Cisco Secure Firewall eStreamer 統合ガイド

バージョン 7.2
2023 年 5 月 26 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスココンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【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。

はじめに

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

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

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

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

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

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

eStreamer バージョン 7.2 の主要な変更点

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

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

このガイドの使用方法

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

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

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

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

前提条件

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

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

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

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

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

表記法

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

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

Cisco 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。

ベストプラクティス

eStreamer を使用する際は、次に示す API の最善の使用方法を推奨します。

設計

- クライアントには、Python で記述されたシスコの着脱可能な eStreamer クライアントを基盤として使用することを検討してください。これにより、SIEM のスキーマでデータをフォーマットする際にプラグインを構築するだけで済みます。
- スキーマのあらゆる部分がカスタマー ベースのどこかしらで重要となるため、eStreamer クライアントは API で提供できるすべての内容をサポートするように構築してください。
  - メッセージの構造を理解する：『eStreamer Integration Guide』で理解を深めます。
  - メタデータ構造およびコード構造で定義されたレコードを取得する：ほとんどのレコードでメッセージを解析できます。
  - メタデータの一般的な仕組みについて理解する（メタデータ レコードの事前送信など）。

  - オブジェクト モデルについて理解する：レコードを相互に関連付ける方法と、レコードに関連付けられるメタデータの内容について理解を深めます。

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

テスト

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

eStreamer アプリケーション プロトコルについて

Cisco Secure Firewall 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 サーバーまたは 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 サーバーに送信し、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（2-9 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 サーバーとの接続を確立し、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 サーバー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 サーバー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（2-7 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（2-8 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、事前に 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 サーバーが応答し、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 サーバー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 サーバーで内部認証局（内部 CA）によって署名されている）ことを確認します。

（注）　Cisco は、クライアントが eStreamer サーバー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、Cisco 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 サーバー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 サーバーは接続を閉じます。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、Cisco 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
title	eStreamer
generationQualifier	server

接続後の検証が終了すると、eStreamer サーバー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（2-7 ページ）を参照してください。
- 要求の変更: 要求の変更（2-7 ページ）を参照してください。
- 完全修飾イベントのリクエスト：次を参照してください。完全修飾イベントのリクエスト（2-5 ページ）

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（2-13 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 (2-13 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 (2-7 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 (2-13 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 (2-15 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、サーバー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 2-22 (2-43 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 (2-13 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 (2-37 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（2-45 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（2-7 ページ）を参照してください。

完全修飾イベントのリクエスト

複雑なバイナリ形式でイベントを受信する代わりに、クライアントがこのオプションを使用して、JSON や CSV などのテキスト形式で完全修飾イベントをリクエストすることを推奨します。このオプションを使用する場合、バイナリ形式について説明しているこのドキュメントの大部分は無関係です。SDK パッケージの python_client サブディレクトリには、このオプションを使用するためのサンプルコードが含まれています。

このオプションは現在、接続イベント、侵入イベント、侵入パケット、ファイルイベントなど、いくつかのイベントタイプに関する情報の要求のみをサポートしています。他のイベントタイプをバイナリ形式で受信する必要がある場合は、完全修飾およびバイナリイベント形式に個別のクライアント接続を使用する必要があります。

完全修飾イベントを要求するには、文書化されている「イベントストリーム要求メッセージ」を使用し、メッセージの最後に JSON 形式の構成ブロックを追加します。リクエストには、以下に示す通常の 5 つのバイナリ整数が含まれ、その後に次のような JSON 形式の構成の詳細が続きます。

```
<Header Version (1)>
<Message Type (2)>
<Message Length>
<Initial Timestamp>
<Request Flags>
<JSON-format Configuration Block>
```

バイナリメッセージ長フィールドには、バイナリヘッダーの長さと JSON ブロックの長さが含まれている必要があります。JSON ブロックの後の終了 Null 文字はオプションですが、Null が含まれる場合、メッセージ長には Null 文字を含める必要があります。要求フラグフィールドでは、ビット 23（拡張イベントヘッダー）のみがサポートされます。他のビットはすべてゼロ、特に、ビット 30（拡張要求）はゼロである必要があります。

クライアントが要求メッセージを送信すると、要求されたイベントタイプがサーバー側 [UI eStreamer 設定（UI eStreamer Configuration）] ページで有効になっている場合、eStreamer サービスはすぐにイベントデータの送信を開始します。

JSON ファイルの形式

この例は、eStreamer SDK の `json_request.json` ファイルにも含まれています。

```
{
"Events":
{
"ConnectionEvent":
```

```
{
"FieldSetDef":
{
"OutputFieldSet": ["HeaderFieldSet", "ConnectionKeySet", "DetailFieldSet"]
},
"Fields": ["OutputFieldSet"]
},
"IntrusionEvent":
{
"FieldSetDef":
{
"OutputFieldSet": ["HeaderFieldSet", "ConnectionKeySet", "DetailFieldSet", "Impact"]
},
"Fields": ["OutputFieldSet"]
},
"IntrusionPacket":
{
"FieldSetDef":
{
"OutputFieldSet": ["HeaderFieldSet", "DetailFieldSet"]
},
"Fields": ["OutputFieldSet"]
},
"FileEvent":
{
"FieldSetDef":
{
"OutputFieldSet": ["HeaderFieldSet", "ConnectionKeySet", "DetailFieldSet"]
},
"Fields": ["OutputFieldSet"]
}
},
"OutputFormat":
{
"Transform": "Text",
"TransformConfig": "JSON"
}
}
```

Events セクションで、クライアントが受信するイベントタイプごとにブロックを指定します。4 つのサンプルタイプ（ConnectionEvent、IntrusionEvent、IntrusionPacket、および FileEvent）がサポートされています。各イベントの FieldSetDef セクションでは、そのイベントタイプのイベントに含まれるフィールドまたはフィールドセットをリストする OutputFieldSet を指定する必要があります。サンプルファイルではフィールドセットのみを指定していますが、フィールド名とフィールドセットの任意の組み合わせを使用できます。

各イベントタイプで使用可能なフィールドのリスト、および事前定義されたフィールドセットは、Firepower Management Center の /etc/sf/EventHandler/EventCatalog/EventCatalog.json ファイルにあります。ファイルの末尾にある Fields セクションで、目的のイベントタイプ（IntrusionEventなど）を探し、次に Fields ブロックと FieldSetDef ブロックを参照して、そのイベントタイプで使用可能な内容を確認します。

OutputFormat セクションには、出力の設定があります。Transform フィールドは常に Text であり、TransformConfig フィールドで出力変換形式を指定します。例に示されているのは JSON ですが、CSV も指定できます。FlatBuffer と同様に他のテキスト形式も使用できますが、使用する形式のドキュメントを要求する必要があります。

JSON 出力が TransformConfig で指定されている場合、出力には、要求された各フィールドの名前と値のペアが含まれますが、イベントに関係のないフィールドはスキップされます（たとえば、SSL フィールドを要求し、イベントで SSL が使用されなかった場合、出力には SSL フィールドは含まれません）。

TransformConfig で CSV 出力が指定されている場合、出力には、構成にリストされている順序で目的のフィールドが含まれています。フィールドがイベントに関連していない場合、CSV にはそのフィールドのコンマのみが含まれます。バージョン間でフィールドセットが変更され、CSV の互換性がなくなる可能性があるため、CSV を要求する際には事前定義されたフィールドセットを使用しないでください。

完全修飾イベントメッセージ

イベントメッセージは、「メッセージ バンドル フォーマット」、メッセージタイプ 4002 の eStreamer ドキュメントで説明されているようにバンドルに含まれています。

記載されているように、クライアントは、eStreamer サーバーに Null メッセージを送信して、受信した各データバンドルを確認し、追加のデータの受け入れが可能なことを示す必要があります。

サポートされているすべてのイベントタイプについて、イベントデータメッセージは、「相関レコードヘッダー」など、さまざまなイベントタイプの eStreamer ドキュメントで説明されているバイナリヘッダーで始まります。唯一の違いは、データブロックの形式が要求された形式（JSON、CSV など）である点です。クイックリファレンスとして、基本構造を次に示します。

```
<Header Version (1)>
<Message Type (3)>
<Message Length>
<Record Type (with optional Netmap ID when requested)>
<Record Length>
<Timestamp (when request bit 23 is specified)>
<Reserved (when request bit 23 is specified)>
<Data>
```

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 Cisco Secure Firewall 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 サーバーは、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（2-46 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（2-11 ページ）を参照してください。

接続の終了

eStreamer サーバーは、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（2-11 ページ）を参照してください。

eStreamer サーバーは、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 サーバー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 サーバー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(Message Header)(2-10 ページ)を参照してください。

表 2-2　　eStreamer メッセージ タイプ

メッセージ タイプ	名前	説明
[0]	ヌル メッセージ	eStreamer サーバー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(2-11 ページ)を参照してください。
1	エラー メッセージ	eStreamer サーバー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(2-11 ページ)を参照してください。
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(2-13 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(2-21 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(2-30 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(2-36 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(2-36 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）

メッセージ タイプ	名前	説明
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（2-45 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（2-37 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（2-46 ページ）を参照してください。

eStreamer メッセージ ヘッダー（Message Header）

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。

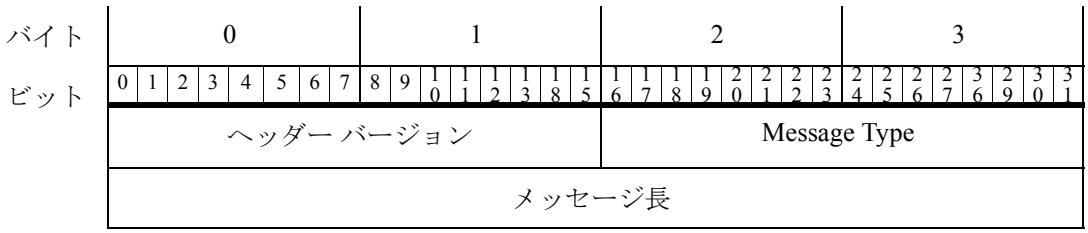


表 2-3　標準の eStreamer メッセージ ヘッダー フィールド

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（2-9 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。

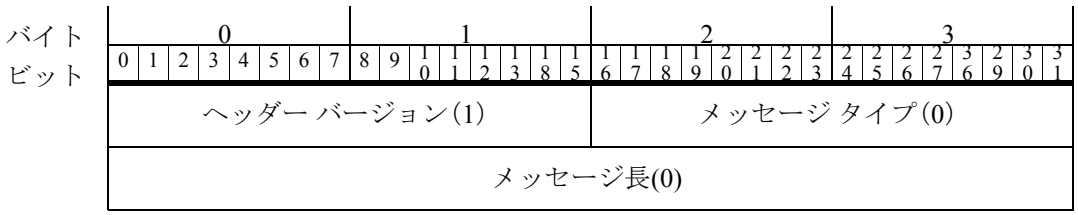
ヌル メッセージの形式

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。

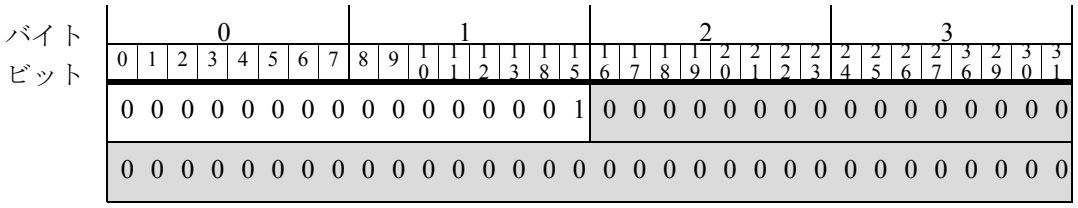
クライアントは、追加のデータを受け入れる準備ができていることを示すために、ヌル メッセージを eStreamer サーバーに送信します。eStreamer サービスは、データが送信されていないときに接続のアクティブ状態を維持するために、ヌル メッセージをクライアントに送信します。ヌル メッセージのメッセージ長の値は、常に 0 に設定されています。

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。



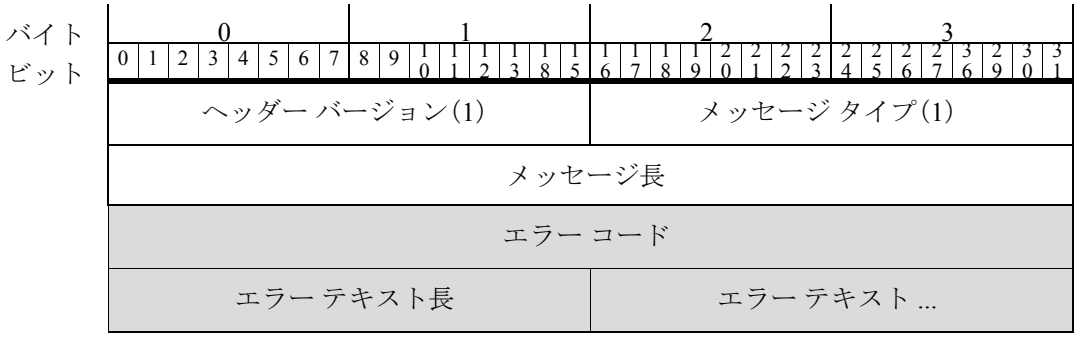
ヒント　このガイドの例は、どのビットが設定されているかを明確に示すためにバイナリ形式で表示されています。これは、イベント要求メッセージ フィールドやイベント影響フィールドなど、一部のメッセージにとって重要です。

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、Cisco 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。

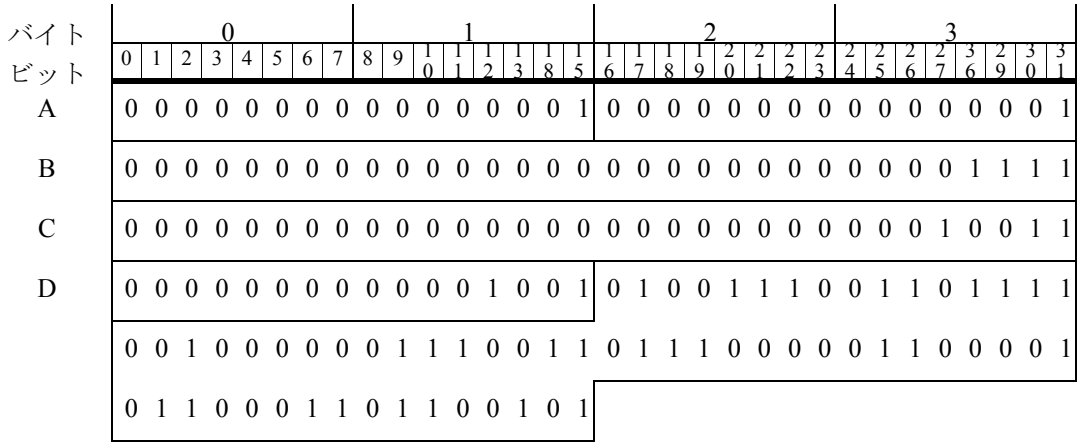


次の表では、エラー コード メッセージの各フィールドについて説明します。

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	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（variable）	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。



上記の例では、次の情報を確認できます。

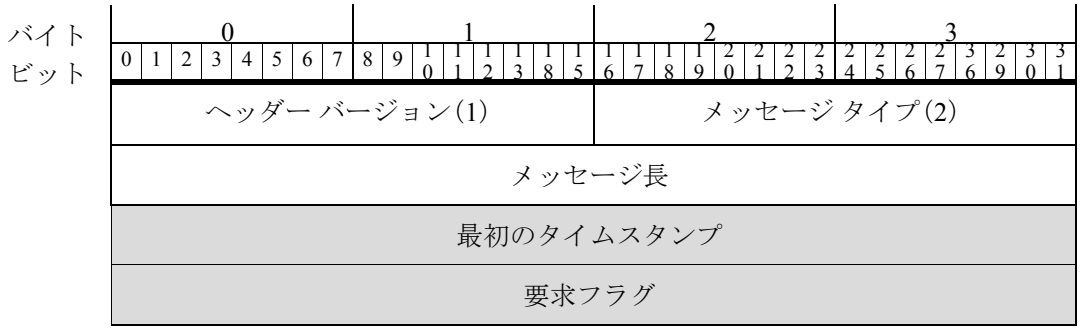
文字	説明
A	最初の 2 バイトは、標準ヘッダー値 1 を示します。2 番目の 2 バイトは値 1 を示し、送信がエラー メッセージであることを示します。
B	この行は、それに続くメッセージ データの量を示します。この例では、15 バイト（バイナリで 1111）のデータが続きます。
C	この行には、エラー コードが表示されます。この例では、メッセージに値 19（10011）が含まれています。したがって、エラー番号 19 がメッセージで送信されます。
D	この行には、エラー メッセージのバイト数（1001、または 9 バイト）が含まれ、エラー メッセージ自体が次の 9 バイトに続きます。エラー 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（2-14 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（2-15 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（「サーバー 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。前回のセッションで使用した最後のレコードのアーカイブ タイムスタンプを使用しても、eStreamer サービスによって以前のレコードまたはメタデータが再送されることはありません。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。

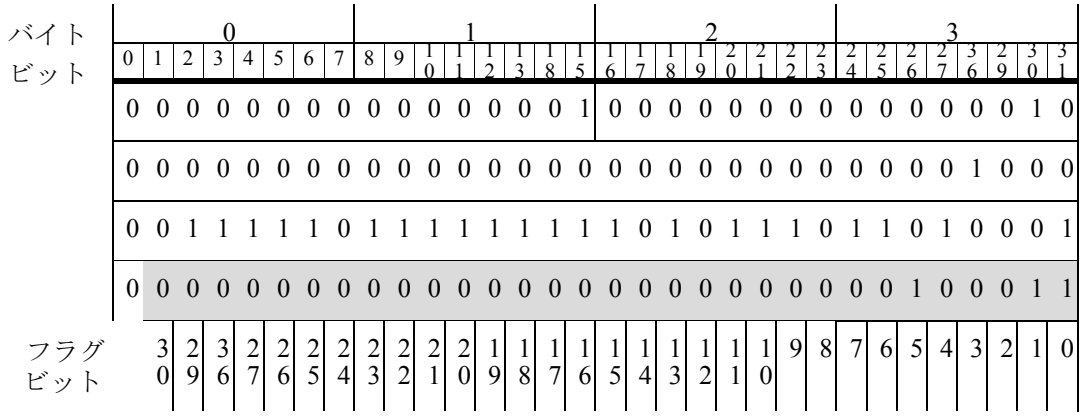
要求フラグ

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ー/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 (2-15 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 Cisco Secure Firewall 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 (2-19 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 (2-15 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 (2-47 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 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。
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（3-20 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（2-16 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-127 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。

表 2-6　　要求フラグ（続き）

ビット フィールド	説明
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（2-47 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（2-47 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（4-56 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-357 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、ユーザー 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 • ユーザー 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、ユーザー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（2-47 ページ）を参照してください。
ビット 21	バージョン 1 ユーザー イベントの送信を要求します。ユーザー イベントの詳細については、ユーザー 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、ユーザー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-357 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 サーバー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（Message Header）（2-10 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（4-56 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 B-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（B-70 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、ユーザー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

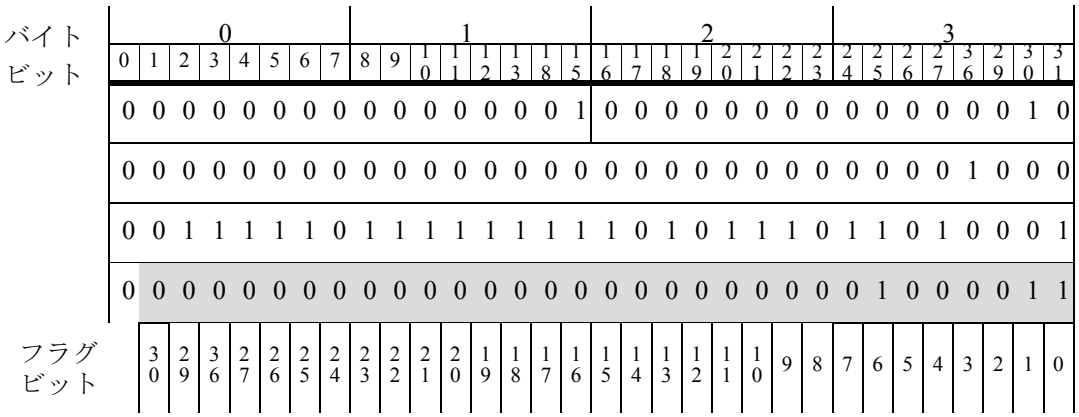
要求されたデータのタイプ	4.9.0.x	4.9.1.x	4.10.x	5.0+	5.1	5.1.1+
パケット データ	ビット 0	ビット 0	ビット 0	ビット 0	ビット 0	ビット 0
侵入イベント	ビット 2	ビット 2	ビット 2	ビット 2	ビット 2	ビット 30
メタデータ	ビット 20	ビット 20	ビット 20	ビット 20	ビット 20	ビット 20
検出イベント	ビット 24	ビット 25	ビット 28	ビット 30	ビット 30	ビット 30
相関イベント	ビット 22	ビット 22	ビット 29	ビット 30	ビット 30	ビット 30
イベント追加データ	—	—	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
ユーザー 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）

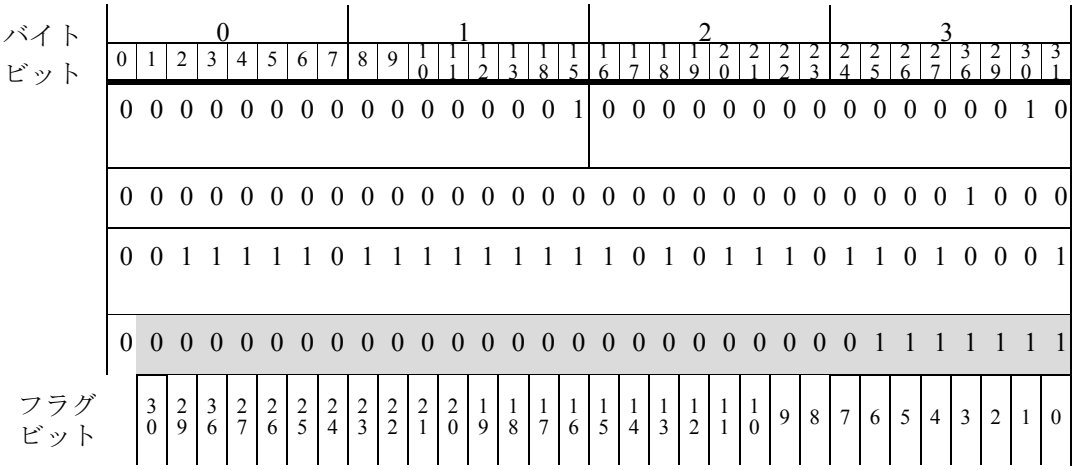
要求されたデータのタイプ	4.9.0.x	4.9.1.x	4.10.x	5.0+	5.1	5.1.1+
マルウェア イベント	—	—	—	—	—	ビット 30
ファイル イベント	—	—	—	—	—	ビット 30

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。

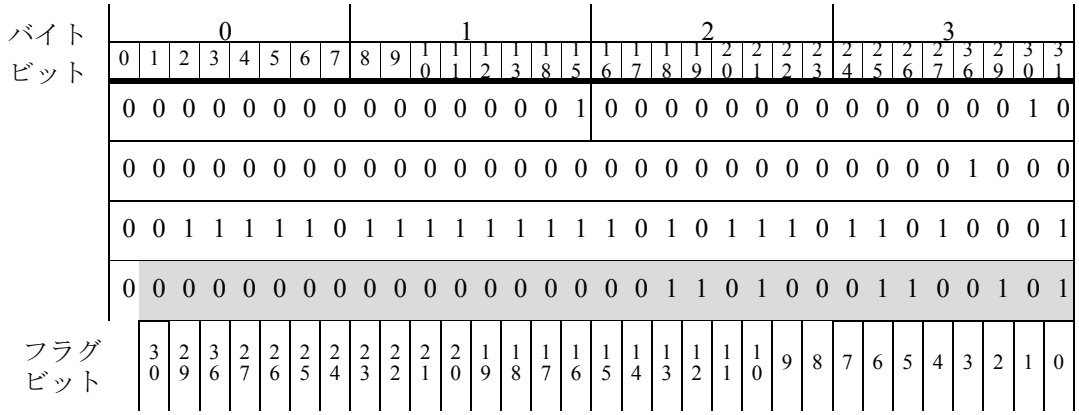
次の例では、バージョン 1 のメタデータとパケット フラグの両方を使用して、タイプ 7（Cisco Secure Firewall システム 3.2+ と互換性あり）の侵入イベントを要求しています。



Cisco Secure Firewall 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）の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（2-36 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（Message Header）（2-10 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。

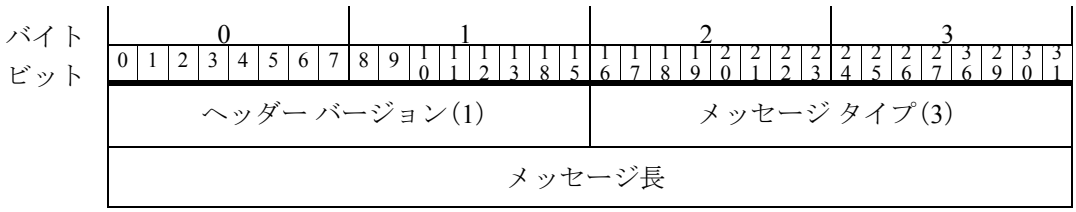
- 侵入イベント データ レコードとすべてのメタデータ レコードについては 侵入イベントとメタデータ メッセージの形式（2-22 ページ）。これらのメッセージは固定長フィールドを持ちます。

- 検出イベントまたはユーザー 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(2-24 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(2-26 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(2-26 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(2-28 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(2-28 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(2-29 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。



Netmap ID	レコード タイプ 表 3-1（3-1 ページ）を参照してください
レコード長	
eStreamer サーバー タイムスタンプ（eStreamer Server Timestamp） （イベントのみ、メタデータ レコードでは使用されません）	
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 ...	

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

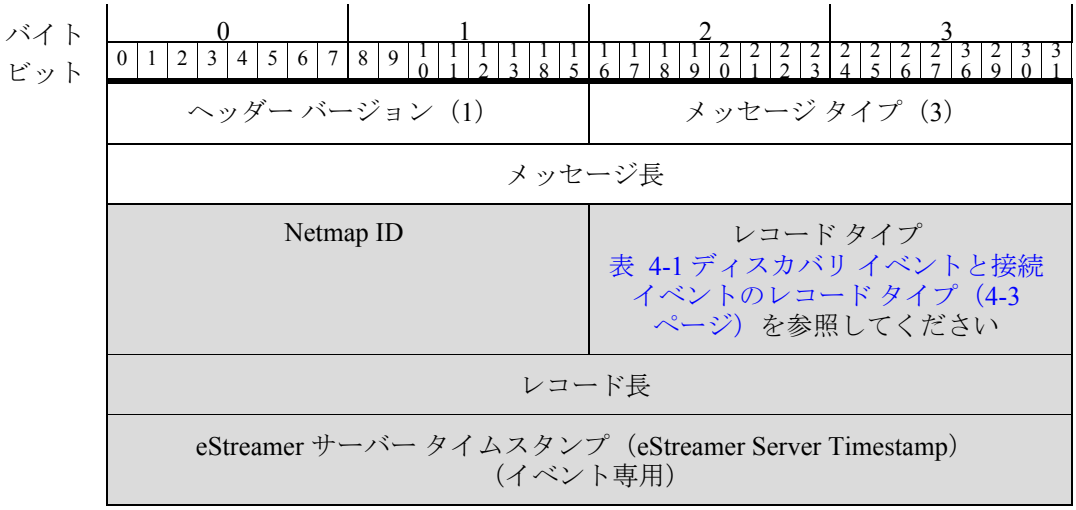
フィールド	データタイプ	説明
Netmap ID	uint16	このフィールドの第 1 ビットは、ヘッダーがアーカイブ タイムスタンプを含む拡張ヘッダーであるかどうかを示すフラグです。残りの 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプションのフィールドです。このフィールドは、使用されていない場合は空のままです。Netmap ID は、メタデータで提供されるドメインにマップされます。
レコード タイプ	uint16	データ レコードのコンテンツ タイプを識別します。レコード タイプのリストについては、表 3-1 侵入イベントと一般的なメタデータのレコード タイプ（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 サーバー タイムスタンプ（eStreamer Server Timestamp）	uint32	イベントが eStreamer サーバー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ー 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 (4-44 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（4-43 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（4-65 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 サーバー タイムスタンプ（eStreamer Server Timestamp）	uint32	イベントが eStreamer サーバー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+（4-42 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

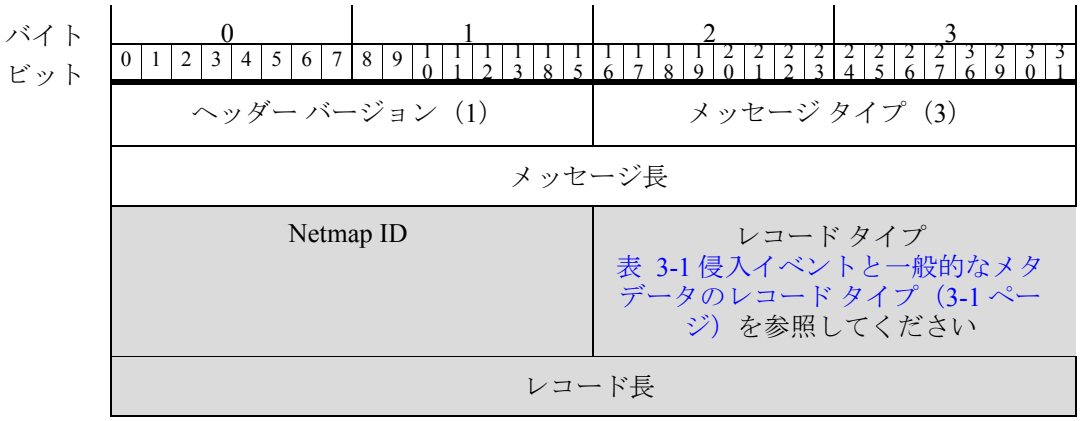
接続統計情報を含むメッセージの構造は、検出イベント メッセージと同じです。一般的なメッセージ形式の情報については、検出イベント メッセージの形式（2-24 ページ）を参照してください。接続イベント メッセージは、それらが組み込むデータ ブロック タイプの点で区別されます。

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。



eStreamer サーバー タイムスタンプ（eStreamer Server Timestamp） （イベントのみ、メタデータ レコードでは使用されません）
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（4-65 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 サーバー タイムスタンプ（eStreamer Server Timestamp）	uint32	イベントが eStreamer サーバー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。

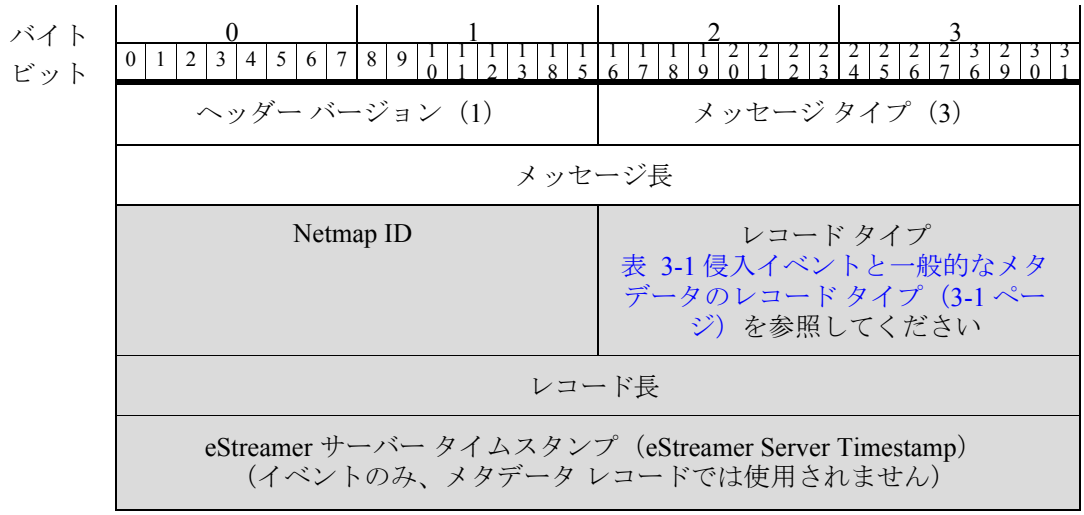
イベント追加データ メッセージの形式

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（3-58 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 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（3-58 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 サーバー タイムスタンプ（eStreamer Server Timestamp）	uint32	イベントが eStreamer サーバー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。

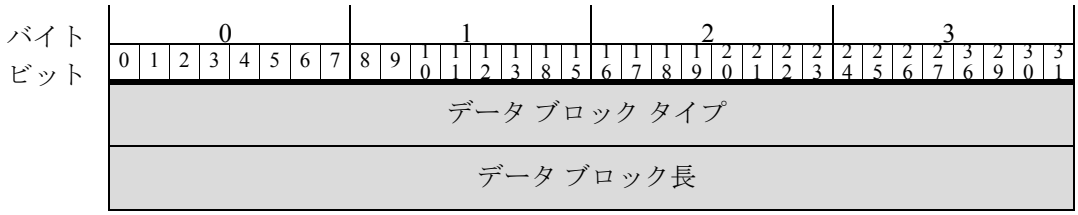


表 2-12

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（4-65 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 3-24 シリーズ 2 のブロック タイプ（3-58 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。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。

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ーに送信します。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。


バイト
ビット
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
ヘッダー バージョン（1）
メッセージ タイプ（5）
メッセージ長
データ タイプ
フラグ
開始 IP アドレス
開始 IP アドレス、続き
開始 IP アドレス、続き
開始 IP アドレス、続き
終了 IP アドレス
終了 IP アドレス、続き
終了 IP アドレス、続き
終了 IP アドレス、続き

次の表では、メッセージ フィールドについて説明します。

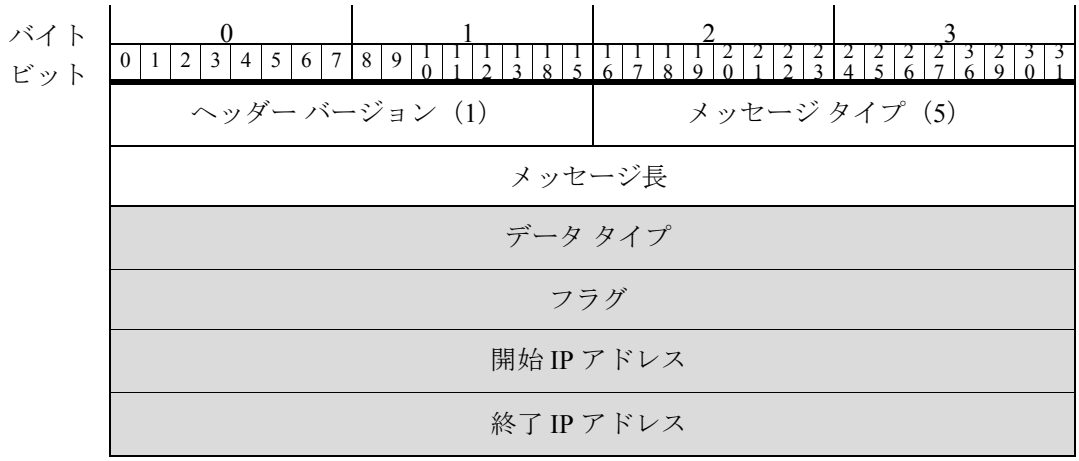
表 2-13　ホスト要求メッセージ フィールド

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.x データ（ブロック 111 を使用。フル ホスト プロファイル データ ブロック 5.0 ～ 5.0.2（B-374 ページ）を参照してください）。 • 7：複数ホストのバージョン 5.0.x データ（ブロック 111 を使用。フル ホスト プロファイル データ ブロック 5.0 ～ 5.0.2（B-374 ページ）を参照してください）。 • 8：複数ホストのバージョン 5.1.x データ（ブロック 111 を使用。フル ホスト プロファイル データ ブロック 5.1.1（B-384 ページ）を参照してください）。 • 9：複数ホストのバージョン 5.1.x データ（ブロック 111 を使用。フル ホスト プロファイル データ ブロック 5.1.1（B-384 ページ）を参照してください）。 • 10：ルール ドキュメンテーション データ（ブロック 27 を使用。ルール ドキュメンテーションのメッセージ形式（2-34 ページ）を参照してください）。 • 11：複数ホストのバージョン 5.2x データ（ブロック 111 を使用。フル ホスト プロファイル データ ブロック 5.2.x（B-395 ページ）を参照してください）。 • 12：複数ホストのバージョン 5.2.x データ（ブロック 111 を使用。フル ホスト プロファイル データ ブロック 5.2.x（B-395 ページ）を参照してください）。 • 13：複数ホストのバージョン 5.3+ 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）を参照してください）。 • 14：複数ホストのバージョン 5.3+ 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）を参照してください）。
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（Cisco Secure Firewall システム に格納されているホストに関するユーザー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 2-13　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[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（Cisco Secure Firewall システム に格納されているホストに関するユーザー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[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）。

ルール ドキュメンテーションのメッセージ形式

ルール ドキュメンテーション プロファイルを受信するには、ルール ドキュメンテーション メッセージを送信します。ジェネレータ ID、署名 ID、およびリビジョンでこれらを要求します。

ルール ドキュメンテーション情報の要求を含むすべてのデータ要求では、イベント ストリーム要求メッセージを送信することで、最初にセッションを初期化しておく必要があります。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、ルール ドキュメンテーション メッセージ（タイプ 10）を使用してルールを指定します。

以下のグラフィックに、ルール ドキュメンテーション メッセージの形式を示します。網掛けされたフィールドは、ルール ドキュメンテーションのメッセージ形式に固有です。これを次の表で定義します。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 2-15　ルール ドキュメンテーション メッセージ フィールド

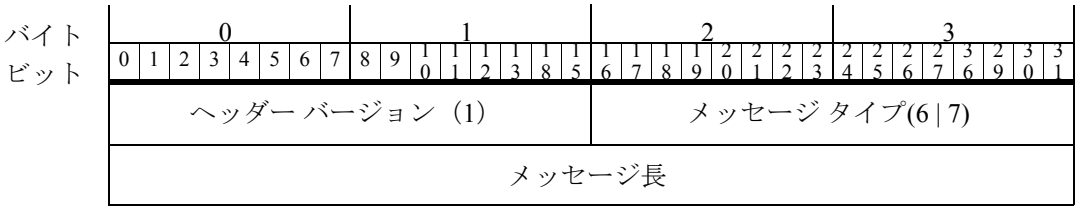
フィールド	データタイプ	説明
データ タイプ	uint32	ルール ドキュメンテーション データ ブロックのデータを要求します。この値は常に 10 です。5.2 以上のルール ドキュメントのデータ ブロック（3-112 ページ）を参照してください。
フラグ	32 ビット フィールド	• 0x00000001：ルール ドキュメンテーション データ ブロックの [注記（Notes）] フィールドに Cisco Secure Firewall システムに格納されているホストに関するユーザー定義の情報が読み込まれます。 • 0x00000002：サービス ブロックの [バナー（Banner）] フィールドが（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。
シグネチャ ID	uint32	要求したルールの ID 番号。
ジェネレータ ID	uint32	要求したルールの Cisco Secure Firewall 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。
予約済み	uint8[20]	このフィールドは現在使用されていません。

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。



完全なホスト プロファイル データ ブロック タイプ 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（4-66 ページ）を参照してください
長さ（Length）
完全なホスト プロファイル データ ブロック（Full Host Profile Data Block）

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。

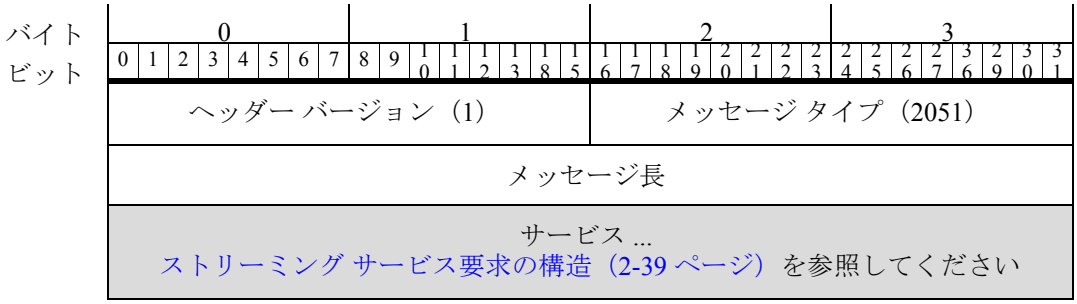
表 2-16

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（4-66 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（variable）	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（4-66 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、サーバー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（2-39 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。

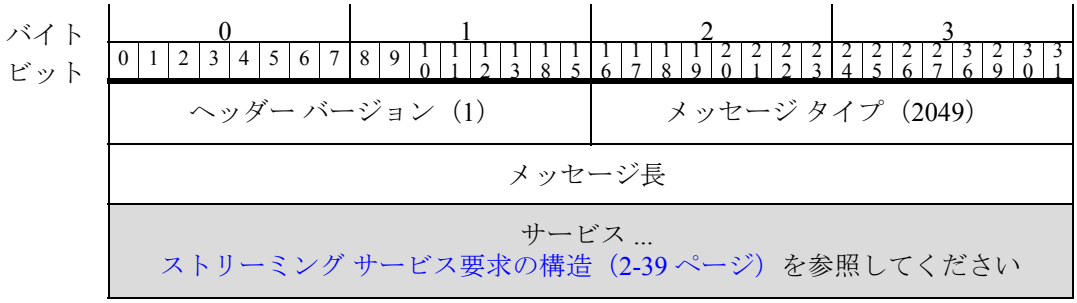
表 2-17　ストリーミング情報メッセージのフィールド

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。
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（2-39 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（2-39 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 2-18　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 2-18　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（2-39 ページ）を参照してください。

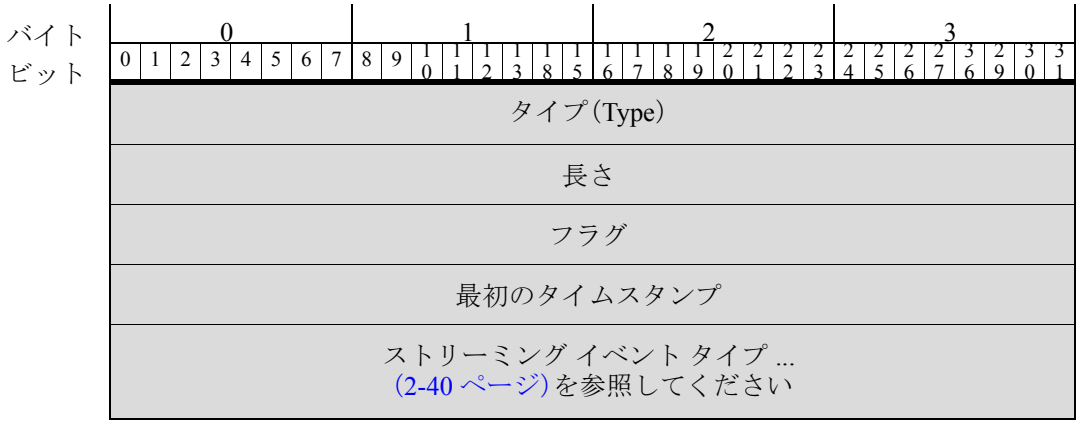
ストリーミング サービス要求の構造

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、サーバー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ー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、(2-40 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。



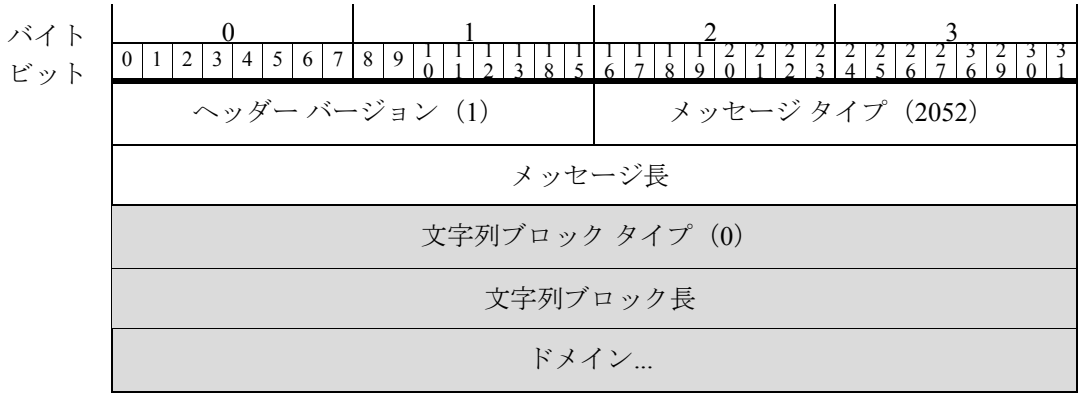
ストリーミング サービス要求構造のフィールドは次のとおりです。

表 2-19　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 サーバー 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。（2-40 ページ）を参照してください。 • [イベント タイプ] と [バージョン（Version）] 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。 （2-40 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 2-20　　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。

