。これらのデータ ブロックのホスト脆弱性 ID は、Cisco 検出の ID ではなく、サード パーティ スキャナ ID であることに注意してください。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+(4-116 ページ)を参照してください。
リスト ブロック タイプ	uint32	属性データを伝える属性値データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのデータ ブロックを含む)。
属性値データ ブロック*	変数	属性値データ ブロックのリスト。このリスト内のデータ ブロックの説明の詳細については、属性値データ ブロック(4-84 ページ)を参照してください。

フル ホスト プロファイル データ ブロック 5.1.1

フル ホスト プロファイル データ ブロック バージョン 5.1.1 には、1 つのホストを記述するフル セットのデータが含まれています。このデータ セットの形式を次の図に示し、次表で説明します。図には、リスト データ ブロックを除き、カプセル化データ ブロック フィールドを提示していない点にご注意ください。これらのカプセル化データ ブロックは、検出と接続データ構造の概要 (4-1 ページ)で別途説明します。フル ホスト プロファイル データ ブロックのブロック タイプ値は、135 です。これによりデータ ブロック 111 は廃止されます。

(注)　次の図において、ブロック名の横にあるアスタリスク(*)は、データ ブロックのインスタンスが複数発生する可能性があることを示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	フル ホスト プロファイル データ ブロック(135)																															
	データ ブロック長																															
	IPアドレス																															
	ホップ								汎用リスト ブロック タイプ(31)																								
	汎用リスト ブロック タイプ(続き)								汎用リスト ブロック長																							
OS 派生フィンガープリント	汎用リスト ブロック長(続き)								オペレーティング システム フィンガープリント ブロック タイプ(130)*																							
	OS フィンガープリント ブロック タイプ(130)*(続き)								オペレーティング システム フィンガープリント ブロック長																							
	OS フィンガープリント ブロック長(続き)								オペレーティング システム派生のフィンガープリント データ...																							
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
サーバ フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム サーバのフィンガープリント データ...																															

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
クライアント フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム クライアントのフィンガープリント データ…																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
VDB ネイティブ フィンガー プリント 1	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム VDB のフィンガープリント データ…																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
VDB ネイティブ フィンガー プリント 2	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム VDB のフィンガープリント データ…																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
ユーザ フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム ユーザのフィンガープリント データ…																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
スキャン フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム スキャンのフィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
アプリケーション フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム アプリケーションのフィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
競合 フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム競合のフィンガープリント データ…																															
(TCP)フル サーバ データ	リスト ブロック タイプ(11)…																															
	リスト ブロック長...																															
	(TCP)フル サーバ データ ブロック(104)*																															
(UDP)フル サーバ データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	(UDP)フル サーバ データ ブロック(104)*																															
ネットワーク プロトコル データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	(ネットワーク)プロトコル データ ブロック(4)*																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
トランスポート プロトコル データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	(トランスポート)プロトコル データ ブロック(4)*																															
MAC アドレス データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	ホスト MAC アドレス データ ブロック(95)*																															
	最後の確認日時																															
	ホスト タイプ																															
	ビジネス上の重要度																VLAN ID															
	VLAN タイプ								VLAN 優先順位								汎用リスト ブロック タイプ(31)															
ホスト クライアント データ	汎用リスト ブロック タイプ(続き)																汎用リスト ブロック長															
	汎用リスト ブロック長(続き)																フル ホスト クライアント アプリケーション データ ブロック(112)*															
NetBIOS 名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	NetBIOS 名前文字列...																															
注記 データ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	注記文字列...																															
(VDB)ホスト Vuln	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	(VDB)ホスト脆弱性データ ブロック(85)*																															
(サード パーティ/VDB) ホスト Vuln	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	(サードパーティ/VDB)ホスト脆弱性データ ブロック(85)*																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
サード パーティ スキャン ホスト Vuln	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	元の Vuln ID を持つ(サード パーティ スキャン)ホスト脆弱性データ ブロック(85)*																															
属性値 データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	属性値データ ブロック*																															
	モバイル								改造								VLAN の有無															

次の表は、フル ホスト プロファイル 5.1.1 レコードのコンポーネントについての説明です。

表 B-47　フル ホスト プロファイル レコード 5.1.1 のフィールド

フィールド	データ タイプ	説明
IPアドレス	uint8[4]	IP アドレス オクテットの、ホストの IP アドレス。
ホップ	uint8	ホストからのデバイスまでのネットワーク ホップ数。
汎用リスト ブロック タイプ	uint32	ホストの既存のフィンガープリントから派生したフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム派生のフィンガープリント データ ブロック*	変数	ホストの既存のフィンガープリントから派生したホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	サーバ フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。

表 B-47　フル ホスト プロファイル レコード 5.1.1 のフィールド(続き)

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント(サーバ フィンガープリント)データ ブロック*	変数	サーバ フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	クライアント フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(クライアント フィンガープリント)データ ブロック*	変数	クライアント フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	Cisco VDB フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(VDB)ネイティブ フィンガープリント(1)データ ブロック*	変数	Cisco 脆弱性データベース(VDB)のフィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	Cisco VDB フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。