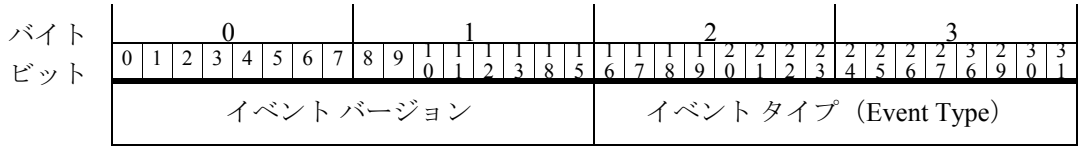
ストリーミング イベント タイプの構造

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。

```
Event Version = 0
Event Type = 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 2-21　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 2-22 拡張要求のイベント タイプとバージョン（2-43 ページ）を参照してください。
イベント タイプ（Event Type）	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 2-22 拡張要求のイベント タイプとバージョン（2-43 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 2-22　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.x 10：7.0 以降	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許可リストイベント	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 2-22　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.x 16：7.0.x 17：7.1 以降	71
ユーザー イベント	1：4.7 ～ 4.10.x 2：5.0.x 3：5.1 ～ 5.1.x 4：5.2 5：6.0 6：6.1 7：6.2+	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.x 8：7.0 以降	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.x 7：7.0 以降	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、サーバーは 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。サーバー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 2-23

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 2-24

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	28	/*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 2-24

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*/

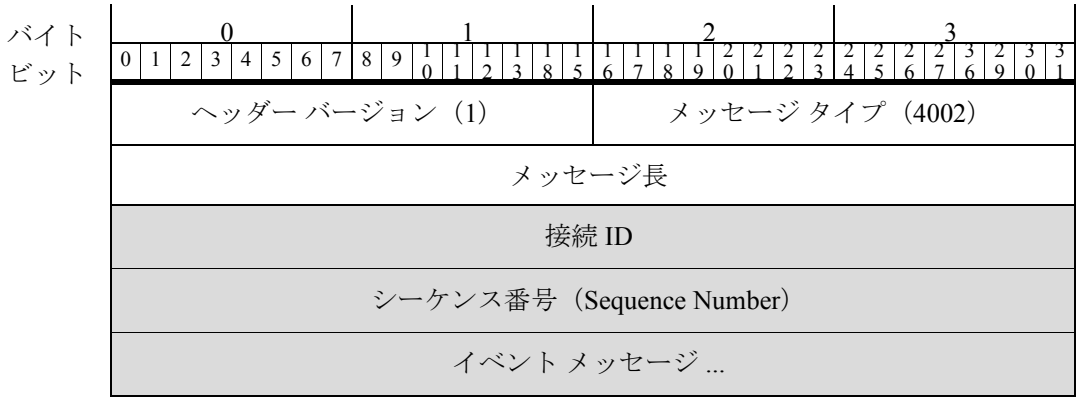
メッセージ バンドルの形式

クライアントが拡張要求を送信すると、eStreamer サーバー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 2-25　　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。

表 2-25　メッセージ バンドル 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。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	サーバー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 サーバー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ー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 サーバーは、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（2-15 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。

要求されたメタデータと環境によって、送信されるメタデータの量が大幅に異なる可能性があります。

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。キャッシュ サイズが制限されているクライアント アプリケーションでキャッシュがいっぱいになった場合は、クライアントがストリーミング中のイベントのメタデータ値をすべて受信できるようにキャッシュを消去して eStreamer サービスに再接続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。再接続すると、クライアントは要求メッセージで「最初のタイムスタンプ」を指定して、イベントの重複や不足を回避できるようになります。

CHAPTER 3

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（2-21 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（Legacy）	侵入影響アラート データ（B-66 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（3-22 ページ）
62	該当なし	2	ユーザ メタデータ	現在（Current）	ユーザー レコード（3-26 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（3-27 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（3-28 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（3-30 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（3-31 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（Legacy）	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（Legacy）	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）	レガシー（Legacy）	侵入イベント追加データ レコード（B-69 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）	レガシー（Legacy）	侵入イベント追加データのメタデータ（B-71 ページ）
112	128	1	5.1 ～ 5.3.x の相関イベント	レガシー（Legacy）	相関イベント 5.1 ～ 5.3.x（B-366 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	14	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（3-33 ページ）
116	14	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	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	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（3-37 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（4-25 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（4-26 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（4-27 ページ）
123	該当なし	該当なし	管理対象Deviceのメタデータ	現在（Current）	管理対象Device 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 ポリシー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（3-87 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（3-85 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（3-39 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）	レガシー（Legacy）	マルウェア イベント データ ブロック 5.1.1.x（B-77 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（Legacy）	マルウェア イベント データ ブロック 5.2.x（B-83 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（Legacy）	マルウェア イベントのデータ ブロック 5.3（B-90 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（Legacy）	マルウェア イベント データ ブロック 5.3.1（B-97 ページ）
125	47	2	マルウェア イベント（バージョン 5.4.x）	レガシー（Legacy）	マルウェア イベント データ ブロック 5.4.x（B-105 ページ）
125	62	2	マルウェア イベント（バージョン 6.x）	レガシー（Legacy）	マルウェア イベント データ ブロック 6.x（B-116 ページ）
125	80	2	マルウェア イベント（バージョン 7.0 以上）	現在（Current）	マルウェア イベントのデータ ブロック 7.0 以上（3-100 ページ）
127	14	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（3-40 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（3-42 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	エンドポイント向け AMP 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）	エンドポイント向け AMPディテクタ タイプのメタデータ（3-43 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...
131	該当なし	該当なし	エンドポイント向け AMP 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）	エンドポイント向け AMP ファイル タイプのメタデータ（3-44 ページ）
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（3-114 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（Legacy）	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（Legacy）	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（3-73 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（3-74 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（3-76 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（3-77 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（3-78 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（3-79 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（3-80 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（3-81 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（3-83 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（3-84 ページ）
400	34	2	侵入イベント レコード 5.2.x	レガシー（Legacy）	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（Legacy）	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（Legacy）	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（Legacy）	侵入イベント レコード 5.4.x（B-38 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）

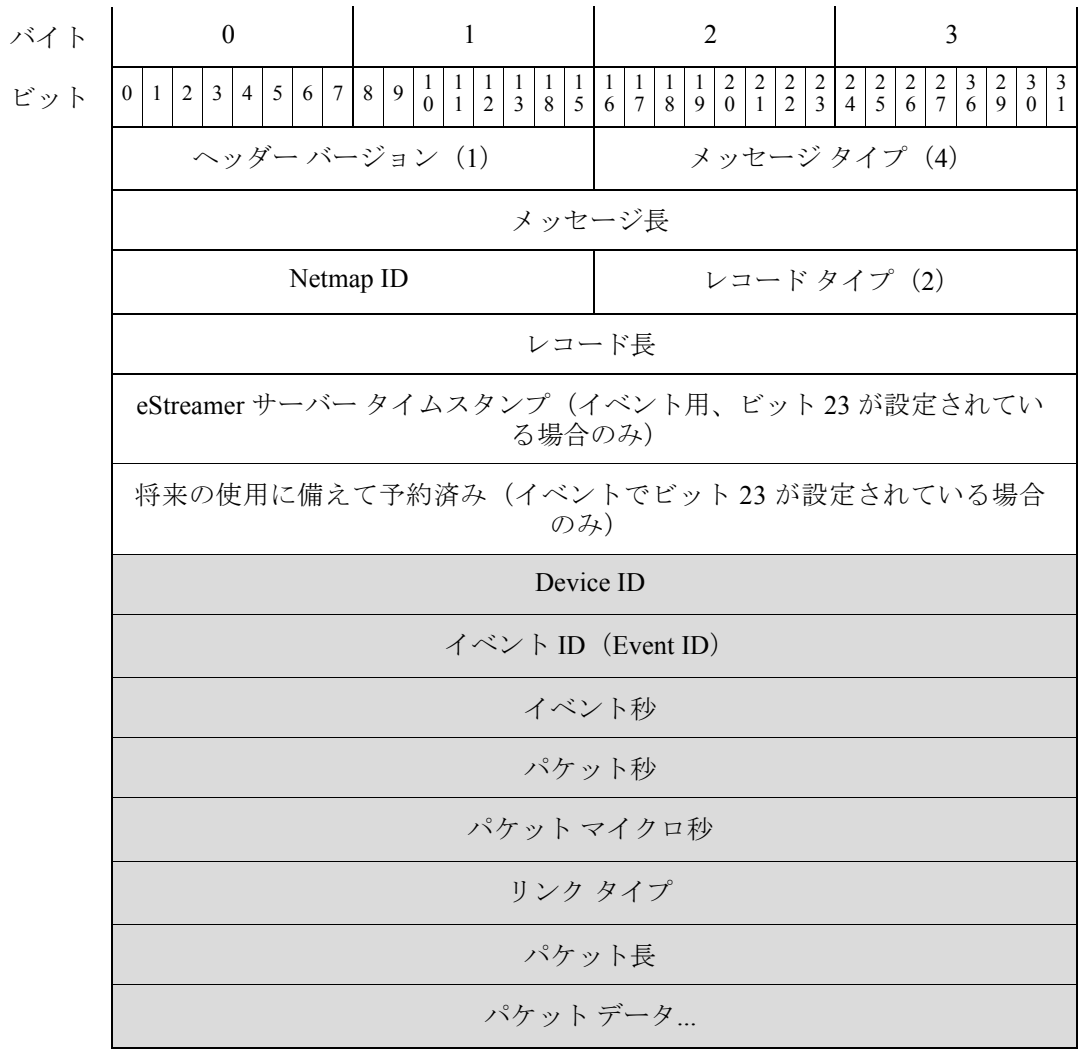
レコード タイプ	ブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
400	60	2	侵入イベント レコード 6.x	レガシー（Legacy）	侵入イベント レコード 6.x（B-47 ページ）
400	81	2	侵入イベント レコード 7.0	レガシー（Legacy）	侵入イベント レコード 7.0（B-56 ページ）
400	85	2	侵入イベント レコード 7.1 以上	現在（Current）	侵入イベント レコード 7.1 以上（3-9 ページ）
500	32	2	ファイル イベント（バージョン 5.2.x）	レガシー（Legacy）	ファイル イベント 5.2.x（B-317 ページ）
500	38	2	ファイル イベント（バージョン 5.3）	レガシー（Legacy）	ファイル イベント 5.3（B-321 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（Legacy）	ファイル イベント 5.3.1（B-328 ページ）
500	46	2	ファイル イベント（バージョン 5.4.x）	現在（Current）	7.0 以降のファイルイベント（3-89 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（Legacy）	ファイル イベント 5.2.x（B-317 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（Legacy）	ファイル イベント 5.3（B-321 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（Legacy）	ファイル イベント 5.3.1（B-328 ページ）
502	46	2	ファイル イベント（バージョン 5.4.x）	レガシー（Legacy）	ファイル イベント 5.4.x（B-334 ページ）
502	72	2	ファイル イベント（バージョン 6.x）	レガシー（Legacy）	6.x のファイルイベント（B-345 ページ）
502	79	2	ファイル イベント（バージョン 7.0 以上）	現在（Current）	7.0 以降のファイルイベント（3-89 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（3-113 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（Legacy）	ファイル イベント SHA ハッシュ 5.1.1 ～ 5.2.x（B-356 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（3-111 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（3-118 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（3-119 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（3-120 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（3-120 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...
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（3-121 ページ）
520	28	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（3-122 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（3-123 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（3-125 ページ）
601	51	2	SSL ルール ID	現在（Current）	SSL ルール ID（3-126 ページ）
602	該当なし	該当なし	SSL 暗号スイート	現在（Current）	5.4 以上の SSL 証明書の詳細のデータ ブロック（3-133 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（3-128 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 サーバー証明書ステータス（3-129 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（3-130 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（3-131 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（3-132 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（3-132 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（3-133 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（3-137 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（2-15 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（2）															
レコード長																																
eStreamer サーバー 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）																																
Device ID																																
イベント ID（Event 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

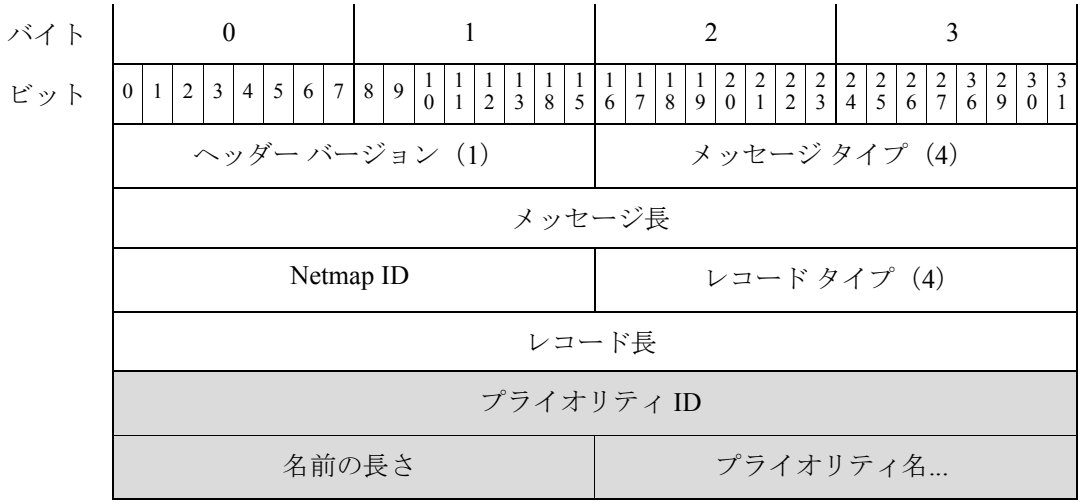
フィールド	データタイプ	説明
Device ID	uint32	デバイス ID 番号。バージョン 3 または 4 のメタデータの要求により関連付けられているデバイス名を取得できます。詳細については、管理対象Device レコードのメタデータ (3-38 ページ) を参照してください。
イベント ID（Event ID）	uint32	イベント ID 番号。
イベント秒	uint32	イベントが発生した秒（01/01/1970 以降）。
パケット秒	uint32	パケットがキャプチャされた秒（01/01/1970 以降）。
パケット マイクロ秒	uint32	パケットがキャプチャされたマイクロ秒（100 万分の 1 秒）の増分。

表 3-2　パケット レコード フィールド（続き）

フィールド	データタイプ	説明
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（variable）	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（2-15 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

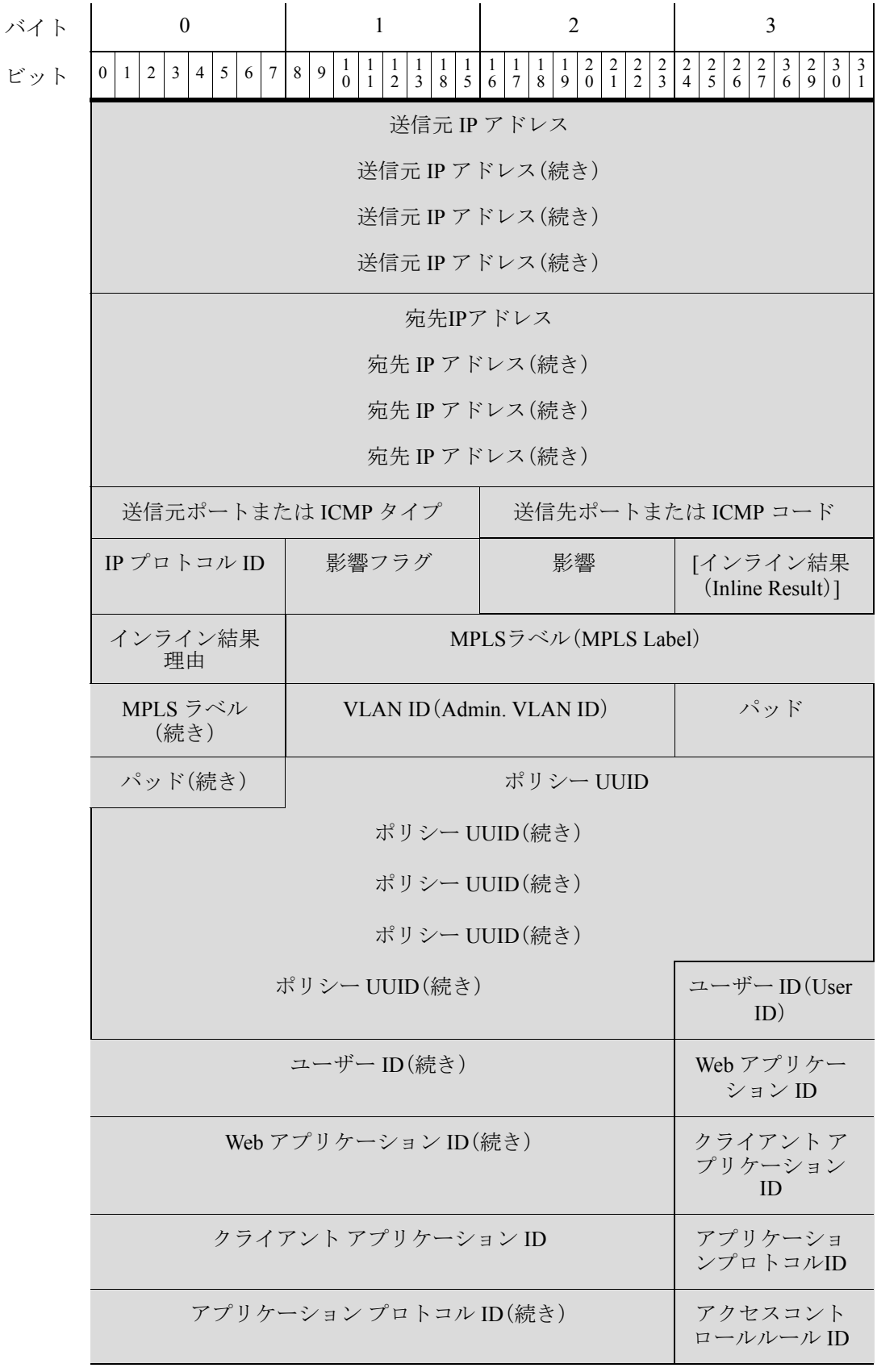
フィールド	データタイプ	説明
プライオリティ ID	uint32	プライオリティ ID 番号を表示します。
名前の長さ	uint16	プライオリティ名に含まれるバイト数。
プライオリティ名	変数（variable）	プライオリティ ID に対応するプライオリティ名（1 - 高、2 - 中、3 - 低）。

侵入イベント レコード 7.1 以上

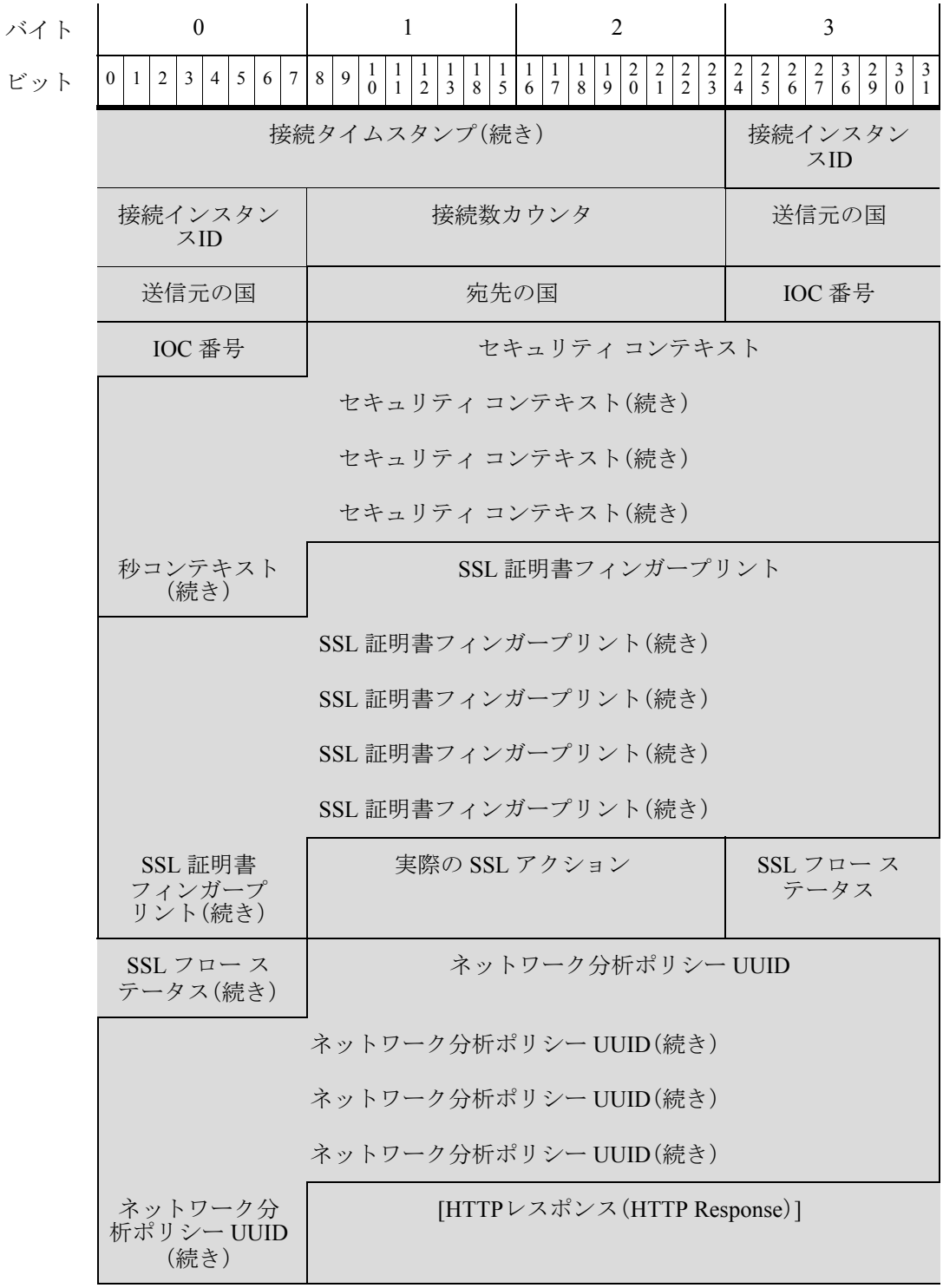
侵入イベント レコードのフィールドは、次の図で網掛けされています。レコードタイプは 400 であり、ブロックタイプはデータブロックのシリーズ 2 セットの 85 です。これはブロック タイプ 81 に取って代わります。エクストライベントデータに以前含まれていた XFF フィールドが追加されました。

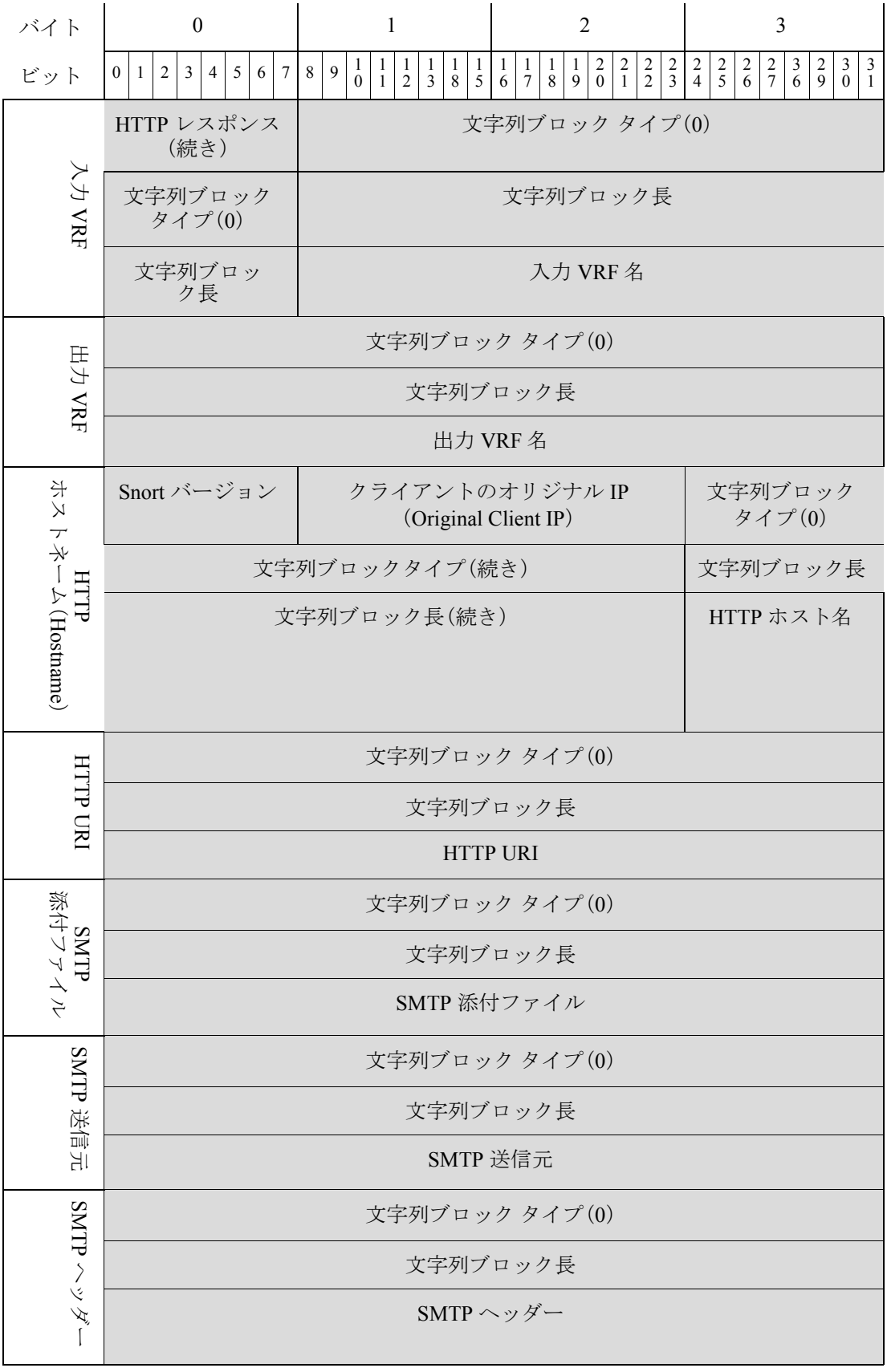
ストリーム要求メッセージでイベントタイプコード 12 とバージョンコード 11 を要求する拡張要求によってのみ、eStreamer から 7.1 以降の侵入イベントを要求できます（拡張要求の送信の詳細については、拡張要求の送信（2-4 ページ）を参照してください）。

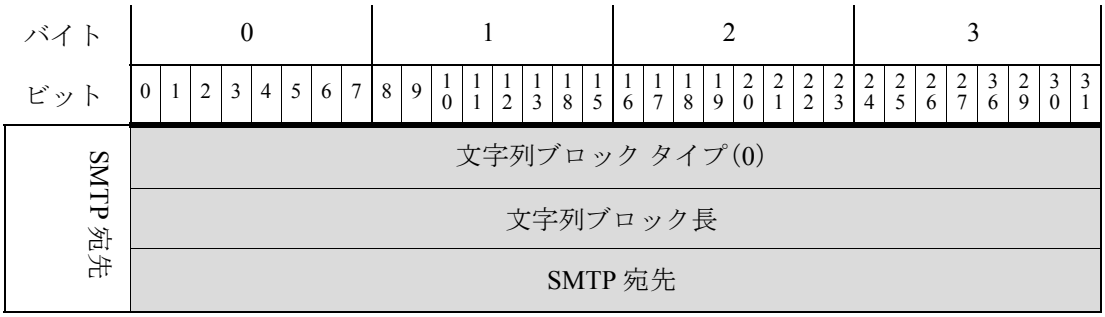
バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（400）															
レコード長																																
eStreamer サーバー 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（85）																																
ブロック長																																
デバイスID（Device ID）																																
イベント ID（Event 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 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
[インライン結果（Inline Result）]
インライン結果理由
MPLSラベル（MPLS Label）
MPLS ラベル（続き）
VLAN ID（Admin. VLAN ID）
パッド
パッド（続き）
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）
ポリシー UUID（続き）
ユーザー ID（User ID）
ユーザー 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）
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
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）
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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
アクセスコントロールルール 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)
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)
インターフェイス出力 UUID(続き)
秒ゾーン入力 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 ゾーン入力 UUID(続き)
秒ゾーン出力 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)
セキュリティ ゾーン出力 UUID(続き)
接続タイムスタンプ


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
接続タイムスタンプ(続き)
接続インスタンスID
接続インスタンスID
接続数カウンタ
送信元の国
送信元の国
宛先の国
IOC 番号
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)
秒コンテキスト(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
SSL フロー ステータス(続き)
ネットワーク分析ポリシー UUID
ネットワーク分析ポリシー UUID(続き)
ネットワーク分析ポリシー UUID(続き)
ネットワーク分析ポリシー UUID(続き)
ネットワーク分析ポリシー UUID(続き)
[HTTP レスポンス(HTTP Response)]


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 VRF
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)
文字列ブロック長
文字列ブロック長
入力 VRF 名
出力 VRF
文字列ブロック タイプ(0)
文字列ブロック長
出力 VRF 名
HTTP ホストネーム(Hostname)
Snort バージョン
クライアントのオリジナル IP（Original Client IP）
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)
HTTP ホスト名
HTTP URI
文字列ブロック タイプ(0)
文字列ブロック長
HTTP URI
SMTP 添付ファイル
文字列ブロック タイプ(0)
文字列ブロック長
SMTP 添付ファイル
SMTP 送信元
文字列ブロック タイプ(0)
文字列ブロック長
SMTP 送信元
SMTP ヘッダー
文字列ブロック タイプ(0)
文字列ブロック長
SMTP ヘッダー



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 7.1 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 85 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（Device 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Device 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（Event 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 Cisco Secure Firewall 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。

表 3-4　侵入イベント レコード 7.1 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 7.1 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	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ー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ーを実行しているか（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ー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）。Cisco Secure Firewall 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 7.1 以上のフィールド（続き）

フィールド	データタイプ	説明
[インライン結果（Inline Result）]	uint8	インライン結果を示す値。 • 0:合格 • 1:ドロップ • 2:ドロップされる可能性あり（設定では許可されていない） • 3:部分的にドロップ • 4:ブロック • 5:ブロック対象 • 6:部分的にブロック • 7:ドロップ • 8:ドロップ対象 • 9:拒否 • 10:拒否対象 • 11:応答 • 12:応答対象 • 13:書き換え • 14:書き換え対象
インライン結果理由	uint8	インライン結果の理由を示す値。 • 1:パッシブモードまたはタップモードのインターフェイス • 2:「検出」検査モードの侵入ポリシー • 3:「検出」検査モードのネットワーク分析ポリシー • 4:接続タイムアウト • 5:接続クローズ（内部使用） • 6:接続クローズ（内部使用） • 7:接続クローズ（内部使用）
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID（Admin. 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。
ユーザー ID（User ID）	uint32	ユーザーの内部 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）。

表 3-4　侵入イベント レコード 7.1 以上のフィールド（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 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。
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 サーバー証明書の SHA1 ハッシュ。

表 3-4　侵入イベント レコード 7.1 以上のフィールド（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 3-4　侵入イベント レコード 7.1 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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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。
HTTP レスポンス	uint32	HTTP 要求の応答コード。

表 3-4　侵入イベント レコード 7.1 以上のフィールド（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	入力 VRF 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。ブロックタイプとヘッダーフィールドの 8 バイト、および入力 VRF 名フィールドのバイト数が含まれています。
入力 VRF 名	string	トラフィックがネットワークに入るときに通過する仮想ルータ。
文字列ブロック タイプ	uint32	出力 VRF 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。ブロックタイプとヘッダーフィールドの 8 バイト、および出力 VRF 名フィールドのバイト数が含まれています。
出力 VRF 名	string	トラフィックがネットワークから出るときに通過する仮想ルータの名前。
Snort バージョン	uint8	Snort のバージョン番号。
元のイニシエータ IP	uint16	接続の元のイニシエータ IP アドレスが含まれています。
文字列ブロック タイプ	uint32	HTTP ホスト名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。ブロックタイプとヘッダーフィールドの 8 バイト、および HTTP ホスト名フィールドのバイト数が含まれています。
HTTP ホスト名（HTTP Hostname）	string	HTTP 接続で見つかったホスト名が含まれています。
文字列ブロック タイプ	uint32	HTTP 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	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの 8 バイト、および HTTP URI フィールドのバイト数が含まれています。
HTTP URI	string	HTTP 接続で見つかった Universal Resource Indicator が含まれています。
文字列ブロック タイプ	uint32	SMTP 添付ファイ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	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの 8 バイト、および SMTP 添付ファイルフィールドのバイト数が含まれています。

表 3-4　侵入イベント レコード 7.1 以上のフィールド（続き）

フィールド	データタイプ	説明
SMTP 添付ファイル	string	[MIMEコンテンツ傾向（MIME Content-Disposition）] ヘッダーから取得された MIME 添付ファイル名が含まれています。このフィールドに入力するには、SMTP プリプロセッサの [MIME添付ファイル名のログ（Log MIME Attachment Names）] オプションを有効にする必要があります。複数の添付ファイル名がサポートされます。
文字列ブロックタイプ	uint32	SMTP 送信元アドレス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。ブロックタイプとヘッダーフィールドの 8 バイト、および SMTP 送信元フィールドのバイト数が含まれています。
SMTP 送信元	string	SMTP MAIL FROM コマンドから取得された電子メール送信者のアドレスが含まれています。このフィールドに入力するには、SMTP プリプロセッサの [送信元アドレスのログ（Log From Address）] オプションを有効にする必要があります。複数の送信者アドレスがサポートされます。
文字列ブロックタイプ	uint32	SMTP ヘッダ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。ブロックタイプとヘッダーフィールドの 8 バイト、および SMTP ヘッダーフィールドのバイト数が含まれています。
SMTP ヘッダー	string	電子メールのヘッダーから取得したデータが含まれています。 電子メールのヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーのログ（Log Headers）] オプションを有効にする必要があります。
文字列ブロックタイプ	uint32	SMTP 宛先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	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの 8 バイト、および SMTP 宛先フィールドのバイト数が含まれています。
SMTP 宛先	string	SMTP RCPT TO コマンドから取得された電子メール受信者のアドレスが含まれています。このフィールドに入力するには、SMTP プリプロセッサの [宛先アドレスのログ（Log To Address）] オプションを有効にする必要があります。複数の受信者アドレスがサポートされます。

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（4-65 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（2-13 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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 タイプ（153）																																
侵入影響アラート ブロック長																																
イベント ID（Event ID）																																
Device ID																																
イベント秒																																
影響																																
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）																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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 153 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（Event ID）	uint32	イベント ID 番号を表示します。
Device 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）

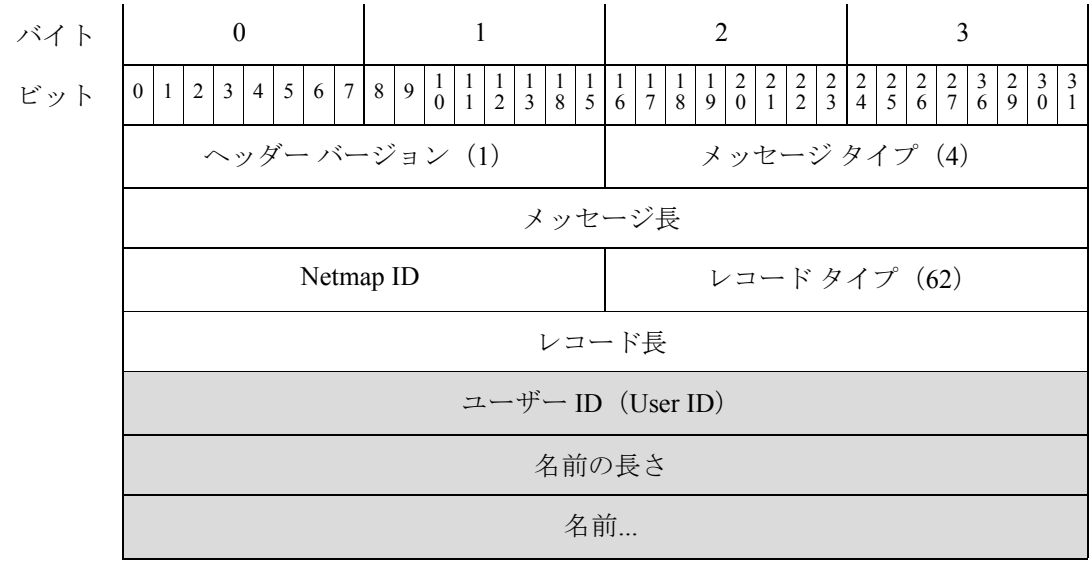
フィールド	データタイプ	説明
影響	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01（ビット 0）：送信元または宛先ホストはシステムによってモニターされるネットワーク内にあります。 • 0x02（ビット 1）：送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04（ビット 2）：送信元または宛先ホストはイベントのポート上のサーバーを実行しているか（TCP または UDP の場合）、IP プロトコルを使用します。 • 0x08（ビット 3）：イベントの送信元または宛先ホストのオペレーティング システムにマップ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ー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）。Cisco Secure Firewall 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（1-4 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（1-4 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 (4-75 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。

ユーザー レコード

メタデータを要求すると、Cisco Secure Firewall 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ーに関する情報を取得できます。eStreamer サービスは、ユーザー レコード内のイベントのユーザー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。ユーザー レコードには、ユーザー ID と対応する名前が含まれています。ユーザーのメタデータ レコードを使用すると、メタデータとユーザー ID 値を関連付けることによってイベントと関連付けられたユーザー名を特定できます（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、ユーザー情報が送信されます。要求フラグ (2-15 ページ) を参照してください）。



次の表は、ユーザー レコードのフィールドについての説明です。

表 3-6　ユーザー レコードのフィールド

フィールド	データタイプ	説明
ユーザー ID（User ID）	uint32	ユーザー ID 番号。このフィールドは、このレコードの固有キーです。

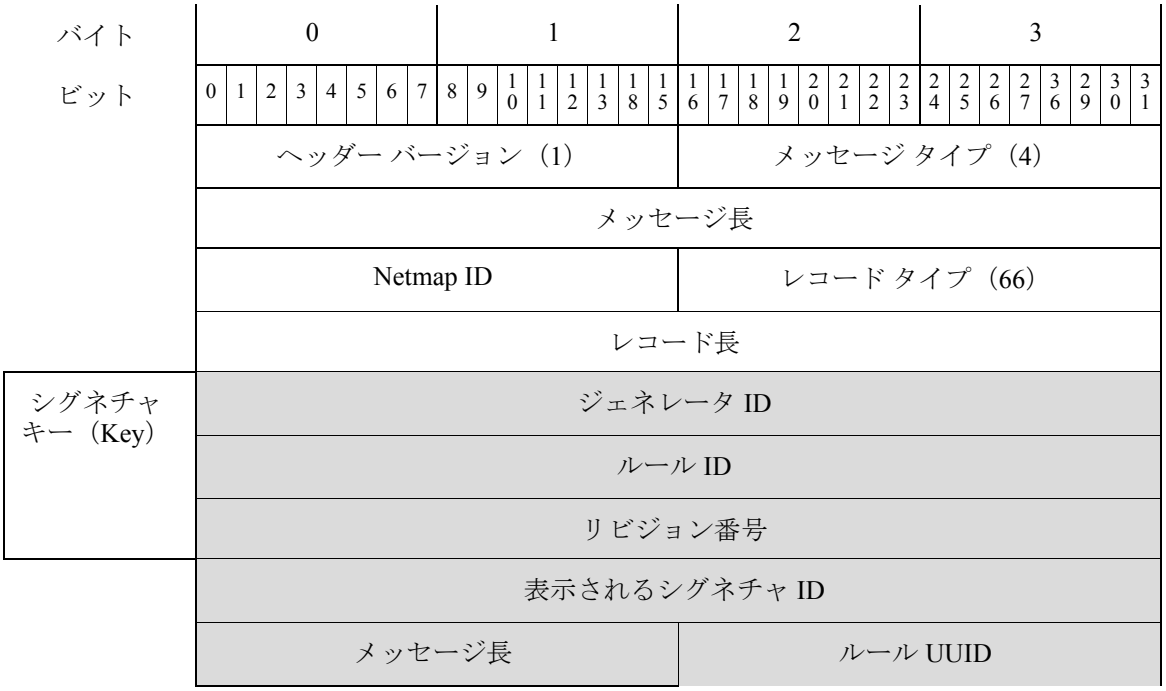
表 3-6　ユーザー レコードのフィールド（続き）

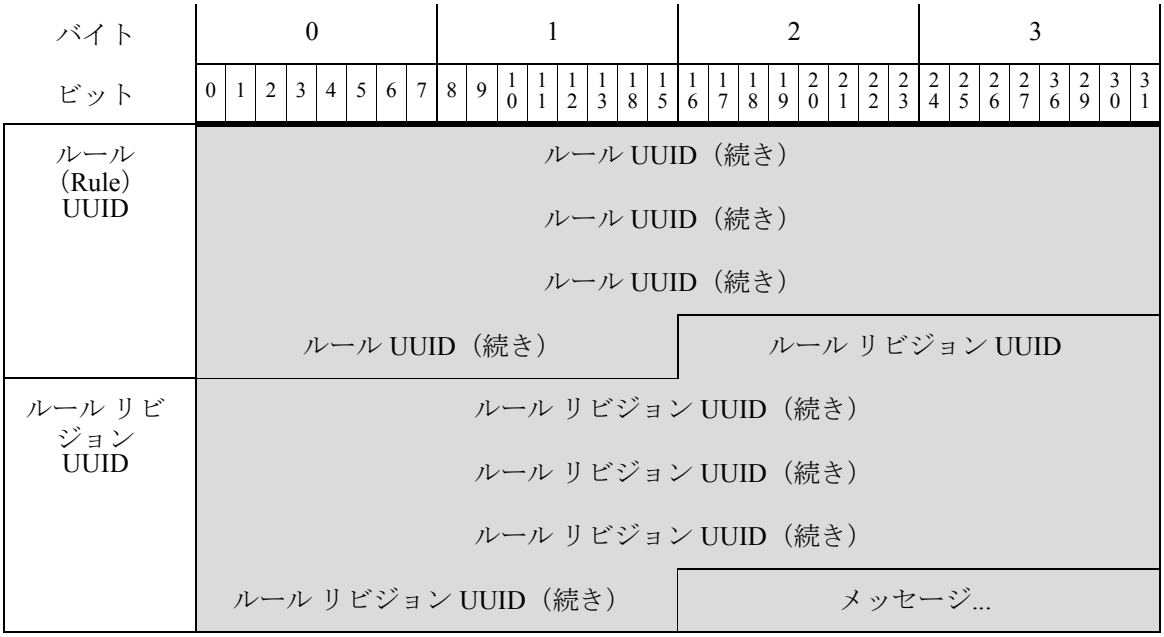
フィールド	データタイプ	説明
名前の長さ	uint32	ユーザー名に含まれるバイト数。
[名前（Name）]	string	ユーザーの名前。

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（2-15 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。

ファイアウォールの設定によって、何万にも及ぶルールが存在します。ルールごとに、個々のレコードのルール メッセージ レコードが生成される場合があります。メタデータのキャッシュやこのレコードの要求を実行する場合は、必ず十分なメモリを割り当てるようにしてください。





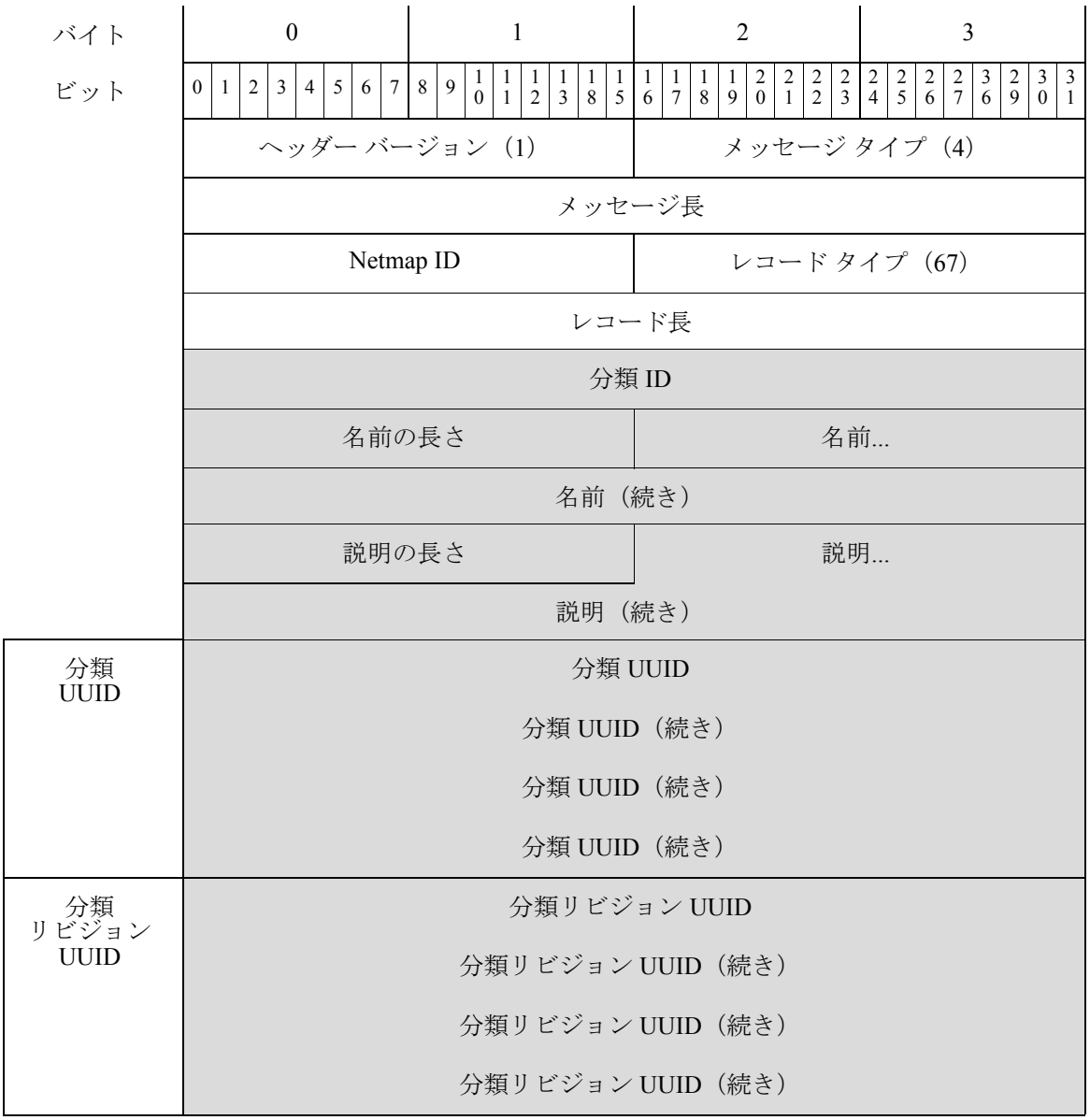
次の表は、各ルール固有のフィールドについての説明です。

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	Cisco Secure Firewall 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 (variable)	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 (2-15 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。



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(Name)]	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。

表 3-8　分類レコード フィールド（続き）

フィールド	データタイプ	説明
UUID	uint8[16]	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（2-15 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（69）															
	レコード長																															
	相関ポリシー ID																															
	名前の長さ																名前...															
	説明の長さ																説明...															
相関ポリシー UUID	相関ポリシー UUID 相関ポリシー UUID（続き） 相関ポリシー UUID（続き） 相関ポリシー UUID（続き）																															
相関ポリシー リビジョン UUID	相関ポリシー リビジョン UUID 相関ポリシー リビジョン UUID（続き） 相関ポリシー リビジョン UUID（続き） 相関ポリシー リビジョン UUID（続き）																															

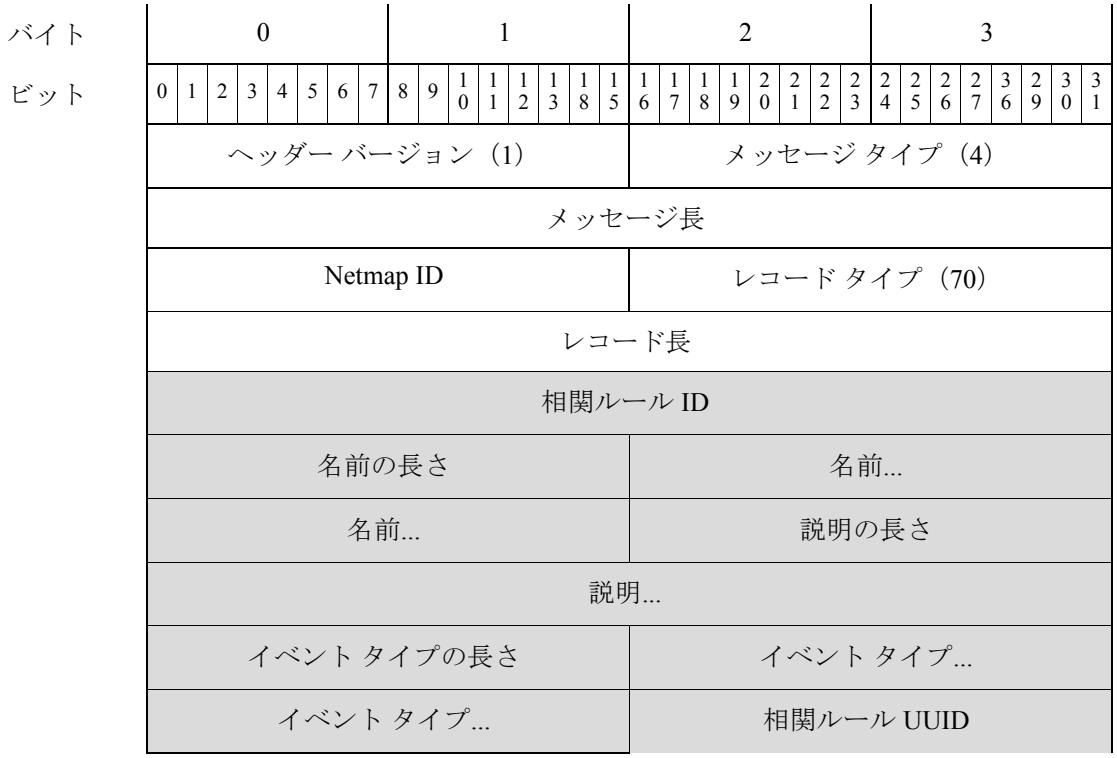
次の表は、相関ポリシー レコードのフィールドについての説明です。

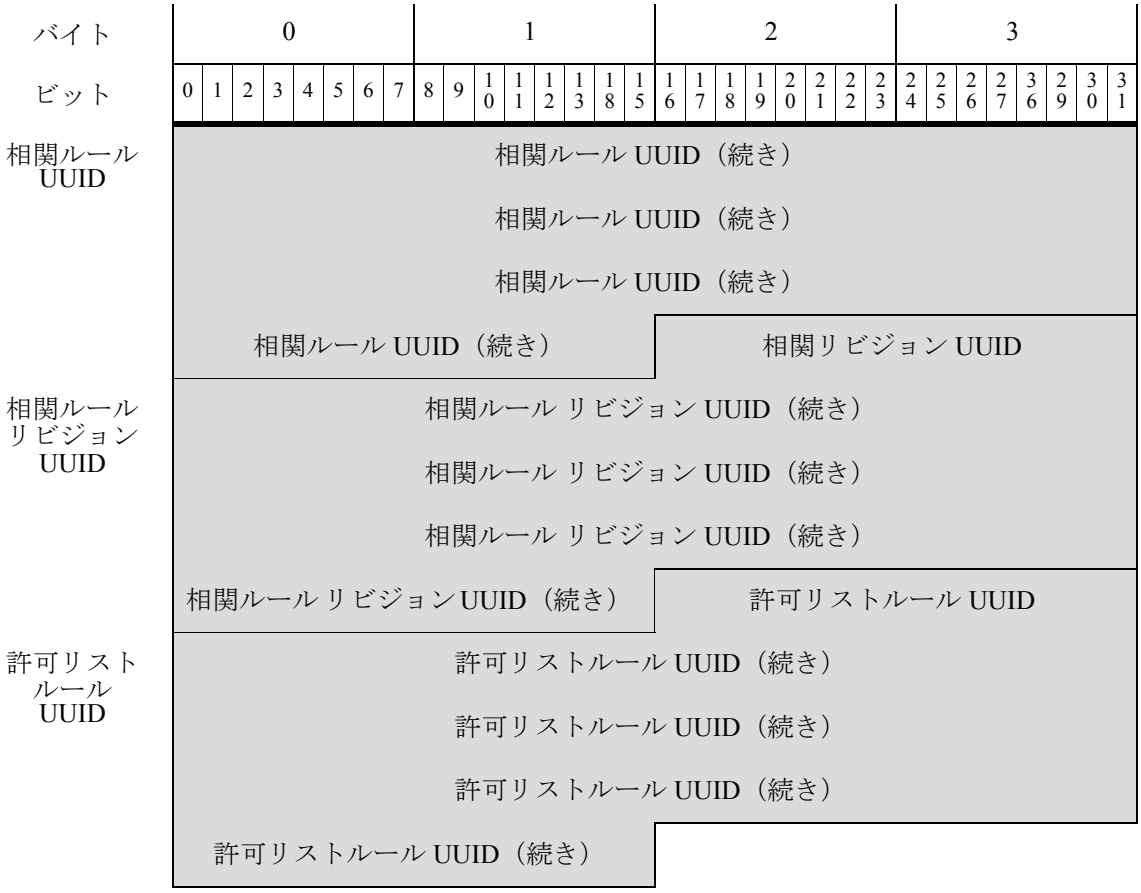
表 3-9　相関ポリシー レコード フィールド

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。このフィールドは、このレコードの固有キーです。
名前の長さ	uint16	相関ポリシー名に含まれるバイト数。
[名前（Name）]	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。
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（2-15 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。このフィールドは、このレコードの固有キーです。
名前の長さ	uint16	相関ルール名に含まれるバイト数。
[名前(Name)]	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（Event Type）	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。

表 3-10　相関ルール レコード フィールド（続き）

フィールド	データタイプ	説明
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。
許可リスト UUID	uint8[16]	許可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。

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 (2-15 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（115）															
レコード長																																
セキュリティ ゾーン名のデータ ブロック（14）																																
セキュリティ ゾーン名のデータ ブロック長																																
セキュリティ ゾーン UUID																																
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 ゾーン名...																																

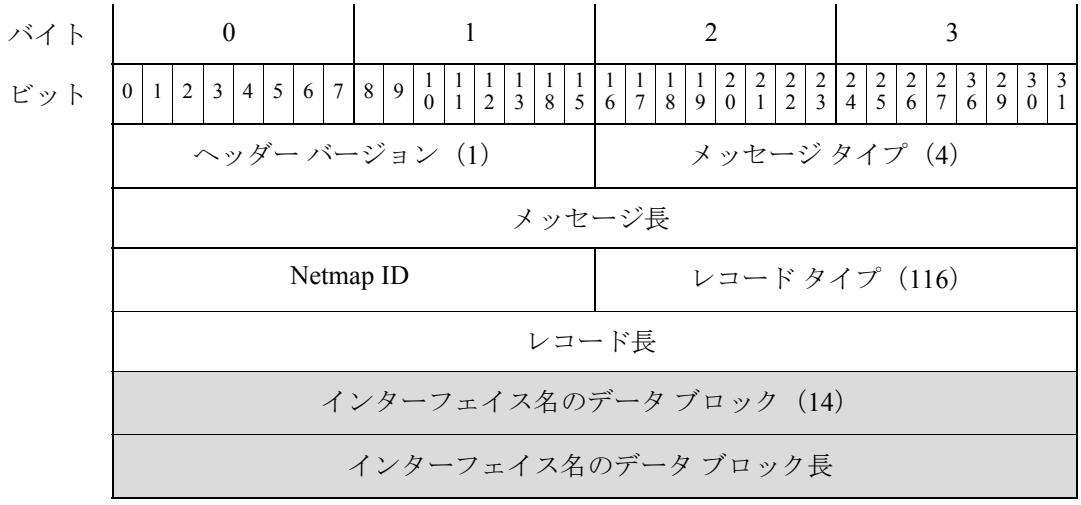
次の表は、セキュリティ ゾーン名のデータ ブロックのフィールドについての説明です。

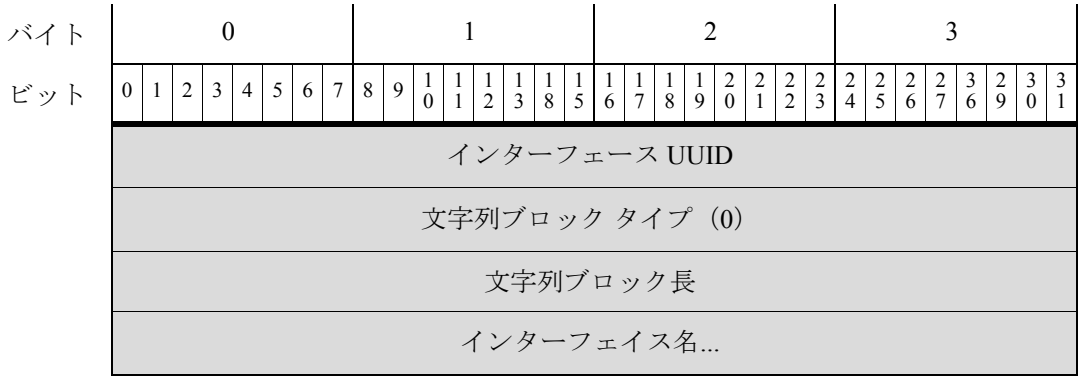
表 3-11　セキュリティ ゾーンの名のデータ ブロック フィールド

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。このフィールドは、このレコードの固有キーです。
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(2-15 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。





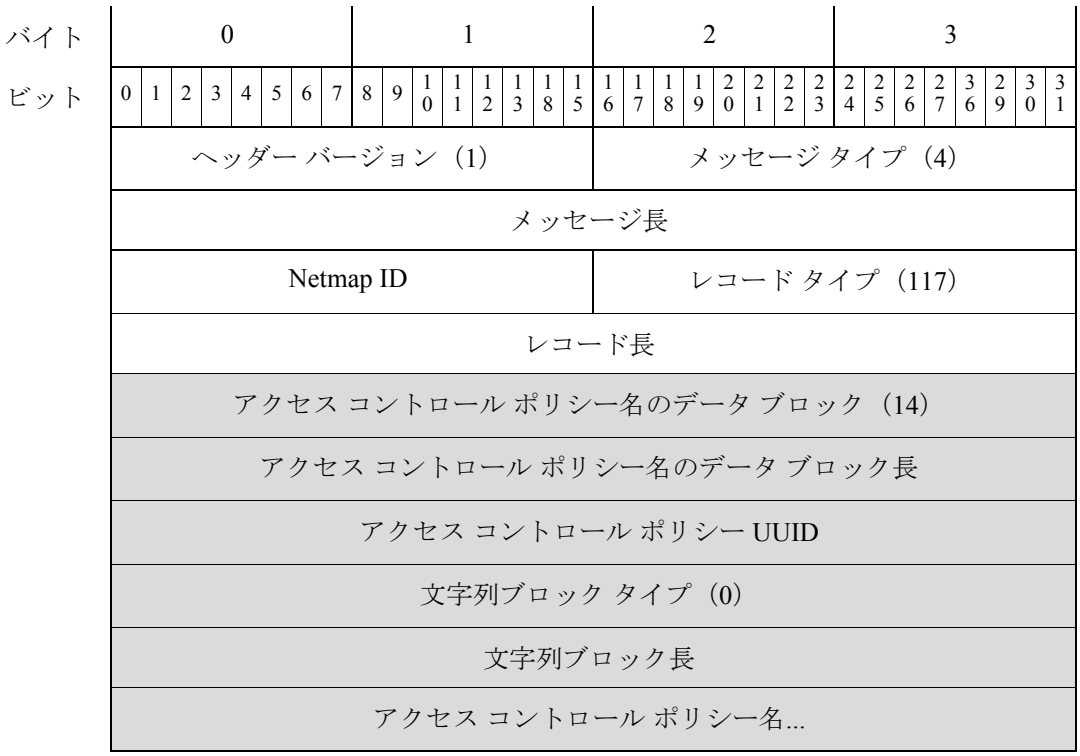
次の表は、インターフェイス名のデータ ブロックのフィールドについての説明です。

表 3-12　　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。
インターフェース 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。このフィールドは、このレコードの固有キーです。
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(2-15 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 3-13　　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 番号このフィールドは、このレコードの固有キーです。
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(2-15 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（119）															
	レコード長																															
	アクセス コントロール ルール ID のデータ ブロック（15）																															
	アクセス コントロール ルール ID のデータ ブロック長																															
AC ルール UUID	アクセス ルール ポリシー UUID アクセス コントロール ルール UUID（続き） アクセス コントロール ルール UUID（続き） アクセス コントロール ルール UUID（続き）																															
	アクセス コントロール ルール ID																															
	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	アクセス コントロール ルール名...																															

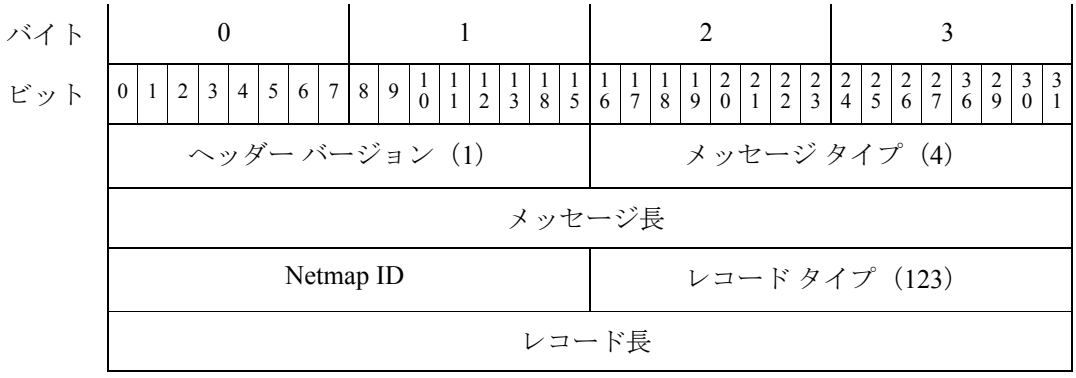
次の表では、アクセス コントロール ルール ID データ ブロックのフィールドについて説明します。

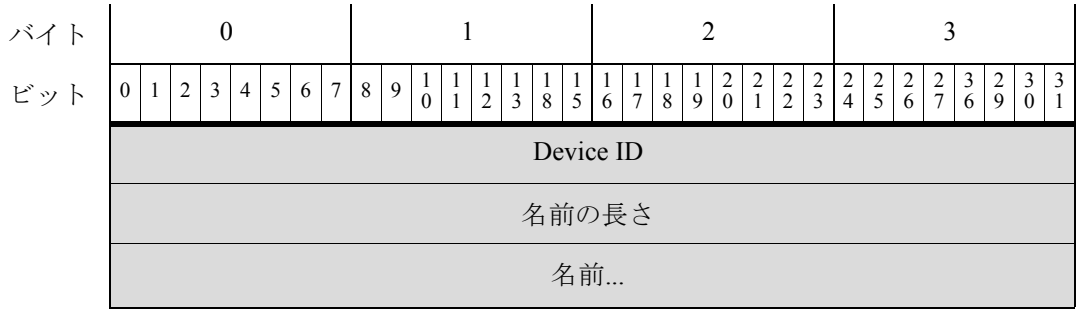
表 3-14　　アクセス コントロール ルール ID のデータ ブロック フィールド

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]	アクセス コントロール ルールの UUID。このフィールドとアクセス コントロール ルール ID を合わせると、このレコードの固有キーになります。
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。このフィールドとアクセス コントロール ルール UUID を合わせると、このレコードの固有キーになります。
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Device レコードのメタデータ

eStreamer サービスは、管理対象 Device 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 (2-15 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 Device 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 Device レコードのフィールドについての説明です。

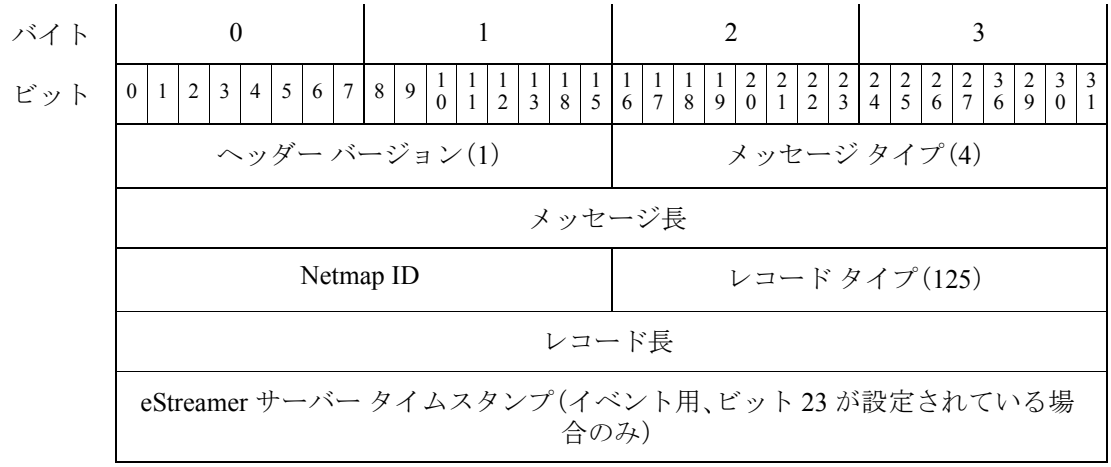
表 3-15　管理対象 Device レコード フィールド

フィールド	データタイプ	説明
Device ID	uint32	管理対象デバイス ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	名前に含まれるバイト数。
[名前（Name）]	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（2-15 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。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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）																																
マルウェア イベントのデータ ブロック																																

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。

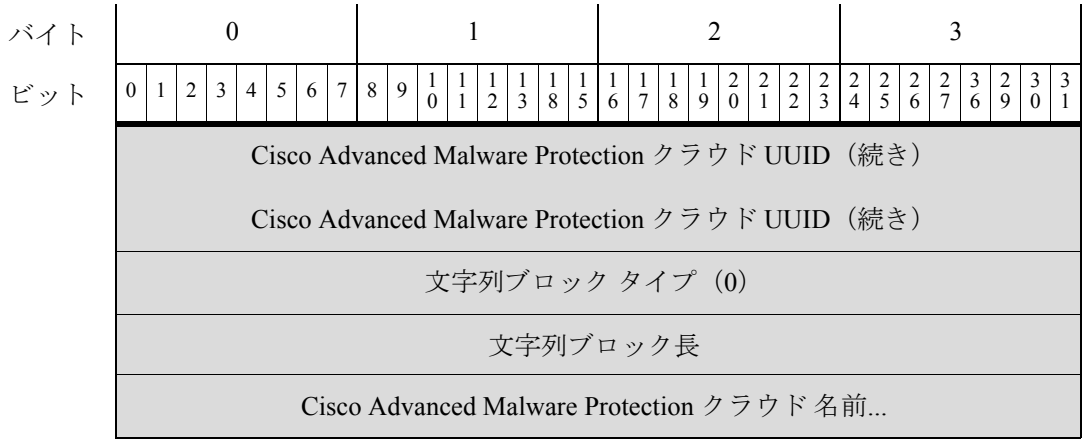
表 3-16　　マルウェア イベント レコード フィールド

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（variable）	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 7.0 以上（3-100 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 クラウド の名前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（AMP クラウドまたは単にクラウドと呼ばれる）Cisco Advanced Malware Protection クラウドの名前に関する情報を含むメタデータを送信します。この形式を以下に示します。（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 クラウド名の情報が送信されます。要求フラグ（2-15 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 クラウド 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（127）															
レコード長																																
Cisco Advanced Malware Protection クラウド 名のデータ ブロック（14）																																
Cisco Advanced Malware Protection クラウド名のデータ ブロック長																																
Cisco Advanced Malware Protection クラウド UUID Cisco Advanced Malware Protection クラウド UUID（続き）																																



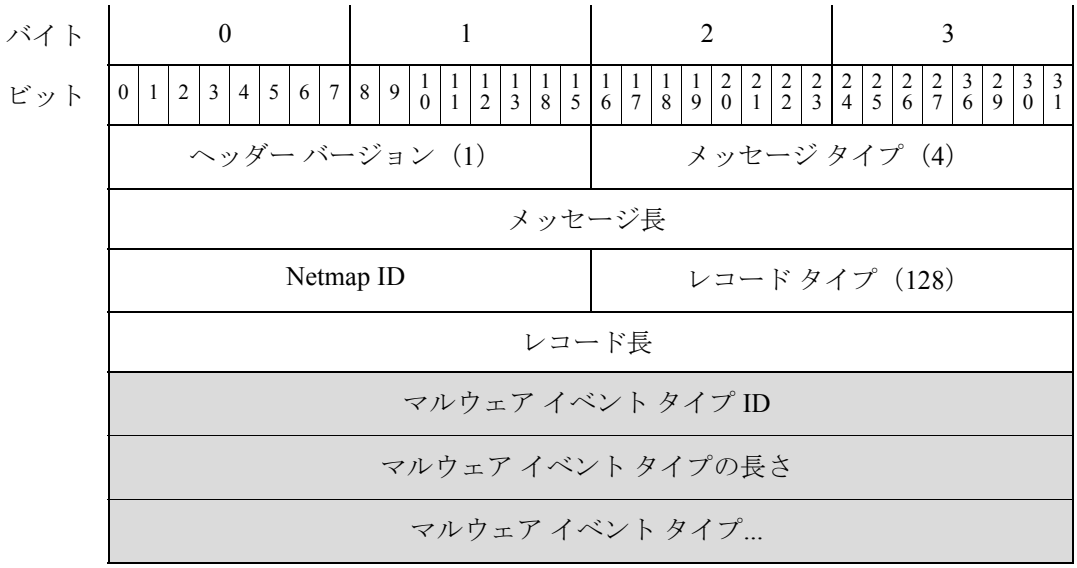
次の表は、Cisco Advanced Malware Protection クラウド 名のデータ ブロックのフィールドについての説明です。

表 3-17　Cisco Advanced Malware Protection クラウド名のデータ 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 クラウド名のデータ ブロック タイプ	uint32	Cisco Advanced Malware Protection クラウド名のデータ 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 クラウド名のデータ 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 クラウド UUID	uint8[16]	接続イベントに関連付けられた Cisco Advanced Malware Protection クラウド の固有識別子として機能する Cisco Advanced Malware Protection クラウド ID 番号。このフィールドは、このレコードの固有キーです。
文字列ブロック タイプ	uint32	Cisco Advanced Malware Protection クラウド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	Cisco Advanced Malware Protection クラウド 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 クラウド 名のバイト数が含まれます。
Cisco Advanced Malware Protection クラウド名	string	Cisco Advanced Malware Protection クラウド名。

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 (2-15 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。



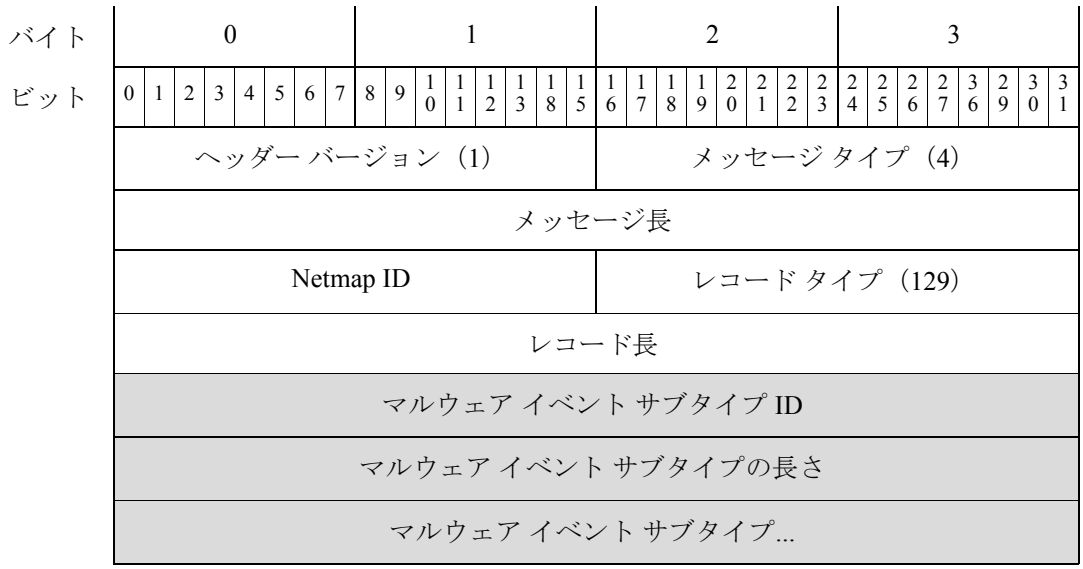
次の表は、マルウェア イベント タイプ レコードのフィールドについての説明です。

表 3-18　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。このフィールドは、このレコードの固有キーです。
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 (2-15 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。



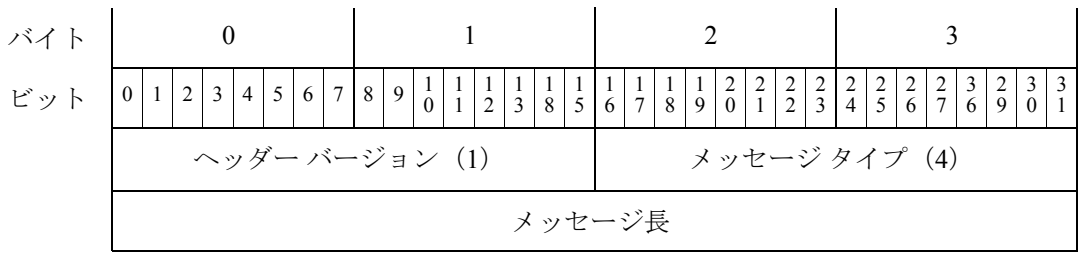
次の表は、マルウェア イベント サブタイプ レコードのフィールドについての説明です。

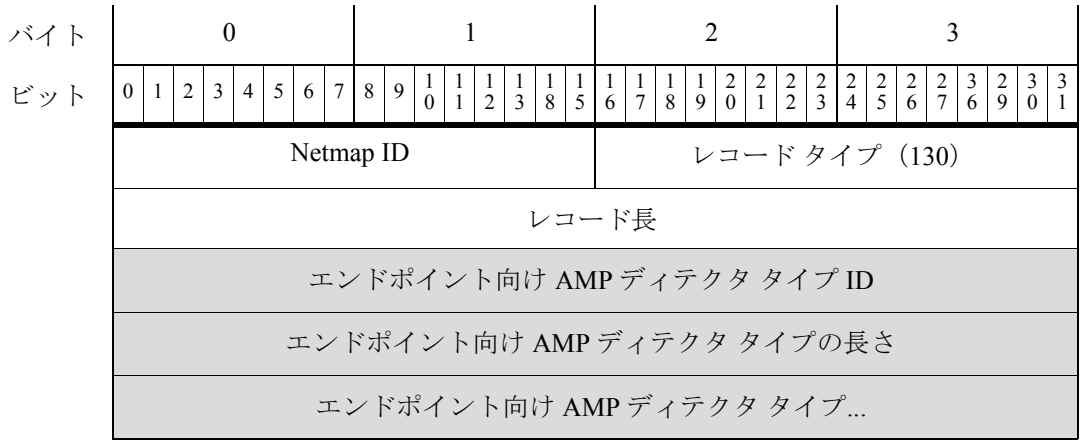
表 3-19　　マルウェア イベント サブタイプ レコード フィールド

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。このフィールドは、このレコードの固有キーです。
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。

エンドポイント向け AMPディテクタ タイプのメタデータ

eStreamer サービスは、エンドポイント向け AMP ディテクタ タイプ レコード内のイベントの エンドポイント向け AMP 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、エンドポイント向け AMP ディテクタ タイプ情報が送信されます。要求フラグ（2-15 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 エンドポイント向け AMP 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。





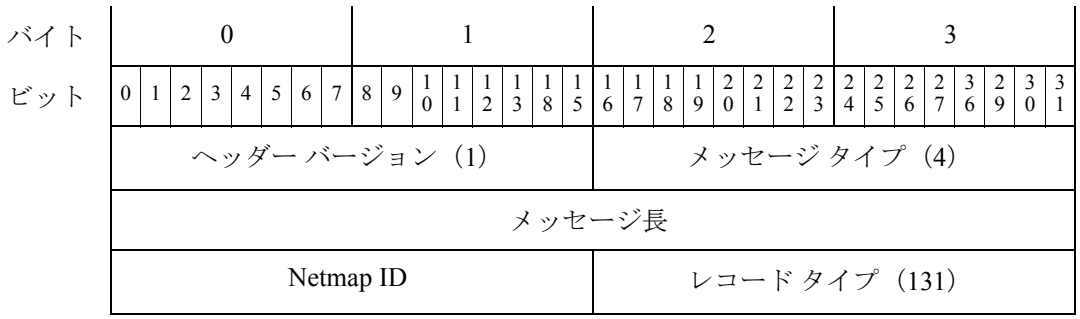
次の表は、エンドポイント向け AMP ディテクタ タイプ レコードのフィールドについての説明です。

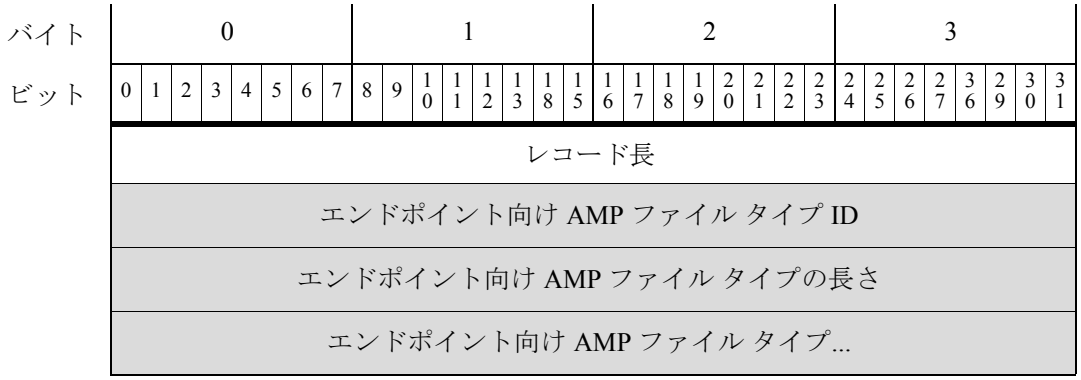
表 3-20　エンドポイント向け AMPディテクタ タイプ レコード フィールド

フィールド	データタイプ	説明
エンドポイント向け AMP ディテクタ タイプ ID	uint32	エンドポイント向けAMPディテクタ タイプID番号。このフィールドは、このレコードの固有キーです。
エンドポイント向け AMP ディテクタ タイプの長さ	uint32	エンドポイント向け AMP ディテクタ タイプに含まれるバイト数。
エンドポイント向け AMP ディテクタ タイプ	string	エンドポイント向け AMP ディテクタのタイプ。

エンドポイント向け AMP ファイル タイプのメタデータ

eStreamer サービスは、エンドポイント向け AMP ファイル タイプ レコード内のイベントの エンドポイント向け AMP 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、エンドポイント向け AMP ファイル タイプ情報が送信されます。要求フラグ（2-15 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 エンドポイント向け AMP 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。





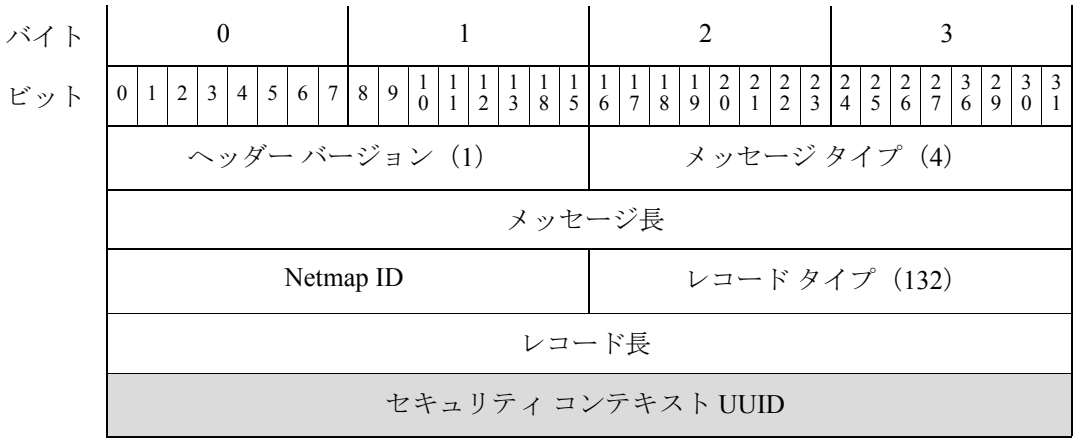
次の表は、エンドポイント向け AMP ファイル タイプ レコードのフィールドについての説明です。

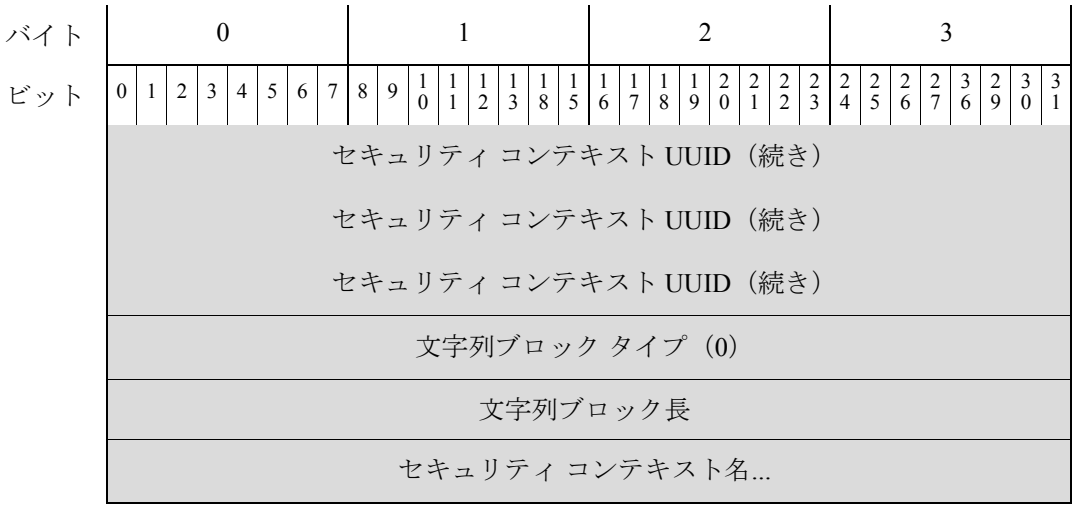
表 3-21　エンドポイント向け AMP ファイル タイプ レコード フィールド

フィールド	データタイプ	説明
エンドポイント向け AMP ファイル タイプ ID	uint32	エンドポイント向け AMP ファイル タイプ ID 番号。このフィールドは、このレコードの固有キーです。
エンドポイント向け AMP ファイル タイプの長さ	uint32	エンドポイント向け AMP ファイル タイプに含まれるバイト数。
エンドポイント向け AMP 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（2-15 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 3-22　　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。このフィールドは、このレコードの固有キーです。
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。

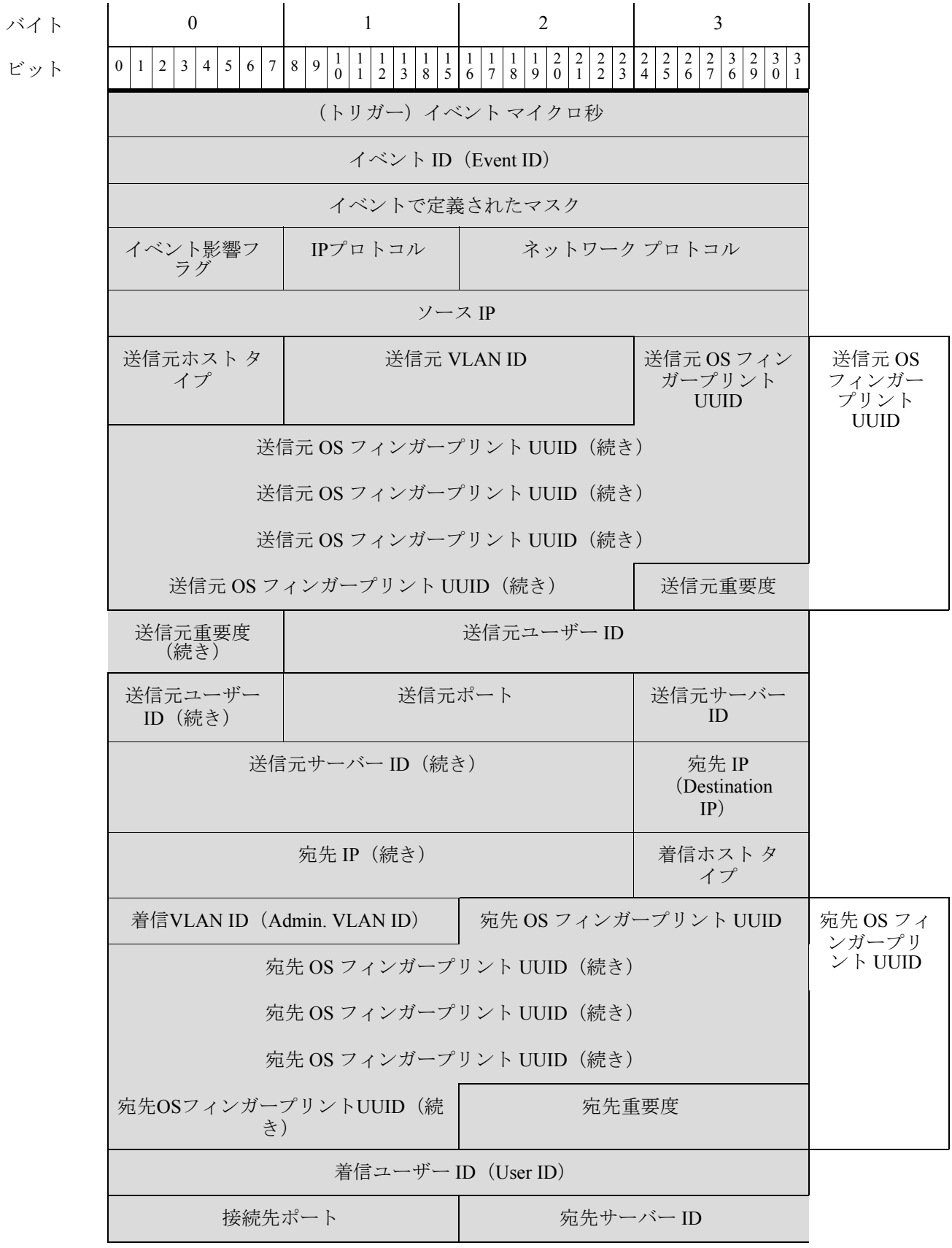
バージョン 5.4 以上の相関イベントには、位置情報、セキュリティ インテリジェンス、および SSL サポートのフィールド新たに加わります。

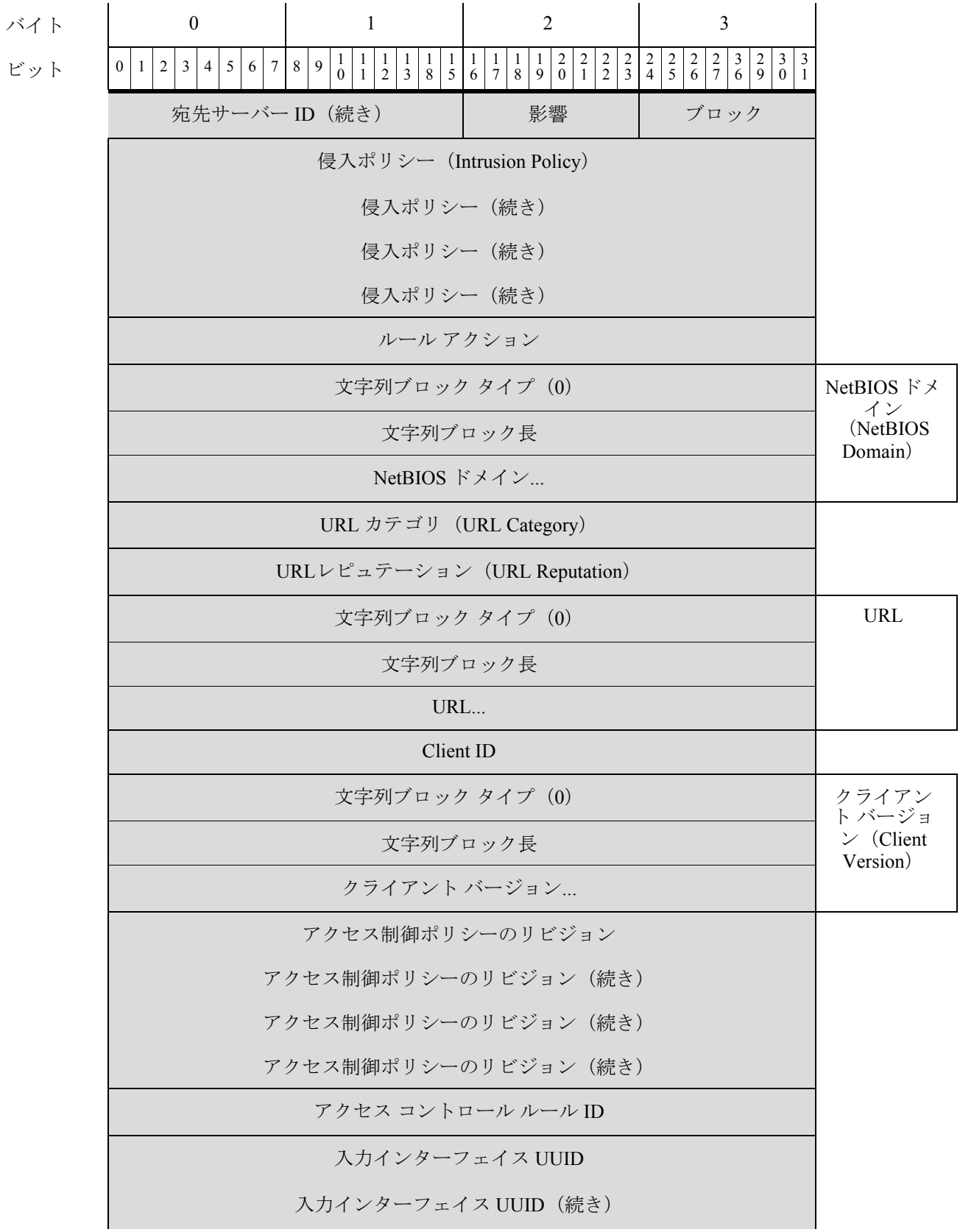
ストリーム要求メッセージでイベント タイプ コード 31 とバージョン コード 9 を要求する拡張要求によってのみ、eStreamer から 5.4 以上の相関イベントを要求できます（拡張要求の送信の詳細については、拡張要求の送信（2-4 ページ）を参照してください）。オプションで、最初のイベン

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、ユーザー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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）																																
相関ブロックのタイプ（156）																																
相関ブロック長																																
デバイスID （Device ID）																																
（相関）イベント秒																																
イベント ID（Event ID）																																
ポリシー ID																																
ルール ID																																
[プライオリティ（Priority）]																																
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（Event Type）							
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																																

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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
（トリガー）イベント マイクロ秒
イベント ID（Event 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）
送信元ユーザー ID
送信元ユーザー ID（続き）
送信元ポート
送信元サーバー ID
送信元サーバー ID（続き）
宛先 IP（Destination IP）
宛先 IP（続き）
着信ホスト タイプ
着信VLAN ID（Admin. 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
着信ユーザー ID（User ID）
接続先ポート
宛先サーバー 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
宛先サーバー ID（続き）
影響
ブロック
侵入ポリシー（Intrusion Policy）
侵入ポリシー（続き）
侵入ポリシー（続き）
侵入ポリシー（続き）
ルール アクション
文字列ブロック タイプ（0）
文字列ブロック長
NetBIOS ドメイン...
NetBIOS ドメイン（NetBIOS Domain）
URL カテゴリ（URL Category）
URL レピュテーション（URL Reputation）
文字列ブロック タイプ（0）
文字列ブロック長
URL...
URL
Client ID
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 バージョン...
クライアント バージョン（Client Version）
アクセス制御ポリシーのリビジョン
アクセス制御ポリシーのリビジョン（続き）
アクセス制御ポリシーのリビジョン（続き）
アクセス制御ポリシーのリビジョン（続き）
アクセス コントロール ルール ID
入力インターフェイス UUID
入力インターフェイス 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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）																																
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（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（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（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																	宛先の国															
セキュリティ インテリジェンス 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
セキュリティ インテリジェンス UUID（続き）																																
セキュリティ インテリジェンス UUID（続き）																																
セキュリティ インテリジェンス UUID（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）																																
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（続き）																																
実際の SSL アクション																																
SSL フロー ステータス																																
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）																																

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（4-65 ページ）を参照してください。

表 3-23　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（4-65 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（Device 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Device 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（Event 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、サービス 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、サービス 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（Priority）]	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（4-75 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（Event Type）	uint8	相関イベントが、侵入、ホスト検出、またはユーザー 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：ユーザー
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Device 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 3-23　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
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 Cisco Secure Firewall 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（Event 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 3-21 (3-45 ページ) を参照してください。

表 3-23　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
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ー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ーを実行しているか（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ー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）。Cisco Secure Firewall 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）。
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（1-4 ページ）を参照してください。

表 3-23　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、サービス 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、ユーザー定義の重要度値: • 0:なし • 1:低 • 2:中 • 3:高
送信元ユーザー 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ーの ID 番号。
送信元ポート	uint16	イベントの送信元ポート。
送信元サーバー ID	uint32	送信元ホスト上で実行するサーバーの 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(1-4 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、サービス 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、ユーザー定義の重要度値: • 0:なし • 1:低 • 2:中 • 3:高

表 3-23　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
宛先ユーザー 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ーの 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ーの ID 番号。
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）
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。
侵入ポリシー（Intrusion Policy）	uint8[16]	イベントに関連付けられた侵入ポリシーの UUID。
ルール アクション	uint32	イベントをトリガーしたルールのユーザー インターフェイスで選択したアクション（許可、ブロックなど）。
文字列ブロック タイプ	uint32	NetBIOS 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 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（4-75 ページ）を参照してください。
文字列ブロック長	uint32	イベント説明の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 NetBIOS ドメイン内のバイト数が含まれます。
NetBIOS ドメイン（NetBIOS Domain）	string	NetBIOS ドメインの名前。
URL カテゴリ	uint32	URL カテゴリを指定する番号。詳細については、URL カテゴリ レコード メタデータ（4-26 ページ）を参照してください。
URL レピュテーション	uint32	URL レピュテーションの ID 番号。URL レピュテーション レコード メタデータ（4-27 ページ）を参照してください
文字列ブロック タイプ	uint32	URL 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 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（4-75 ページ）を参照してください。

表 3-23　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
文字列ブロック長	uint32	イベント説明の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 URL のバイト数が含まれます。
URL	string	関連イベントをトリガーした URL です。
Client ID	uint32	イベントを検出したクライアントの ID 番号。
文字列ブロック タイプ	uint32	クライアント 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 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（4-75 ページ）を参照してください。
文字列ブロック長	uint32	イベント説明の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、およびクライアント バージョン内のバイト数が含まれます。
クライアント バージョン（Client Version）	string	イベントを検出したクライアントのバージョン。
アクセス制御ポリシーのリビジョン	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。
アクセス コントロール ルール ID	uint32	イベントをトリガーしたルールの内部 ID。
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。

表 3-23　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 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。
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)」

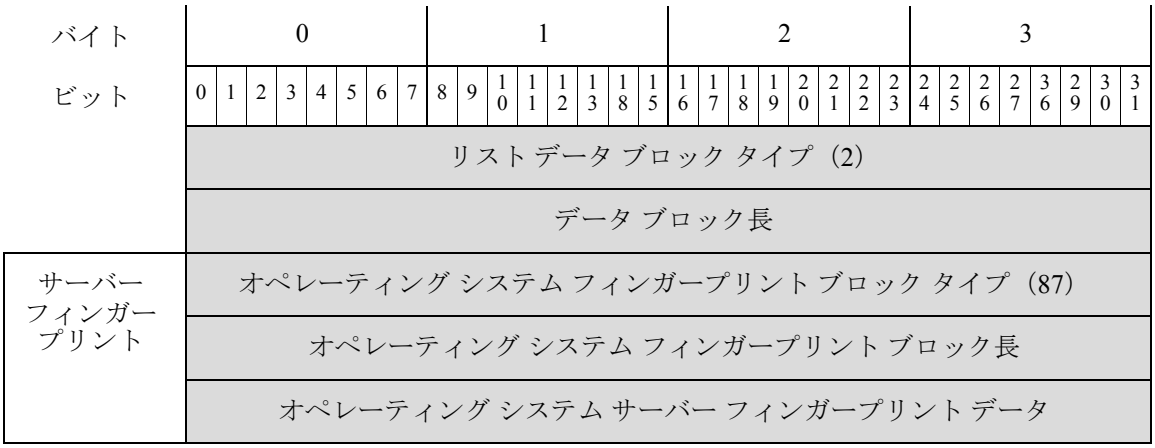
表 3-23　相関イベント 5.4 以上のデータ フィールド（続き）

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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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 サーバー証明書の 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 3-24 (3-60 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 3-24　　シリーズ 2 のブロック タイプ

タイプ (Type)	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 (3-66 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 (3-67 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 (3-68 ページ) を参照してください。

表 3-24　シリーズ 2 のブロック タイプ（続き）

タイプ（Type）	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（3-69 ページ）を参照してください。
4	イベント追加データ	レガシー	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（B-69 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（B-71 ページ）を参照してください。
14	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（3-69 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（3-72 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 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ー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-73 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-97 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（3-73 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（3-74 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（3-85 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（3-87 ページ）を参照してください。

表 3-24　シリーズ 2 のブロック タイプ（続き）

タイプ（Type）	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-313 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（3-72 ページ）。
24	マルウェア イベント	レガシー	Cisco Advanced Malware Protection 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ー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-77 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-73 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-97 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-356 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（3-111 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（3-114 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（3-122 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-317 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-313 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-321 ページ）。

表 3-24　シリーズ 2 のブロック タイプ（続き）

タイプ（Type）	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 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ー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-83 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-77 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-90 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-90 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-83 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-90 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-321 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 7.0 以上（3-100 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（4-38 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（3-111 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-356 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 3-24　シリーズ 2 のブロック タイプ（続き）

タイプ（Type）	目次	データ ブロック ステータス	説明
54	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 5.3.1（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）。ブロック 45 により廃止される予定です侵入イベント レコード 5.4.x（B-38 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-328 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-321 ページ）。ブロック 46 により廃止される予定です7.0 以降のファイルイベント（3-89 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 7.0 以上（3-100 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-90 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 7.0 以上（3-100 ページ）。
45	侵入イベント	レガシー	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 5.4.x（B-38 ページ）」を参照してください。ブロック 42 は廃止予定です侵入イベント レコード 5.3.1（B-32 ページ）。ブロック 60 により廃止される予定です侵入イベント レコード 6.x（B-47 ページ）。
46	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。マルウェア イベントのデータ ブロック 7.0 以上（3-100 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-328 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 7.0 以上（3-100 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-97 ページ）。
50	SSL 証明書の詳細	現在（Current）	SSL 証明書に関する情報が含まれています。5.4 以上の SSL 証明書の詳細のデータ ブロック（3-133 ページ）を参照してください。
51	SSL ルール ID	現在（Current）	SSL ルールに関する情報が含まれています。SSL ルール ID（3-126 ページ）を参照してください

表 3-24　シリーズ 2 のブロック タイプ（続き）

タイプ（Type）	目次	データ ブロック ステータス	説明
72	ファイル イベント	レガシー	ファイルイベントに関する情報が含まれています。「6.x のファイルイベント（B-345 ページ）」を参照してください。ブロック 46 は廃止予定ですファイル イベント 5.4.x（B-334 ページ）。ブロックタイプ 79 で廃止されます。マルウェア イベントのデータ ブロック 7.0 以上（3-100 ページ）
57	ユーザー レコード	現在（Current）	ユーザーに関する情報が含まれています。ユーザー レコード（3-26 ページ）を参照してください
58	エンドポイント プロファイル（Endpoint Profile）	現在（Current）	ネットワークエンドポイントに関する情報が含まれています。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（3-78 ページ）を参照してください
59	アクセス コントロール ポリシー ルールの理由	現在（Current）	アクセス コントロール ポリシー ルールに関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（3-85 ページ）を参照してください
60	侵入イベント	レガシー	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 6.x（B-47 ページ）」を参照してください。ブロック 45 は廃止予定です侵入イベント レコード 5.3.1（B-32 ページ）。ブロック 81 により廃止される予定です侵入イベント レコード 7.1 以上（3-9 ページ）。
61	名前説明マッピング	現在（Current）	多くの状況で、名前を説明にマッピングするために使用されます。名前説明マッピングのデータ ブロック（3-71 ページ）を参照してください
62	マルウェア イベント	レガシー	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 6.x（B-116 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-97 ページ）。ブロックタイプ 80 で廃止されます。マルウェア イベントのデータ ブロック 7.0 以上（3-100 ページ）
64	アクセス コントロール ポリシー名	現在（Current）	アクセス コントロール ポリシー名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（3-87 ページ）を参照してください
79	ファイル イベント	現在（Current）	ファイルイベントに関する情報が含まれています。「7.0 以降のファイルイベント（3-89 ページ）」を参照してください。ブロック 56 は廃止予定です6.x のファイルイベント（B-345 ページ）。

表 3-24　シリーズ 2 のブロック タイプ（続き）

タイプ（Type）	目次	データ ブロック ステータス	説明
80	マルウェア イベント	現在（Current）	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 7.0 以上（3-100 ページ）」を参照してください。ブロック 62 は廃止予定ですマルウェア イベント データ ブロック 6.x（B-116 ページ）。
81	侵入イベント	現在（Current）	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 7.1 以上（3-9 ページ）」を参照してください。ブロック 60 は廃止予定です侵入イベント レコード 6.x（B-47 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（2-29 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（3-66 ページ）
- BLOB データ ブロック（3-67 ページ）
- リスト データ ブロック（3-68 ページ）
- 汎用リストのデータ ブロック（3-69 ページ）
- UUID 文字列マッピングのデータ ブロック（3-69 ページ）
- 名前説明マッピングのデータ ブロック（3-71 ページ）

文字列データ ブロック

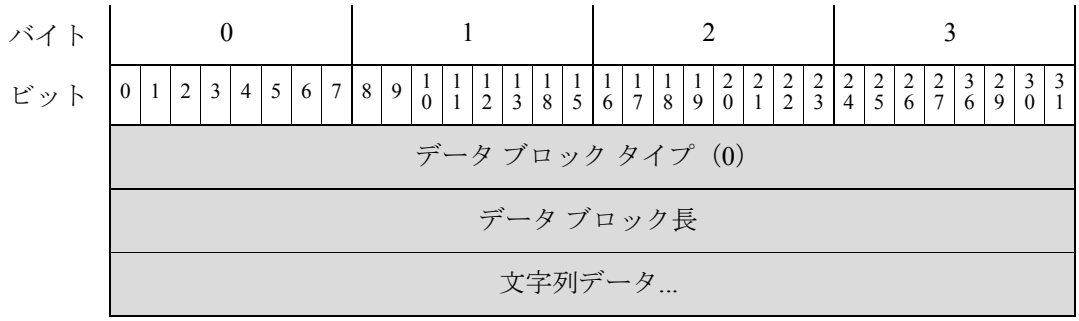
eStreamer サービスは、文字列データ ブロックを使用してメッセージの文字列データを送信します。通常、これらのブロックは、オペレーティング システムやサーバー名などを識別するために他のデータ ブロック内に表示されます。

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。

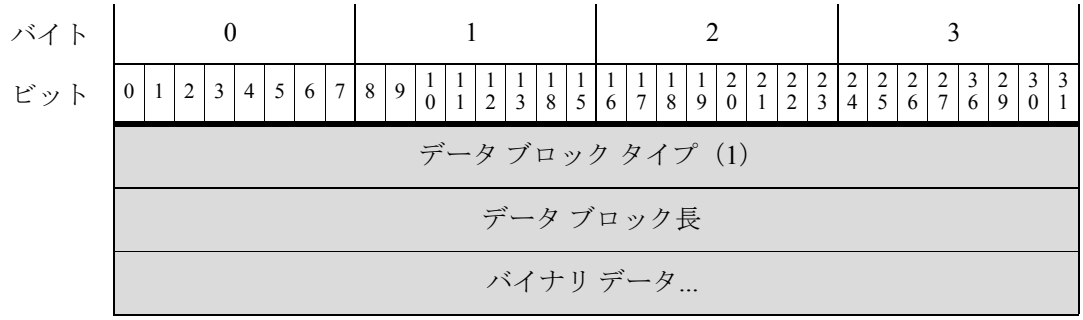
表 3-25　　文字列ブロック フィールド

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ー 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。



次の表に、BLOB データ ブロックのフィールドの説明を示します。

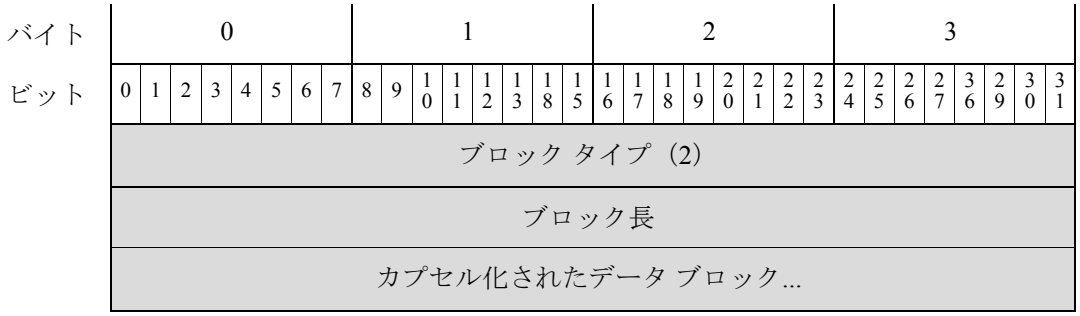
表 3-26　BLOB データ ブロック フィールド

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（variable）	サーバー 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 サーバー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。

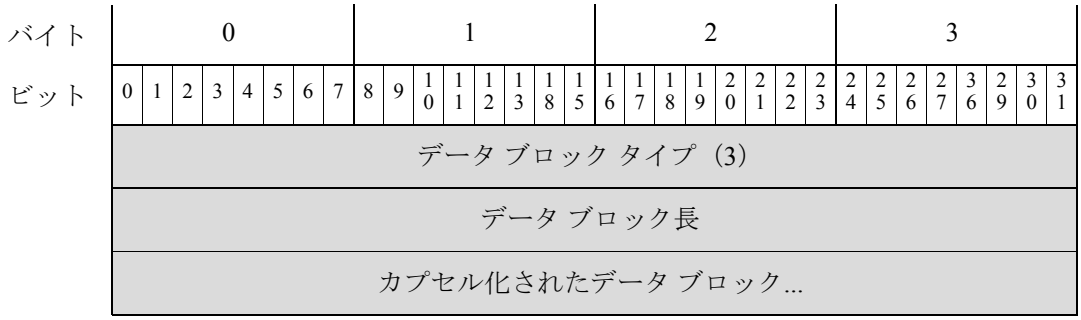
表 3-27　リスト データ フィールド

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 つのサブサーバー データ ブロックがあるとすると、この値には、サブサーバー 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（variable）	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。

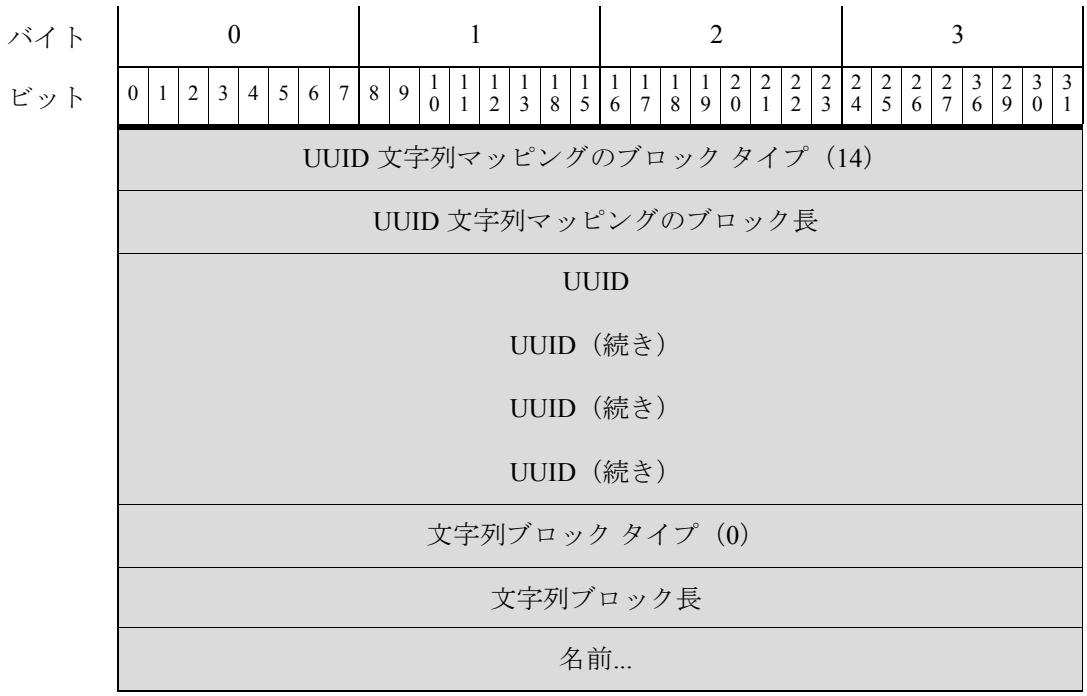
表 3-28　　汎用リスト データ ブロックのフィールド

フィールド	バイト数	説明
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（variable）	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 3-29　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。このフィールドは、このレコードの固有キーです。
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（Name）]	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 3-30　　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。このフィールドは、このレコードの固有キーです。
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（Name）]	string	イベントまたはオブジェクトの名前。

表 3-30　名前説明マッピングのデータ 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	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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(Name)]	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。

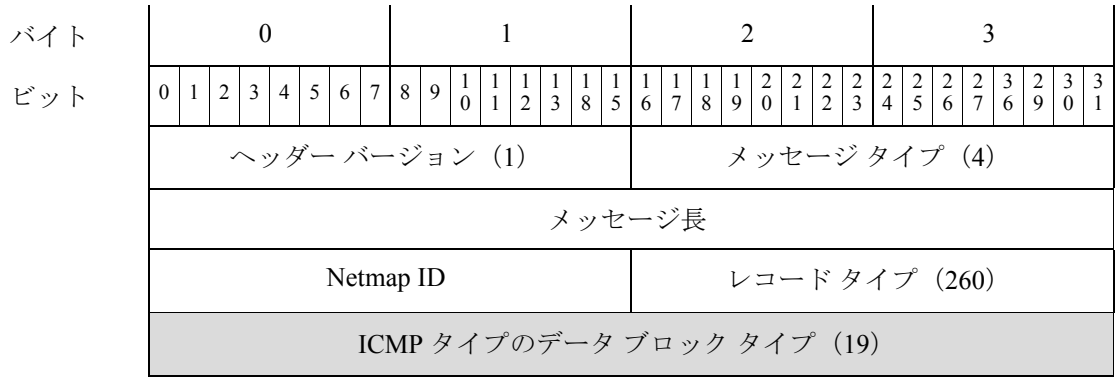
表 3-31　　アクセス コントロール ポリシー ルール ID のメタデータ ブロック フィールド

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。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID。このフィールドは、このレコードの固有キーです。
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(Name)]	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。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ICMP タイプのデータのブロック長																															
	タイプ（Type）																プロトコル															
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、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 3-32　　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（Type）	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（270）															
	ICMP コードのデータ ブロック タイプ（20）																															
	ICMP コードのデータ ブロック長																															
	コード（Code）																タイプ															
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 3-33　　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（Code）	uint16	イベントの ICMP コード。
タイプ（Type）	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。

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（282）															
レコード長																																
セキュリティ インテリジェンス UUID セキュリティ インテリジェンス UUID（続き） セキュリティ インテリジェンス UUID（続き） セキュリティ インテリジェンス 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 インテリジェンスのカテゴリ...																																

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 3-34　　セキュリティ コンテキスト名のレコード フィールド

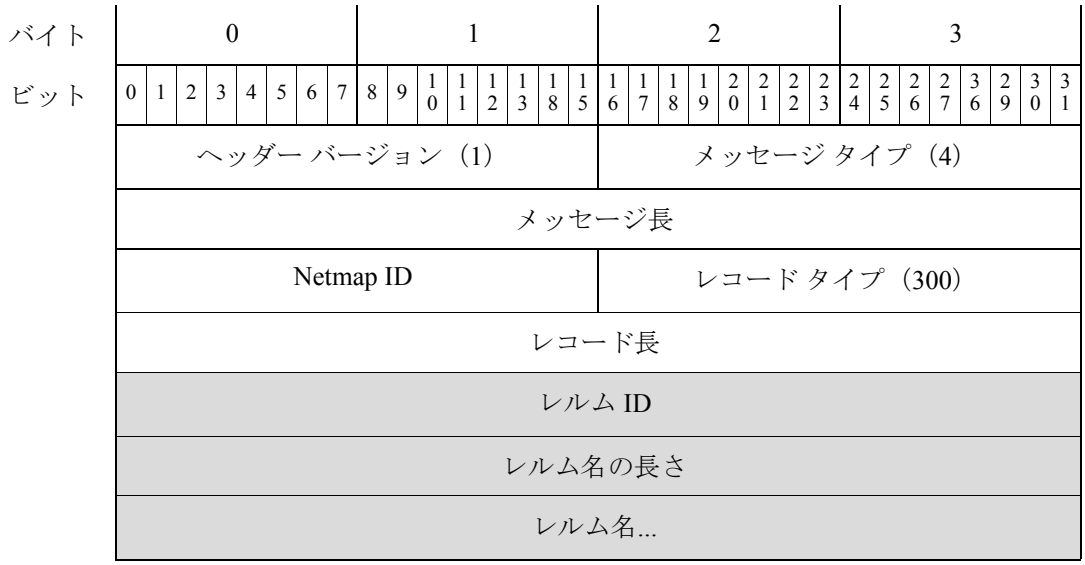
フィールド	データタイプ	説明
セキュリティ インテリジェンス UUID	uint8[16]	セキュリティ インテリジェンスの UUID。このフィールドは、このレコードの固有キーです。
文字列ブロック タイプ	uint32	セキュリティ インテリジェンス カテゴリを含む文字列データ ブロックを開始します。この値は常に 0 です。

表 3-34　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 3-35　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。このフィールドは、このレコードの固有キーです。
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。

	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(301)															
		エンドポイント プロファイルのブロック タイプ(58)																															
		エンドポイント プロファイルのデータのブロック長																															
		ID																															
プロファイル名(Profile Name)		文字列ブロック タイプ(0)																															
		文字列ブロック長																															
		プロファイル名...																															
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...																															

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 3-36　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

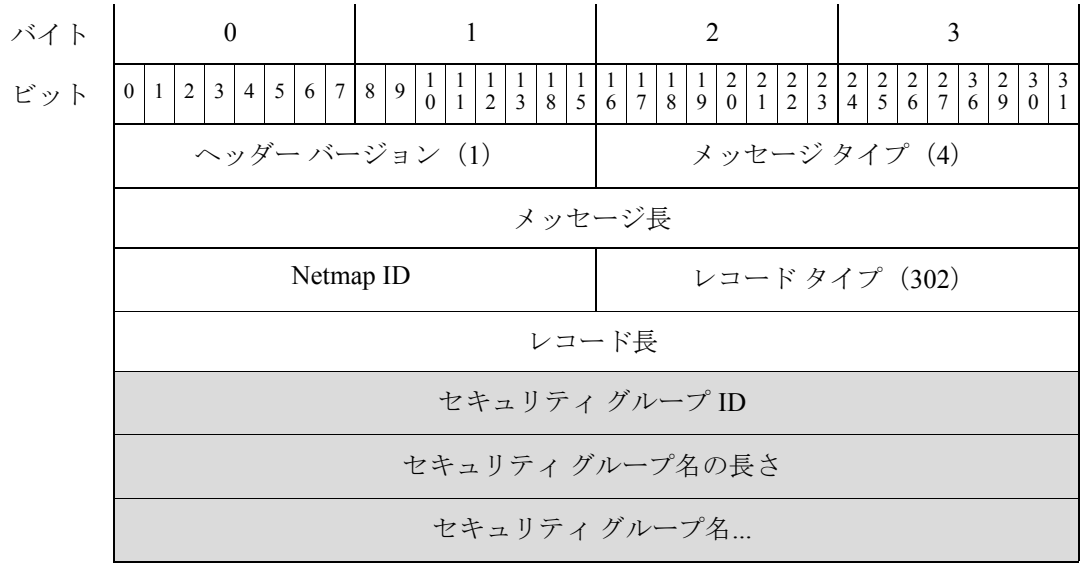
フィールド	データタイプ	説明
エンドポイント プロファイルのデータ ブロック タイプ	uint32	エンドポイント プロファイル データ ブロックを開始します。この値は常に 58 です。
エンドポイント プロファイルのデータのブロック長	uint32	エンドポイント プロファイルのデータ ブロックの合計バイト数です。エンドポイント プロファイルのデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
ID	uint32	エンドポイント ID 番号。

表 3-36　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（Profile Name）	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 3-37　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。このフィールドは、このレコードの固有キーです。
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。

	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（320）																
		レコード長																															
		名前説明のブロック タイプ（61）																															
		名前説明のデータ ブロック長																															
		DNS レコード ID																															
DNS レコード タイプ名		文字列ブロック タイプ（0）																															
		文字列ブロック長																															
		DNS レコード タイプ名...																															
DNS レコード タイプの説明		文字列ブロック タイプ（0）																															
		文字列ブロック長																															
		DNS レコード タイプの説明...																															

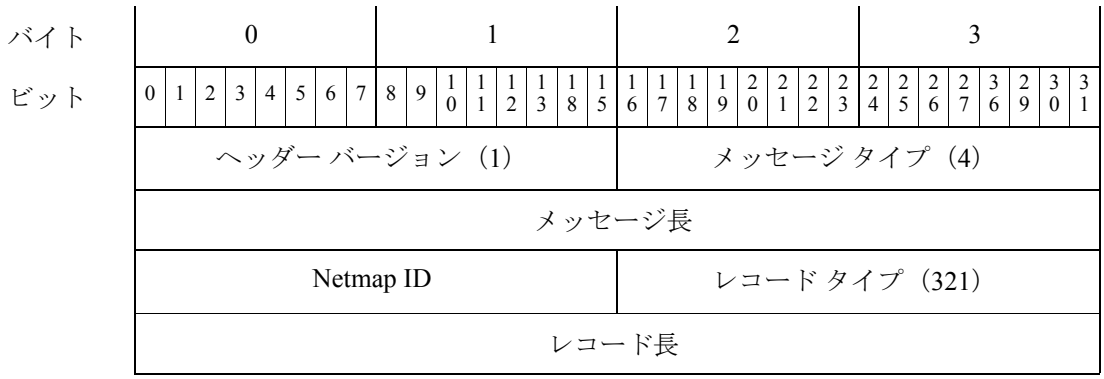
次の表は、DNS レコード タイプのメタデータのレコードのフィールドについての説明です。

表 3-38　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
名前説明のデータ ブロック タイプ	uint32	名前説明のデータ ブロックを開始します。この値は常に 61 です。
名前説明のデータ ブロック長	uint32	名前説明のデータ ブロック内の総バイト数。これには、名前説明のデータ ブロックのタイプ フィールドおよび長さフィールド用の 8 バイトと、その後のデータのバイト数が含まれます。
DNS レコード ID	uint32	DNS レコード ID 番号。このフィールドは、このレコードの固有キーです。
文字列ブロック タイプ	uint32	DNS レコード タイプ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	DNS レコード タイプ名文字列のデータ ブロック内に含まれるバイト数。これには、ブロック タイプ フィールドおよびヘッダー フィールド用の 8 バイトと、DNS レコード タイプ名フィールド内のバイト数が含まれます。
DNS レコード タイプ名	string	DNS レコード タイプの名前。
文字列ブロック タイプ	uint32	DNS レコード 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	DNS レコード タイプ説明文字列のデータ ブロック内に含まれるバイト数。これには、ブロック タイプ フィールドおよびヘッダー フィールド用の 8 バイトと、DNS レコード タイプ説明フィールド内のバイト数が含まれます。
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。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	名前説明のブロック タイプ（61）																															
	名前説明のデータ ブロック長																															
	DNS 応答 ID																															
DNSレスポンス タイプ名	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	DNS レスポンス タイプ名...																															
DNSレスポンス タイプの説明	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	DNS レスポンス タイプの説明...																															

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 3-39　　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
名前説明のデータ ブロック タイプ	uint32	名前説明のデータ ブロックを開始します。この値は常に 61 です。
名前説明のデータ ブロック長	uint32	名前説明のデータ ブロック内の総バイト数。これには、名前説明のデータブロックのタイプフィールドおよび長さフィールド用の 8 バイトと、その後のデータのバイト数が含まれます。
DNS 応答 ID	uint32	DNS レスポンス ID 番号。このフィールドは、このレコードの固有キーです。
文字列ブロック タイプ	uint32	DNS レスポンス タイプ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	DNS レスポンス タイプ名文字列のデータ ブロック内に含まれるバイト数。これには、ブロック タイプ フィールドおよびヘッダー フィールド用の 8 バイトと、DNS レスポンス タイプ名フィールド内のバイト数が含まれます。
DNS レスポンス タイプ名	string	DNS レスポンス タイプの名前。
文字列ブロック タイプ	uint32	DNS レスポンス 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。

表 3-39　DNS レスポンス タイプのメタデータ フィールド（続き）

フィールド	データタイプ	説明
文字列ブロック長	uint32	DNS レスポンス タイプ説明文字列のデータ ブロック内に含まれるバイト数。これには、ブロック タイプ フィールドおよびヘッダー フィールド用の 8 バイトと、DNS レスポンスタイプ説明フィールド内のバイト数が含まれます。
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。

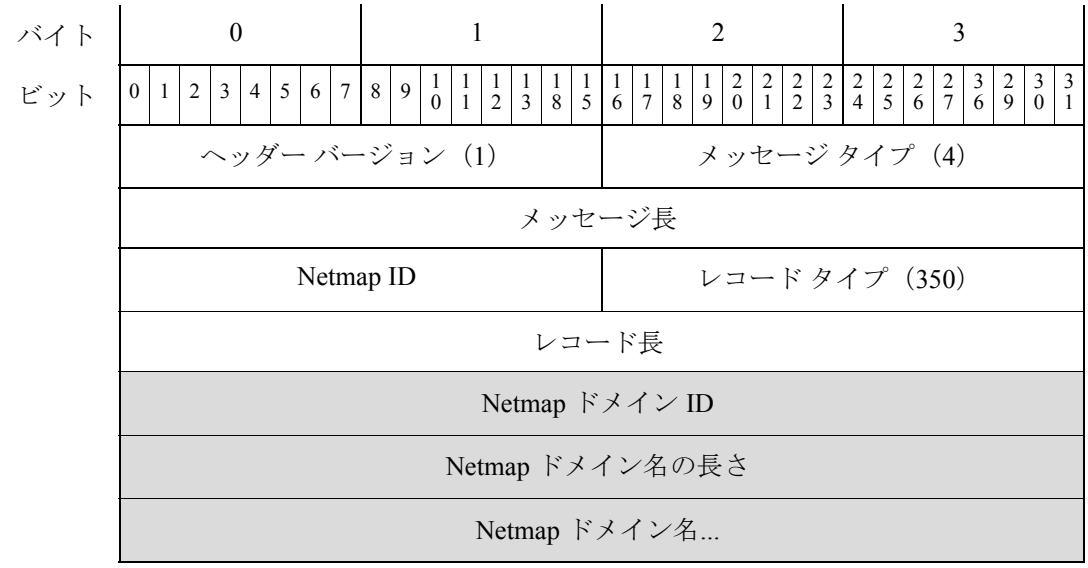
次の表は、シンクホールのメタデータのレコードのフィールドについての説明です。

表 3-40　　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
UUID 文字列データ ブロック タイプ	uint32	UUID 文字列データ ブロックを開始します。この値は常に 14 です。
UUID 文字列データ ブロック長	uint32	UUID 文字列データ ブロック内の総バイト数。これには、UUID 文字列データ ブロックのタイプ フィールドおよび長さフィールド用の 8 バイトと、その後のデータのバイト数が含まれます。
シンクホール UUID	uint8[16]	シンクホールの UUID 番号。このフィールドは、このレコードの固有キーです。
文字列ブロック タイプ	uint32	シンクホ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	シンクホール名文字列のデータ ブロック内に含まれるバイト数。これには、ブロック タイプ フィールドおよびヘッダー フィールド用の 8 バイトと、シンクホール名フィールド内のバイト数が含まれます。
シンクホール名	string	シンクホールの名前。

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。

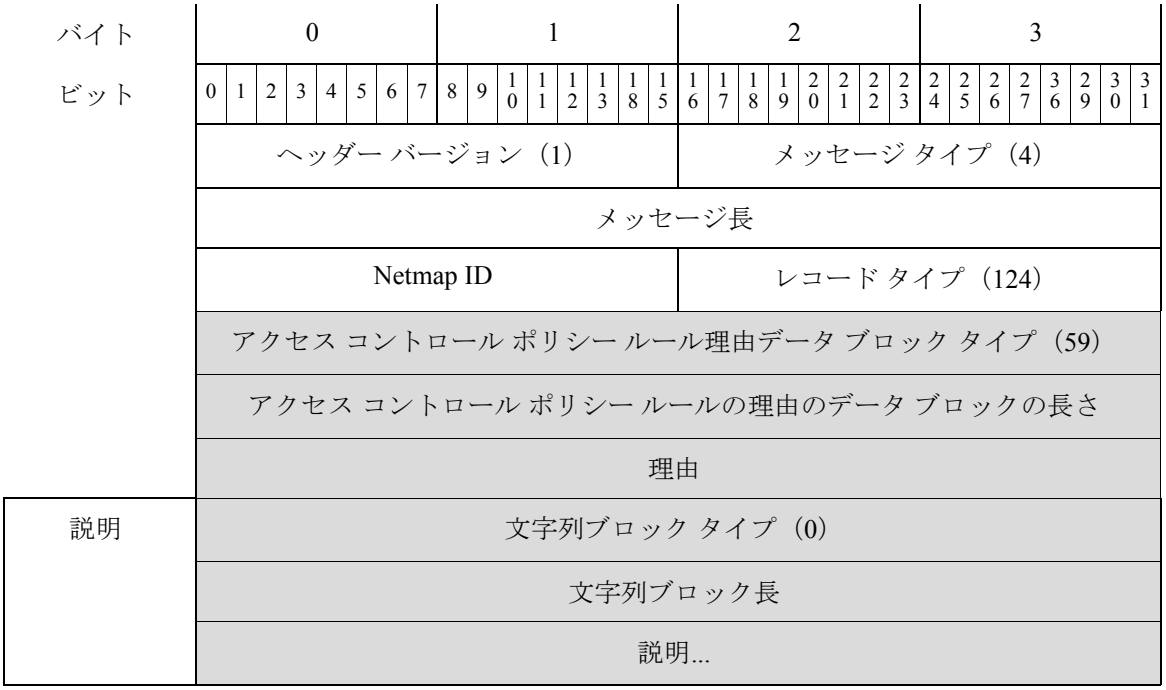
表 3-41　シンクホールのメタデータのレコード フィールド

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。このフィールドは、このレコードの固有キーです。
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。



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 3-42　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。 ルールの理由は、複数のビットを設定できるバイナリ ビットマップです。ルールには、複数の理由がある場合があります。ビット値は次のとおりです。 • **1**：IP ブロック • **2**：IP モニター • **4**：ユーザー バイパス • **8**：ファイル モニター • **16**：ファイル ブロック • **32**：侵入モニター • **64**：侵入ブロック • **128**：ファイル再開ブロック • **256**：ファイル再開許可 • **512**：ファイルカスタム検出 • **1024**：SSL ブロック • **2048**：DNS ブロック • **4096**：DNS モニター • **8192**：URL ブロック • **16384**：URL モニター • **32768**：コンテンツ制約 • **65536**：インテリジェント アプリケーション バイパス • **131072**：WSA 脅威
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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	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（64）																															
	アクセス コントロール ポリシー名のデータ ブロック長																															
	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（Sensor ID）																															
[名前（Name）]	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 3-43　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

表 3-43　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
センサー ID（Sensor 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(Name)]	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 3-44　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

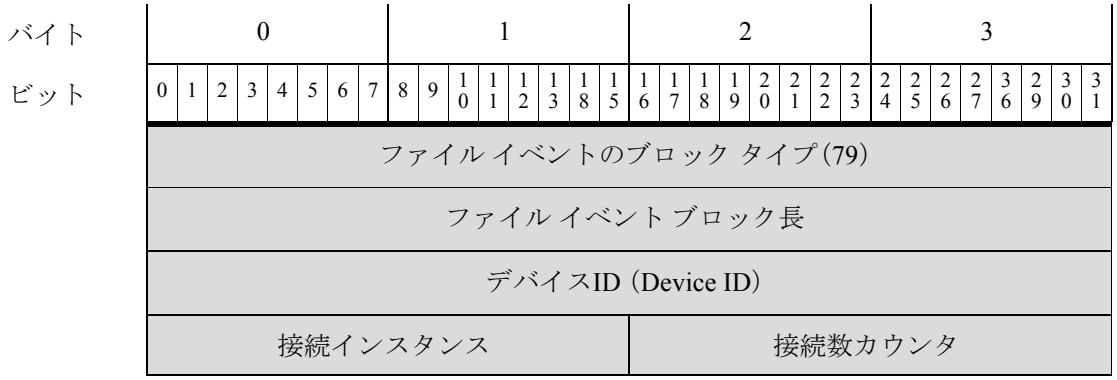
フィールド	データタイプ	説明
IP レピュテーション カテゴリのデータ ブロック タイプ	uint32	IP レピュテーション カテゴリのデータ ブロックを開始します。この値は常に 22 です。
IP レピュテーション カテゴリのデータ ブロックの長さ	uint32	IP レピュテーション カテゴリのデータ ブロックの合計バイト数です。IP レピュテーション カテゴリのデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID。
ポリシー UUID	uint8[16]	イベントをトリ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。

7.0 以降のファイルイベント

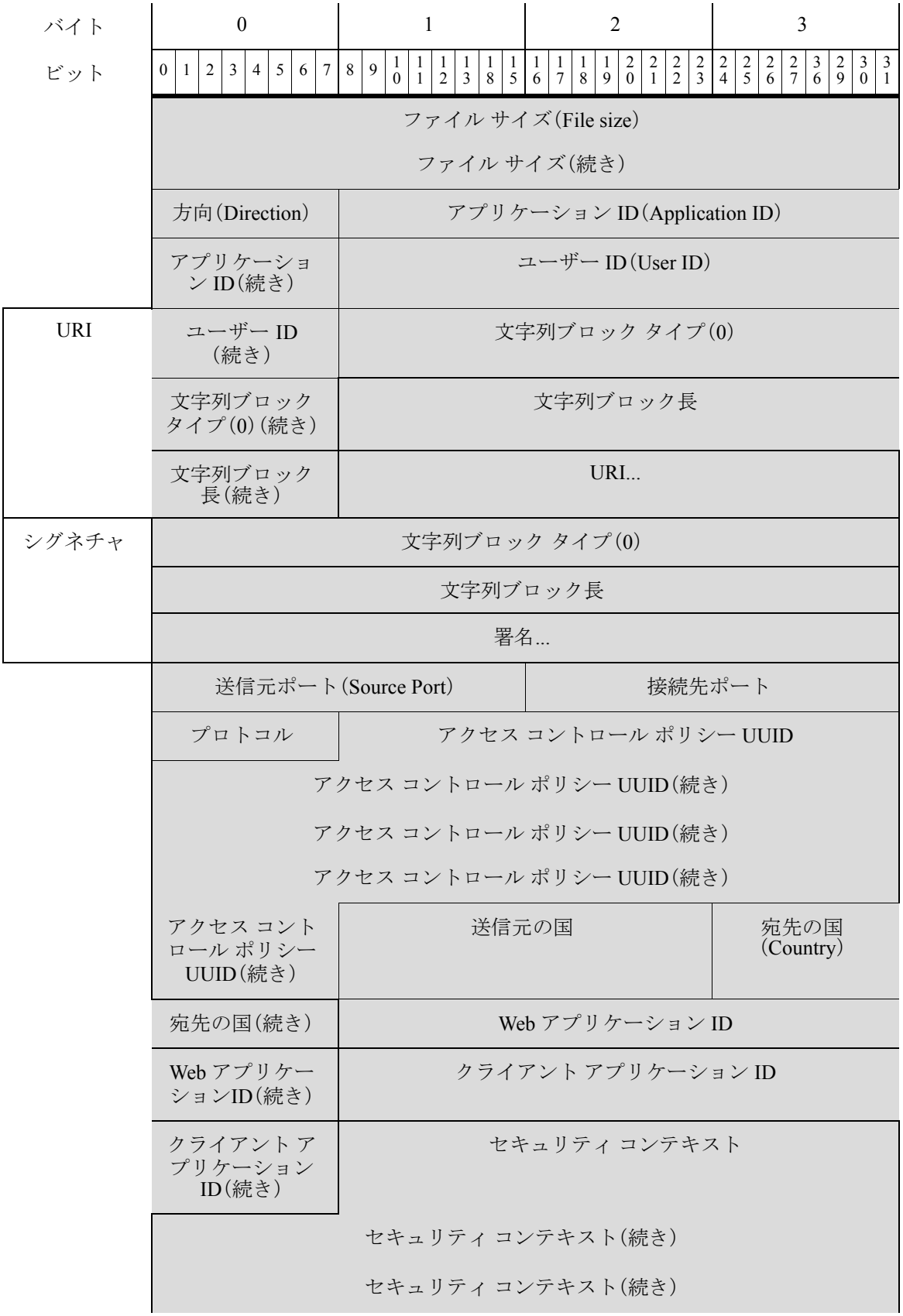
ファイル イベントのデータ ブロックには、ネットワーク経由で送信されるファイルの情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイルイベントは、シリーズ 2 グループのブロックのブロックタイプ 79 です。これはブロック タイプ 56 に取って代わります。Virtual Routing and Forwarding のフィールド。

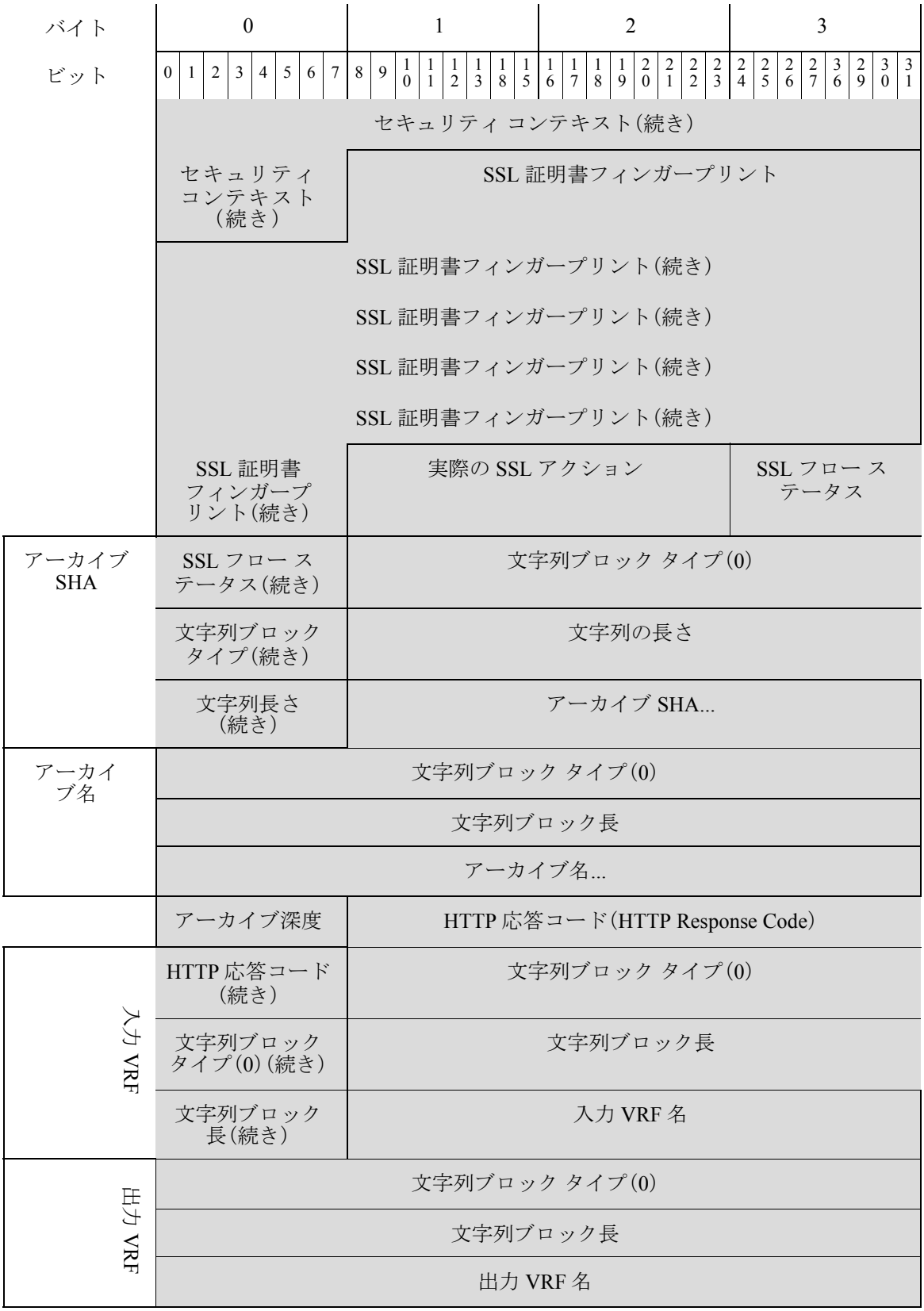
ファイルイベントレコードを要求するには、イベントバージョン 7 およびイベントコード 111 の要求メッセージ内に、ファイルイベントフラグ（要求フラグフィールドのビット 30）を設定します。要求フラグ（2-15 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（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																															
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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
ファイル サイズ(File size)
ファイル サイズ(続き)
方向(Direction)
アプリケーション ID(Application ID)
アプリケーション ID(続き)
ユーザー ID(User ID)
URI
ユーザー 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(Source Port)
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(Country)
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)
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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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
HTTP 応答コード(HTTP Response Code)
入力 VRF
HTTP 応答コード(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)
入力 VRF 名
出力 VRF
文字列ブロック タイプ(0)
文字列ブロック長
出力 VRF 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 3-45　7.0 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 79 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（Device 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 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 AMP クラウド サービスが要求に応答しなかった。 • 5（CUSTOM SIGNATURE）：ファイルがユーザー定義のハッシュと一致するため、ユーザー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 3-45　7.0 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 3-45　7.0 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ー制限超過によるキャパシティの処理):サーバー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 3-45　7.0 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:マルウェア許可リスト • 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、エンドポイント向け AMP 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 3-45　7.0 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 サイズ（File size）	uint64	ファイルのサイズ（バイト単位）。
方向（Direction）	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（Application 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。
ユーザー ID（User 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ーの 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	ユーザーが指定した 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 サーバー証明書の SHA1 ハッシュ。

表 3-45　7.0 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
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 3-45　7.0 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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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 3-45　7.0 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。
HTTP 応答コード(HTTP Response Code)	uint32	HTTP 応答コード。
文字列ブロックタイプ	uint32	入力 VRF 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。ブロックタイプとヘッダーフィールドの 8 バイト、および入力 VRF 名フィールドのバイト数が含まれています。
入力 VRF 名	文字列	トラフィックがネットワークに入るときに通過する仮想ルータ。
文字列ブロックタイプ	uint32	出力 VRF 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。ブロックタイプとヘッダーフィールドの 8 バイト、および出力 VRF 名フィールドのバイト数が含まれています。
出力 VRF 名	文字列	トラフィックがネットワークから出るときに通過する仮想ルータの名前。

マルウェア イベントのデータ ブロック 7.0 以上

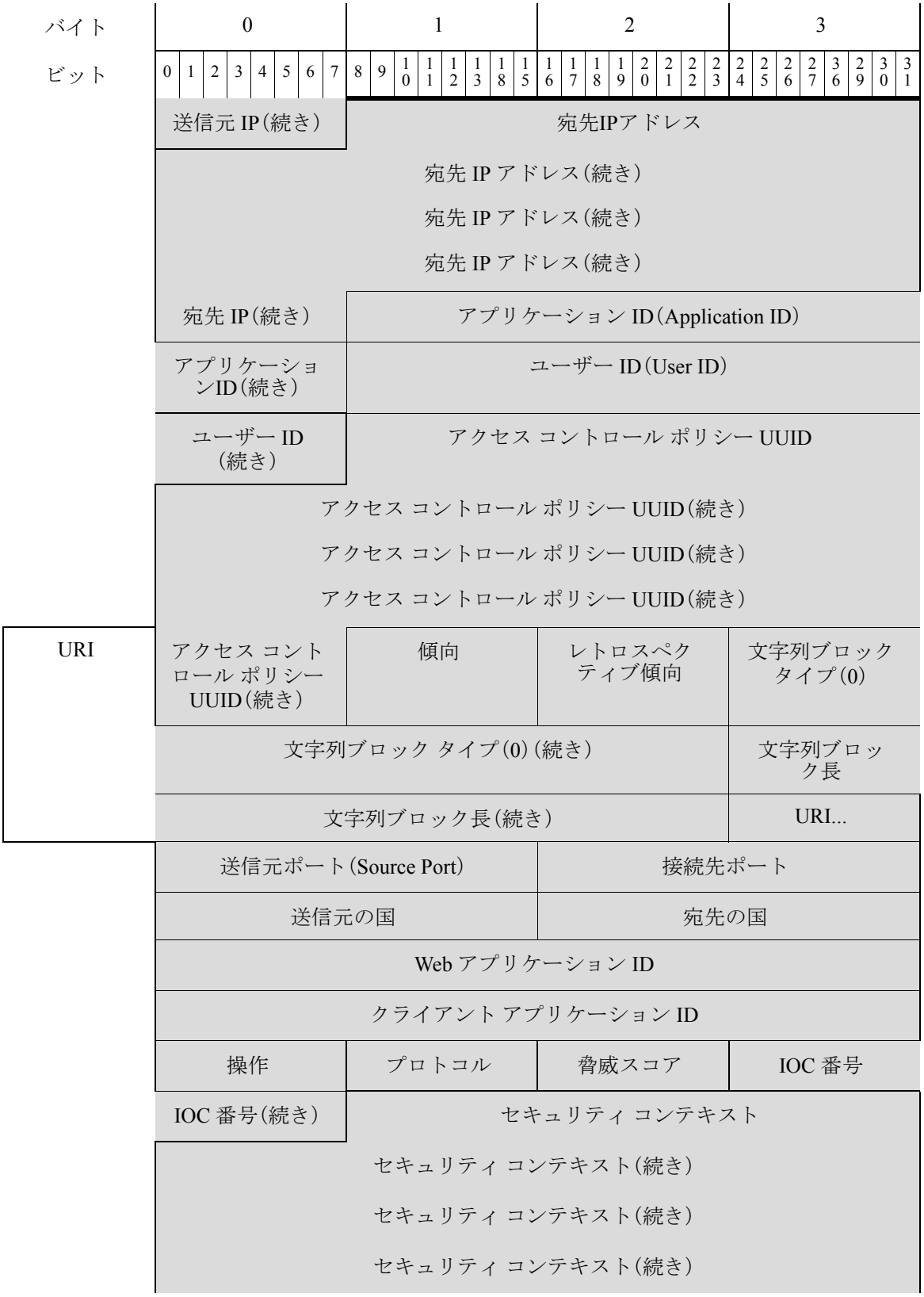
eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザーに関する情報が含まれています。マルウェアイベントのデータブロックは、シリーズ 2 グループのブロックのブロックタイプ 80 です。これはブロック 62 に置き換わります。Virtual Routing and Forwarding のフィールドが追加されました。

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 8 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	マルウェア イベントのブロック タイプ(80)																															
	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...																							
ユーザー (User)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザー...																															
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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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(File size)																															
	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(Name)]	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 (Device 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(Direction)								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 18 15
16 17 18 19 20 21 22 23
24 25 26 27 36 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（Application ID）
アプリケーションID（続き）
ユーザー ID（User ID）
ユーザー 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（Source Port）
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）

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）								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）								文字列ブロック タイプ（0）																							
	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								HTTP レスポンス（HTTP Response）																							
入力 VRF	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（続き）								文字列ブロック長																							
	文字列ブロック長（続き）								入力 VRF 名																							
出力 VRF	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	出力 VRF 名																															

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 3-46　　7.0 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 80 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 エンドポイント向け AMP 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 クラウドの、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	ユーザー文字列データ 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、およびユーザー フィールドのバイト数を含む)。
ユーザー(User)	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ー。これらのユーザーはユーザー 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 3-46　7.0 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	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（File size）	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、エンドポイント向け AMP 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。

表 3-46　7.0 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
デバイスID（Device 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（Direction）	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（Application 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。
ユーザー ID（User 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ーの 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 AMP 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 AMP クラウド サービスが要求に応答しなかった。 • 5（CUSTOM SIGNATURE）：ファイルがユーザー定義のハッシュと一致するため、ユーザーが指定した方法で処理されました。

表 3-46　7.0 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
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：マルウェア許可リスト • 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	ユーザーが指定した 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。

表 3-46　7.0 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
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 サーバー証明書の 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 3-46　7.0 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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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。

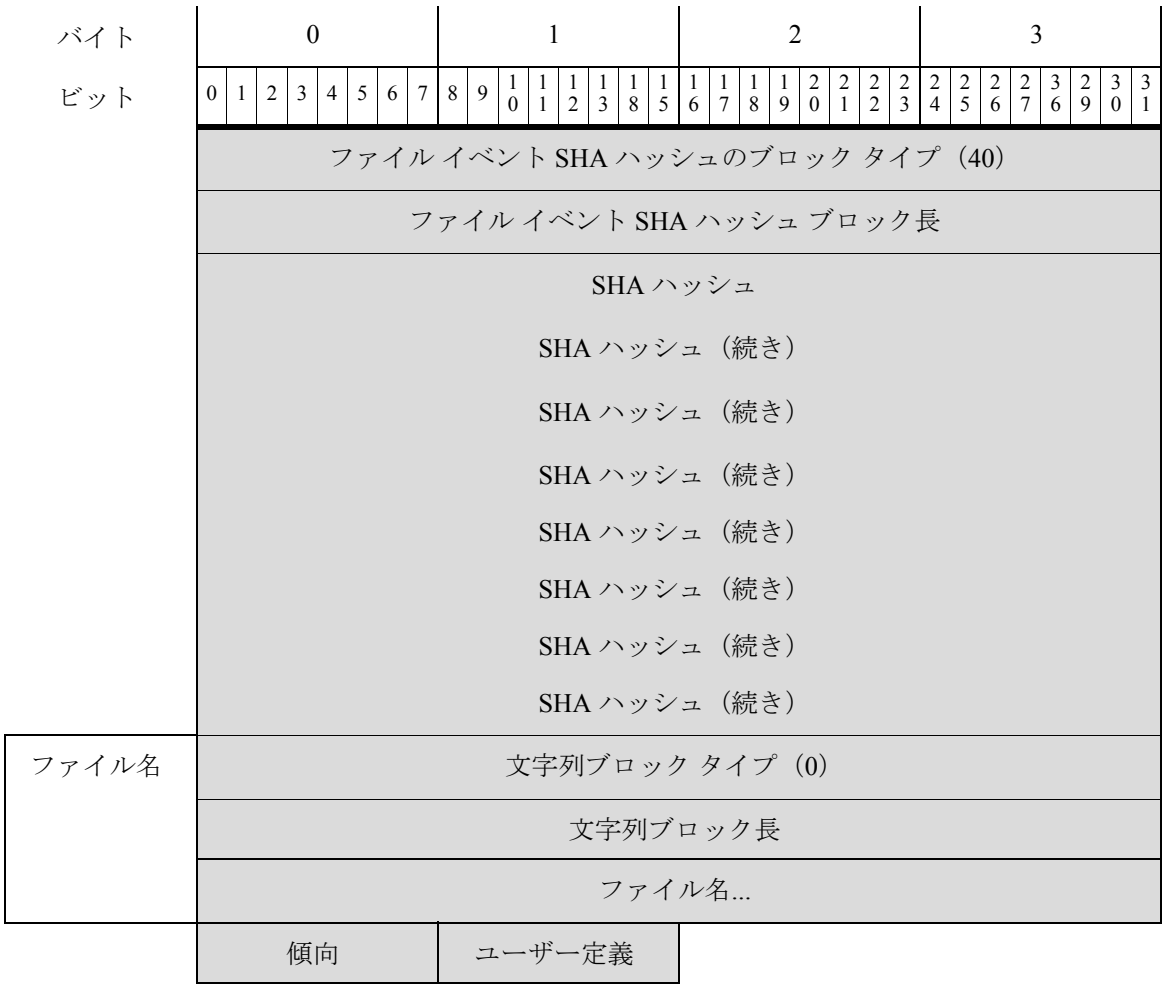
表 3-46　7.0 以上のマルウェア イベントのデータ ブロック フィールド（続き）

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。
文字列ブロック タイプ	uint32	入力 VRF 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。ブロックタイプとヘッダーフィールドの 8 バイト、および入力 VRF 名フィールドのバイト数が含まれています。
入力 VRF 名	文字列	トラフィックがネットワークに入るときに通過する仮想ルータ。
文字列ブロック タイプ	uint32	出力 VRF 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。ブロックタイプとヘッダーフィールドの 8 バイト、および出力 VRF 名フィールドのバイト数が含まれています。
出力 VRF 名	文字列	トラフィックがネットワークから出るときに通過する仮想ルータの名前。

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 3-47　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。

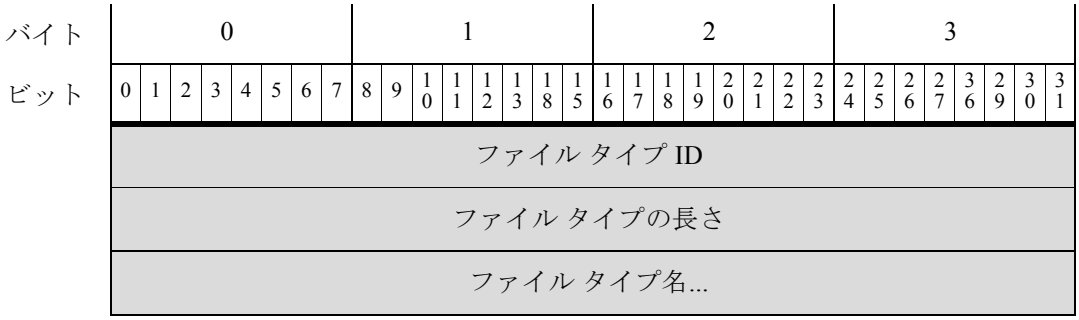
表 3-47　ファイル イベント SHA ハッシュのデータ ブロック フィールド（続き）

フィールド	データタイプ	説明
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。
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 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 AMP クラウド サービスが要求に応答しなかった。 • `5`（CUSTOM SIGNATURE）：ファイルがユーザー定義のハッシュと一致するため、ユーザーが指定した方法で処理されました。
ユーザー定義	uint8	ファイル名の表示方法を示します。 • `0`：AMP 定義 • `1`：ユーザー定義

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（2-15 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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																																



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。

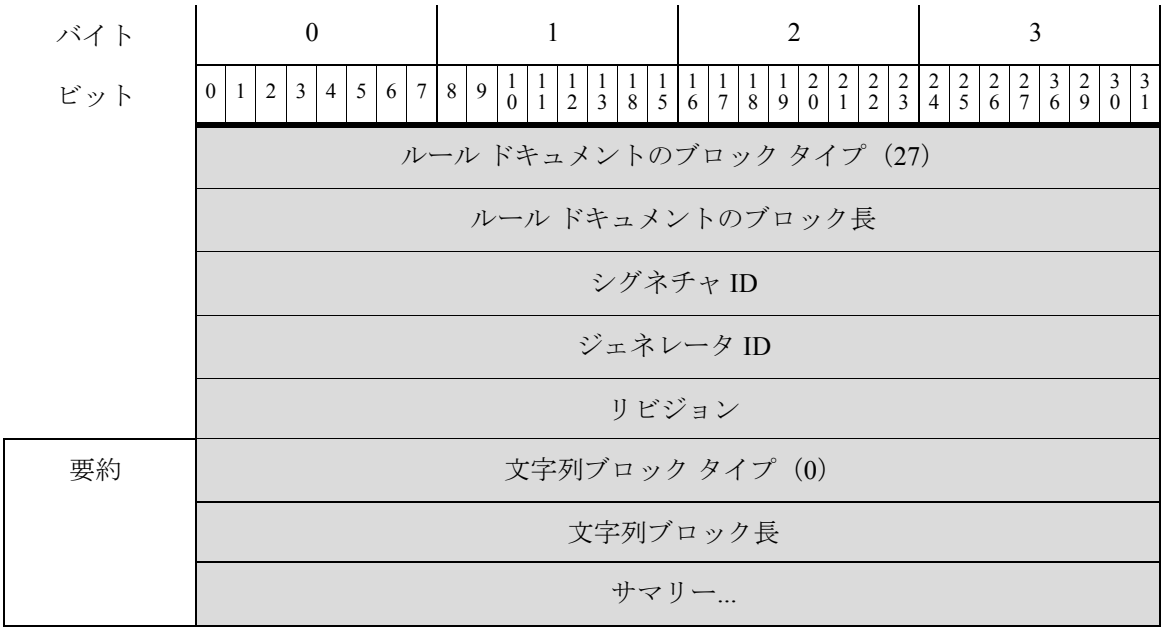
表 3-48　　ファイル タイプ ID のレコード フィールド

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。このフィールドは、このレコードの固有キーです。
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（2-30 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 3-49　　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 Cisco Secure Firewall 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。
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。

表 3-49　ルール ドキュメントのデータ ブロック フィールド（続き）

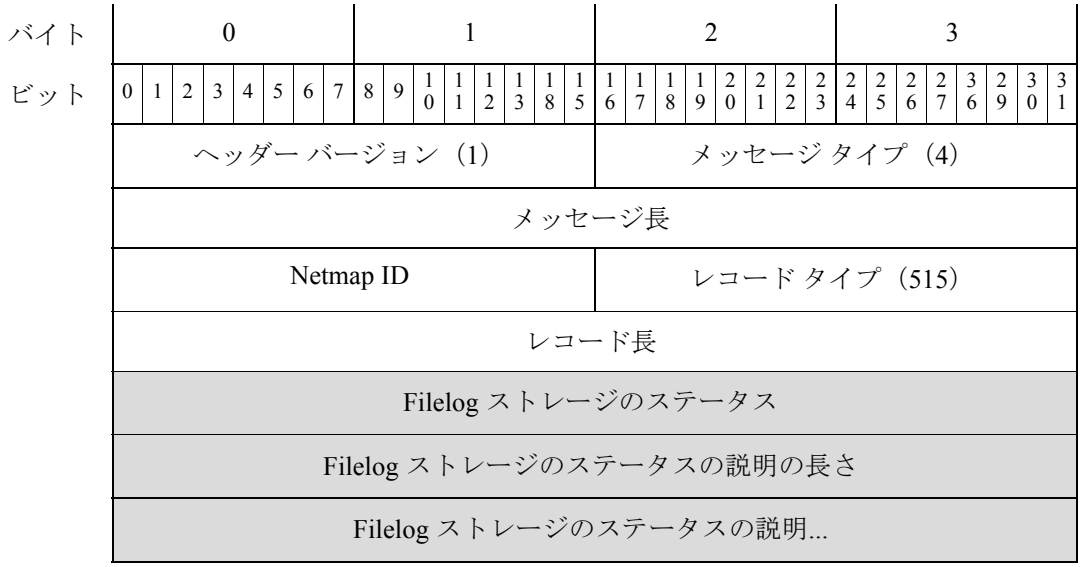
フィールド	データタイプ	説明
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと詳細情報 フィールドのバイト数が含まれます。
詳細情報	string	基礎となる脆弱性、ルールが実際に検索する内容、および影響を受けるシステムに関する情報。
文字列ブロック タイプ	uint32	ルールに関連付けられた影響を受けるシステムのリストを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バ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。
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。

表 3-49　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。



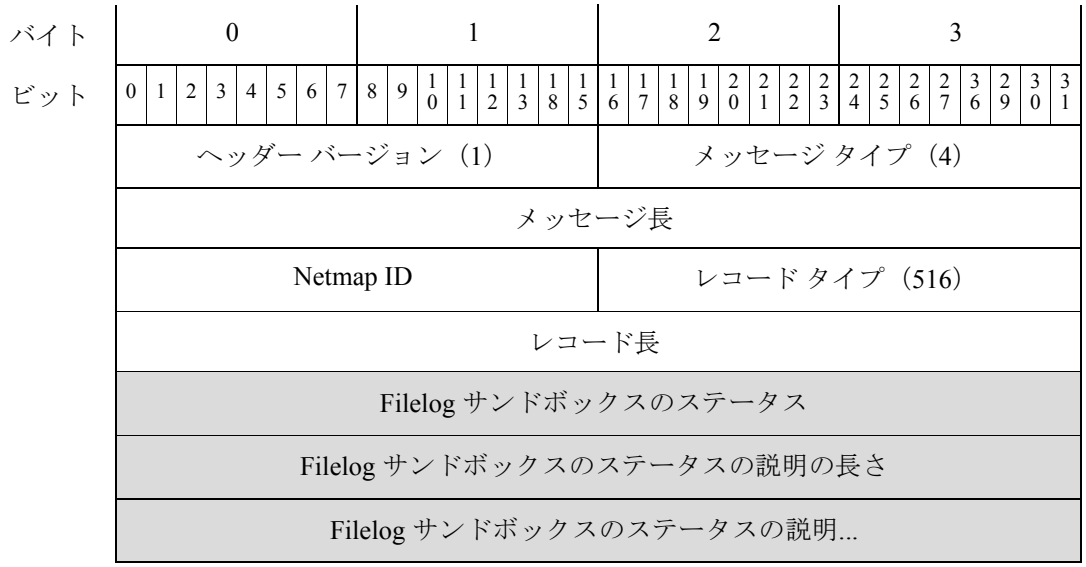
次の表は、Filelog ストレージのメタデータのレコードのフィールドについての説明です。

表 3-50　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。このフィールドは、このレコードの固有キーです。
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 3-51　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。このフィールドは、このレコードの固有キーです。
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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（517）															
レコード長																																
Filelog Spero のステータス																																
Filelog Spero のステータスの説明の長さ																																
Filelog Spero のステータスの説明...																																

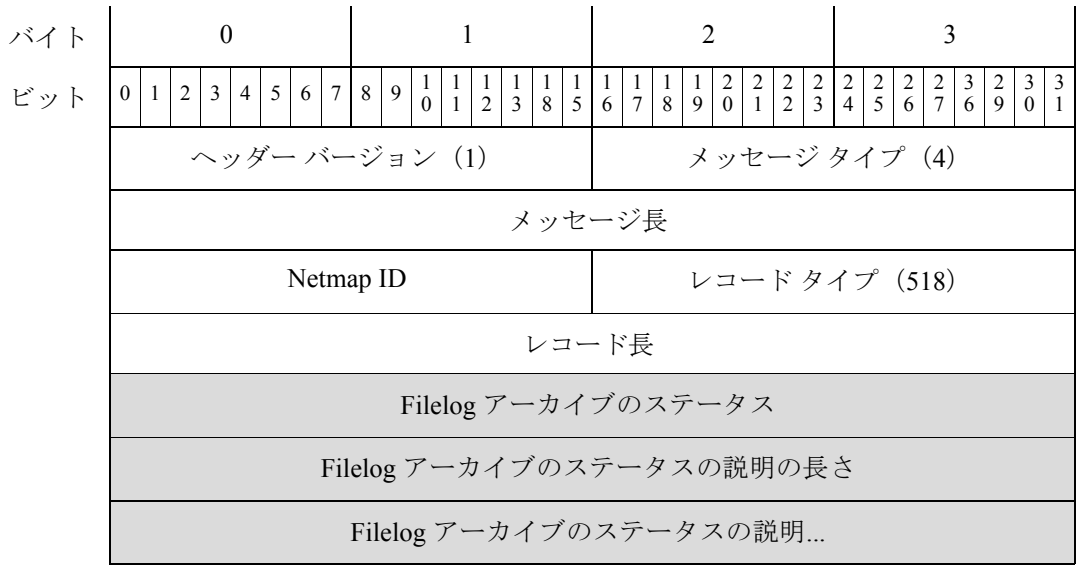
次の表は、Filelog Spero のメタデータのレコードのフィールドについての説明です。

表 3-52　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。このフィールドは、このレコードの固有キーです。
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。



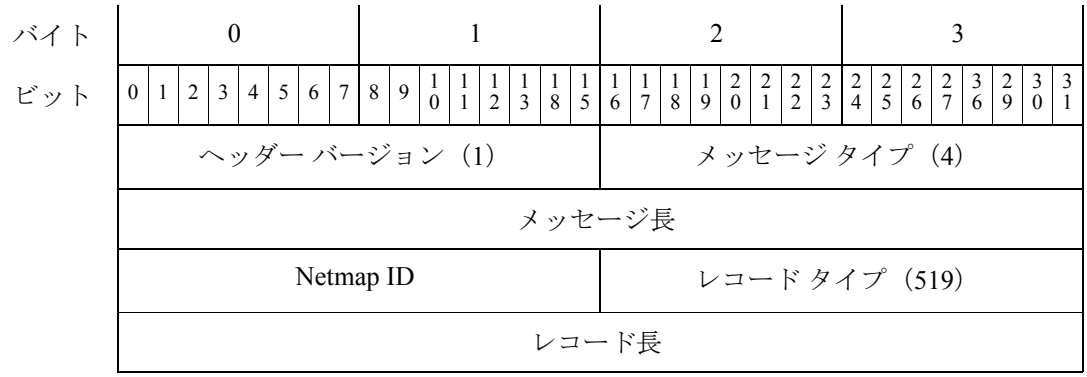
次の表は、Filelog アーカイブのメタデータのレコードのフィールドについての説明です。

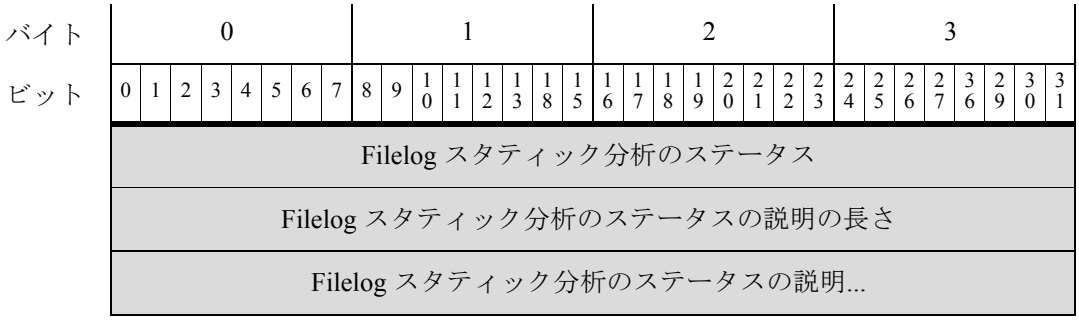
表 3-53　Filelog アーカイブのメタデータのレコード フィールド

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。このフィールドは、このレコードの固有キーです。
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。

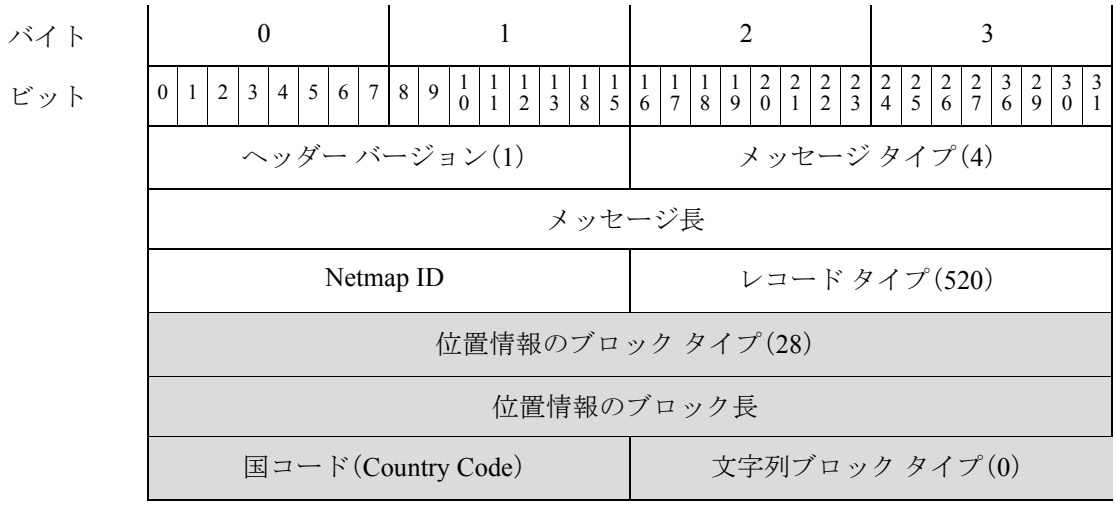
表 3-54　Filelog スタティック分析のメタデータのレコード フィールド

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。このフィールドは、このレコードの固有キーです。
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。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
国名（Country Name）	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）																国名...															

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。

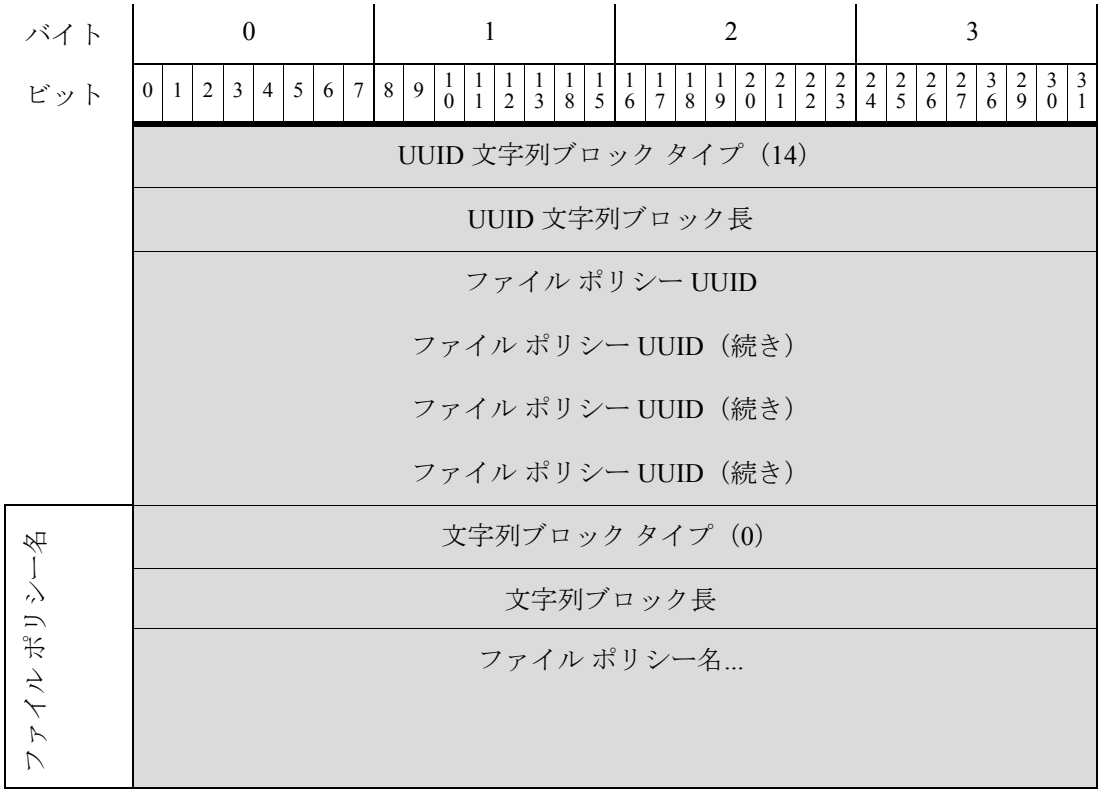
表 3-55　位置情報のデータ ブロック フィールド

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（Country Code）	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（Country Name）	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（2-15 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（530）															
レコード長																																



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 3-56　　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
UUID 文字列データ ブロック タイプ	uint32	UUID 文字列データ ブロックを開始します。この値は常に 14 です。
UUID 文字列データ ブロック長	uint32	UUID 文字列データ ブロック内の総バイト数。これには、UUID 文字列データ ブロックのタイプ フィールドおよび長さフィールド用の 8 バイトと、その後のデータのバイト数が含まれます。
ファイル ポリシー UUID	uint8[16]	ファイル ポリシーの UUID。このフィールドは、このレコードの固有キーです。
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（2-15 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 3-57　SSL ポリシー名レコード フィールド

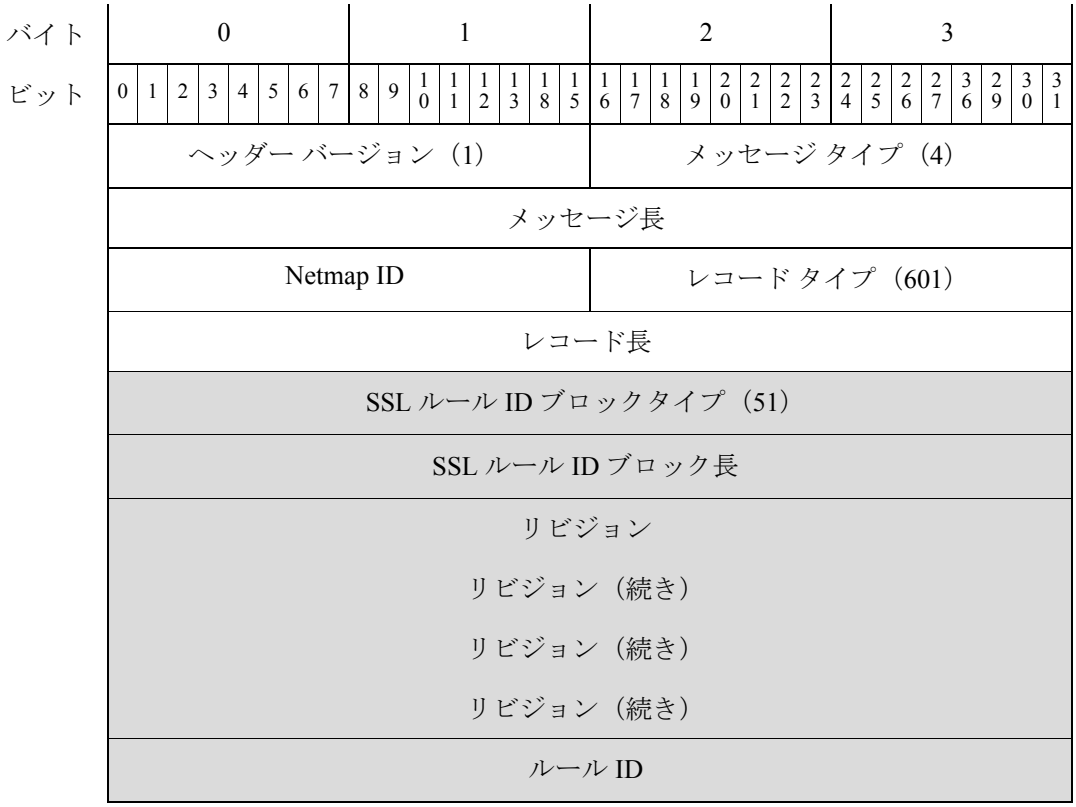
フィールド	データタイプ	説明
UUID 文字列データ ブロック タイプ	uint32	UUID 文字列データ ブロックを開始します。この値は常に 14 です。
UUID 文字列データ ブロック長	uint32	UUID 文字列データ ブロック内の総バイト数。これには、UUID 文字列データ ブロックのタイプ フィールドおよび長さフィールド用の 8 バイトと、その後のデータのバイト数が含まれます。

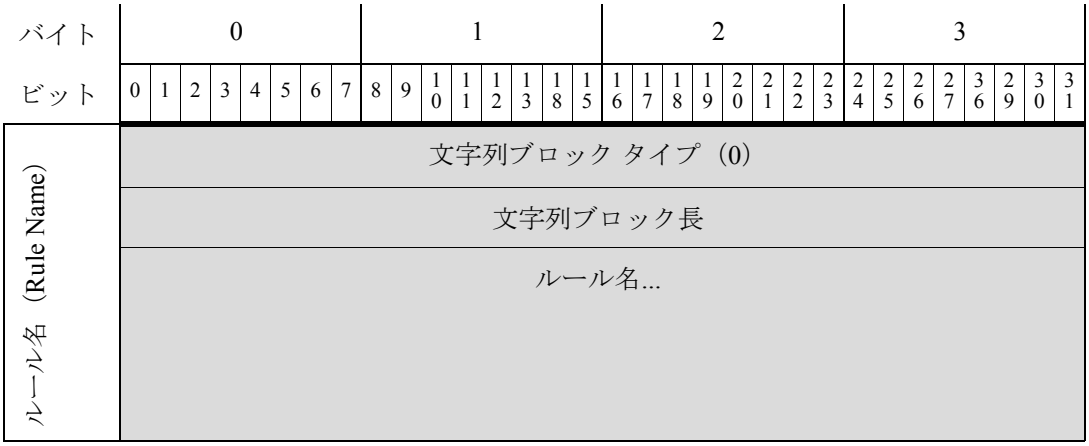
表 3-57　SSL ポリシー名レコード フィールド（続き）

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。このフィールドは、このレコードの固有キーです。
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（2-15 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。





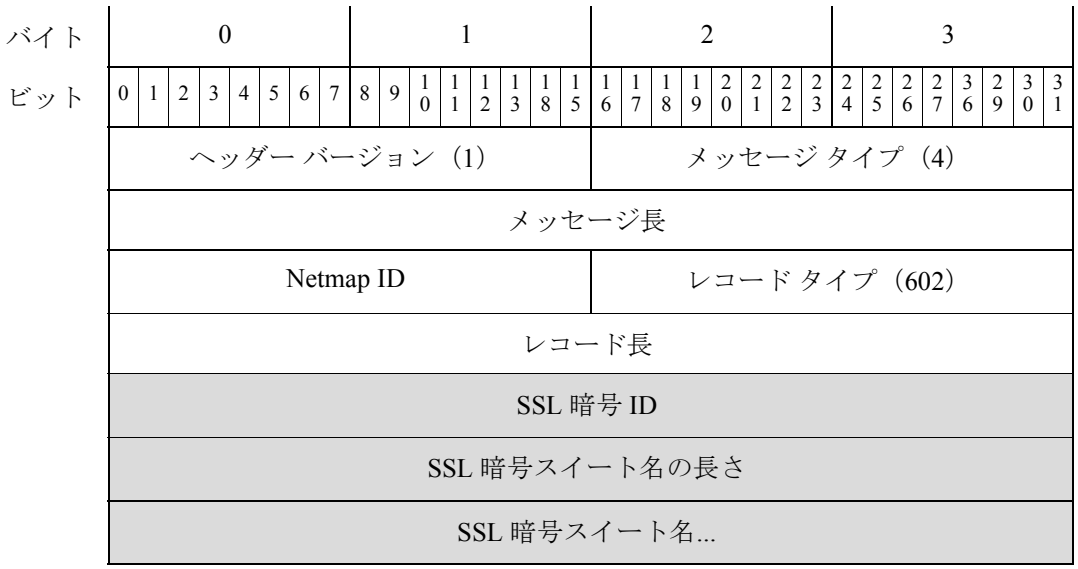
次の表は、SSL ルール ID レコードのフィールドについての説明です。

表 3-58　　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 ルール ID ブロック タイプ	uint32	SSL ルール ID データブロックのブロックタイプ。この値は常に 51 です。
SSL ルール ID ブロック長	uint32	SSL ルール ID データブロックのバイト数。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 ID ブロックのバイト数が含まれます。
リビジョン	uint8[16]	SSL ルール リビジョンの UUID。このフィールドとルール ID を組み合わせると、このレコードの固有キーとなります。
ルール ID	uint32	SSL ルール ID 番号。このフィールドとリビジョンを組み合わせると、このレコードの固有キーとなります。
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

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（2-15 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。



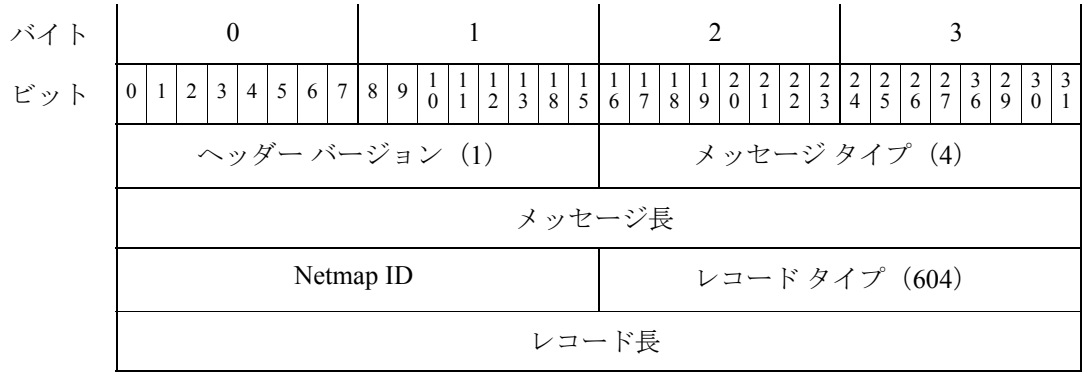
次の表は、SSL 暗号スイート レコードのフィールドについての説明です。

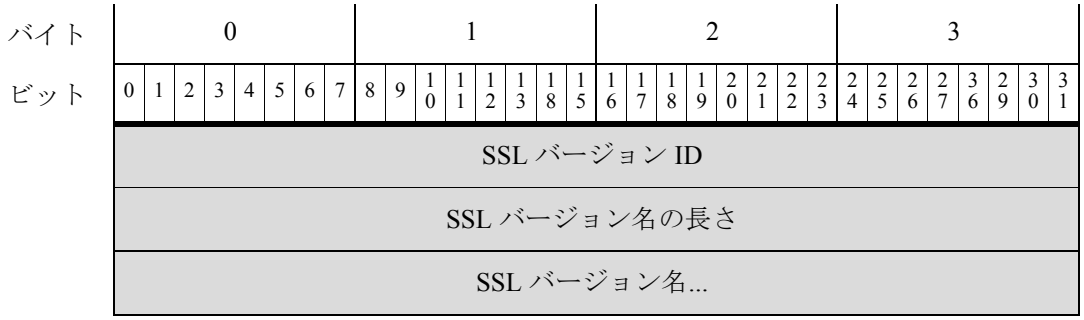
表 3-59　　SSL 暗号スイート フィールド

フィールド	データタイプ	説明
SSL 暗号 ID	uint32	SSL 暗号 ID 番号。このフィールドは、このレコードの固有キーです。
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（2-15 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。





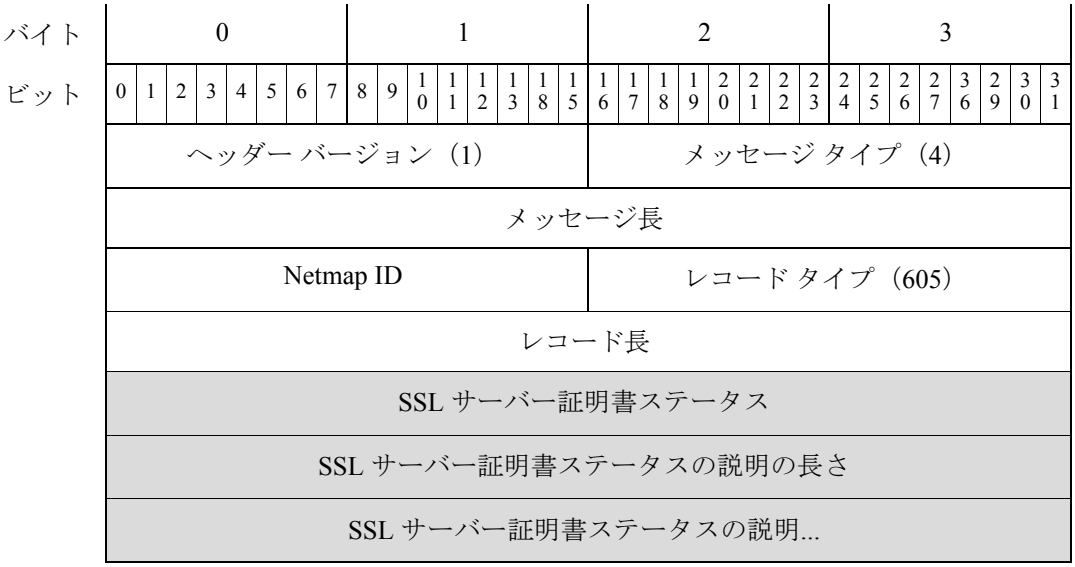
次の表は、SSL バージョン レコードのフィールドについての説明です。

表 3-60　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。このフィールドは、このレコードの固有キーです。
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 サーバー証明書ステータス

eStreamer サービスは、SSL サーバー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 サーバー証明書ステータスの情報が送信されます。要求フラグ（2-15 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 サーバー証明書ステータス レコードを示す値 605 があることに注意してください。



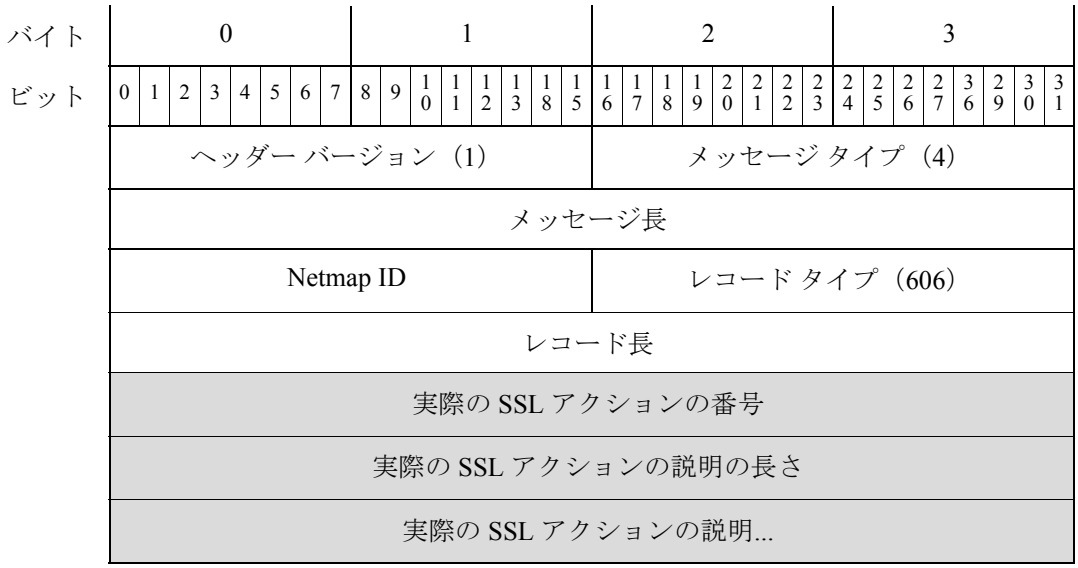
次の表は、SSL サーバー証明書ステータス レコードのフィールドについての説明です。

表 3-61　SSL サーバー証明書ステータス レコード フィールド

フィールド	データタイプ	説明
SSL サーバー証明書ステータス	uint32	SSL サーバー証明書ステータス番号。このフィールドは、このレコードの固有キーです。
SSL サーバー証明書ステータスの説明の長さ	uint32	SSL サーバー証明書ステータスの説明に含まれるバイト数。
SSL サーバー証明書ステータスの説明	string	SSL サーバー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（2-15 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 3-62　実際の SSL アクション フィールド

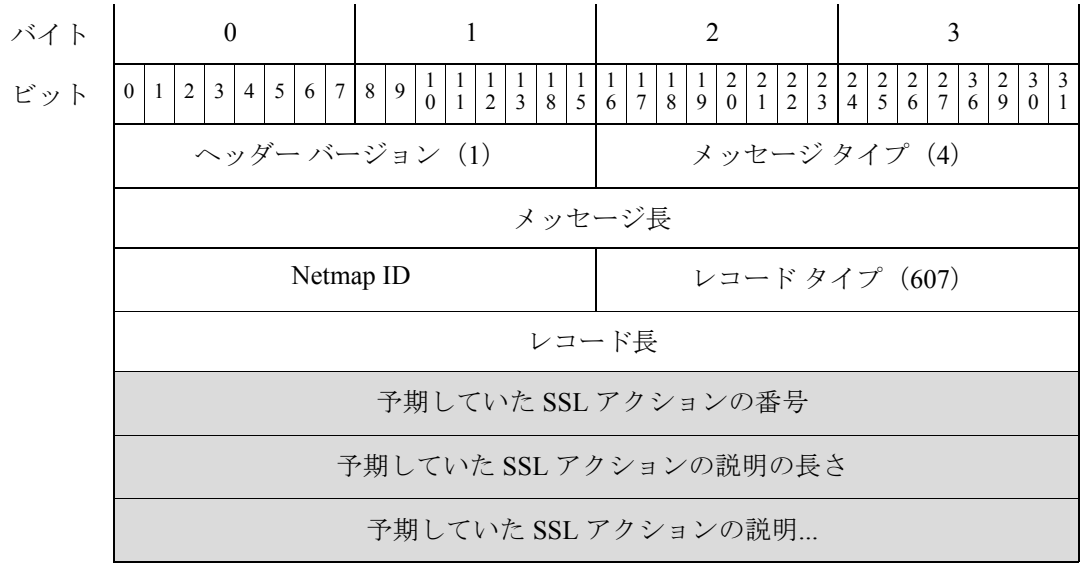
フィールド	データタイプ	説明
実際の SSL アクションの番号	uint32	実際の SSL アクションを指定する番号。このフィールドは、このレコードの固有キーです。

表 3-62　実際の SSL アクション 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（2-15 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。



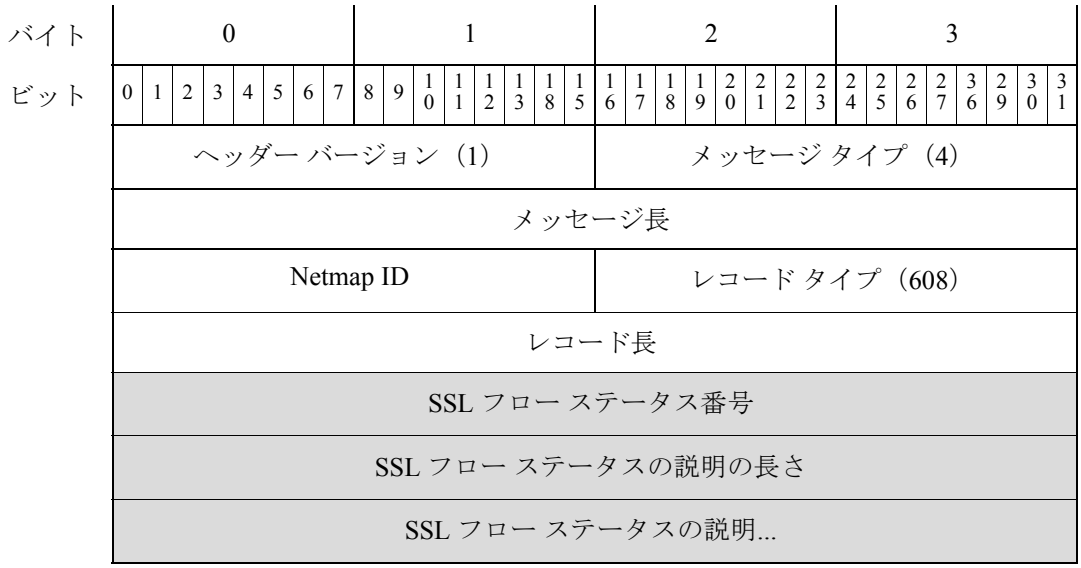
次の表は、予期していた SSL アクション レコードのフィールドについての説明です。

表 3-63　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。このフィールドは、このレコードの固有キーです。
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（2-15 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。



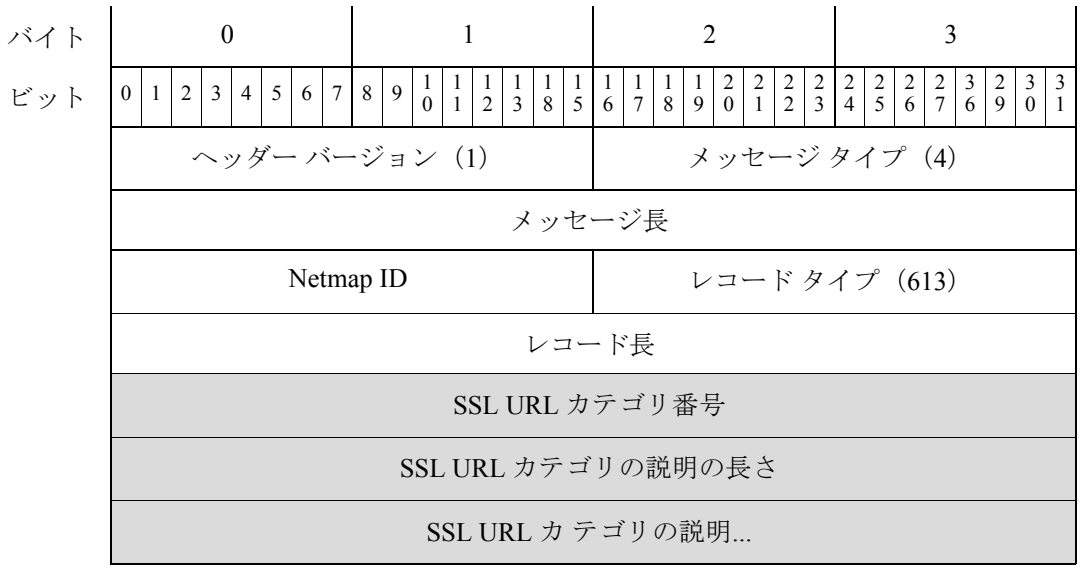
次の表は、SSL フロー ステータス レコードのフィールドについての説明です。

表 3-64　　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。このフィールドは、このレコードの固有キーです。
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（2-15 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。

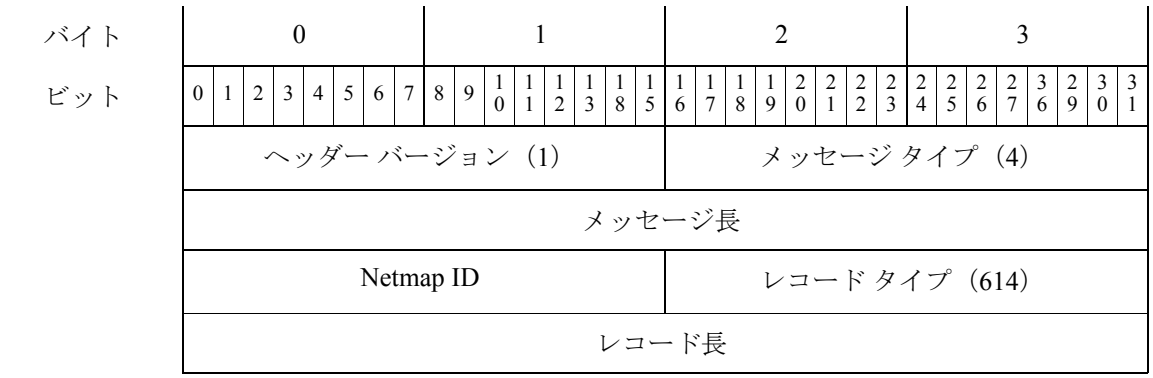
表 3-65　　SSL URL カテゴリ フィールド

フィールド	データタイプ	説明
SSL URL カテゴリ番号	uint32	SSLURLカテゴリを指定する番号。このフィールドは、このレコードの固有キーです。
SSL URL カテゴリの説明の長さ	uint32	SSLサーバー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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
		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（Serial Number） シリアル番号（続き） シリアル番号（続き） シリアル番号（続き） 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...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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...																															
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 3-66　SSL 証明書の詳細のデータ ブロック フィールド

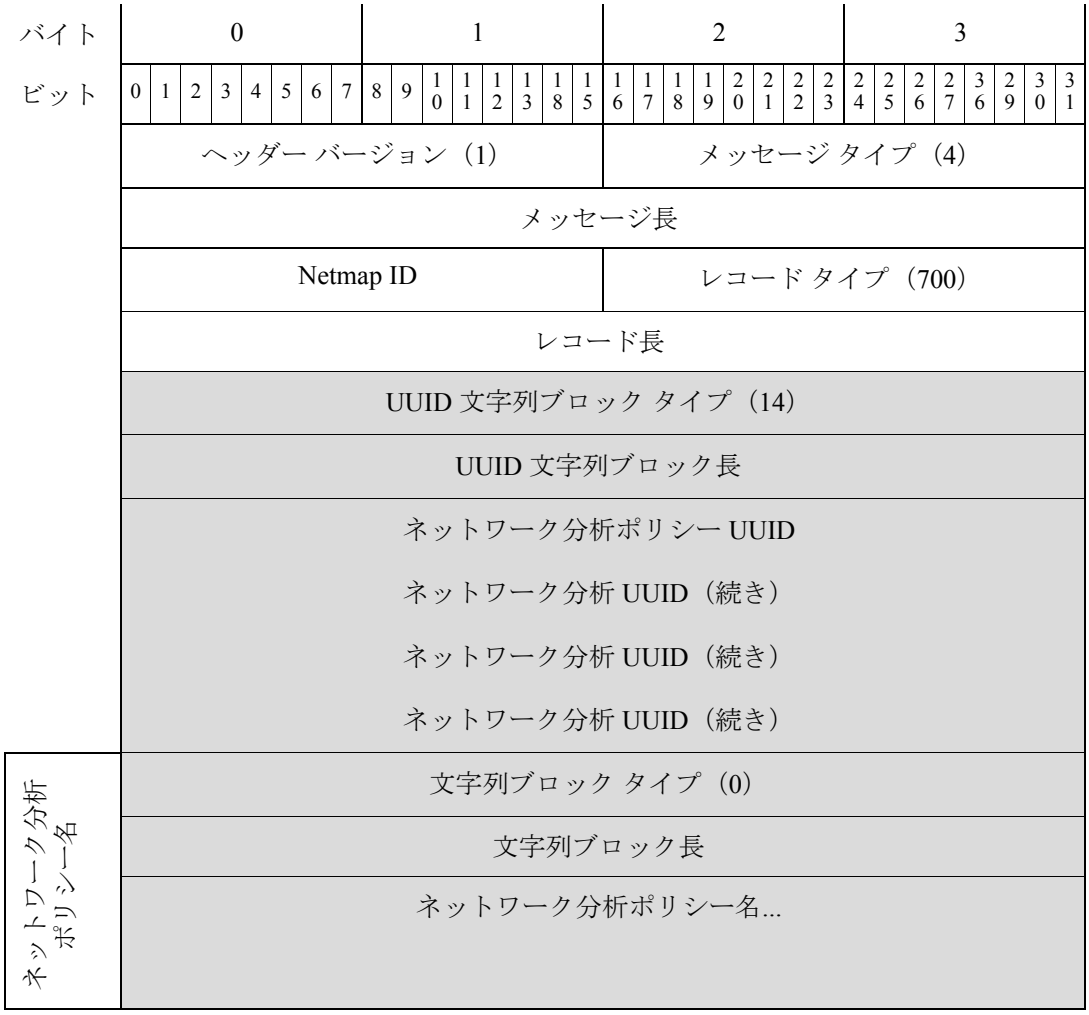
フィールド	データタイプ	説明
SSL 証明書の詳細のデータ ブロック タイプの詳細	uint32	SSL 証明書の詳細のデータ ブロックを開始します。この値は常に 50 です。
SSL 証明書の詳細のデータ ブロック長	uint32	SSL 証明書の詳細のデータ ブロックの合計バイト数です。SSL 証明書の詳細のデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
フィンガープリント SHA ハッシュ	uint8[20]	SSL サーバー証明書の SHA1 ハッシュ。
公開キーの SHA ハッシュ	uint8[20]	証明書に含まれる公開キーの認証に使用する SHA ハッシュ値。
シリアル番号（Serial Number）	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。
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。

表 3-66　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。
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（2-15 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 3-67　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
UUID 文字列データ ブロック タイプ	uint32	UUID 文字列データ ブロックを開始します。この値は常に 14 です。
UUID 文字列データ ブロック長	uint32	UUID 文字列データ ブロック内の総バイト数。これには、UUID 文字列データ ブロックのタイプ フィールドおよび長さフィールド用の 8 バイトと、その後のデータのバイト数が含まれます。
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。このフィールドは、このレコードの固有キーです。
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。

表 3-67　ネットワーク分析ポリシー名 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	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、新規ユーザーとユーザー アクティビティの検出を報告するユーザー 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 サーバー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（2-15 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（2-21 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、ユーザー 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ー ID をユーザー名に変換するなど、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+（4-42 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（4-46 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。
- イベント タイプ別のユーザー データ構造（4-63 ページ）では、eStreamer が各種ユーザー 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（4-65 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。
- ユーザー脆弱性データ ブロック 5.0+（4-169 ページ）では、複雑なユーザー 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+（4-42 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（4-66 ページ）またはユーザー脆弱性データ ブロック 5.0+（4-169 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(4-47 ページ)
11	103	1	新規 TCP サーバー	現在（Current）	サーバー メッセージ(4-48 ページ)
12	103	1	新規 UDP サーバー	現在（Current）	サーバー メッセージ(4-48 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(4-49 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(4-49 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(4-50 ページ)
16	103	1	TCP サーバー情報更新	現在（Current）	サーバー メッセージ(4-48 ページ)
17	103	1	UDP サーバー情報更新	現在（Current）	サーバー メッセージ(4-48 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(4-51 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(4-52 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(4-52 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(4-52 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(4-52 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(4-52 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(4-52 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(4-52 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(4-52 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(4-53 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...
36	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(4-53 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(4-50 ページ)
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(4-53 ページ)
34	18	1	VLAN タグ情報更新	現在（Current）	VLAN タグ情報更新メッセージ(4-54 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(4-50 ページ)
54	35	1	NetBIOS 名変更	現在（Current）	NetBIOS 名変更メッセージ(4-54 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(4-52 ページ)
45	37	1	更新バナー	現在（Current）	更新バナー メッセージ(4-55 ページ)
46	55	1	ホスト属性を追加	現在（Current）	属性メッセージ(4-59 ページ)
47	55	1	ホスト属性を更新	現在（Current）	属性メッセージ(4-59 ページ)
48	55	1	ホスト属性を削除	現在（Current）	属性メッセージ(4-59 ページ)
51	103	1	TCP サーバー信頼度更新	レガシー	サーバー メッセージ(4-48 ページ)
52	103	1	UDP サーバー信頼度更新	レガシー	サーバー メッセージ(4-48 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(4-51 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(4-9 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(4-11 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(4-14 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(4-15 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...
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（4-16 ページ）
63	該当なし	該当なし	サーバー メタデータ	現在（Current）	サービス 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-179 ページ）
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-195 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-202 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-210 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-224 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-239 ページ）
71	163	1	接続統計情報	レガシー	接続統計データブロック 6.2 ～ 6.7.x（B-274 ページ）
71	173	1	接続統計情報	レガシー	接続統計データ ブロック 7.0（B-292 ページ）
71	174	1	接続統計情報	現在（Current）	接続統計データ ブロック 7.1+（4-125 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（4-56 ページ）
74	該当なし	該当なし	ユーザー設定 OS	現在（Current）	ユーザー サーバー メッセージとオペレーティング システム メッセージ（4-60 ページ）
75	該当なし	該当なし	ユーザー設定サーバー	現在（Current）	ユーザー サーバー メッセージとオペレーティング システム メッセージ（4-60 ページ）
76	83	1	ユーザー削除プロトコル	現在（Current）	ユーザー プロトコル メッセージ（4-60 ページ）
77	60	1	ユーザー削除クライアント アプリケーション	現在（Current）	ユーザー クライアント アプリケーション メッセージ（4-61 ページ）
78	78	1	ユーザー削除アドレス	現在（Current）	ユーザー追加/削除ホスト メッセージ（4-57 ページ）
79	77	1	ユーザー削除サーバー	現在（Current）	ユーザー削除サーバー メッセージ（4-58 ページ）
80	80	1	ユーザー設定の有効な脆弱性	現在（Current）	バージョン4.6.1+ のユーザー設定脆弱性メッセージ（4-57 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...
81	80	1	ユーザー設定の無効な脆弱性	現在（Current）	バージョン4.6.1+ のユーザー設定脆弱性メッセージ(4-57 ページ)
82	81	1	ユーザー設定ホスト重要度	現在（Current）	ユーザー設定ホスト重要度メッセージ(4-58 ページ)
83	55	1	ユーザー設定属性値	現在（Current）	属性値メッセージ(4-59 ページ)
84	82	1	ユーザー削除属性値	現在（Current）	属性値メッセージ(4-59 ページ)
85	78	1	ユーザー追加ホスト	現在（Current）	ユーザー追加/削除ホスト メッセージ(4-57 ページ)
86	該当なし	該当なし	ユーザー追加サーバー	現在（Current）	ユーザー サーバー メッセージとオペレーティング システム メッセージ(4-60 ページ)
87	60	1	ユーザー追加クライアント アプリケーション	現在（Current）	ユーザー クライアント アプリケーション メッセージ(4-61 ページ)
88	83	1	ユーザー追加プロトコル	現在（Current）	ユーザー プロトコル メッセージ(4-60 ページ)
89	142	1	ユーザー追加スキャン結果	現在（Current）	スキャン結果を追加メッセージ(4-61 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	ユーザー ドロップ変更イベント	現在（Current）	ユーザー変更メッセージ(4-64 ページ)
93	120	1	ユーザー削除変更イベント	現在（Current）	ユーザー変更メッセージ(4-64 ページ)
94	120	1	新規ユーザー識別イベント	現在（Current）	ユーザー変更メッセージ(4-64 ページ)
95	121	1	ユーザー ログイン変更イベント	現在（Current）	ユーザー情報更新メッセージ ブロック(4-64 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(4-19 ページ)
98	57	2	ユーザー レコード	現在（Current）	ユーザー 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(4-62 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(4-62 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...
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（4-62 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（4-20 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（4-50 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）
114	121	1	失敗したユーザーのログイン イベント	現在（Current）	ユーザー情報更新メッセージ ブロック（4-64 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（3-33 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）
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（3-37 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（4-25 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（4-26 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（4-27 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（4-28 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（4-29 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（4-31 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（4-33 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（4-63 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（4-38 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...
162	148	1	ユーザー ホスト IOC の削除	Current	ユーザー IOC の変更データ ブロック 5.3+（4-85 ページ）
163	148	1	ユーザー ホスト IOC の有効化	Current	ユーザー IOC の変更データ ブロック 5.3+（4-85 ページ）
164	148	1	ユーザー ホスト IOC の無効化	Current	ユーザー IOC の変更データ ブロック 5.3+（4-85 ページ）
170	95	1	VPN ユーザーのログイン イベント	Current	ユーザー情報更新メッセージ ブロック（4-64 ページ）
171	95	1	VPN ユーザーのログオフ イベント	現在（Current）	ユーザー情報更新メッセージ ブロック（4-64 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（4-34 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（4-35 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。Cisco Secure Firewall 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（2-47 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（2-47 ページ）を参照してください。

ホスト ディスカバリ レコードとユーザー 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:

- フィンガープリント レコード（4-9 ページ）
- クライアント アプリケーション レコード（4-10 ページ）
- 脆弱性レコード（4-11 ページ）
- 重要度レコード（4-13 ページ）
- ネットワーク プロトコル レコード（4-14 ページ）
- 属性レコード（4-15 ページ）
- スキャン タイプ レコード（4-16 ページ）
- サービス レコード（4-16 ページ）
- ソース タイプ レコード（4-17 ページ）
- ソース アプリケーション レコード（4-18 ページ）
- ソースディテクタ レコード（4-19 ページ）
- サードパーティ スキャナの脆弱性レコード（4-20 ページ）
- ユーザー レコード（4-21 ページ）

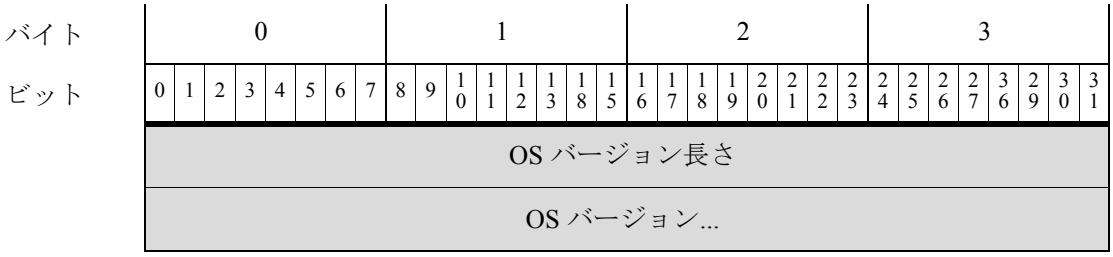
- Web アプリケーション レコード（4-22 ページ）
- 侵入ポリシー名レコード（4-23 ページ）
- アクセス コントロール ルール アクション レコード メタデータ（4-25 ページ）
- URL カテゴリ レコード メタデータ（4-26 ページ）
- URL レピュテーション レコード メタデータ（4-27 ページ）
- アクセス コントロール ルール理由メタデータ（4-28 ページ）
- セキュリティ インテリジェンス カテゴリ メタデータ（4-34 ページ）
- セキュリティ インテリジェンス送信元/宛先レコード（4-35 ページ）

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（2-15 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（54）															
	レコード長																															
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）																															
	OS 名長さ																															
	OS 名...																															
	OS ベンダー長さ																															
	OS ベンダー...																															



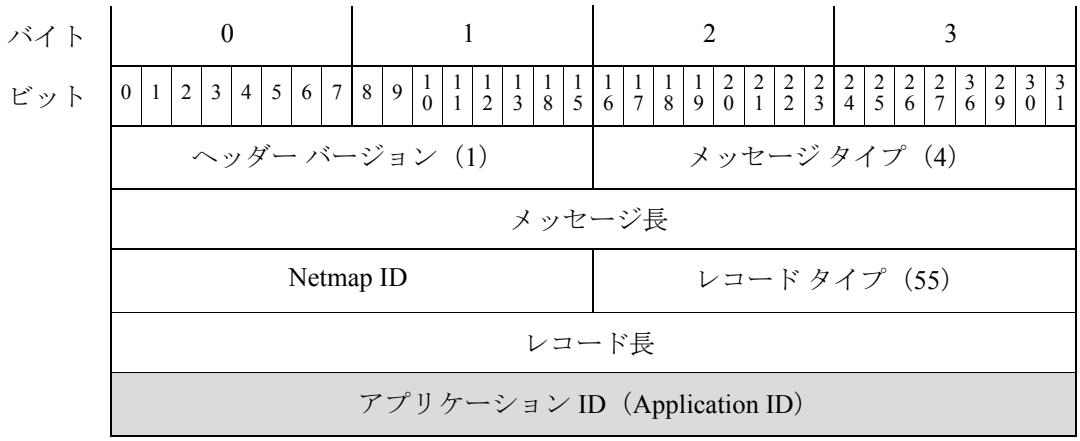
次の表では、フィンガープリント レコードのフィールドについて説明します。

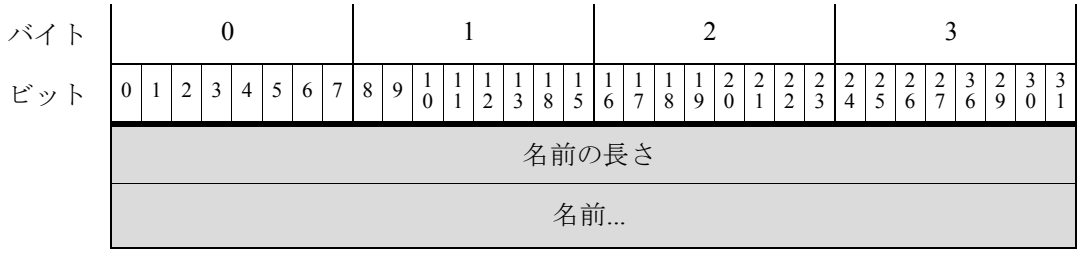
表 4-2　フィンガープリント レコードのフィールド

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。このフィールドは、このレコードの固有キーです。
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（2-15 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。





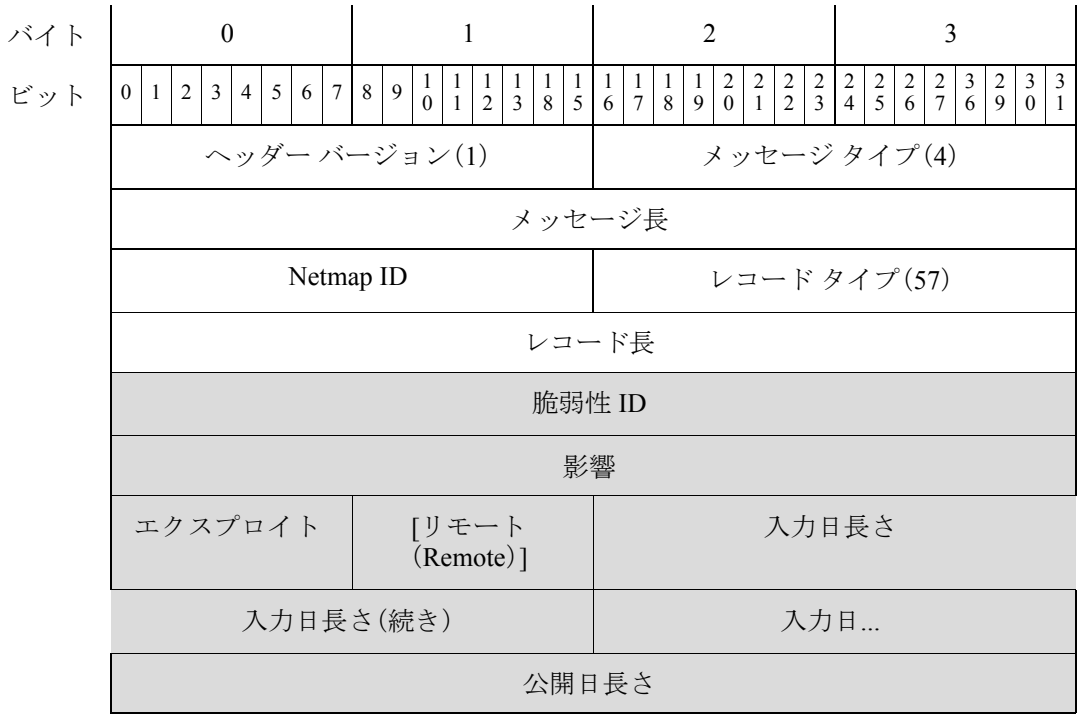
次の表では、クライアント アプリケーション レコードのフィールドについて説明します。

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（Application 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。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	名前に含まれるバイト数。
[名前（Name）]	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（2-15 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。



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

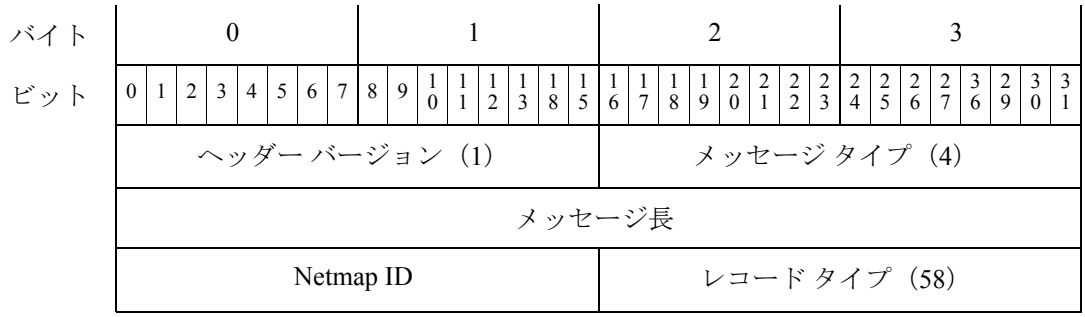
フィールド	データタイプ	説明
脆弱性 ID	uint32	脆弱性 ID 番号このフィールドは、このレコードの固有キーです。
影響	uint32	侵入データ、ホスト ディスカバリ イベント、脆弱性アセスメント間の相関に基づいて決定した影響レベルに対応した、脆弱性の影響。ここに設定可能な値の範囲は 1 ～ 10 です。最も深刻な場合で 10 です。脆弱性の影響度の値は、Bugtraq エントリの作成者が設定します。
エクスプロイト	uint8	脆弱性に既知のエクスプロイトがあるかどうかを示します。有効な値は次のとおりです。 • 0:はい • 1:いいえ

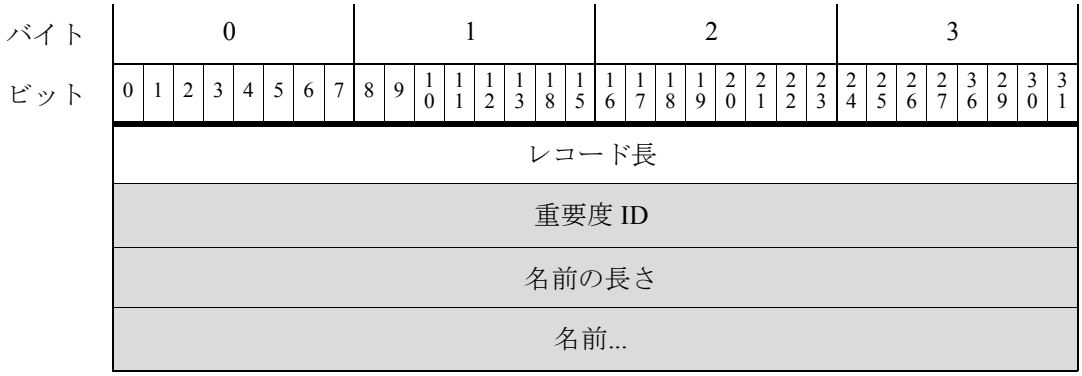
表 4-4　脆弱性レコードのフィールド（続き）

フィールド	データタイプ	説明
[リモート(Remote)]	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。
役職(Title)	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(2-15 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。





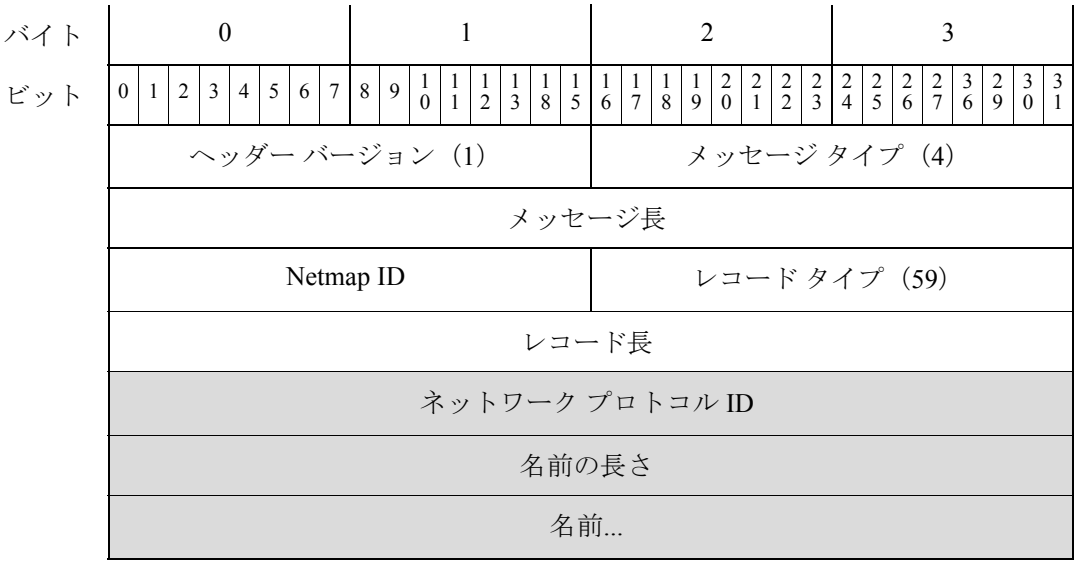
次の表では、重要度レコードのフィールドについて説明します。

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。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	重要度レベルのバイト数。
[名前（Name）]	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（2-15 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。



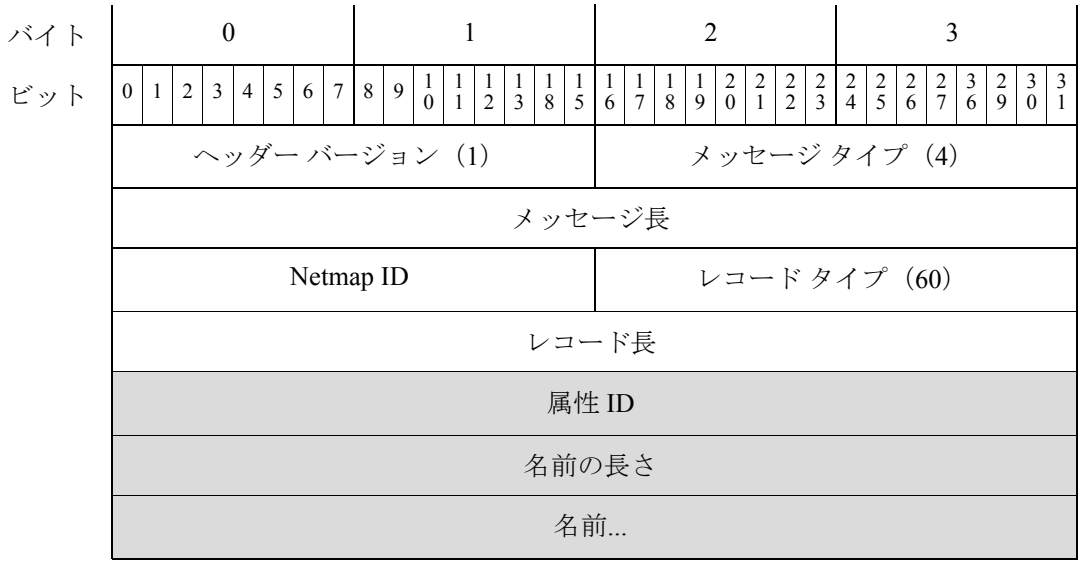
次の表では、ネットワーク プロトコル レコードのフィールドについて解説します。

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。このフィールドは、このレコードの固有キーです。
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(Name)]	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(2-15 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。



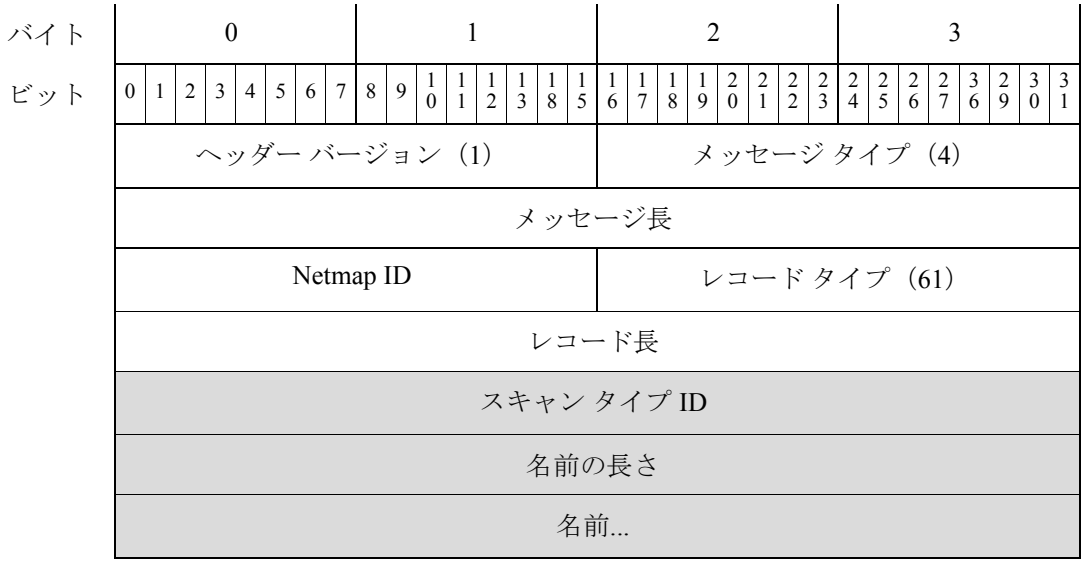
次の表では、属性レコードのフィールドについて説明します。

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
Attribute ID	uint32	属性 ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	属性名のバイト数。
[名前(Name)]	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 (2-15 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。



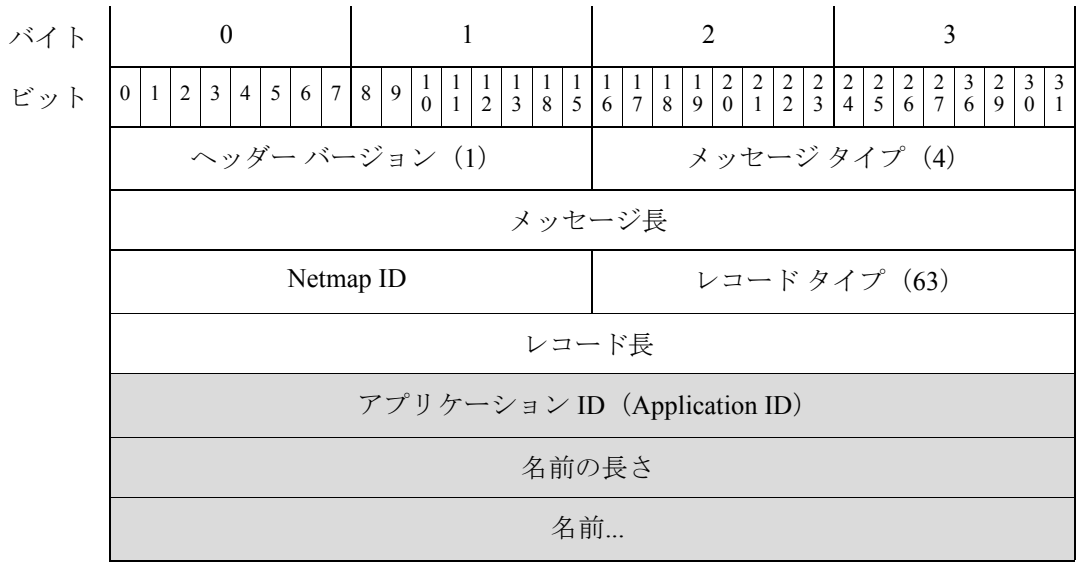
次の表では、スキャン タイプ レコードのフィールドについて説明します。

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。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	スキャン タイプ名のバイト数。
[名前(Name)]	string	スキャン タイプ名。

サービス レコード

eStreamer サービスは、次の形式のサービス レコードで、イベントのサービス情報を格納したメタデータを送信します。サービス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。(サービス情報は、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 (2-15 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、サービス レコードを示す 63 です。



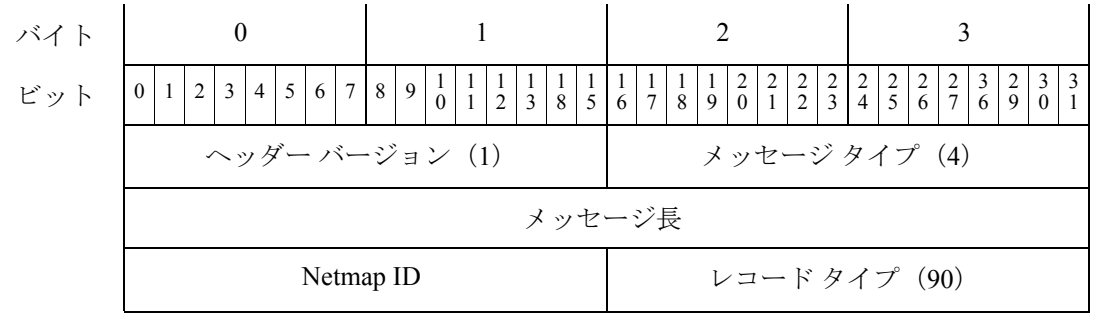
次の表では、サービス レコードのフィールドについて説明します。

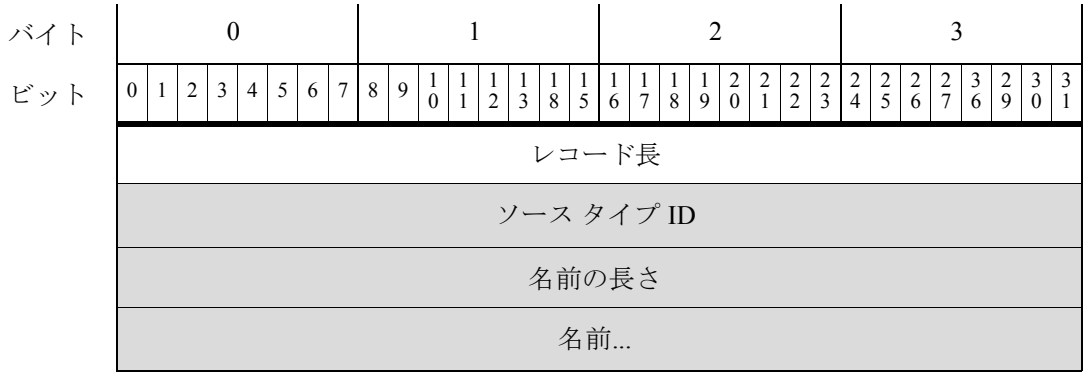
表 4-9　　サービス レコードのフィールド

フィールド	データタイプ	説明
アプリケーション ID（Application 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。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	サービス名に含まれるバイト数。
[名前（Name）]	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（2-15 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。





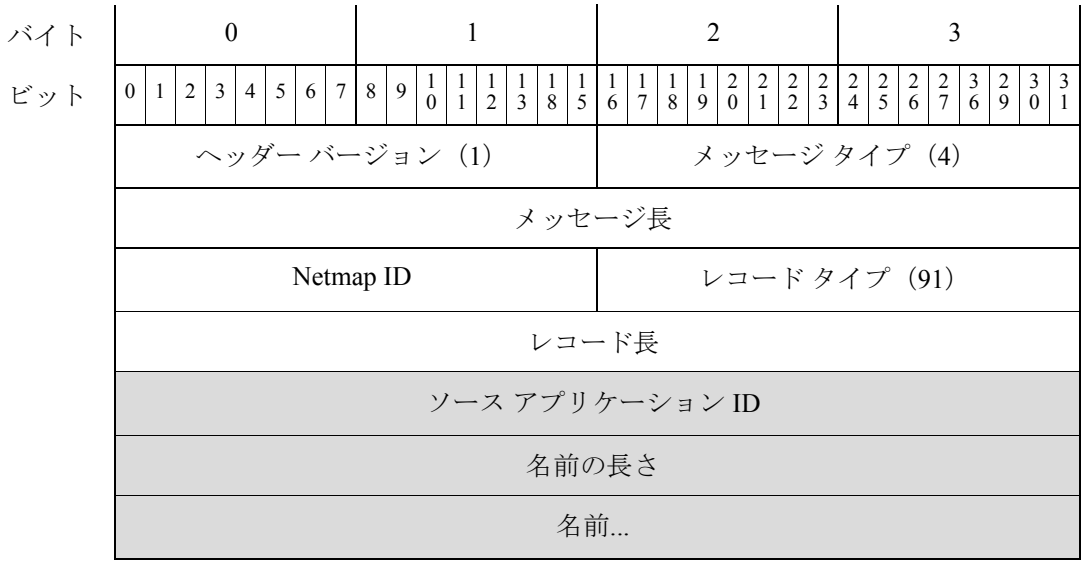
次の表では、ソース タイプ レコードのフィールドについて説明します。

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。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	送信元タイプ名のバイト数。
[名前（Name）]	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（2-15 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。



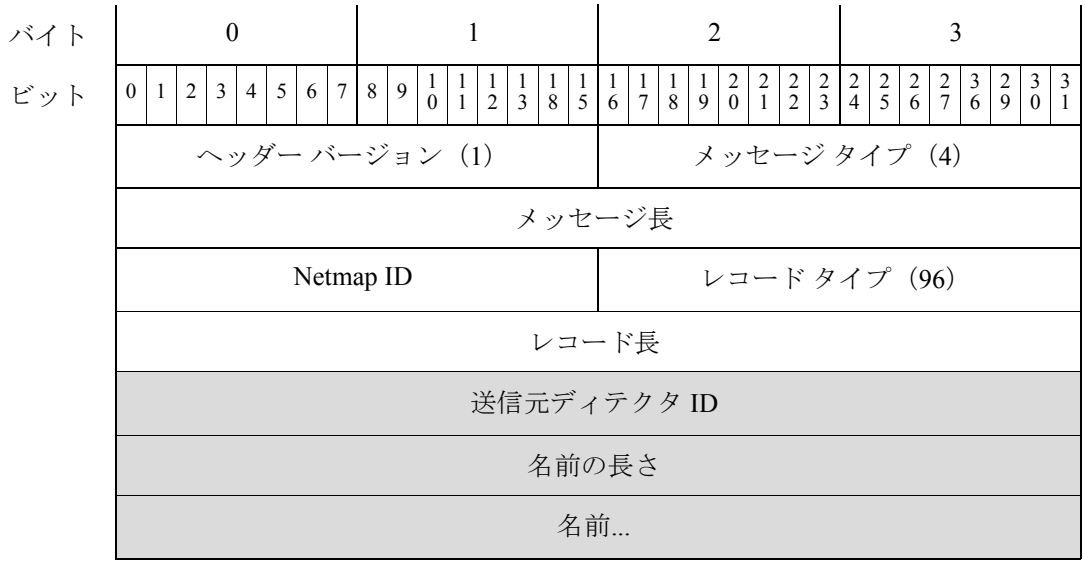
次の表では、ソース アプリケーション レコードのフィールドについて説明します。

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。このフィールドは、このレコードの固有キーです。
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(Name)]	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(2-15 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。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	送信元タイプ名のバイト数。
[名前(Name)]	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、サードパーティ スキャナ脆弱性レコード内の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以下の形式で送信します。(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(2-15 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。このフィールドとスキャナ タイプを合わせると、このレコードの固有キーとなります。
スキャナ タイプ	uint32	サードパーティ スキャナ タイプ。このフィールドと脆弱性 ID を合わせると、このレコードの固有キーとなります。
タイトル長さ	uint32	タイトル フィールド長さ。

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（続き）

フィールド	データタイプ	説明
役職（Title）	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

ユーザー レコード

eStreamer サービスは、次の形式のユーザー レコードで、システムが検出したユーザー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、ユーザー情報が送信されます。要求フラグ（2-15 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、ユーザー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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																																
ユーザー データ ブロック タイプ（57）																																
ユーザー データ ブロック長																																
ユーザー ID（User 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																																
ユーザー名...																																

次の表は、ユーザー レコードのフィールドについての説明です。

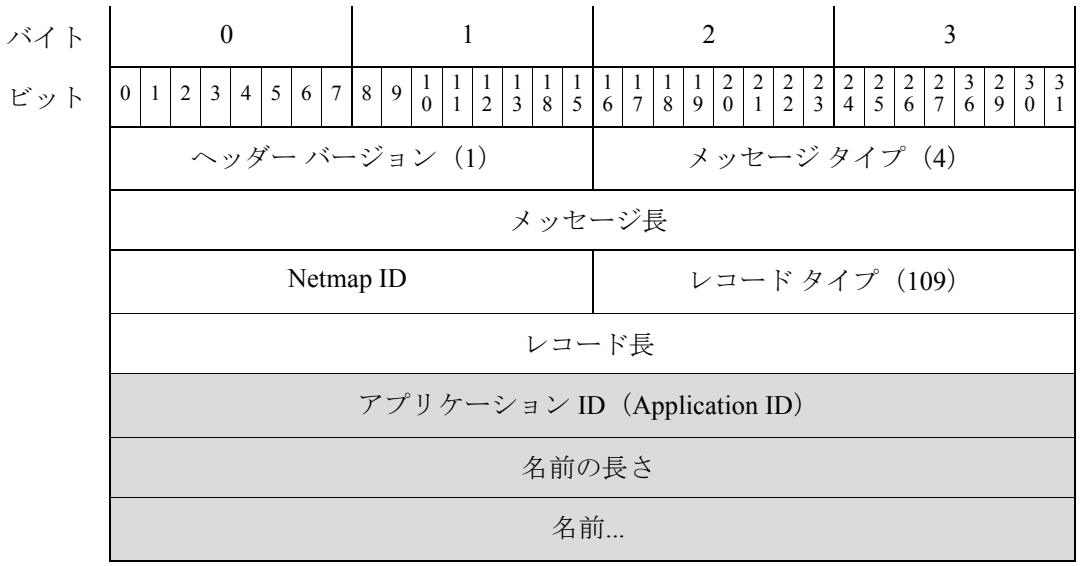
表 4-14　ユーザー レコードのフィールド

フィールド	データタイプ	説明
ユーザー データ ブロック タイプ	uint32	ユーザー 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。
ユーザー 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。
ユーザー ID（User ID）	uint32	ユーザーの固有識別情報。このフィールドは、このレコードの固有キーです。
プロトコル	uint32	ユーザー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 フィールドとヘッダー フィールドの 8 バイトにユーザー名フィールドのバイト数を加えたユーザー名文字列データ ブロックのバイト数。
[ユーザー名（Username）]	string	ユーザーの名前

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（2-15 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。



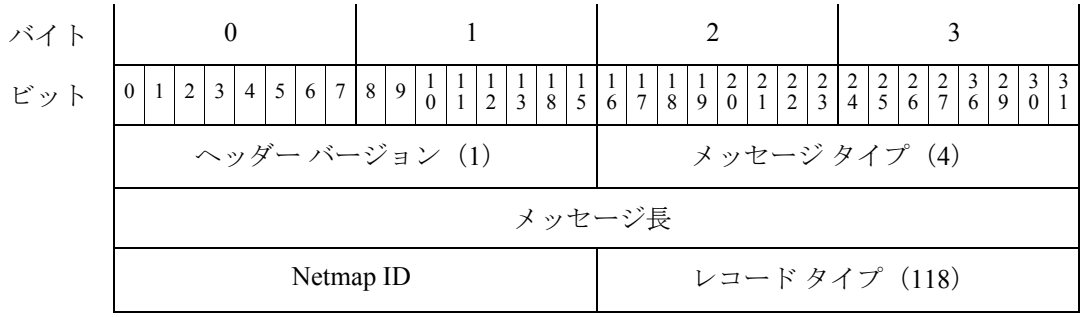
次の表では、Web アプリケーション レコードのフィールドについて説明します。

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。このフィールドは、このレコードの固有キーです。
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(2-15 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。



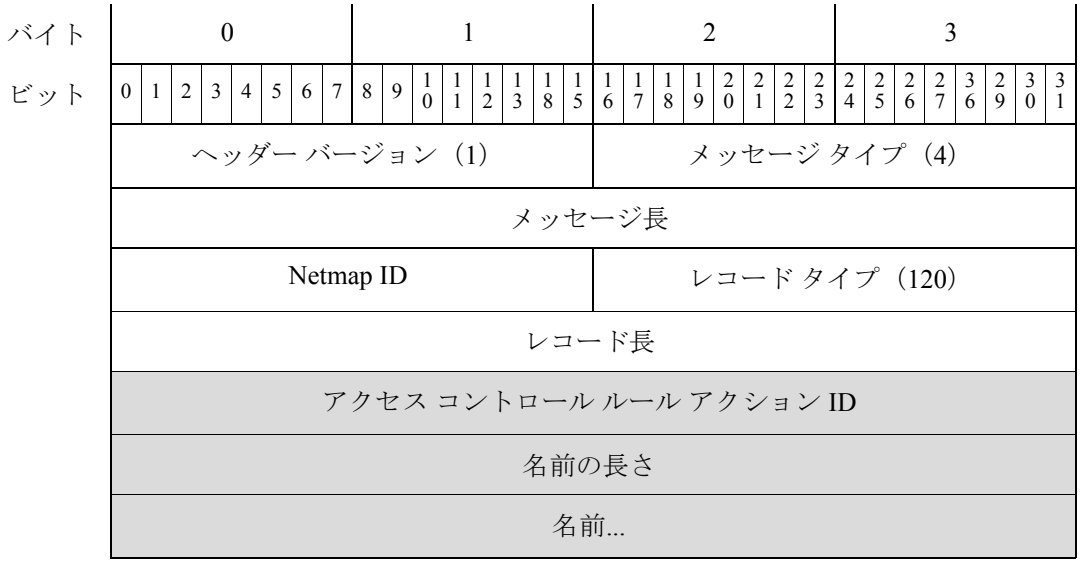
次の表では、侵入ポリシー名データ ブロックのフィールドについて説明します。

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。このフィールドは、このレコードの固有キーです。
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 (2-15 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

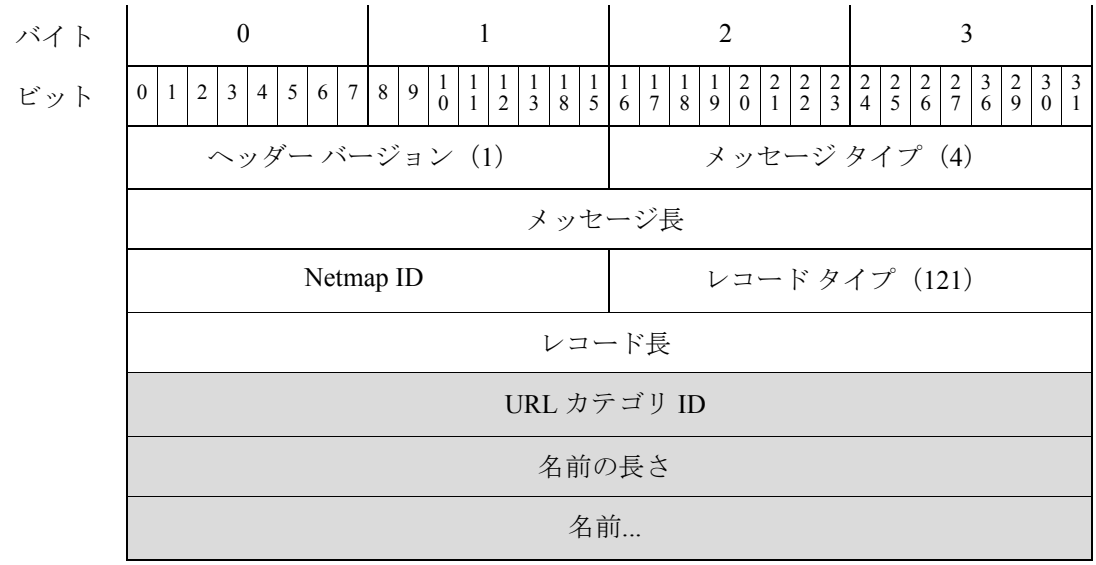
フィールド	データタイプ	説明
アクセス コントロール ルール アクション ID	uint32	アクセス コントロール ルール アクションの ID 番号。このフィールドは、このレコードの固有キーです。

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（続き）

フィールド	データタイプ	説明
名前の長さ	uint32	名前に含まれるバイト数。
[名前(Name)]	string	ファイアウォール ルール アクション名。 有効な値は次のとおりです。 • 1:「保留中」 • 2:「許可」 • 3:「信頼」 • 4:「ブロック」 • 5:「リセットしてブロック」 • 6:「モニター」 • 7:「インタラクティブブロック」 • 8:「リセット付きインタラクティブブロック」 • 14:「FastPath」 • 22:「ドメインが見つかりません」 • 23:「シンクホール」

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 (2-15 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。



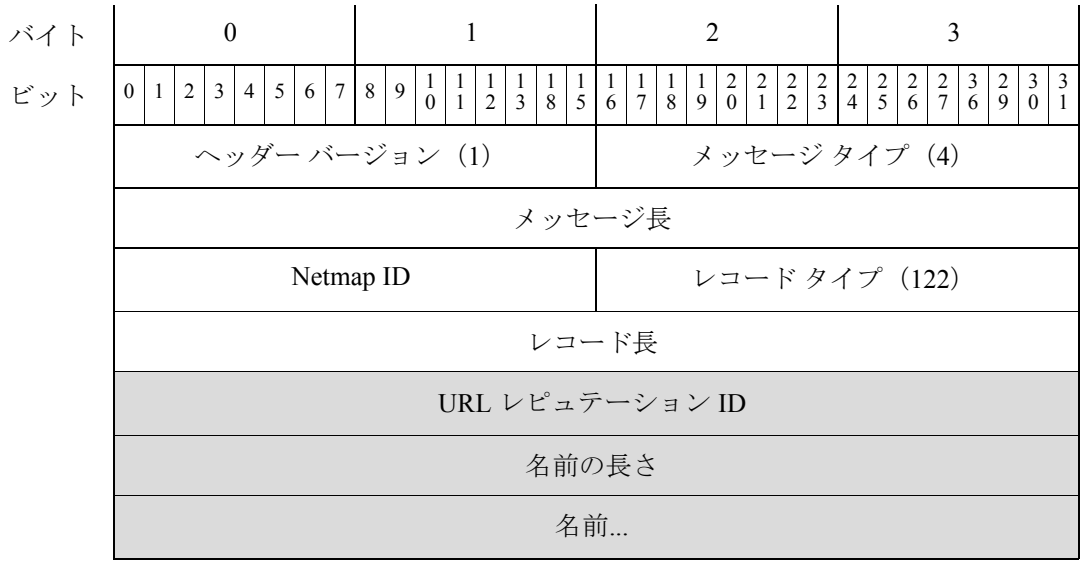
次の表では、URL カテゴリ レコードのフィールドについて説明します。

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。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	名前に含まれるバイト数。
[名前（Name）]	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（2-15 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。



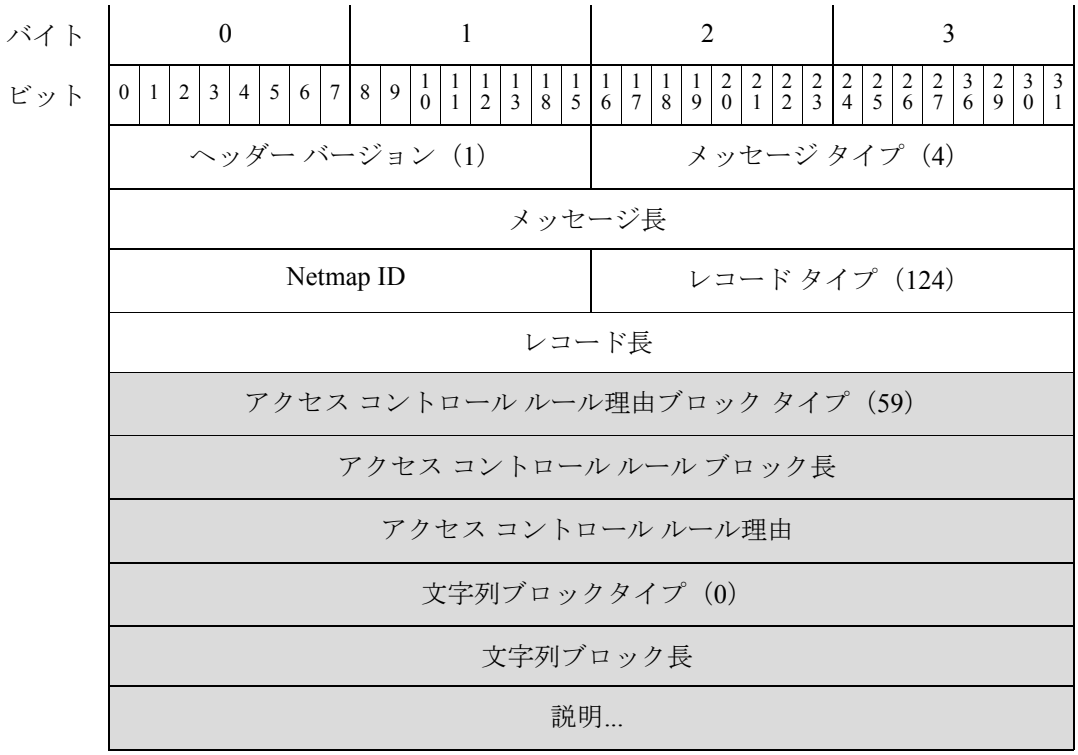
次の表では、URL レピュテーション レコードのフィールドについて説明します。

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。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	名前に含まれるバイト数。
[名前（Name）]	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（2-15 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 6.0+（4-214 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 59 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 59 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。

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（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	uint32	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。このフィールドは、このレコードの固有キーです。 イベントをトリガーしたルールの理由の番号。 ルールの理由は、複数のビットを設定できるバイナリ ビットマップです。ルールには、複数の理由がある場合があります。ビット値は次のとおりです。 • **1**：IP ブロック • **2**：IP モニター • **4**：ユーザー バイパス • **8**：ファイル モニター • **16**：ファイル ブロック • **32**：侵入モニター • **64**：侵入ブロック • **128**：ファイル再開ブロック • **256**：ファイル再開許可 • **512**：ファイルカスタム検出 • **1024**：SSL ブロック • **2048**：DNS ブロック • **4096**：DNS モニター • **8192**：URL ブロック • **16384**：URL モニター • **32768**：コンテンツ制約 • **65536**：インテリジェント アプリケーション バイパス • **131072**：WSA 脅威
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（2-15 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+ (4-218 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（145）															
	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（Sensor 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 ポリシー データ ブロックのフィールドについて説明します。

表 4-21　アクセス コントロール ポリシー メタデータのフィールド

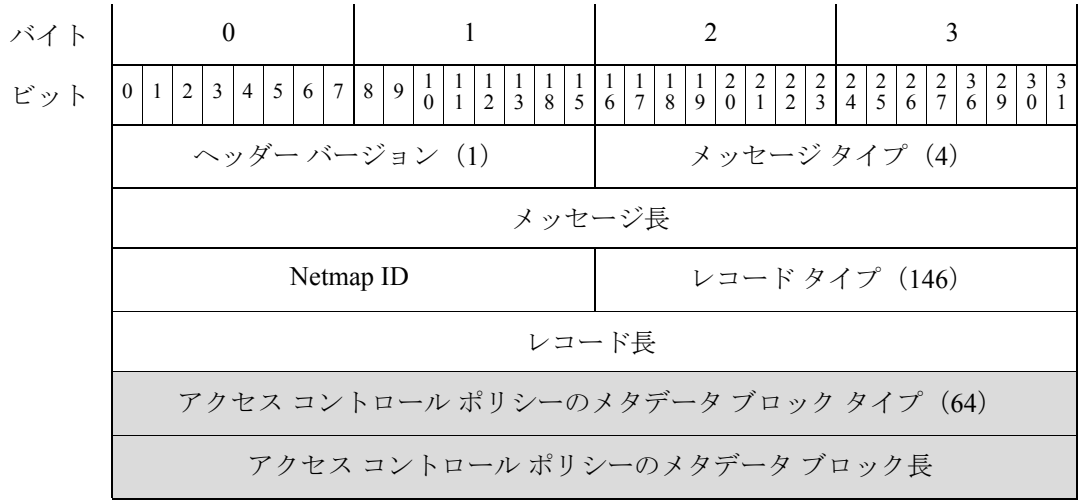
フィールド	データタイプ	説明
アクセス コントロール ポリシーのメタデータ ブロック タイプ	uint32	アクセス コントロール ポリシー メタデータ ブロックを開始します。この値は常に 64 です。これはシリーズ 2 のデータ ブロックです。
アクセス コントロール ポリシーのメタデータ ブロック長	uint32	アクセス コントロール ポリシーのメタデータ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ポリシー メタデータ ブロックの合計バイト数。

表 4-21　アクセス コントロール ポリシー メタデータのフィールド（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 ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの UUID。このフィールドは、このレコードの固有キーです。
センサー ID（Sensor 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。このフィールドは、このレコードの固有キーです。
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（Name）]	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（2-15 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+（4-218 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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（Sensor 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...																															

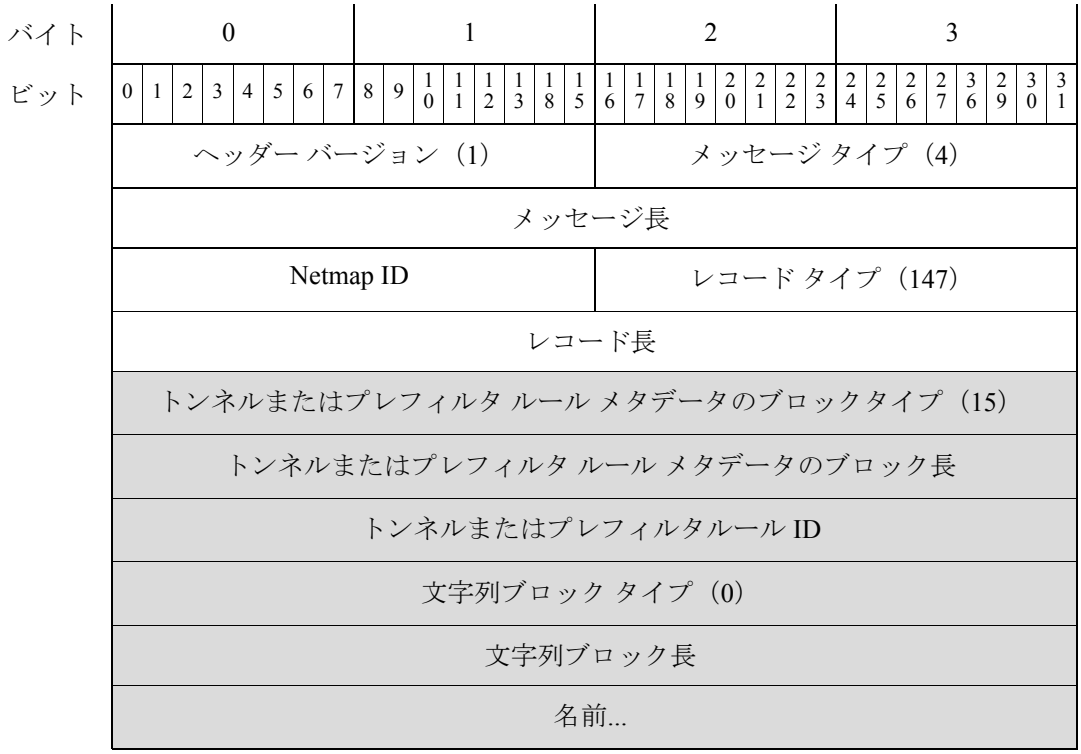
次の表では、プレフィルタ ポリシー メタデータ ブロックのフィールドについて説明します。

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
プレフィルタ ポリシー ブロック タイプ	uint32	プレフィルタ ポリシー 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。
プレフィルタ ポリシー ブロック長	uint32	プレフィルタ ポリシー 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、後続のデータのバイト数を加えたプレフィルタ ポリシー 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。このフィールドとセンサー ID を合わせると、このレコードの固有キーとなります。
センサー ID（Sensor 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。このフィールドとアクセス コントロール ポリシー UUID を合わせると、このレコードの固有キーになります。
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（Name）]	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（2-15 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（4-212 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 59 です。



次の表は、トンネルまたはプレフィルタ ルール 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 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
トンネルまたはプレフィルタルールのブロックタイプ	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。
トンネルまたはプレフィルタルールのブロック長	uint32	トンネルまたはプレフィルタ 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、後続のデータのバイト数を加えたトンネルまたはプレフィルタルールブロックの合計バイト数。

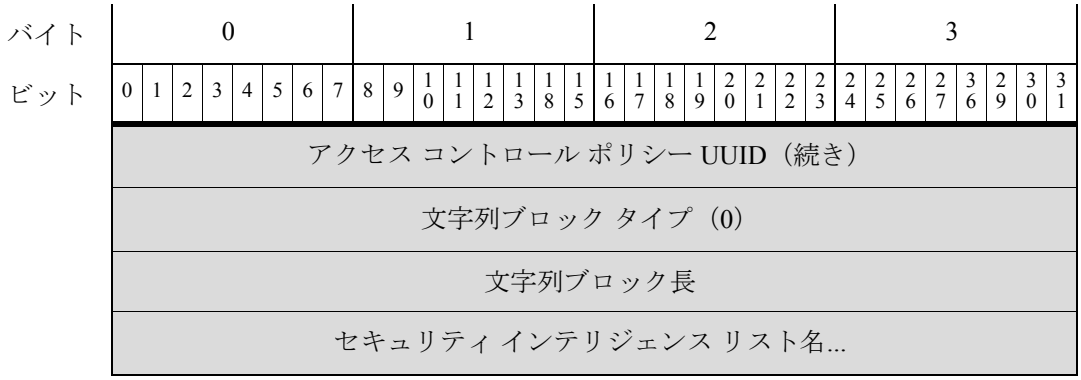
表 4-23　トンネルまたはプレフィルタ ルール理由メタデータ フィールド（続き）

フィールド	データタイプ	説明
トンネルまたはプレフィルタルール ID	uint32	トンネルまたはプレフィルタルールの内部 シスコ 識別子。
文字列ブロック タイプ	uint32	トンネルまたはプレフィルタルールの UUID とトンネルまたはプレフィルタルール ID に関連付けられた説明的な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(Name)]	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。セキュリティ インテリジェンス カテゴリ 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(2-15 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+(4-215 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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）																																



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。

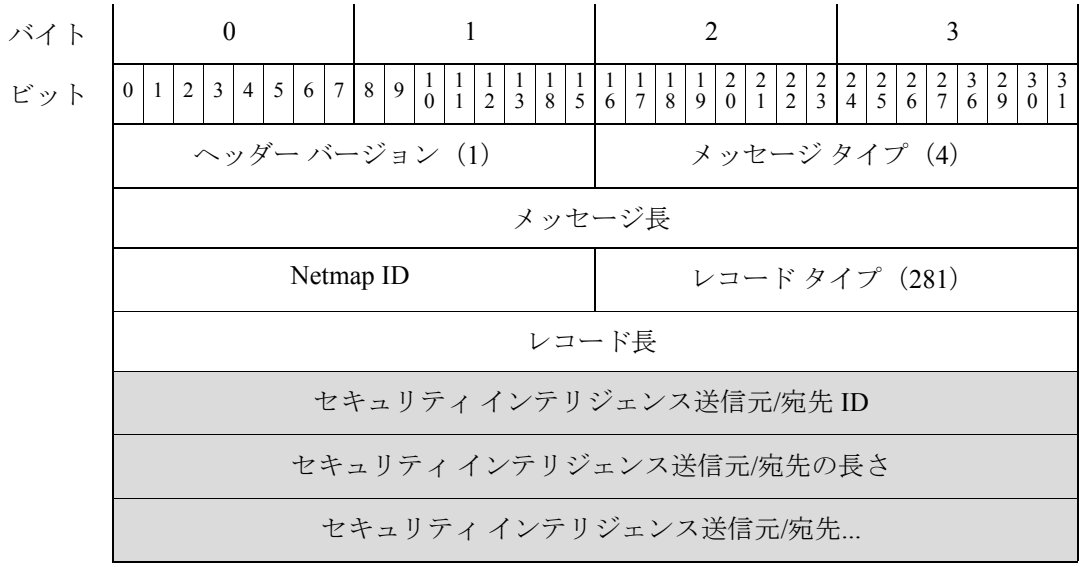
表 4-24　　セキュリティ インテリジェンス カテゴリ メタデータのフィールド

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	接続によってトリガーされた IP ブロックリストまたは許可リストの ID。このフィールドとアクセス コントロール ポリシー UUID を合わせると、このレコードの固有キーになります。
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。このフィールドとセキュリティ インテリジェンス リスト ID を合わせると、このレコードの固有キーとなります。
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 リスト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	接続によってトリガーされた IP カテゴリブロックリストまたは許可リストの名前。

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（2-15 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。



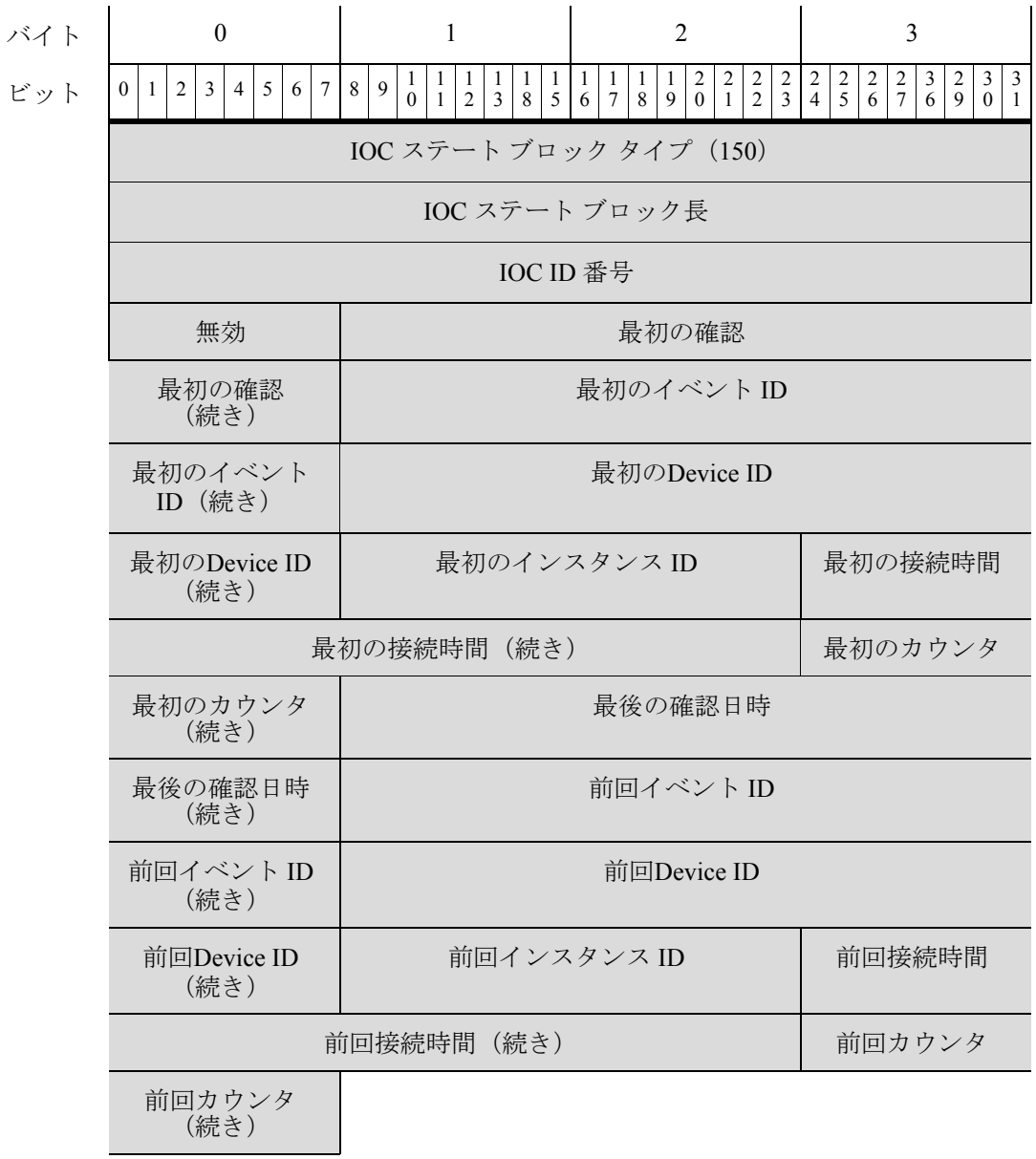
次の表では、セキュリティ インテリジェンス送信元/宛先レコードのフィールドについて説明します。

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。このフィールドは、このレコードの固有キーです。
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。

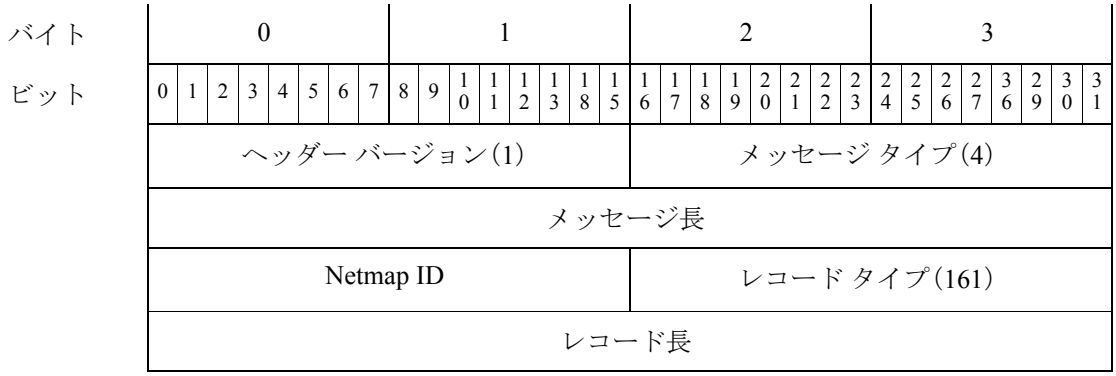
表 4-26　IOC ステート データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
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Device 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。
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 DeviceID	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	IOC 名ブロック タイプ（39）																															
	IOC 名ブロック長																															
	IOC ID 番号																															
カテゴリ（Category）	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	カテゴリ...																															
イベント タイプ（Event Type）	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。

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
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（Event Type）	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 エンドポイント向け AMP • Excel Compromise Detected by エンドポイント向け AMP • 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 エンドポイント向け AMP • Java launched shell • PDF Compromise Detected by エンドポイント向け AMP • PowerPoint Compromise Detected by エンドポイント向け AMP • PowerPoint launched shell • QuickTime Compromise Detected by エンドポイント向け AMP • 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 エンドポイント向け AMP • Threat Detected by エンドポイント向け AMP - Executed • Threat Detected by エンドポイント向け AMP - Not Executed • Threat Detected in File Transfer • Word Compromise Detected by エンドポイント向け AMP • 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、ユーザー、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（4-46 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-127 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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	Device 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（Event Type）																															
	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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
Device 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Device 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（1-4 ページ）を参照してください。
MAC アドレス	uint8[6]	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（Event Type）	uint32	イベント タイプ（新規イベントは 1000、変更イベントは、1001、ユーザー入力イベントは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（4-46 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（4-46 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ー 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（Event Type）	イベント サブタイプ
新規ホスト	[1000]	1
新規 TCP サーバー	[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 サーバー	[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 サーバー情報更新	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 サーバー情報更新	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
最終検出時のホスト	1001	15

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（Event Type）	イベント サブタイプ
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 サーバー信頼度更新	1001	25
UDP サーバー信頼度更新	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
ユーザー設定の有効な脆弱性（レガシー）	1002	1
ユーザー設定の無効な脆弱性（レガシー）	1002	2
ユーザー削除アドレス（レガシー）	1002	3
ユーザー削除サーバー（レガシー）	1002	4
ユーザー設定ホスト重要度	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
ユーザー設定脆弱性資格	1002	12
ユーザーポリシー制御	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
ユーザー設定オペレーティング システム	1002	16
ユーザー アカウント確認	1002	17
ユーザー アカウント更新	1002	18
ユーザー設定サーバー	1002	19
ユーザー削除アドレス（現在）	1002	20
ユーザー削除サーバー（現在）	1002	21

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（Event Type）	イベント サブタイプ
ユーザー設定の有効な脆弱性（現在）	1002	22
ユーザー設定の無効な脆弱性（現在）	1002	23
ユーザー 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
ユーザー追加ホスト	1002	27
ユーザー追加サーバー	1002	28
ユーザー追加クライアント アプリケーション	1002	29
ユーザー追加プロトコル	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
新規ユーザー アイデンティティ	1004	1
ユーザー ログイン	1004	2
ユーザー アイデンティティを削除	1004	3
ユーザー アイデンティティをドロップ。ユーザー上限に到達	1004	4
失敗したユーザーのログイン	1004	5
VPN ユーザーのログイン	1004	8
VPN ユーザーのログオフ	1004	9
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（4-46 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（4-47 ページ）
- サーバー メッセージ（4-48 ページ）
- 新規ネットワーク プロトコル メッセージ（4-49 ページ）
- 新規トランスポート プロトコル メッセージ（4-49 ページ）

- クライアント アプリケーション メッセージ(4-50 ページ)
- IP アドレス変更メッセージ(4-50 ページ)
- オペレーティング システム更新メッセージ(4-51 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(4-52 ページ)
- ホップ変更メッセージ(4-52 ページ)
- ホップ変更メッセージ(4-52 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(4-52 ページ)
- MAC アドレス メッセージ(4-53 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(4-53 ページ)
- VLAN タグ情報更新メッセージ(4-54 ページ)
- NetBIOS 名変更メッセージ(4-54 ページ)
- 更新バナー メッセージ(4-55 ページ)
- ポリシー制御の概要(4-55 ページ)
- 接続統計データ メッセージ(4-56 ページ)
- 接続チャンク メッセージ(4-56 ページ)
- バージョン4.6.1+ のユーザー設定脆弱性メッセージ(4-57 ページ)
- ユーザー追加/削除ホスト メッセージ(4-57 ページ)
- ユーザー削除サーバー メッセージ(4-58 ページ)
- ユーザー設定ホスト重要度メッセージ(4-58 ページ)
- 属性メッセージ(4-59 ページ)
- 属性値メッセージ(4-59 ページ)
- ユーザー サーバー メッセージとオペレーティング システム メッセージ(4-60 ページ)
- ユーザー プロトコル メッセージ(4-60 ページ)
- ユーザー クライアント アプリケーション メッセージ(4-61 ページ)
- スキャン結果を追加メッセージ(4-61 ページ)
- 新規オペレーティング システム メッセージ(4-62 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(4-62 ページ)
- ホスト IOC セット メッセージ(4-63 ページ)

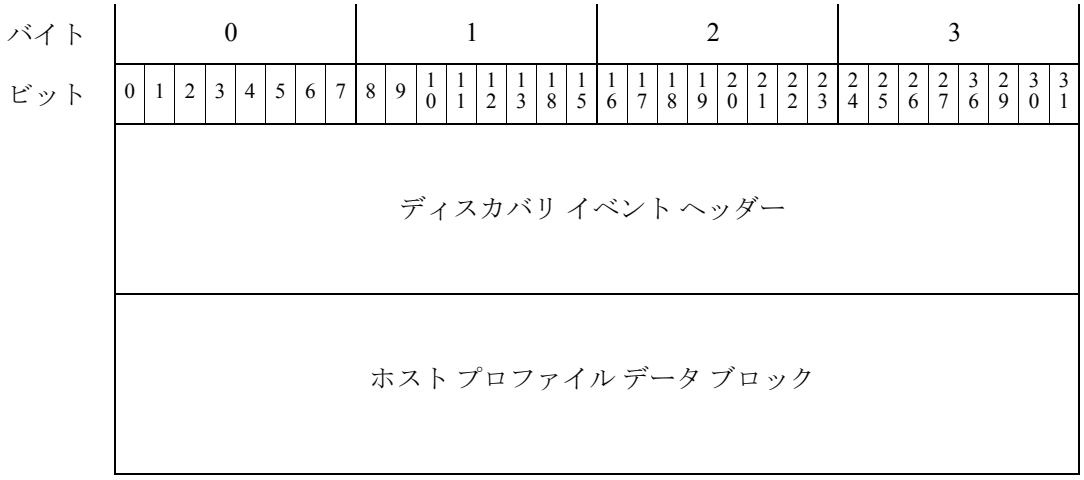
以下の項のデータ ブロック図は、ホスト ディスカバリ イベント メッセージで返る各種レコード データ ブロックです。

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+(4-175 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ーのサーバー情報のみです。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ー 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-373 ページ）を参照してください。



サーバー メッセージ

次の TCP サーバー イベント メッセージと UDP サーバー 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+（4-42 ページ）参照）があり、サーバー データ ブロック（ホスト サーバー データ ブロック 4.10.0+（4-149 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。

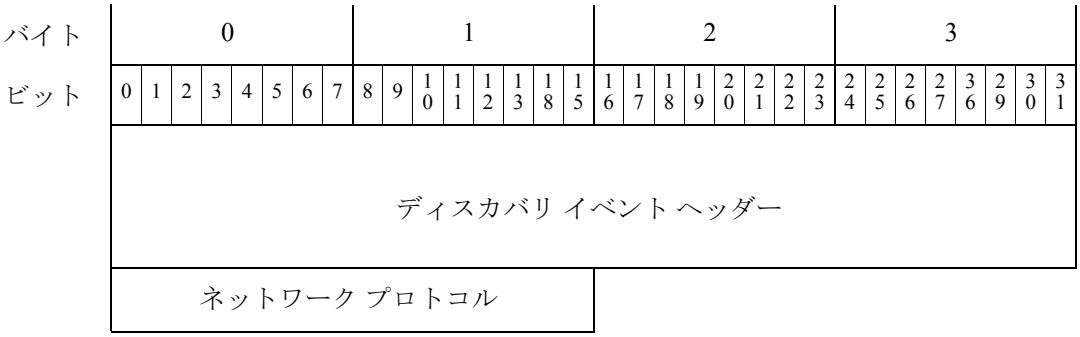
- 新規 TCP サーバー
- 新規 UDP サーバー
- TCP サーバー情報更新
- UDP サーバー情報更新
- TCP サーバー信頼度更新
- UDP サーバー信頼度更新

(注)　サーバー 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。サーバー 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:

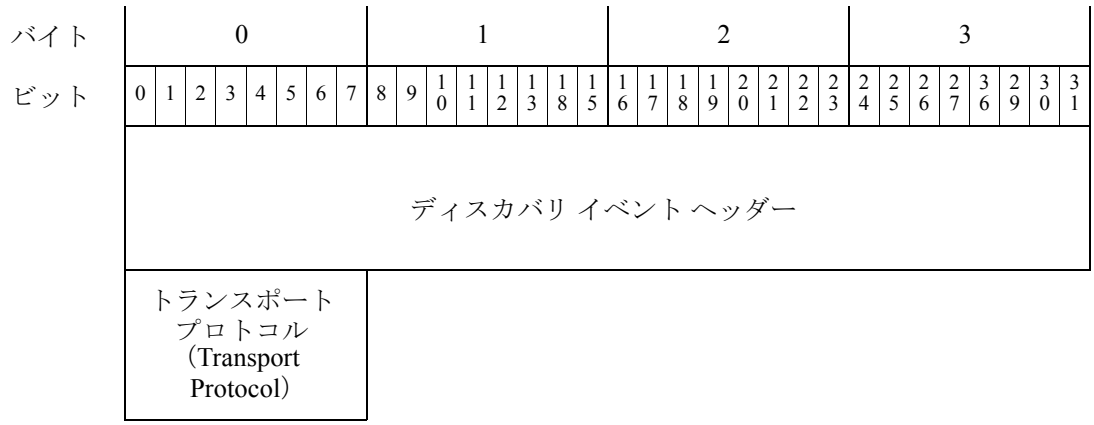
新規ネットワーク プロトコル メッセージ

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+（4-42 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

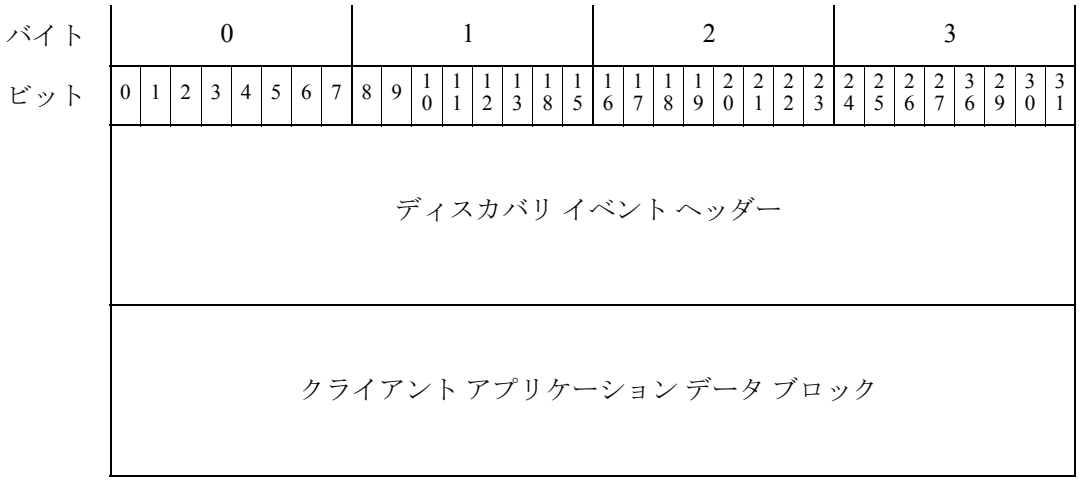
新規トランスポート プロトコルのイベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照。シリーズ 1 のブロック タイプ 4）と、トランスポート プロトコル番号の 1 バイト フィールド（次の表の値を使用）があります。



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+（4-42 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（4-167 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。

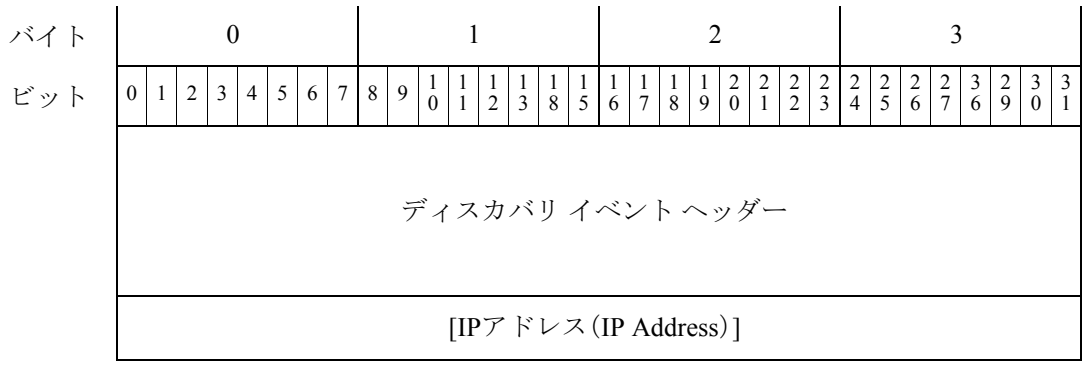


IP アドレス変更メッセージ

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+（4-42 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。

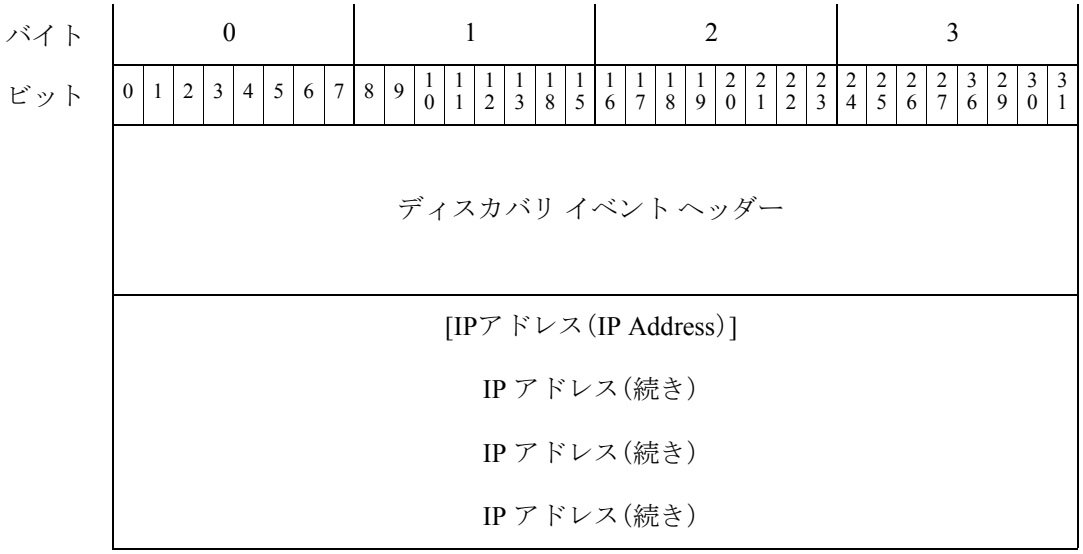
次の場合は、IP アドレスに（IP アドレス オクテット）4 バイトを使用します。

- 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



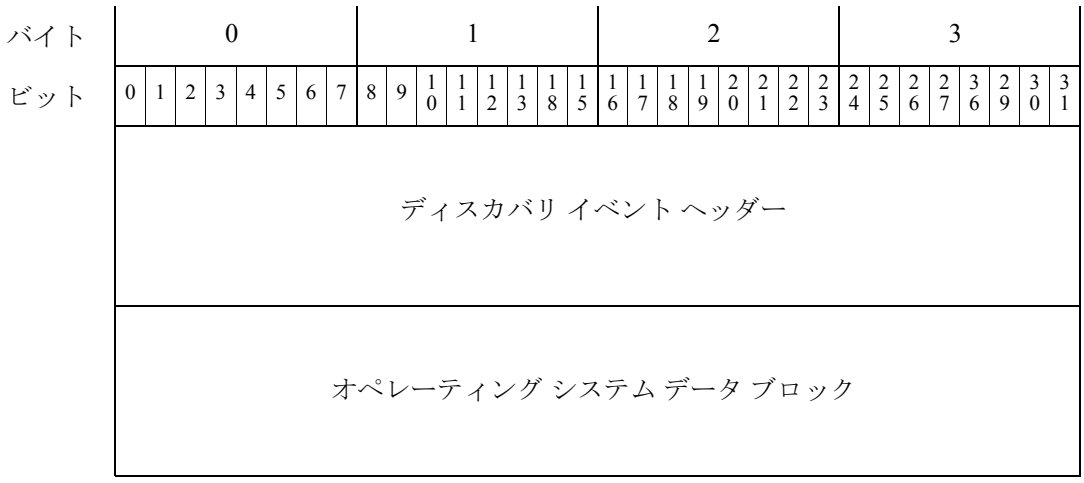
次の場合は、IP アドレスに（IP アドレス オクテット）16 バイトを使用します。

- 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

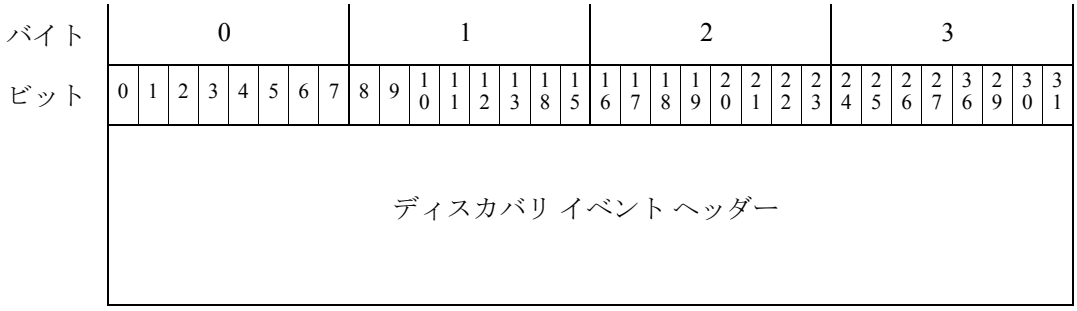
OS 情報更新イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照）があり、オペレーティング システム データ ブロック（オペレーティング システム データ ブロック 3.5+（4-91 ページ） を参照。シリーズ 1 のブロック タイプ 53）がそれに続きます。



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

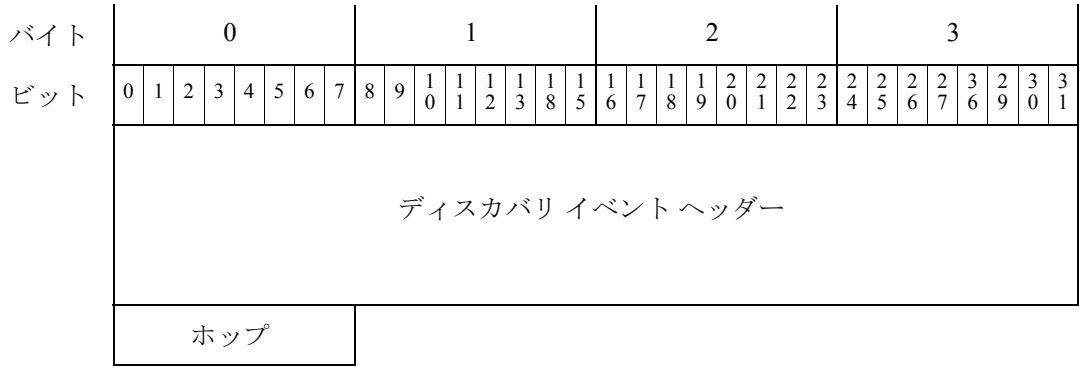
次のホスト イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照）があります。他にデータはありません。

- ホスト IP アドレスを再利用
- ホスト タイムアウト
- ホスト削除：ホスト制限に到達
- ホストのドロップ：ホスト制限に到達



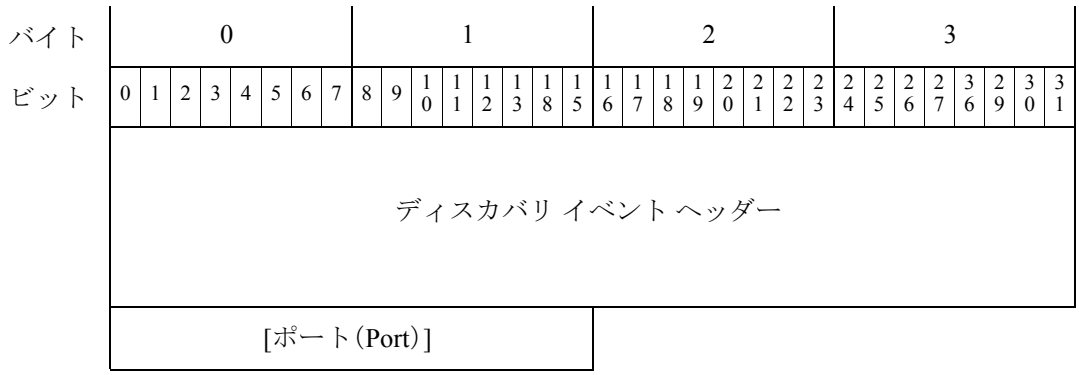
ホップ変更メッセージ

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+（4-42 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+（4-42 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。

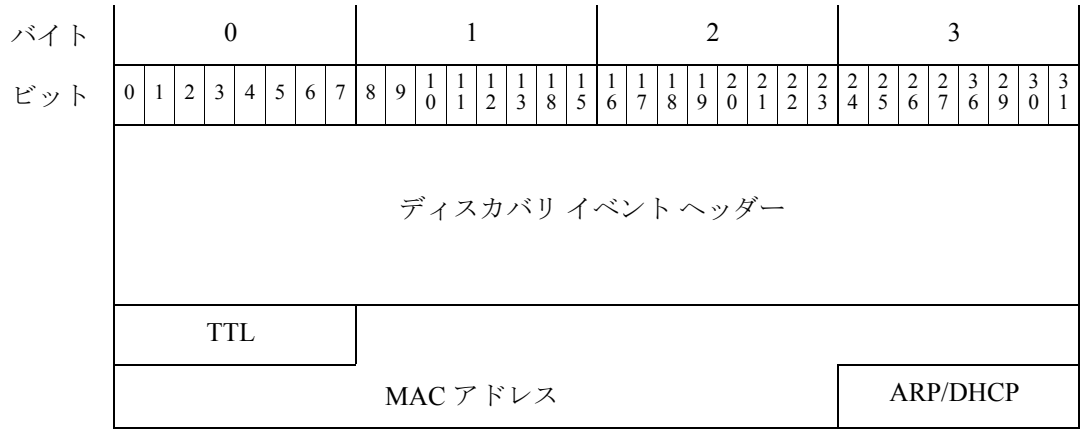


MAC アドレス メッセージ

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+(4-42 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(4-53 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+(4-122 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**。

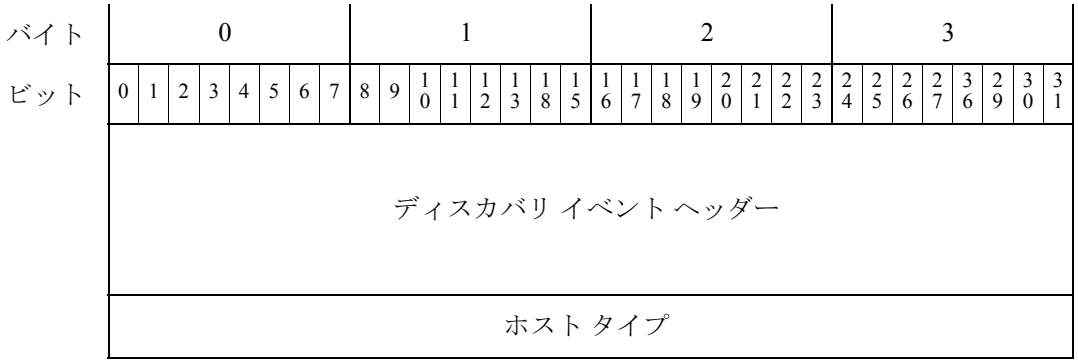


ブリッジ/ルータとして識別したホスト メッセージ

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+(4-42 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。

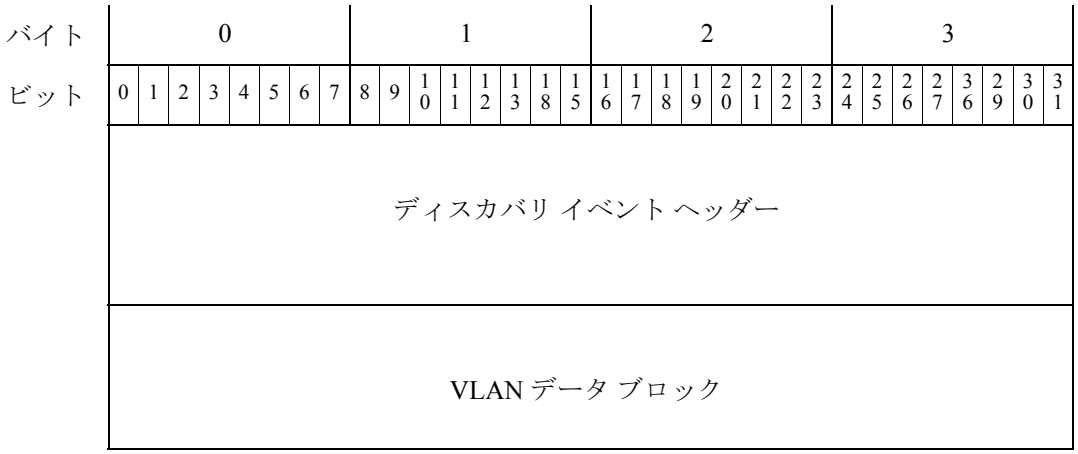
- 0：ホスト

- 1 — ルータ
- 2:ブリッジ



VLAN タグ情報更新メッセージ

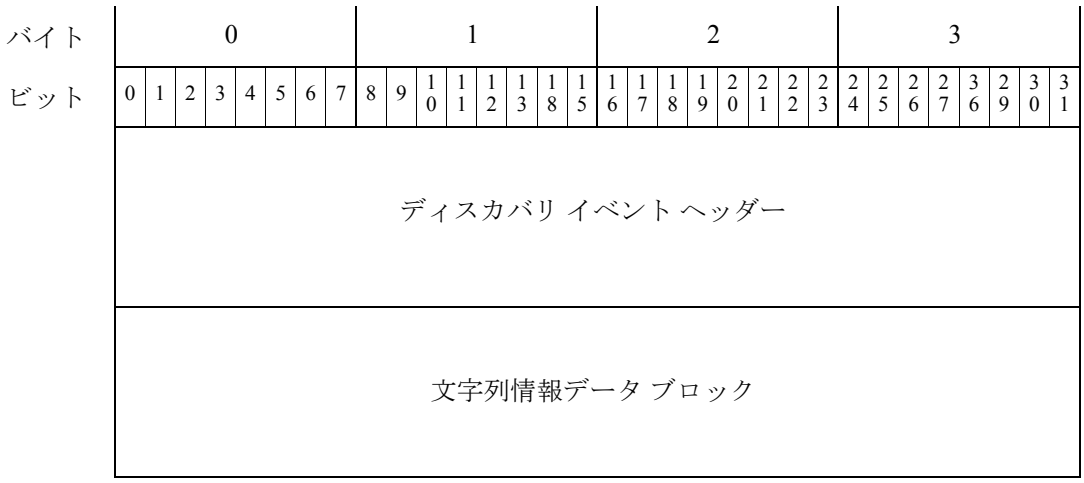
VLAN タグ情報更新イベントには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）があり、VLAN データ ブロックが続きます（VLAN データ ブロック（4-82 ページ）を参照）。VLAN データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 14 です。



NetBIOS 名変更メッセージ

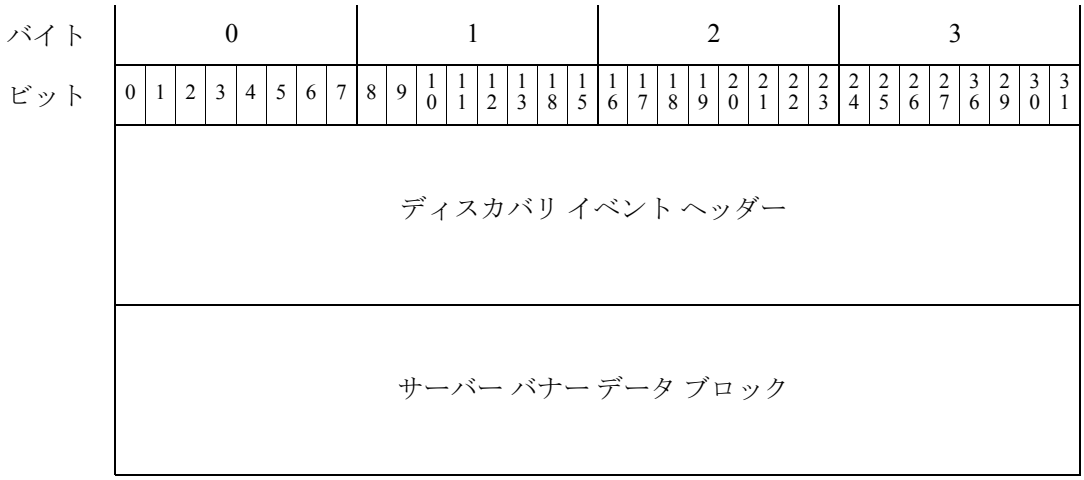
NetBIOS 名を変更イベント メッセージには、標準ディスカバリ イベント ヘッダーがあり（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）、文字列データ ブロックがそれに続きます（文字列情報データ ブロック（4-83 ページ）を参照）。文字列情報データ ブロックのブロック タイプは、シリーズ 1 のブロック タイプ 35 です。

（注）　NetBIOS ドメインを変更イベントを、Cisco Secure Firewall 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+（4-42 ページ）を参照）があり、サーバー バナーのデータ ブロックがそれに続きます（サーバー バナー データ ブロック（4-82 ページ）を参照）。サーバー 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+（4-42 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（4-92 ページ）を参照してください。

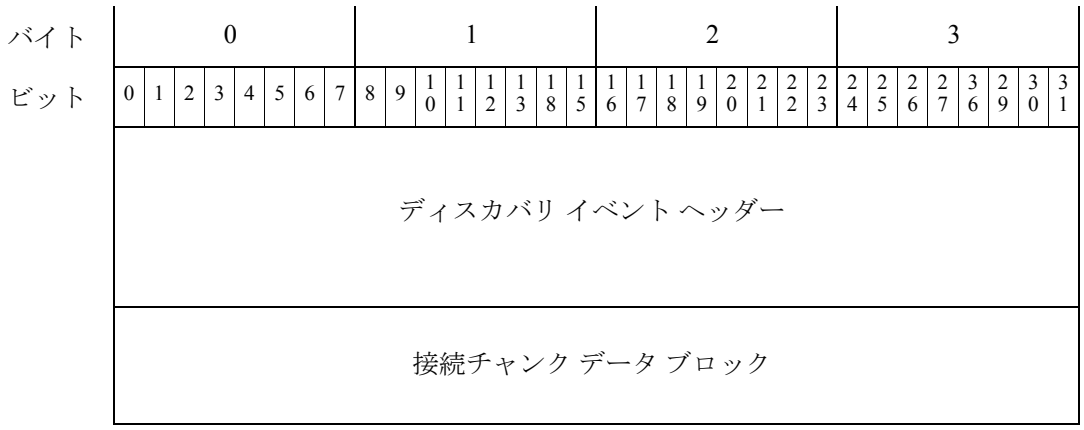
接続統計データ メッセージ

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+（4-42 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。バージョンの 6.1+ の接続統計データ ブロックの形式については、接続統計データ ブロック 7.1+（4-125 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）。

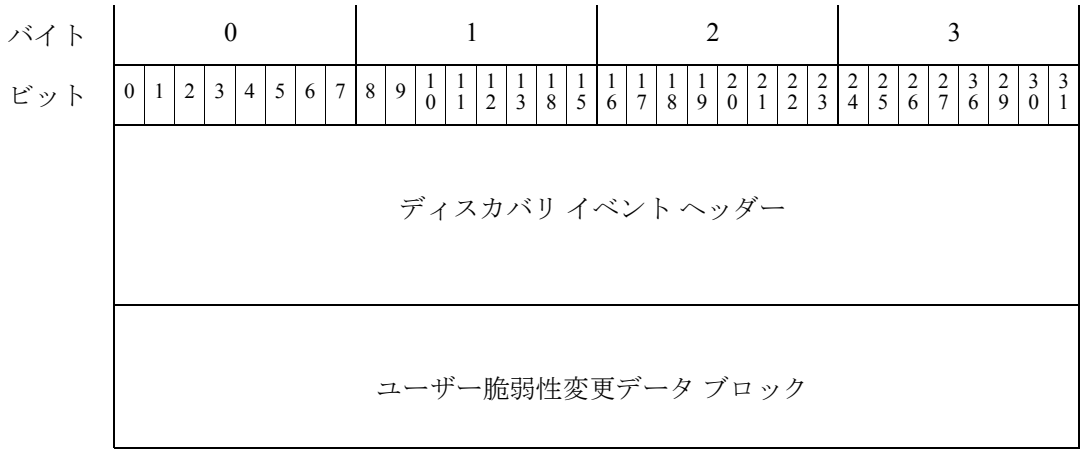
接続チャンク メッセージ

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+（4-42 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（4-106 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+ のユーザー設定脆弱性メッセージ

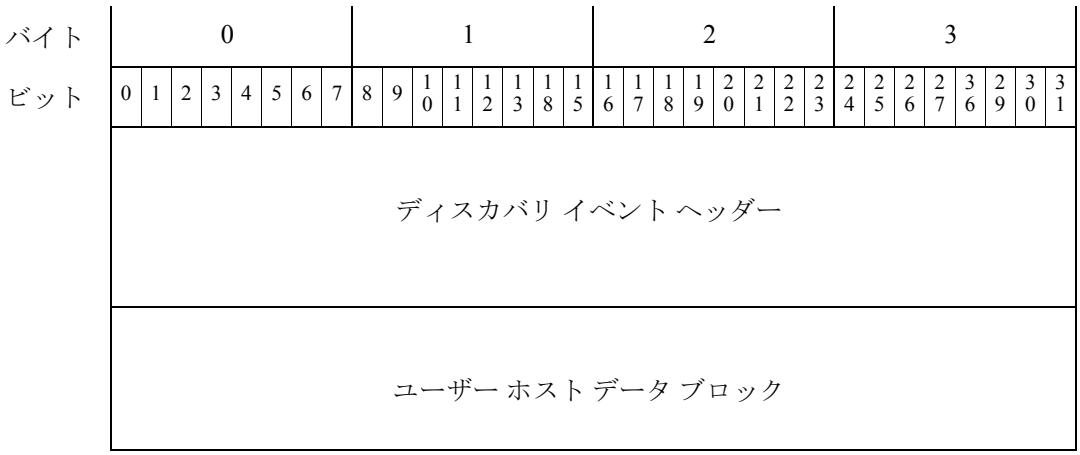
ユーザー設定の有効な脆弱性、ユーザー設定の無効な脆弱性、ユーザー脆弱性資格メッセージは、同じデータ形式を使用します。すなわち、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）にユーザー脆弱性変更データ ブロックが続きます（ユーザー脆弱性変更データ ブロック 4.7+（4-113 ページ）を参照。シリーズ 1 のブロック タイプ 80）。これらはレコード タイプ、イベント タイプ、イベント サブタイプで区別します。



ユーザー追加/削除ホスト メッセージ

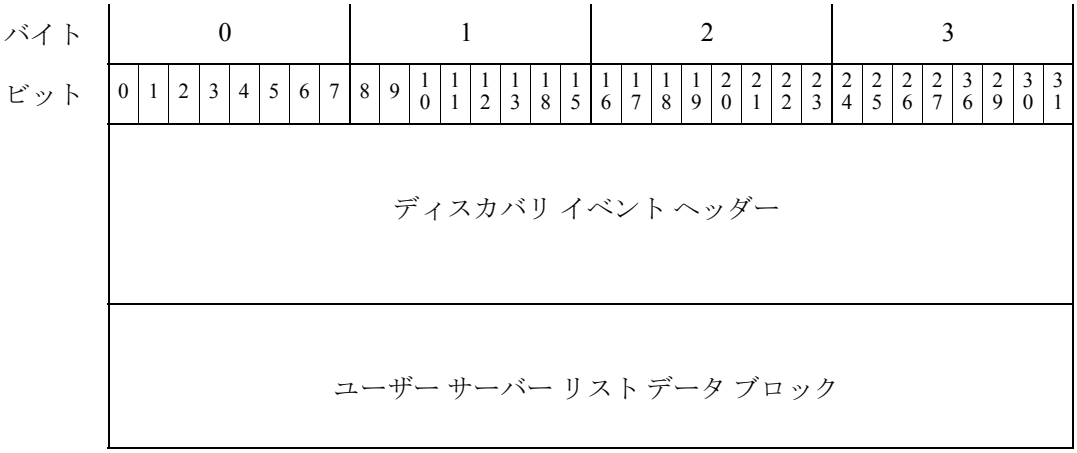
次のホスト入力イベント メッセージには、標準ディスカバリ イベント ヘッダーがあり（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）、ユーザー ホスト データ ブロックがそれに続きます（ユーザー ホスト データ ブロック 4.7+（4-111 ページ）を参照。シリーズ 1 のブロック タイプ 78）。

- ユーザー削除アドレス
- ユーザー追加ホスト



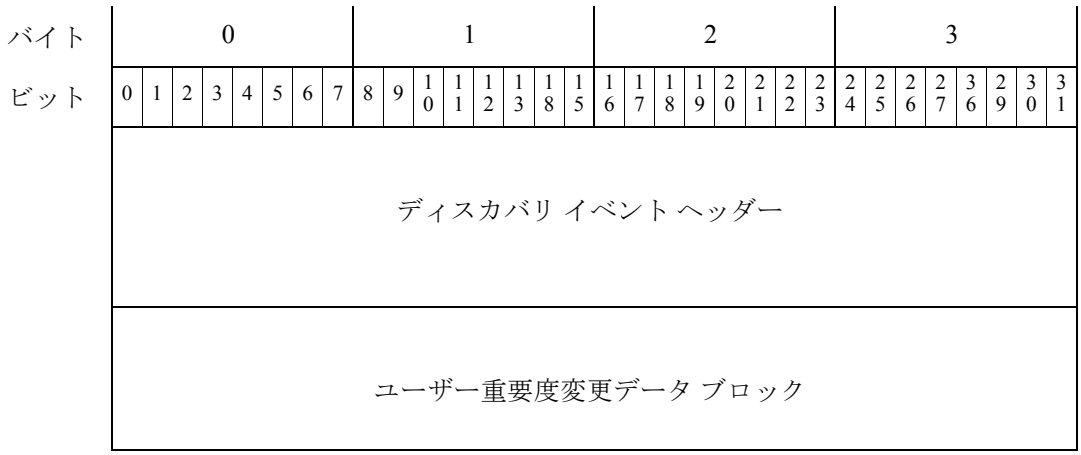
ユーザー削除サーバー メッセージ

ユーザー削除サーバー 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+（4-42 ページ）を参照）、ユーザー サーバー リスト データ ブロックがそれに続きます（ユーザー サーバー リスト データ ブロック（4-110 ページ）を参照）。ユーザー サーバー 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。



ユーザー設定ホスト重要度メッセージ

ユーザー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+（4-42 ページ）を参照）、ユーザー重要度変更データ ブロックがそれに続きます（ユーザー重要度変更データ ブロック 4.7+（4-114 ページ）を参照）。ユーザー重要度変更データ 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+（4-42 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（4-93 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

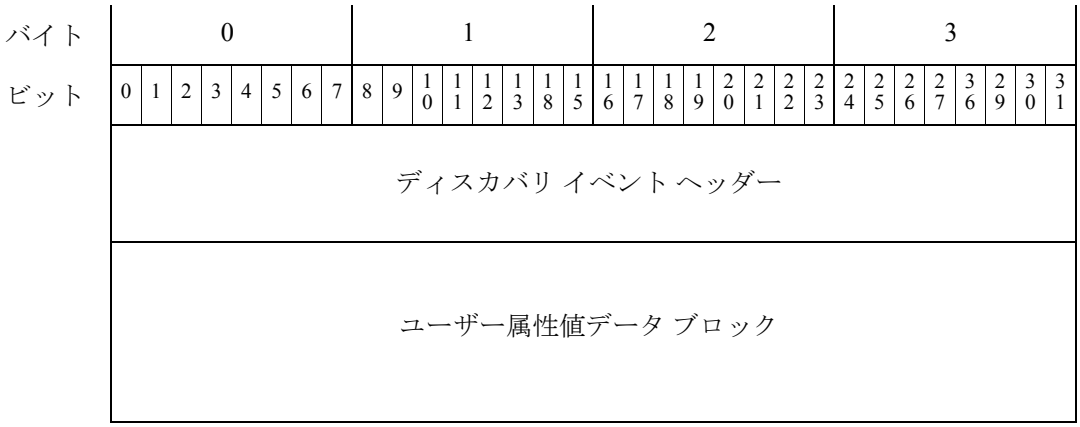
これらのイベントは、それぞれ次の形式を使用します:

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+（4-42 ページ）を参照）があり、ユーザー属性値データ ブロック（ユーザー属性値データ ブロック 4.7+（4-116 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:

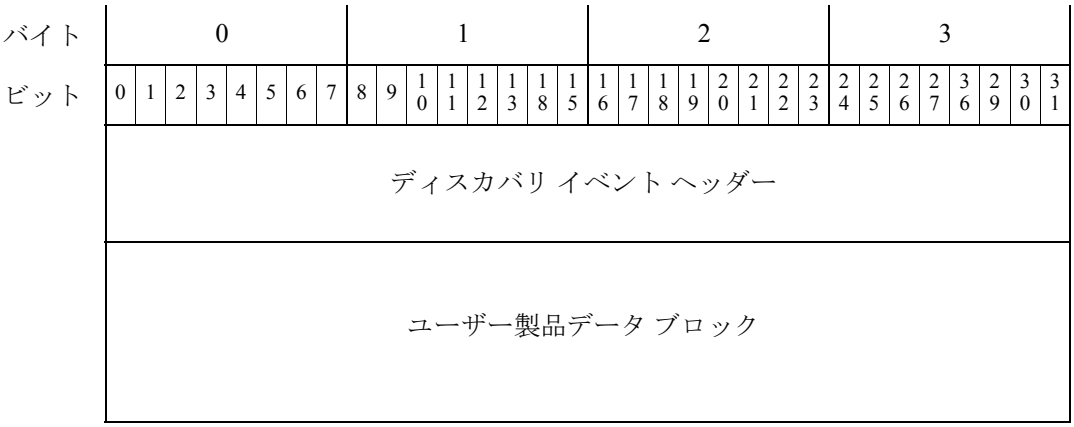


ユーザー サーバー メッセージとオペレーティング システム メッセージ

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+(4-42 ページ) を参照)があり、ユーザー製品データ ブロック(ユーザー製品データ ブロック 5.1+(4-183 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
- サーバー定義を設定
- サーバーの追加(Add Server)

これらのイベントは、それぞれ次の形式を使用します:



ユーザー 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+(4-42 ページ) を参照)があり、ユーザー プロトコル リスト データ ブロック(ユーザー プロトコル リスト データ ブロック 4.7+(4-118 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

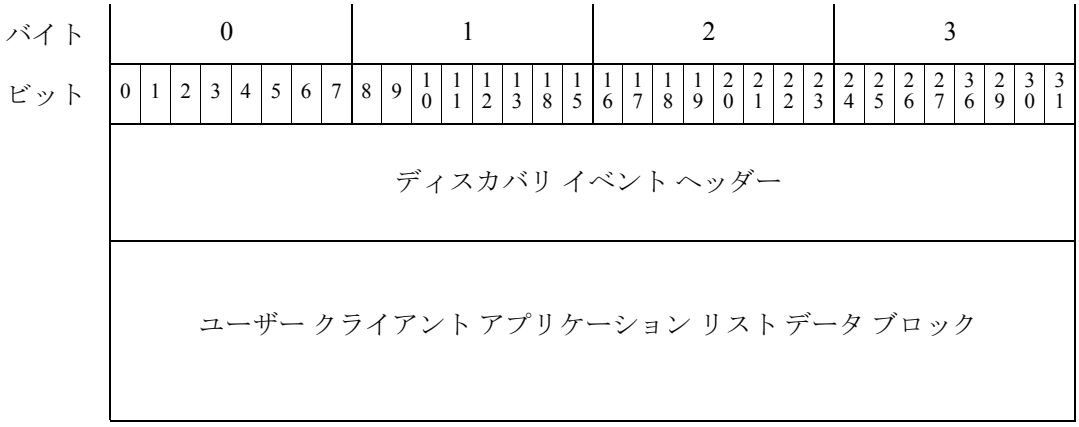
これらのイベントは、それぞれ次の形式を使用します:

ユーザー 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+(4-42 ページ) を参照)があり、ユーザー クライアント アプリケーション リスト データ ブロック(ユーザー クライアント アプリケーション リスト データ ブロック(4-99 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

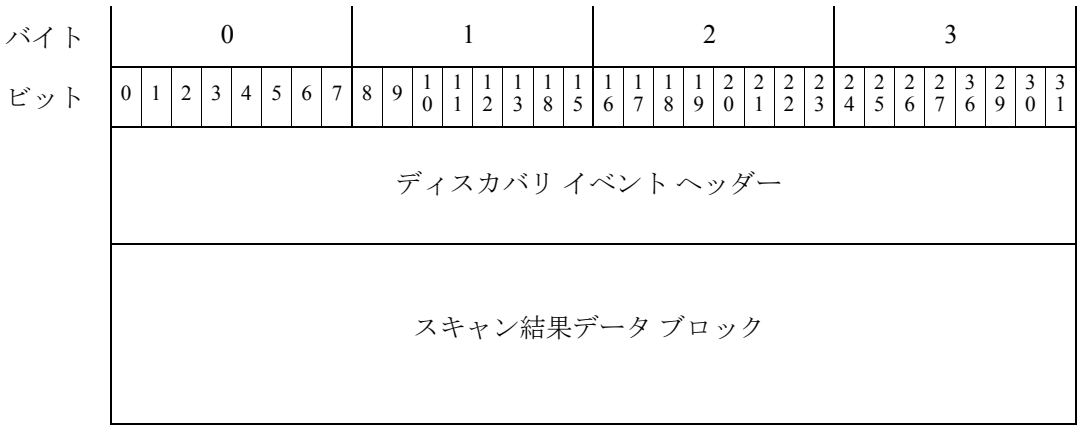
これらのイベントは、それぞれ次の形式を使用します:



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+(4-42 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(スキャン結果データ ブロック 5.2+(4-146 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+（4-42 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+（4-172 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

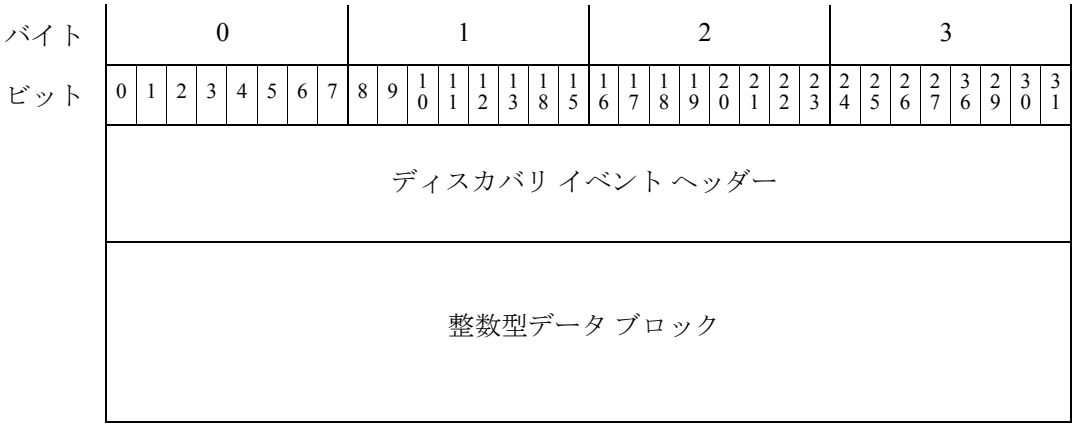
アイデンティティ競合イベント メッセージとアイデンティティ タイムアウト イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照）があり、アイデンティティ データ ブロックがそれに続きます（アイデンティティ データ ブロック（4-120 ページ） を参照）。アイデンティティ データ ブロックのブロック タイプは、シリーズ 1 ブロック タイプ 94 です。これらのメッセージは、フィンガープリント送信元アイデンティティで競合またはタイムアウトが発生すると生成されます。

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+（4-42 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（4-81 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 タイプ別のユーザー 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ー 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。

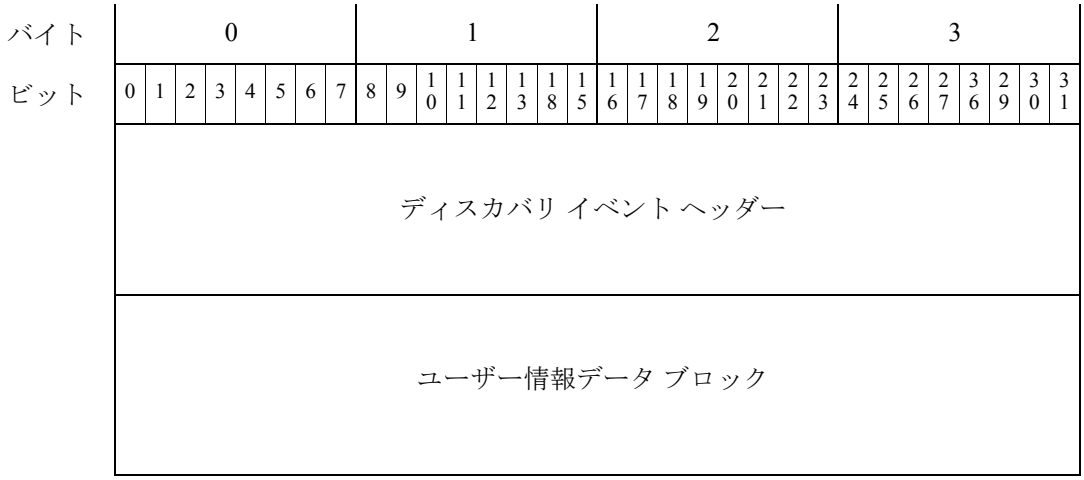
- ユーザー変更メッセージ（4-64 ページ）
- ユーザー情報更新メッセージ ブロック（4-64 ページ）

ユーザー変更メッセージ

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

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

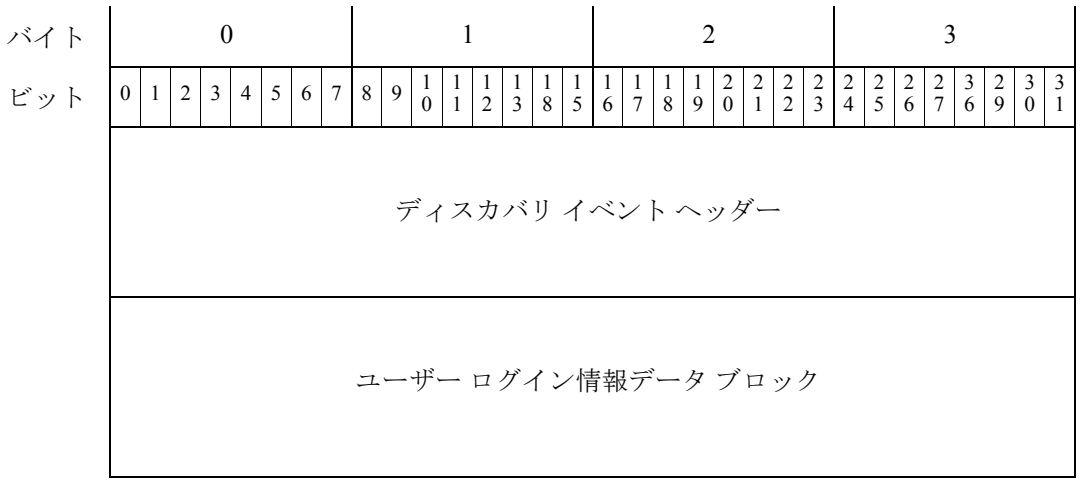
ユーザー変更イベント メッセージには、標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-42 ページ) を参照)があり、ユーザー情報データ ブロックがそれに続きます(6.0+ の情報データ ユーザー ブロック(4-201 ページ) を参照)。ユーザー情報データ ブロックはシリーズ 1 ブロック タイプ 120 です。



ユーザー情報更新メッセージ ブロック

システムがユーザーのログインの変更(ユーザー 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、ユーザー情報更新メッセージが送信されます。このブロックは、ユーザーがログインに失敗したとき(失敗したユーザーのログイン イベント:イベント タイプ 1004、サブタイプ 5)、VPN ユーザーがログインするとき(VPN ユーザーのログイン イベント:イベント タイプ 1004、サブタイプ 8)、または VPN ユーザーがログオフするとき(VPN ユーザーのログオフ イベント:イベント タイプ 1004、サブタイプ 9)にも使用されます。

ユーザー情報更新イベント 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+(4-42 ページ) を参照)とユーザー ログイン情報データ ブロックがあります(ユーザー ログイン情報データ ブロック 6.2+(4-207 ページ) を参照)。ユーザー 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。

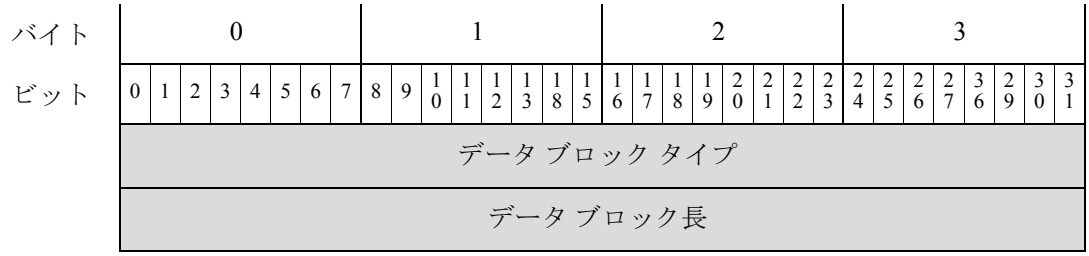


ディスカバリ（シリーズ1）ブロック

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（2-29 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 (4-75 ページ)
- BLOB データ ブロック (4-76 ページ)
- リスト データ ブロック (4-77 ページ)
- 汎用リスト ブロック (4-78 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 (4-66 ページ) を参照してください。ユーザー イベント ブロック タイプについては、表 4-86 (4-191 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 (Type)	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 (4-75 ページ) を参照してください。
1	サブサーバー	現在 (Current)	サーバーで検出したサブサーバーに関する情報を格納します。詳細については、サブサーバー データ ブロック (4-78 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 (4-80 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 (4-81 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 (4-76 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（Type）	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（4-77 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（4-82 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（3-22 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（4-78 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（4-83 ページ）を参照してください。
37	サーバー バナー	現在（Current）	サーバー バナー データを格納します。詳細については、サーバー バナー データ ブロック（4-82 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（4-87 ページ）を参照してください。
54	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（Attribute Value）	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（4-87 ページ）を参照してください。
51	フル サブサーバー	現在（Current）	サーバーで検出したサブサーバーに関する情報を格納します。フル サーバー情報ブロックとフル ホスト プロファイルで参照します。各サブサーバーの脆弱性情報を格納します。詳細については、フル サブサーバー データ ブロック（4-89 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（Type）	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+（4-91 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）	ユーザー 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（4-92 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（4-93 ページ）を参照してください。
72	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	ユーザー プロトコル	現在（Current）	ユーザー入力のプロトコル情報を格納します。詳細については、ユーザー プロトコル データ ブロック（4-96 ページ）を参照してください。