表 B-47　フル ホスト プロファイル レコード 5.1.1 のフィールド（続き）

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント（VDB）ネイティブ フィンガープリント（2）データ ブロック*	変数	Cisco 脆弱性データベース（VDB）のフィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	ユーザによって追加されたフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。
オペレーティング システム フィンガープリント（ユーザ フィンガープリント）データ ブロック*	変数	ユーザによって追加されたホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	脆弱性スキャナによって追加されたフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。
オペレーティング システム フィンガープリント（スキャン フィンガープリント）データ ブロック*	変数	脆弱性スキャナによって追加されたホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	アプリケーションによって追加されたフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。

表 B-47　フル ホスト プロファイル レコード 5.1.1 のフィールド(続き)

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント(アプリケーション フィンガープリント)データ ブロック*	変数	アプリケーションによって追加されたホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	フィンガープリント競合解決により選択されたフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(競合フィンガープリント)データ ブロック*	変数	フィンガープリント競合解決により選択されたホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
リストブロック タイプ	uint32	TCP サービス データを伝えるフル サーバ データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのフル サーバ データ ブロック長が含まれています。
(TCP)フル サーバ データ ブロック*	変数	ホスト上の TCP サービスに関するデータを伝えるフル サーバ データ ブロックのリスト。このデータ ブロックの説明の詳細については、フル ホスト サーバ データ ブロック 4.10.0+(4-145 ページ)を参照してください。
リストブロック タイプ	uint32	UDP サービス データを伝えるフル サーバ データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのフル サーバ データ ブロック長が含まれています。
(UDP)フル サーバ データ ブロック*	変数	ホスト上の UDP サブサーバに関するデータを伝えるフル サーバ データ ブロックのリスト。このデータ ブロックの説明の詳細については、フル ホスト サーバ データ ブロック 4.10.0+(4-145 ページ)を参照してください。
リストブロック タイプ	uint32	ネットワーク プロトコル データを伝えるプロトコル データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。

表 B-47　フル ホスト プロファイル レコード 5.1.1 のフィールド（続き）

フィールド	データ タイプ	説明
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのプロトコル データ ブロック長が含まれています。
（ネットワーク）プロトコル データ ブロック*	変数	ホスト上のネットワーク プロトコルに関するデータを伝えるプロトコル データ ブロックのリスト。このデータ ブロックの説明の詳細については、プロトコル データ ブロック（4-78 ページ）を参照してください。
リストブロック タイプ	uint32	トランスポート プロトコル データを伝えるプロトコル データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのプロトコル データ ブロック長が含まれています。
（転送）プロトコル データ ブロック*	変数	ホスト上のトランスポート プロトコルに関するデータを伝えるプロトコル データ ブロックのリスト。このデータ ブロックの説明の詳細については、プロトコル データ ブロック（4-78 ページ）を参照してください。
リストブロック タイプ	uint32	ホスト MAC アドレス データ ブロックを含むリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リストのバイト数（リスト ヘッダーと、カプセル化されたすべてのホスト MAC アドレス データ ブロックを含む）。
ホスト MAC アドレス データ ブロック*	変数	ホスト MAC アドレス データ ブロックのリスト。このデータ ブロックの説明の詳細については、ホスト MAC アドレス 4.9+（4-119 ページ）を参照してください。
最後の確認日時	uint32	システムがホストのアクティビティを検出した最終時刻を表す UNIX タイムスタンプ。
ホスト タイプ	uint32	ホストのタイプを示します。次の値を指定します。 • 0：ホスト • 1：ルータ • 2：ブリッジ • 3：NAT（ネットワーク アドレス変換デバイス） • 4：LB（ロード バランサ）
ビジネス上の重要度	uint16	ビジネスに対するホストの重要度を示します。
VLAN ID	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグにカプセル化されたパケットのタイプ。
VLAN 優先順位	uint8	VLAN タグに含まれる優先順位値。
汎用リスト ブロック タイプ	uint32	クライアント アプリケーション データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。

表 B-47　フル ホスト プロファイル レコード 5.1.1 のフィールド(続き)

フィールド	データ タイプ	説明
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのクライアント アプリケーション データ ブロックを含む)。
フル ホスト クライアント アプリケーション データ ブロック*	変数	クライアント アプリケーション データのブロックのリスト。このデータ ブロックの説明の詳細については、フル クライアント アプリケーション データ ブロック 5.0+(4-159 ページ)を参照してください。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	ホスト注記の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	注記文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、および注記文字列のバイト数を含む)。
注記	string	ホストの注記ホスト属性の内容が含まれます。
汎用リスト ブロック タイプ	uint32	VDB 脆弱性データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのデータ ブロックを含む)。
(VDB)ホスト脆弱性データ ブロック*	変数	Cisco 脆弱性データベース(VDB)で識別される脆弱性の、ホスト脆弱性データ ブロックのリスト。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+(4-116 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	サード パーティ スキャン脆弱性データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのデータ ブロックを含む)。
(サード パーティ/VDB)ホスト脆弱性データ ブロック*	変数	サード パーティ スキャナから送信され、Cisco 脆弱性データベース(VDB)でカタログされているホスト脆弱性に関する情報が含まれている、ホスト脆弱性データ ブロック。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+(4-116 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	サード パーティ スキャン脆弱性データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのデータ ブロックを含む)。