59	ユーザー クライアント アプリケーション	レガシー	ユーザー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、ユーザー 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-130 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	ユーザー クライアント アプリケーション リスト	現在（Current）	ユーザー 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、ユーザー クライアント アプリケーション リスト データ ブロック（4-99 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-415 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。
62	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（4-102 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（4-104 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（4-105 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（Type）	目次	データ ブロック ステータス	説明
65	ユーザー製品	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、ユーザー製品データ ブロック 5.0.x（B-134 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-186 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（4-108 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	ユーザー サーバー	現在（Current）	ユーザー入力イベントのサーバー情報を格納します。詳細については、ユーザー サーバー データ ブロック（4-109 ページ）を参照してください。
77	ユーザー サーバー リスト	現在（Current）	ユーザー サーバー ブロックのリストを格納します。詳細については、ユーザー サーバー リスト データ ブロック（4-110 ページ）を参照してください。
78	ユーザー ホスト	現在（Current）	ユーザー 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、ユーザー ホスト データ ブロック 4.7+（4-111 ページ）を参照してください。
79	ユーザー脆弱性	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	ユーザー 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、ユーザー脆弱性変更データ ブロック 4.7+（4-113 ページ）を参照してください。
81	ユーザー重要度	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、ユーザー重要度変更データ ブロック 4.7+（4-114 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（Type）	目次	データ ブロック ステータス	説明
82	ユーザー属性値	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、ユーザー属性値データ ブロック 4.7+（4-116 ページ）を参照してください。
83	ユーザー 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、ユーザー プロトコル リスト データ ブロック 4.7+（4-118 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+（4-119 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-166 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	サーバー情報	レガシー	サーバー フィンガープリントで使用するサーバー情報を格納します（本製品の旧バージョンを参照のこと）。
89	ホスト/サーバー	レガシー	ホスト サーバー情報を格納します（本製品の旧バージョンを参照のこと）。
90	フル ホスト サーバー	レガシー	ホスト サーバー情報を格納します（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+（4-175 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（4-120 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+（4-122 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（4-123 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。

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（Type）	目次	データ ブロック ステータス	説明
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/サーバー	レガシー	ホスト サーバー情報を格納します（本製品の旧バージョンを参照のこと）。
99	フル ホスト サーバー	レガシー	ホスト サーバー情報を格納します（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-132 ページ）を参照してください。
103	ホスト/サーバー	現在（Current）	ホスト サーバー情報を格納します。詳細については、ホスト サーバー データ ブロック 4.10.0+（4-149 ページ）を参照してください。
104	フル ホスト サーバー	現在（Current）	ホスト サーバー情報を格納します。詳細については、フル ホスト サーバー データ ブロック 4.10.0+（4-151 ページ）を参照してください。
105	サーバー情報	レガシー	サーバー フィンガープリントで使用するサーバー情報を格納します。詳細については、4.10.x、5.0 ～ 5.0.2 のサーバー情報データ ブロック（4-155 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 サーバー情報	現在（Current）	ホストで検出したサーバーに関する情報を格納します。詳細については、フル サーバー情報データ ブロック（4-158 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（4-160 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（4-162 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（Type）	目次	データ ブロック ステータス	説明
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-374 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。
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+（4-165 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-168 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	サーバー情報	現在（Current）	サーバー フィンガープリントで使用するサーバー情報を格納します。詳細については、4.10.x、5.0 ～ 5.0.2 のサーバー情報データ ブロック（4-155 ページ）を参照してください。
118	ユーザー製品	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、ユーザー製品データ ブロック 5.0.x（B-134 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-186 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（4-167 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（4-124 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。

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（Type）	目次	データ ブロック ステータス	説明
124	ユーザー脆弱性	現在（Current）	ホスト脆弱性に関する情報を格納します。ユーザー脆弱性データ ブロック 5.0+（4-169 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。
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-173 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+（4-172 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Device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+ のモバイルDevice 情報データ ブロック（4-173 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-395 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	ユーザー製品	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、ユーザー製品データ ブロック 5.1+（4-183 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-384 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（4-106 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。

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（Type）	目次	データ ブロック ステータス	説明
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-186 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。
138	ユーザー クライアント アプリケーション	現在（Current）	ユーザー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+ のユーザー クライアント アプリケーション 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 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+（4-175 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（4-101 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。スキャン結果データ ブロック 5.2+（4-146 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（4-103 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-179 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+（4-84 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。
148	ユーザー IOC の変更	Current	ユーザーの IOC への変更に関する情報が含まれています。詳細については、ユーザー IOC の変更データ ブロック 5.3+（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（Type）	目次	データ ブロック ステータス	説明
149	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-195 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-202 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。
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-210 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-224 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	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 6.0.x（B-239 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。
163	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 7.1+（4-125 ページ）を参照してください。これはブロック タイプ 160 に置き換わります。

文字列データ ブロック

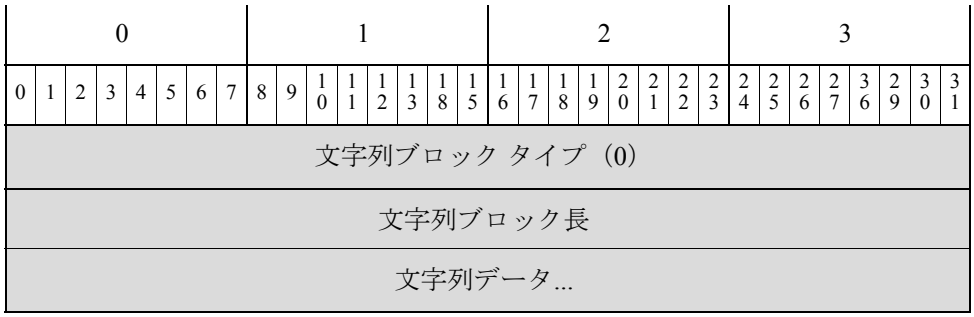
文字列データ ブロックは、シリーズ 1 ブロックの文字列データ送信に使用します。他のシリーズ 1 データ ブロックで、主に、たとえば、オペレーティング システムやサーバー名の記述に使用します。

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。

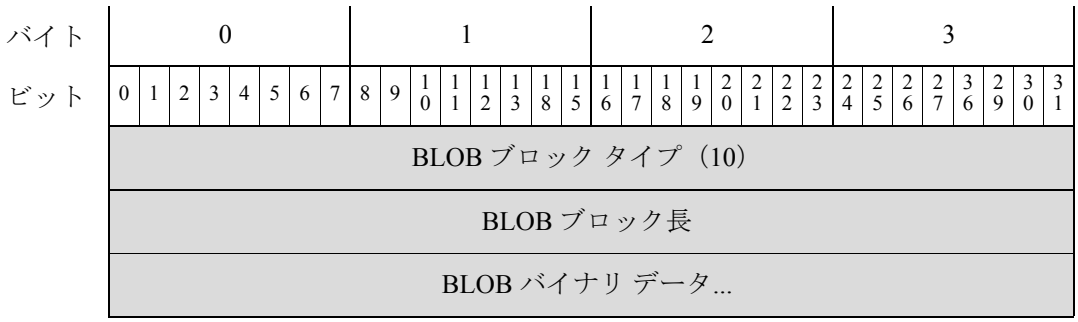
表 4-31　　文字列データ ブロックのフィールド

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ー 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。

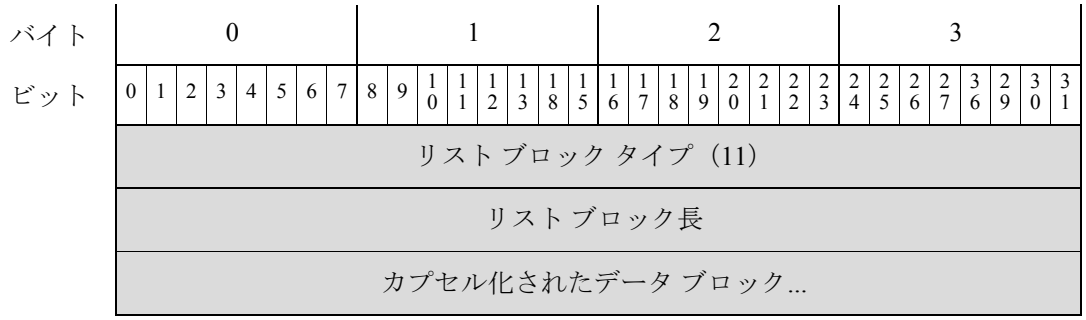
表 4-32　BLOB データ ブロック フィールド

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（variable）	バイナリ データ（通常、サーバー 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 サーバーのリストを送信する場合、データを含むサーバー 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 つのサブサーバー データ ブロックがある場合、その値は、サブサーバー 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（variable）	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。

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（variable）	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。

サブサーバー データ ブロック

サブサーバー データ ブロックは、個々のサブサーバー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ーに呼び出されたサーバーであり、脆弱性に関連付けられています。サブサーバー 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 1 です。

次の図は、サブサーバー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	サブサーバー ブロック タイプ(1)																															
	サブサーバー ブロック長																															
サブサーバー [名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	サブサーバー名...																															
ベンダー [名前(Name)]	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 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 4-35　　サブサーバー 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
サブサーバー ブロック タイプ	uint32	サブサーバー データ ブロックを開始します。この値は常に 1 です。
サブサーバー ブロック長	uint32	サブサーバー 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ブサーバー 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	サブサーバー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ー名のバイト数を加えたサブサーバー名文字列データ ブロックのバイト数。
サブサーバー名	string	サブサーバーの名前。
文字列ブロック タイプ	uint32	サブサーバー 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。

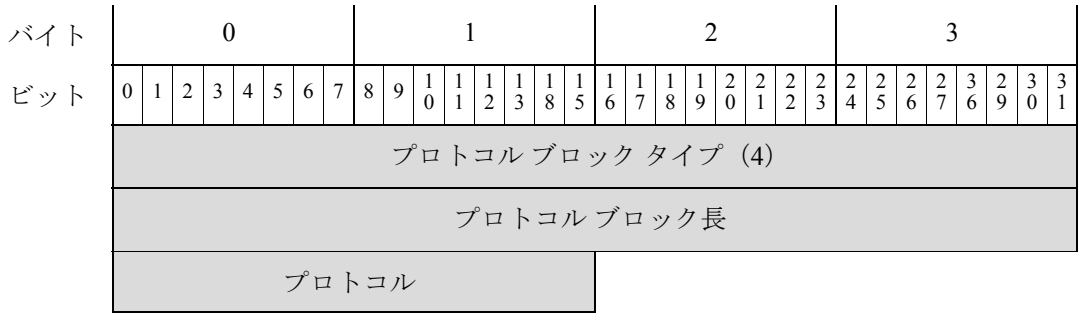
表 4-35　サブサーバー データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
ベンダー名（Vendor Name）	string	サブサーバー ベンダー名。
文字列ブロック タイプ	uint32	サブサーバー 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ー 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	サブサーバー長

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。

表 4-36　プロトコル データ ブロックのフィールド（続き）

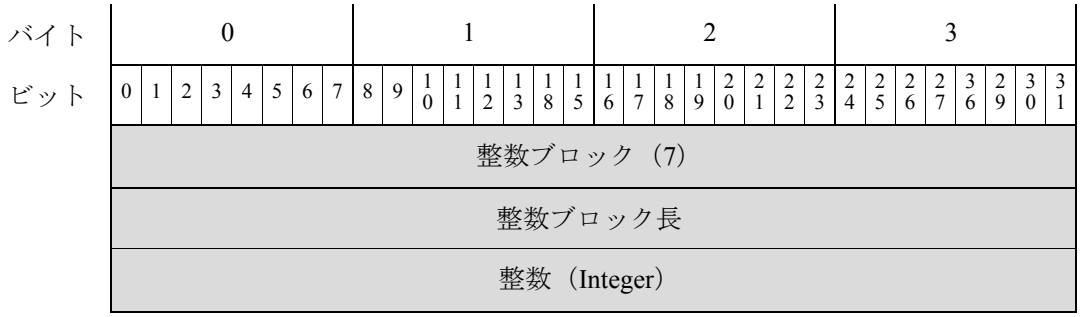
フィールド	データタイプ	説明
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6：TCP • 17：UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048：IP

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。



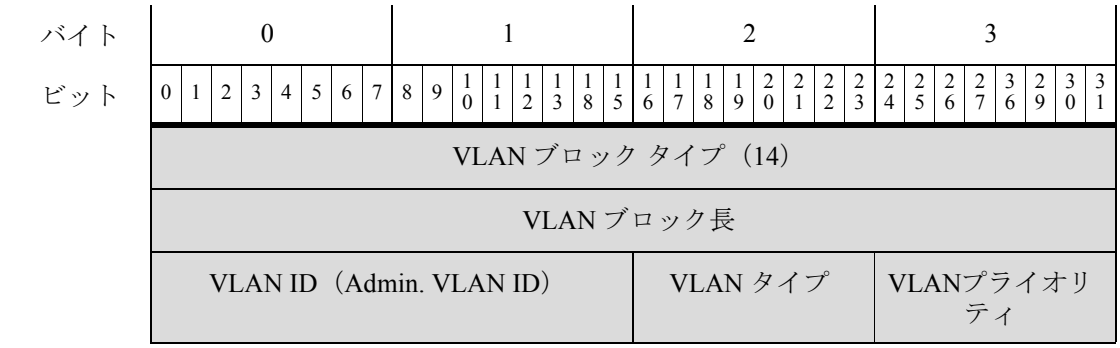
次の表では、整数型データ ブロックのフィールドについて説明します。

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

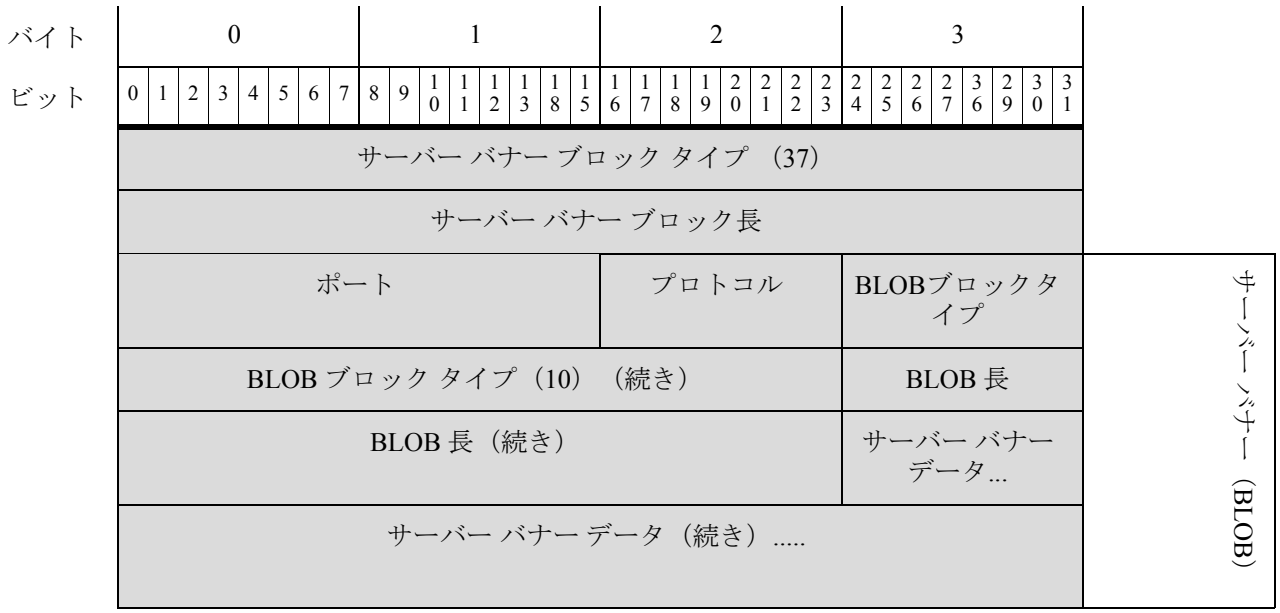
フィールド	データタイプ	説明
VLAN ブロック タイプ	uint32	VLAN データ ブロックを開始します。この値は常に 14 です。
VLAN ブロック長	uint32	VLAN データ ブロックのバイト数。この値は常に 12 です。
VLAN ID（Admin. VLAN ID）	uint16	ホストがメンバーとして所属している VLAN を示す VLAN ID 番号を格納します。
VLAN タイプ	uint8	VLAN タグ内でカプセル化されるパケットのタイプ。 • 0:イーサネット • 1:トークン リング
VLAN プライオリティ	uint8	VLAN タグに含まれる優先順位値。

サーバー バナー データ ブロック

サーバー バナー データ ブロックには、ホストで実行するサーバーのバナーに関する情報があります。これにはサーバー ポート、プロトコル、バナー データを格納します。サーバー 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、サーバー 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、サーバー 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。

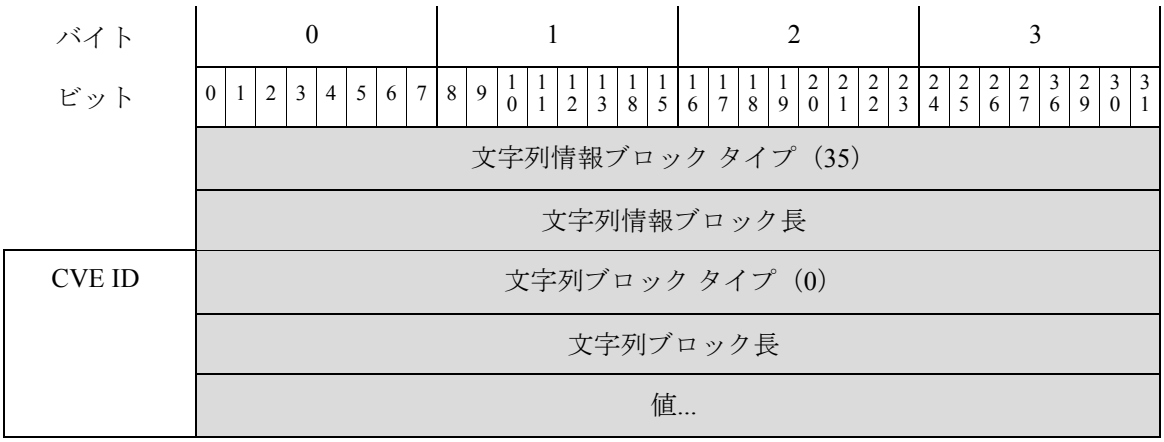
表 4-39　サーバー バナー データ ブロックのフィールド

フィールド	データタイプ	説明
サーバー バナー ブロック タイプ	uint32	サーバー 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。
サーバー バナー ブロック長	uint32	サーバー 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ー バナー データ ブロックの合計バイト数。
[ポート(Port)]	uint16	サーバーを実行するポート番号。
プロトコル	uint8	サーバーのプロトコル番号。
BLOB ブロック タイプ	uint32	サーバー 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* バイトがサーバー 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。

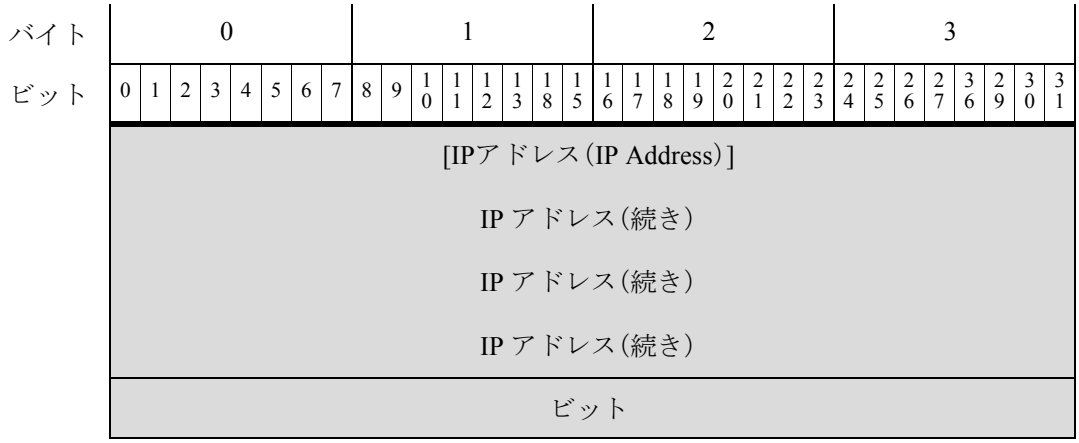
表 4-40　　文字列情報データ ブロックのフィールド

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。

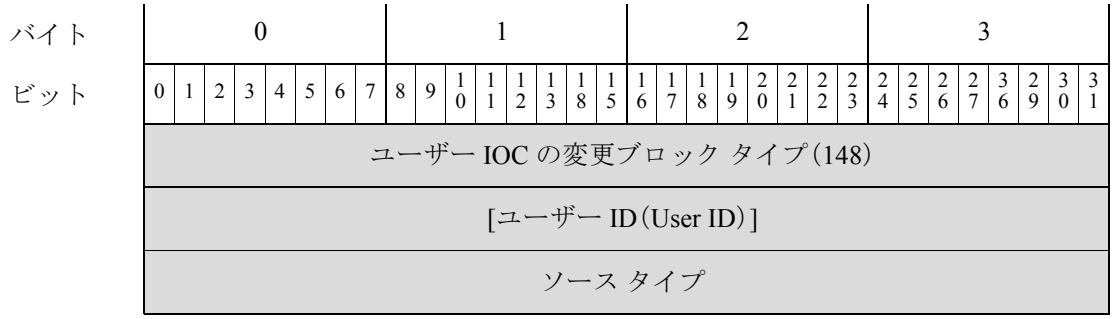
表 4-41　属性アドレス データ ブロック 5.2+ のフィールド

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(IP Address)]	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。

ユーザー IOC の変更データ ブロック 5.3+

ユーザー IOC の変更データ ブロックには、ユーザーが行った IOC の変更に関する情報が含まれています。これは、ユーザー ホスト IOC の削除、ユーザー ホスト IOC の有効化、およびユーザー ホスト IOC の無効化レコード内で使用されます。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 148 です。

次の図で、ユーザー IOC 変更データ ブロックの基本構造を示します。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
[IPアドレス（IP Address）]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*																															
	IOC ID																															
	ターゲット UID																															

次の表で、ユーザー IOC 変更データ ブロックのフィールドについて説明します。

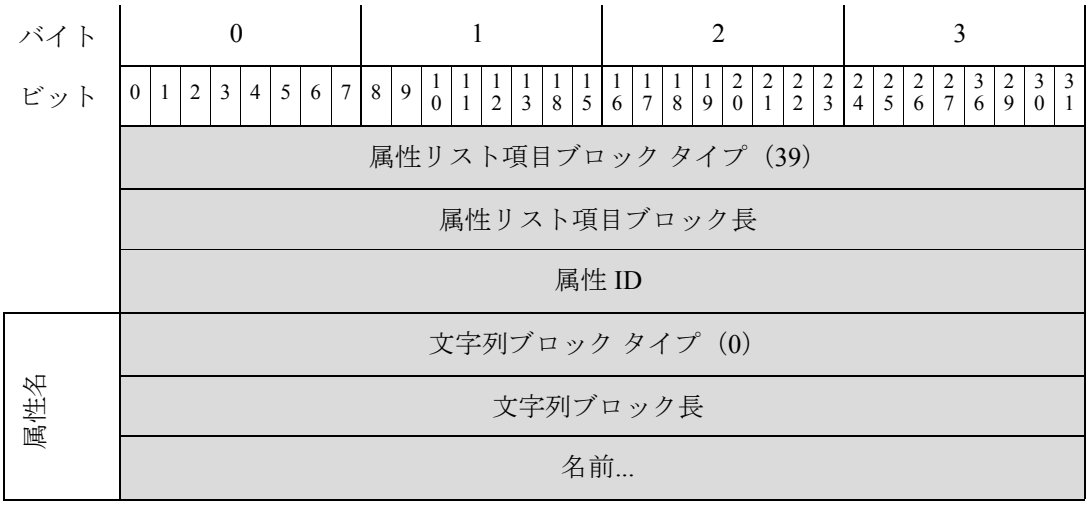
表 4-42　　ユーザー IOC の変更データ ブロック 5.3+ フィールド

フィールド	データタイプ	説明
ユーザー IOC の変更ブロック タイプ	uint32	ユーザー IOC の変更データ ブロックを開始します。この値は、常に `148` です。
ユーザー ID（User ID）	uint32	IOC に変更を加えたユーザーの ID 番号。
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` • ユーザーがクライアント 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`
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（variable）	ユーザー入力の 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（4-101 ページ）を参照してください。
IOC ID	uint32	変更された IOC の ID 番号。
ターゲット UID	unit32	eStreamer 出力でサポートされているイベントでは使用されません。

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。

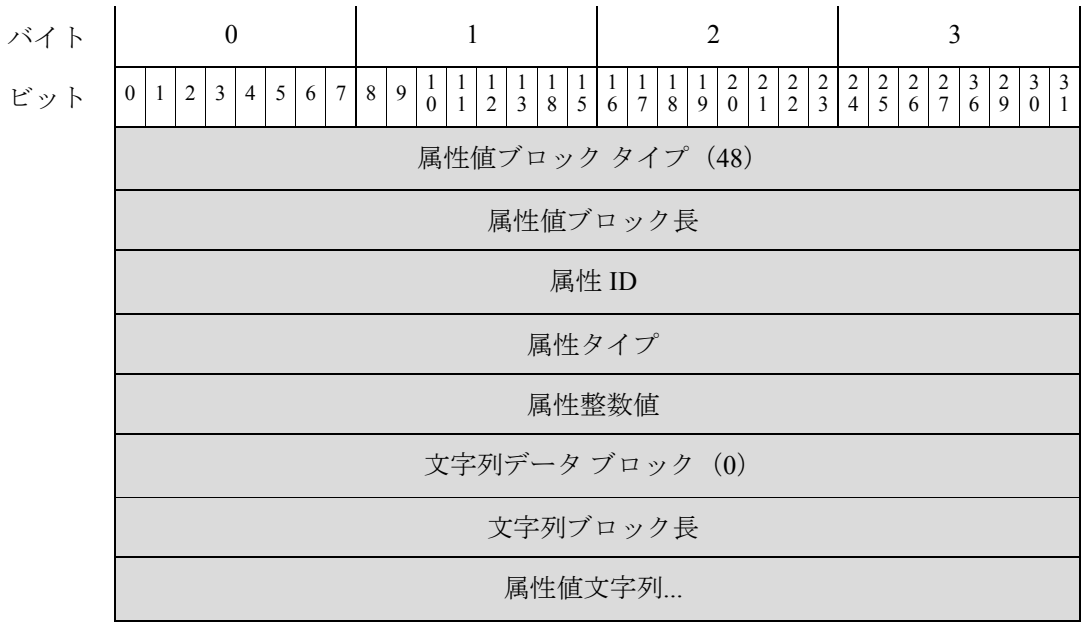
表 4-43　　属性リスト項目データ ブロックのフィールド

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（Name）]	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 4-44　　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。

表 4-44　属性値データ 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	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（Attribute Value）	string	属性値。

フル サブサーバー データ ブロック

フル サーバー データ ブロックは、ホストで検出したサーバーに関連付けられたサブサーバーに関する情報を伝えます。サブサーバーに関する情報には、ホスト上のサブサーバーのベンダー、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。サブサーバーは、固有の関連脆弱性があるサーバーの読み込み可能なモジュールです。フル ホスト サーバー データ ブロックには、ホストで検出した各サーバーのフル サブサーバー データ ブロックが含まれます。フル ホスト サーバー 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 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 サブサーバー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
フル サブサーバー ブロック タイプ（51）																																
フル サブサーバー 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																																
サブサーバー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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																																
（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 サブサーバー 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 4-45　フル サブサーバー 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
フル サブサーバー ブロック タイプ	uint32	フル サブサーバー ブロックを開始します。この値は常に 51 です。
フル サブサーバー ブロック長	uint32	フルサブサーバー 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、後続のフル サブサーバー ブロックのバイト数を加えたフル サブサーバー 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	サブサーバー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ー名のバイト数を加えたサブサーバー名文字列データ ブロックのバイト数。
サブサーバー名	string	サブサーバー名。
文字列ブロック タイプ	uint32	サブサーバー 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。
サブサーバー ベンダー名	string	サブサーバー ベンダーの名前。
文字列ブロック タイプ	uint32	サブサーバー 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ー バージョンのバイト数を加えたサブサーバー バージョン文字列データ ブロックのバイト数。
サブサーバー バージョン	string	サブサーバー長

表 4-45　フル サブサーバー 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	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（variable）	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+（4-119 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（variable）	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+（4-119 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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。

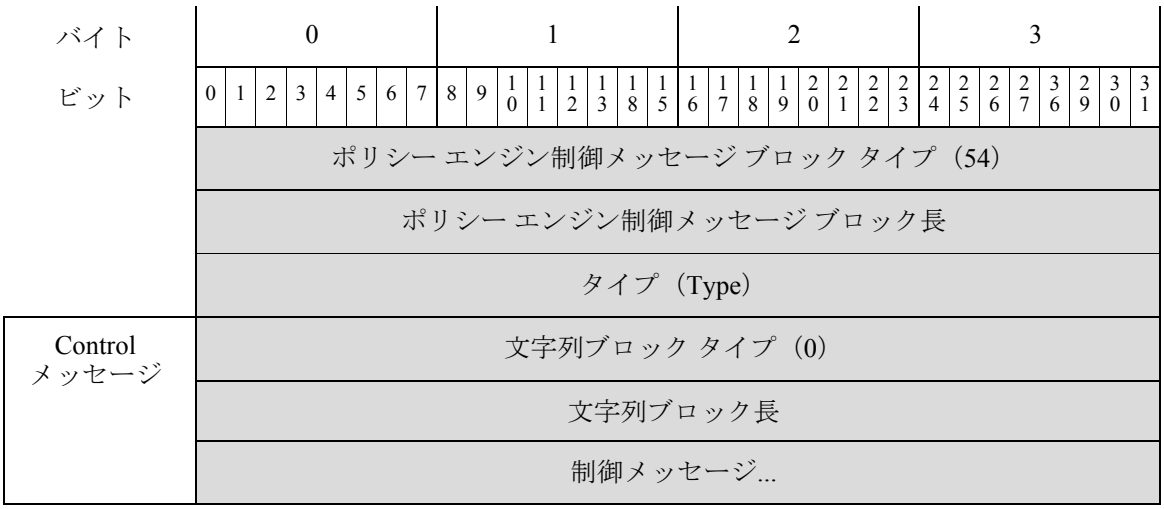
表 4-46　　オペレーティング システムのデータ ブロック 3.5+ のフィールド

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 4-47　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

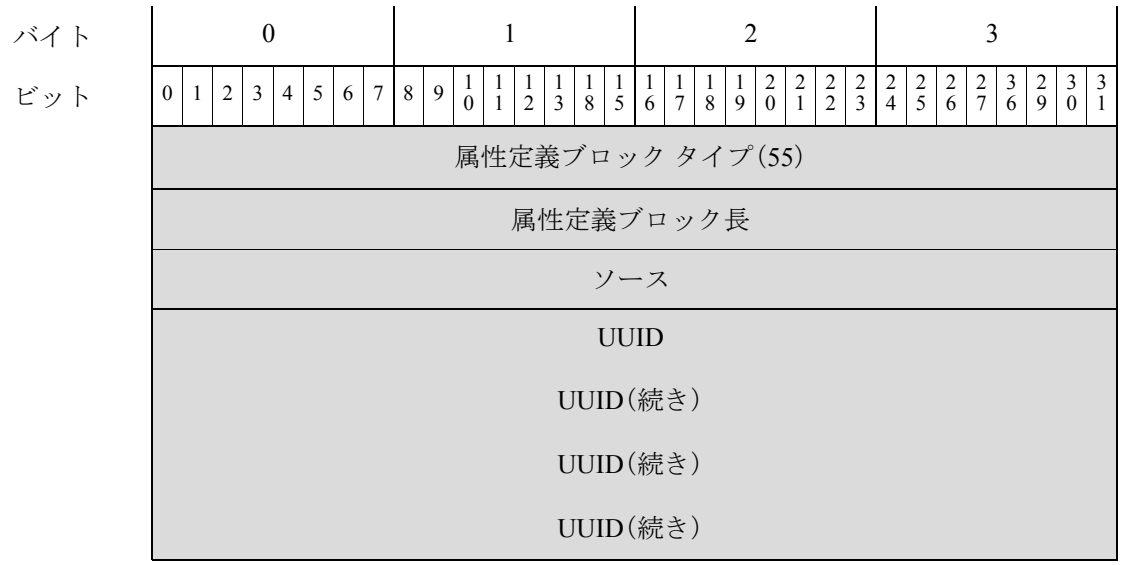
フィールド	データタイプ	説明
ポリシー エンジン制御メッセージ ブロック タイプ	uint32	ポリシー エンジン制御メッセージ データ ブロックを開始します。この値は常に 54 です。
ポリシー エンジン制御メッセージ長さ	uint32	ポリシー エンジン制御ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のポリシー エンジン制御データのバイト数を加えたポリシー エンジン制御メッセージ データ ブロックの合計バイト数。
タイプ	uint32	イベントのポリシーのタイプを示します。
文字列ブロック タイプ	uint32	制御メッセージを含む文字列データ ブロックを開始します。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（4-59 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。



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 4-48　　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。

表 4-48　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
ソース	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）、ユーザー、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（Name）]	string	属性定義名。
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。

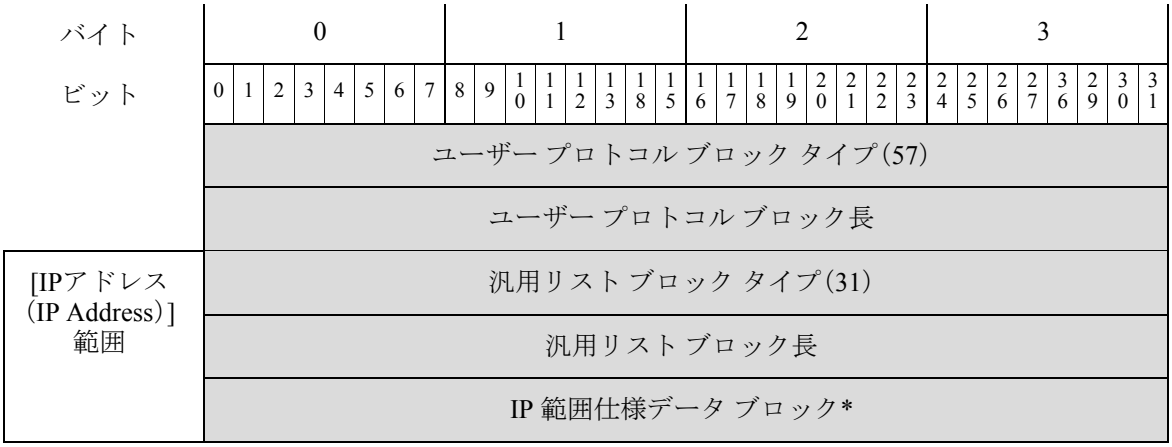
表 4-48　属性定義データ ブロックのフィールド（続き）

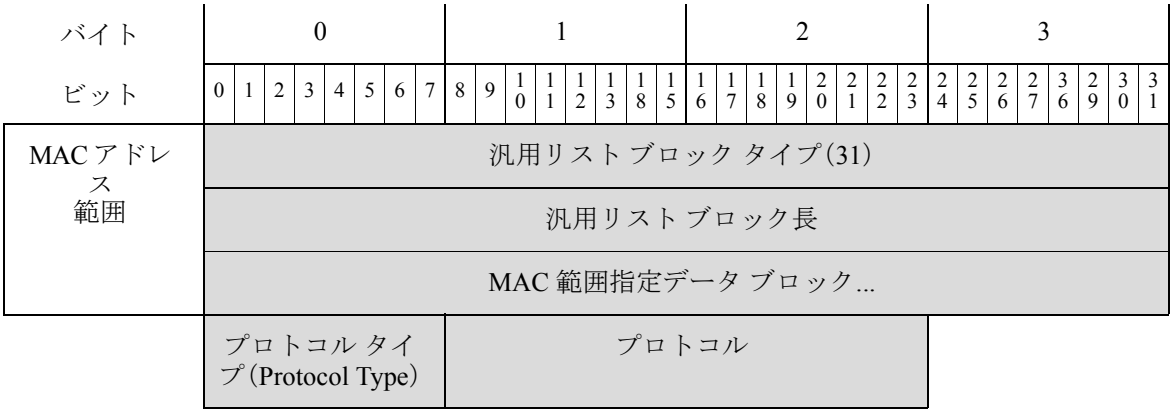
フィールド	データタイプ	説明
属性リスト項目ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトに属性リスト項目のバイト数を加えた属性リスト項目文字列データ ブロックのバイト数。
属性リスト項目	変数（variable）	属性リスト項目データ ブロック（4-87 ページ）に記載の属性リスト項目データ。
リスト ブロック タイプ	uint32	ホストの IP アドレスを属性とともに伝える属性アドレス データ ブロックで構成されるリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、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。
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（variable）	属性アドレス データ ブロック 5.2+（4-84 ページ）に記載されている属性アドレス データ。

ユーザー プロトコル データ ブロック

ユーザー 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。ユーザー 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、ユーザー プロトコル データ ブロックの基本構造です。





次の表では、ユーザー 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 4-49　ユーザー 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
ユーザー プロトコル ブロック タイプ	uint32	ユーザー 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。
ユーザー プロトコル ブロック長	uint32	ユーザー 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、後続のユーザー プロトコル データのバイト数を加えたユーザー 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（variable）	ユーザー入力の 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（4-101 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（variable）	ユーザー入力の 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（4-104 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+ のユーザー クライアント アプリケーション データ ブロック

ユーザー 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ーの 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 7.2 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。ユーザー 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。ブロック タイプ 59 を置換します。

次の図は、ユーザー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ユーザー クライアント アプリケーション ブロック タイプ（138）																																
	ユーザー クライアント アプリケーション ブロック長																																
IP Range 仕様	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...																																
	ペイロード タイプ（Payload Type）																																
	Web アプリケーション ID																																

次の表は、ユーザー 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 4-50　ユーザー 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
ユーザー クライアント アプリケーション ブロック タイプ	uint32	ユーザー 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。
ユーザー クライアント アプリケーション ブロック長	uint32	ユーザー 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（ユーザー 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ー 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（variable）	ユーザー入力の 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（4-101 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）。

ユーザー クライアント アプリケーション リスト データ ブロック

ユーザー 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ーの 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。ユーザー 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、ユーザー 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ユーザー クライアント アプリケーション ブロック タイプ(60)																															
	ユーザー クライアント アプリケーション ブロック長																															
	ソース タイプ																															
	ソース																															
ユーザー クライアント アプリケーション リスト 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																															
	ユーザー クライアント アプリケーション リスト データ ブロック...																															

次の表では、ユーザー 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 4-51　ユーザー 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
ユーザー 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	ユーザー 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。
ユーザー クライアント アプリケーション リスト ブロック長	uint32	ユーザー 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、後続のユーザー 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ー 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 • ユーザーがクライアント 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	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)、ユーザー、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 4-51　ユーザー 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（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。
ユーザー クライアント アプリケーション ブロック	変数（variable）	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ー クライアント アプリケーション データ ブロック。ユーザー 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+ のユーザー クライアント アプリケーション データ ブロック（4-98 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、ユーザー プロトコル、ユーザー クライアント アプリケーション、アドレス指定、ユーザー製品、ユーザー サーバー、ユーザー ホスト、ユーザー脆弱性、ユーザー重要度、ユーザー属性値データ 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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。

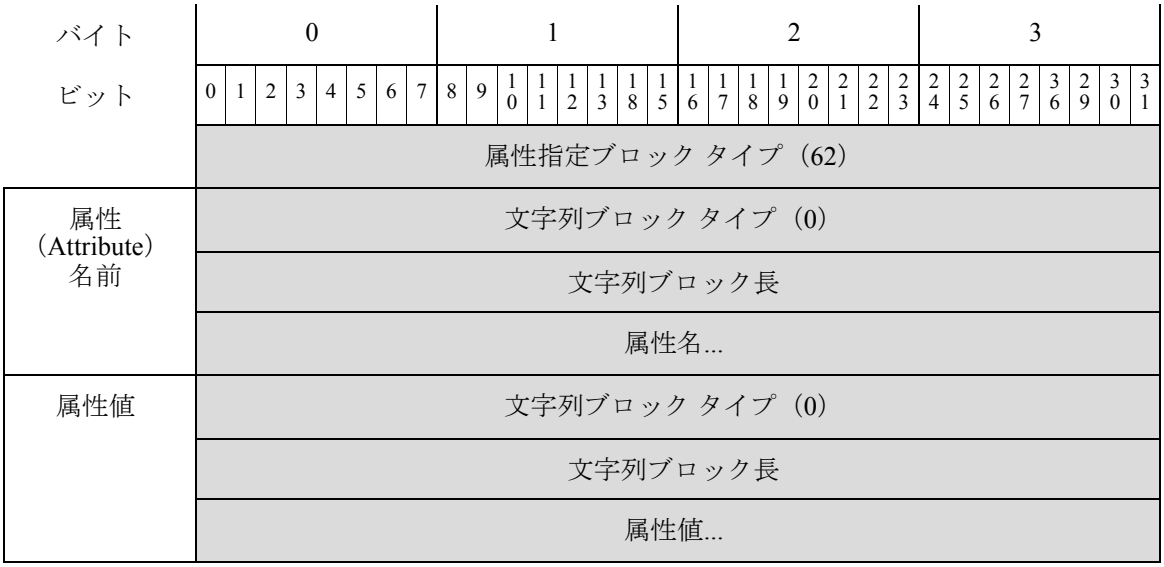
表 4-52　IP アドレス範囲データ ブロックのフィールド

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。



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 4-53　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。

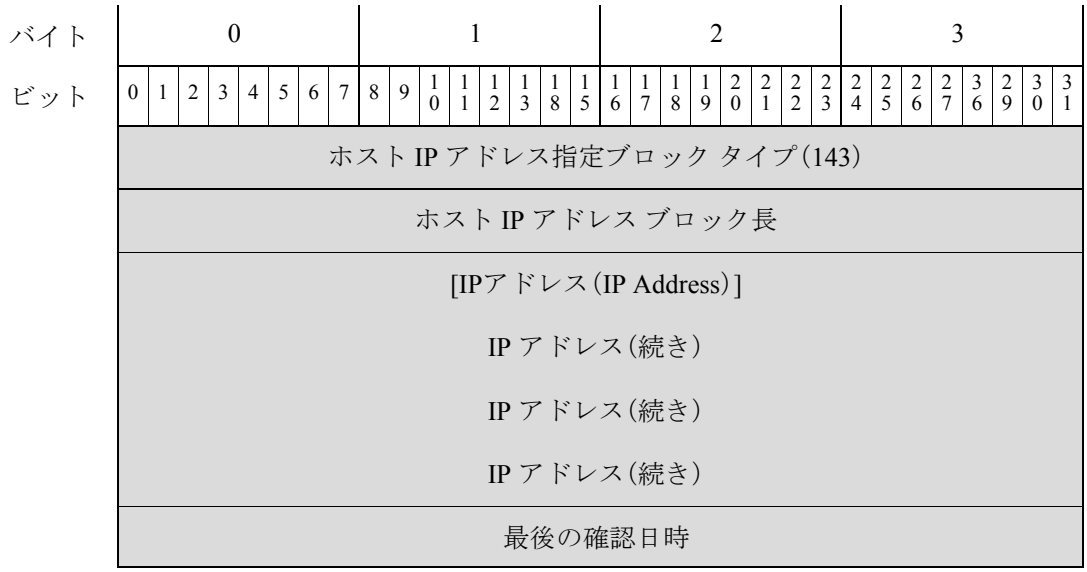
表 4-53　　属性指定データ ブロックのフィールド（続き）

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（Attribute Value）	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（Attribute Name）	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、ユーザー プロトコル、アドレス指定、ユーザー 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 4-54　　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(IP Address)]	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、ユーザー プロトコル、アドレス指定、ユーザー 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 4-55　　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。

表 4-55　MAC 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	データタイプ	説明
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。

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。

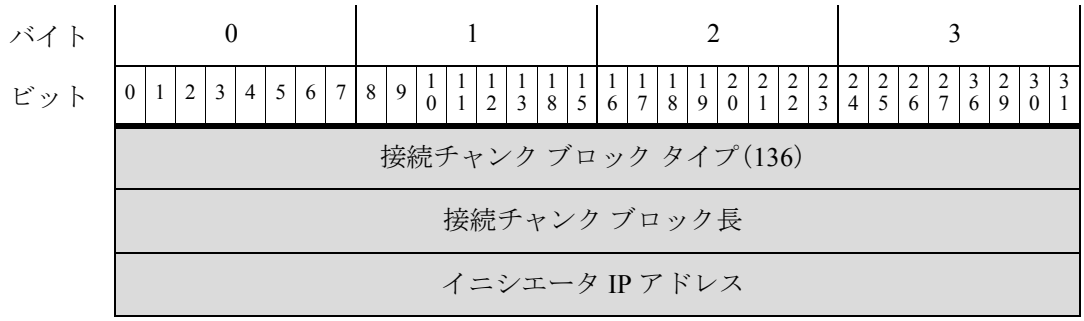
表 4-56　アドレス指定データ ブロックのフィールド

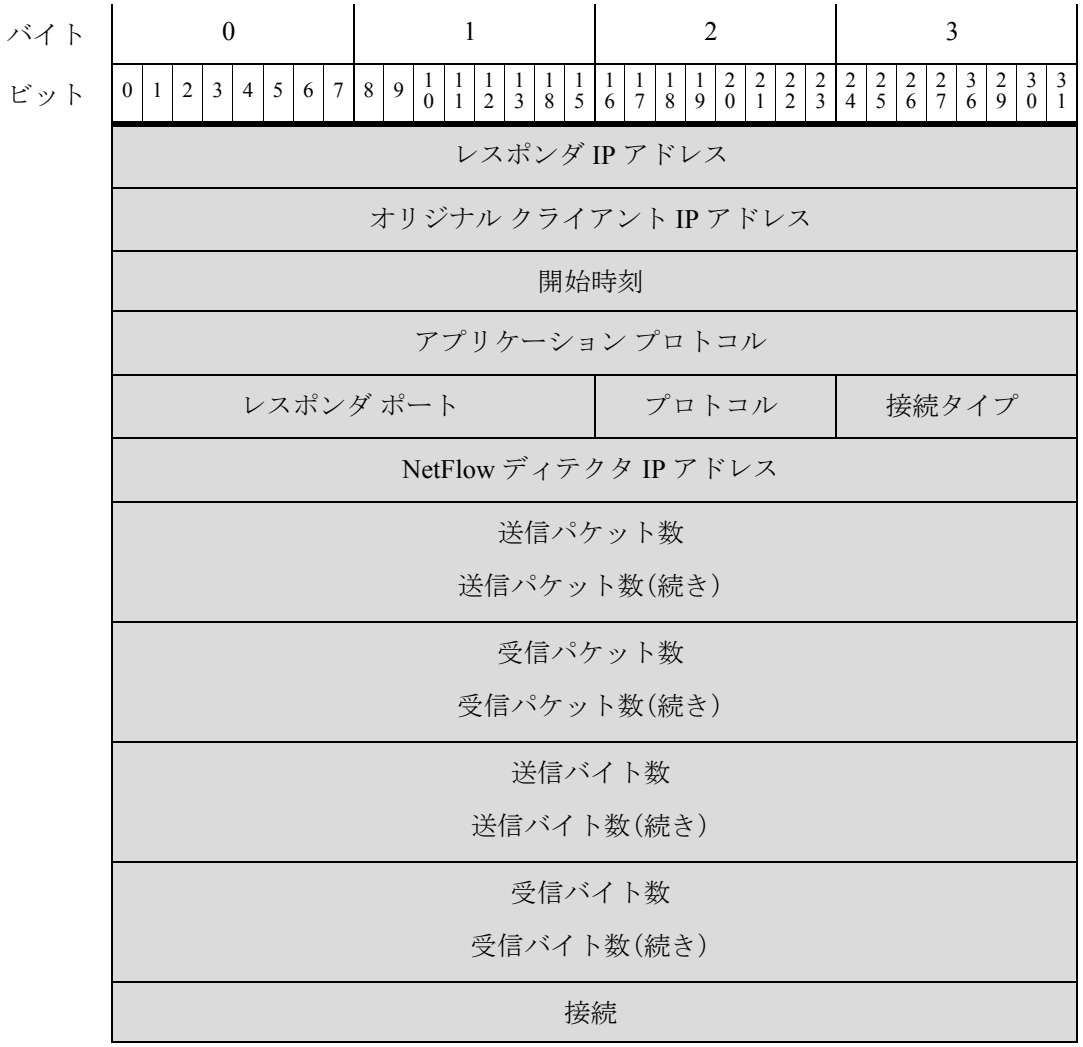
フィールド	バイト数	説明
アドレス指定データ ブロック タイプ	uint32	アドレス指定データ ブロックを開始します。この値は常に 64 です。
アドレス指定ブロック長	uint32	アドレス指定ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のアドレス指定データのバイト数を加えたアドレス指定データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック 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（variable）	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（4-101 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。
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（variable）	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（4-104 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 4-57　　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。

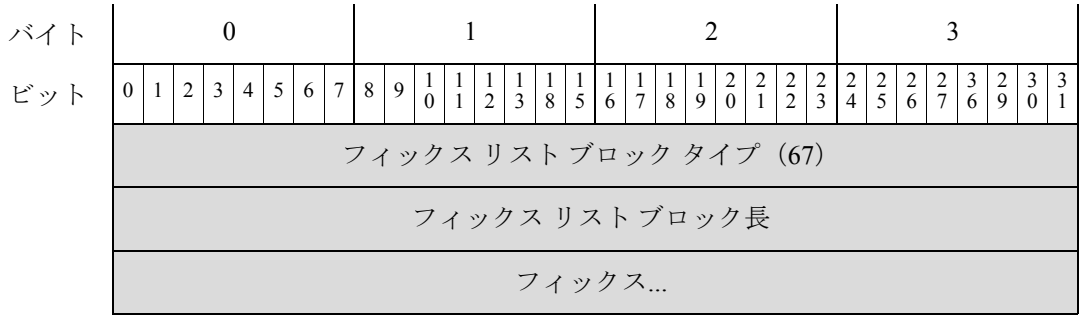
表 4-57　接続チャンク データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
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	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	ユーザー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。
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、ユーザー製品データ 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 4-58　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。

ユーザー サーバー データ ブロック

ユーザー サーバー データ ブロックには、ユーザー入力のサーバーの詳細を格納します。ユーザー サーバー 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 76 です。

次の図は、ユーザー サーバー データ ブロックの基本構造です。

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

表 4-59　ユーザー サーバー データ ブロックのフィールド

フィールド	バイト数	説明
ユーザー サーバー データ ブロック タイプ	uint32	ユーザー サーバー データ ブロックを開始します。この値は常に 76 です。
ユーザー サーバー ブロック長	uint32	ユーザー サーバー 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、後続のユーザー サーバー データのバイト数を加えたユーザー サーバー データ ブロックの合計バイト数。

表 4-59　ユーザー サーバー 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。
IP アドレス範囲指定データ ブロック	変数（variable）	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。
[ポート（Port）]	uint16	サーバーで使用するポート。
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

ユーザー サーバー リスト データ ブロック

ユーザー サーバー リスト データ ブロックには、ユーザー入力のサーバー リスト データ ブロックを格納します。ユーザー サーバー 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、ユーザー サーバー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ユーザー サーバー リスト データ ブロック タイプ（77）																																
	ユーザー サーバー リスト ブロック長																																
	ソース タイプ																																
	ソース																																
ユーザー（User）サーバー 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																																
	ユーザー サーバー データ ブロック*																																

次の表では、ユーザー サーバー 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。

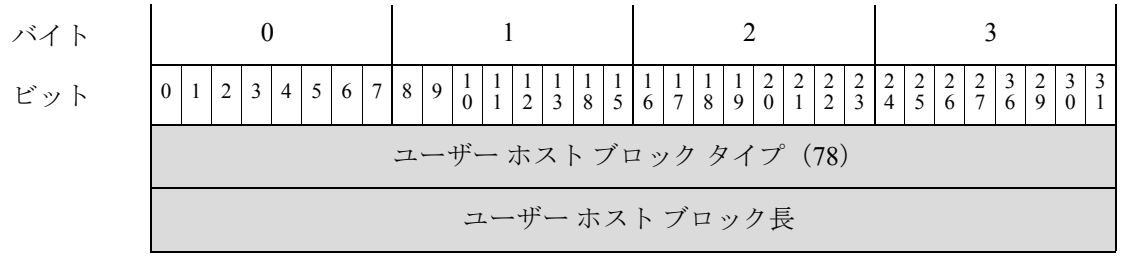
表 4-60　ユーザー サーバー リスト データ ブロックのフィールド

フィールド	バイト数	説明
ユーザー サーバー リスト データ ブロック タイプ	uint32	ユーザー サーバー 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。
ユーザー サーバー リスト ブロック長	uint32	ユーザー サーバー 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、後続のユーザー サーバー リスト データのバイト数を加えたユーザー サーバー 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）がサーバー データを検出した場合、0 • ユーザーがサーバー データを提供した場合、1 • サードパーティ スキャナがサーバー 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 ツールでサーバー データを提供した場合、3
ソース	uint32	サーバー 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）、ユーザー、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。
ユーザー サーバー データ ブロック	変数（variable）	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ー サーバー データ ブロック。

ユーザー ホスト データ ブロック 4.7+

ユーザー ホスト データ ブロックは、ユーザー追加/削除ホスト メッセージ（4-57 ページ）で使用し、ホスト範囲、ユーザー ホスト入力イベントから得られるユーザー 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。ユーザー 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、ユーザー 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																															
	ソース タイプ																															

次の表では、ユーザー 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 4-61　　ユーザー 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
ユーザー ホスト ブロック タイプ	uint32	ユーザー 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。
ユーザー ホスト ブロック長	uint32	ユーザー 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、後続のユーザー ホスト データのバイト数を加えたユーザー 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（variable）	ユーザー入力の 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（4-101 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（variable）	ユーザー入力の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（4-104ページ） を参照してください。

表 4-61　ユーザー 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	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）、ユーザー、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 • ユーザーがホスト 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

ユーザー脆弱性変更データ ブロック 4.7+

ユーザー脆弱性変更データ 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ー、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。ユーザー脆弱性変更データ 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。前のユーザー脆弱性変更データ 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、ユーザー脆弱性変更メッセージで使用します（バージョン4.6.1+ のユーザー設定脆弱性メッセージ（4-57 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ユーザー脆弱性変更データ ブロック タイプ（80）																																
	ユーザー脆弱性変更ブロック長																																
	ソース																																
	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																																
	ユーザー脆弱性データ 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 4-62　ユーザー脆弱性変更データ ブロックのフィールド

フィールド	バイト数	説明
ユーザー脆弱性変更データ ブロック タイプ	uint32	ユーザー脆弱性変更データ ブロックを開始します。この値は常に 80 です。
ユーザー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ー脆弱性変更データ ブロックの合計バイト数。
ソース	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）、ユーザー、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 • ユーザー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（Type）	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。
ユーザー脆弱性データ ブロック	変数（variable）	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ー脆弱性データ ブロック。詳細については、ユーザー脆弱性データ ブロック 5.0+（4-169 ページ）を参照してください。

ユーザー重要度変更データ ブロック 4.7+

ユーザー重要度データ 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ーの 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。ユーザー重要度データ 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。前のユーザー重要度データ 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。

ユーザー設定ホスト重要度メッセージ（4-58 ページ） にあるように、ユーザー設定ホスト重要度メッセージでは、ユーザー重要度データ ブロックを使用します。

次の図は、ユーザー重要度データ ブロックの基本構造です。

次の表では、ユーザー重要度データ ブロックのフィールドについて説明します。

表 4-63　ユーザー重要度データ ブロックのフィールド

フィールド	バイト数	説明
ユーザー重要度データ ブロック タイプ	uint32	ユーザー重要度データ ブロックを開始します。この値は常に 81 です。
ユーザー重要度ブロック長	uint32	ユーザー重要度ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザー重要度データのバイト数を加えたユーザー重要度データ 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（variable）	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	uint32	ユーザー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）、ユーザー、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 4-63　ユーザー重要度データ 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）がユーザー重要度値を提供した場合、0 • ユーザーがユーザー重要度値を提供した場合、1 • サードパーティ スキャナがユーザー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 ツールでユーザー重要度値を提供した場合、3
重要度値	uint32	ユーザーの重要度値。

ユーザー属性値データ ブロック 4.7+

ユーザー属性値データ 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、ユーザーの 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。ユーザー属性値データ 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。前のユーザー属性値データ 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、ユーザー属性値データ ブロックの構造です。

次の表では、ユーザー属性値データ ブロックのフィールドについて説明します。

表 4-64　ユーザー属性値データ ブロックのフィールド

フィールド	バイト数	説明
ユーザー属性値データ ブロック タイプ	uint32	ユーザー属性値データ ブロックを開始します。この値は常に 82 です。
ユーザー属性値ブロック長	uint32	ユーザー属性値ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザー属性ブロック 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（variable）	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	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）、ユーザー、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）がユーザー属性を提供した場合、0 • ユーザーが属性値を提供した場合、1 • サードパーティ スキャナがユーザー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 ツールでユーザー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（variable）	バイナリ形式でユーザー属性値を格納します。

ユーザー プロトコル リスト データ ブロック 4.7+

ユーザー 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ーの 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。ユーザー 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。ユーザー プロトコル データ ブロックの詳細については、ユーザー プロトコル データ ブロック（4-96 ページ）を参照してください。

ユーザー プロトコル メッセージ（4-60 ページ）にあるように、ユーザー プロトコル メッセージでは、ユーザー 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、ユーザー プロトコル リスト データ ブロックの基本構造です。

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 4-65　ユーザー 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
ユーザープロトコル リスト ブロック タイプ	uint32	ユーザー 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。
ユーザープロトコル リスト ブロック長	uint32	ユーザー 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、後続のユーザー プロトコル リスト データのバイト数を加えたユーザー プロトコル リスト データ ブロックの合計バイト数。

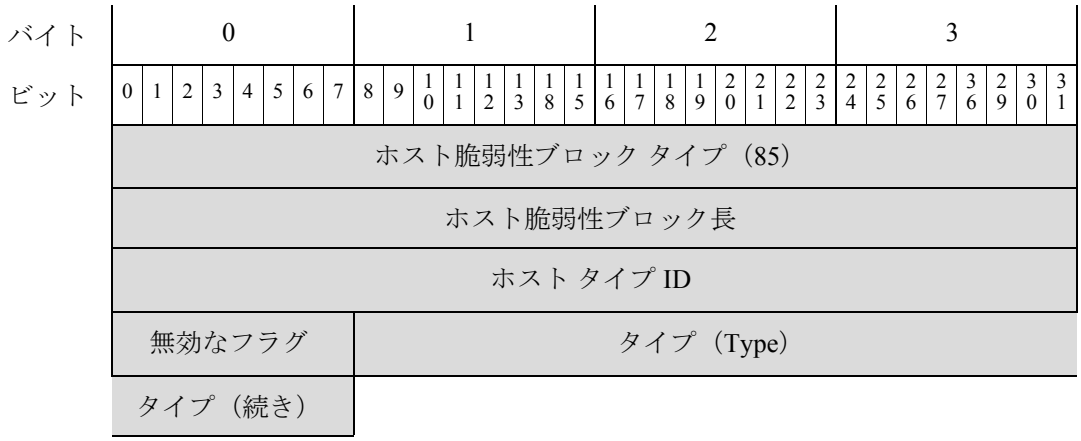
表 4-65　ユーザー プロトコル リスト データ ブロックのフィールド（続き）

フィールド	バイト数	説明
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 • ユーザーがプロトコル 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	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）、ユーザー、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。
ユーザー プロトコル データ ブロック	変数（variable）	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ー 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 サーバー、フル サブサーバー 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 4-66　　ホスト脆弱性データ ブロックのフィールド

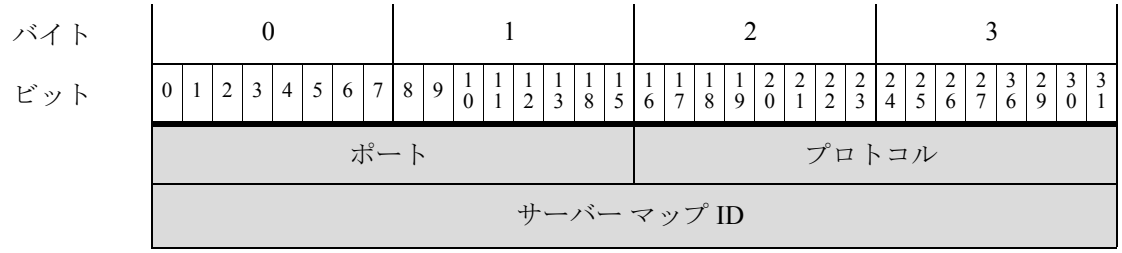
フィールド	データタイプ	説明
ホスト脆弱性ブロック タイプ	uint32	ホスト脆弱性データ ブロックを開始します。この値は常に 85 です。
ホスト脆弱性ブロック長	uint32	ホスト脆弱性ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のホスト脆弱性データのバイト数を加えたホスト脆弱性データ ブロックの合計バイト数。
ホスト タイプ ID	uint32	脆弱性の ID 番号。
無効なフラグ	uint8	脆弱性がそのホストで有効であるかどうかを示す値。
タイプ（Type）	uint32	脆弱性のタイプ。

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 システムやサーバー 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（ユーザー、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（4-62 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	アイデンティティ データ ブロック タイプ（94）																															
	アイデンティティ データ ブロック長																															
	アイデンティティ データ送信元タイプ																															
	アイデンティティ データ送信元 ID																															
アイデンティティ UUID	アイデンティティ UUID アイデンティティ UUID（続き） アイデンティティ UUID（続き） アイデンティティ UUID（続き）																															



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 4-67　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。
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 • ユーザー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）、ユーザー、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（Port）]	uint16	アイデンティティがサーバー アイデンティティの場合、サーバー データを含むパケットで使用するポートを示します。

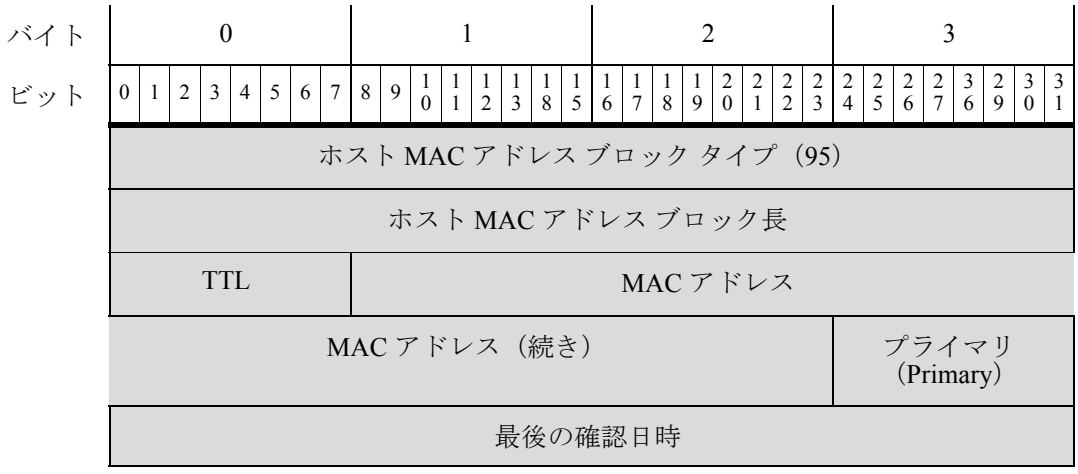
表 4-67　アイデンティティ データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
プロトコル	uint16	アイデンティティがサーバー アイデンティティの場合、ネットワーク プロトコルの IANA 番号またはサーバー 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
サーバーマップ ID	uint32	アイデンティティがサーバー アイデンティティの場合、サーバーの ID、ベンダー、バージョンの組み合わせを表すサーバー 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。

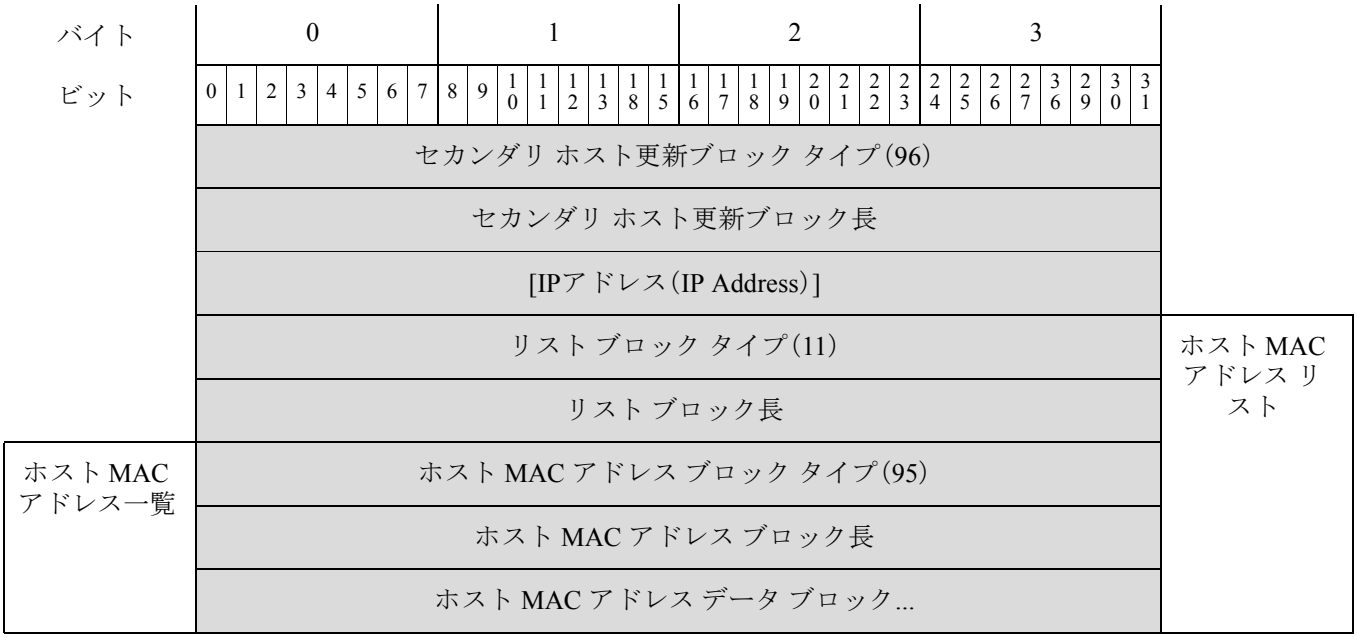
表 4-68　　ホスト MAC アドレス データ ブロックのフィールド

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（Primary）	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。

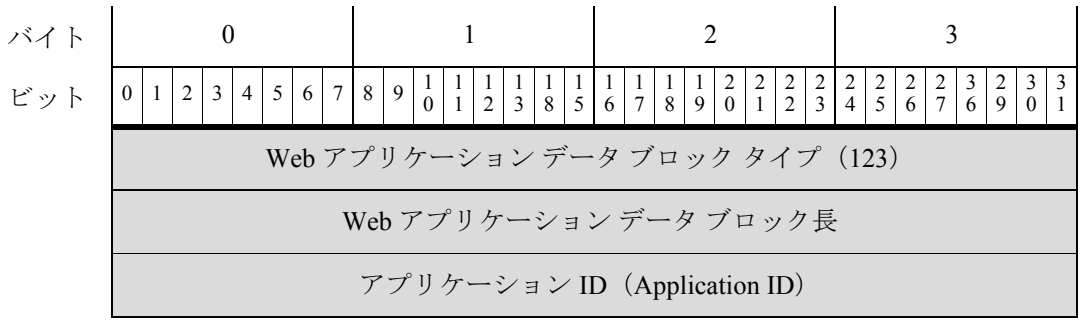
表 4-69　セカンダリ ホスト更新データ ブロックのフィールド

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(IP Address)]	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。
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 4-70　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（Application 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 7.1+

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。TLS Confidence フィールド、クライアント アプリケーション ディテクタ フィールド、および NAT フィールドが追加されました。バージョン 7.0 以降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 174 です。これはブロック タイプ173 接続統計データ ブロック 7.0（B-292 ページ） に置き換わります。

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 16 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（2-15 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。

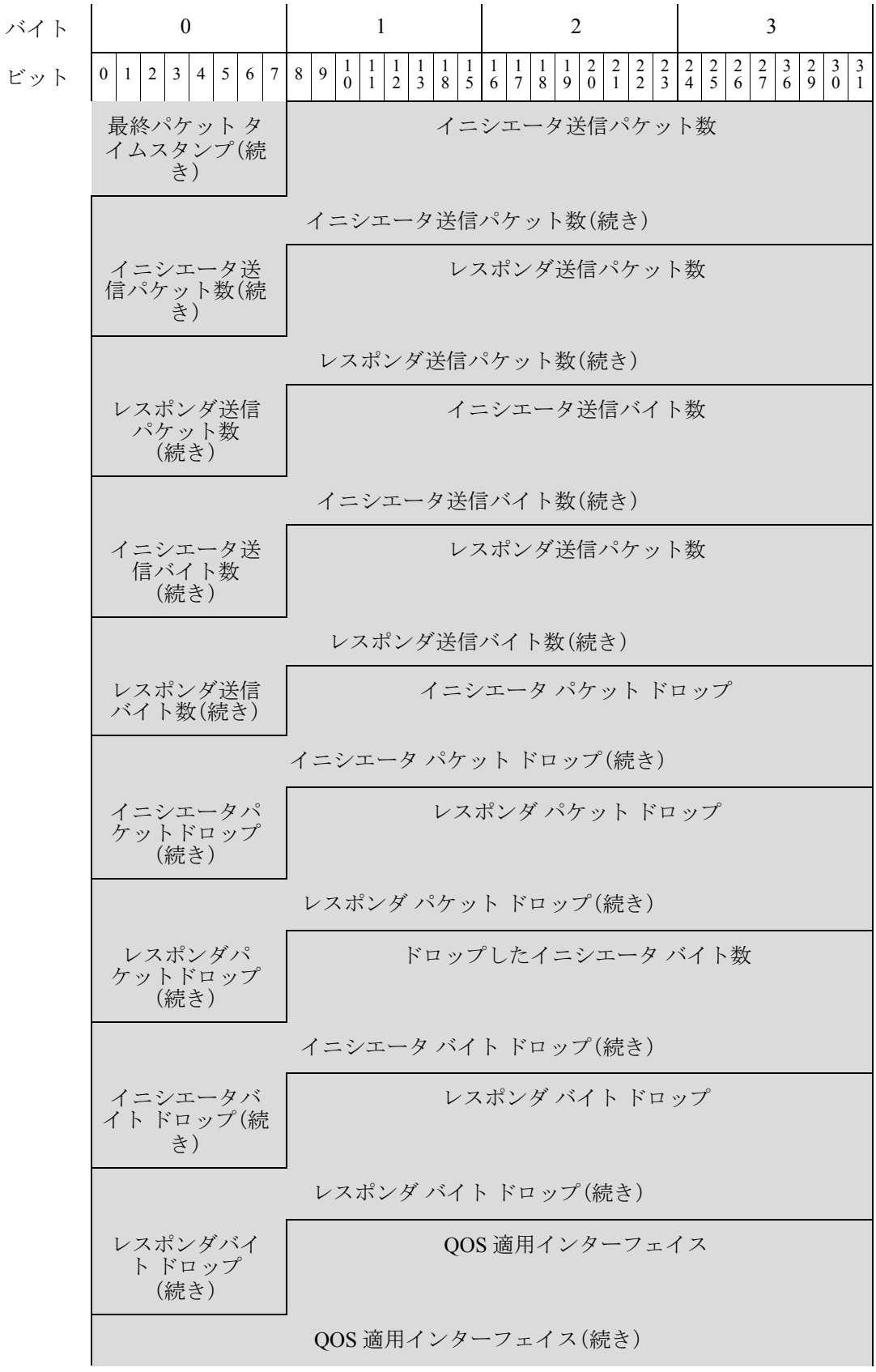
接続統計データ メッセージの詳細については、接続統計データ メッセージ（4-56 ページ）を参照してください。

次の図は、7.1+ の接続統計データ ブロックの形式です。

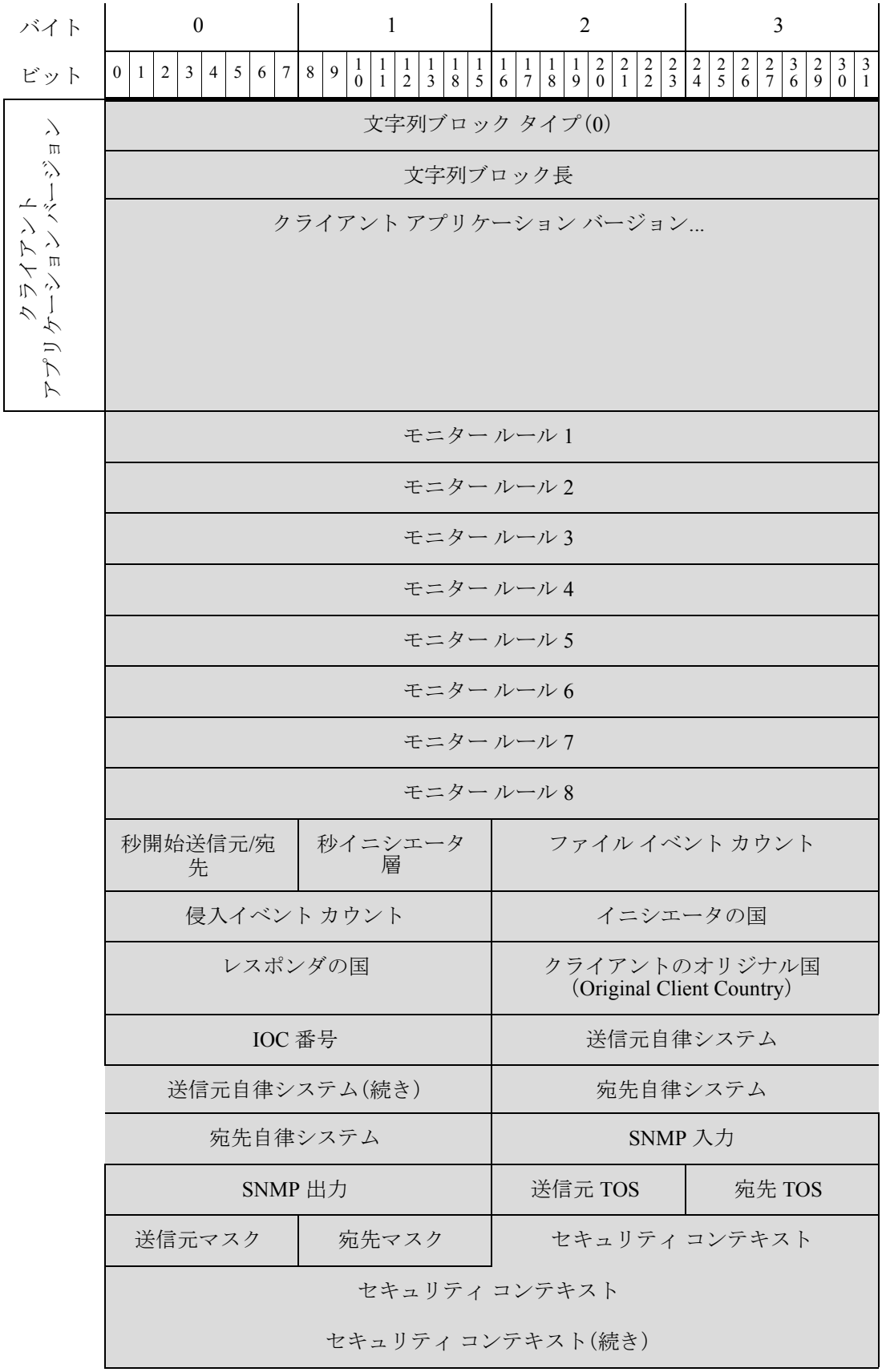
7

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
接続統計データ ブロック タイプ（174）																																
接続統計データ ブロック長																																
デバイスID（Device 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																																
レスポンダ IP アドレス（続き）																																

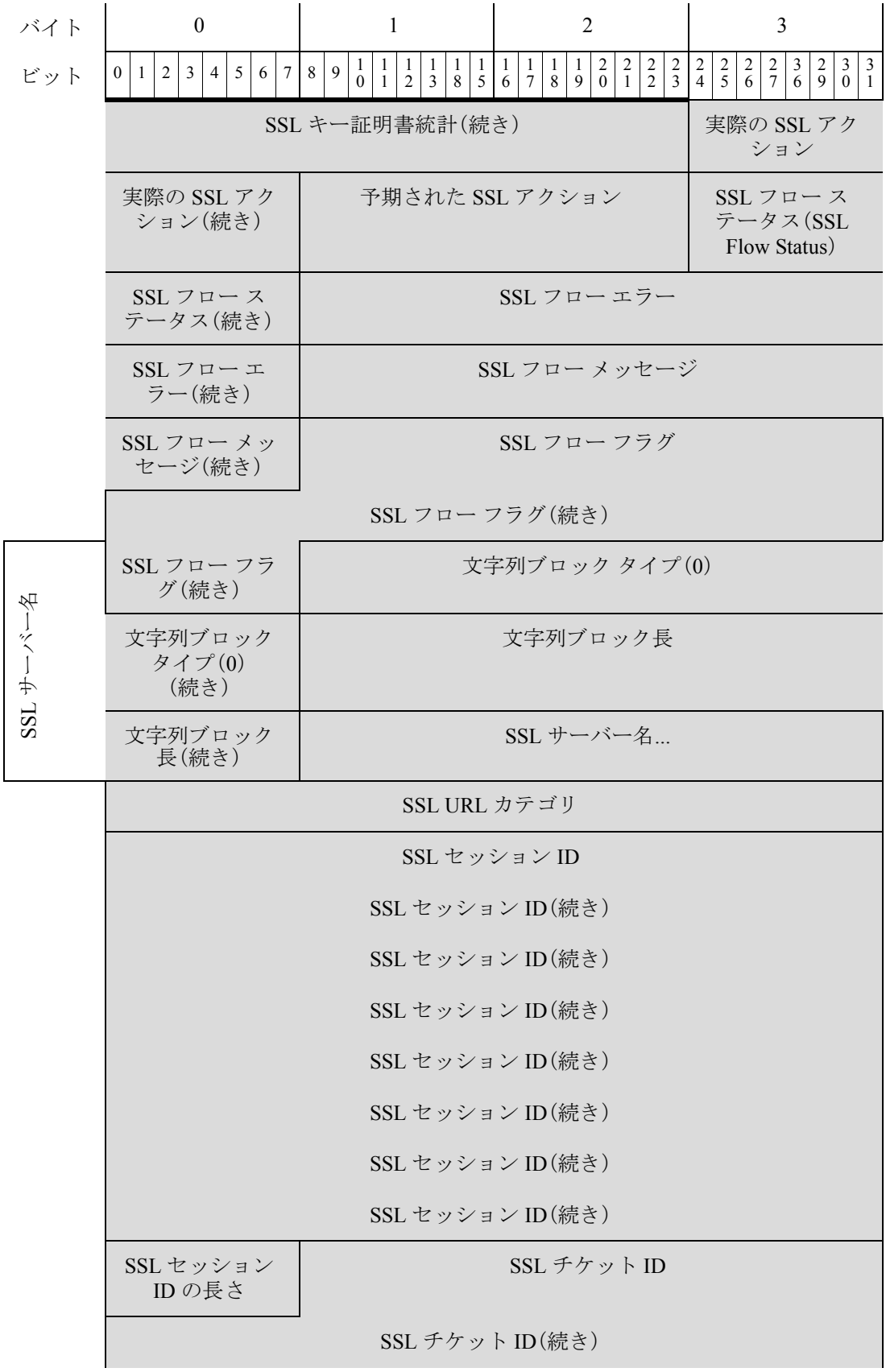
バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
レスポンダ IP アドレス（続き）																																
レスポンダ IP アドレス（続き）																																
オリジナル クライアント IP アドレス																																
オリジナル クライアント IP アドレス（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																																
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																																
トンネル 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（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																							

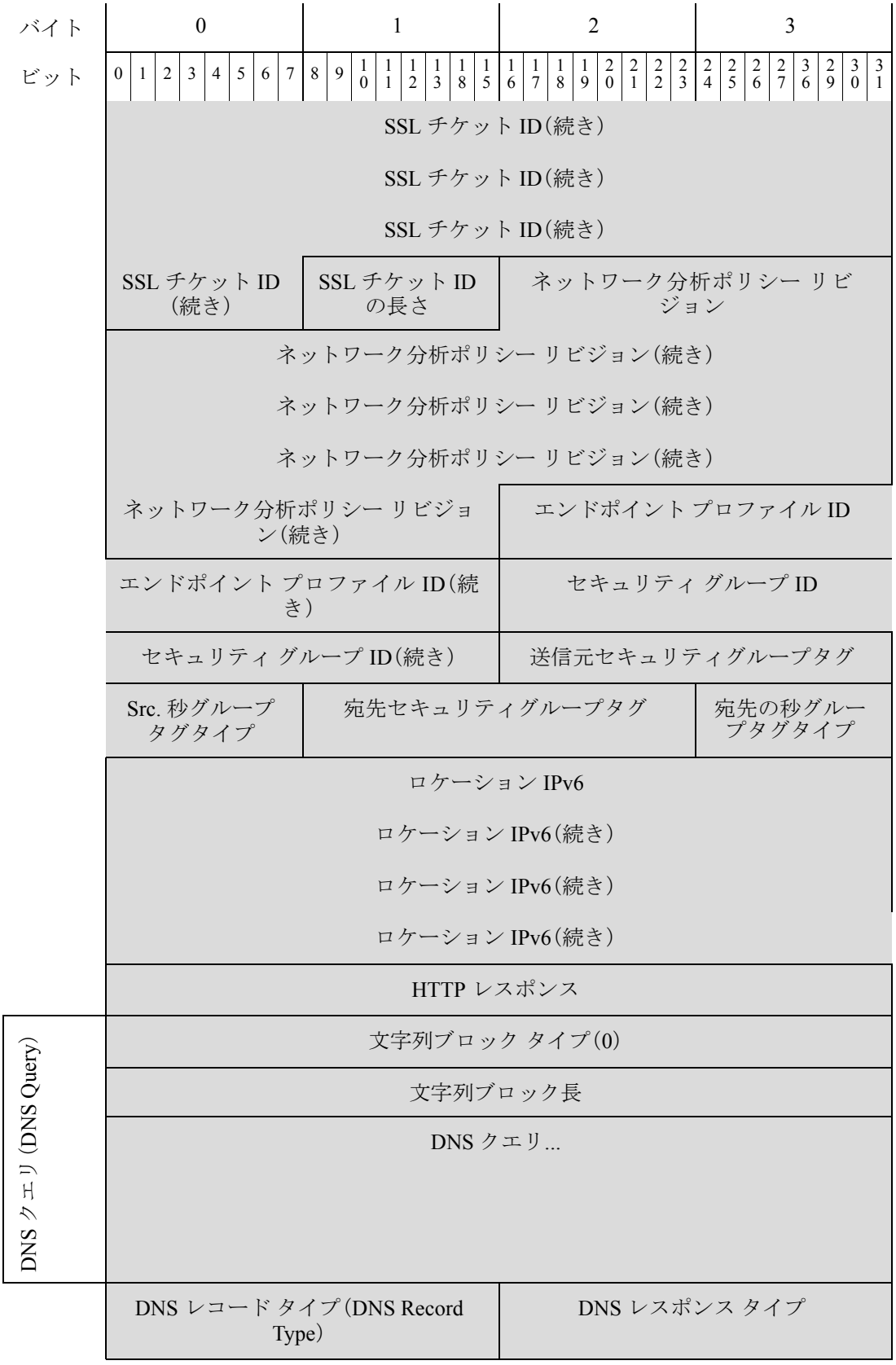

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
最終パケット タイムスタンプ(続き)
イニシエータ送信パケット数
イニシエータ送信パケット数(続き)
イニシエータ送信パケット数(続き)
レスポンダ送信パケット数
レスポンダ送信パケット数(続き)
レスポンダ送信パケット数(続き)
イニシエータ送信バイト数
イニシエータ送信バイト数(続き)
イニシエータ送信バイト数(続き)
レスポンダ送信パケット数
レスポンダ送信バイト数(続き)
レスポンダ送信バイト数(続き)
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)

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	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）								ユーザー ID（User ID）																							
	ユーザー 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）																							
クライアント URL	文字列ブロック タイプ（続き）								文字列ブロック長																							
クライアント URL	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 [名前（Name）]	文字列ブロック タイプ（0）																															
NetBIOS [名前（Name）]	文字列ブロック長																															
NetBIOS [名前（Name）]	NetBIOS 名...																															

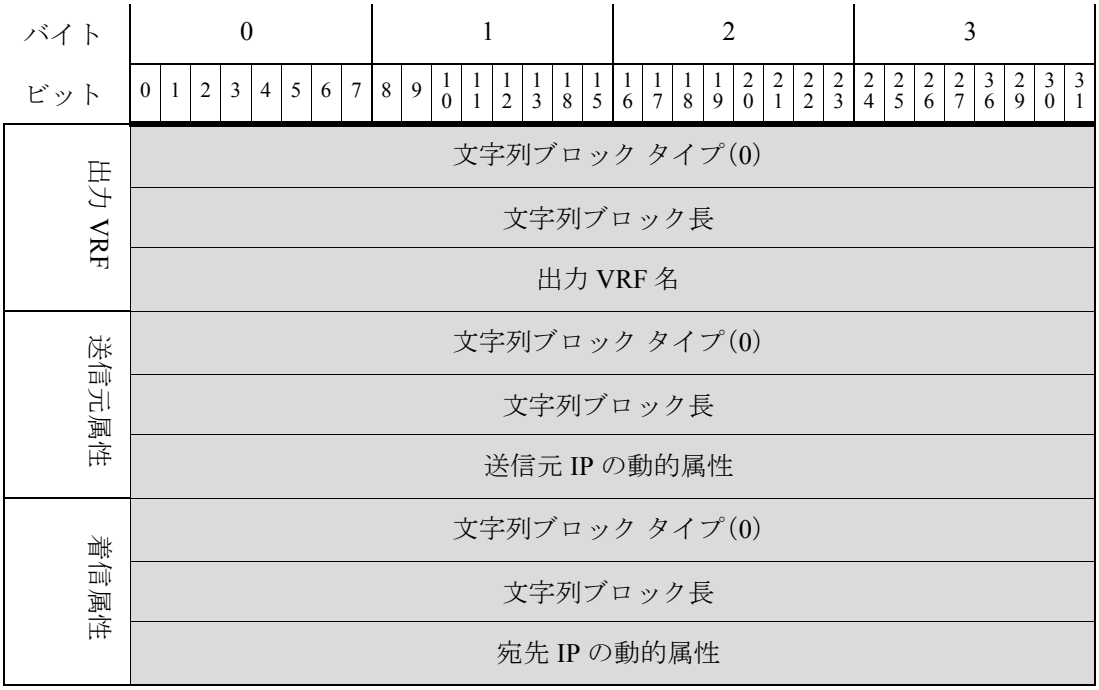

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
クライアント アプリケーション バージョン
文字列ブロック タイプ(0)
文字列ブロック長
クライアント アプリケーション バージョン...
モニター ルール 1
モニター ルール 2
モニター ルール 3
モニター ルール 4
モニター ルール 5
モニター ルール 6
モニター ルール 7
モニター ルール 8
秒開始送信元/宛先
秒イニシエータ層
ファイル イベント カウント
侵入イベント カウント
イニシエータの国
レスポンダの国
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)


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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(Admin. 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...
ユーザー 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
ユーザー 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


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
SSL キー証明書統計(続き)
実際の SSL アクション
実際の SSL アクション(続き)
予期された SSL アクション
SSL フロー ステータス(SSL Flow Status)
SSL フロー ステータス(続き)
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)
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 サーバー名...
SSL サーバー名
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)


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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
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）
送信元セキュリティグループタグ
Src. 秒グループ タグタイプ
宛先セキュリティグループタグ
宛先の秒グループタグタイプ
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）
HTTP レスポンス
DNS クエリ（DNS Query）
文字列ブロック タイプ（0）
文字列ブロック長
DNS クエリ...
DNS レコード タイプ（DNS Record Type）
DNS レスポンス 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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
脅威インテリジェンスカテゴリ
TLS FP プロセス
文字列ブロック タイプ（0）
文字列ブロック長
TLS FP プロセス
プロセス信頼度
マルウェア信頼度
マルウェアインデックス
クライアントディテクタ
NAT イニシエータポート
NAT レスポンダポート
NAT イニシエータ IP アドレス
NAT イニシエータ IP アドレス（続き）
NAT イニシエータ IP アドレス（続き）
NAT イニシエータ IP アドレス（続き）
NAT レスポンダ IP アドレス
NAT レスポンダ IP アドレス（続き）
NAT レスポンダ IP アドレス（続き）
NAT レスポンダ IP アドレス（続き）
入力 VRF
文字列ブロック タイプ（0）
文字列ブロック長
入力 VRF 名



次の表では、7.1+ 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 4-71　接続統計データ ブロック 7.1+ 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	7.1+ の接続統計データ ブロックを開始します。値は常に 174 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（Device 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。

表 4-71　接続統計データ ブロック 7.1+ のフィールド （続き）

フィールド	データタイプ	説明
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	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	uint16	そのルールに対してユーザー 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（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。
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。

表 4-71　接続統計データ ブロック 7.1+ 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 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）。
ユーザー ID（User ID）	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 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。
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。
モニター ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニター ルールの ID。

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

フィールド	データタイプ	説明
モニター ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニター ルールの ID。
モニター ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニター ルールの ID。
モニター ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニター ルールの ID。
モニター ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニター ルールの ID。
モニター ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニター ルールの ID。
モニター ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニター ルールの ID。
モニター ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニター 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 アドレスが IP ブロックリストに一致しているかどうか。
セキュリティ インテリジェンス層	uint8	IP ブロ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。
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。

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

フィールド	データタイプ	説明
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（Admin. 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	ユーザー 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	ユーザー 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、およびユーザー エージェント フィールドのバイト数を含む)。
ユーザー エージェント	string	セッションのユーザー 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 サーバー証明書の 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 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

フィールド	データタイプ	説明
SSL サーバー証明書ステータス	uint32	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):サーバー証明書のステータスは評価されませんでした。 • 1(不明):サーバー証明書のステータスは判別できませんでした。 • 2(有効):サーバー証明書は有効です。 • 4(自己署名済み):サーバー証明書は自己署名です。 • 16(無効な発行者):サーバー証明書に無効な発行者があります。 • 32(無効な署名):サーバー証明書に無効な署名があります。 • 64(期限切れ):サーバー証明書は期限切れです。 • 128(まだ有効でない):サーバー証明書はまだ有効ではありません。 • 256(取り消し):サーバー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 4-71　接続統計データ ブロック 7.1+ 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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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 4-71　接続統計データ ブロック 7.1+ 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ー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 サーバー名文字列データ 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 サーバー名フィールドのバイト数を含む）。

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

フィールド	データタイプ	説明
SSL サーバー名	string	SSL Client Hello でサーバー名に指定された名前。
SSL URL カテゴリ	uint32	サーバー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ー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ーがセッション 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 によりユーザーに割り当てられた ID 番号。
送信元セキュリティグループタグ	uint16	接続の送信元のセキュリティグループタグ。
送信元セキュリティ グループ タグ タイプ	uint8	送信元セキュリティグループタグの割り当て方法: • 0:不明 • 1:インライン • 2:セッションディレクトリ • 3:Security Group Tag Exchange Protocol（SXP）
宛先セキュリティグループタグ	uint16	接続の宛先のセキュリティグループタグ。
宛先セキュリティ グループ タグ タイプ	uint8	宛先セキュリティグループタグの割り当て方法: • 0:不明 • 1:インライン • 2:セッションディレクトリ • 3:Security Group Tag Exchange Protocol（SXP）
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。

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

フィールド	データタイプ	説明
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 サーバー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。
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。接続に関連付けられた 3 つのセキュリティ インテリジェンス リストが存在する場合があります。
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。接続に関連付けられた 3 つのセキュリティ インテリジェンス リストが存在する場合があります。
脅威インテリジェンスカテゴリ	uint32	イベントに関連付けられた脅威インテリジェンスカテゴリ。これは、関連メタデータの脅威インテリジェンスリストにマップされます。
文字列ブロック タイプ	uint32	TLS フィンガープリントプロセ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	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの 8 バイトとTLS フィンガープリント プロセス フィールドのバイト数が含まれます。
TLS フィンガープリント プロセス	文字列	暗号化された可視性エンジンからの識別されたフィンガープリントのプロセス名ファミリ。
TLSFP プロセス信頼度	uint8	暗号化された可視性エンジン（EVE）が適切なプロセスを検出しているかを示す 0 ? 100% の範囲内の信頼値。たとえば、プロセス名が Firefox で、信頼スコアが 80% の場合、エンジンが検出したプロセスが Firefox であると 80% 信頼していることを示します。

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

フィールド	データタイプ	説明
TLSFP マルウェア信頼度	uint8	暗号化された可視性エンジン（EVE）によって検出されたプロセスにマルウェアが含まれていることを示す 0 ? 100% の範囲内の信頼値。マルウェア信頼度スコアが非常に高い場合（90% など）、[TLS fingerprint Process Name] フィールドには [Malware] と表示されます。
TLS FP マルウェアインデックス	uint8	暗号化された可視性エンジン（EVE）によって検出されたプロセスにマルウェアが含まれる確率のレベル。このフィールドは、マルウェア信頼スコアの値に基づいて、帯域（[Very High]、[High]、[Medium]、[Low]、または [Very Low]）を示します。
クライアントアプリケーション ディテクタ タイプ	uint8	このフィールドには、クライアントの検出元が表示されます。アプリケーションが暗号化されておらず、通常のロジックを使用して検出された場合は 0 になり、暗号化された可視性エンジンによって検出された場合は 1 になります。
NAT イニシエータポート	uint16	セッションイニシエータで使用されるポート。
NAT レスポンダポート	uint16	セッションレスポンダで使用されるポート番号。
NAT イニシエータ IP	uint8[16]	セッションイニシエータの NAT 変換後の IP アドレス。
NAT レスポンダ IP	uint8[16]	セッションレスポンダの NAT 変換後の IP アドレス。
文字列ブロックタイプ	uint32	入力 VRF 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。ブロックタイプとヘッダーフィールドの 8 バイト、および入力 VRF 名フィールドのバイト数が含まれています。
入力 VRF 名	文字列	トラフィックがネットワークに入るときに通過する仮想ルータ。
文字列ブロックタイプ	uint32	出力 VRF 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。ブロックタイプとヘッダーフィールドの 8 バイト、および出力 VRF 名フィールドのバイト数が含まれています。
出力 VRF 名	文字列	トラフィックがネットワークから出るときに通過する仮想ルータの名前。
文字列ブロックタイプ	uint32	送信元 IP の動的属性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。ブロックタイプとヘッダーフィールドの 8 バイト、および送信元 IP の動的属性フィールドのバイト数が含まれています。
送信元 IP の動的属性	文字列	送信元 IP アドレスに関連付けられた動的属性。

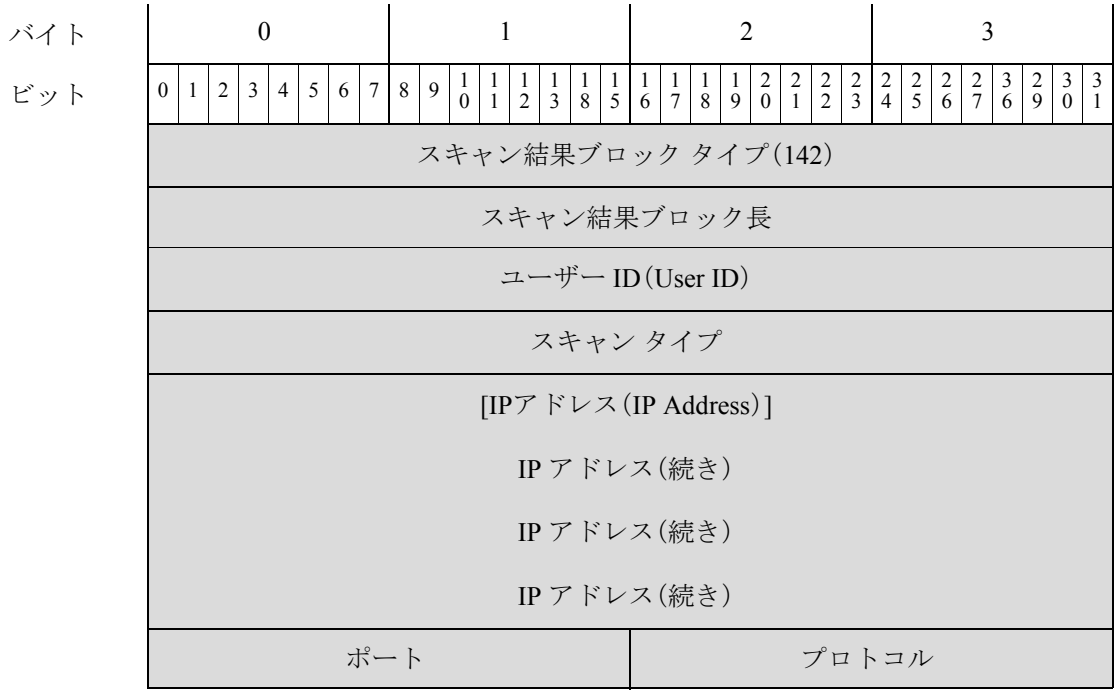
表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

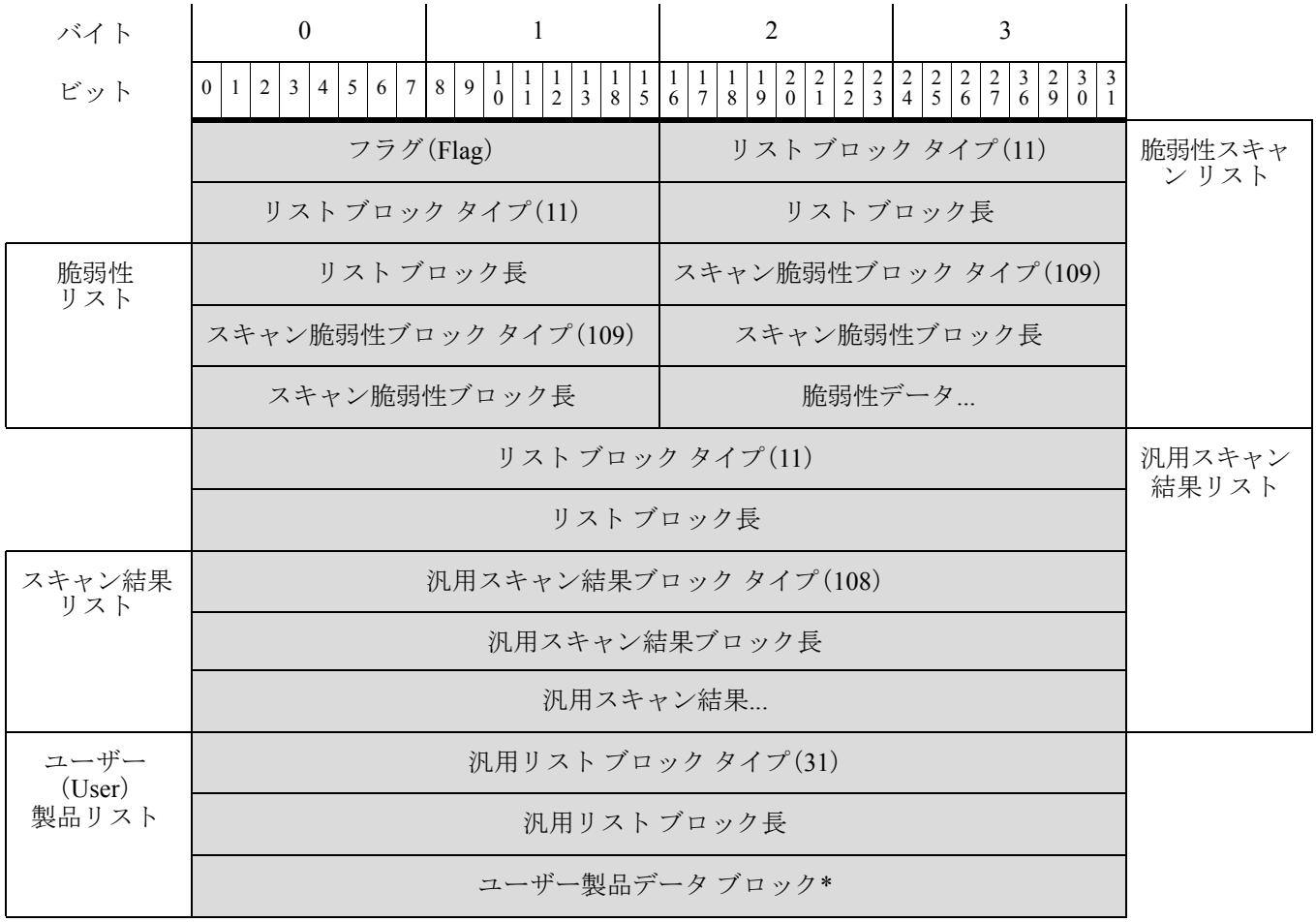
フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	宛先 IP の動的属性の名前を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの 8 バイト、および宛先 IP の動的属性フィールドのバイト数が含まれています。
宛先 IP の動的属性	文字列	宛先 IP アドレスに関連付けられた動的属性。

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 4-72　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)。
ユーザー ID (User ID)	uint32	スキャン結果をインポートしたユーザー、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ーのユーザー 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(IP Address)]	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(Port)]	uint16	結果の脆弱性の影響を受ける、サブサーバーで使用されるポート。

表 4-72　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
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ー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 4-72　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 アプリケーションからのホスト入力データを伝送するユーザー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。
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ー製品データ ブロックを含む）。
ユーザー製品データ ブロック*	変数（variable）	ホスト入力データを含むユーザー製品データ ブロック。このデータブロックの説明の詳細については、ユーザー製品データ ブロック 5.1+（4-183 ページ）を参照してください。

ホスト サーバー データ ブロック 4.10.0+

ホスト サーバー データ ブロックは、ホストで検出したサーバーに関する情報を伝えます。ここには、検出したサーバーごとにブロックとともに、サーバーが実行している 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 サーバー データ ブロックは、新規と変更された TCP サーバーと UDP サーバーのメッセージに含まれます。詳細については、サーバー メッセージ（4-48 ページ）を参照してください。ホスト サーバー 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 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 サーバー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 4-73　　ホスト サーバー 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
ホスト サーバー ブロック タイプ	uint32	ホスト サーバー 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 サーバー ブロック長	uint32	ホスト サーバー 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 バイト数を加えたホスト サーバー データ ブロックの合計バイト数。
[ポート(Port)]	uint16	サーバーが実行しているポート番号。
ヒット	uint32	サーバー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ー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ー情報データ 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。
サーバー情報データ ブロック*	変数(variable)	リスト ブロック長の最大バイト数を上限としたサーバー情報データ ブロック。詳細は、4.10.x、5.0 ～ 5.0.2 のサーバー情報データ ブロック (4-155 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(variable)	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 (4-124 ページ) を参照してください。

フル ホスト サーバー データ ブロック 4.10.0+

フル ホスト サーバー データ ブロックは、サーバー 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ーに関するサードパーティ脆弱性などサーバーに関する情報を伝えます。フル ホスト サーバー データ ブロックには、そのサーバーの各サブサーバーのフル サブサーバー情報データ 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 サーバーと UDP サーバーのフル ホスト サーバー データ ブロックを格納します。フル ホスト サーバー 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 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 サーバー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	フル サーバー ブロック タイプ(104)																																
	フル サーバー ブロック長																																
	[ポート(Port)]																	ヒット															
サブサーバー - 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 サーバー情報データ ブロック (106)*															
サブサーバー - ユーザー (User)	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 サーバー情報データ ブロック タイプ(106)*																																
サブサーバー - 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 サーバー情報データ ブロック(106)*																																
サブサーバー - Application	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 サーバー情報データ ブロック(106)*																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	信頼度																															
サーバー バナー	BLOB ブロック タイプ(10)																															
	BLOB ブロック長																															
	サーバー バナー 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 Application	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 サーバー 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　　フル ホスト サーバー 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 サーバー ブロック タイプ	uint32	フル サーバー データ ブロックを開始します。この値は常に 104 です。
フル サーバー ブロック長	uint32	フル サーバー 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、後続のフル サーバー データのバイト数を加えたフル サーバー データ ブロックの合計バイト数。
[ポート(Port)]	uint16	サーバー ポート番号。
ヒット	uint32	サーバーが受信したヒット数。

表 4-74　フル ホスト サーバー 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 タイプ	uint32	検出したサブサーバー 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。
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ー情報データ ブロックを含む汎用リスト データ ブロックのバイト数。
サブサーバー情報 - シスコ データ ブロック *	変数（variable）	シスコ が検出したホスト サーバーのサブサーバーに関する情報を含むフル サーバー情報データ 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 サーバー情報データ ブロック（4-158 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	ユーザーが追加したサブサーバー データを伝えるサブサーバー情報データ 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ー情報データ ブロックを含む汎用リスト データ ブロックのバイト数。
サブサーバー情報 - ユーザーが追加したデータ ブロック *	変数（variable）	ユーザーが検出したホスト サーバーのサブサーバーに関する情報を含むフル サーバー情報データ 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 サーバー情報データ ブロック（4-158 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ー データを伝えるサブサーバー情報データ 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ー情報データ ブロックを含む汎用リスト データ ブロックのバイト数。
サブサーバー情報 - スキャンで追加したデータ ブロック *	変数（variable）	スキャナが検出したホスト サーバーのサブサーバーに関する情報を含むフル サーバー情報データ 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 サーバー情報データ ブロック（4-158 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ー データを伝えるサブサーバー情報データ 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ー情報データ ブロックを含む汎用リスト データ ブロックのバイト数。
サブサーバー情報 - アプリケーションが追加したデータ ブロック *	変数（variable）	アプリケーションが検出したホスト サーバーのサブサーバーに関する情報を含むフル サーバー情報データ 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 サーバー情報データ ブロック（4-158 ページ）を参照してください。

表 4-74　フル ホスト サーバー 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
信頼度	uint32	フル サーバー 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。
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。
サーバー バナー データ	byte[*n*]	パケットの最初の *n* バイトがサーバー 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（variable）	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+（4-119 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 スキャナで得られ、すでに VDB に登録されている脆弱性に関する情報を格納したサードパーティ ホスト脆弱性データを伝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。
（サード パーティ /VDB）ホスト脆弱性データ ブロック*	変数（variable）	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+（4-119 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。

表 4-74　フル ホスト サーバー 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
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（variable）	サードパーティ スキャナで識別されたが VDB には登録されていない脆弱性に関する、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+（4-119 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。
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（variable）	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 のサーバー情報データ ブロック

サーバー情報データ ブロックは、サーバー ID、サーバー ベンダーとバージョン、送信元情報など、サーバーに関する情報を伝えます。サーバー情報データ 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。サーバー情報データ ブロックは、ホスト サーバー ブロックとフル ホスト サーバー 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 サーバー データ ブロック 4.10.0+（4-149 ページ）と フル ホスト サーバー データ ブロック 4.10.0+（4-151 ページ）を参照してください。

次の図は、サーバー情報データ 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
サーバー情報ブロック タイプ（105 | 117）																																
サーバー情報ブロック長																																
アプリケーション ID（Application ID）																																
文字列ブロック タイプ（0）																																
文字列ブロック長																																
サーバー ベンダー名文字列...																																

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	文字列ブロック タイプ（0）																																
	文字列ブロック長																																
	サーバー バージョン文字列...																																
	前回の使用（Last Used）																																
	ソース タイプ																																
	ソース																																
	リスト ブロック タイプ（11）																																
	リスト ブロック長																																
サブサーバー	サブサーバー ブロック タイプ（1）*																																
	サブサーバー ブロック長																																
	サブサーバー データ...																																

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

表 4-75　　サーバー情報データ ブロックのフィールド

フィールド	データタイプ	説明
サーバー情報ブロック タイプ	uint32	サーバー情報データ 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。
サーバー情報ブロック長	uint32	サーバー情報データ ブロックの合計バイト数。サーバー情報ブロック タイプ フィールドと長さフィールドの 8 バイト、サーバー 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（Application ID）	uint32	検出したサーバー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	サーバー 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 バイトにサーバー 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。
サーバー ベンダー名	string	サーバー ベンダーの名前。

表 4-75　サーバー情報データ 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	サーバー 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 バイトにサーバー バージョンのバイト数を加えたサーバー バージョン文字列データ ブロックのバイト数。
サーバー バージョン	string	サーバー バージョン
前回使用時刻	uint32	トラフィックで前回サーバー情報を使用した時刻を示します。
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）がサーバー データを提供した場合、0 • ユーザーがサーバー データを提供した場合、1 • サードパーティ スキャナがサーバー 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 ツールでサーバー データを提供した場合、3
ソース	uint32	サーバー 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）、ユーザー、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	サブサーバー 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ー 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。
サブサーバー ブロック タイプ	uint32	最初のサブサーバー データ ブロックを開始します。このデータ ブロックには、他のサブサーバー 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。
サブサーバー ブロック長	uint32	サブサーバー 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 バイト数を加えた各サブサーバー データ ブロックの合計バイト数。
サブサーバー データ	変数（variable）	サブサーバー データ ブロック（4-78 ページ） に記載のサブサーバー データ。

フル サーバー情報データ ブロック

フル サーバー情報データ ブロックは、サブサーバーのアプリケーション プロトコル、ベンダー、バージョン、関連サブサーバーなど、ホストで検出したサーバーに関する情報を伝えます。サブサーバーごとに、情報は、フル サブサーバーデータ ブロックに格納します（フル サブサーバー データ ブロック（4-89 ページ）を参照）。フル サーバー情報データ 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 サーバー情報データ 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	フル サーバー ブロック タイプ（106）																															
	フル サーバー 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																															
	リスト ブロック タイプ（11）																															
	リスト ブロック長																															
サブサーバー	フル サブサーバー ブロック タイプ（51）*																															
	フル サブサーバー ブロック長																															
	フル サブサーバー データ...																															

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

表 4-76　フル サーバー情報データ 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 サーバー情報ブロック タイプ	uint32	フル サーバー情報データ ブロックを開始します。この値は常に 106 です。
フル サーバー情報ブロック長	uint32	フル サーバー 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、後続のフル サーバー データのバイト数を加えたフル サーバー情報データ ブロックの合計バイト数。
アプリケーション プロトコル ID	uint32	サーバー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（Vendor Name）	string	サーバー 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	サーバーのバージョン。
前回の使用（Last Used）	uint32	システムが使用中のサーバー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）がサーバー データを提供した場合、0 • ユーザーがサーバー 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 ツールでサーバー データを提供した場合、3
ソース	uint32	サーバー 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）、ユーザー、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	サブサーバー データを伝えるフル サーバー情報データ 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。

表 4-76　フル サーバー情報データ 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
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 サブサーバー 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 サブサーバー データ ブロックが続きます。
フル サブサーバー ブロック タイプ	uint32	最初のフル サブサーバー 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 サブサーバー 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。
フル サブサーバー ブロック長	uint32	フル サブサーバー 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 バイト数を加えた各フル サブサーバー データ ブロックの合計バイト数。
フル サブサーバー データ ブロック*	uint32	このサーバーのサブサーバーを含むフル サブサーバー 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 サブサーバー データ ブロック (4-89 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、スキャン結果データ ブロック 5.2+ (4-146 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。

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 4-77　　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(Port)]	uint16	結果の脆弱性による影響を受けたサーバーが使用するポート。
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	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ーのバイト数を加えたサブサーバー文字列データ ブロックのバイト数。
スキャン結果サブサーバー	string	サブサーバー。
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。

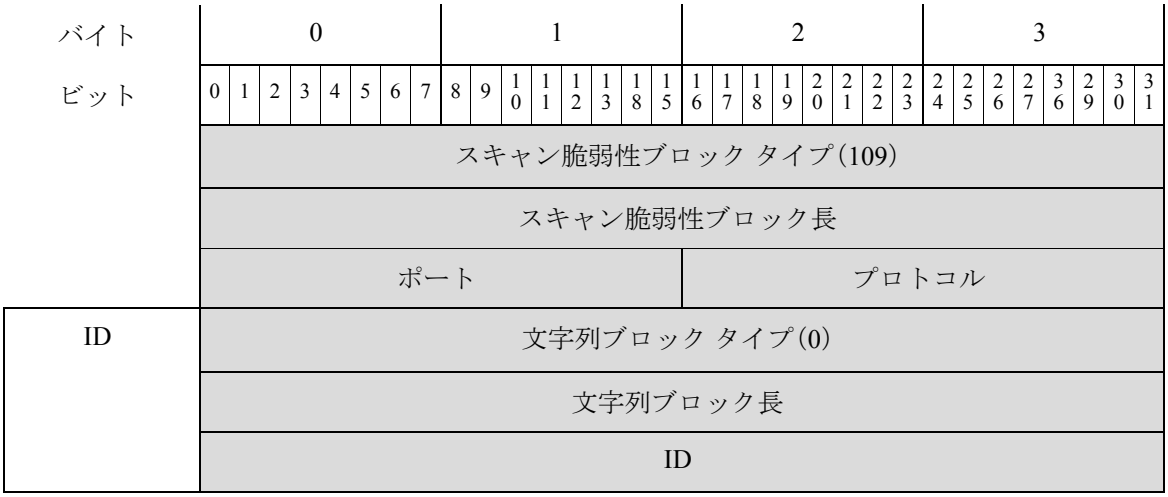
表 4-77　汎用スキャン結果データ ブロックのフィールド（続き）

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	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ーのバイト数を加えたサブサーバー文字列データ ブロックのバイト数。
スキャン結果サブサーバー	string	サブサーバー（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、スキャン結果データ ブロック 5.2+（4-146 ページ）およびスキャン結果を追加メッセージ（4-61 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
[名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	脆弱性名...																															
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...																															
説明クリーン	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 4-78　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(Port)]	uint16	脆弱性の影響を受けるサブサーバーで使用するポート。

表 4-78　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（Name）]	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）。

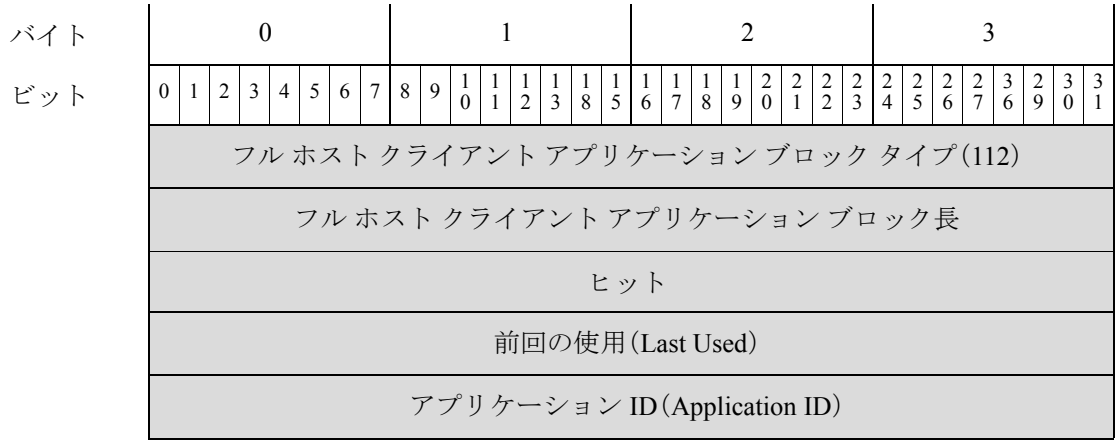
表 4-78　スキャン脆弱性データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
リスト ブロック 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。
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（4-81 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（4-83 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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 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...																															
	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 4-79　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 (Application 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)。

表 4-79　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 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（variable）	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（variable）	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
		ヒット																															
		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 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 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 4-80　　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 4-80　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（variable）	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（4-124 ページ）を参照してください。

ユーザー脆弱性データ ブロック 5.0+

ユーザー脆弱性データ ブロックは、脆弱性について記述し、ユーザー脆弱性変更ブロック内で使用します。さらに、ユーザー脆弱性変更ブロックはユーザー設定有効脆弱性イベントとユーザー設定無効脆弱性イベントで使用します。5.0+ のユーザー脆弱性データ 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。ユーザー脆弱性変更データ ブロックの詳細については、ユーザー脆弱性変更データ ブロック 4.7+（4-113 ページ）を参照してください。

次の図は、ユーザー脆弱性変更データ ブロックの形式です。

次の表では、ユーザー脆弱性データ ブロックのフィールドについて説明します。

表 4-81　ユーザー脆弱性データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザー脆弱性ブロック タイプ	uint32	ユーザー脆弱性データ ブロックを開始します。この値は常に 124 です。
ユーザー脆弱性ブロック長	uint32	ユーザー脆弱性ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザー脆弱性データのバイト数を加えたユーザー脆弱性データ 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（variable）	ユーザー入力からの 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（4-101 ページ） を参照してください。

表 4-81　ユーザー脆弱性データ 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(Port)]	uint16	脆弱性の影響を受けるサーバーで使用するポート。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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 Device 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Device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 4-82　オペレーティング 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（ユーザーやスキャナ）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ー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Device情報データ ブロック	変数（variable）	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 Device 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+ のモバイルDevice 情報データ ブロック（4-173 ページ） を参照してください。

5.1+ のモバイルDevice 情報データ ブロック

次の図は、モバイル Device 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 Device 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	モバイル Device 情報ブロック タイプ(131)																															
	モバイル Device 情報ブロック長																															
モバイル Device 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 Device 文字列データ...																															
	モバイル Device 最後の確認日時																															
	Mobile																															
	改造																															

ここでは、5.1+ で返るモバイル Device 情報データ ブロックを記述します。

表 4-83　　モバイルDevice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 Device 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 Device 情報ブロック長	uint32	モバイル Device 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 Device 情報データのバイト数を加えたモバイル Device 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 Device 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。
モバイル Device 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。
Mobile	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ホスト プロファイル ブロック タイプ(139)																															
	ホスト プロファイル ブロック長																															
	[IPアドレス(IP Address)] IP アドレス(続き) IP アドレス(続き) IP アドレス(続き)																															
サーバー 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)																サーバー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 Device 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Device フィンガープリント データ ブロック*																															
IPv6 サーバー 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 サーバー 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*																															
ユーザー 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																															
	ユーザー エージェント フィンガープリント データ ブロック*																															
TCP サーバー ブロック*	リスト ブロック タイプ(11)																															TCP のリスト サーバー
	リスト ブロック長																															
	TCP サーバー データ ブロック																															
UDP サーバー ブロック*	リスト ブロック タイプ(11)																															UDP のリスト サーバー
	リスト ブロック長																															
	UDP サーバー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31	
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																																
	Mobile								改造								VLAN の有無								VLAN ID(Admin. 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 プライオリティ								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								
NetBIOS [名前(Name)]	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 4-84　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(IP Address)]	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	サーバー 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	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(サーバー フィンガープリント)データ ブロック*	変数(variable)	サーバー 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+(4-172 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	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(variable)	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+(4-172 ページ) を参照してください。

表 4-84　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 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（variable）	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+（4-172 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（variable）	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+（4-172 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）。
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（variable）	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+（4-172 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 サーバー 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。

表 4-84　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(IPv6 サーバー)データ ブロック*	変数(variable)	IPv6 サーバー 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+(4-172 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	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(variable)	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+(4-172 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)。
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(variable)	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+(4-172 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	ユーザー 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)。

表 4-84　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(ユーザー エージェント フィンガープリント)データ ブロック*	変数（variable）	ユーザー 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+（4-172 ページ）を参照してください。
リストブロック タイプ	uint32	TCP サーバー データを伝えるサーバー 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ー データ ブロックを加えた値です。 このフィールドには、ゼロ以上のサーバー データ ブロックが続きます。
TCP サーバー データ ブロック	変数（variable）	TCP サーバーを記述するホスト サーバー 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 サーバー データ ブロック 4.10.0+(4-149 ページ) を参照してください。
リストブロック タイプ	uint32	UDP サーバー データを伝えるサーバー 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ー データ ブロックを加えた値です。 このフィールドには、ゼロ以上のサーバー データ ブロックが続きます。
UDP サーバー データ ブロック	uint32	UDP サーバーを記述するホスト サーバー 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 サーバー データ ブロック 4.10.0+(4-149 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 (4-80 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。

表 4-84　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（4-80 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+（4-122 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）
Mobile	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。
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（Admin. 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。

表 4-84　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
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（variable）	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+（4-165 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。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。

ユーザー製品データ ブロック 5.1+

ユーザー製品データ 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送します。このデータ ブロックは スキャン結果データ ブロック 5.2+（4-146 ページ）と ユーザー サーバー メッセージとオペレーティング システム メッセージ（4-60 ページ）で使用します。ユーザー製品データ 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、ユーザー製品データ 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
[IPアドレス（IP Address）]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 ユーザー製品																															
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																															
	サーバー 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																															
	マイナー用バージョン文字列...																															

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
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...																															
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)																															

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
Device 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	Device 文字列...																															
修正のリスト	Mobile								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、ユーザー製品データ ブロックのコンポーネントについて説明します。

表 4-85　　ユーザー製品データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザー製品データブロック タイプ	uint32	ユーザー製品データ ブロックを開始します。5.1+ の場合、この値は 134 です。
ユーザー製品ブロック長	uint32	ユーザー製品データ ブロックのバイトの合計数(ユーザー製品ブロック 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ー製品データのバイト数を含む)。
ソース	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)、ユーザー、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) がデータを提供した場合、0 • ユーザー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。

表 4-85　ユーザー製品データ 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
IP 範囲仕様データ ブロック*	変数（variable）	ユーザー入力の 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（4-101 ページ）を参照してください。
[ポート（Port）]	uint16	ユーザーが指定するポート。
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 ユーザー製品	uint32	ユーザー 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	ユーザー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	ユーザー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	ユーザー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。
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	ユーザー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	ユーザー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	ユーザー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ー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。

表 4-85　ユーザー製品データ 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
サーバー ID	uint32	ユーザー入力に指定したホスト サーバーのアプリケーション プロトコルの Cisco Secure Firewall 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 Cisco Secure Firewall システム OS 定義にマップ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 Cisco Secure Firewall システム OS 定義にマップ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	ユーザー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 Cisco Secure Firewall 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 Cisco Secure Firewall 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 Cisco Secure Firewall 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	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall 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。
文字列ブロック タイプ	uint32	ユーザー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 Cisco Secure Firewall 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	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall 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 Cisco Secure Firewall システム オペレーティング システム定義の最新のメジャー 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。

表 4-85　ユーザー製品データ 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	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	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall 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における最新のバージョン番号。
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 Cisco Secure Firewall システム オペレーティング システム定義の最新のマイナー 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	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall 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における最新のバージョン番号。
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 Cisco Secure Firewall システム オペレーティング システム定義の最新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	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall 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における最新のリビジョン番号。
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 Cisco Secure Firewall 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。
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	string	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall 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 Cisco Secure Firewall 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	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システムのパッチ番号。

表 4-85　ユーザー製品データ 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	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 Cisco Secure Firewall 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）。
内線番号	string	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall 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	ユーザー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）。
Device 文字列	string	モバイル デバイス ハードウェア情報。
Mobile	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	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ー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（variable）	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（4-108 ページ）を参照してください。

ユーザー データ ブロック

ユーザー データ ブロックはユーザー 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（4-65 ページ）を参照してください。

（注）　ユーザー 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、ユーザー イベント メッセージに表示される可能性のあるユーザー 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、Cisco Secure Firewall 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 4-86　ユーザー データ ブロック タイプ

タイプ（Type）	目次	データ ブロック カテゴリ	説明
73	ユーザー ログイン情報	レガシー	システムが検出したユーザーのログイン情報の変更を格納します。詳細については、ユーザー ログイン情報データ ブロック 5.0 ～ 5.0.2（B-141 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	ユーザー アカウント更新メッセージ	現在（Current）	ユーザー アカウント情報の変更を格納します。詳細については、ユーザー アカウント更新メッセージ データ ブロック（4-192 ページ）を参照してください。
75	4.7 ～ 4.10.x のユーザー情報	レガシー	システムが検出したユーザーの情報の変更を格納します。詳細については、ユーザー情報データ ブロック 5.x（B-156 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 のユーザー情報	現在（Current）	システムが検出したユーザーの情報の変更を格納します。詳細については、ユーザー情報データ ブロック 5.x（B-156 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	ユーザー ログイン情報	レガシー	システムが検出したユーザーのログイン情報の変更を格納します。詳細については、ユーザー ログイン情報データ ブロック 5.0 ～ 5.0.2（B-141 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。
127	ユーザー ログイン情報	レガシー	システムが検出したユーザーのログイン情報の変更を格納します。詳細については、ユーザー ログイン情報データ ブロック 5.1 ～ 5.4.x（B-143 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（4-36 ページ）を参照してください。
158	6.0+ のユーザー情報	現在（Current）	システムが検出したユーザー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 ユーザー ブロック（4-201 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	ユーザー ログイン情報	レガシー	システムが検出したユーザーのログイン情報の変更を格納します。詳細については、ユーザー ログイン情報データ ブロック 6.0.x（B-145 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。

表 4-86　ユーザー データ ブロック タイプ（続き）

タイプ（Type）	目次	データ ブロック カテゴリ	説明
165	ユーザー ログイン情報	レガシー	システムが検出したユーザーのログイン情報の変更を格納します。詳細については、ユーザー ログイン情報データ ブロック 6.1.x（B-149 ページ）を参照してください。これはブロック タイプ 159 に置き換わります。これはブロック タイプ 167 に更新しました。
166	VPN セッション情報	現在（Current）	システムによって検出された VPN セッションに関する情報が含まれています。詳細については、6.2+ の VPN セッション データ ブロック（4-204 ページ）を参照してください。
167	ユーザー ログイン情報	現在（Current）	システムが検出したユーザーのログイン情報の変更を格納します。詳細については、ユーザー ログイン情報データ ブロック 6.2+（4-207 ページ）を参照してください。これはブロック タイプ 165 に置き換わります。

ユーザー アカウント更新メッセージ データ ブロック

ユーザー 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ーのアカウント情報に伝えます。

ユーザー 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、ユーザー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ユーザー アカウント更新メッセージ ブロック タイプ（74）																															
	ユーザー アカウント更新メッセージ ブロック長																															
ユーザー（User）[名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー名...																															
ファースト [名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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 [名前（Name）]	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...																															
県	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	県...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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																															
郵便番号コード(Code)	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...																															
参照先	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...																															
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...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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 Phone	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	IP 電話...																															
ユーザー 1	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー 1...																															
ユーザー 2	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー 2...																															
ユーザー 3	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ユーザー 4	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザー 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、ユーザー 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 4-87　　ユーザー 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
ユーザー アカウント更新メッセージブロック タイプ	uint32	ユーザー 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。
ユーザー アカウント更新メッセージ ブロック長	uint32	ユーザー 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、後続のユーザー 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ー 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	ユーザーのユーザ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	ユーザー名文字列データ 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、およびユーザー名のバイト数を含む)。
[ユーザー名（Username）]	string	ユーザーのユーザー名。

表 4-87　ユーザー 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	ユーザー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	ユーザーの名前。
文字列ブロック タイプ	uint32	ユーザーのミドル 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	ユーザーのミドル ネーム イニシャル。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの姓。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの姓名。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの役職。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーのスタッフ アイデンティティ。
文字列ブロック タイプ	uint32	ユーザー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。

表 4-87　ユーザー 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
アドレス（Address）	string	ユーザーの住所。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの住所から得た市町村郡。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの県。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの住所から得た国または地域。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの住所から得た郵便番号。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの住所から得た建物。
文字列ブロック タイプ	uint32	ユーザー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。
参照先	string	ユーザーの住所から得た場所。
文字列ブロック タイプ	uint32	ユーザー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。

表 4-87　ユーザー 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	ユーザーの住所から得たルーム。
文字列ブロックタイプ	uint32	ユーザー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	ユーザーの住所から得た会社。
文字列ブロックタイプ	uint32	ユーザー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	ユーザーの住所から得た部門。
文字列ブロックタイプ	uint32	ユーザー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	ユーザーの住所から得た部署。
文字列ブロックタイプ	uint32	ユーザー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	ユーザーの住所から得たオフィス。
文字列ブロックタイプ	uint32	ユーザー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	ユーザーの住所から得た郵便配達先。
文字列ブロックタイプ	uint32	ユーザー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	ユーザーの電子メール アドレス。

表 4-87　ユーザー 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	ユーザー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	ユーザーの電話番号。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーのインターネット電話番号。
文字列ブロック タイプ	uint32	ユーザーの代替ユーザ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 バイトにユーザー名のバイト数を加えたユーザー文字列データ ブロックのバイト数。
ユーザー 1	string	ユーザーの代替ユーザー名。
文字列ブロック タイプ	uint32	ユーザーの代替ユーザ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 バイトにユーザー名のバイト数を加えたユーザー文字列データ ブロックのバイト数。
ユーザー 2	string	ユーザーの代替ユーザー名。
文字列ブロック タイプ	uint32	ユーザーの代替ユーザ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 バイトにユーザー名のバイト数を加えたユーザー文字列データ ブロックのバイト数。
ユーザー 3	string	ユーザーの代替ユーザー名。
文字列ブロック タイプ	uint32	ユーザーの代替ユーザ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 バイトにユーザー名のバイト数を加えたユーザー文字列データ ブロックのバイト数。
ユーザー 4	string	ユーザーの代替ユーザー名。
文字列ブロック タイプ	uint32	ユーザーの電子メール 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。

表 4-87　ユーザー 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
電子メール エイリアス 1	string	ユーザーの電子メール アドレス。
文字列ブロック タイプ	uint32	ユーザーの電子メール 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	ユーザーの電子メール アドレス。
文字列ブロック タイプ	uint32	ユーザーの電子メール 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	ユーザーの電子メール アドレス。

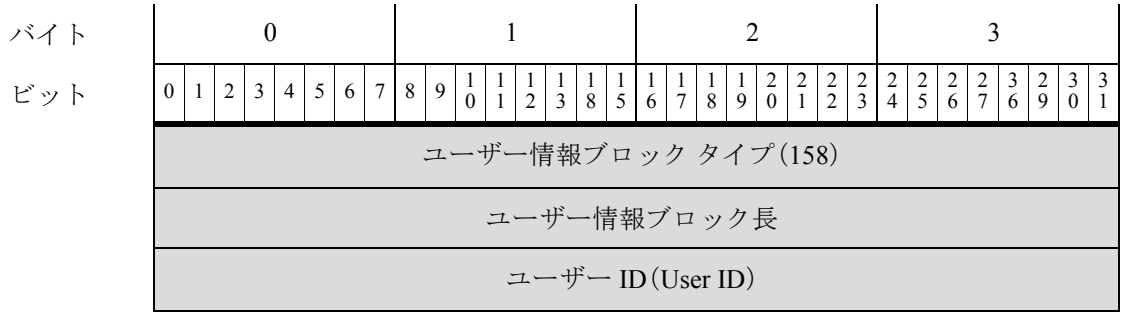
6.0+ の情報データ ユーザー ブロック

ユーザー情報データ ブロックはユーザー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ーの情報を伝えます。詳細については、ユーザー変更メッセージ（4-64 ページ）を参照してください。

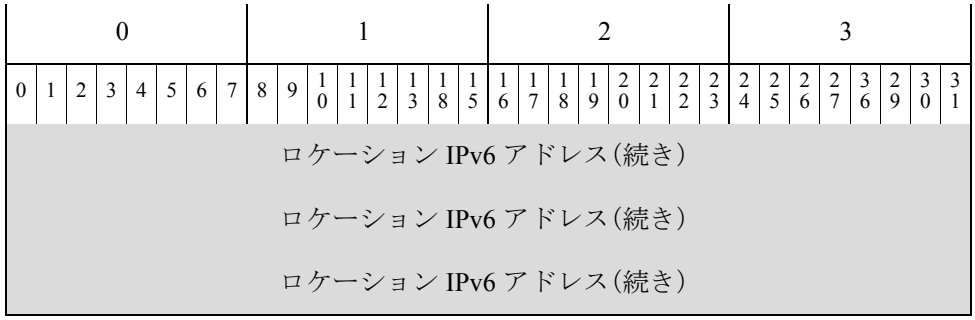
ユーザー情報データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 158 です。ユーザー重要度データ ブロックには、新しいエンドポイント プロファイル フィールド、セキュリティ インテリジェンスフィールド、IPv6 フィールドがあります。

ユーザー情報データ 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、ユーザー情報データ ブロック 5.x（B-156 ページ）を参照してください。

次の図は、ユーザー情報データ 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ユーザー（User）[名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー名...																															
	レルム ID																															
	プロトコル																															
ファースト [名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	名...																															
姓 [名前（Name）]	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、ユーザー情報データ ブロックのコンポーネントについての説明です。

表 4-88　ユーザー情報データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザー情報ブロック タイプ	uint32	ユーザー情報データ ブロックを開始します。この値は 158 です。
ユーザー情報ブロック長	uint32	ユーザー情報データブロックのバイトの合計数（ユーザー 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ー情報データのバイト数を含む）。
ユーザー ID（User ID）	uint32	ユーザーの ID 番号。
文字列ブロック タイプ	uint32	ユーザーのユーザ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	ユーザー名文字列データ 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、およびユーザー名のバイト数を含む）。
[ユーザー名（Username）]	string	ユーザーのユーザー名。
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	ユーザー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	ユーザー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	ユーザーの名前。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの姓。
文字列ブロック タイプ	uint32	ユーザー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。

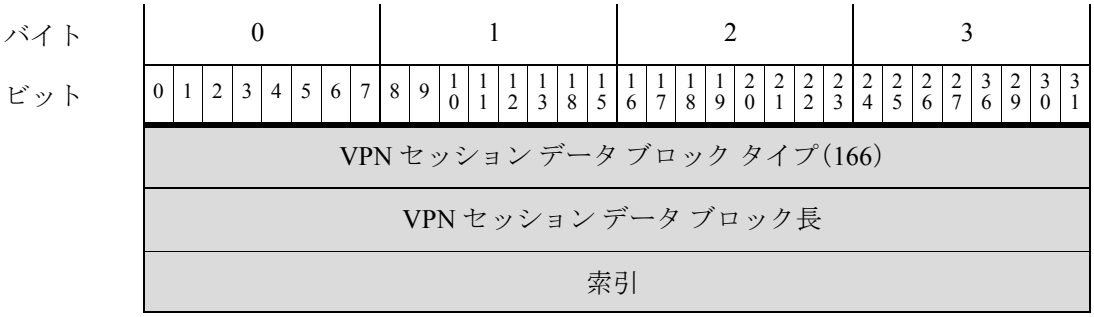
表 4-88　ユーザー情報データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
文字列ブロック長	uint32	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	ユーザーの電子メール アドレス。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの部署名。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの電話番号。
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。

6.2+ の VPN セッション データ ブロック

バージョン 6.2+ の VPN セッション データ ブロックには、シリーズ 1 グループのブロックのブロック タイプ 166 が含まれています。このデータ ブロックで VPN セッション情報を説明します。

次の図に、6.2+ の VPN セッション データ ブロックの形式を示します。



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
[グループ ポリシー（Group Policy）]	タイプ（Type）								文字列ブロック タイプ（0）																							
	文字列ブロック タイプ								文字列ブロック長																							
	文字列ブロック長								グループ ポリシー...																							
接続プロファイル	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	接続プロファイル...																															
	クライアント IP アドレス																															
	クライアント IP アドレス（続き）																															
	クライアント IP アドレス（続き）																															
	クライアント IP アドレス（続き）																															
クライアント オペレーティング システム	クライアントの国（Client Country）																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）																クライアント オペレーティング システム...															
クライアント アプリケーション	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...																															
	接続期間（Connection Duration）																															
	送信バイト数																															
	送信バイト数（続き）																															
	受信バイト数（Bytes Received）																															
	受信バイト数（続き）																															

次の表に、VPN セッション データ ブロックのフィールドについての説明を示します。

表 4-89　VPN セッション 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
VPN セッション データ ブロック タイプ	uint32	VPN セッション データ ブロックを開始します。この値は常に 166 です。
VPN セッション ブロック長	uint32	VPN セッション データ ブロック内の総バイト数。これには、VPN セッション データ ブロックのタイプ フィールドおよび長さフィールド用の 8 バイトと、その後の VPN データ フィールド内のバイト数が含まれます。
索引	uint32	セッションを識別するために VPN デバイスによって生成された番号。
タイプ（Type）	uint8	VPN セッションのタイプ。有効な値は次のとおりです。 • 0：不明 • 1：Cisco IKEv1 クライアント • 2：AnyConnect IKEv1 クライアント • 3：AnyConnect SSL • 4：WebVPN クライアントレス • 5：サイト間 IKEv2 • 6：サイト間 IKEv2 • 7：汎用 IKEv2 RA クライアント
文字列ブロック タイプ	uint32	VPN セッションのグループ ポリシ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	ユーザー名文字列のデータ ブロック内のバイト数。これには、ブロック タイプ フィールドおよび長さフィールド用の 8 バイトと、グループ ポリシー内のバイト数が含まれます。
[グループ ポリシー（Group Policy）]	string	VPN セッションが確立されたときにクライアントに割り当てられたグループ ポリシーの名前。
文字列ブロック タイプ	uint32	VPN セッションの接続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	ユーザー名文字列のデータ ブロック内のバイト数。これには、ブロック タイプ フィールドおよび長さフィールド用の 8 バイトと、接続プロファイル内のバイト数が含まれます。
接続プロファイル	string	VPN セッションで使用する接続プロファイル（トンネル グループ）の名前。
クライアント IP アドレス	uint8[16]	VPN クライアント デバイスの IP アドレス。
クライアントの国（Client Country）	uint16	VPN クライアントの国のコード。
文字列ブロック タイプ	uint32	クライアント デバイスで使用されるオペレーティング システ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。

表 4-89　VPN セッション データ ブロック フィールド（続き）

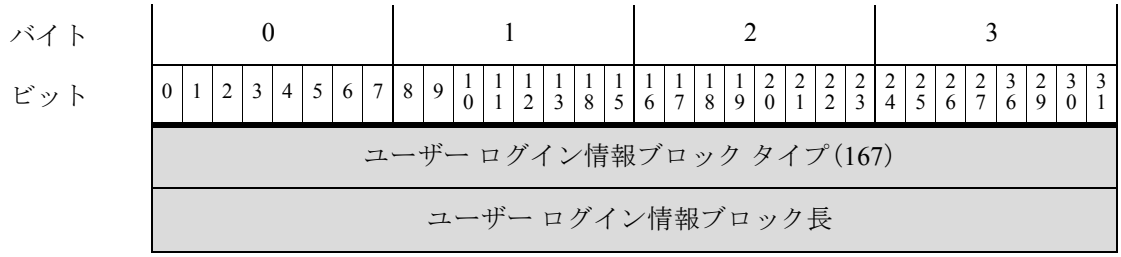
フィールド	データタイプ	説明
文字列ブロック長	uint32	ユーザー名文字列のデータ ブロック内のバイト数。これには、ブロック タイプ フィールドおよび長さフィールド用の 8 バイトと、オペレーティング システム名内のバイト数が含まれます。
クライアント オペレーティング システム	string	クライアント デバイスのオペレーティング システム。
文字列ブロック タイプ	uint32	クライアント デバイスで使用される VPN アプリケーションを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザー名文字列のデータ ブロック内のバイト数。これには、ブロック タイプ フィールドおよび長さフィールド用の 8 バイトと、VPN アプリケーション内のバイト数が含まれます。
クライアント アプリケーション	string	クライアント デバイスの VPN アプリケーション。
接続期間（Connection Duration）	uint32	VPN セッションの期間（秒単位）VPN ログアウト アクションにだけ指定されます。それ以外は 0 です。
送信バイト数	uint64	VPN セッション中に VPN クライアントに送信されるバイト数。VPN ログアウト アクションにだけ指定されます。それ以外は 0 です。
受信バイト数	uint64	VPN セッション中に VPN クライアントから受信したバイト数。VPN ログアウト アクションにだけ指定されます。それ以外は 0 です。

ユーザー ログイン情報データ ブロック 6.2+

ユーザー ログイン情報データ ブロックは、ユーザー情報更新メッセージで使用され、検出されたユーザーのログイン情報の変更を伝えます。詳細については、ユーザー情報更新メッセージ ブロック（4-64 ページ）を参照してください。

バージョン 6.2+ では、ユーザー ログイン情報データ ブロックには、シリーズ 1 グループのブロック内にブロック タイプ 167 が含まれています。VPN サポート用の新しいフィールドがあります。これはブロック タイプ 165 に置き換わります。詳細については、ユーザー ログイン情報データ ブロック 6.1.x（B-149 ページ）を参照してください。

次の図は、ユーザー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	Timestamp																															
	IPv4 アドレス（IPv4 Address）																															
ユーザー（User）[名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー名...																															
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...																															
	ユーザー ID（User 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																															
	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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								承認タイプタイプ（Type）								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...															
説明	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	説明...																															
VPN セッション	VPN セッション データ ブロック タイプ（166）																															
	VPN セッション データ ブロック長																															
	VPN セッション...																															

次の表は、ユーザー 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 4-90　　ユーザー 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
ユーザー ログイン情報ブロック タイプ	uint32	ユーザー ログイン情報データ ブロックを開始します。バージョン 6.2+ の場合、この値は 167 です。
ユーザー ログイン情報ブロック長	uint32	ユーザー ログイン情報データ ブロックのバイトの合計数（ユーザー 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ー ログイン情報データのバイト数を含む）。
Timestamp	uint32	イベントのタイムスタンプ。
IPv4 アドレス（IPv4 Address）	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（1-4 ページ）を参照してください。
文字列ブロック タイプ	uint32	ユーザーのユーザ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	ユーザー名文字列データ 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、およびユーザー名のバイト数を含む）。
[ユーザー名（Username）]	string	ユーザーのユーザー名。

表 4-90　ユーザー 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	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ー名文字列データ ブロックのバイト数。
ドメイン	string	ユーザーがログインしているドメイン。
ユーザー ID（User ID）	uint32	ユーザーの 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。
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。
プロトコル	uint32	ユーザー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（Port）]	uint16	ユーザー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ー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ー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	ユーザー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	ユーザーの電子メール アドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザー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]	ユーザー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。

表 4-90　ユーザー 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
ログイン タイプ	uint8	検出されたユーザー ログインのタイプ。
認証タイプ（Authentication Type）	uint8	ユーザー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。
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	Active Directory サーバーの名前など、このアクティビティのレポーター。
文字列ブロック タイプ	uint32	説明の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	説明文字列のデータ ブロック内のバイト数。これには、ブロック タイプ フィールドおよび長さフィールド用の 8 バイトと、説明フィールド内のバイト数が含まれます。
説明	string	ログインまたはログオフ アクティビティの説明。
VPN セッション ブロック タイプ	uint32	VPN セッション データを含む VPN セッション データ ブロックを開始します。この値は常に 166 です。
VPN セッション データ ブロック長	uint32	VPN セッション のデータ ブロック内のバイト数。これには、ブロック タイプ フィールドおよび長さフィールド用の 8 バイトと、VPN セッション データ ブロック内のバイト数が含まれます。
VPN セッション データ	VPN セッション データ	ログインを VPN セッションに関連付けた場合は、検出された VPN セッションに関する情報。VPN セッションが存在するときのみ使用されます。

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 4-91　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（Type）	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（4-212 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	レガシー	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 ポリシー ルール理由データ ブロック（B-416 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+（4-215 ページ）を参照してください。
57	ユーザー データ（User Data）	現在（Current）	ユーザー レコード メタデータ メッセージが、ユーザーを検出したユーザー ID 番号、プロトコル、そしてユーザー名を提供するために使用します。ユーザー データ ブロック（4-217 ページ）を参照してください。
59	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 6.0+（4-214 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 4-92　　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。このフィールドとアクセス コントロール ルール ID を合わせると、このレコードの固有キーになります。
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。このフィールドとアクセス コントロール ルール UUID を合わせると、このレコードの固有キーになります。

表 4-92　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（Name）]	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 6.0+

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 59 です。これはブロック タイプ 21 に取って代わります。

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 4-93　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 59 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 4-93　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	uint32	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。このフィールドは、このレコードの固有キーです。 イベントをトリガーしたルールの理由の番号。 ルールの理由は、複数のビットを設定できるバイナリ ビットマップです。ルールには、複数の理由がある場合があります。ビット値は次のとおりです。 • **1**：IP ブロック • **2**：IP モニター • **4**：ユーザー バイパス • **8**：ファイル モニター • **16**：ファイル ブロック • **32**：侵入モニター • **64**：侵入ブロック • **128**：ファイル再開ブロック • **256**：ファイル再開許可 • **512**：ファイルカスタム検出 • **1024**：SSL ブロック • **2048**：DNS ブロック • **4096**：DNS モニター • **8192**：URL ブロック • **16384**：URL モニター • **32768**：コンテンツ制約 • **65536**：インテリジェント アプリケーション バイパス • **131072**：WSA 脅威
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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 4-94　　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	接続によってトリガーされた IP ブロックリストまたは許可リストの ID。このフィールドとアクセス コントロール ポリシー UUID を合わせると、このレコードの固有キーになります。
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。このフィールドとセキュリティ インテリジェンス リスト ID を合わせると、このレコードの固有キーとなります。

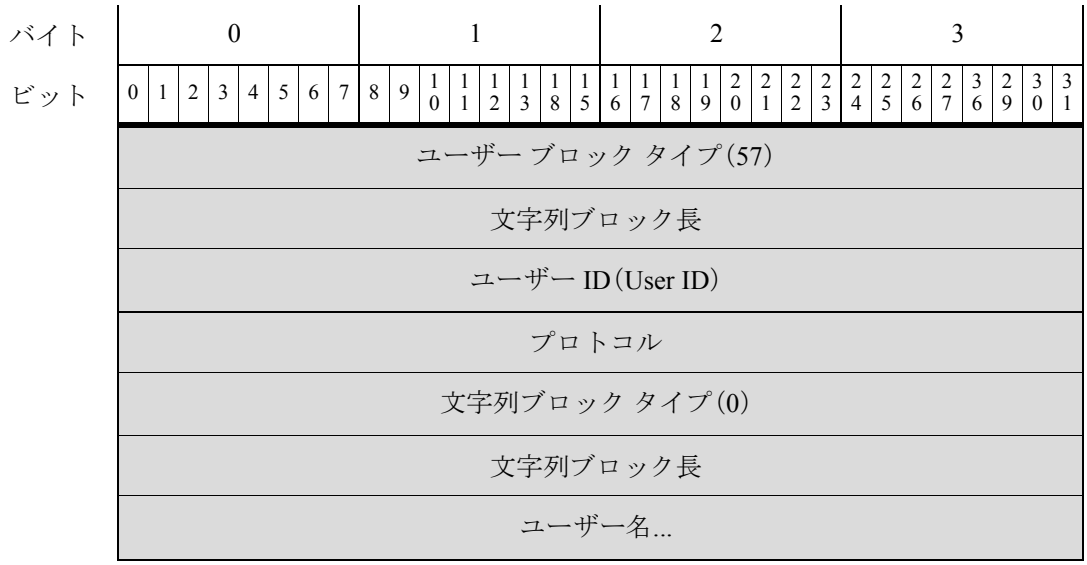
表 4-94　セキュリティ インテリジェンス カテゴリ データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	セキュリティ インテリジェンス リスト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	接続でトリガーされたセキュリティ インテリジェンス カテゴリ IP ブロックリストまたは許可リストの名前。

ユーザー データ ブロック

eStreamer サービスは、ユーザー レコード メタデータ メッセージのユーザーデータ ブロックで、ユーザー ID 番号、ユーザーを検出したプロトコル、そしてユーザー名を提供します。ユーザー 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、ユーザー データ ブロックの構造です。



次の表では、ユーザー データ ブロックのフィールドについて説明します。

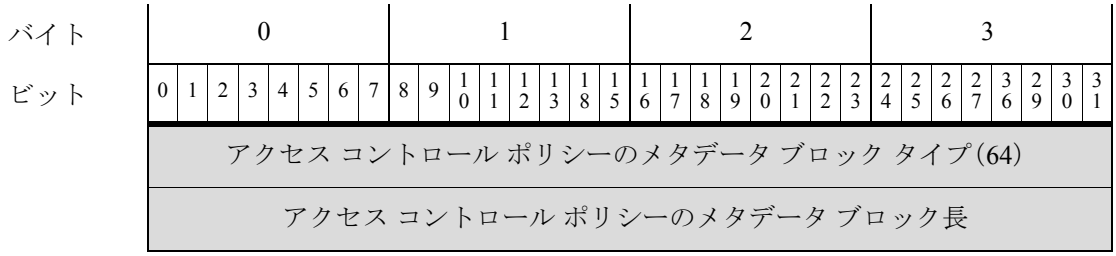
表 4-95　ユーザー データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザー ブロック タイプ	uint32	ユーザー 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、後続のデータのバイト数を加えたユーザー ブロックの合計バイト数。
ユーザー ID（User ID）	uint32	ユーザーの固有識別情報。このフィールドは、このレコードの固有キーです。
プロトコル	uint32	ユーザー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 フィールドとヘッダー フィールドの 8 バイトにユーザー名フィールドのバイト数を加えたユーザー名文字列データ ブロックのバイト数。
[ユーザー名（Username）]	string	ユーザーの名前

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 ポリシーのメタデータブロックは、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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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（Sensor 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...																															

次の表は、アクセス コントロール ポリシー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 4-96　　アクセス コントロール ポリシーのメタ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。このフィールドは、このレコードの固有キーです。
センサー ID（Sensor 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（Name）]	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 サーバーはホスト 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（2-36 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（4-65 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-374 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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																															
サーバー 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 サーバー 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																															
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																															
ユーザー(User) 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 ユーザー 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(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…																															


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 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
Application 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
Mobile 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 サーバー 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 サーバー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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																															
ユーザー 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 ユーザー エージェント フィンガープリント データ…																															
(TCP)全サーバー データ	リスト ブロック タイプ(11)…																															
	リスト ブロック長…																															
	(TCP)全サーバー データ ブロック(104)*																															
(UDP)全サーバー データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	(UDP)全サーバー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
トランスポート(Transport)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(Admin. 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 [名前(Name)]	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(Notes)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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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(Attribute)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*																															
	Mobile								改造								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(variable)	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 (4-103 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	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 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（variable）	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+（4-172 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	サーバー 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	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（サーバー フィンガープリント）データ ブロック*	変数（variable）	サーバー 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+（4-172 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	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（variable）	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+（4-172 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	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 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(variable)	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+(4-172 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	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 2)データ ブロック*	変数(variable)	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+(4-172 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	ユーザー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	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(ユーザー フィンガープリント)データ ブロック*	変数(variable)	ユーザー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+(4-172 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	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 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(variable)	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+(4-172 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	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(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(variable)	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+(4-172 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	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(variable)	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+(4-172 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	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 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(モバイル)データ ブロック*	変数(variable)	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+(4-172 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 サーバー 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	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 サーバー フィンガープリント)データ ブロック*	変数(variable)	IPv6 サーバー 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+(4-172 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	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(variable)	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+(4-172 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)。
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(variable)	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+(4-172 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	ユーザー 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（ユーザー エージェント）データ ブロック*	変数（variable）	ユーザー 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+（4-172 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ー 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ー データ ブロック長から成る 8 バイトを含みます。
（TCP）全サーバー データ ブロック*	変数（variable）	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ー 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 サーバー データ ブロック 4.10.0+（4-151 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ー 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ー データ ブロック長から成る 8 バイトを含みます。
（UDP）全サーバー データ ブロック*	変数（variable）	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ー 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 サーバー データ ブロック 4.10.0+（4-151 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
（ネットワーク）プロトコル データ ブロック*	変数（variable）	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 ブロックの説明の詳細については、プロトコル データ ブロック (4-80 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。
（トランスポート）プロトコル データ ブロック*	変数（variable）	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 ブロックの説明の詳細については、プロトコル データ ブロック (4-80 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（variable）	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+ (4-122 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 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（Admin. 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。

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（variable）	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+（4-165 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。
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（Notes）	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（variable）	Cisco 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+（4-119 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（variable）	サードパーティの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+（4-119 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。

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
(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（variable）	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、Cisco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+ (4-119 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。
属性値データ ブロック*	変数（variable）	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 (4-87 ページ) を参照してください。
Mobile	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（variable）	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 (4-36 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、ユーザーはそれを eStreamer サーバーに接続し、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 サーバー*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 サーバーで eStreamer を有効にします。

   eStreamer サーバーへのアクセス許可、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 サーバーでの 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/サーバー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 サーバーでの eStreamer の設定

ライセンス:任意(Any)

eStreamer サーバーとして使用する 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 サーバーを設定し、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ー 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

ライセンス:任意（Any）

eStreamer サーバー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）
- 相関イベントと許可リストイベント
- 影響フラグ アラート
- ユーザー 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:

アクセス:管理

ステップ 1　[システム（System）] > [統合（Integration）] > [eStreamer（eStreamer）] を選択します。

ステップ 2　**eStreamer** をクリックします。

[] ページには、[イベント設定（eStreamer Event Configuration）] メニューが表示されます。
eStreamer

ステップ 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 サーバー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許可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。
- [ユーザー アクティビティ イベント（User Activity Events）]：ユーザー 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 サーバー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 サーバー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、ユーザー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（2-15 ページ）を参照してください。

ステップ 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

ライセンス：任意（Any）

eStreamer がクライアントにイベントを送信する前に、eStreamer サーバーのピア 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 サーバー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：

アクセス：管理

ステップ 1　[システム（System）] > [統合（Integration）] > [eStreamer（eStreamer）] を選択します。

[eStreamer] ページが表示されます。

ステップ 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。

ステップ 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、ホスト入力サーバーはホストを 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。

ステップ 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。

ステップ 5　[Save] をクリックします。

eStreamer サーバーはクライアント 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/サーバー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 [クライアント(eStreamer Client)] の下に表示された状態で、[クライアント(eStreamer Client)] ページが再表示されます。Management Center

ステップ 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。

ステップ 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

ライセンス: 任意(Any)

eStreamer サービスはユーザー 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

ライセンス: 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

表 6-1　eStreamer 管理オプション （続き）

オプション	説明	選択するオプション番号
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

ライセンス: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（6-5 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

ライセンス: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:

アクセス:管理

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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、Perl モジュール、および Python スクリプトのセットです。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 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 Python 参照クライアントの実行（6-14 ページ）

eStreamer 参照クライアントの設定

eStreamer 参照クライアントを使用するには、まず環境と要件に合わせて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 参照クライアントのダウンロード（6-6 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（6-9 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（6-9 ページ）
- Perl テストスクリプトで要求されるデータについて（6-9 ページ）
- Perl テストスクリプトで要求されるデータタイプの変更（6-11 ページ）
- 参照クライアントの証明書の作成（6-8 ページ）

eStreamer 参照クライアントのダウンロード

eStreamer 参照クライアントファイルを含む eStreamerSDK.zip パッケージは、Cisco サポートサイトからダウンロードできます。eStreamerSDK.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 サーバー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 サーバー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。

- `python_client/estreamer_client.py`

  この Python スクリプトを使用して、SSL 接続を介した侵入イベント要求をテストできます。

- `python_client/estreamer_connection.py`

  この Python スクリプトは、eStreamer サーバーに接続します。`estreamer_client.py` に必要なスクリプトです。

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:

ステップ 1　OpenSSL を http://openssl.org/source/ からダウンロードします。

ステップ 2　`/Usr/local/src` にソースを展開します。

ステップ 3　Configure スクリプトを実行して、ソースを設定します。

ステップ 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。

参照クライアントの証明書の作成

ライセンス:任意（Any）

参照クライアントを使用する前に、クライアントを実行するコンピュータ用の証明書を Management Center または管理対象デバイスで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。

参照クライアントの証明書を作成するには、次の手順を実行します。

アクセス:管理

ステップ 1　[システム（System）] > [統合（Integration）] > [eStreamer（eStreamer）] を選択します。

[] ページが表示されます。

ステップ 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。

ステップ 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、ホスト入力サーバーはホストを 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。

ステップ 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。

ステップ 5　[Save] をクリックします。

eStreamer サーバーはクライアント 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/サーバー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 [クライアント（eStreamer Client）] の下に表示された状態で、[クライアント（eStreamer Client）] ページが再表示されます。Management Center

ステップ 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。

ステップ 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。

Python 参照クライアントの一般的な前提条件のロード

eStreamer Python 参照クライアントを実行する前に、次の手順を実行する必要があります。

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 サーバーへの 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。

参照クライアントのダウンロードと解凍

eStreamer 参照クライアントを含む EventStreamerSDK.zip ファイルは、Cisco 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。

Perl 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（2-36 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（2-41 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（2-13 ページ）、相関ポリシー レコード（3-30 ページ）、相関ルール レコード（3-31 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（4-46 ページ）、およびイベント タイプ別のユーザー データ構造（4-63 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（2-21 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（2-21 ページ）および侵入イベント レコード 7.1 以上（3-9 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（2-21 ページ）および侵入イベント レコード 7.1 以上（3-9 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。

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 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（2-21 ページ）および侵入イベント レコード 7.1 以上（3-9 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`* `json=<filename>`	[該当なし（N/A）]	イベントストリーム要求、メッセージタイプ 2、ビット 23 を `1`、その他すべてのビットを `0` に設定。<filename> という名前の JSON ファイルを送信します。	提供される侵入、接続、およびファイルイベント データ（JSON 形式）。

Perl 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（2-15 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

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_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	14	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	ユーザー 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 サーバー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
$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	28	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。

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 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(6-13 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)

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 サーバーおよび 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 eStreamerServerIPAddress -h HostIPAddresses
```