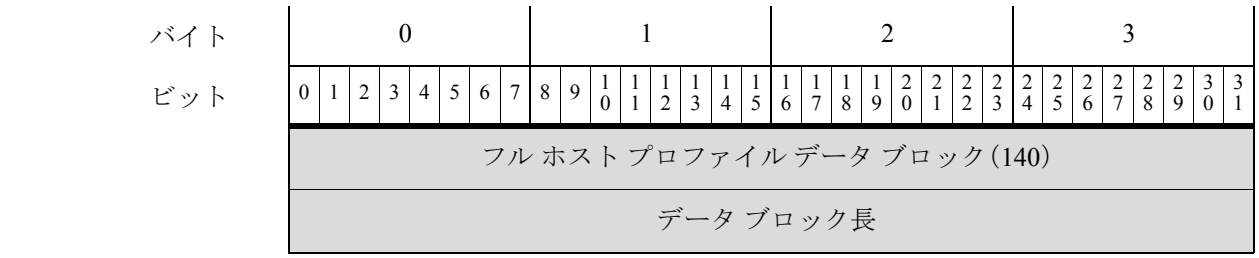
表 B-47　フル ホスト プロファイル レコード 5.1.1 のフィールド（続き）

フィールド	データ タイプ	説明
（サードパーティ スキャン）ホスト脆弱性データ ブロック*	変数	サード パーティ スキャナから送信されたホスト脆弱性データ ブロック。これらのデータ ブロックのホスト脆弱性 ID は、Cisco 検出の ID ではなく、サード パーティ スキャナ ID であることに注意してください。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+（4-116 ページ）を参照してください。
リスト ブロック タイプ	uint32	属性データを伝える属性値データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのデータ ブロックを含む）。
属性値データ ブロック*	変数	属性値データ ブロックのリスト。このリスト内のデータ ブロックの説明の詳細については、属性値データ ブロック（4-84 ページ）を参照してください。
モバイル	uint8	オペレーティング システムがモバイル デバイスで動作しているかどうかを示す true/false フラグ。
改造	uint8	モバイル デバイスのオペレーティング システムがジェイルブレイクされているかどうかを示す true/false フラグ。
VLAN の有無	uint8	VLAN が存在するかどうかを示します。 • 0：はい • 1：いいえ

フル ホスト プロファイル データ ブロック 5.2.x

フル ホスト プロファイル データ ブロック バージョン 5.2.x には、1 つのホストを記述するフル セットのデータが含まれています。このデータ セットの形式を次の図に示し、次表で説明します。図には、リスト データ ブロックを除き、カプセル化データ ブロック フィールドを提示していない点にご注意ください。これらのカプセル化データ ブロックは、検出と接続データ構造の概要（4-1 ページ）で別途説明します。フル ホスト プロファイル データ ブロックのブロック タイプ値は、140 です。これは以前のバージョン（ブロック タイプが 135 である）に取って代わります。

（注） 次の図において、ブロック名の横にあるアスタリスク（*）は、データ ブロックのインスタンスが複数発生する可能性があることを示しています。



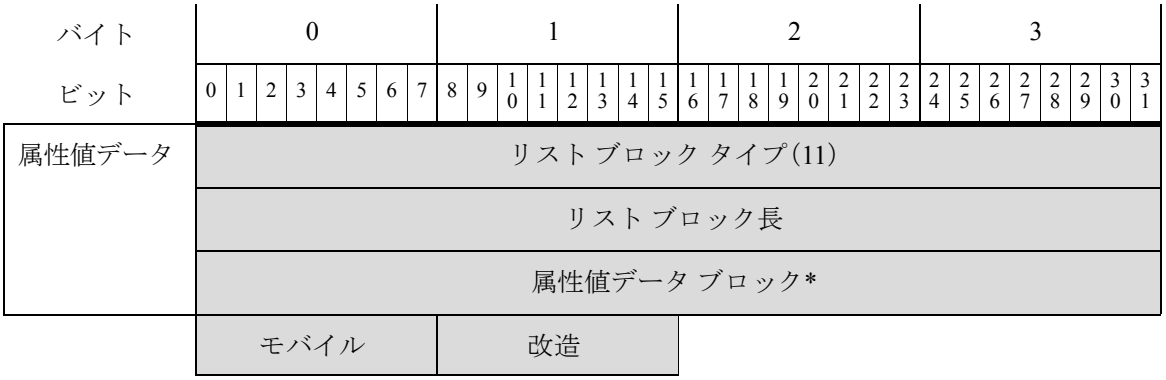
	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ホスト ID																																
	ホスト ID（続き）																																
	ホスト ID（続き）																																
	ホスト ID（続き）																																
IP アドレス	リスト ブロック タイプ（11）																																
	リスト ブロック長																																
	IP アドレス データ ブロック（143）*																																
	ホップ									汎用リスト ブロック タイプ（31）																							
	汎用リスト ブロック タイプ（続き）									汎用リスト ブロック長																							
OS 派生フィンガープリント	汎用リスト ブロック長（続き）									オペレーティング システム フィンガープリント ブロック タイプ（130）*																							
	OS フィンガープリント ブロック タイプ（130）*（続き）									オペレーティング システム フィンガープリント ブロック長																							
	OS フィンガープリント ブロック長（続き）									オペレーティング システム派生のフィンガープリント データ…																							
	汎用リスト ブロック タイプ（31）																																
	汎用リスト ブロック長																																
サーバ フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ（130）*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム サーバのフィンガープリント データ…																																
	汎用リスト ブロック タイプ（31）																																
	汎用リスト ブロック長																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
クライアント フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム クライアントのフィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
VDB ネイティブ フィンガー プリント 1	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム VDB のフィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
VDB ネイティブ フィンガー プリント 2	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム VDB のフィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
ユーザ フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム ユーザのフィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
スキャン フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム スキャンのフィンガープリント データ…																															
	汎用リスト ブロック タイプ(31)																															