たとえば、10.10.0.4 の IP アドレスの eStreamer サーバーへの接続を介した 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 eStreamerServerIPAddress -o pcap -f ResultingPCAPFile
```

たとえば、10.10.0.4 の IP アドレスの eStreamer サーバー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 eStreamerServerIPAddress -o csv -f ResultingCSVFile
```

たとえば、10.10.0.4 の IP アドレスの eStreamer サーバー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 サーバーへのレコードの送信

侵入イベント データを SNMP サーバー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 サーバーの名前を示します。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 サーバー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 eStreamerServerIPAddress -o snmp
    -f SNMPServerName
```

たとえば、10.10.0.4 の IP アドレスの eStreamer サーバー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 サーバー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 サーバー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 eStreamerServerIPAddress -o syslog
```

たとえば、10.10.0.4 の IP アドレスの eStreamer サーバー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 eStreamerServerIPAddress
```

または

```
./ssl_test.pl -i eStreamerServerIPAddress
```

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
```

eStreamer Python 参照クライアントの実行

eStreamer Python 参照クライアントスクリプトは、Cisco Secure Firewall システム Management Center eStreamer サービスからイベントデータを取得するための非常にシンプルな新しいメカニズムです。イベント情報をバイナリデータで返す代わりに、イベントは JSON や CSV などの形式の完全修飾テキストとして返されます。

この API は、接続イベント、侵入イベント、およびファイルイベントの 3 つのイベントタイプに関する情報の要求のみをサポートしています。他のすべてのイベントについては別のクライアントを使用する必要があります。eStreamer 統合ガイドに記載されている通常の方法を参照してください。

Python コードでは、新しいメカニズムを使用する簡単なサンプルクライアントが提供されます。Perl サンプルクライアントコードも変更され、オプションでこの新しいメカニズム（`json=<filename>` コマンドライン引数を使用）を使用できるようになりましたが、Python のサンプルは新しいメカニズムのみサポートしているため、はるかに簡単です。

使用例:

```
./estreamer_client.py --server 192.168.1.1 --configfile json_request.json --pkcs12_file
192.168.1.2_8.pkcs12 --start all
```

表 6-5　Python スクリプトの引数

引数...	実行内容...
`-h、--help`	このヘルプメッセージを表示して終了します。
`--server SERVER`	eStreamer サーバーの IP アドレスを指定します。この IP アドレスは、クライアントを実行しているマシンからアクセスできる必要があります。
`--port` PORT	eStreamer サーバーのポートを指定します。デフォルトは `8302`
`--configfile` CONFIGFILE	JSON 形式の構成ファイルを提供します。詳細については、JSON ファイルの形式（2-5 ページ）を参照してください。
`--pkcs12_file` PKCS12_FILE	eStreamer サーバーへの認証用の PKCS12 ファイルを提供します。
`--pkcs12_password` PKCS12_PASSWORD	必要に応じて、PKCS12 パスワードを提供します。
`--debug`	デバッグモードを有効にします。
`--start` {now,all,bookmark}	イベントのストリーミング開始時間
`--outfile` OUTFILE	イベントを格納する出力ファイル。デフォルトでは stdout に出力

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-31 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）
- 6.1.x の接続統計データ ブロックの例（A-15 ページ）
- バージョン 5.1+ ユーザー イベントの例（A-28 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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
14	0	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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	1	1	0	1	0	0	1	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
28	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	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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。

ケース	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。
14	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。

ケース	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ー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ー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、ユーザーの内部 ID 番号が含まれます。該当のユーザーが存在しないため、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。
28	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。

ケース	説明
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 サーバー証明書の SHA1 ハッシュの最初の部分が含まれます。
41	SSL が使用された場合、この行には、SSL サーバー証明書の 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 サーバー証明書の 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	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	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	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
14	0	0	0	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。

ケース	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（3-66 ページ）を参照してください。
14	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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	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	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	1	1	
6	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	0
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	1	1	1	0	1	0	0	0	1	0	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。

ケース	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。

ケース	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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	0	1	1	1	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	1	0	0	0	0	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	0	1	0	1	0	1	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	1	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	1	0	1	0	0	0	1	1	1	0	0	1	0
	0	1	1	0	1	1	1	1	0	1	1	0	1	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
	0	0	1	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	1	0	1	1	1	0	1	0	0
	0	1	1	0	1	0	0	1	0	1	1	1	0	1	1	0	0	1	1	0	1	0	0	1	0	1	1	1	0	1	0	0
7	0	1	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	1	0	0	0	0	1
	0	0	1	0	0	0	0	0	0	1	0	0	1	1	1	0	0	1	1	0	0	1	0	1	0	1	1	1	0	1	0	0
	0	1	1	1	0	1	1	1	0	1	1	0	1	1	1	1	0	1	1	1	0	0	1	0	0	1	1	0	1	0	1	1
	0	0	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1	0	0	1	0	0	1	1	0	1	1	1	1
	0	1	1	0	1	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0	0	0	1	0	0	0	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	1	0	0	1	0	0	0	0	0
	0	1	0	0	0	1	0	0	0	1	1	0	0	1	0	1	0	1	1	1	0	1	0	0	0	1	1	0	0	1	0	1
	0	1	1	0	0	0	1	1	0	1	1	1	0	1	0	0	0	1	1	0	0	1	0	1	0	1	1	0	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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。

ケース	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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	0	1	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	0	1	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。

ケース	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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	1	1	0	1	1	1	1	0	1	1	1	0	1	0	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	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	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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	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。

ケース	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、Cisco Secure Firewall 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。

6.1.x の接続統計データ ブロックの例

次の図に、接続統計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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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	1	0	1	1	0	0	1	1	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	1	0	0	0	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	1	0	1	0	1	1	1	1	0	0
5	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0	0	0	1	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	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	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	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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
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	0	1	1
14	0	0	0	0	0	0	0	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
15	1	1	0	1	0	0	0	1	1	0	0	0	0	1	0	0	1	1	1	1	1	0	1	1	0	1	0	1	0	1	1	1
16	0	0	0	0	1	0	0	0	1	0	1	1	1	0	1	0	0	0	0	0	1	1	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	1	0	1	0	0	0	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	1	0	1	0	0	0	0	1	0	0
20	0	0	0	0	0	0	0	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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
21	0	1	0	1	1	0	0	1	1	1	1	0	0	1	0	0	0	1	0	1	0	0	0	0	0	1	0	1	1	1	0	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	1	0	0	1	1	0	0	0	1	0	1	1	0	1	1	1	1	1	0	0	0	1	1	1	0	1	1	1	0	1
	1	1	1	1	0	1	1	1	0	0	1	1	0	0	0	1	1	0	1	0	1	0	0	0	0	1	0	1	1	1	1	0
22	0	1	1	0	0	0	0	0	1	1	0	1	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	0	1	1	0	0	0	0	1	0	0	0	0	1	1	1	0	0	0	0	1	0	0	1	1	0	1	1	0	0	0
	1	1	0	1	0	1	1	0	1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0
23	0	1	0	1	1	0	0	1	1	0	0	1	0	0	0	1	0	0	1	0	0	1	1	0	1	1	0	1	1	1	1	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	1	0	0	1	1	0	0	0	1	0	1	1	0	1	1	1	1	1	0	0	0	1	1	1	0	1	1	1	1	1
	1	1	1	1	0	1	1	1	0	0	1	1	0	0	0	1	1	0	1	0	1	0	0	0	0	1	0	1	1	1	1	0
24	0	1	1	0	0	0	0	0	1	0	0	0	1	1	0	1	0	1	1	0	1	1	0	0	1	1	1	1	0	1	0	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	0	1	1	0	0	0	0	1	0	0	0	0	1	1	1	0	0	0	0	1	0	0	1	1	0	1	1	0	0	0
	1	1	0	1	0	1	1	0	1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0	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
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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
	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	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	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	1	0	0	1	0	0	0	0	0	1	1	0	0	0	0	1	0	0	1	0	1	0	1	1	1	1	1	0	1	0	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
	0	0	0	0	0	0	0	0	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	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	1	1	1	1	1	1	0	1	0	0	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	0	1
29	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	1	1
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	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	1	0	0	0	0	1	0	1	0
33	0	0	0	0	0	0	0	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	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	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35	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	1	1	0	0
36	0	1	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0
37	0	0	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0
38	0	0	1	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	0	0	0	0	0	0	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	1	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
	0	0	0	0	0	0	0	0	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
	0	0	0	0	0	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
41	1	1	0	0	1	1	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	0	0	0	0	0	0	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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
	0	0	0	0	0	0	0	0	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
	0	0	0	0	0	0	0	0	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
45	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
46	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
47	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
48	0	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
49	0	1	0	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	1	0	0
50	0	1	1	0	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
51	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
52	0	0	0	0	0	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
53	0	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	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
55	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
72	0	0	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	0
57	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
58	0	0	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	0
59	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
60	0	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	1	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
61	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	0	0	0	0	0
62	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
63	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
65	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
66	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
67	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
68	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
69	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
70	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
71	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
72	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
73	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
74	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
76	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
77	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
78	0	0	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	0
79	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
80	0	0	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	0
81	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
82	0	0	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	0
	0	0	0	0	0	0	0	0	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
83	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
84	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
85	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
86	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
87	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
88	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
89	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
90	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
91	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
92	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
93	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
94	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
95	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
96	0	0	0	0	0	0	0	0	0	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	1	0	0	1	1	1	1	0	0	0	1	1	0	0	1	0	1	1	0	1	1	1	0	0	0	0
	0	1	1	1	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	1	0	1	0	0	1	1	0	0	1	1	0	1	1	1	1	0	0	1	1	0	1	1	0	1	1	0	0	0	1
97	1	0	0	1	1	1	0	0	1	0	1	1	0	1	0	1	0	1	0	1	0	0	1	1	1	1	1	1	1	1	0	1
98	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
99	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
101	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
102	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
103	0	0	0	0	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
104	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
105	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
106	0	0	0	0	0	0	0	0	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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
107	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	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。

ケース	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 716 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 71 を示し、接続統計レコードを表します。
4	この行は、後続のイベント レコードの長さが 700 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、2016 年 10 月 10 日(月)の 午前 8 時 48 分 52 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、ディスカバリ イベントを生成したデバイスの ID 番号を指定しています。デバイス ID は 1 です。
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、イベントに関連するホストの MAC アドレスが含まれます。MAC アドレスは 00:00:00:00:00:00 です。
10	この行の最初の 16 ビットには、MAC アドレスの残りの部分が含まれます。次の 8 ビットでは、ホストが IPv6 アドレスであるかどうかを示すフラグです。最後の 8 ビットは空白です。これは将来の使用に備えて予約されています。
11	この行には、イベントが発生した時刻の UNIX タイムスタンプが含まれます。
12	この行には、イベント マイクロ秒が含まれます。この場合は、0 です。
13	この行には、イベント タイプが含まれます。この場合、タイプは 1003 です。
14	この行には、イベント サブタイプが含まれます。この場合、イベント サブタイプは 1 です。これは、イベント タイプ 1003 とともに、これが接続統計イベントであることを意味します。
15	この行はファイル番号に使用されます。これは内部専用です。
16	この行はファイルの位置に使用されます。これは内部専用です。
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。この場合、IPv6 アドレス 0:3eb:0:1:d184:fb57:8ba:c00 が含まれています。
18	この行には、ブロック タイプが含まれます。値は 163 です。これは、接続統計データ ブロック タイプを示しています。

ケース	説明
19	この行には、データ ブロックの長さが含まれ、644 バイトのデータが含まれていることを示しています。
20	この行は、ディスカバリ イベントを生成したデバイスの ID 番号を指定しています。デバイス ID は 1 です。
21	入力セキュリティ ゾーンが含まれます。ゾーンは 59e4505c-4493-11e6-a62d-f1dff731a85 です。
22	出力セキュリティ ゾーンが含まれます。ゾーンは 60d50c80-4493-11e6-9843-84d8d6a3e008 です。
23	入力インターフェイスが含まれます。インターフェイスは 599126de-4493-11e6-a62d-f1dff731a85e です。
24	出力インターフェイスが含まれます。インターフェイスは 608d6cf4-4493-11e6-9843-84d8d6a3e008 です。
25	この行には、接続イベントで示されているセッションを開始したホストの IP アドレスが含まれます。IP アドレスは 172.16.3.5 です。
26	この行には、開始ホストに応答したホストの IP アドレスが含まれます。IP アドレスは 72.48.149.244 です。
27	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。この例では、これは空白です。
28	この行には、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が含まれます。リビジョン番号は 00000000-0000-0000-0000-000057e9c39d です。
29	イベントをトリガーしたルールの内部識別子が含まれます。このルールは、268439603 です。
30	この行には、イベントをトリガーしたトンネル ルールの内部識別子が含まれます。このイベントはトンネル ルールでトリガーされなかったため、値は 0 です。
31	この行の最初の 2 バイトには、ルールで指定されたアクションが含まれます。この場合、値は 4 で、アクションが *ブロック* であったことを示しています。最後の 2 バイトにはルールの理由が含まれます。この場合、64 で、*侵入ブロック*を意味します。
32	最初の 2 バイトには、ルールの理由の残りが含まれます。次の 2 バイトには、イニシエータ ホストで使用されたポートが含まれます(43786)。
33	この行の最初の 2 バイトには、レスポンダ ポートが含まれます(443)。残りの 2 バイトには、TCP フラグが含まれます。
34	この行の最初のバイトには、プロトコルが含まれます(6)。これは、このイベントが TCP を介して発生したことを示します。残りの 24 バイトには、Netflow ソースの IP アドレスの最初の部分が含まれます(00000000-0000-0000-0000-000000000000)。
35	この行の最初のバイトには、Netflow ソースの最後の 8 ビットが含まれます。次の 2 バイトには、イベントを生成した Snort のインスタンスの識別子が含まれます(7)。残りのバイトには、接続数カウンタが含まれます。
36	この行の最初のバイトには、接続数カウンタの残りの部分が含まれます。最後の 24 ビットには、セッションで交換された最初のパケットの UNIX タイムスタンプの先頭が含まれます。このタイムスタンプは 1476103731 です。これは、2016 年 10 月 10 日(月)午前 8 時 48 分 51 秒を示しています。

ケース	説明
37	最初のバイトには、最初のパケットのタイムスタンプの残りの部分が含まれます。残りの 3 バイトは、セッションで交換される最後のパケットのタイムスタンプが含まれています。このタイムスタンプも 2016 年 10 月 10 日（月）午前 8 時 48 分 51 秒を示し、セッションが 1 秒未満で終了したことを示しています。
38	この行の最初のバイトには、最終パケット タイムスタンプの最後の 8 ビットが含まれます。残りの 24 ビットには、開始ホストから送信されたパケット数が含まれます。この場合は 13 です。
39	この行の最初のバイトは、イニシエータ送信パケット数の残りの部分です。次の 24 ビットには、レスポンダから送信されたパケット数が含まれます（0）。
40	この行の最初のバイトは、レスポンダ送信パケット数の残りの部分です。次の 24 ビットには、イニシエータから送信されたバイト数が含まれます（1743）。
41	最初のバイトはイニシエータ送信バイトの最終バイトで、残りの 24 ビットでレスポンダ送信バイトが開始します（0）。
54	最初のバイトはレスポンダ送信バイトの最終バイトで、残りの 24 ビットでイニシエータ パケット ドロップが開始します（0）。
43	最初のバイトはイニシエータ パケット ドロップの最後で、残りの 24 ビットでレスポンダ パケット ドロップが開始します（0）。
44	最初のバイトはレスポンダ パケット ドロップの最後で、残りの 24 ビットでイニシエータ バイト ドロップが開始します（0）。
45	最初のバイトはイニシエータ バイト ドロップの最後で、残りの 24 ビットでレスポンダ バイト ドロップが開始します（0）。
46	最初のバイトはレスポンダ バイト ドロップの最後で、残りの 24 ビットでレート制限が適用されたインターフェイスの名前が開始します（00000000-0000-0000-0000-000000000000）。
47	この行の最初のバイトは、QOS 適用インターフェイスの残りの部分です。残りの部分は、接続に適用された QOS ルールです。このインターフェイスには QOS ルールが適用されていないため、ID は 0 です。
48	この行の最初のバイトは、QOS ルール ID の残りの部分です。残りの部分は、トラフィックを生成したホストに最後にログインしたユーザーの ID 番号です（16466）。
49	この行の最初のバイトは、ユーザー ID の残りの部分です。残りの部分は、接続で使用されたアプリケーション プロトコルです。1122 は HTTPS 接続であることを示しています。
50	この行の最初のバイトは、アプリケーション プロトコル ID の残りの部分です。残りは、URL カテゴリです。
51	この行の最初のバイトは、URL カテゴリの残りの部分です。残りは、URL レピュテーションです。0 は、「リスク不明」を意味します。
52	この行の最初のバイトは、URL レピュテーションの残りの部分です。残りは、クライアント アプリケーション ID です。1296 は、「SSL クライアント」を意味します。
53	この行の最初のバイトは、クライアント アプリケーション ID の残りの部分です。残りは、Web アプリケーション ID です。0 は、「不明」を意味します。
54	この行の最初のバイトは、Web アプリケーション ID の残りの部分です。この行の残りの部分では、ブロック タイプが開始します。0 は、文字列ブロック タイプの先頭を示します。

ケース	説明
55	この行の最初のバイトは、文字列ブロック タイプの残りの部分です。残りはブロック長です。これは、クライアント アプリケーション URL に、ヘッダーと長さを含む 8 バイトが含まれていることを示しており、クライアント アプリケーション URL にデータが存在しないことを意味します。
72	この行の最初のバイトは、文字列ブロック長の残りの部分です。クライアント アプリケーション URL にはデータが存在しないため、この行の残りはブロック タイプ 0 で開始しています。これは、NetBIOS 名の文字列ブロック タイプの先頭を示しています。
57	この行の最初のバイトは、文字列ブロック タイプの残りの部分です。残りはブロック長です。これは、NetBIOS 名に、ヘッダーと長さを含む 8 バイトが含まれていることを示しており、NetBIOS 名にデータが存在しないことを意味します。
58	この行の最初のバイトは、文字列ブロック長の残りの部分です。NetBIOS 名にはデータが存在しないため、この行の残はブロック タイプ 0 で開始しています。これは、クライアント アプリケーション バージョンの文字列ブロック タイプの先頭を示しています。
59	この行の最初のバイトは、文字列ブロック タイプの残りの部分です。残りはブロック長です。これは、クライアント アプリケーション バージョンに、ヘッダーと長さを含む 8 バイトが含まれていることを示しており、クライアント アプリケーション バージョンにデータが存在しないことを意味します。
60	この行には、クライアント アプリケーション バージョン ブロック長の残りのバイトが含まれます。最後の 3 バイトは、接続イベントに関連付けられている 1 番目のモニター ルールの ID です（268439553）。
61	この行には、1 番目のモニター ルールの ID の最終バイトが含まれています。残りの 3 バイトは、2 番目のモニター ルールの ID です（0）。
62	この行には、2 番目のモニター ルールの ID の最終バイトが含まれています。残りの 3 バイトは、3 番目のモニター ルールの ID です（0）。
63	この行には、3 番目のモニター ルールの ID の最終バイトが含まれています。残りの 3 バイトは、4 番目のモニター ルールの ID です（0）。
64	この行には、4 番目のモニター ルールの ID の最終バイトが含まれています。残りの 3 バイトは、5 番目のモニター ルールの ID です（0）。
65	この行には、6 番目のモニター ルールの ID の最終バイトが含まれています。残りの 3 バイトは、7 番目のモニター ルールの ID です（0）。
66	この行には、7 番目のモニター ルールの ID の最終バイトが含まれています。残りの 3 バイトは、8 番目のモニター ルールの ID です（0）。
67	この行には、8 番目のモニター ルールの ID の最終バイトが含まれています。この行の 2 番目のバイトは、送信元または宛先の IP アドレスが IP ブロックリストと一致しているかどうかを示しています。この行の 3 番目のバイトは、IP ブロックリストに一致した IP 層です。最後のバイトで、ファイル イベントカウントが開始します（0）。
68	この行の最初のバイトは、ファイル イベントカウントの残りの部分です。次の 2 バイトには、侵入イベントカウントが含まれています。最後のバイトには、イニシエータの国が含まれます。この場合は 0 で、「不明」を意味します。
69	この行の最初のバイトは、イニシエータの国の第 2 バイトです。次の 2 バイトは、レスポンダの国です（840）。最後のバイトで、クライアントのオリジナル国が開始します。この場合は 0 で、「不明」を意味します。

ケース	説明
70	この行の最初のバイトは、クライアントのオリジナル国の最後です。次の 2 バイトは、IOC 番号です（0）。最後のバイトは、送信元自律システムの先頭バイトです（0）。
71	この行の最初の 3 バイトは、送信元自律システムです。最後のバイトは、宛先自律システムの先頭バイトです（0）。
72	この行の最初の 3 バイトは、宛先自律システムです。最後のバイトは、入力インターフェイスの SNMP インデックスです（0）。
73	この行の最初のバイトは、入力インターフェイスの SNMP インデックスです。次の 2 バイトは、出力インターフェイスの SNMP インデックスです（0）。この行の最後のバイトは、着信インターフェイス用のタイプ オブ サービス設定です（0）。
74	この行の最初のバイトは、発信インターフェイス用のタイプ オブ サービス設定です（0）。2 番目のバイトは、送信元マスクです（0）。3 番目のバイトは、宛先マスクです（0）。最後のバイトは、トラフィックが通過したセキュリティ コンテキストの ID 番号の先頭です。この場合、セキュリティ コンテキストは 00000000：0000：0000：0000-000000000000 です。
75	この行の最初の 3 バイトは、セキュリティ コンテキストの残りの部分です。最後のバイトは VLAN ID です（0）。
76	最初のバイトは VLAN ID です。最後の 3 つのバイトでは、値 0 で文字列ブロックが開始しています。この文字列ブロックには、参照ホストの名前が含まれています。
77	最初のバイトは、文字列ブロック タイプの残りの部分です。最後の 3 バイトで、ブロック タイプと長さを含む文字列ブロックの合計長を示しています。この場合の 8 バイトは、参照ホストがないため文字列ブロックにはデータが存在しないことを意味します。
78	最初のバイトは、文字列ブロック長の残りの部分です。最後の 3 つのバイトでは、値 0 で文字列ブロックが開始しています。この文字列ブロックには、ユーザー エージェントが含まれます。
79	最初のバイトは、文字列ブロック タイプの残りの部分です。最後の 3 バイトで、ブロック タイプと長さを含む文字列ブロックの合計長を示しています。この場合の 8 バイトは、ユーザー エージェントがないため文字列ブロックにはデータが存在しないことを意味します。
80	最初のバイトは、文字列ブロック長の残りの部分です。最後の 3 つのバイトでは、値 0 で文字列ブロックが開始しています。この文字列ブロックには、HTTP リファラが含まれます。
81	最初のバイトは、文字列ブロック タイプの残りの部分です。最後の 3 バイトで、ブロック タイプと長さを含む文字列ブロックの合計長を示しています。この場合の 8 バイトは、HTTP リファラがないため文字列ブロックにはデータが存在しないことを意味します。
82	この行の最初のバイトには、文字列ブロック長の最後が含まれます。最後の 3 バイトには、SSL 証明書のフィンガー プリントが含まれます（00000000000000000000）。
83	この行の最初のバイトには、SSL 証明書のフィンガー プリント ID の最後が含まれます。この行の残りの部分には、SSL ポリシー ID が含まれます（00000000-0000-0000-0000-000000000000）。
84	この行の最初のバイトは、SSL ポリシー ID の最後です。最後の 3 バイトは、SSL ルール ID です（0）。

ケース	説明
85	この行の最初のバイトは、SSL ルール ID の残りの部分です。次の 2 バイトは、SSL 暗号スイートです。0 は、TLS_NULL_WITH_NUL_NULL を意味します。最後のバイトは、SSL バージョンです(0)。
86	この行には SSL サーバー証明書ステータスが含まれます。0 は、未チェック を意味します。
87	この行の最初の 2 バイトは、実際の SSL アクションです。0 は、不明 を意味します。次の 2 バイトは、予想された SSL アクションです。0 は、不明を意味します。
88	この行の最初の 2 バイトは、SSL フロー ステータスです。0 は、不明 を意味します。次の 2 バイトは、SSL フロー エラーです。0 は、不明を意味します。
89	この行の最初の 2 バイトは、SSL フロー エラーの残りの部分です。次の 2 バイトは、SSL フロー メッセージです(0)。
90	この行の最初の 2 バイトは、SSL フロー メッセージです。次の 2 バイトは、SSL フロー フラグです(0)。
91	この行の最初の 2 バイトは、SSL フロー フラグの残りの部分です。次の 2 バイトで、SSL サーバー名の文字列ブロックが開始します(タイプ 0)。
92	この行の最初の 2 バイトで、文字列ブロック タイプが終了します。次の 2 バイトには、文字列ブロック長が含まれます。ブロック長は 8 です。これには、ブロックのタイプと長さが含まれ、文字列ブロックにデータが含まれていないことを意味します。
93	最初の 2 バイトには、文字列ブロック長の残りが含まれます。次の 2 バイトには、SSL URL カテゴリが含まれます。0 は、不明を意味します。
94	この行の最初の 2 バイトには、SSL URL カテゴリの残りの部分が含まれます。次の 2 バイトで、SSL セッション ID が開始します(00000000000000000000000000000000)。
95	この行の最初のバイトには、SSL セッション ID の最後が含まれます。次のバイトには、SSL セッション ID の長さが含まれます(0)。次の 2 バイトで、SSL チケット ID が開始します(00000000000000000000)。
96	この行の最初の 2 バイトには、SSL チケット ID の最後が含まれます。3 番目のバイトには、SSL チケット ID の長さが含まれます(0)。最後のバイトで、ネットワーク分析ポリシー リビジョンが開始します(4e78cb70-7842-11e6-a99b-cdb19cb553fd)。
97	この行の最初の 3 バイトには、ネットワーク分析ポリシー リビジョンの最後が含まれます。最後のバイトで、エンドポイント プロファイル ID が開始します(0)。
98	この行の最初の 3 バイトは、エンドポイント プロファイル ID です。残りのバイトで、セキュリティ グループ ID が開始します(0)。
99	この行の最初の 3 バイトは、セキュリティ グループ ID です。残りのバイトで、ロケーション IPv6 が開始します。これは、ISE と通信するインターフェイスの IP アドレスで、空白です。
100	この回線の最初の 3 バイトは、ロケーション IPv6 の最後です。残りのバイトで、HTTP レスポンスが開始します。0 は HTTP レスポンスがないことを意味します。
101	この回線の最初の 3 バイトは、HTTP レスポンスの最後です。残りのバイトで、文字列ブロックが開始します。タイプ 0 は DNS クエリです。
102	最初の 3 バイトで、文字列ブロック タイプが完了します。残りのバイトには、ブロックのタイプと長さを含む文字列ブロック長が含まれます。8 バイトは、DNS クエリにデータが存在しないことを意味します。
103	最初の 3 バイトで、文字列ブロック長が終了します。この行の残りのバイトで、DNS レコード タイプが開始します(71)。

ケース	説明
104	この行の最初のバイトで、DNS レコード タイプが終了します。次の 2 バイトは、DNS レスポンス タイプです(0)。最後のバイトで、DNS TTL が開始します。
105	この行の最初の 3 バイトは、DNS TTL です。最後のバイトで、シンクホール UUID が開始します(00000000-0000-0000-0000-000000000000)。
106	この行の最初の 3 バイトで、シンクホール UUID が終了します。最後のバイトで、最初のセキュリティ インテリジェンス リストが開始します(0)。
107	この行の最初の 3 バイトで、最初のセキュリティ インテリジェンス リストが終了します。最後のバイトで、2 番目のセキュリティ インテリジェンス リストが開始します(0)。

バージョン 5.1+ ユーザー イベントの例

次の図に、ユーザー 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	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	0	1	1	1	0	0	0	1	1	0	0	1	0	0	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	0	1	1	1	1	1	0	1	1	0
14	0	0	0	0	0	0	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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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
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	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
28	0	0	0	0	0	0	0	0	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、ユーザー情報更新メッセージを表します。
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。ユーザー変更メッセージを示す値 1004 が含まれています。
14	この行には、イベント サブタイプが含まれます。ユーザー 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 で示されるユーザー 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。

番号	説明
20	この行は、ユーザー 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ー名です。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（3-66 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、ユーザー名が「301@10.4.11.175」であることを示しています。
25	この行は、ユーザーの ID 番号を示します。
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（3-66 ページ）を参照してください。
28	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、このユーザー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、ユーザー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 サーバーの名前です。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（3-66 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 サーバーがないためです。

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-32 ページ）
- 新しい TCP サーバー メッセージの例（A-33 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 18 15	16 17 18 19 20 21 22 23	24 25 26 27 36 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	
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	

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31	
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 サーバー メッセージの例

次の図に、3.0+ の新しい TCP サーバー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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	

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31	
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	0	1	1	0	0	0	0	0	標準メッセージ ヘッダーの終了
サーバー 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	0	1	1	0	0	サーバー データ ブロックの開始
サーバー長（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	0	1	1	0	1	0	0	0	0
サーバー 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	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	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	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	0	
サーバー名（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	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	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	1	1	1	1	0	1	0	0	0	0	1	
サーバー ベンダー（Apache + Null バイト）	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	1	0	0	0		
	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	0	0	文字列ブロック ヘッダー

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31	
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	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（22 バイト）	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1	1	0	0	0	1	0	0	1	0	1	1	1	0	
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	サブサーバー 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	0	0	1	0	1	1	1	1	0	
サブサーバー 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	サブサーバー ブロックの開始
サブサーバー長（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	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	0	1	0	0	0		
サブサーバー名 - 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		

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31	
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	
サブサーバー 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	サブサーバー 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	サブサーバー ブロックの開始
サブサーバー 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	サブサーバー長
サブサーバー長（48 バイト）	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	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	
サブサーバー名 - 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	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

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31	
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	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	0	
サブサーバー 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	サブサーバー 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	1	1	0	0	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	1	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	
サーバー バナー（HTTP/1.1 414 要求）- 短縮されたサーバー 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	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	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	サーバー 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 Cisco Secure Firewall 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、Cisco Secure Firewall 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（2-15 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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）																																
Device ID																																
イベント ID（Event 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																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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（Source Port）																	接続先ポート															
IP プロトコル ID									影響フラグ								影響								ブロック							
MPLS ラベル																																
VLAN ID（Admin. 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）																																
ユーザー ID（User 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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-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
Device 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Device 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（Event 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 Cisco Secure Firewall システム プリプロセッサの ID 番号。

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
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。
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ー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ーを実行しているか（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ー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）。Cisco Secure Firewall 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（Admin. 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。
ユーザー ID	uint32	ユーザーの内部 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（2-15 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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）																																
Device ID																																
イベント ID（Event 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）																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
送信元 IPv6 アドレス（続き）																																
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（Admin. 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）																																
ユーザー ID（User 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）																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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）																																

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
Device 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Device 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（Event 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。

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
ジェネレータ ID	uint32	イベントを生成した Cisco Secure Firewall 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 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ー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ーを実行しているか（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ー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）。Cisco Secure Firewall 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（Admin. 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。
ユーザー ID（User ID）	uint32	ユーザーの内部 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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																																
Device ID																																
イベント ID（Event 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（Admin. 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）																																
ユーザー ID（User 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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）。
Device 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Device 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（Event 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 Cisco Secure Firewall 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ー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ーを実行しているか（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ー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）。Cisco Secure Firewall 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（Admin. 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。
ユーザー ID（User ID）	uint32	ユーザーの内部 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-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
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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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																																
Device ID																																
イベント ID（Event 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																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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（Admin. 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）																																
ユーザー ID（User 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																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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）																																
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）。
Device 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Device 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（Event 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 Cisco Secure Firewall 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ー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ーを実行しているか（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ー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）。Cisco Secure Firewall 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（Admin. 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。
ユーザー ID（User ID）	uint32	ユーザーの内部 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（Admin. 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）																																
ユーザー ID（User 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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）。
Device 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Device 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（Event 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 Cisco Secure Firewall 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ー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ーを実行しているか（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ー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）。Cisco Secure Firewall 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（Admin. 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。
ユーザー ID（User ID）	uint32	ユーザーの内部 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)。

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
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

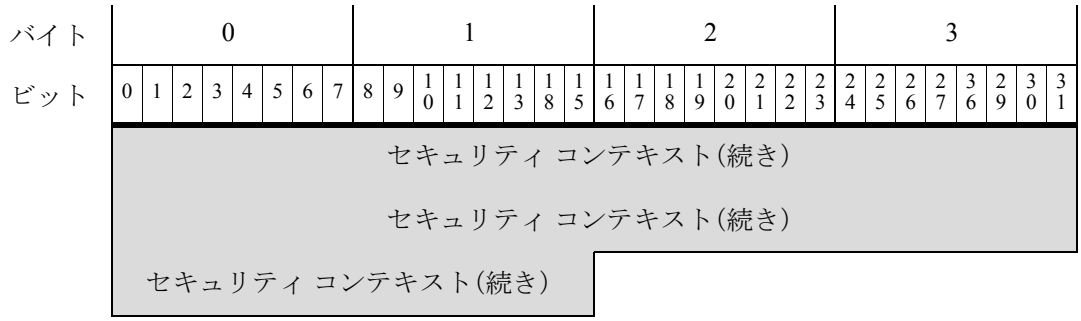
侵入イベント レコードのフィールドは、次の図で網掛けされています。レコード タイプは 400 であり、ブロック タイプはシリーズ 2 セットのデータ ブロックの 42 です。

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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（Admin. 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）																																
ユーザー ID（User 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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															
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）																																



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（Device 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Device 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（Event 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 Cisco Secure Firewall 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。

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
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
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ー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ーを実行しているか（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ー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）。Cisco Secure Firewall 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`

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	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）
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（Admin. 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。
ユーザー ID（User ID）	uint32	ユーザーの内部 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。

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
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。
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

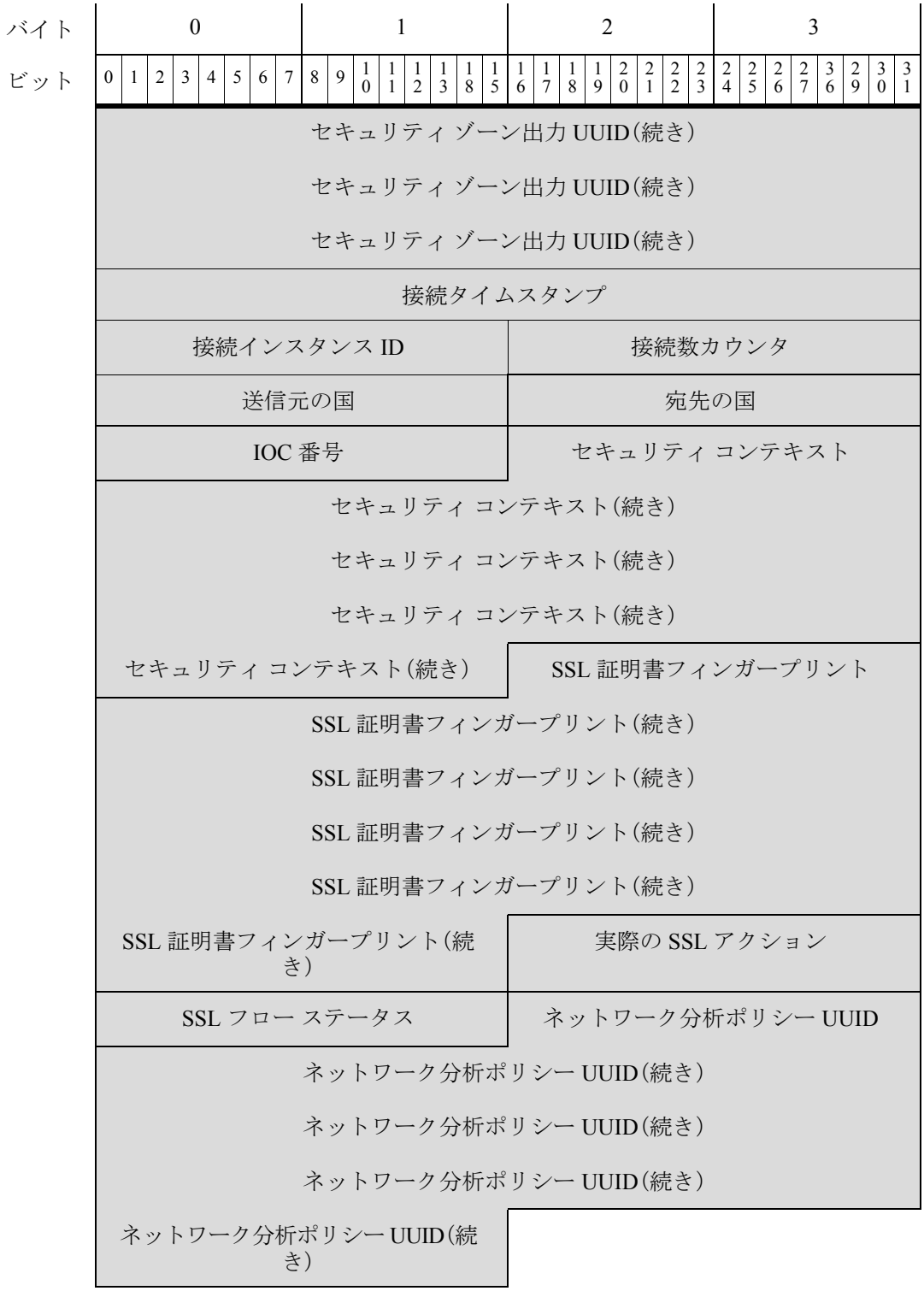
侵入イベント レコードのフィールドは、次の図で網掛けされています。レコード タイプは 400 であり、ブロック タイプはシリーズ 2 セットのデータ ブロックの 45 です。これはブロック タイプ 42 に取って代わり、ブロック タイプ 60 により取って代わられます。SSL サポート用およびネットワーク分析ポリシー用のフィールドが追加されました。

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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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）																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ブロック タイプ(45)																																
ブロック長																																
デバイスID（Device ID）																																
イベント ID（Event 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）																																
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（Admin. VLAN ID）																	パッド															
ポリシー UUID 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
ポリシー UUID（続き）																																
ポリシー UUID（続き）																																
ユーザー ID（User 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																																
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																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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)
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
ネットワーク分析ポリシー UUID
ネットワーク分析ポリシー UUID(続き)
ネットワーク分析ポリシー UUID(続き)
ネットワーク分析ポリシー UUID(続き)
ネットワーク分析ポリシー 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-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（Device 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Device 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（Event 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 Cisco Secure Firewall 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ー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ーを実行しているか（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ー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）。Cisco Secure Firewall 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（Admin. 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。
ユーザー ID（User ID）	uint32	ユーザーの内部 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-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
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。
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 サーバー証明書の 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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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。

侵入イベント レコード 6.x

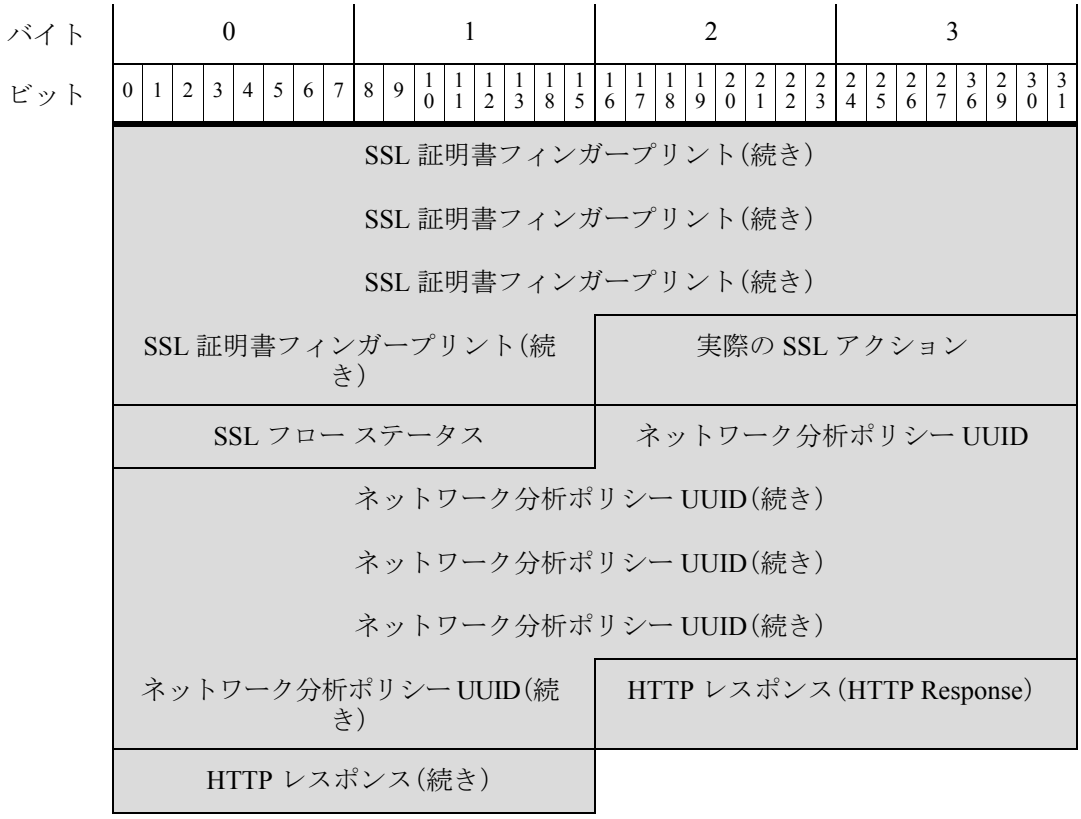
侵入イベント レコードのフィールドは、次の図で網掛けされています。レコード タイプは 400 で、ブロック タイプはシリーズ 2 セットのデータ ブロックの 60 です。これはブロックタイプ 45 に取って代わり、7.0 ではブロックタイプ 81 により取って代わられます。HTTP レスポンス フィールドが追加されました。

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.x 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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（Device ID）																																
イベント ID（Event 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（Admin. 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）																																
ユーザー ID（User 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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）																	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）																																



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-8　　侵入イベント レコード 6.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 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（Device 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Device 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（Event 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。

表 B-8　侵入イベント レコード 6.x のフィールド（続き）

フィールド	データタイプ	説明
ジェネレータ ID	uint32	イベントを生成した Cisco Secure Firewall 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 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 B-8　侵入イベント レコード 6.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ー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ーを実行しているか（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ー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）。Cisco Secure Firewall 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 B-8　侵入イベント レコード 6.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（Admin. 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。
ユーザー ID（User ID）	uint32	ユーザーの内部 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。

表 B-8　侵入イベント レコード 6.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。
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 サーバー証明書の 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-8　侵入イベント レコード 6.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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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。
HTTP レスポンス	uint32	HTTP 要求の応答コード。

侵入イベント レコード 7.0

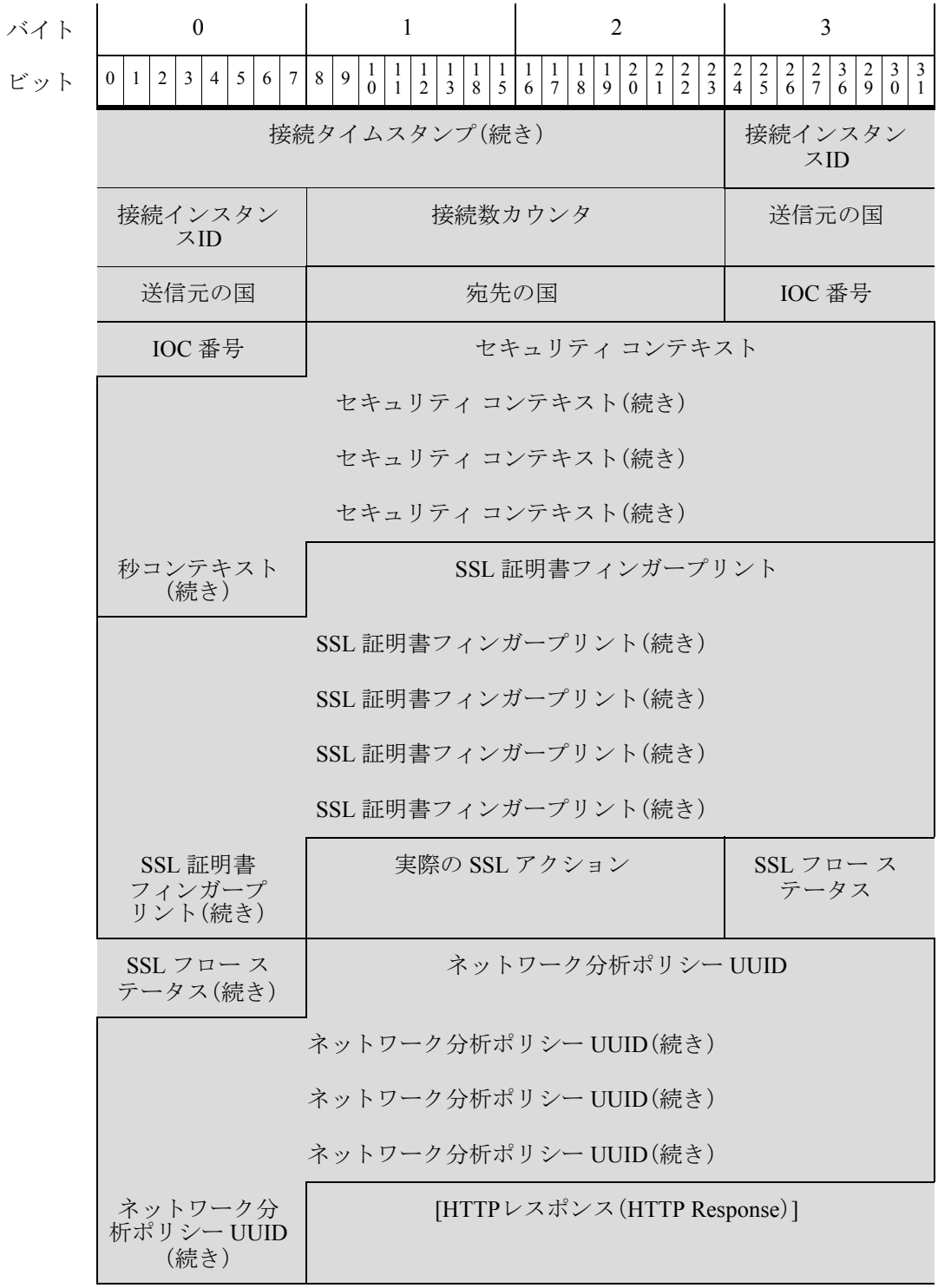
侵入イベント レコードのフィールドは、次の図で網掛けされています。レコードタイプは 400 であり、ブロックタイプはデータブロックのシリーズ 2 セットの 81 です。これはブロックタイプ 60 に取って代わり、ブロックタイプ 85 により取って代わられます。インライン結果の理由、入力および出力仮想ルート転送、および Snort バージョンのフィールドが追加されました。ブロック フィールドの名前がインライン結果に変更されました。

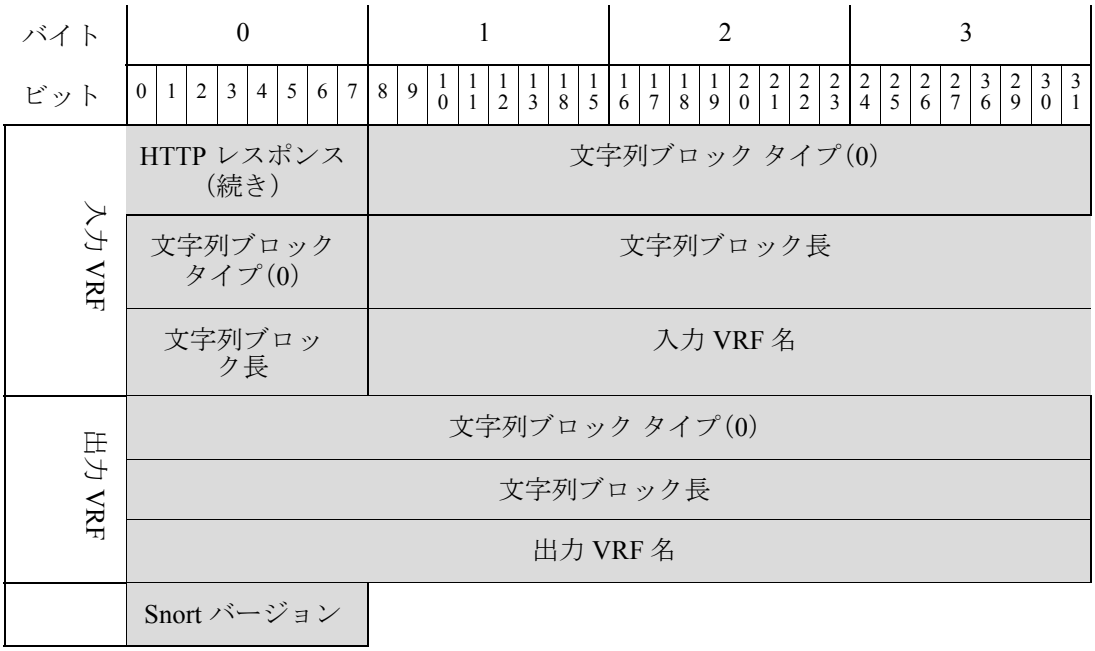
ストリーム要求メッセージでイベントタイプコード 12 とバージョンコード 10 を要求する拡張要求によってのみ、eStreamer から 7.0 の侵入イベントを要求できます（拡張要求の送信の詳細については、拡張要求の送信（2-4 ページ）を参照してください）。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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（81）																																
ブロック長																																
デバイスID（Device ID）																																
イベント ID（Event 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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								[インライン結果（Inline Result）]							
インライン結果理由									MPLSラベル（MPLS Label）																							
MPLS ラベル（続き）									VLAN ID（Admin. VLAN ID）																パッド							
パッド（続き）									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） ポリシー UUID（続き）																									ユーザー ID（User ID）							
ユーザー 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）																									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																									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）																									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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
アクセスコントロールルール 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)
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)
インターフェイス出力 UUID(続き)
秒ゾーン入力 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 ゾーン入力 UUID(続き)
秒ゾーン出力 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)
セキュリティ ゾーン出力 UUID(続き)
接続タイムスタンプ


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
接続タイムスタンプ(続き)
接続インスタンスID
接続インスタンスID
接続数カウンタ
送信元の国
送信元の国
宛先の国
IOC 番号
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)
秒コンテキスト(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
SSL フロー ステータス(続き)
ネットワーク分析ポリシー UUID
ネットワーク分析ポリシー UUID(続き)
ネットワーク分析ポリシー UUID(続き)
ネットワーク分析ポリシー UUID(続き)
ネットワーク分析ポリシー UUID(続き)
[HTTPレスポンス(HTTP Response)]



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-9　　侵入イベント レコード 7.0 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 81 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（Device 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Device 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（Event 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 Cisco Secure Firewall 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 B-9　侵入イベント レコード 7.0 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 B-9　侵入イベント レコード 7.0 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ー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ーを実行しているか（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ー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）。Cisco Secure Firewall 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 B-9　侵入イベント レコード 7.0 のフィールド（続き）

フィールド	データタイプ	説明
[インライン結果(Inline Result)]	uint8	インライン結果を示す値。 • 0:合格 • 1:ドロップ • 2:ドロップされる可能性あり(設定では許可されていない) • 3:部分的にドロップ
インライン結果理由	uint8	インライン結果の理由を示す値。 • 1:パッシブモードまたはタップモードのインターフェイス • 2:「検出」検査モードの侵入ポリシー • 3:「検出」検査モードのネットワーク分析ポリシー • 4:接続タイムアウト • 5:接続クローズ(内部使用) • 6:接続クローズ(内部使用) • 7:接続クローズ(内部使用)
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID（Admin. 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。
ユーザー ID（User ID）	uint32	ユーザーの内部 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。

表 B-9　侵入イベント レコード 7.0 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 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。
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 サーバー証明書の 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-9　侵入イベント レコード 7.0 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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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。
HTTP レスポンス	uint32	HTTP 要求の応答コード。

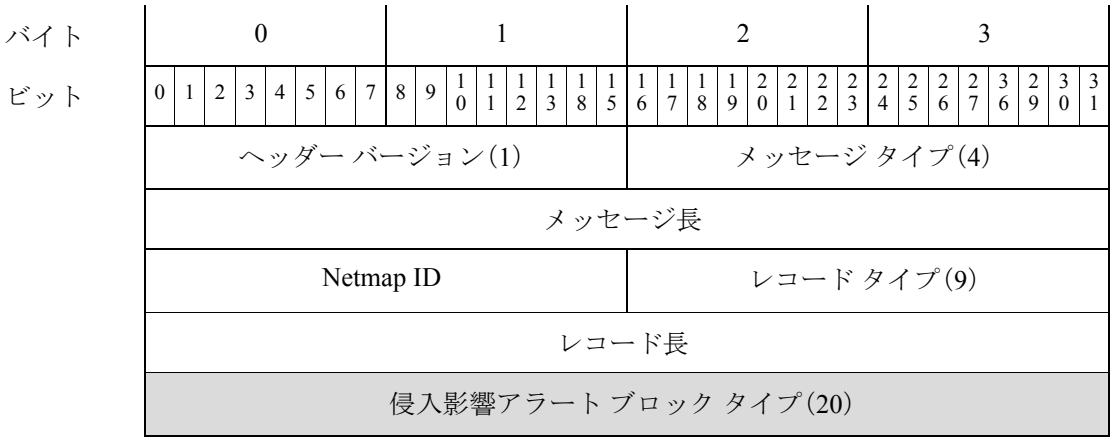
表 B-9　侵入イベント レコード 7.0 のフィールド（続き）

フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	入力 VRF 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。ブロックタイプとヘッダーフィールドの 8 バイト、および入力 VRF 名フィールドのバイト数が含まれています。
入力 VRF 名	文字列	トラフィックがネットワークに入るときに通過する仮想ルータ。
文字列ブロック タイプ	uint32	出力 VRF 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。ブロックタイプとヘッダーフィールドの 8 バイト、および出力 VRF 名フィールドのバイト数が含まれています。
出力 VRF 名	文字列	トラフィックがネットワークから出るときに通過する仮想ルータの名前。
Snort バージョン	uint8	Snort のバージョン番号。

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（4-65 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（2-13 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	侵入影響アラート ブロック長																															
	イベント ID（Event ID）																															
	Device 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-10　　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（Event ID）	uint32	イベント ID 番号を表示します。
Device 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-10　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ー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ーを実行しているか（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ー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）。Cisco Secure Firewall 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-10　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（4-75 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。

侵入イベント追加データ レコード

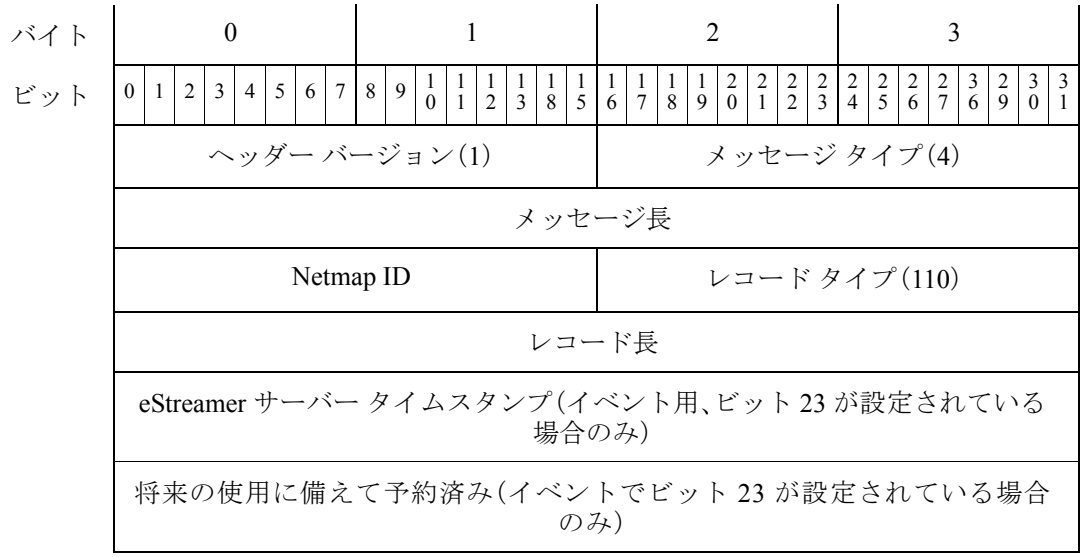
eStreamer サービスは、侵入イベント追加データ レコードの侵入イベントに関連付けられたイベント追加データを送信します。レコード タイプは常に 110 です。

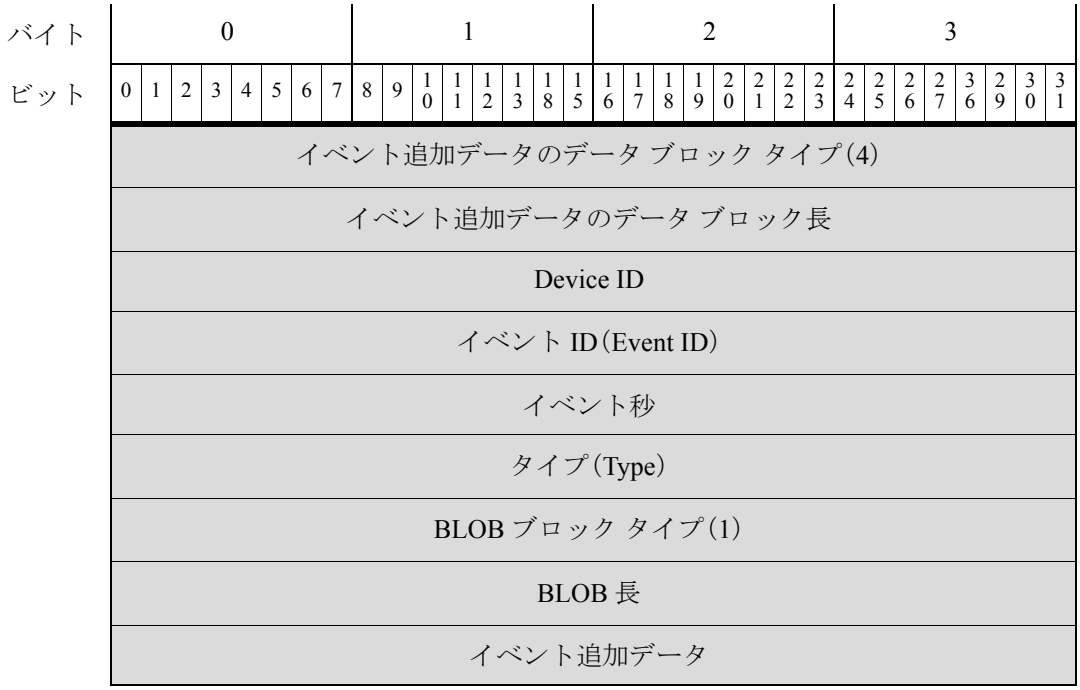
このレコードは、バージョン 7.1 で廃止されました。引き続き要求はできますが、レコードは生成されません。

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（3-60 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 サーバー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（B-71 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（2-15 ページ）を参照してください。





イベント追加データのブロック構造には、Cisco Secure Firewall 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 B-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 (3-60 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。
Device ID	uint32	管理対象デバイス ID 番号。
イベント ID (Event 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(Type)	uint32	追加データのタイプの識別子。次に例を示します。 • 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。

表 B-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 （続き）

フィールド	データタイプ	説明
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（variable）	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。

このレコードは、バージョン 7.1 で廃止されました。引き続き要求はできますが、レコードは生成されません。

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 (2-15 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。

ブロック構造には、Cisco Secure Firewall 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 B-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(Type)	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。このフィールドは、このレコードの固有キーです。
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(Name)]	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)。

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ー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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
		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...															
ユーザー（User）		文字列ブロック タイプ（0）																															
		文字列ブロック長																															
		ユーザー...																															
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（File size）																															
		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（Name）]		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...																							

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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 イベントのデータ 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 エンドポイント向け AMP 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。
Timestamp	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。
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。

表 B-13　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
文字列ブロック長	uint32	ユーザー文字列データ 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、およびユーザー フィールドのバイト数を含む)。
ユーザー(User)	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ー。これらのユーザーはユーザー 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(File size)	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。
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。

マルウェア イベント データ ブロック 5.1.1.x

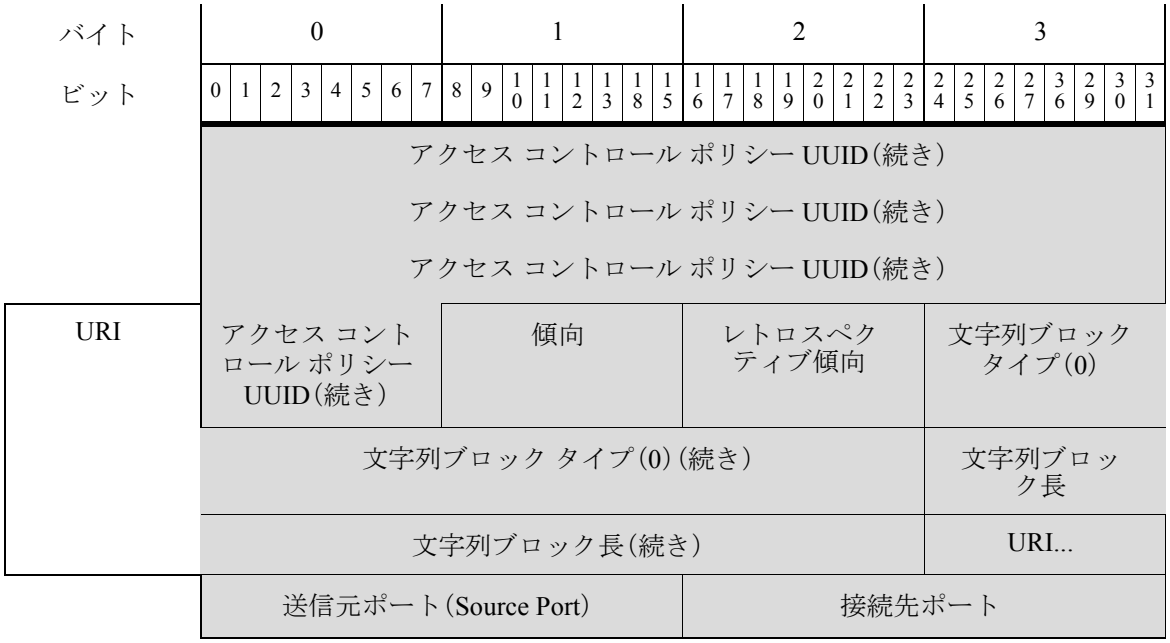
eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザーに関する情報が含まれています。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 24 です。マルウェア イベント レコードの一部として、イベント バージョン 2 およびイベント コード 101 の要求メッセージ内にマルウェア イベント フラグ(要求フラグ フィールドのビット 30)を設定して、イベントを要求します。

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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
マルウェア イベント ブロック タイプ(24)																																
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)																																

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
		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...															
ユーザー（User）		文字列ブロック タイプ（0）																															
		文字列ブロック長																															
		ユーザー...																															
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（File size）																															
		ファイル タイプ								ファイルのタイムスタンプ																							

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
親ファイル [名前(Name)]	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...																															
	Device 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(Direction)								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(Application ID)																							
	アプリケーションID（続き）								ユーザー ID(User ID)																							
	ユーザー ID（続き）								アクセス コントロール ポリシー UUID																							



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 B-14　　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 エンドポイント向け AMP 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。
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。

表 B-14　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
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	ユーザー文字列データ 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、およびユーザー フィールドのバイト数を含む)。
ユーザー(User)	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ー。これらのユーザーはユーザー 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 (File size)	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。

表 B-14　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
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。
Device 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(Direction)	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(Application 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。
ユーザー ID(User 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ーの ID 番号。

表 B-14　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）

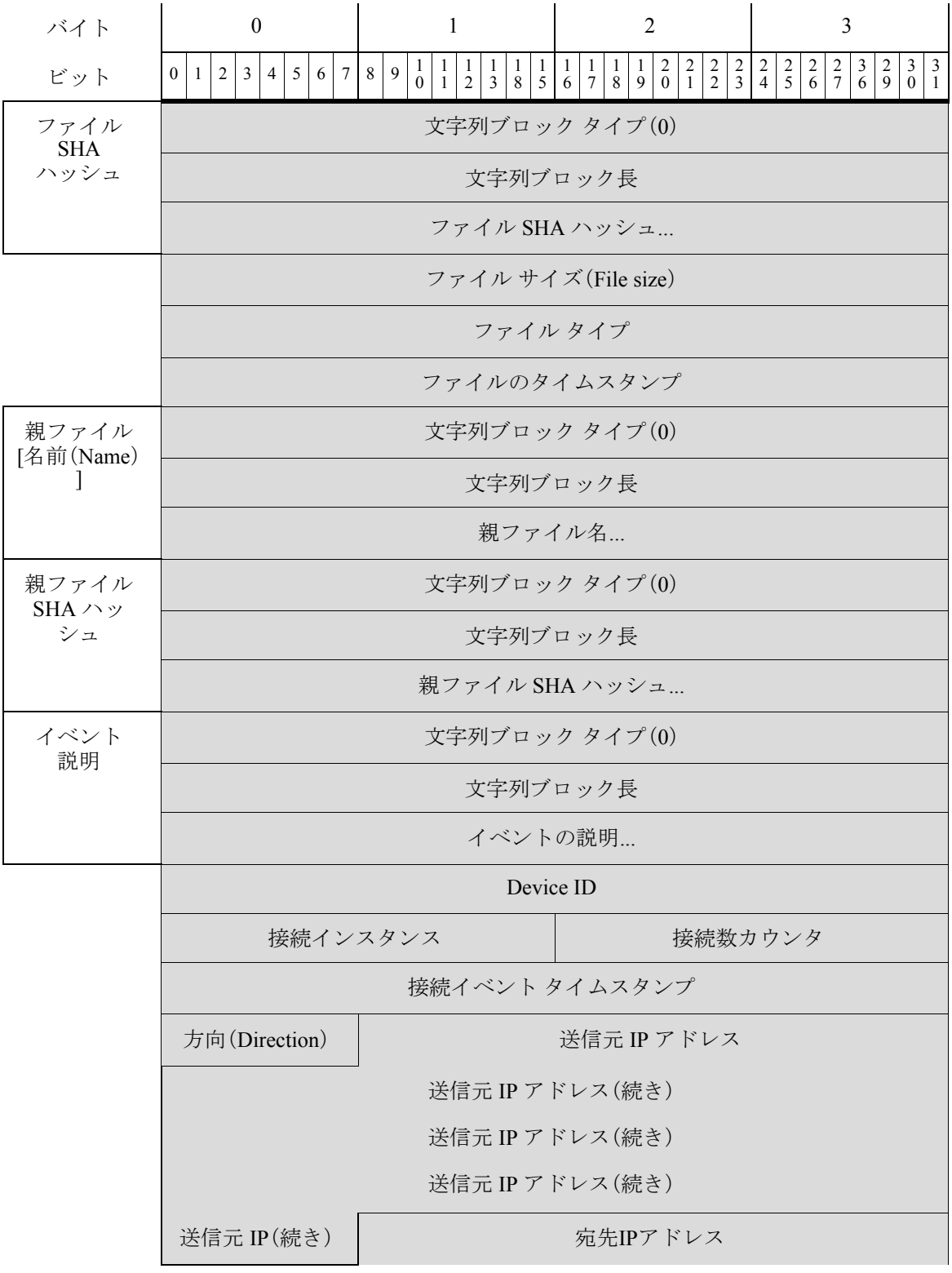
フィールド	データタイプ	説明
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する ID 番号。
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1（CLEAN）：ファイルはクリーンであり、マルウェアは含まれていません。 • 2（UNKNOWN）：ファイルにマルウェアが含まれているかどうかは不明です。 • 3（MALWARE）：ファイルにはマルウェアが含まれています。 • 4（CACHE_MISS）：ソフトウェアは Cisco クラウドに特性を確認する要求を送信できませんでした。 • 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。

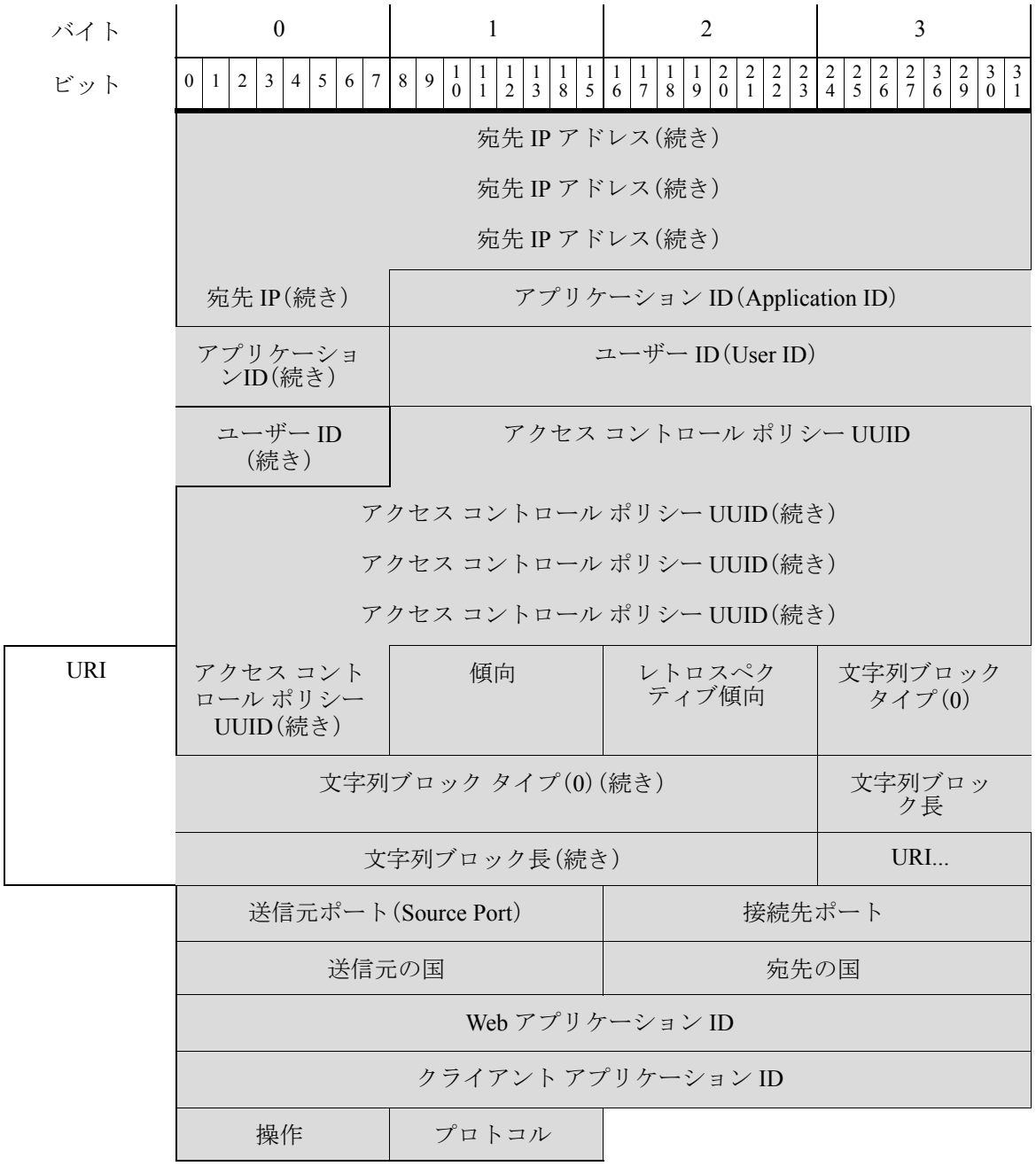
マルウェア イベント データ ブロック 5.2.x

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ー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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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...															
ユーザー(User)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザー...																															
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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 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(File size)
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(Name)]
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...
Device 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(Direction)
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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 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(Application ID)
アプリケーション ID(続き)
ユーザー ID(User ID)
ユーザー 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(Source Port)
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 イベントのデータ ブロックのフィールドについての説明です。

表 B-15　　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 エンドポイント向け AMP 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	ユーザー文字列データ 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、およびユーザー フィールドのバイト数を含む)。
ユーザー(User)	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ー。これらのユーザーはユーザー 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-15　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（File size）	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。
Device ID	uint32	イベントを生成したデバイスの ID。

表 B-15　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（Direction）	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（Application 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。
ユーザー ID（User 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ーの 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。

表 B-15　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	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:マルウェア許可リスト
プロトコル	uint8	ユーザーが指定した 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ー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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	マルウェア イベント ブロック タイプ(35)																															
	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...																							
ユーザー (User)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザー...																															
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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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(File size)																															
	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(Name)]	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...																															
	Device 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(Direction)								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 18 15
16 17 18 19 20 21 22 23
24 25 26 27 36 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(Application ID)
アプリケーションID(続き)
ユーザー ID(User ID)
ユーザー 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(Source Port)
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 イベントのデータ ブロックのフィールドについての説明です。

表 B-16　　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 エンドポイント向け AMP 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	ユーザー文字列データ 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、およびユーザー フィールドのバイト数を含む)。
ユーザー(User)	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ー。これらのユーザーはユーザー 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-16　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 (File size)	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、エンドポイント向け AMP 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。

表 B-16　　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
Device 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（Direction）	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（Application 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。
ユーザー ID（User 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ーの 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）：ファイルがユーザー定義のハッシュと一致するため、ユーザー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-16　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：マルウェア許可リスト
プロトコル	uint8	ユーザーが指定した 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

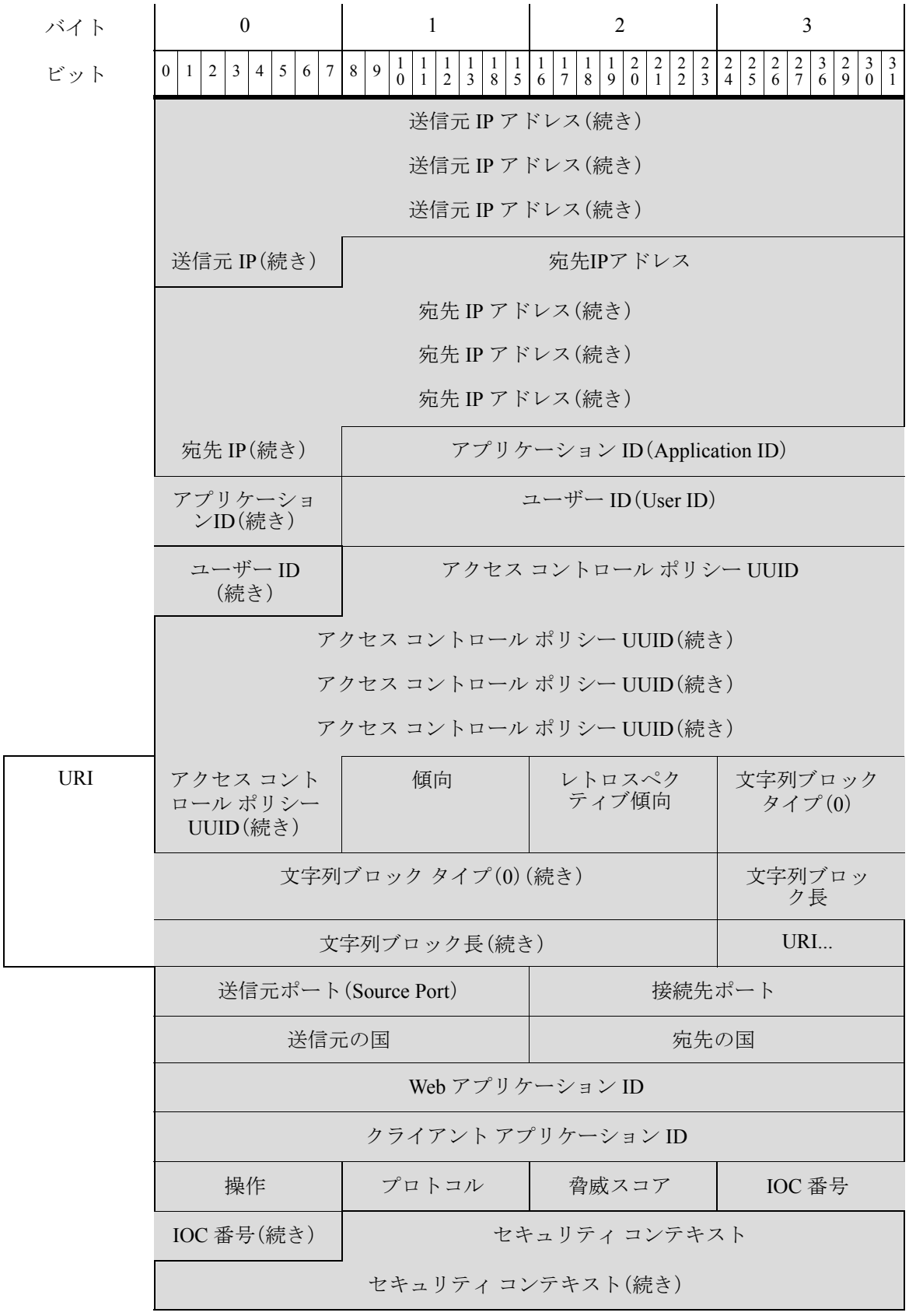
eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザーに関する情報が含まれています。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 44 で

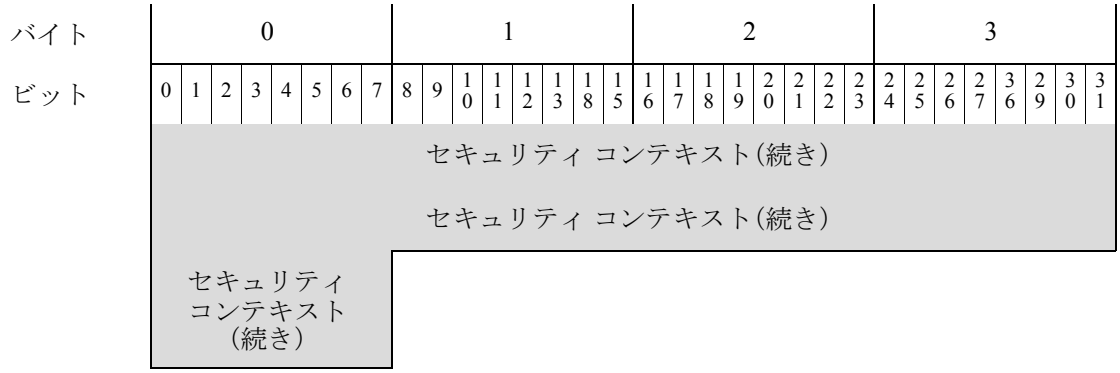
す。これはブロック 35 に取って代わります。マルウェア イベント レコードの一部として、イベント バージョン 5 およびイベント コード 101 の要求メッセージ内にマルウェア イベント フラグ（要求フラグ フィールドのビット 30）を設定して、イベントを要求します。

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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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...																							
ユーザー（User）	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 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(File size)																															
	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(Name)]	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 (Device 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(Direction)								送信元 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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(Application ID)
アプリケーションID(続き)
ユーザー ID(User ID)
ユーザー 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(Source Port)
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 イベントのデータ ブロックのフィールドについての説明です。

表 B-17　　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 エンドポイント向け AMP 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 クラウド 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	ユーザー文字列データ 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、およびユーザー フィールドのバイト数を含む)。

表 B-17　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
ユーザー（User）	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ー。これらのユーザーはユーザー 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（File size）	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、エンドポイント向け AMP 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-17　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（Device 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(Direction)	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（Application 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。
ユーザー ID（User 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ーの 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-17　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）：ファイルがユーザー定義のハッシュと一致するため、ユーザー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：マルウェア許可リスト

表 B-17　　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）

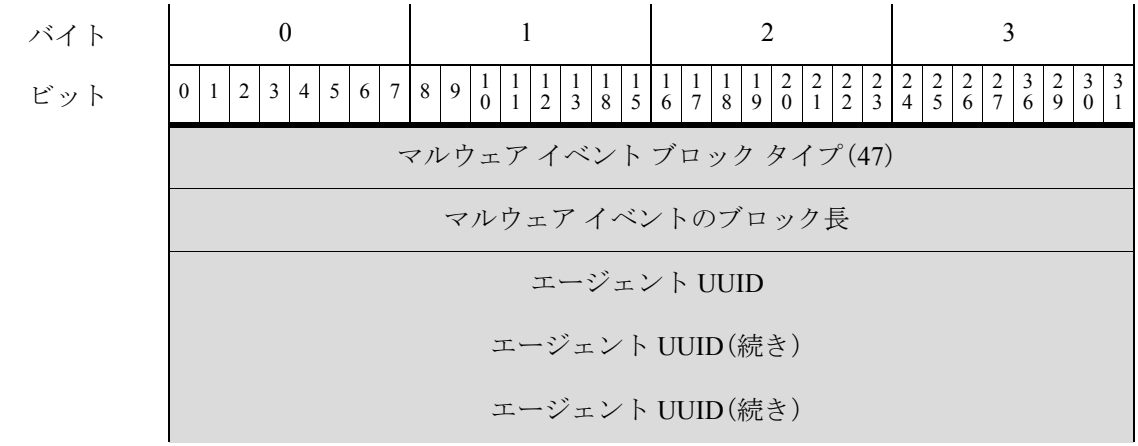
フィールド	データタイプ	説明
プロトコル	uint8	ユーザーが指定した IANA プロトコル数。次に例を示します。 • 1：ICMP • 4：IP • 6：TCP • 17：UDP これは現時点では TCP のみです。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値（0 ～ 100）。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト（仮想ファイアウォール）の ID 番号。マルチコンテキスト モードの ASA FirePOWER 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

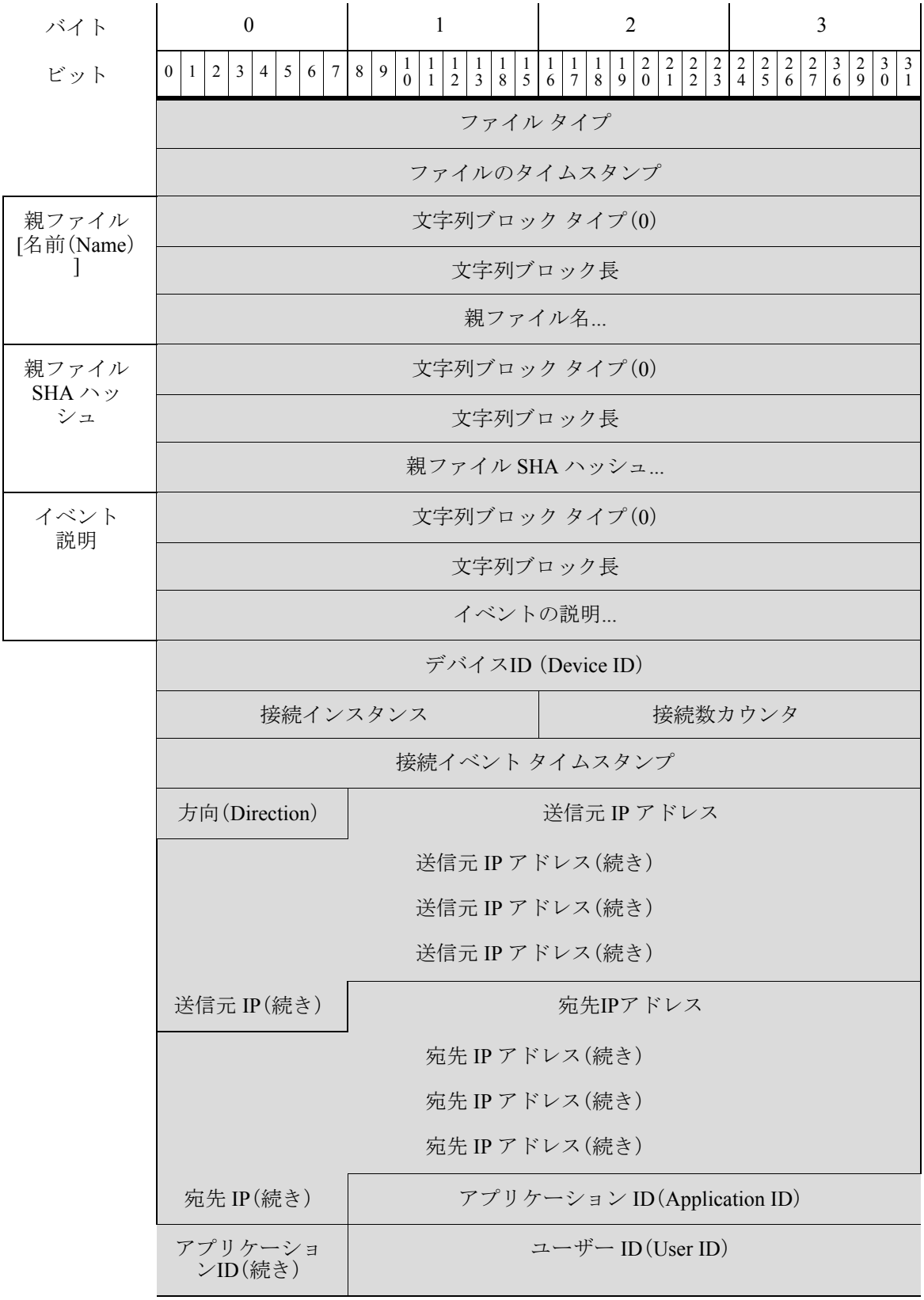
eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザーに関する情報が含まれています。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 47 です。これはブロック 44 に取って代わり、ブロックによって取って代わられます。SSL とファイル アーカイブ サポート用のフィールドが追加されました。

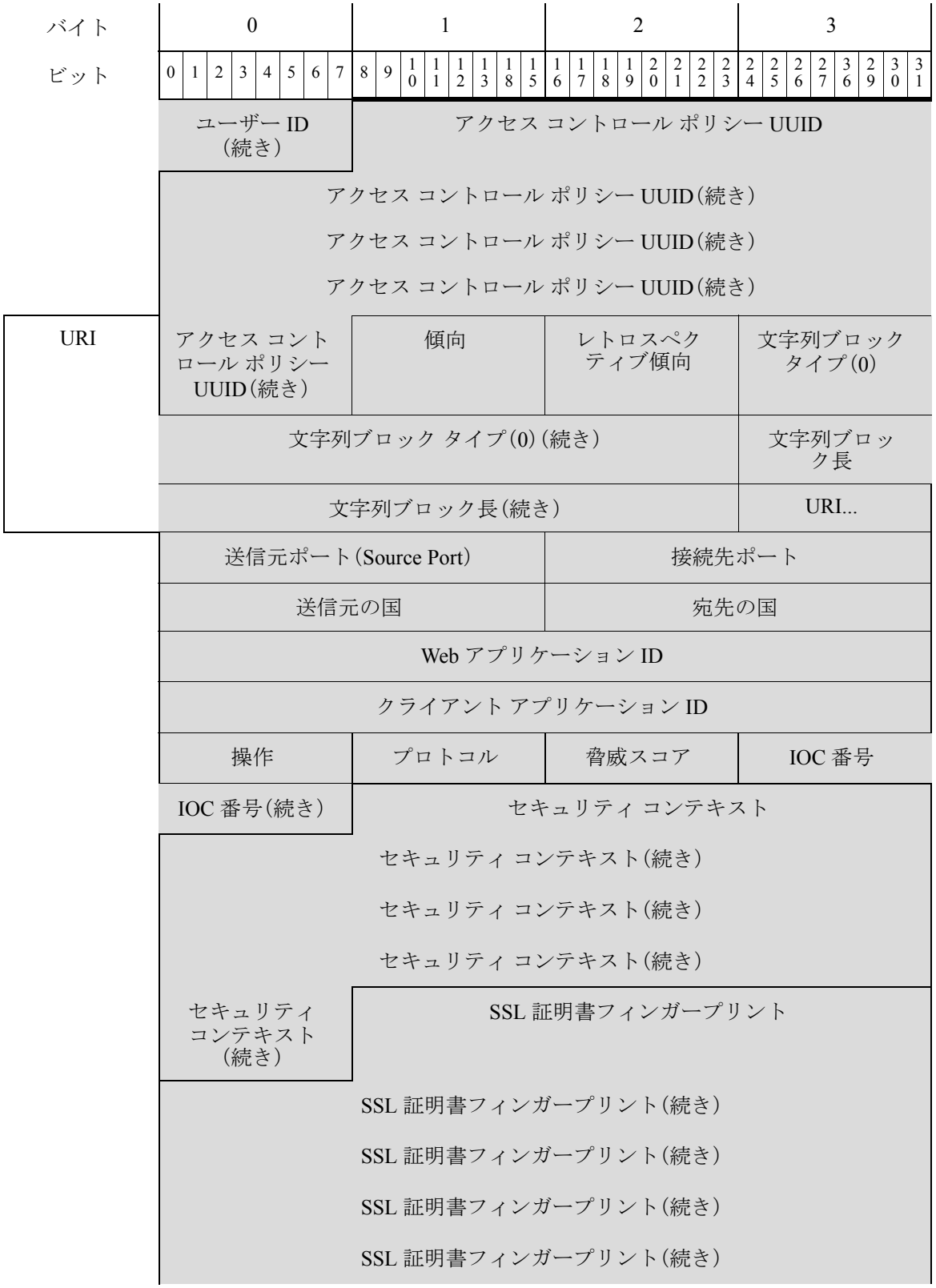
マルウェア イベント レコードの一部としてイベントを要求するには、イベント バージョン 6 およびイベント コード 101 の要求メッセージ内に、マルウェア イベント フラグ（要求フラグ フィールドのビット 30）を設定します。

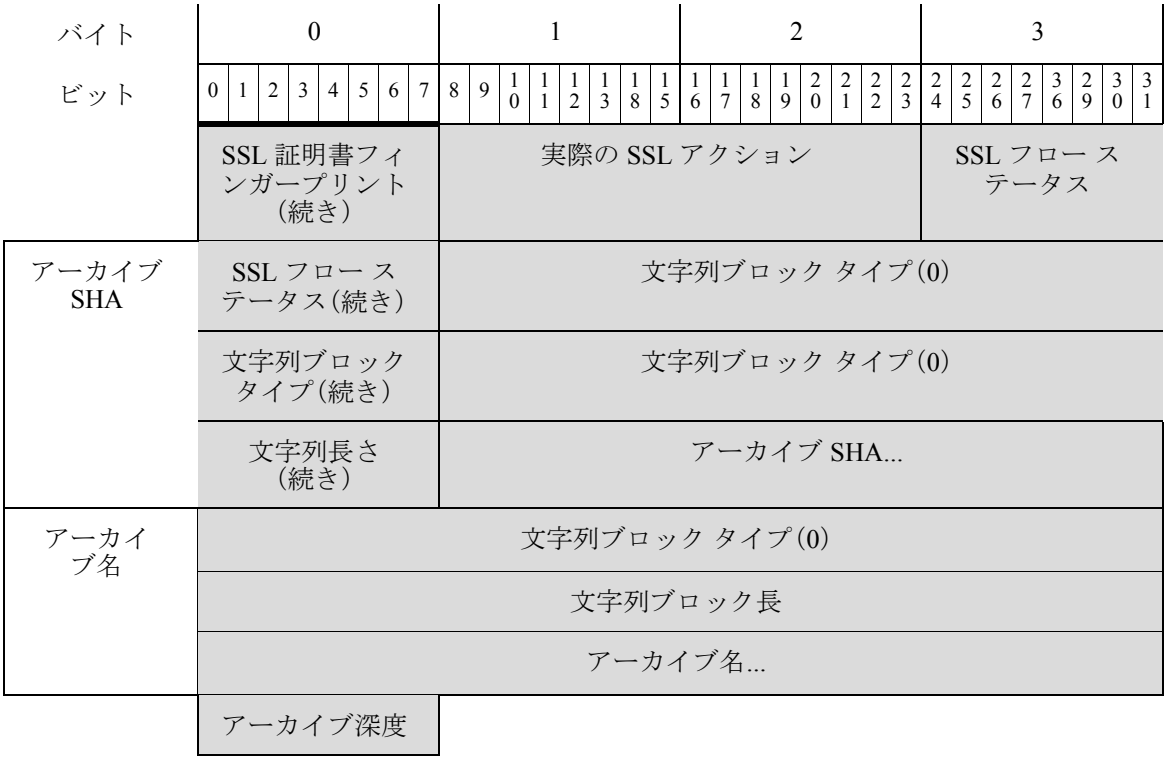
次の図は、マルウェア イベント データ ブロックの構造を示しています。



	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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...																							
ユーザー（User）	文字列ブロック タイプ（0）																																
	文字列ブロック長																																
	ユーザー...																																
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（File size）																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 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(Name)]
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 (Device 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(Direction)
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(Application ID)
アプリケーションID(続き)
ユーザー ID(User 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
ユーザー 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（Source Port）
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）



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 B-18　　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 エンドポイント向け AMP 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 クラウド 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 B-18　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	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	ユーザー文字列データ 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、およびユーザー フィールドのバイト数を含む)。
ユーザー(User)	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ー。これらのユーザーはユーザー 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(File size)	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、エンドポイント向け AMP 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 B-18　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	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（Device 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(Direction)	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(Application 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。
ユーザー ID(User 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ーの ID 番号。

表 B-18　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
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）：ファイルがユーザー定義のハッシュと一致するため、ユーザー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-18　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:マルウェア許可リスト • 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	ユーザーが指定した 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 サーバー証明書の SHA1 ハッシュ。

表 B-18　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-18　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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー証明書の検証エラー」 • 28:「無効な操作」

表 B-18　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）

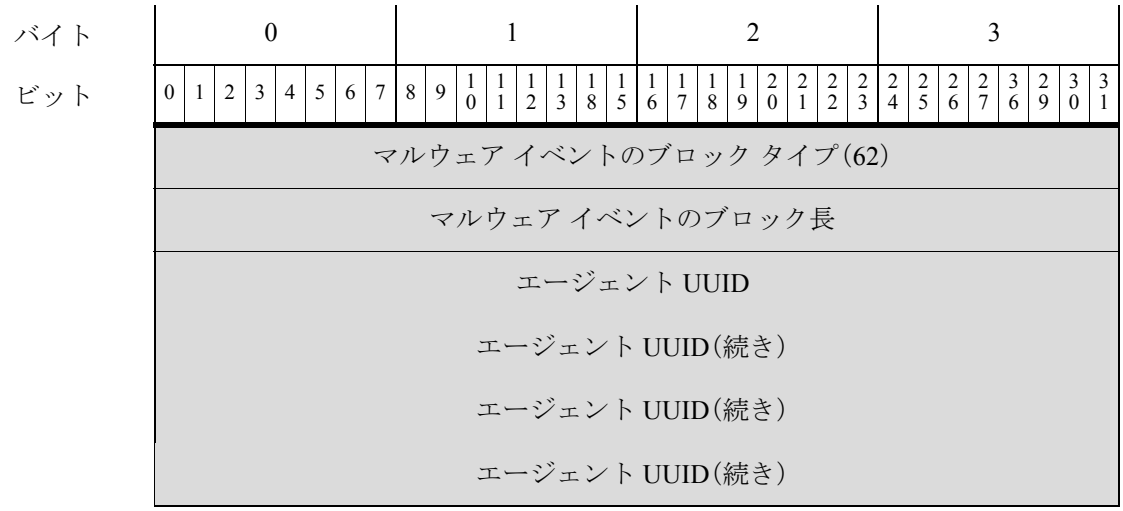
フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	アーカイブ SHA を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	アーカイブ SHA 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および侵入ポリシー名のバイト数を含む)。
アーカイブ SHA	string	ファイルが含まれる親アーカイブの SHA1 ハッシュ。
文字列ブロック タイプ	uint32	アーカイブ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	アーカイブ名文字列データ 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 データ ブロック 6.x

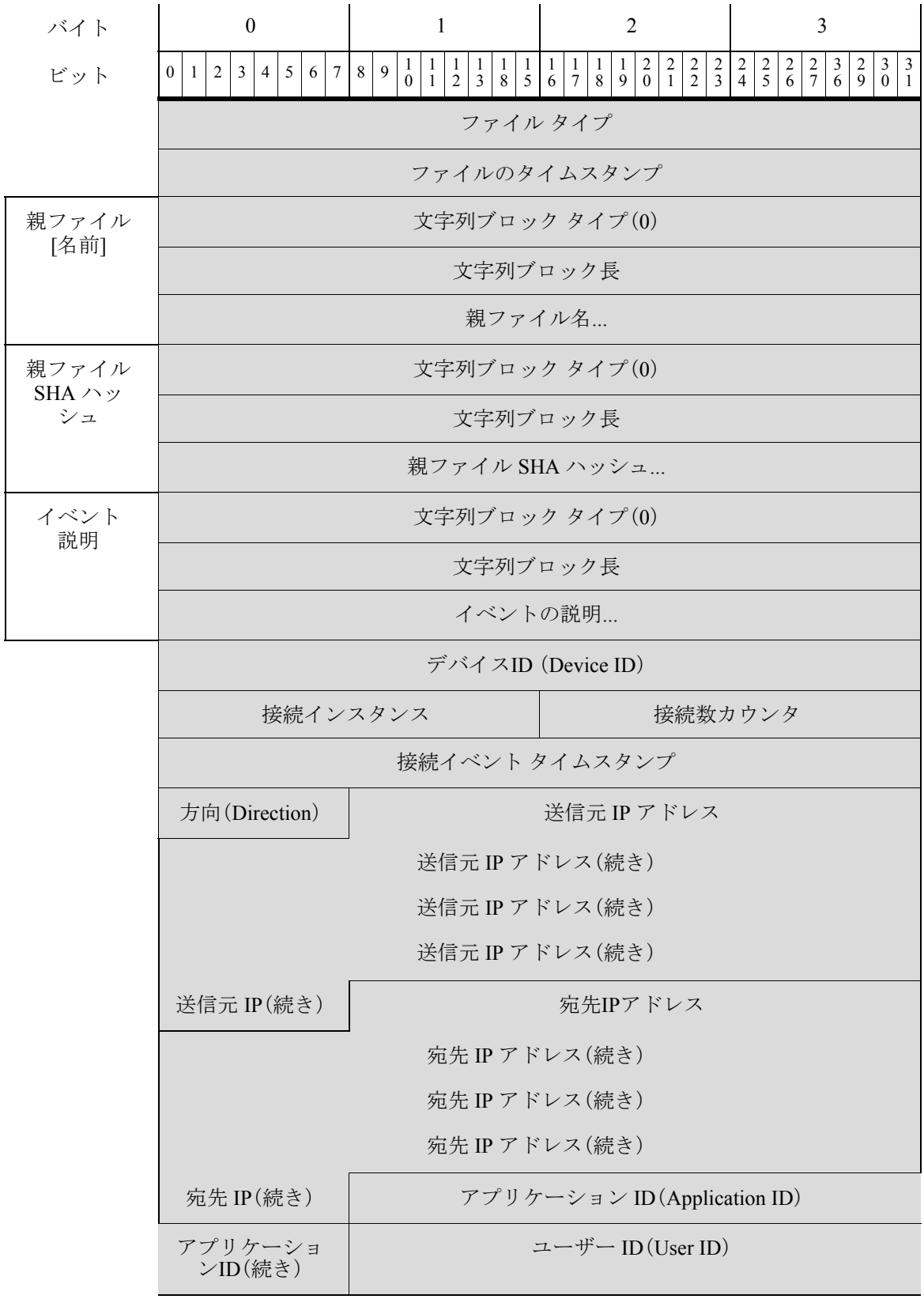
eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザーに関する情報が含まれています。マルウェア イベントのデータ ブロックは、シリーズ 2 グループのブロックのブロック タイプ 62 です。これはブロック 47 に取って代わります。HTTP レスポンスのフィールドが追加されました。これはブロック 80 により取って代わられます。

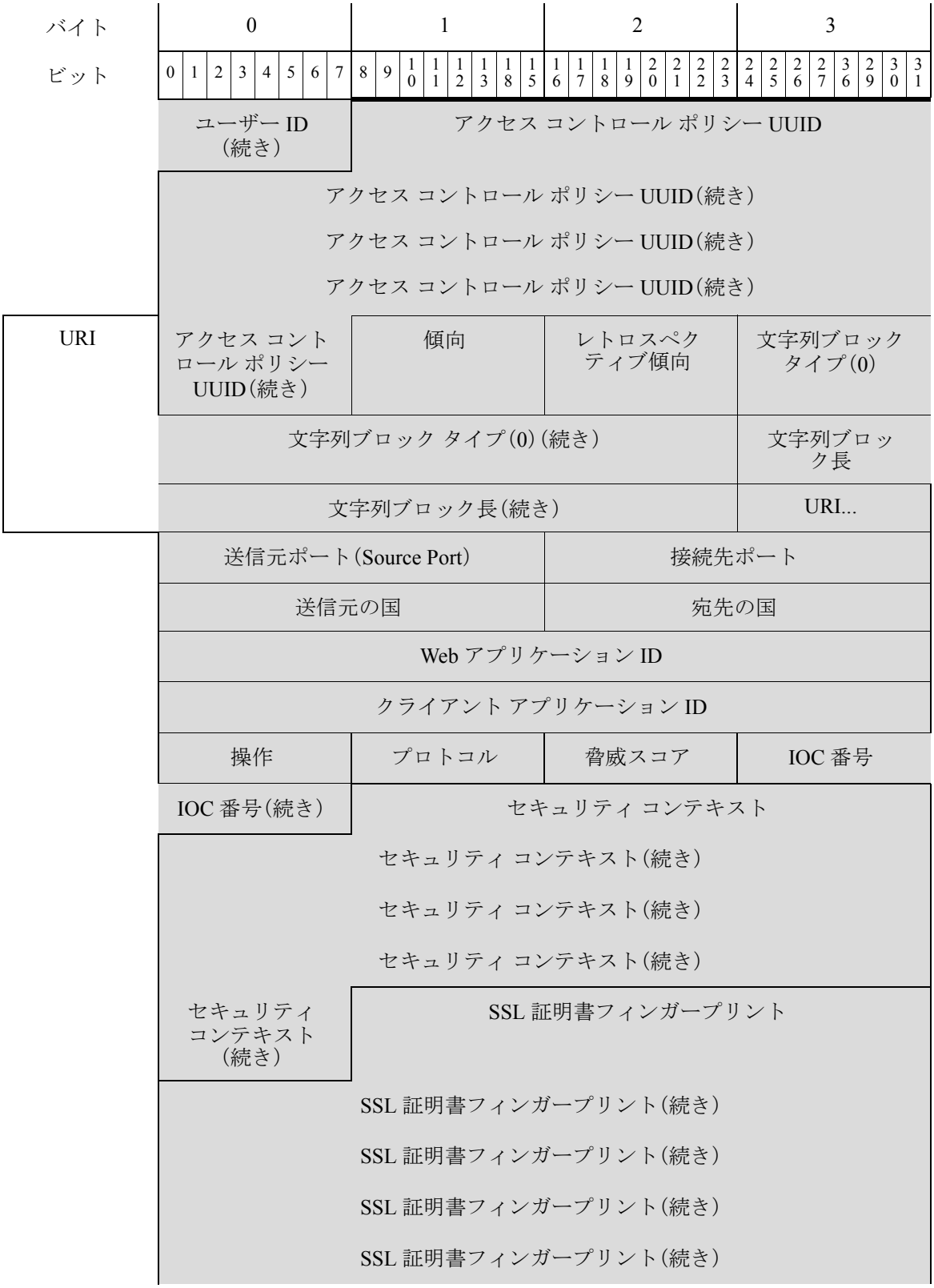
イベント バージョンが 7 でイベント コードが 101 の要求メッセージでマルウェア イベント フラグ([要求フラグ(Request Flags)] フィールドのビット 30)を設定することで、マルウェア イベント レコードの一部としてイベントを要求します。

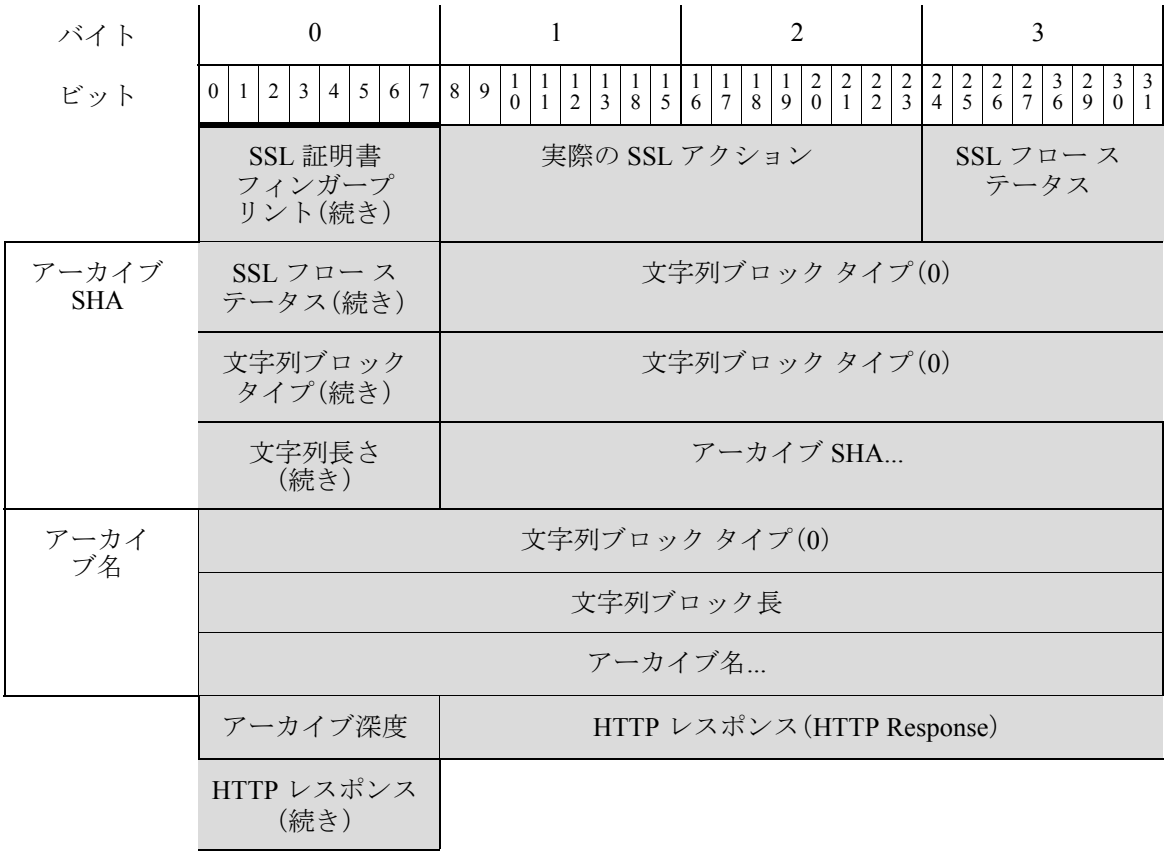
次の図に、マルウェア イベントのデータ ブロックの構造を示します。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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...																							
ユーザー	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー...																															
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（File size）																															


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 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]
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 (Device 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(Direction)
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(Application ID)
アプリケーション ID(続き)
ユーザー ID(User 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
ユーザー 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（Source Port）
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）



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 B-19　　マルウェア イベント データ ブロック 6.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 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 エンドポイント向け AMP 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 クラウドの、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。

表 B-19　マルウェア イベント データ ブロック 6.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	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	ユーザー文字列データ 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、およびユーザー フィールドのバイト数を含む）。
ユーザー（User）	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ー。これらのユーザーはユーザー 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（File size）	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、エンドポイント向け AMP 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。

表 B-19　マルウェア イベント データ ブロック 6.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（Device 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(Direction)	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(Application 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。

表 B-19　マルウェア イベント データ ブロック 6.x のフィールド（続き）

フィールド	データタイプ	説明
ユーザー ID（User 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ーの 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 AMP 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 AMP クラウド サービスが要求に応答しなかった。 • 5（CUSTOM SIGNATURE）：ファイルがユーザー定義のハッシュと一致するため、ユーザー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-19　マルウェア イベント データ ブロック 6.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:マルウェア許可リスト • 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	ユーザーが指定した 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 サーバー証明書の SHA1 ハッシュ。

表 B-19　マルウェア イベント データ ブロック 6.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-19　マルウェア イベント データ ブロック 6.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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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-19　マルウェア イベント データ ブロック 6.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。
HTTP レスポンス	uint32	HTTP 要求の応答コード。

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、ユーザー、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(4-46 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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	Device ID																																
	[IPアドレス(IP Address)]																																
	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(Event Type)																							
	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-20　　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
Device 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Device 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(IP Address)]	uint32	イベントに関連するホストの IP アドレス。
MAC アドレス	uint8[6]	イベントに関連するホストの MAC アドレス。

表 B-20　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
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（Event Type）	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、ユーザー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（4-46 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（4-46 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 サーバー データ ブロック

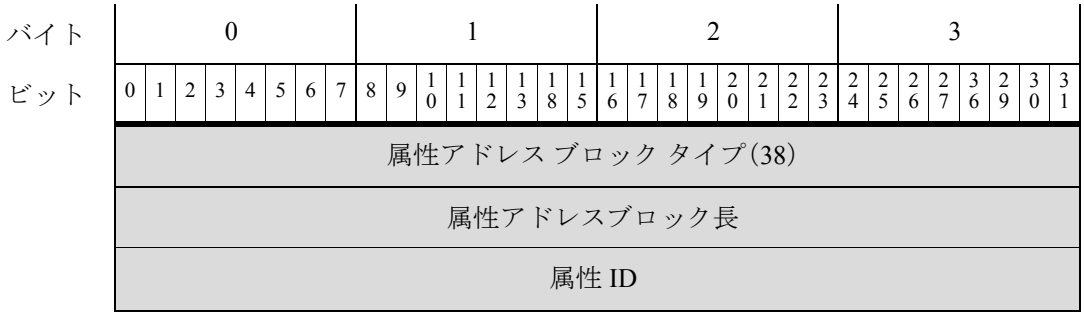
詳細については、次の項を参照してください。

- 属性アドレス データ ブロック 5.0 ～ 5.1.1.x（B-129 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。



[IPアドレス(IP Address)]
ビット

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-21　　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(IP Address)]	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。

- ユーザー 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-130 ページ)

ユーザー 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

ユーザー 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ーの 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。ユーザー 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、ユーザー 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
	ユーザー クライアント アプリケーション ブロック タイプ(59)																																
	ユーザー クライアント アプリケーション ブロック長																																
[IPアドレス(IP Address)] 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、ユーザー 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-22　ユーザー 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
ユーザー クライアント アプリケーション ブロック タイプ	uint32	ユーザー 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。
ユーザー クライアント アプリケーション ブロック長	uint32	ユーザー 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(ユーザー 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ー 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(variable)	ユーザー入力の 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 4-59 ユーザー サーバー データ ブロックのフィールド(4-109 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。

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-132 ページ）
- ユーザー製品データ ブロック 5.0.x（B-134 ページ）
- ユーザー情報データ ブロック 5.x（B-156 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。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	スキャン結果ブロック タイプ（102）																																
	スキャン結果ブロック長																																
	ユーザー ID（User ID）																																
	スキャン タイプ																																
	[IP アドレス（IP Address）]																																
	ポート																	プロトコル															
脆弱性スキャン リスト	フラグ（Flag）																	リスト ブロック タイプ（11）															
	リスト ブロック タイプ（11）																	リスト ブロック長															
脆弱性リスト	リスト ブロック長																	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 タイプ（109）																	スキャン脆弱性ブロック長															
	スキャン脆弱性ブロック長																	脆弱性データ...															
汎用スキャン結果リスト	リスト ブロック タイプ（11）																																
	リスト ブロック長																																
スキャン結果リスト	汎用スキャン結果ブロック タイプ（108）																																
	汎用スキャン結果ブロック長																																
	汎用スキャン結果...																																

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-23　　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)。
ユーザー ID (User ID)	uint32	スキャン結果をインポートしたユーザー、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ーのユーザー 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(IP Address)]	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(Port)]	uint16	結果の脆弱性の影響を受ける、サブサーバーで使用されるポート。
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(Flag)	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。

表 B-23　スキャン結果データ ブロックのフィールド（続き）

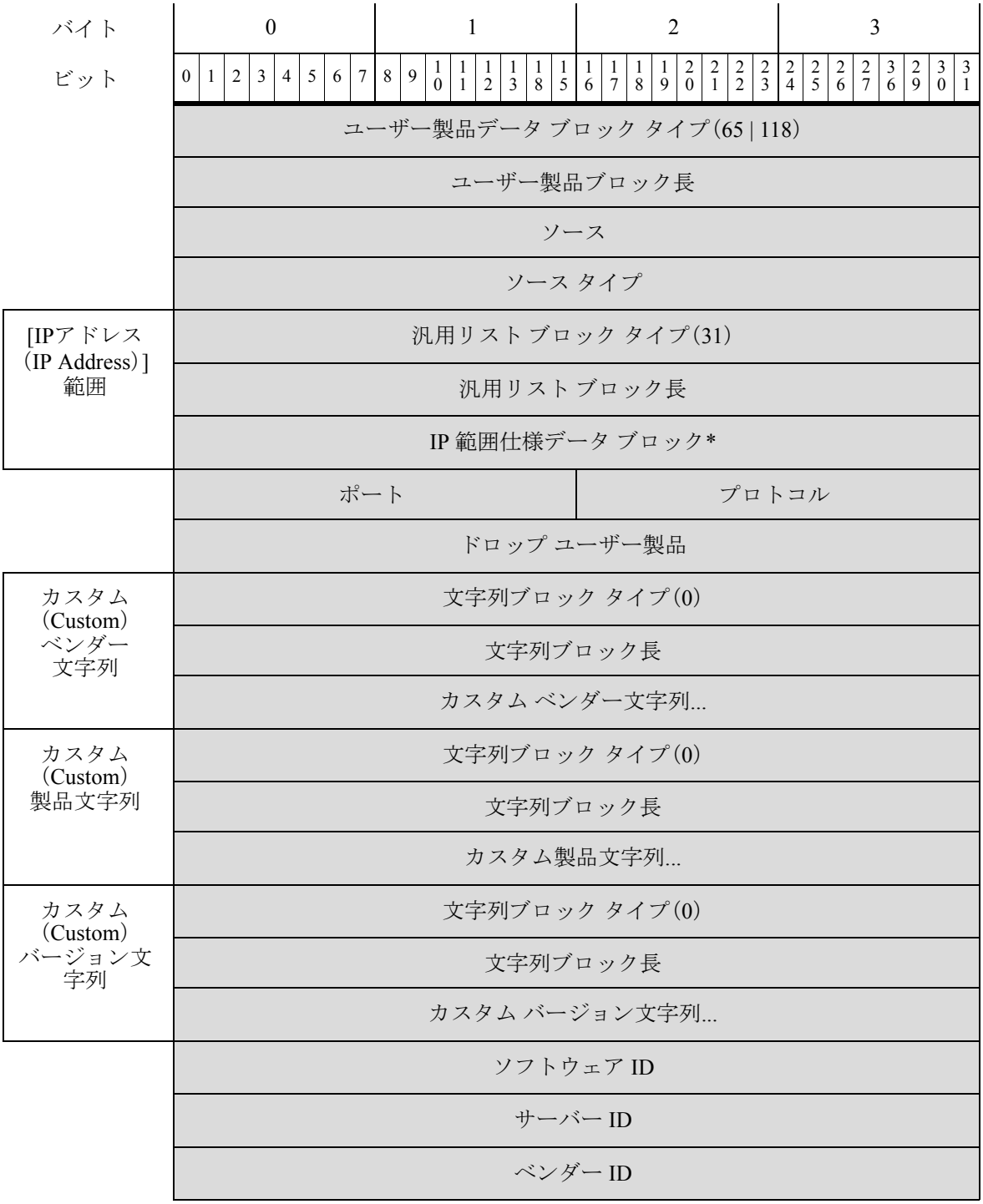
フィールド	データタイプ	説明
スキャン脆弱性ブロック タイプ	uint32	スキャン中に検出された脆弱性を記述するスキャン脆弱性データ ブロックを開始します。この値は常に 109 です。
スキャン脆弱性ブロック長	uint32	スキャン脆弱性データ ブロックのバイト数（接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン脆弱性データのバイト数を含む）。
脆弱性データ	string	各脆弱性に関する情報。
リスト ブロック タイプ	uint32	トランスポート スキャン脆弱性データを伝えるスキャン脆弱性データ ブロックで構成されるリスト データ ブロックを開始します。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ー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ー製品データ 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。
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ー製品データ ブロックを含む）。
ユーザー製品データ ブロック*	変数（variable）	ホスト入力データを含むユーザー製品データ ブロック。このデータ ブロックの説明の詳細については、ユーザー製品データ ブロック 5.1+（4-183 ページ）を参照してください。

ユーザー製品データ ブロック 5.0.x

ユーザー製品データ 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 接続統計データ ブロック 6.0.x（B-239 ページ）と ユーザー サーバー メッセージとオペレーティング システム メッセージ（4-60 ページ）で使用します。ユーザー製品データ 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、ユーザー製品データ 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
		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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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*																															

次の表では、ユーザー製品データ ブロックのコンポーネントについて説明します。

表 B-24　　ユーザー製品データ 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
ユーザー製品データブロック タイプ	uint32	ユーザー製品データ 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。
ユーザー製品ブロック長	uint32	ユーザー製品データ ブロックのバイトの合計数(ユーザー製品ブロック 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ー製品データのバイト数を含む)。
ソース	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(variable)	ユーザー入力の 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(4-101 ページ) を参照してください。
[ポート(Port)]	uint16	ユーザーが指定するポート。

表 B-24　ユーザー製品データ 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
プロトコル	uint16	ユーザーが指定した 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 ユーザー製品	uint32	ユーザー 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	ユーザー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	ユーザー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	ユーザー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。
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	ユーザー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	ユーザー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	ユーザー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	Cisco データベースの特定のリビジョンのサーバーまたはオペレーティング システムの ID。
サーバー ID	uint32	ユーザー入力に指定したホスト サーバーのアプリケーション プロトコルの Cisco 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。

表 B-24　ユーザー製品データ 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 タイプ	uint32	ユーザー入力内のサード 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	ユーザー入力内のサード 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	ユーザー入力内のサード 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。
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	ユーザー入力内のサード 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	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	ユーザー入力内のサード 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。

表 B-24　ユーザー製品データ 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	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	ユーザー入力内のサード 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	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	ユーザー入力内のサード 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)。
ビルド	string	ユーザー入力内のサード 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	ユーザー入力内のサード 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	ユーザー入力内のサード 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。

表 B-24　ユーザー製品データ 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
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ー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（variable）	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（4-108 ページ）を参照してください。

レガシー ユーザー 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。

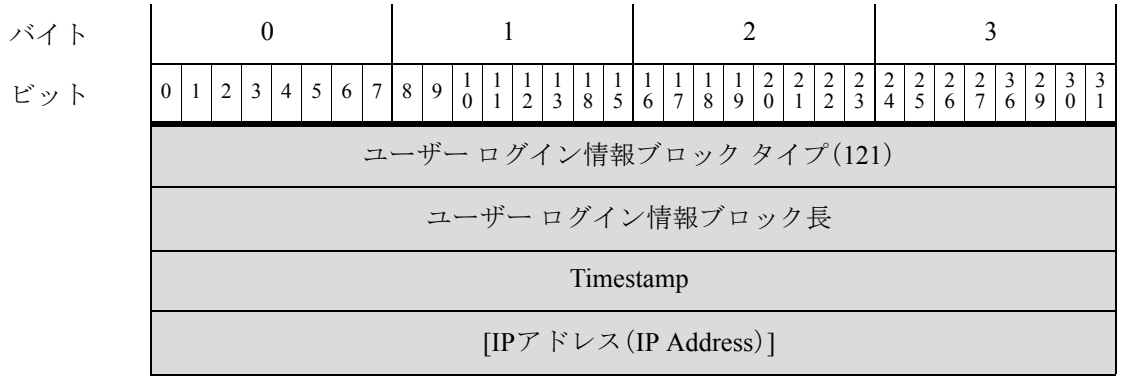
- ユーザー ログイン情報データ ブロック 5.0 ～ 5.0.2（B-141 ページ）
- ユーザー ログイン情報データ ブロック 5.1 ～ 5.4.x（B-143 ページ）
- ユーザー ログイン情報データ ブロック 6.0.x（B-145 ページ）
- ユーザー ログイン情報データ ブロック 6.1.x（B-149 ページ）
- ユーザー情報データ ブロック 5.x（B-156 ページ）

ユーザー ログイン情報データ ブロック 5.0 ～ 5.0.2

ユーザー ログイン情報データ ブロックは、ユーザー情報更新メッセージで使用され、検出されたユーザーのログイン情報の変更を伝えます。詳細については、ユーザー情報更新メッセージ ブロック（4-64 ページ）を参照してください。

ユーザー 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、ユーザー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ユーザー（User）[名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー名...																															
	ユーザー ID（User ID）																															
	アプリケーション ID（Application 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、ユーザー 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-25　　ユーザー 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
ユーザー ログイン情報ブロック タイプ	uint32	ユーザー 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。
ユーザー ログイン情報ブロック長	uint32	ユーザー ログイン情報データ ブロックのバイトの合計数（ユーザー 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ー ログイン情報データのバイト数を含む）。
Timestamp	uint32	イベントのタイムスタンプ。
[IPアドレス（IP Address）]	uint8[4]	IP アドレス オクテットの、ユーザー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	ユーザーのユーザ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	ユーザー名文字列データ 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、およびユーザー名のバイト数を含む）。
[ユーザー名（Username）]	string	ユーザーのユーザー名。
ユーザー ID（User ID）	uint32	ユーザーの ID 番号。
アプリケーション ID（Application 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。

表 B-25　ユーザー 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
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの電子メール アドレス。

ユーザー ログイン情報データ ブロック 5.1 ～ 5.4.x

ユーザー ログイン情報データ ブロックは、ユーザー情報更新メッセージで使用され、検出されたユーザーのログイン情報の変更を伝えます。詳細については、ユーザー アカウント更新メッセージ データ ブロック (4-192 ページ) を参照してください。

ユーザー 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ブロック タイプ 127 です。

次の図は、ユーザー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ユーザー ログイン情報ブロック タイプ（127）																															
	ユーザー ログイン情報ブロック長																															
	Timestamp																															
	IPv4 アドレス（IPv4 Address）																															
ユーザー（User）[名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー名...																															
	ユーザー ID（User ID）																															
	アプリケーション ID（Application 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																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	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、ユーザー 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-26　　ユーザー 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
ユーザー ログイン情報ブロック タイプ	uint32	ユーザー 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。
ユーザー ログイン情報ブロック長	uint32	ユーザー ログイン情報データ ブロックのバイトの合計数（ユーザー 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ー ログイン情報データのバイト数を含む）。
Timestamp	uint32	イベントのタイムスタンプ。
IPv4 アドレス（IPv4 Address）	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（1-4 ページ）を参照してください。
文字列ブロック タイプ	uint32	ユーザーのユーザ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	ユーザー名文字列データ 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、およびユーザー名のバイト数を含む）。
[ユーザー名（Username）]	string	ユーザーのユーザー名。
ユーザー ID（User ID）	uint32	ユーザーの ID 番号。
アプリケーション ID（Application 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	ユーザー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。

表 B-26　ユーザー 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	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	ユーザーの電子メール アドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザー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	検出されたユーザー 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 サーバーの名前。

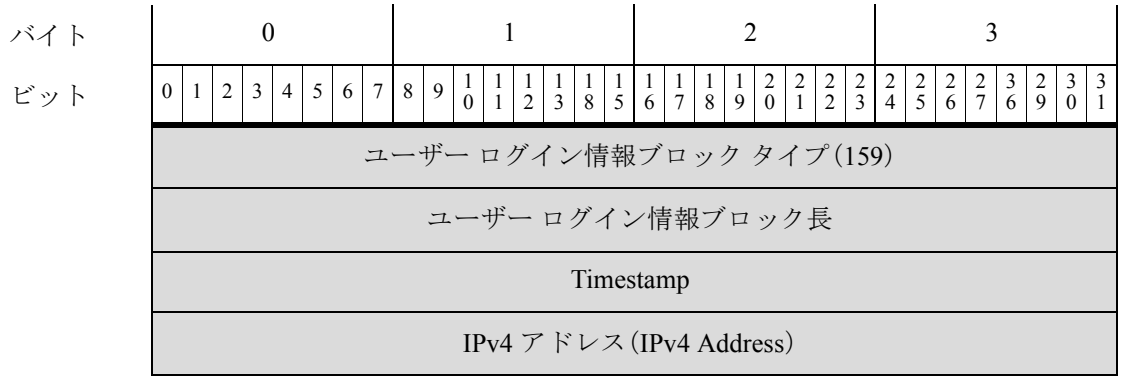
ユーザー ログイン情報データ ブロック 6.0.x

ユーザー ログイン情報データ ブロックは、ユーザー情報更新メッセージで使用され、検出されたユーザーのログイン情報の変更を伝えます。詳細については、ユーザー アカウント更新メッセージ データ ブロック（4-192 ページ）を参照してください。

ユーザー 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。

ユーザー 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、ユーザー ログイン情報データ ブロック 5.1 ～ 5.4.x（B-143 ページ）を参照してください。

次の図は、ユーザー 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
ユーザー (User) [名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザー名...																															
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...																															
	ユーザー ID(User 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																															
	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)																															
	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)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
レポート基準	ログイン タイプ								承認タイプタイプ(Type)								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、ユーザー 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-27　　ユーザー 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
ユーザー ログイン情報ブロック タイプ	uint32	ユーザー 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。
ユーザー ログイン情報ブロック長	uint32	ユーザー ログイン情報データ ブロックのバイトの合計数(ユーザー 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ー ログイン情報データのバイト数を含む)。
Timestamp	uint32	イベントのタイムスタンプ。
IPv4 アドレス(IPv4 Address)	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(1-4 ページ)を参照してください。
文字列ブロック タイプ	uint32	ユーザーのユーザ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	ユーザー名文字列データ 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、およびユーザー名のバイト数を含む)。
[ユーザー名(Username)]	string	ユーザーのユーザー名。
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ー名文字列データ ブロックのバイト数。
ドメイン	string	ユーザーがログインしているドメイン。
ユーザー ID(User ID)	uint32	ユーザーの 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 B-27　ユーザー 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。
プロトコル	uint32	ユーザー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	ユーザー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	ユーザーの電子メール アドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザー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]	ユーザー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	検出されたユーザー ログインのタイプ。
認証タイプ（Authentication Type）	uint8	ユーザー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。
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 サーバーの名前。

ユーザー ログイン情報データ ブロック 6.1.x

バージョン 6.1+ では、ユーザー ログイン情報データ ブロックには、シリーズ 1 グループのブロック内にブロック タイプ 165 が含まれています。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、ユーザー ログイン情報データ ブロック 6.0.x（B-145 ページ）を参照してください。これはブロック タイプ 167 に更新しました。

次の図は、ユーザー 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
	ユーザー ログイン情報ブロック タイプ（165）																															
	ユーザー ログイン情報ブロック長																															
	Timestamp																															
	IPv4 アドレス（IPv4 Address）																															
ユーザー（User）[名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー名...																															
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...																															
	ユーザー ID（User 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																															
	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...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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）																															
	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								承認タイプタイプ（Type）								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、ユーザー 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-28　　ユーザー 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
ユーザー ログイン情報ブロック タイプ	uint32	ユーザー 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。
ユーザー ログイン情報ブロック長	uint32	ユーザー ログイン情報データ ブロックのバイトの合計数（ユーザー 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ー ログイン情報データのバイト数を含む）。
Timestamp	uint32	イベントのタイムスタンプ。
IPv4 アドレス（IPv4 Address）	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（1-4 ページ）を参照してください。
文字列ブロック タイプ	uint32	ユーザーのユーザ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	ユーザー名文字列データ 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、およびユーザー名のバイト数を含む）。

表 B-28　ユーザー 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
[ユーザー名（Username）]	string	ユーザーのユーザー名。
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ー名文字列データ ブロックのバイト数。
ドメイン	string	ユーザーがログインしているドメイン。
ユーザー ID（User ID）	uint32	ユーザーの 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。
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。
プロトコル	uint32	ユーザー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（Port）]	uint16	ユーザー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ー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ー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	ユーザー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	ユーザーの電子メール アドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザーのログインが検出されたホストからの IPv6 アドレス。

表 B-28　ユーザー ログイン情報データ ブロックのフィールド（続き）

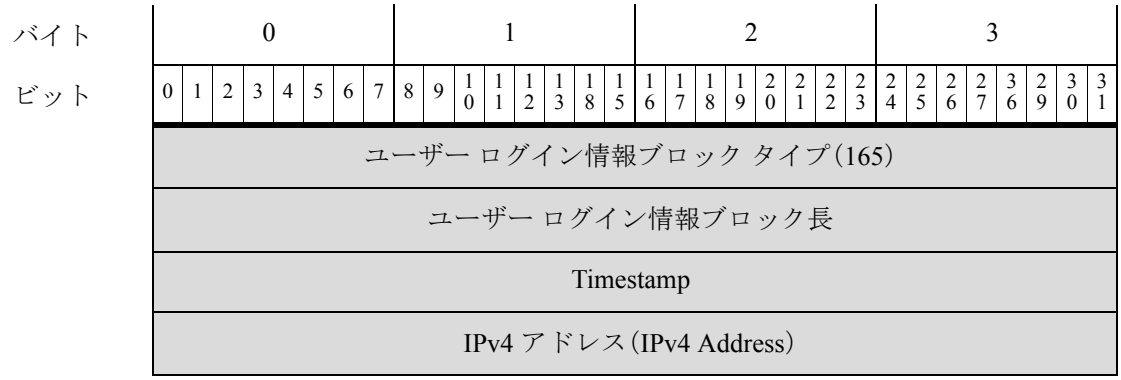
フィールド	データタイプ	説明
ロケーション IPv6 アドレス	uint8[16]	ユーザーがログインした最新の IP アドレス。IPv4 または IPv6 のどちらかのアドレスになります。
ログイン タイプ	uint8	検出されたユーザー ログインのタイプ。
認証タイプ（Authentication Type）	uint8	ユーザーが使用する認証のタイプ。値は次のとおりです。 • 0:認証は不要 • 1:パッシブ認証、AD エージェント、または ISE セッション • 2:キャプティブ ポータルの正常な認証 • 3:キャプティブ ポータルのゲスト認証 • 4:キャプティブ ポータルの失敗認証
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。
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 サーバーの名前。

ユーザー ログイン情報データ ブロック 6.1.x

ユーザー ログイン情報データ ブロックは、ユーザー情報更新メッセージで使用され、検出されたユーザーのログイン情報の変更を伝えます。詳細については、ユーザー情報更新メッセージ ブロック (4-64 ページ)を参照してください。

バージョン 6.1x では、ユーザー ログイン情報データ ブロックには、シリーズ 1 グループのブロック内にブロック タイプ 165 が含まれています。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。これはブロック タイプ 167 に更新しました。詳細については、ユーザー ログイン情報データ ブロック 6.0.x (B-145 ページ)を参照してください。

次の図は、ユーザー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ユーザー（User）[名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー名...																															
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...																															
	ユーザー ID（User 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																															
	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） 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
レポート基準	ログイン タイプ								承認タイプタイプ(Type)								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...															
ドメイン	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、ユーザー 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-29　　ユーザー 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
ユーザー ログイン情報ブロック タイプ	uint32	ユーザー ログイン情報データ ブロックを開始します。バージョン 6.2+ の場合、この値は 165 です。
ユーザー ログイン情報ブロック長	uint32	ユーザー ログイン情報データ ブロックのバイトの合計数(ユーザー 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ー ログイン情報データのバイト数を含む)。
Timestamp	uint32	イベントのタイムスタンプ。
IPv4 アドレス(IPv4 Address)	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(1-4 ページ)を参照してください。
文字列ブロック タイプ	uint32	ユーザーのユーザ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	ユーザー名文字列データ 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、およびユーザー名のバイト数を含む)。
[ユーザー名(Username)]	string	ユーザーのユーザー名。
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ー名文字列データ ブロックのバイト数。
ドメイン	string	ユーザーがログインしているドメイン。
ユーザー ID(User ID)	uint32	ユーザーの ID 番号。

表 B-29　ユーザー 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。
プロトコル	uint32	ユーザー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(Port)]	uint16	ユーザー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ー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ー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	ユーザー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	ユーザーの電子メール アドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザー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]	ユーザー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	検出されたユーザー ログインのタイプ。

表 B-29　ユーザー ログイン情報データ ブロックのフィールド（続き）

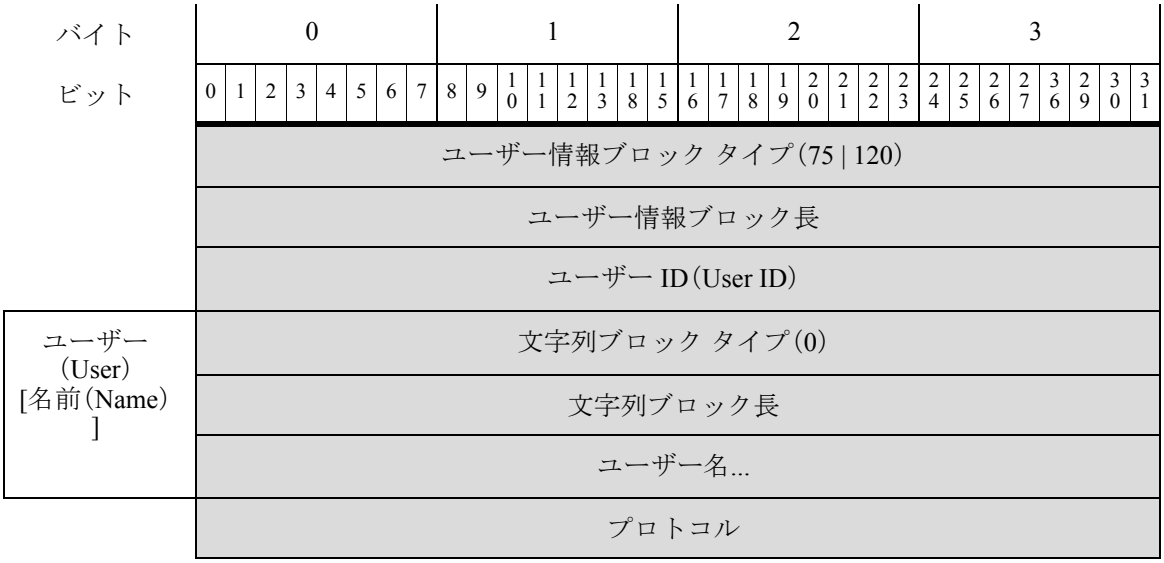
フィールド	データタイプ	説明
認証タイプ（Authentication Type）	uint8	ユーザーが使用する認証のタイプ。値は次のとおりです。 • 0：認証は不要 • 1：パッシブ認証、AD エージェント、または ISE セッション • 2：キャプティブ ポータルの正常な認証 • 3：キャプティブ ポータルのゲスト認証 • 4：キャプティブ ポータルの失敗認証
文字列ブロック タイプ	uint32	レポート基準値を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	レポート基準文字列データブロックのバイト数（ブロック タイプと長さのフィールド用の 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 サーバーの名前。

ユーザー情報データ ブロック 5.x

ユーザー情報データ ブロックはユーザー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ーの情報を伝えます。詳細については、ユーザー変更メッセージ（4-64 ページ）を参照してください。

ユーザー情報データ 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、ユーザー情報データ 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ファースト [名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	名...																															
姓 [名前(Name)]	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...																															

次の表は、ユーザー情報データ ブロックのコンポーネントについての説明です。

表 B-30　　ユーザー情報データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザー情報ブロック タイプ	uint32	ユーザー情報データ 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 以降の場合は 120 です。
ユーザー情報ブロック長	uint32	ユーザー情報データブロックのバイトの合計数(ユーザー 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ー情報データのバイト数を含む)。
ユーザー ID(User ID)	uint32	ユーザーの ID 番号。
文字列ブロック タイプ	uint32	ユーザーのユーザ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。

表 B-30　ユーザー情報データ 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	ユーザー名文字列データ 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、およびユーザー名のバイト数を含む)。
[ユーザー名（Username）]	string	ユーザーのユーザー名。
プロトコル	uint32	ユーザー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	ユーザー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	ユーザーの名前。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの姓。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの電子メール アドレス。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの部署名。
文字列ブロック タイプ	uint32	ユーザー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	ユーザーの電話番号。

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-159 ページ）

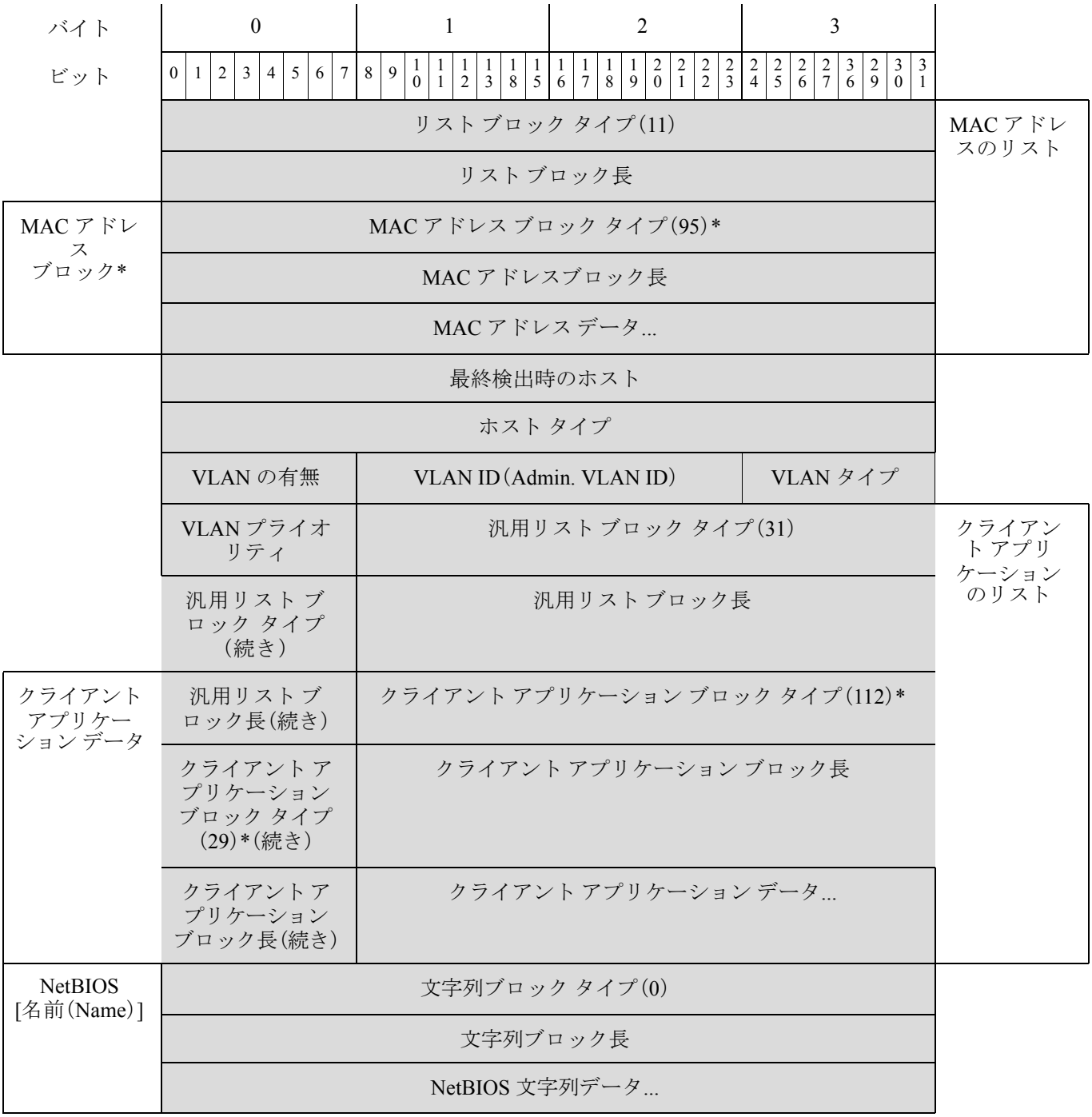
ホスト プロファイル データ ブロック 5.0 ～ 5.0.2

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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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(IP Address)]																																
サーバー 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)																	サーバー 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*																																

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31	
	リスト ブロック タイプ(11)																																TCP サーバーのリスト
	リスト ブロック長																																
TCP サーバー ブロック*	サーバー ブロック タイプ(36)																																
	サーバー ブロック長																																
	TCP サーバー データ...																																
	リスト ブロック タイプ(11)																																UDP サーバーのリスト
	リスト ブロック長																																
UDP サーバー ブロック*	サーバー ブロック タイプ(36)*																																
	サーバー ブロック長																																
	UDP サーバー データ...																																
	リスト ブロック タイプ(11)																																ネットワーク プロトコルのリスト
	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...																																
	リスト ブロック タイプ(11)																																トランスポート プロトコルのリスト
	リスト ブロック長																																
トランスポート(Transport) 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...																																