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用リスト ブロック長																																
アプリケーション フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム アプリケーションのフィンガープリント データ…																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
競合フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム競合のフィンガープリント データ…																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
モバイル フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム モバイル フィンガープリント データ…																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
IPv6 サーバ フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム IPv6 サーバのフィンガープリント データ…																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
Ipv6 クライアントフィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム IPv6 クライアントのフィンガープリント データ…																																

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
IPv6 DHCP フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム IPv6 DHCP のフィンガープリント データ…																																
	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
ユーザ エージェント フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																																
	オペレーティング システム フィンガープリント ブロック長																																
	オペレーティング システム ユーザ エージェントのフィンガープリント データ…																																
(TCP)フル サーバ データ	リスト ブロック タイプ(11)…																																
	リスト ブロック長...																																
	(TCP)フル サーバ データ ブロック(104)*																																
(UDP)フル サーバ データ	リスト ブロック タイプ(11)																																
	リスト ブロック長																																
	(UDP)フル サーバ データ ブロック(104)*																																
ネットワーク プロトコル データ	リスト ブロック タイプ(11)																																
	リスト ブロック長																																
	(ネットワーク)プロトコル データ ブロック(4)*																																
トランスポート プロトコル データ	リスト ブロック タイプ(11)																																
	リスト ブロック長																																
	(トランスポート)プロトコル データ ブロック(4)*																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MAC アドレス データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	ホスト MAC アドレス データ ブロック(95)*																															
	最後の確認日時																															
	ホスト タイプ																															
	ビジネス上の重要度																VLAN ID															
	VLAN タイプ								VLAN 優先順位								汎用リスト ブロック タイプ(31)															
ホスト クライアント データ	汎用リスト ブロック タイプ(続き)																汎用リスト ブロック長															
	汎用リスト ブロック長(続き)																フル ホスト クライアント アプリケーション データ ブロック(112)*															
NetBIOS 名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	NetBIOS 名前文字列...																															
注記 データ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	注記文字列...																															
(VDB)ホスト Vuln	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	(VDB)ホスト脆弱性データ ブロック(85)*																															
(サード パーティ/VDB)ホスト Vuln	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	(サードパーティ/VDB)ホスト脆弱性データ ブロック(85)*																															
サード パーティ スキャンホスト Vuln	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	元の Vuln ID を持つ(サード パーティ スキャン)ホスト脆弱性データ ブロック(85)*																															



次の表は、フル ホスト プロファイル 5.2.x レコードのコンポーネントについての説明です。

表 B-48　フル ホスト プロファイル レコード 5.2.x のフィールド

フィールド	データ タイプ	説明
ホスト ID	uint8[16]	ホストの固有 ID 番号。これは UUID です。
リストブロック タイプ	uint32	TCP サービス データを伝える IP アドレス データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべての IP アドレス データ ブロック長が含まれています。
IPアドレス	変数	ホストの IP アドレスおよび各 IP アドレスを最後に確認した日時。このデータ ブロックの説明の詳細については、ホスト IP アドレス データ ブロック (4-100 ページ) を参照してください。
ホップ	uint8	ホストからのデバイスまでのネットワーク ホップ数。
汎用リスト ブロック タイプ	uint32	ホストの既存のフィンガープリントから派生したフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム派生のフィンガープリント データ ブロック*	変数	ホストの既存のフィンガープリントから派生したホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+ (4-166 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	サーバ フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。

表 B-48　フル ホスト プロファイル レコード 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント(サーバ フィンガープリント)データ ブロック*	変数	サーバ フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	クライアント フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(クライアント フィンガープリント)データ ブロック*	変数	クライアント フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	Cisco VDB フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(VDB)ネイティブ フィンガープリント(1)データ ブロック*	変数	Cisco 脆弱性データベース(VDB)のフィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	Cisco VDB フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。

表 B-48　フル ホスト プロファイル レコード 5.2.x のフィールド（続き）

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント（VDB）ネイティブ フィンガープリント（2）データ ブロック*	変数	Cisco 脆弱性データベース（VDB）のフィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	ユーザによって追加されたフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。
オペレーティング システム フィンガープリント（ユーザ フィンガープリント）データ ブロック*	変数	ユーザによって追加されたホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	脆弱性スキャナによって追加されたフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。
オペレーティング システム フィンガープリント（スキャン フィンガープリント）データ ブロック*	変数	脆弱性スキャナによって追加されたホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	アプリケーションによって追加されたフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。

表 B-48　フル ホスト プロファイル レコード 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント(アプリケーション フィンガープリント)データ ブロック*	変数	アプリケーションによって追加されたホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	フィンガープリント競合解決により選択されたフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(競合フィンガープリント)データ ブロック*	変数	フィンガープリント競合解決により選択されたホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	モバイル デバイス フィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(モバイル)データ ブロック*	変数	モバイル デバイス ホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	IPv6 サーバ フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。

表 B-48　フル ホスト プロファイル レコード 5.2.x のフィールド（続き）

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント（IPv6 サーバ フィンガープリント）データ ブロック*	変数	IPv6 サーバ フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	IPv6 クライアント フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。
オペレーティング システム フィンガープリント（IPv6 クライアント フィンガープリント）データ ブロック*	変数	IPv6 クライアント フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	IPv6 DHCP フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。
オペレーティング システム フィンガープリント（IPv6 DHCP）データ ブロック*	変数	IPv6 DHCP フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-166 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	エージェント フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。

表 B-48　フル ホスト プロファイル レコード 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント(ユーザ エージェント)データ ブロック*	変数	ユーザ エージェント フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
リスト ブロック タイプ	uint32	TCP サービス データを伝えるフル サーバ データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのフル サーバ データ ブロック長が含まれています。
(TCP)フル サーバ データ ブロック*	変数	ホスト上の TCP サービスに関するデータを伝えるフル サーバ データ ブロックのリスト。このデータ ブロックの説明の詳細については、フル ホスト サーバ データ ブロック 4.10.0+(4-145 ページ)を参照してください。
リスト ブロック タイプ	uint32	UDP サービス データを伝えるフル サーバ データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのフル サーバ データ ブロック長が含まれています。
(UDP)フル サーバ データ ブロック*	変数	ホスト上の UDP サブサーバに関するデータを伝えるフル サーバ データ ブロックのリスト。このデータ ブロックの説明の詳細については、フル ホスト サーバ データ ブロック 4.10.0+(4-145 ページ)を参照してください。
リスト ブロック タイプ	uint32	ネットワーク プロトコル データを伝えるプロトコル データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのプロトコル データ ブロック長が含まれています。
(ネットワーク)プロトコル データ ブロック*	変数	ホスト上のネットワーク プロトコルに関するデータを伝えるプロトコル データ ブロックのリスト。このデータ ブロックの説明の詳細については、プロトコル データ ブロック(4-78 ページ)を参照してください。
リスト ブロック タイプ	uint32	トランスポート プロトコル データを伝えるプロトコル データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのプロトコル データ ブロック長が含まれています。
(転送)プロトコル データ ブロック*	変数	ホスト上のトランスポート プロトコルに関するデータを伝えるプロトコル データ ブロックのリスト。このデータ ブロックの説明の詳細については、プロトコル データ ブロック(4-78 ページ)を参照してください。

表 B-48　フル ホスト プロファイル レコード 5.2.x のフィールド（続き）

フィールド	データ タイプ	説明
リストブロック タイプ	uint32	ホスト MAC アドレス データ ブロックを含むリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リストのバイト数（リスト ヘッダーと、カプセル化されたすべてのホスト MAC アドレス データ ブロックを含む）。
ホスト MAC アドレス データ ブロック*	変数	ホスト MAC アドレス データ ブロックのリスト。このデータ ブロックの説明の詳細については、ホスト MAC アドレス 4.9+（4-119 ページ）を参照してください。
最後の確認日時	uint32	システムがホストのアクティビティを検出した最終時刻を表す UNIX タイムスタンプ。
ホスト タイプ	uint32	ホストのタイプを示します。次の値を指定します。 • 0：ホスト • 1：ルータ • 2：ブリッジ • 3：NAT（ネットワーク アドレス変換デバイス） • 4：LB（ロード バランサ）
ビジネス上の重要度	uint16	ビジネスに対するホストの重要度を示します。
VLAN ID	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグにカプセル化されたパケットのタイプ。
VLAN 優先順位	uint8	VLAN タグに含まれる優先順位値。
汎用リスト ブロック タイプ	uint32	クライアント アプリケーション データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのクライアント アプリケーション データ ブロックを含む）。
フル ホスト クライアント アプリケーション データ ブロック*	変数	クライアント アプリケーション データのブロックのリスト。このデータ ブロックの説明の詳細については、フル クライアント アプリケーション データ ブロック 5.0+（4-159 ページ）を参照してください。
文字列ブロック タイプ	uint32	ホスト NetBIOS 名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数（文字列ブロック タイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む）。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	ホスト注記の文字列データ ブロックを開始します。この値は常に 0 です。

表 B-48　フル ホスト プロファイル レコード 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	注記文字列データ ブロックのバイト数(文字列ブロック タイプと長さのフィールド用の 8 バイト、および注記文字列のバイト数を含む)。
注記	string	ホストの注記ホスト属性の内容が含まれます。
汎用リスト ブロック タイプ	uint32	VDB 脆弱性データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのデータ ブロックを含む)。
(VDB)ホスト脆弱性データ ブロック*	変数	Cisco 脆弱性データベース(VDB)で識別される脆弱性の、ホスト脆弱性データ ブロックのリスト。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+(4-116 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	サード パーティ スキャン脆弱性データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのデータ ブロックを含む)。
(サード パーティ/VDB)ホスト脆弱性データ ブロック*	変数	サード パーティ スキャナから送信され、Cisco 脆弱性データベース(VDB)でカタログされているホスト脆弱性に関する情報が含まれている、ホスト脆弱性データ ブロック。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+(4-116 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	サード パーティ スキャン脆弱性データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのデータ ブロックを含む)。
(サードパーティ スキャン)ホスト脆弱性データ ブロック*	変数	サード パーティ スキャナから送信されたホスト脆弱性データ ブロック。これらのデータ ブロックのホスト脆弱性 ID は、Cisco 検出の ID ではなく、サード パーティ スキャナ ID であることに注意してください。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+(4-116 ページ)を参照してください。
リストブロック タイプ	uint32	属性データを伝える属性値データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのデータ ブロックを含む)。
属性値データ ブロック*	変数	属性値データ ブロックのリスト。このリスト内のデータ ブロックの説明の詳細については、属性値データ ブロック(4-84 ページ)を参照してください。

表 B-48　フル ホスト プロファイル レコード 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
モバイル	uint8	オペレーティング システムがモバイル デバイスで動作しているかどうかを示す true/false フラグ。
改造	uint8	モバイル デバイスのオペレーティング システムがジェイルブレイクされているかどうかを示す true/false フラグ。

ホスト プロファイル データ ブロック 5.1.x

次の図は、ホスト プロファイル データ ブロックの形式を示しています。さらに、このデータ ブロックには、ホスト重要度値が含まれていませんが、VLAN のプレゼンス インジケータは含まれています。さらに、このデータ ブロックは、ホストの NetBIOS 名を伝えることができます。ホスト プロファイル データ ブロックのブロック タイプは 132 です。

(注) 次の図のブロック タイプ フィールドの横のアスタリスク(*)は、メッセージにシリーズ 1 データ ブロックのゼロ以上のインスタンスが含まれる可能性があることを示しています。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ホスト プロファイル ブロック タイプ(132)																																
	ホスト プロファイル ブロック長																																
	IPアドレス																																
サーバ フィンガープリント	ホップ									プライマリ/セカンダリ								汎用リスト ブロック タイプ(31)															
	汎用リスト ブロック タイプ(続き)																	汎用リスト ブロック長															
	汎用リスト ブロック長(続き)																	サーバ フィンガープリント データ ブロック*															
クライアント フィンガープリント	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
	クライアント フィンガープリント データ ブロック*																																
SMB フィンガープリント	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
	SMB フィンガープリント データ ブロック*																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
DHCP フィンガープリント	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	DHCP フィンガープリント データ ブロック*																															
モバイル デバイス フィンガープリント	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	モバイル デバイス フィンガープリント データ ブロック*																															
TCP サーバ ブロック*	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	TCP サーバ データ ブロック																															
UDP サーバ ブロック*	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	UDP サーバ データ ブロック																															
ネットワーク プロトコル ブロック*	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	ネットワーク プロトコルのデータ ブロック																															
トランスポート プロトコル ブロック*	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	トランスポート プロトコル データ ブロック																															
MAC アドレス ブロック*	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	ホスト MAC アドレス データ ブロック																															
	最終検出時のホスト																															
	ホスト タイプ																															
	モバイル								改造								VLAN の有無								VLAN ID							

TCP のリスト サーバ	TCP サーバ ブロック*
UDP のリスト サーバ	UDP サーバ ブロック*
ネットワークのリスト プロトコル	ネットワーク プロトコル ブロック*
トランスポート リスト プロトコル	トランスポート プロトコル ブロック*
MAC のリスト アドレス	MAC アドレス ブロック*

次の表は、バージョン 5.1.x により返されるホスト プロファイル データ ブロックのフィールドについての説明です。

表 B-49　　ホスト プロファイル データ ブロック 5.1.x のフィールド

フィールド	データ タイプ	説明
ホスト プロファイル ブロック タイプ	uint32	ホスト プロファイル データ ブロック 5.1.x を開始します。この値は常に 132 です。
ホスト プロファイル ブロック長	uint32	ホスト プロファイル データ ブロックのバイト数(ホスト プロファイル ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くホスト プロファイル データに含まれるバイト数を含む)。
IPアドレス	uint8[4]	IP アドレス オクテットの、プロファイルに記述されているホストの IP アドレス。
ホップ	uint8	ホストからのデバイスまでのホップ数。
プライマリ/セカンダリ	uint8	ホストがそれを検出したデバイスのプライマリまたはセカンダリのどちらのネットワークにあるかを示します。 • 0:ホストはプライマリ ネットワークにあります。 • 1:ホストはセカンダリ ネットワークにあります。
汎用リスト ブロック タイプ	uint32	サーバ フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。

表 B-49　ホスト プロファイル データ ブロック 5.1.x のフィールド(続き)

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント(サーバ フィンガープリント)データ ブロック*	変数	サーバ フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	クライアント フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(クライアント フィンガープリント)データ ブロック*	変数	クライアント フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	SMB フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(SMB フィンガープリント)データ ブロック*	変数	SMB フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	DHCP フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。

表 B-49　ホスト プロファイル データ ブロック 5.1.x のフィールド(続き)

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント(DHCP フィンガープリント)データ ブロック*	変数	DHCP フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	DHCP フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(モバイル デバイス フィンガープリント)データ ブロック*	変数	モバイル デバイス フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)を参照してください。
リストブロック タイプ	uint32	TCP サーバ データを伝えるサーバ データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのサーバ データ ブロックが含まれています。 このフィールドには、ゼロ以上のサーバ データ ブロックが続きます。
TCP サーバ データ ブロック	変数	TCP サーバを記述するホスト サーバ データ ブロック(旧バージョンの製品で説明)。
リストブロック タイプ	uint32	UDP サーバ データを伝えるサーバ データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのサーバ データ ブロックが含まれています。 このフィールドには、ゼロ以上のサーバ データ ブロックが続きます。
UDP サーバ データ ブロック	uint32	UDP サーバを記述するホスト サーバ データ ブロック(旧バージョンの製品で説明)。
リストブロック タイプ	uint32	ネットワーク プロトコル データを伝えるプロトコル データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。

表 B-49　ホスト プロファイル データ ブロック 5.1.x のフィールド(続き)

フィールド	データ タイプ	説明
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのプロトコル データ ブロックが含まれています。 このフィールドには、ゼロ以上のプロトコル データ ブロックが続きます。
ネットワーク プロトコルのデータ ブロック	uint32	ネットワーク プロトコルを記述するプロトコル データ ブロック。このデータ ブロックの説明の詳細については、プロトコル データ ブロック (4-78 ページ) を参照してください。
リストブロック タイプ	uint32	トランスポート プロトコル データを伝えるプロトコル データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのプロトコル データ ブロックが含まれています。 このフィールドには、ゼロ以上のトランスポート プロトコル データ ブロックが続きます。
トランスポート プロトコル データ ブロック	uint32	トランスポート プロトコルを記述するプロトコル データ ブロック。このデータ ブロックの説明の詳細については、プロトコル データ ブロック (4-78 ページ) を参照してください。
リストブロック タイプ	uint32	MAC アドレス データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リストのバイト数(リスト ヘッダーと、カプセル化されたすべての MAC アドレス データ ブロックを含む)。
ホスト MAC アドレス データ ブロック	uint32	ホスト MAC アドレスを記述するホスト MAC アドレス データ ブロック。このデータ ブロックの説明の詳細については、ホスト MAC アドレス 4.9+ (4-119 ページ) を参照してください。
最終検出時のホスト	uint32	システムがホストのアクティビティを検出した最終時刻を表す UNIX タイムスタンプ。
ホスト タイプ	uint32	ホストのタイプを示します。表示される可能性がある値は次のとおりです。 • 0:ホスト • 1:ルータ • 2:ブリッジ • 3:NAT デバイス • 4:LB(ロード バランサ)
モバイル	uint8	検出したホストがモバイル デバイスであるかどうかを示す true/false フラグ。
改造	uint8	ホストが(ジェイルブレイクされていない)モバイル デバイスであるかどうかを示す true/false フラグ。

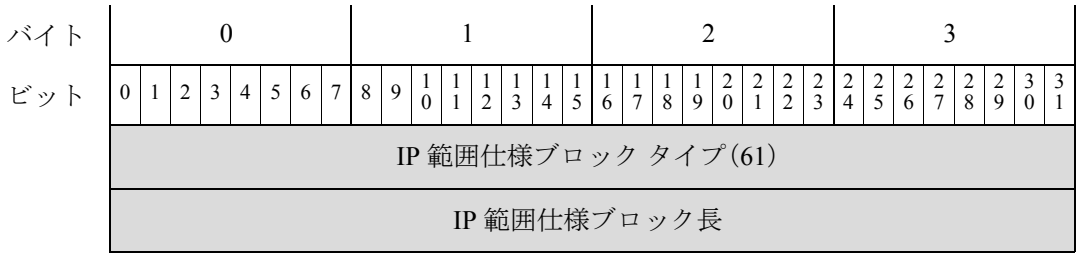
表 B-49　ホスト プロファイル データ ブロック 5.1.x のフィールド(続き)

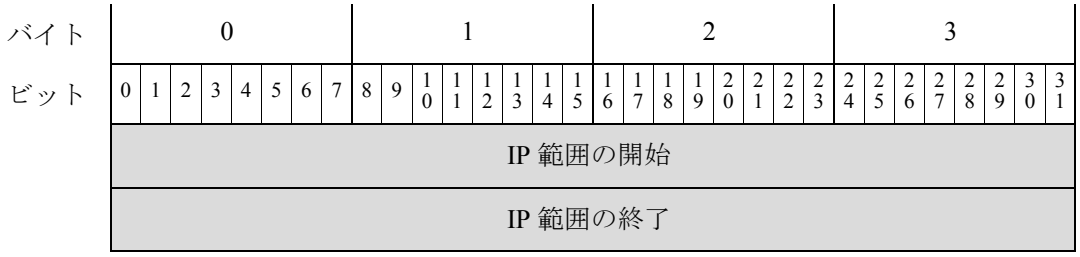
フィールド	データ タイプ	説明
VLAN の有無	uint8	VLAN が存在するかどうかを示します。 • 0:はい • 1:いいえ
VLAN ID	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグにカプセル化されたパケットのタイプ。
VLAN 優先順位	uint8	VLAN タグに含まれる優先順位値。
汎用リスト ブロック タイプ	uint32	クライアント アプリケーション データを伝えるクライアント アプリケーション データ ブロックで構成される汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのクライアント アプリケーション データ ブロックを含む)。
クライアント アプリケーション データ ブロック	uint32	クライアント アプリケーションを記述するクライアント アプリケーション データ ブロック。このデータ ブロックの説明の詳細については、フル クライアント アプリケーション データ ブロック 5.0+(4-159 ページ)を参照してください。
文字列ブロック タイプ	uint32	NetBIOS 名の文字列データ ブロックを開始します。この値は文字列データを示す 0 に設定されます。
文字列ブロック長	uint32	NetBIOS 名データ ブロックのバイト数を示します(文字列ブロック タイプと長さのフィールド用の 8 バイト、および NetBIOS 名のバイト数を含む)。
NetBIOS 文字列データ	変数	ホスト プロファイルに記述されているホストの NetBIOS 名が含まれます。

IP 範囲仕様データ ブロック 5.0 ～ 5.1.1.x

IP 範囲仕様データ ブロックは、一定範囲内の IP アドレスを伝えます。IP 範囲仕様データ ブロックは、ユーザ プロトコル、ユーザ クライアント アプリケーション、アドレス指定、ユーザ製品、ユーザ サーバ、ユーザ ホスト、ユーザ脆弱性、ユーザ重要度、およびユーザ属性値の各データ ブロックで使用されます。IP 範囲仕様データ ブロックのブロック タイプは 61 です。

次の図は、IP 範囲仕様データ ブロックの形式を示しています。





次の表は、IP 範囲仕様データ ブロックのコンポーネントについての説明です。

表 B-50　　IP 範囲仕様データ ブロックのフィールド

フィールド	データ タイプ	説明
IP 範囲仕様データ ブロック タイプ	uint32	IP 範囲仕様データ ブロックを開始します。この値は常に 61 です。
IP 範囲仕様ブロック長	uint32	IP 範囲仕様データ ブロックのバイトの合計数（IP 範囲仕様ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く IP 範囲仕様データのバイト数を含む）。
IP 範囲仕様の開始	uint32	IP アドレス範囲の開始 IP アドレス。
IP 範囲仕様の終了	uint32	IP アドレス範囲の最終 IP アドレス。

アクセス コントロール ポリシー ルール理由データ ブロック

eStreamer サービスは、アクセス コントロール ルールのポリシー ルールの理由のデータ ブロックを使用して、アクセス コントロール ポリシー ルール ID に関する情報を表示します。このデータ ブロックは、シリーズ 2 のブロック タイプ 21 です。

次の図に、アクセス コントロール ポリシー ルール ID のメタデータ ブロックの構造を示します。

次の表に、アクセス コントロール ポリシー ルール ID のメタデータ ブロックのフィールドの説明を示します。

表 B-51　アクセス コントロール ポリシー ルール理由データ ブロックのフィールド

フィールド	データ タイプ	説明
アクセス コントロール ポリシー ルール理由データ ブロック タイプ	uint32	アクセス コントロール ポリシー ルール理由データ ブロックを開始します。この値は常に 21 です。
アクセス コントロール ポリシー ルールの理由のデータ ブロックの長さ	uint32	アクセス コントロール ポリシー ルール理由データ ブロックのバイトの合計数（アクセス コントロール ポリシー ルール理由データ ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む）。
理由	uint16	イベントをトリガーしたルールの理由の番号。
文字列ブロック タイプ	uint32	アクセス コントロール ポリシー ルール理由の説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	ルールの理由の説明。

数字

B

E

I

M

N

O

T

U

V

W

あ

い

え

お

か

く

け

こ

さ

し

す

せ

そ

て

な

ぬ

ね

は

ふ

ほ

ま

め

も

ゆ

よ

り

る

れ