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-31　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(IP Address)]	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	サーバー 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	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(サーバー フィンガープリント)データ ブロック*	変数(variable)	サーバー 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-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	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(variable)	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-166 ページ) を参照してください。

表 B-31　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	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（variable）	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-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（variable）	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-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 サーバー データを伝えるサーバー 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ー データ ブロックを加えた値です。 このフィールドには、ゼロ以上のサーバー データ ブロックが続きます。
サーバー ブロック タイプ	uint32	サーバー データ ブロックを開始します。この値は常に 89 です。
サーバー ブロック長	uint32	サーバー データ ブロックのバイト数（サーバー 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 サーバー データのバイト数を含む）。
TCP サーバー データ	変数（variable）	TCP サーバーを記述するデータ フィールド（旧バージョンの製品で説明）。

表 B-31　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 タイプ	uint32	UDP サーバー データを伝えるサーバー 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ー データ ブロックを加えた値です。 このフィールドには、ゼロ以上のサーバー データ ブロックが続きます。
サーバー ブロック タイプ	uint32	UDP サーバーを記述するサーバー データ ブロックを開始します。この値は常に 89 です。
サーバー ブロック長	uint32	サーバー データ ブロックのバイト数（サーバー 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 サーバー データのバイト数を含む）。
UDP サーバー データ	変数（variable）	UDP サーバーを記述するデータ 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。
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（4-80 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。
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）。

表 B-31　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
トランスポート プロトコル データ	変数（variable）	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 (4-80 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（variable）	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+ (4-122 ページ) で説明）。
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）
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（Admin. 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）。

表 B-31　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
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（variable）	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（4-167 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表す 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。

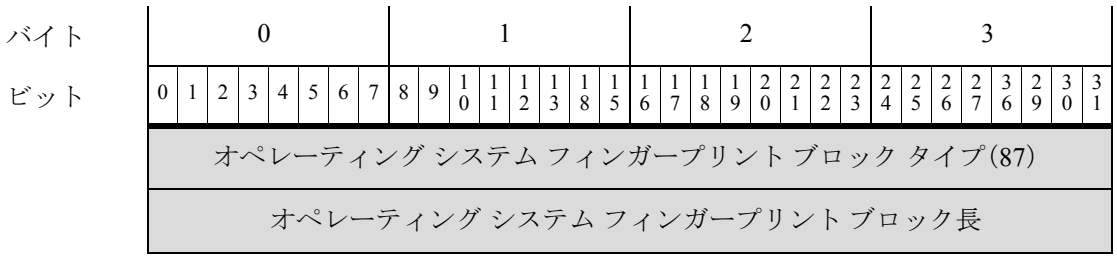
レガシー OS フィンガープリント データ ブロック

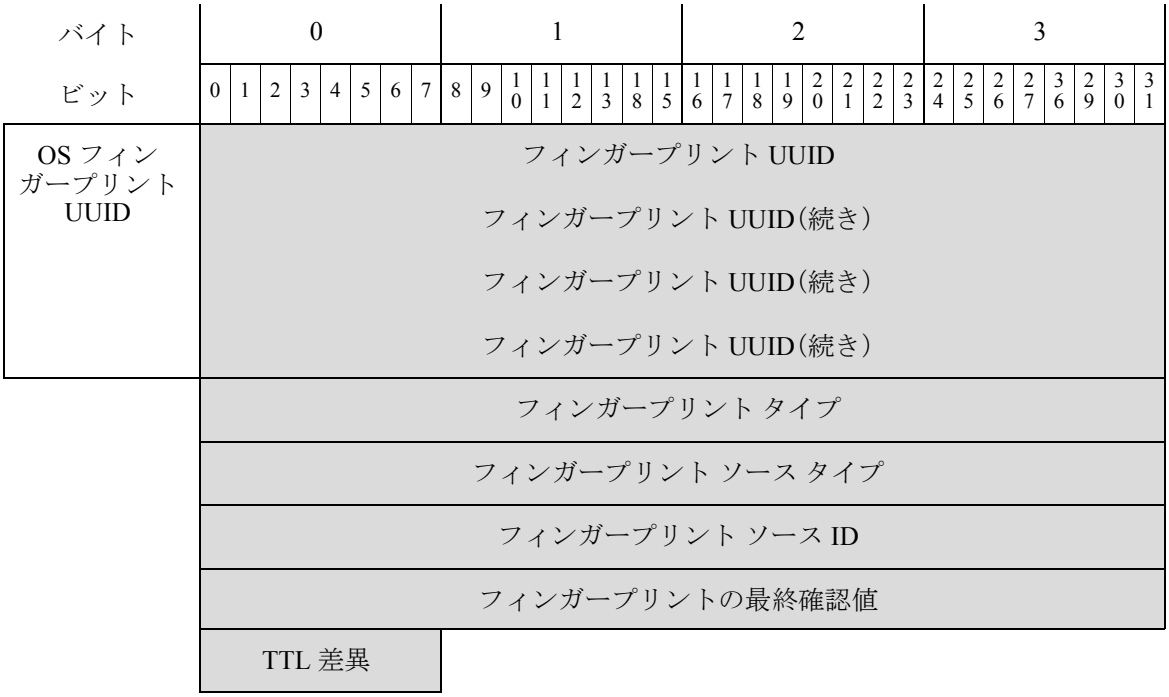
詳細については、次の各項を参照してください。

- 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-166 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 B-32　　オペレーティング 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、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(ユーザーやスキャナ)を示します。

表 B-32　オペレーティング 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（続き）

フィールド	データタイプ	説明
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。

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（B-168 ページ）
- 接続統計データ ブロック 5.1（B-173 ページ）
- 接続統計データ ブロック 5.2.x（B-179 ページ）
- 接続チャンク データ ブロック 5.0 ～ 5.1（B-186 ページ）
- 接続チャンク データ ブロック 5.1.1 ～ 6.0.x（B-187 ページ）
- 接続統計データ ブロック 5.1.1.x（B-189 ページ）
- 接続統計データ ブロック 5.3（B-195 ページ）
- 接続統計データ ブロック 5.3.1（B-202 ページ）
- 接続統計データ ブロック 5.4（B-210 ページ）
- 接続統計データ ブロック 5.4.1（B-224 ページ）
- 接続統計データ ブロック 6.0.x（B-239 ページ）
- 接続統計データ ブロック 6.1.x（B-257 ページ）
- 接続統計データブロック 6.2 ～ 6.7.x（B-275 ページ）
- 接続統計データ ブロック 7.0（B-293 ページ）

接続統計データ ブロック 5.0 ～ 5.0.2

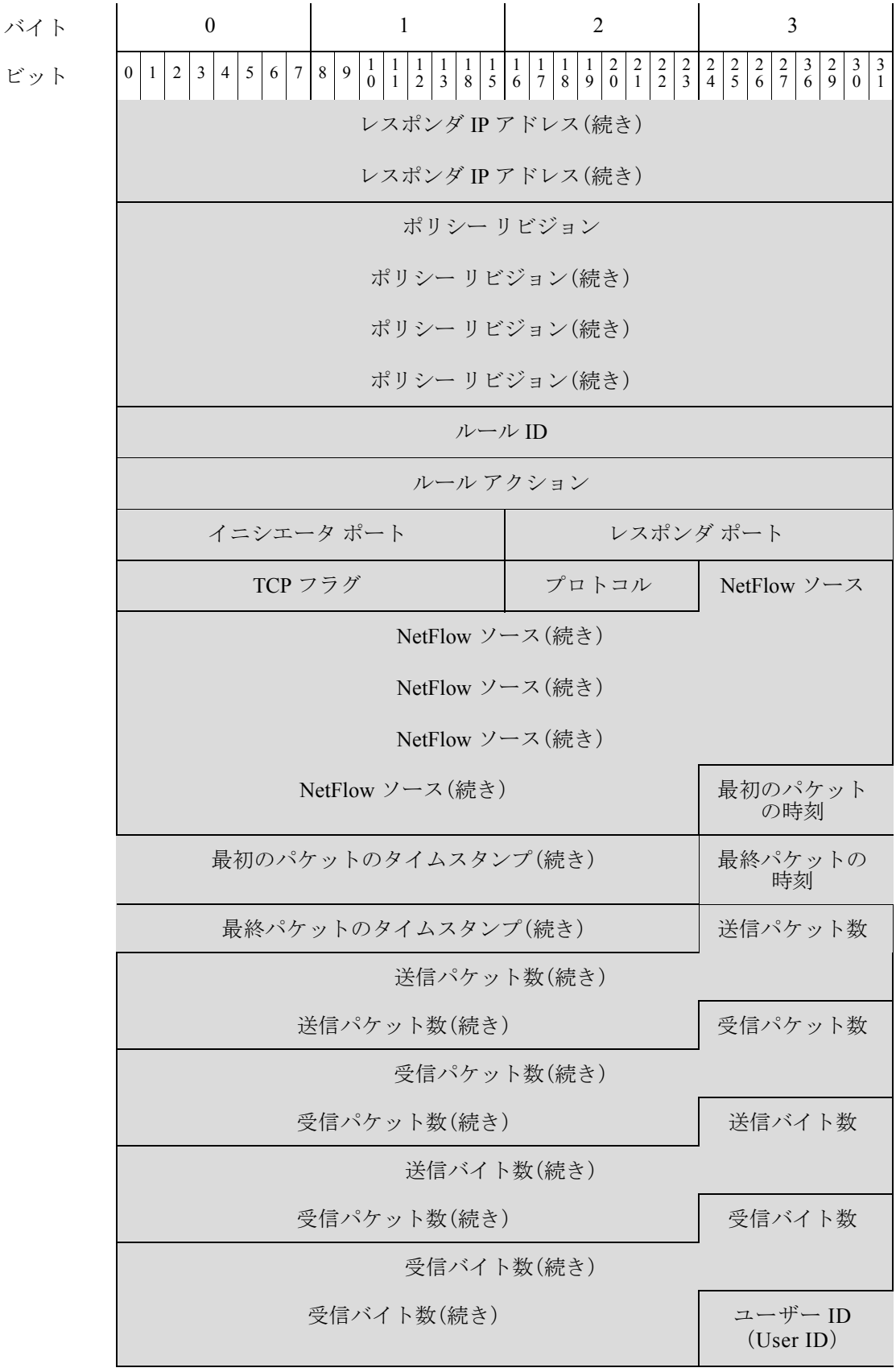
接続統計データ ブロックは、接続データ メッセージで使用されます。接続統計データ ブロック バージョン 5.0 ～ 5.0.2 のブロック タイプは 115 です。

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（4-56 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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																																
Device 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																																
レスポンダ 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(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
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)
ユーザー ID（User 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ユーザー 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)							
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 [名前(Name)]	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-33　　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)。

表 B-33　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
Device 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	uint32	そのルールに対してユーザー 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。
ユーザー ID（User ID）	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 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-33　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
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。
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

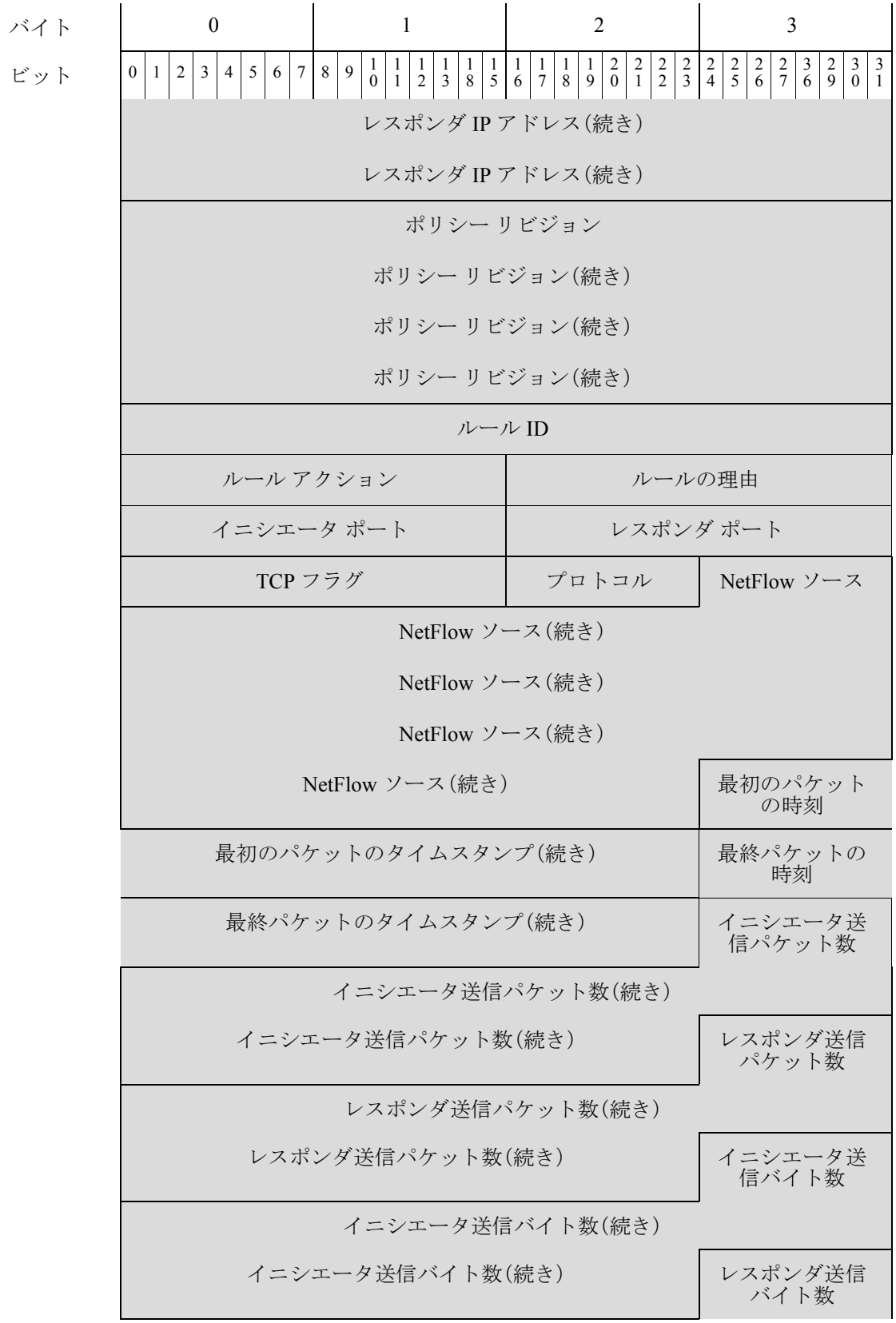
接続統計データ ブロックは、接続データ メッセージで使用されます。バージョン 5.0.2 と 5.1 の間に加えられた接続データ ブロックの変更には、5.1 で導入された設定パラメータ（ルール アクション理由、モニター ルール、セキュリティ インテリジェンス送信元/宛先、セキュリティ インテリジェンス レイヤ）が指定される新規フィールドの追加が含まれます。接続統計データ ブロック バージョン 5.1 のブロック タイプは 126 です。

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（4-56 ページ）を参照してください。

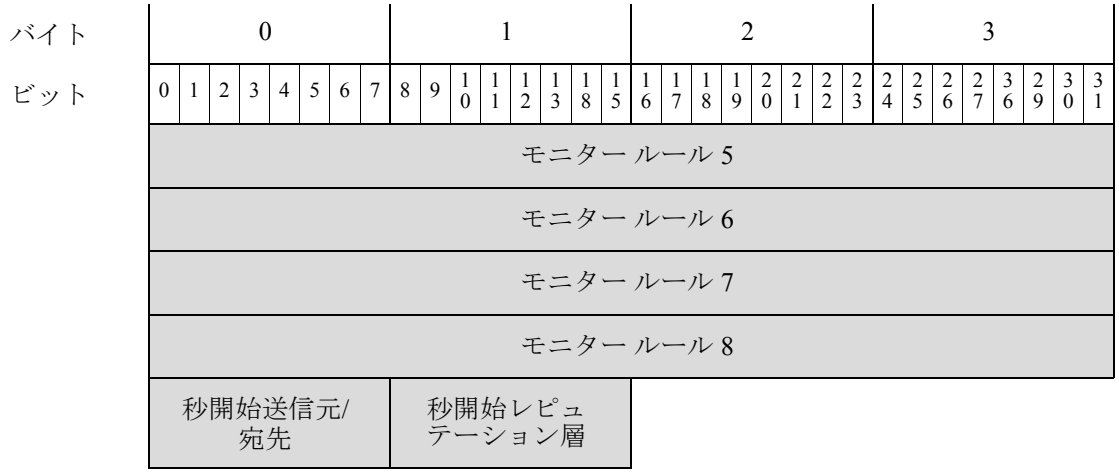
次の図は、接続統計データ ブロック 5.1 の形式を示しています。

::

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
接続データ ブロック タイプ（126）																																
接続データ ブロック長																																
Device 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																																
レスポンダ 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 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)
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)
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

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)																															
	レスポンダ送信バイト数(続き)																								ユーザー ID(User ID)							
	ユーザー 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)							
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 [名前(Name)]	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...																															
	モニター ルール 1																															
	モニター ルール 2																															
	モニター ルール 3																															
	モニター ルール 4																															



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-34　　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)。
Device 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ー 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。

表 B-34　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
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。
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。
ユーザー ID（User ID）	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 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。

表 B-34　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
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。
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。
モニター ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニター ルールの ID。
モニター ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニター ルールの ID。
モニター ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニター ルールの ID。
モニター ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニター ルールの ID。
モニター ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニター ルールの ID。
モニター ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニター ルールの ID。
モニター ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニター ルールの ID。
モニター ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニター 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 アドレスが IP ブロックリストに一致しているかどうか。
セキュリティ インテリジェンス層	uint8	IP ブロ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

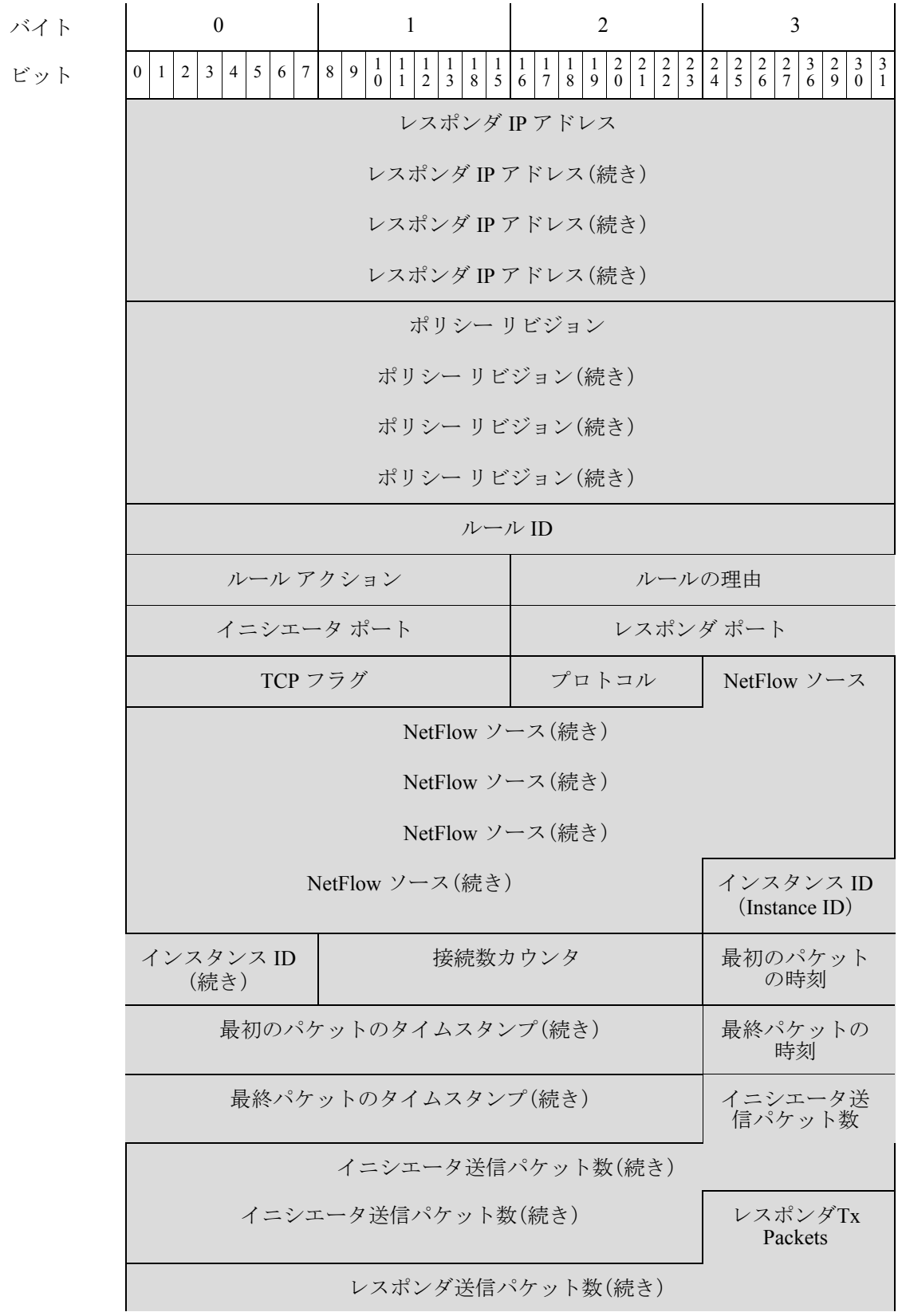
接続統計データ ブロックは、接続データ メッセージで使用されます。バージョン 5.1.1 と 5.2 の間に加えられた接続データ ブロックの変更には、地理位置情報をサポートするための新規フィールドの追加が含まれます。バージョン 5.2.x の接続統計データ ブロックは、シリーズ 1 グループのブロックの、ブロック タイプ 144 です。これにより、ブロック タイプ 137（接続統計データ ブロック 5.1.1.x（B-189 ページ））は廃止されます。

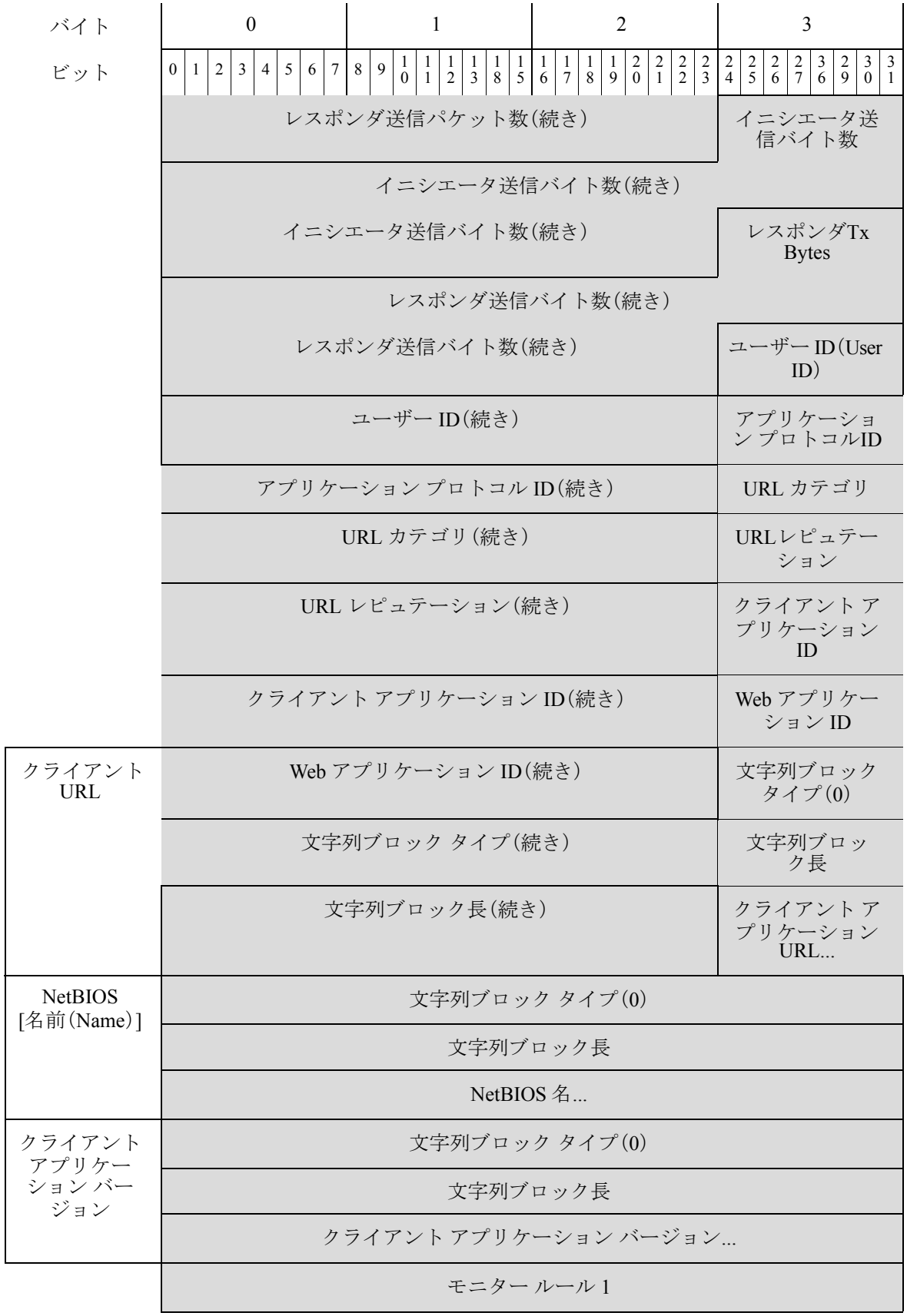
接続統計データ メッセージの詳細については、接続統計データ メッセージ（4-56 ページ）を参照してください。

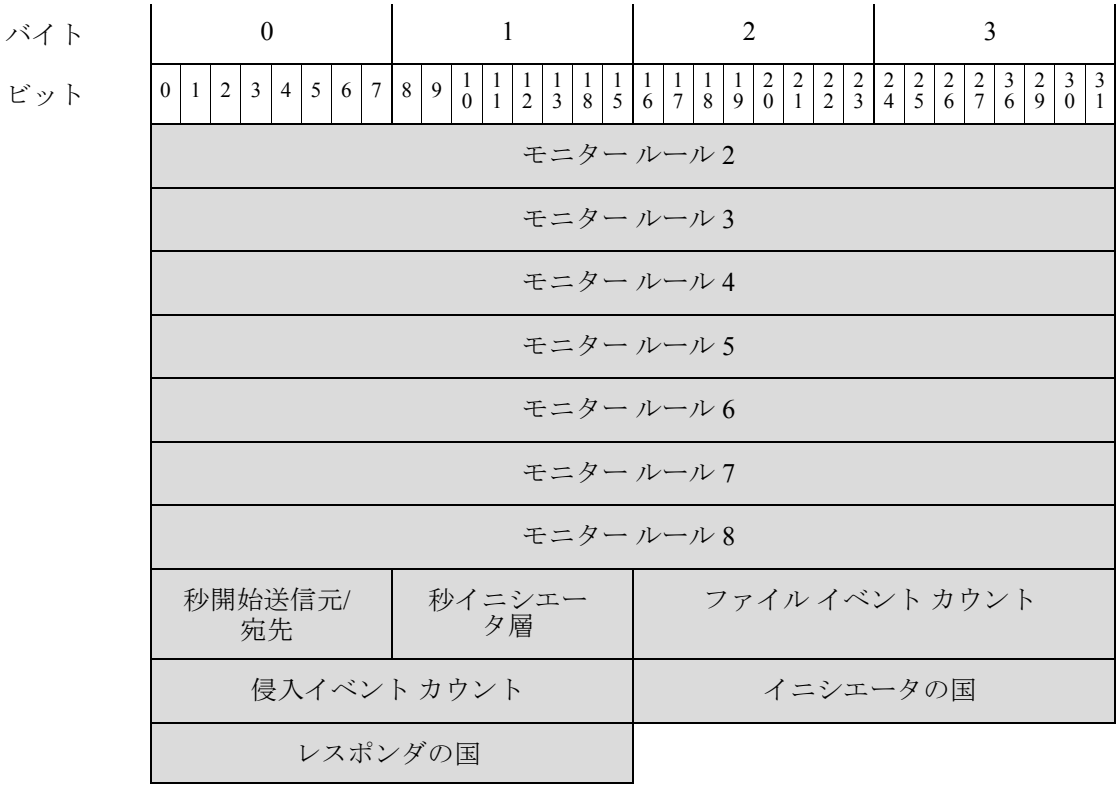
次の図は、接続統計データ ブロック 5.2.x の形式を示しています。

::

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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																																
Device 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 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（Instance 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 Packets
レスポンダ送信パケット数（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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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 Bytes
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)
ユーザー ID(User ID)
ユーザー 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 [名前(Name)]
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...
モニター ルール 1



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-35　　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)。
Device 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。

表 B-35　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
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ー 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（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。
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。
ユーザー ID(User ID)	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 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。

表 B-35　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
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。
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。
モニター ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニター ルールの ID。
モニター ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニター ルールの ID。
モニター ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニター ルールの ID。
モニター ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニター ルールの ID。
モニター ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニター ルールの ID。
モニター ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニター ルールの ID。
モニター ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニター ルールの ID。
モニター ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニター 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 アドレスが IP ブロックリストに一致しているかどうか。
セキュリティ インテリジェンス層	uint8	IP ブロックリストに一致した IP 層。

表 B-35　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
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。

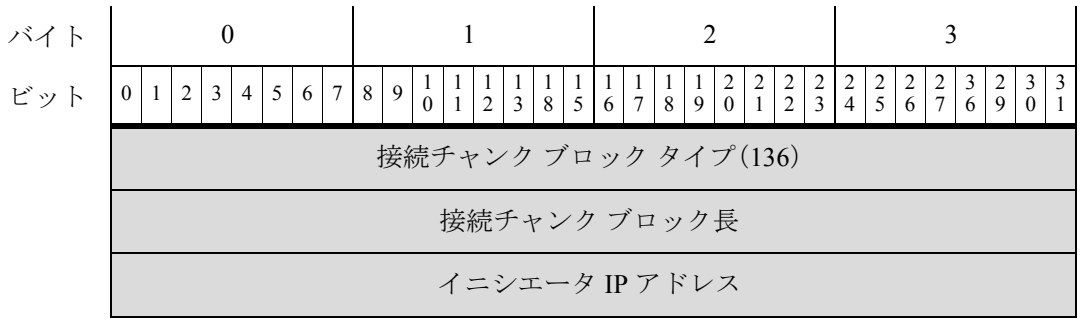
表 B-36　接続チャンク データ ブロックのフィールド

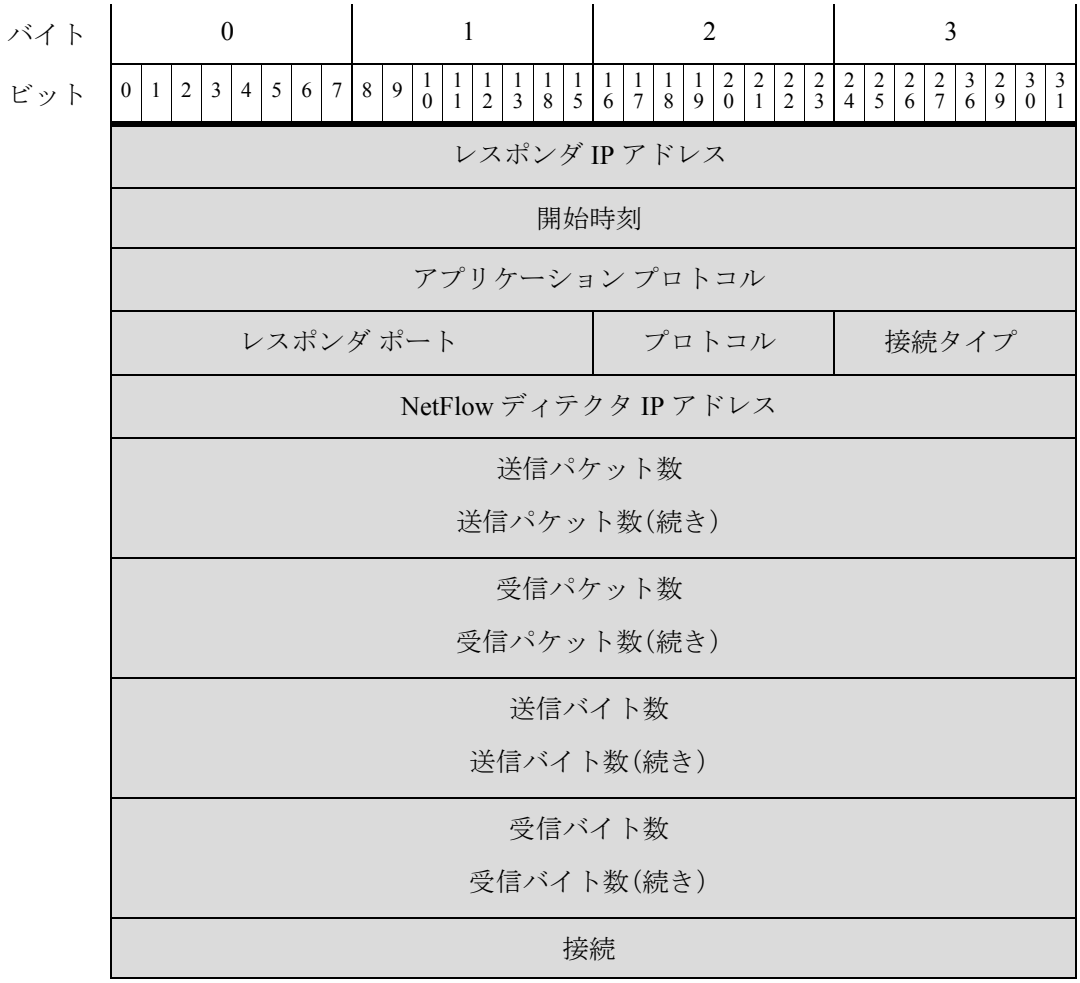
フィールド	データタイプ	説明
接続チャンク ブロック タイプ	uint32	接続チャンク データ ブロックを開始します。この値は、バージョン 4.10.1 以前の場合は 66、バージョン 5.0 の場合は 119 です。
接続チャンク ブロック長	uint32	接続チャンク データ ブロックのバイト数(接続チャンク ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続チャンク データのバイト数を含む)。
イニシエータ IP アドレス	uint8[4]	IP アドレス オクテットの、接続を開始したホストの IP アドレス。
レスポンダ IP アドレス	uint8[4]	IP 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(Application 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	ユーザー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 Device 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-37　　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。

表 B-37　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
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	ユーザー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。
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-173 ページ））は廃止されます。

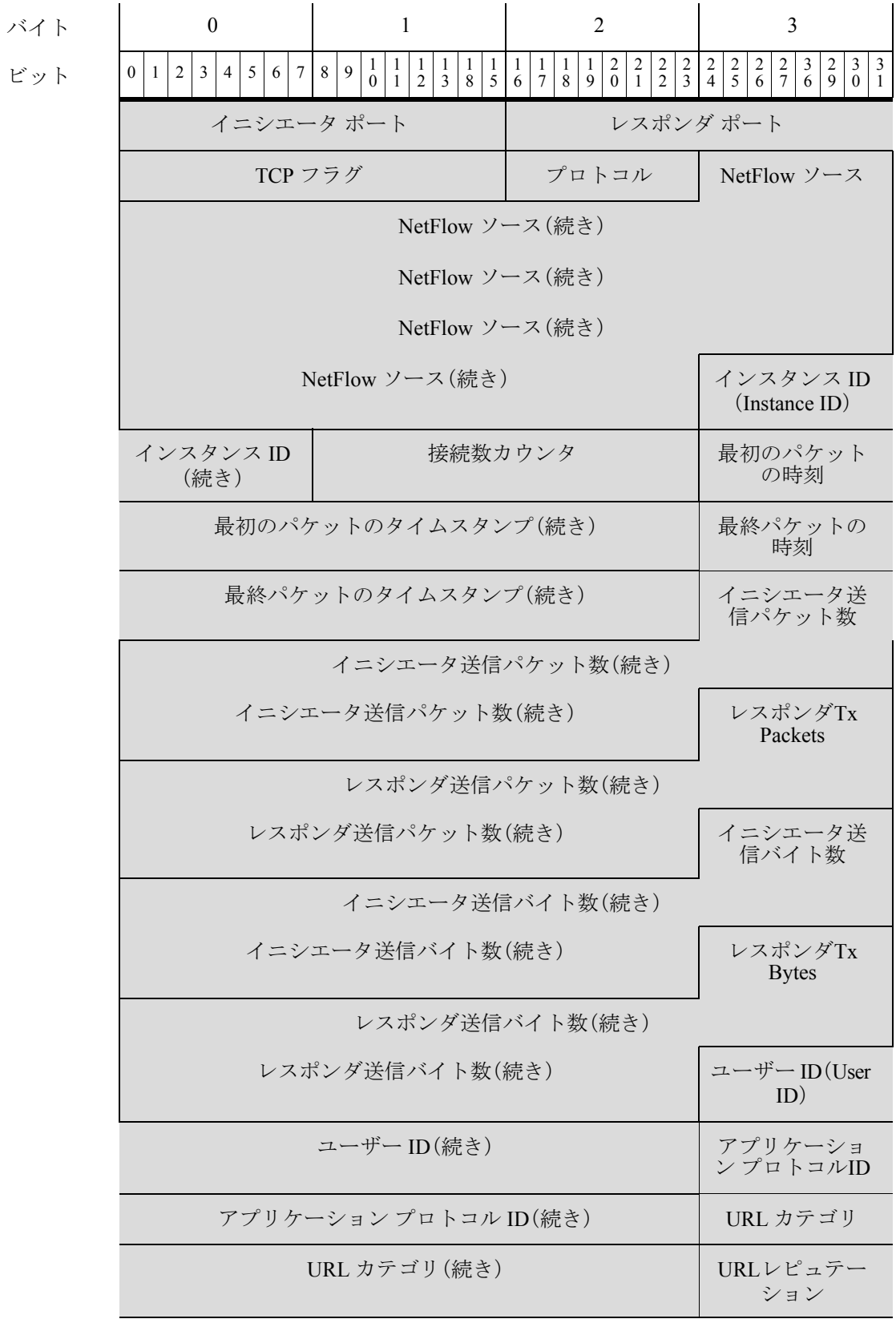
接続統計データ メッセージの詳細については、接続統計データ メッセージ（4-56 ページ）を参照してください。

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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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																																
Device 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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																																
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															


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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（Instance 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 Packets
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 Bytes
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）
ユーザー ID（User ID）
ユーザー 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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	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 [名前(Name)]	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...																															
	モニター ルール 1																															
	モニター ルール 2																															
	モニター ルール 3																															
	モニター ルール 4																															
	モニター ルール 5																															
	モニター ルール 6																															
	モニター ルール 7																															
	モニター 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-38　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）。
Device 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ー 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（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。
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-38　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
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。
ユーザー ID（User ID）	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 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。
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-38　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
モニター ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニター ルールの ID。
モニター ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニター ルールの ID。
モニター ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニター ルールの ID。
モニター ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニター ルールの ID。
モニター ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニター ルールの ID。
モニター ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニター ルールの ID。
モニター ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニター ルールの ID。
モニター ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニター 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 アドレスが IP ブロックリストに一致しているかどうか。
セキュリティ インテリジェンス層	uint8	IP ブロ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-179 ページ））は廃止されます。

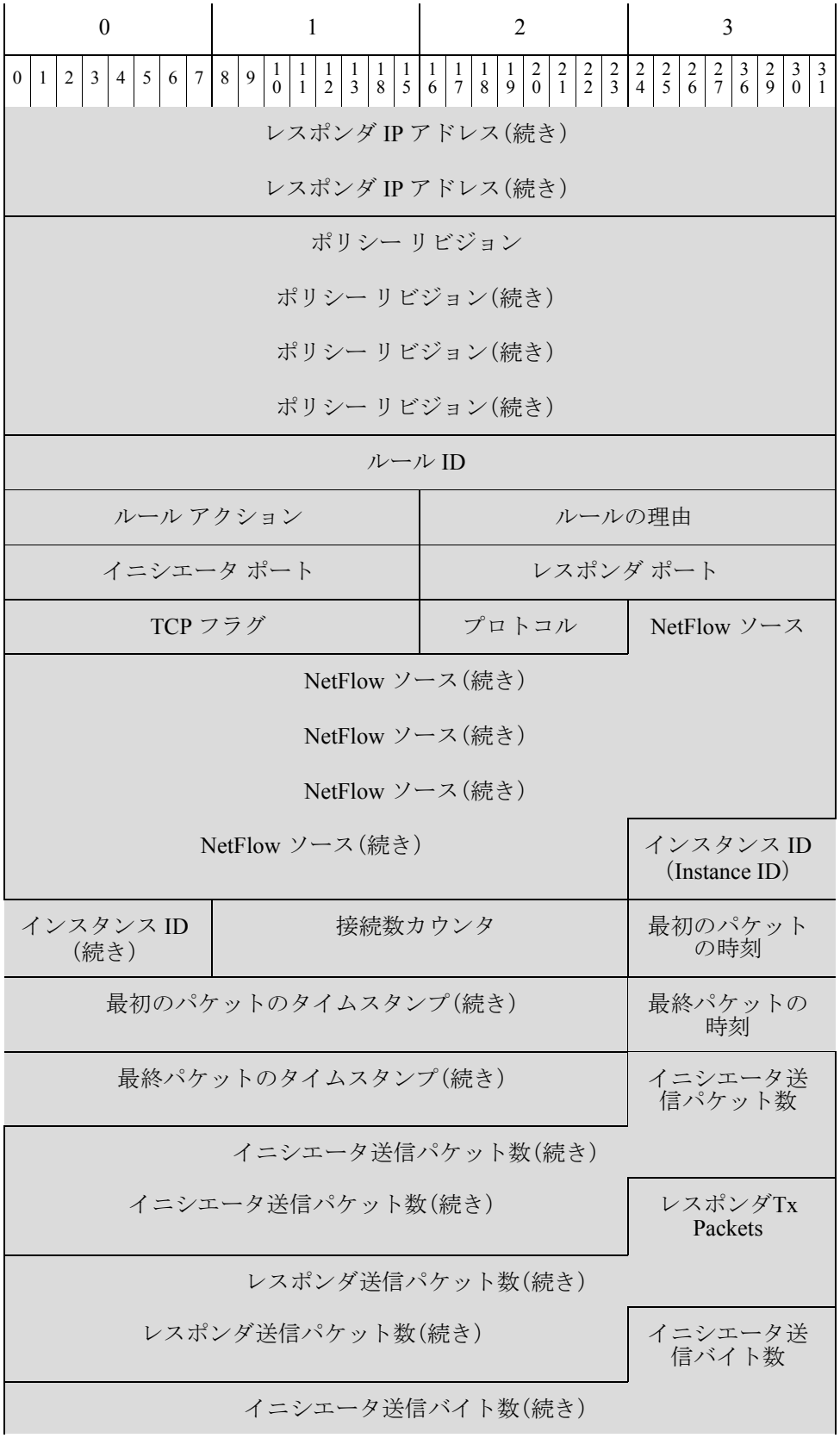
接続イベント レコードを要求するには、イベント バージョン 10 およびイベント コード 71 の要求メッセージ内に、拡張イベント フラグ（要求フラグ フィールドのビット 30）を設定します。要求フラグ（2-15 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

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（4-56 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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																																
Device 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																																
レスポンダ 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(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 (Instance 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 Packets
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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
		イニシエータ送信バイト数(続き)																								レスポンダTx Bytes							
		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)																								ユーザー ID(User ID)							
		ユーザー 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)							
クライアント URL		文字列ブロック タイプ(続き)																								文字列ブロック長							
クライアント URL		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 [名前(Name)]		文字列ブロック タイプ(0)																															
NetBIOS [名前(Name)]		文字列ブロック長																															
NetBIOS [名前(Name)]		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)																															
クライアント アプリケーション バージョン		文字列ブロック長																															
クライアント アプリケーション バージョン		クライアント アプリケーション バージョン...																															
		モニター ルール 1																															
		モニター ルール 2																															
		モニター ルール 3																															

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-39　　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)。
Device 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。

表 B-39　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
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ー 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（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。
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。
ユーザー ID（User ID）	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 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。

表 B-39　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
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。
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。
モニター ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニター ルールの ID。
モニター ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニター ルールの ID。
モニター ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニター ルールの ID。
モニター ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニター ルールの ID。
モニター ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニター ルールの ID。
モニター ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニター ルールの ID。
モニター ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニター ルールの ID。

表 B-39　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
モニター ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニター 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 アドレスが IP ブロックリストに一致しているかどうか。
セキュリティ インテリジェンス層	uint8	IP ブロ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

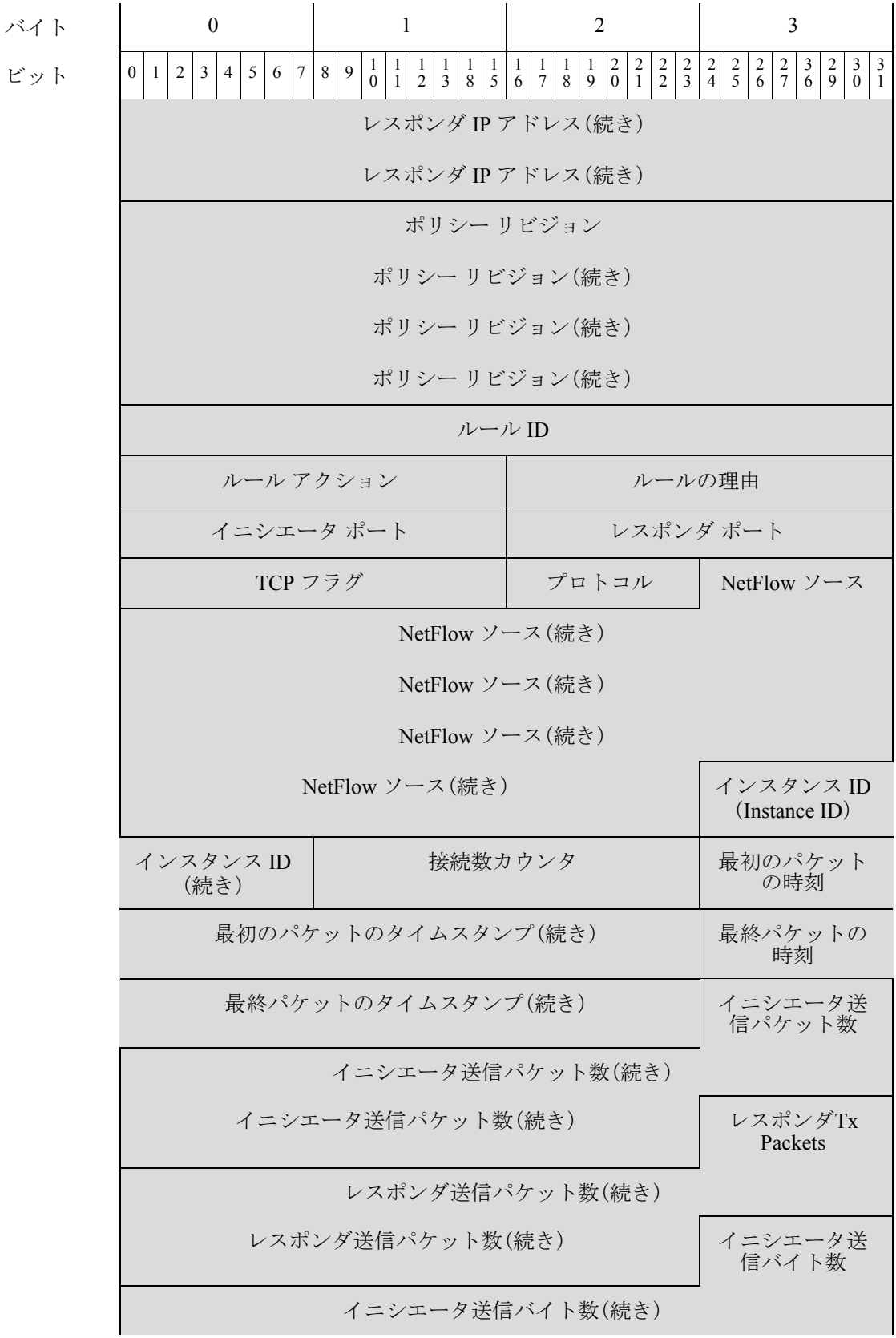
接続統計データ ブロックは、接続データ メッセージで使用されます。バージョン 5.3 と 5.3.1 との間で加えられた接続データ ブロックの唯一の変更は、セキュリティ コンテキスト フィールドの追加です。バージョン 5.3.1 の接続統計データ ブロックは、シリーズ 1 グループのブロックの、ブロック タイプ 154 です。これにより、ブロック タイプ 152（接続統計データ ブロック 5.3 (B-195 ページ)）は廃止されます。

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 (2-15 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 (4-56 ページ)を参照してください。

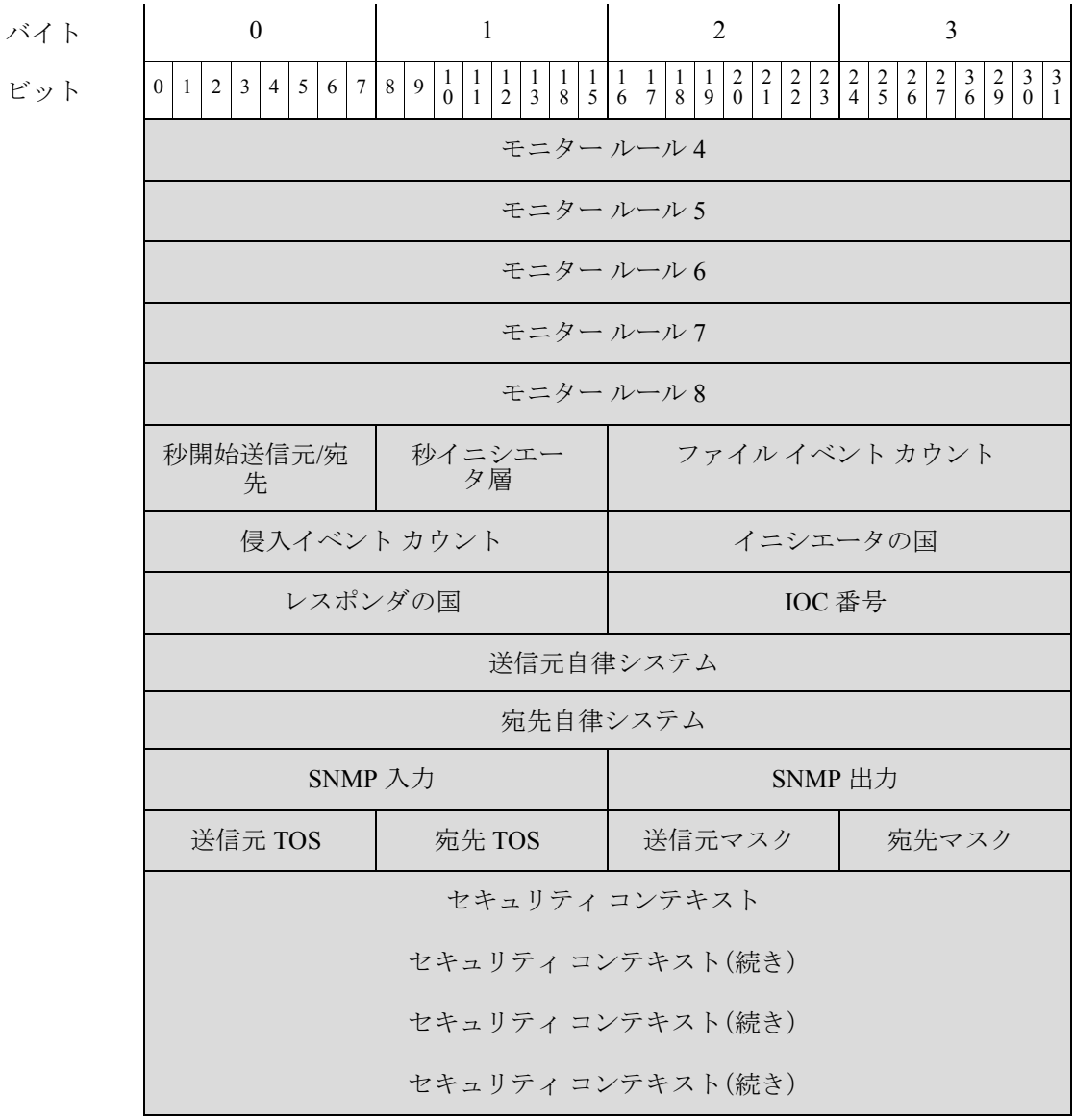
次の図は、接続統計データ ブロック 5.3.1 の形式を示しています。

::

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（Device 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																																
レスポンダ 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(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 (Instance 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 Packets
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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
		イニシエータ送信バイト数（続き）																								レスポンダTx Bytes							
		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）																								ユーザー ID（User ID）							
		ユーザー 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 [名前（Name）]	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...																															
		モニター ルール 1																															
		モニター ルール 2																															
		モニター 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-40　　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（Device 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-40　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ー 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（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。
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。

表 B-40　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
ユーザー ID（User ID）	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 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。
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。
モニター ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニター ルールの ID。
モニター ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニター ルールの ID。
モニター ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニター ルールの ID。
モニター ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニター ルールの ID。

表 B-40　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
モニター ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニター ルールの ID。
モニター ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニター ルールの ID。
モニター ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニター ルールの ID。
モニター ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニター 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 アドレスが IP ブロックリストに一致しているかどうか。
セキュリティ インテリジェンス層	uint8	IP ブロ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

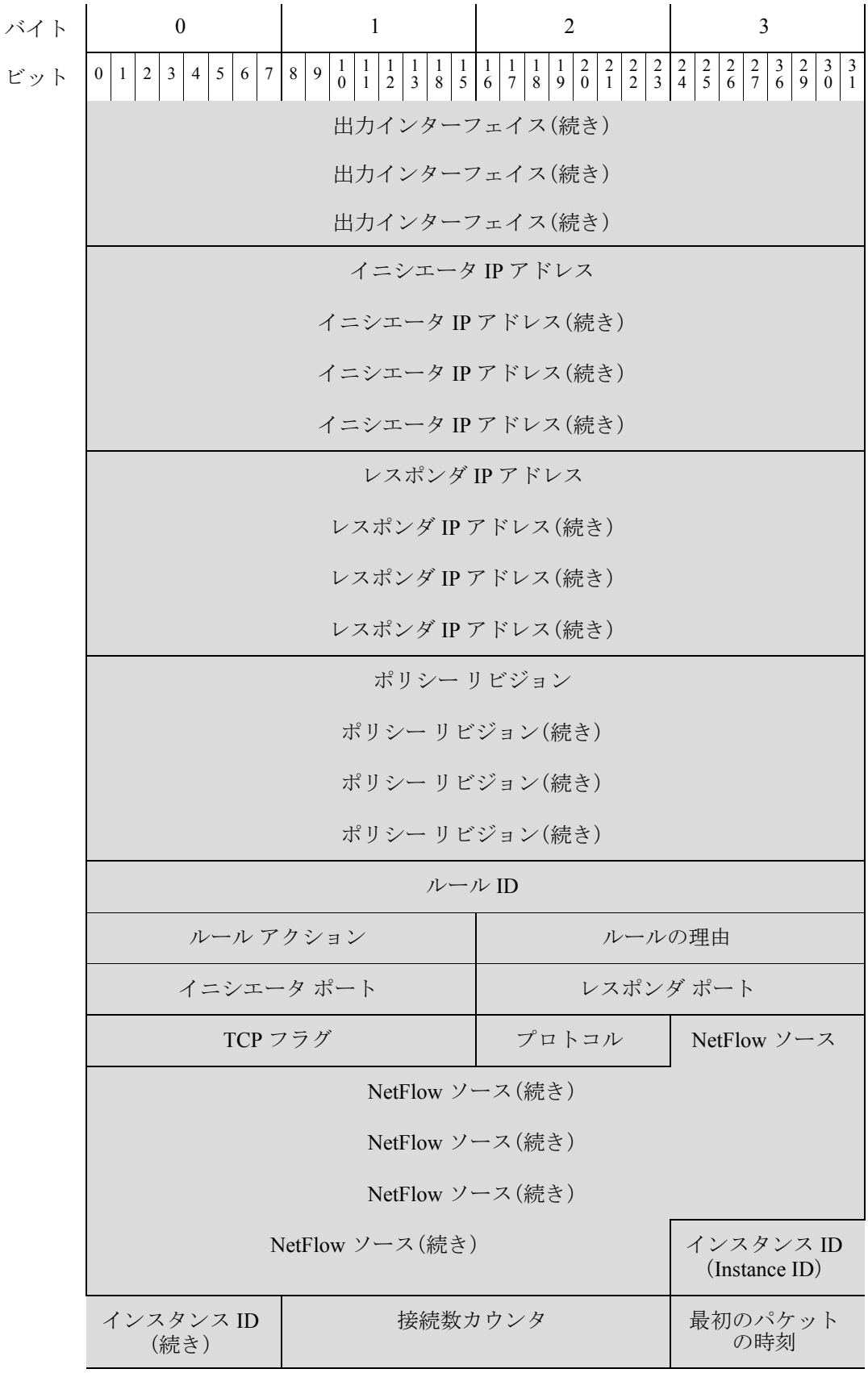
接続統計データ ブロックは、接続データ メッセージで使用されます。接続統計データ ブロック 5.4 には、いくつかの新しいフィールドが追加されました。SSL 接続、HTTP リダイレクション、およびネットワーク分析ポリシーをサポートするためのフィールドが追加されています。バージョン 5.4 の接続統計データ ブロックは、シリーズ 1 グループのブロックの、ブロック タイプ 155 です。これにより、ブロック タイプ 154（接続統計データ ブロック 5.3.1（B-202 ページ））は廃止されます。

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（2-15 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。

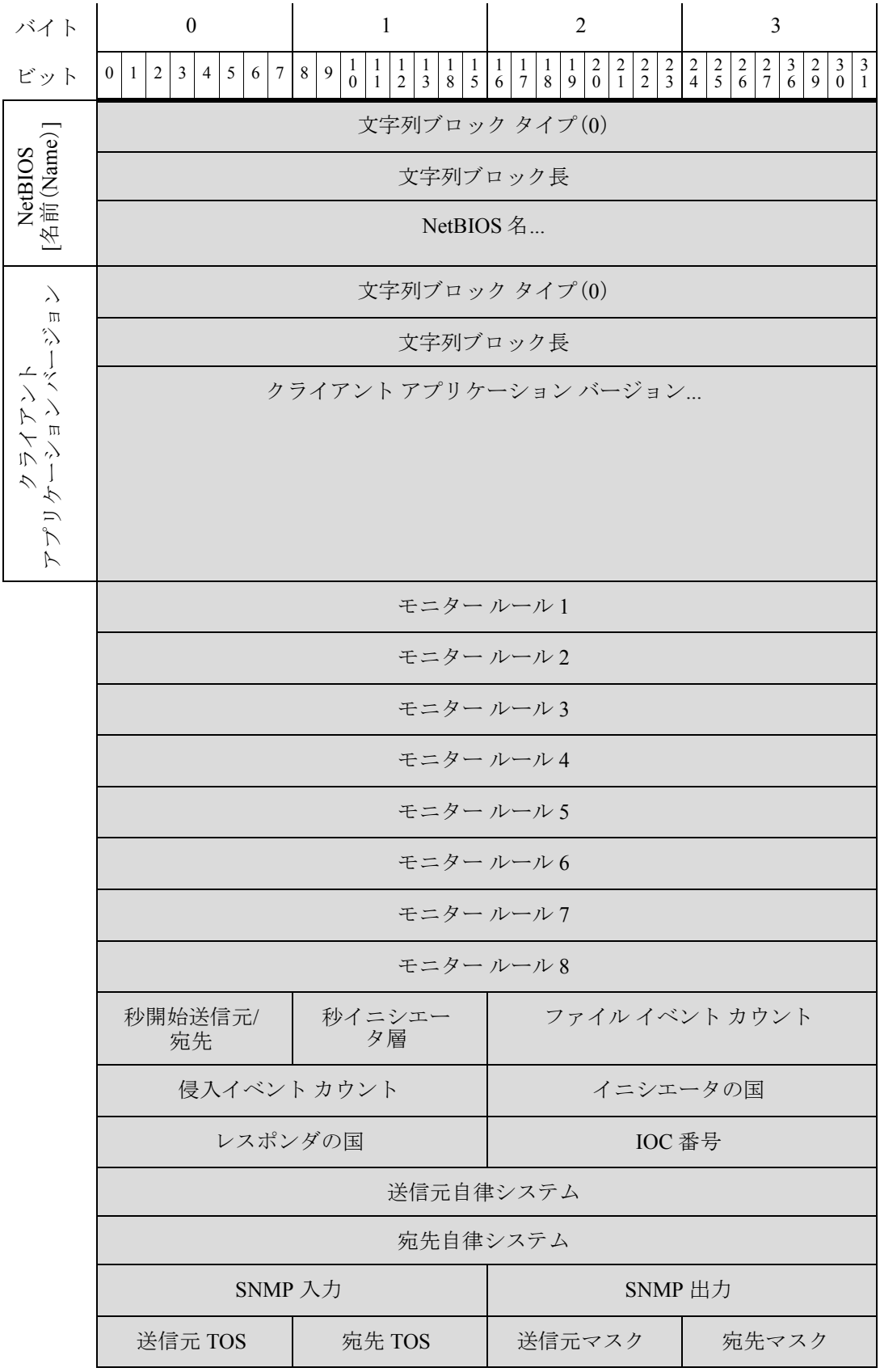
接続統計データ メッセージの詳細については、接続統計データ メッセージ（4-56 ページ）を参照してください。

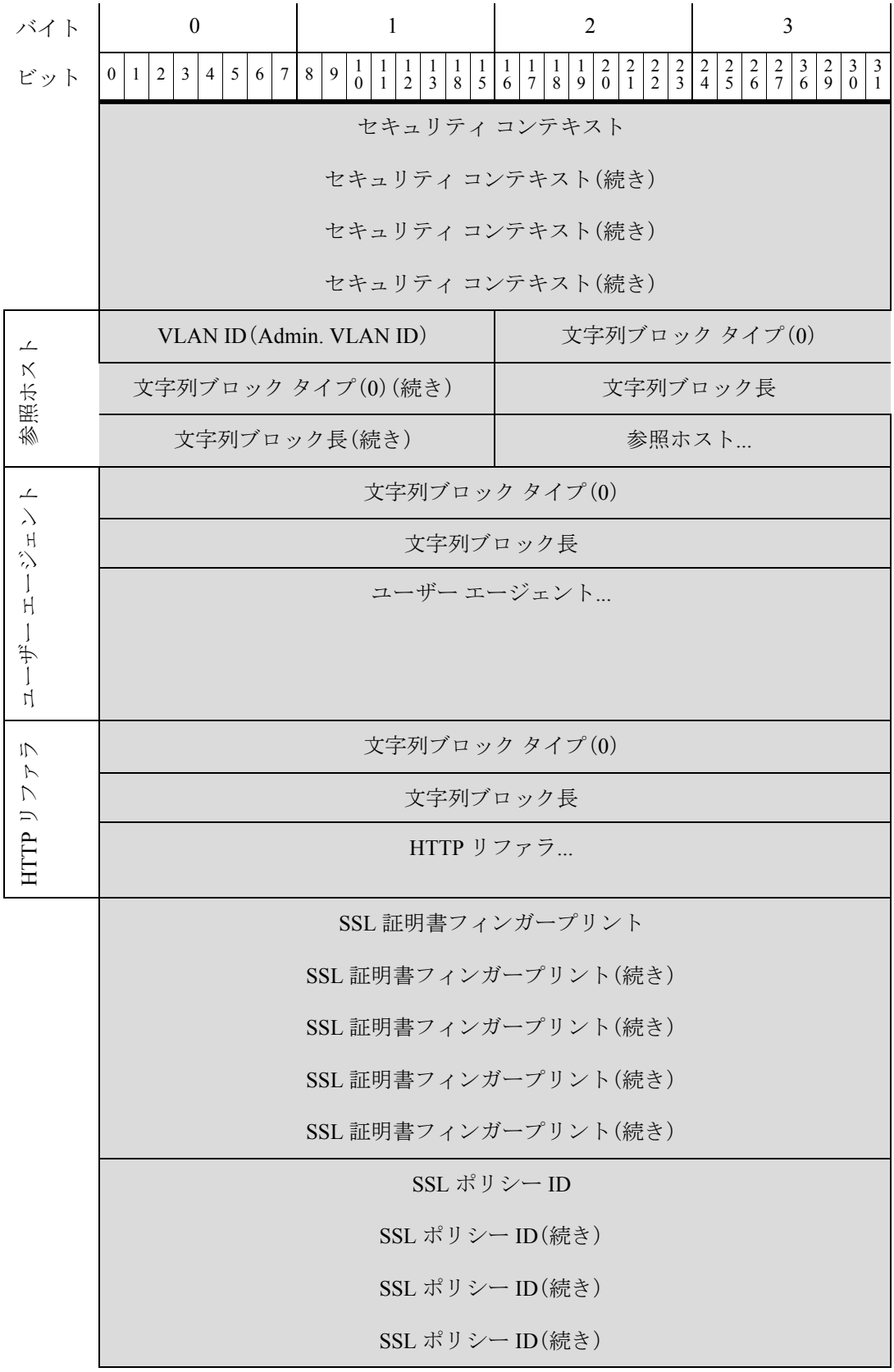
次の図は、接続統計データ ブロック 5.4 の形式を示しています。

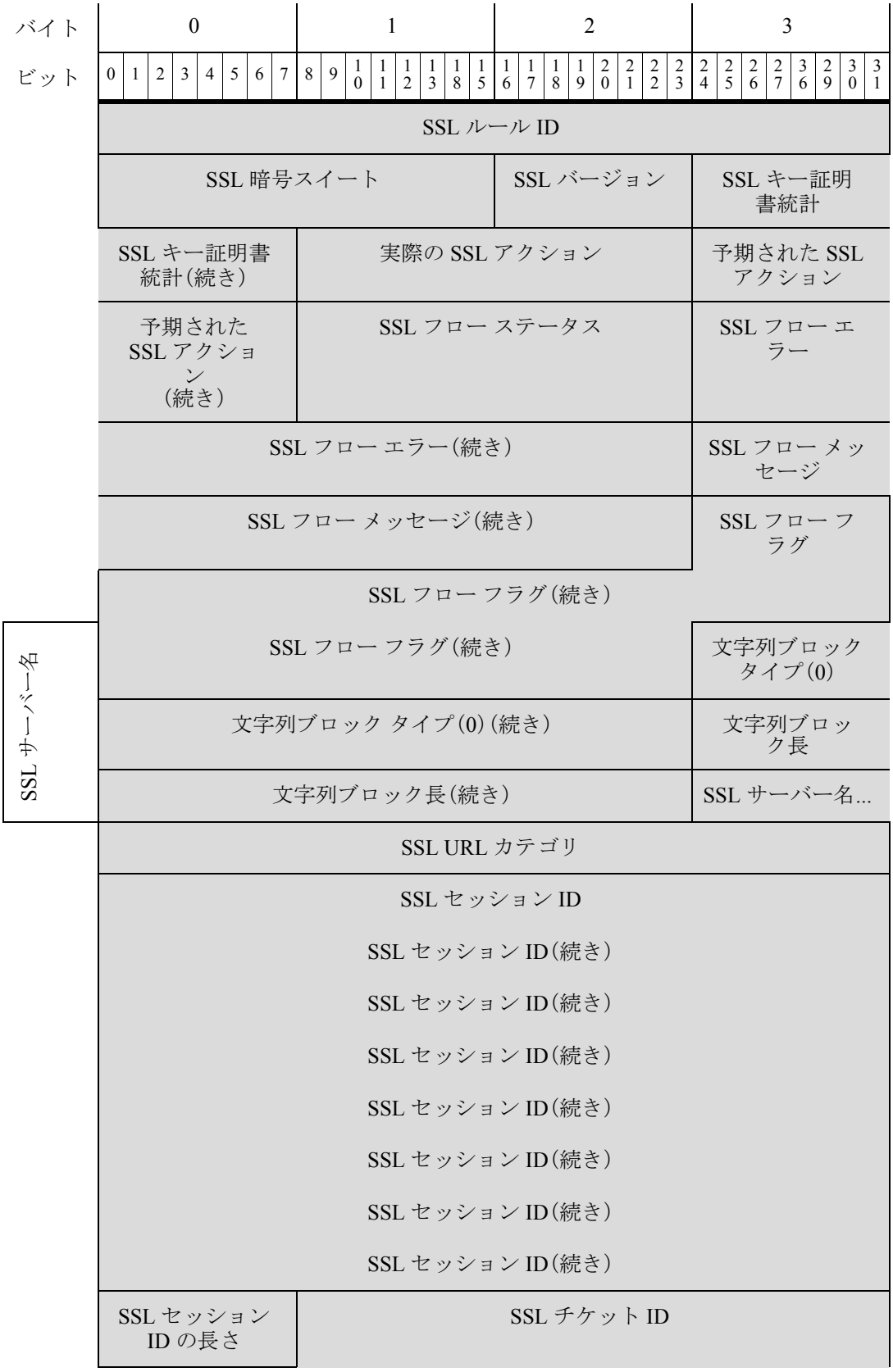
バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
接続データ ブロック タイプ（155）																																
接続データ ブロック長																																
デバイスID（Device ID）																																
入力ゾーン 入力ゾーン（続き） 入力ゾーン（続き） 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																																

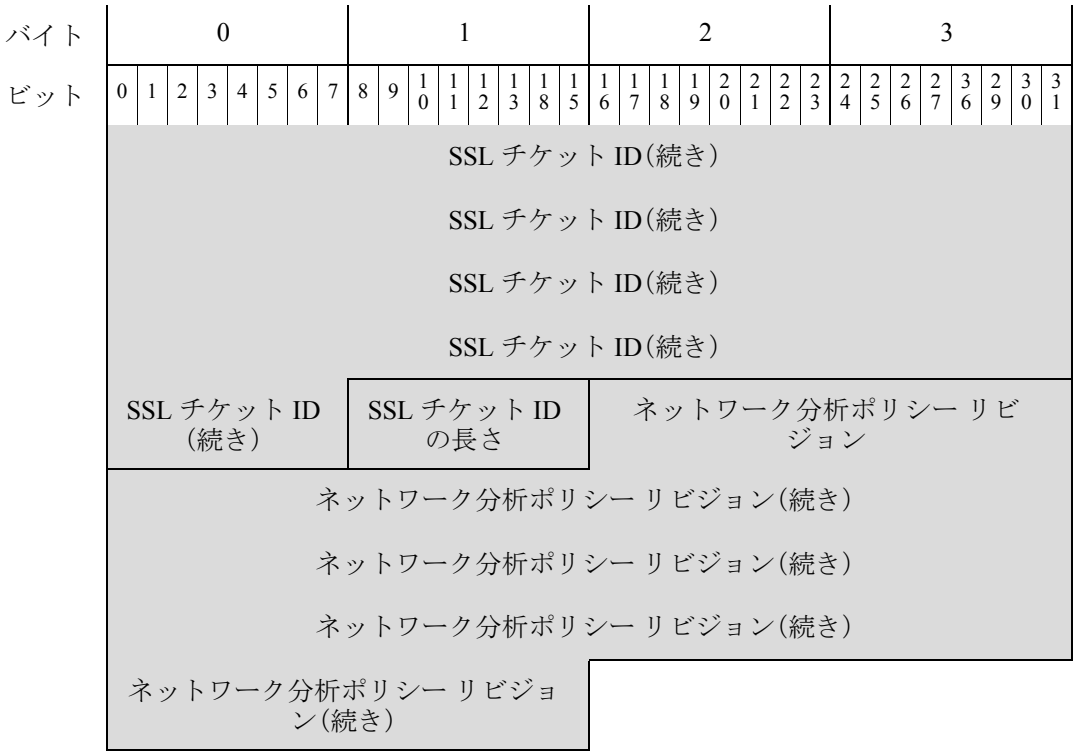

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
出力インターフェイス（続き）
出力インターフェイス（続き）
出力インターフェイス（続き）
イニシエータ IP アドレス
イニシエータ IP アドレス（続き）
イニシエータ IP アドレス（続き）
イニシエータ IP アドレス（続き）
レスポンダ IP アドレス
レスポンダ IP アドレス（続き）
レスポンダ IP アドレス（続き）
レスポンダ IP アドレス（続き）
ポリシー リビジョン
ポリシー 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
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）
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


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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 Packets
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 Bytes
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)
ユーザー ID(User ID)
ユーザー 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...


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
NetBIOS [名前(Name)]
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...
モニター ルール 1
モニター ルール 2
モニター ルール 3
モニター ルール 4
モニター ルール 5
モニター ルール 6
モニター ルール 7
モニター 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


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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(Admin. 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...
ユーザー 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
ユーザー 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)


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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)
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 サーバー名...
SSL サーバー名
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



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-41　　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（Device 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。

表 B-41　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
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ー 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（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。
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。
ユーザー ID（User ID）	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 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)。

表 B-41　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
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。
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。
モニター ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニター ルールの ID。
モニター ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニター ルールの ID。
モニター ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニター ルールの ID。
モニター ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニター ルールの ID。
モニター ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニター ルールの ID。
モニター ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニター ルールの ID。
モニター ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニター ルールの ID。
モニター ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニター ルールの ID。

表 B-41　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
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 アドレスが IP ブロックリストに一致しているかどうか。
セキュリティ インテリジェンス層	uint8	IP ブロ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（Admin. 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	ユーザー 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	ユーザー 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、およびユーザー エージェント フィールドのバイト数を含む）。

表 B-41　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
ユーザー エージェント	string	セッションのユーザー 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 サーバー証明書の 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。
SSL サーバー証明書ステータス	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）：サーバー証明書のステータスは評価されませんでした。 • 1（不明）：サーバー証明書のステータスは判別できませんでした。 • 2（有効）：サーバー証明書は有効です。 • 4（自己署名済み）：サーバー証明書は自己署名です。 • 16（無効な発行者）：サーバー証明書に無効な発行者があります。 • 32（無効な署名）：サーバー証明書に無効な署名があります。 • 64（期限切れ）：サーバー証明書は期限切れです。 • 128（まだ有効でない）：サーバー証明書はまだ有効ではありません。 • 256（取り消し）：サーバー証明書は取り消されました。

表 B-41　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
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-41　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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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-41　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ー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。

表 B-41　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 サーバー名文字列データ 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 サーバー名フィールドのバイト数を含む）。
SSL サーバー名	string	SSL Client Hello でサーバー名に指定された名前。
SSL URL カテゴリ	uint32	サーバー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ー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ーがセッション 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。

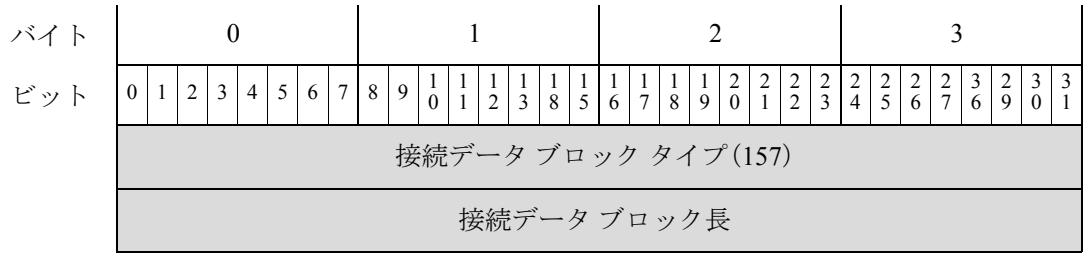
接続統計データ ブロック 5.4.1

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-202 ページ））は廃止されます。

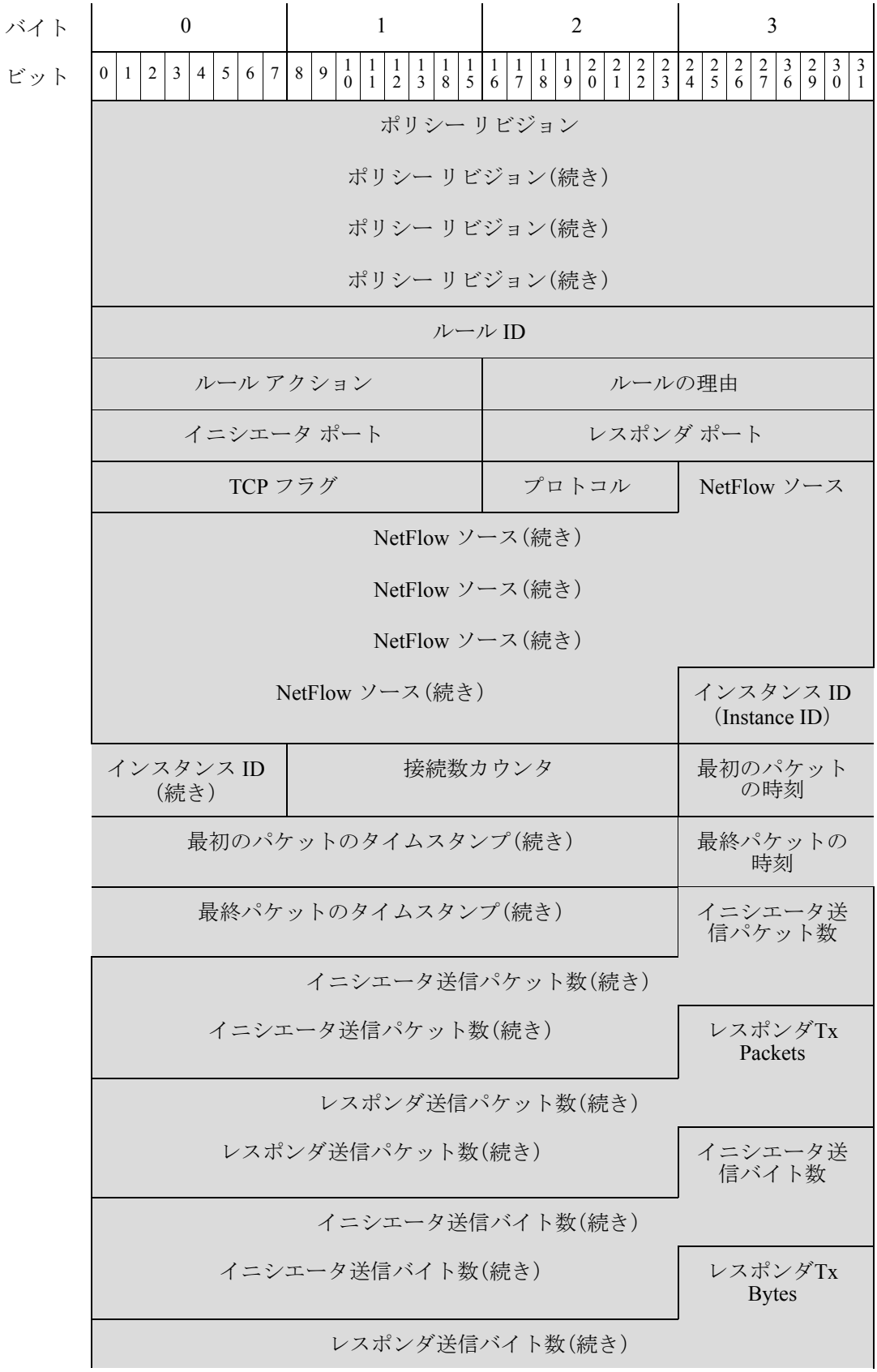
接続イベント レコードを要求するには、イベント バージョン 12 およびイベント コード 71 の要求メッセージ内に、拡張イベント フラグ（要求フラグ フィールドのビット 30）を設定します。要求フラグ（2-15 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

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（4-56 ページ）を参照してください。

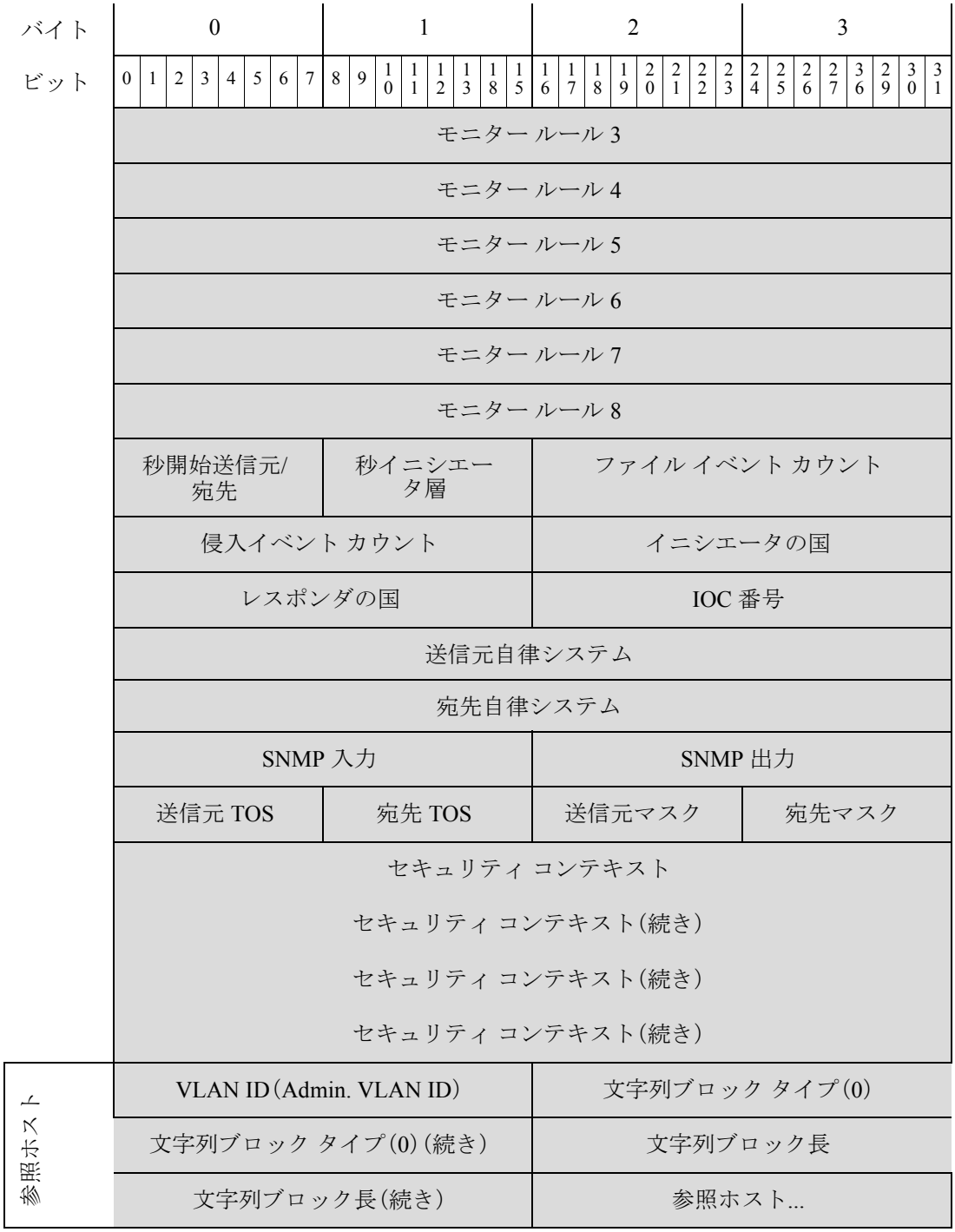
次の図は、接続統計データ ブロック 5.4+の形式を示しています。

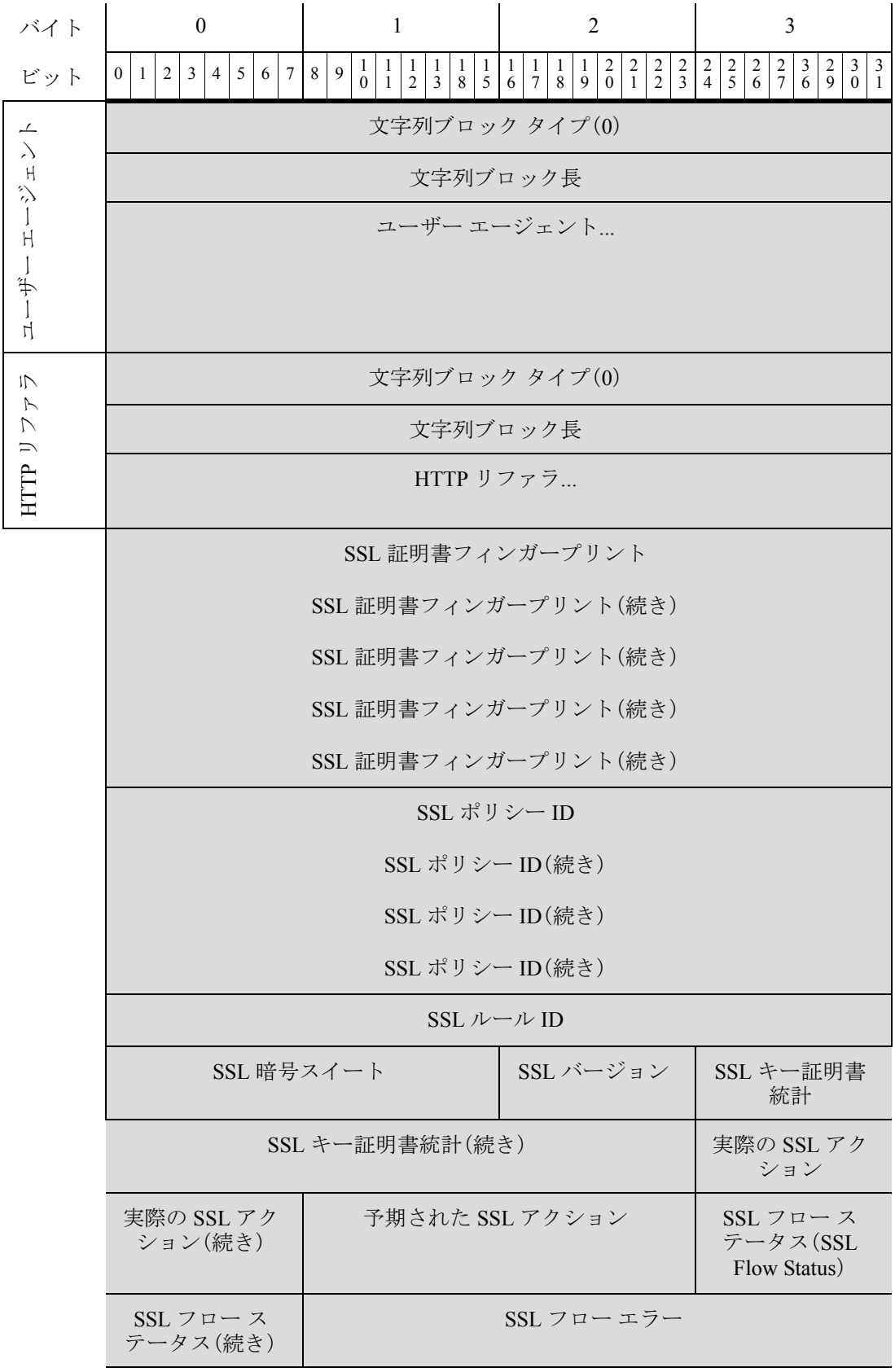


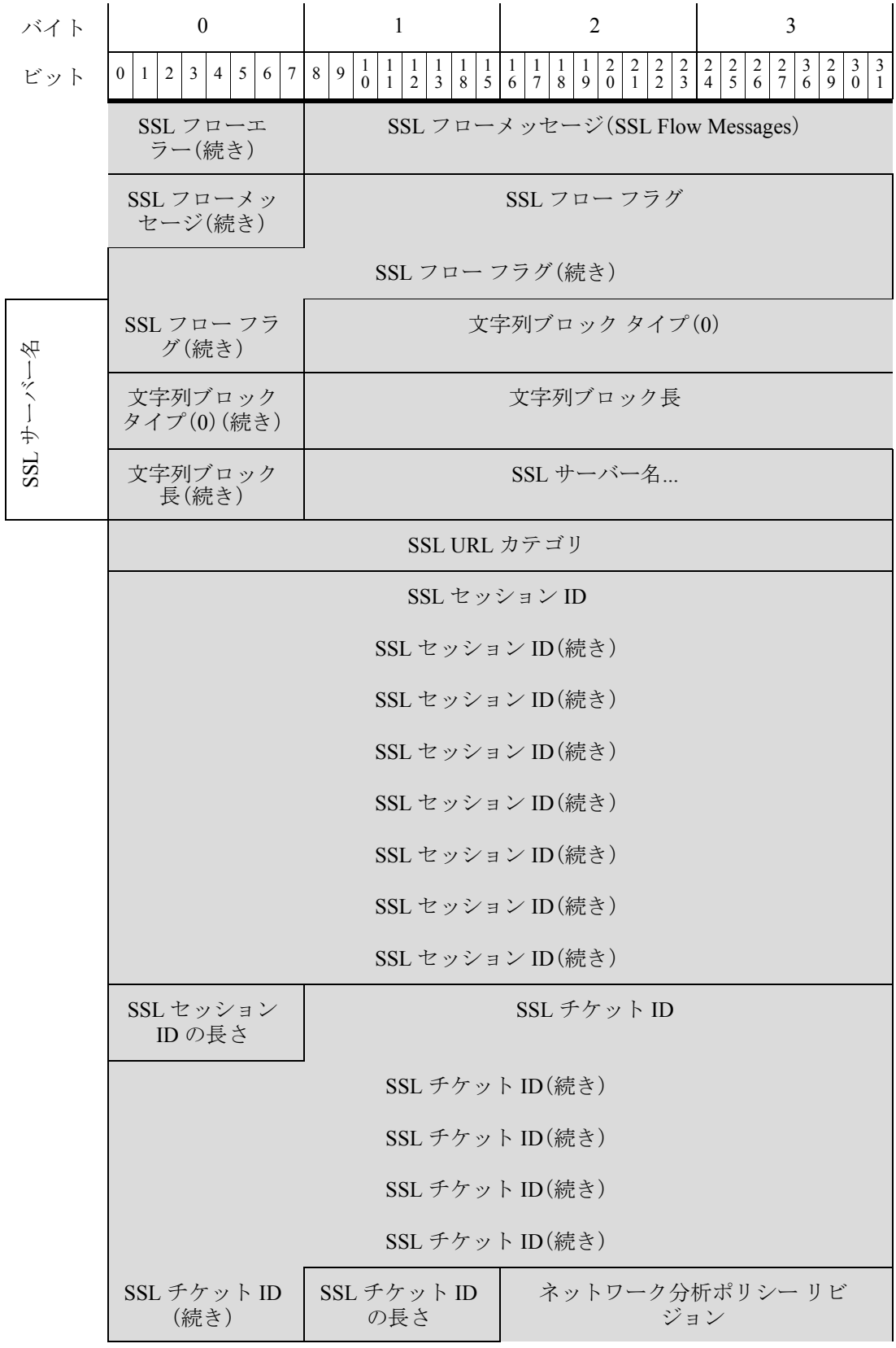
バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
デバイスID（Device ID）																																
入力ゾーン																																
入力ゾーン（続き）																																
入力ゾーン（続き）																																
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																																
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）																																

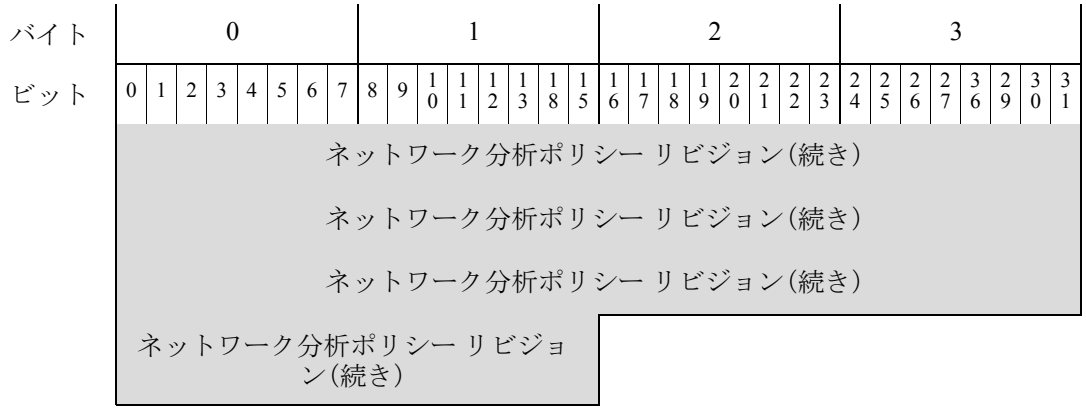

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
ポリシー リビジョン
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ルール ID
ルール アクション
ルールの理由
イニシエータ ポート
レスポンダ ポート
TCP フラグ
プロトコル
NetFlow ソース
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
インスタンス ID (Instance 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 Packets
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 Bytes
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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	レスポンダ送信バイト数（続き）																								ユーザー ID（User ID）							
	ユーザー 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 [名前(Name)]	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...																															
	モニター ルール 1																															
	モニター 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
モニター ルール 3
モニター ルール 4
モニター ルール 5
モニター ルール 6
モニター ルール 7
モニター 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(Admin. 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...


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
ユーザー 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
ユーザー 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
実際の SSL アクション(続き)
予期された SSL アクション
SSL フロー ステータス(SSL Flow Status)
SSL フロー ステータス(続き)
SSL フロー エラー


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
SSL フローエラー(続き)
SSL フローメッセージ(SSL Flow Messages)
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 サーバー名
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 サーバー名...
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



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-42　　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（Device 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ー 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。

表 B-42　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
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（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。
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。
ユーザー ID（User ID）	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 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-42　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。
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。
モニター ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニター ルールの ID。
モニター ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニター ルールの ID。
モニター ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニター ルールの ID。
モニター ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニター ルールの ID。
モニター ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニター ルールの ID。
モニター ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニター ルールの ID。
モニター ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニター ルールの ID。
モニター ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニター 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 アドレスが IP ブロックリストに一致しているかどうか。
セキュリティ インテリジェンス層	uint8	IP ブロ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-42　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（Admin. 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	ユーザー 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	ユーザー 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、およびユーザー エージェント フィールドのバイト数を含む）。
ユーザー エージェント	string	セッションのユーザー 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。

表 B-42　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 証明書フィンガープリント	uint8[20]	SSL サーバー証明書の 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。
SSL サーバー証明書ステータス	uint32	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）：サーバー証明書のステータスは評価されませんでした。 • 1（不明）：サーバー証明書のステータスは判別できませんでした。 • 2（有効）：サーバー証明書は有効です。 • 4（自己署名済み）：サーバー証明書は自己署名です。 • 16（無効な発行者）：サーバー証明書に無効な発行者があります。 • 32（無効な署名）：サーバー証明書に無効な署名があります。 • 64（期限切れ）：サーバー証明書は期限切れです。 • 128（まだ有効でない）：サーバー証明書はまだ有効ではありません。 • 256（取り消し）：サーバー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-42　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-42　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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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-42　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ー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。

表 B-42　接続統計データ ブロック 5.4+のフィールド （続き）

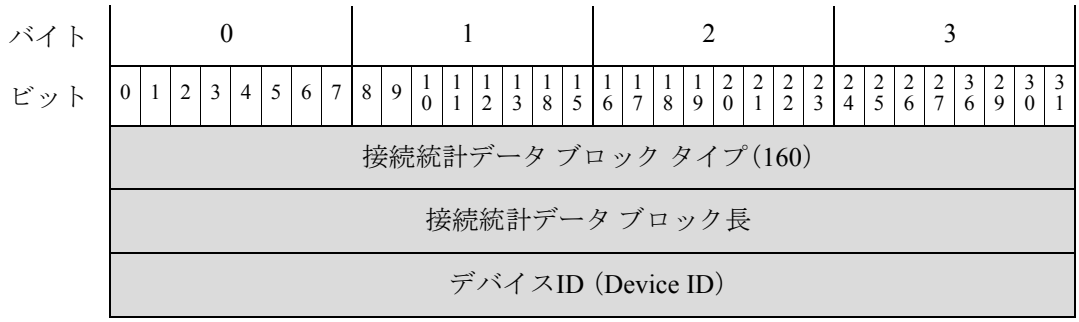
フィールド	データタイプ	説明
文字列ブロック長	uint32	SSL サーバー名文字列データ ブロックに含まれるバイト数（ブロック タイプとヘッダー フィールド用の 8 バイト、および SSL サーバー名フィールドのバイト数を含む）。
SSL サーバー名	string	SSL Client Hello でサーバー名に指定された名前。
SSL URL カテゴリ	uint32	サーバー名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバーがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値
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ーがセッション 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

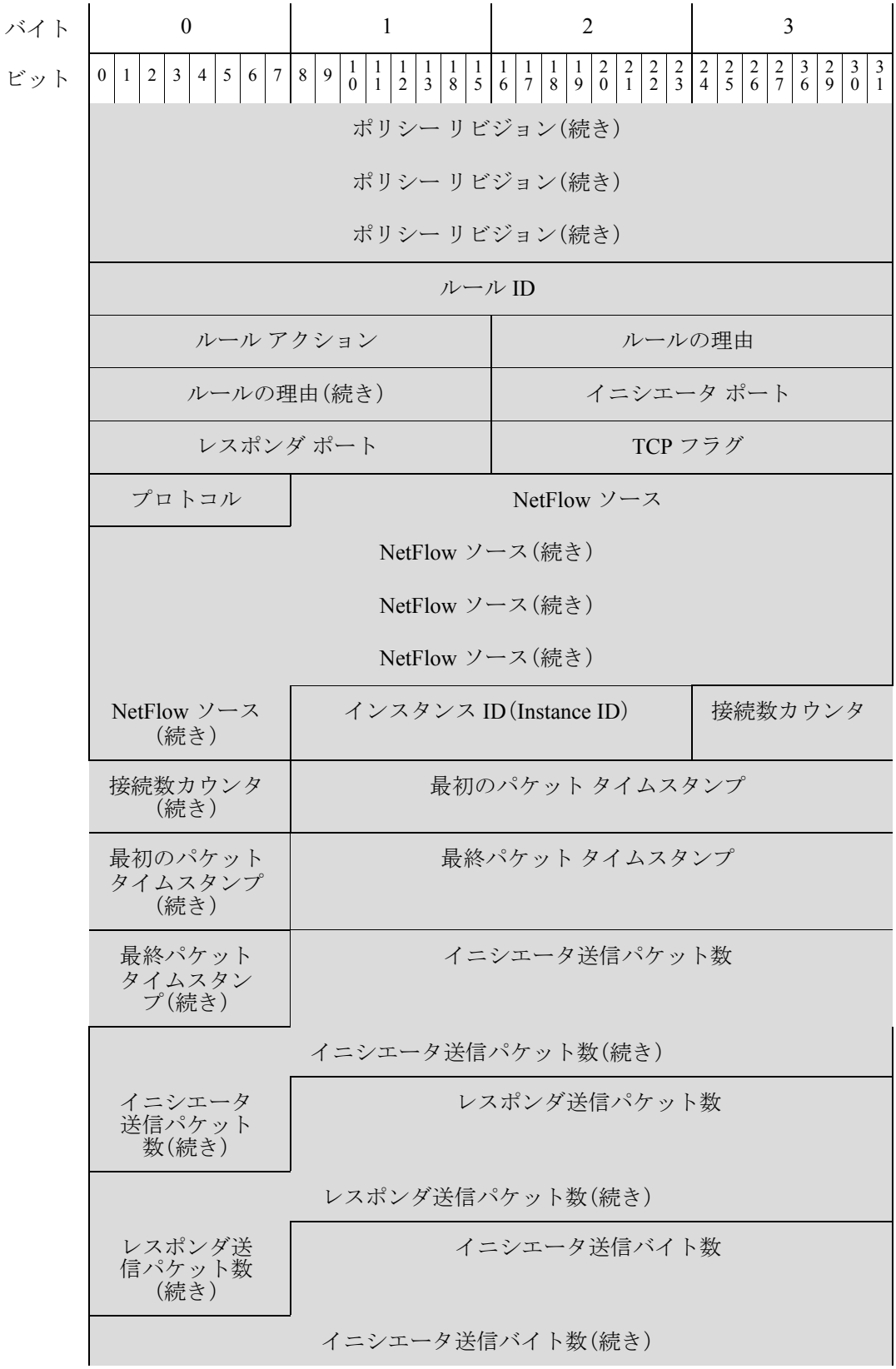
接続統計データ ブロックは、接続データ メッセージで使用されます。接続統計データ ブロック 6.0 には、いくつかの新しいフィールドが追加されました。ISE 統合および複数ネットワーク マップをサポートするために、フィールドが追加されました。バージョン 6.0.x の接続統計データ ブロックは、シリーズ 1 グループのブロックの、ブロック タイプ 160 です。これはブロック タイプ 157（接続統計データ ブロック 5.4.1（B-224 ページ））に取って代わります。DNS ルックアップとセキュリティ インテリジェンスをサポートするため新しいフィールドを追加しました。

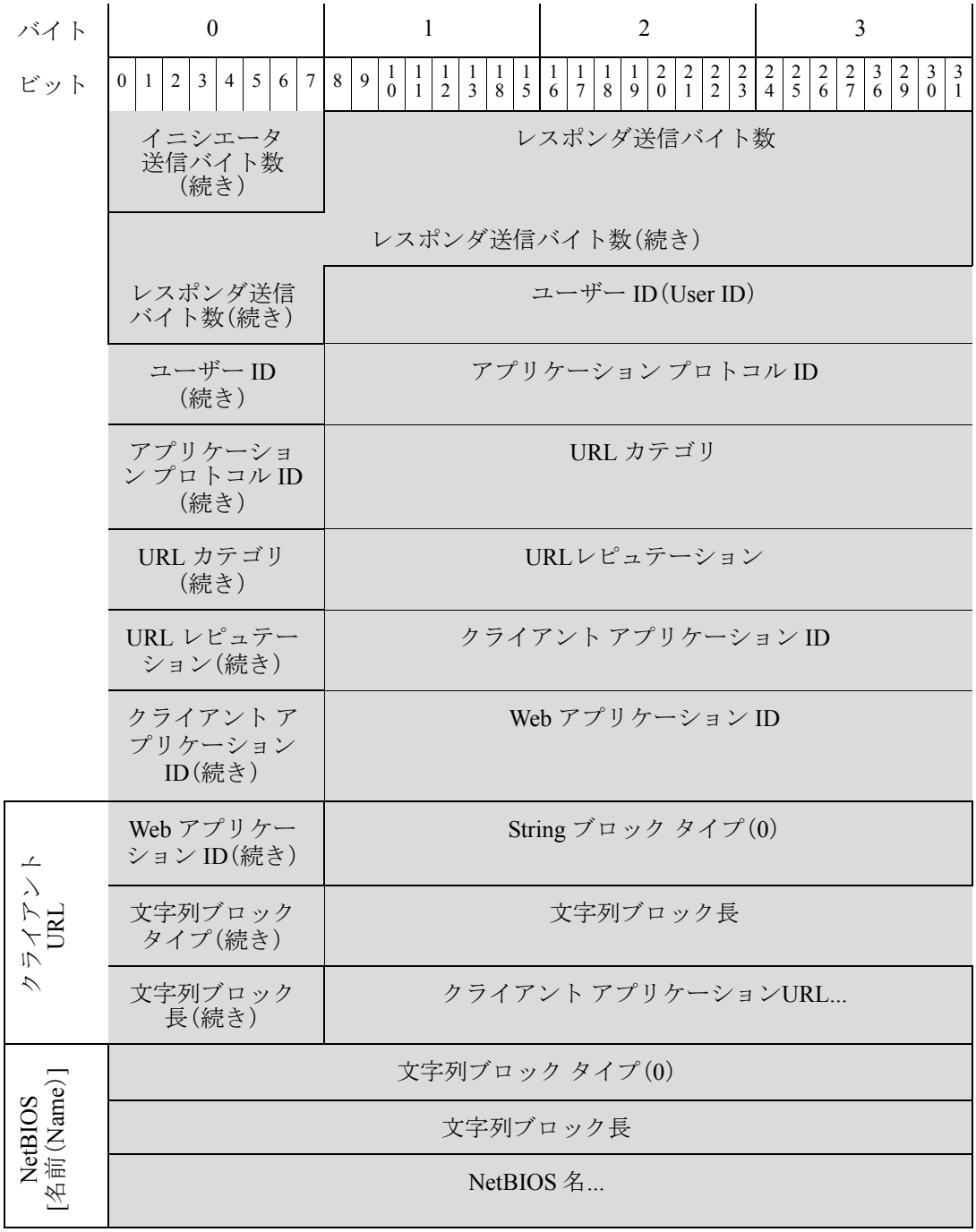
接続イベント レコードは、要求メッセージにイベント バージョン 13 とイベント コード 71 とともに拡張イベント フラグを設定して要求します。要求フラグ（2-15 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

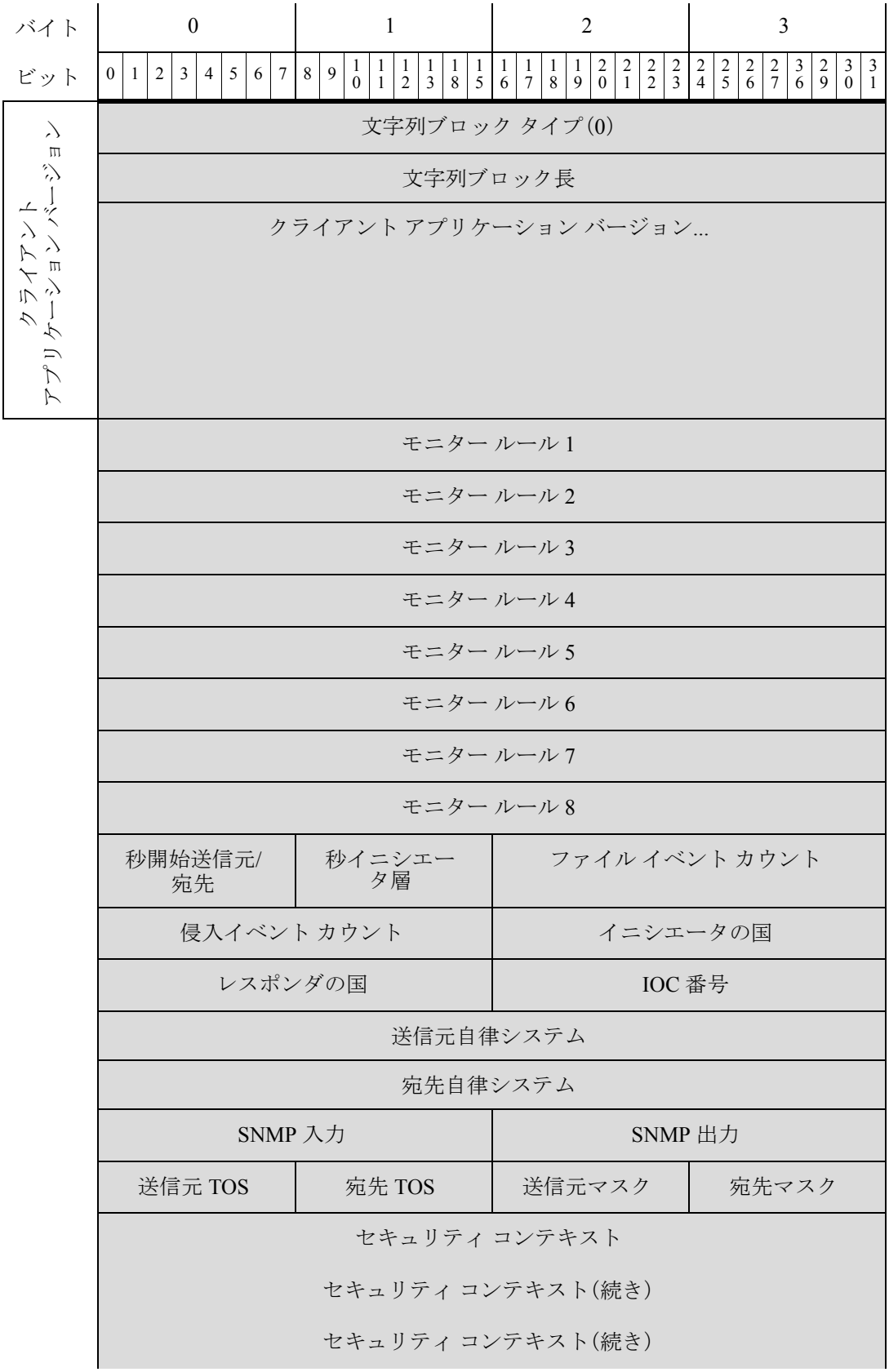
次の図は、接続統計データ ブロック 6.0.x の形式を示しています。

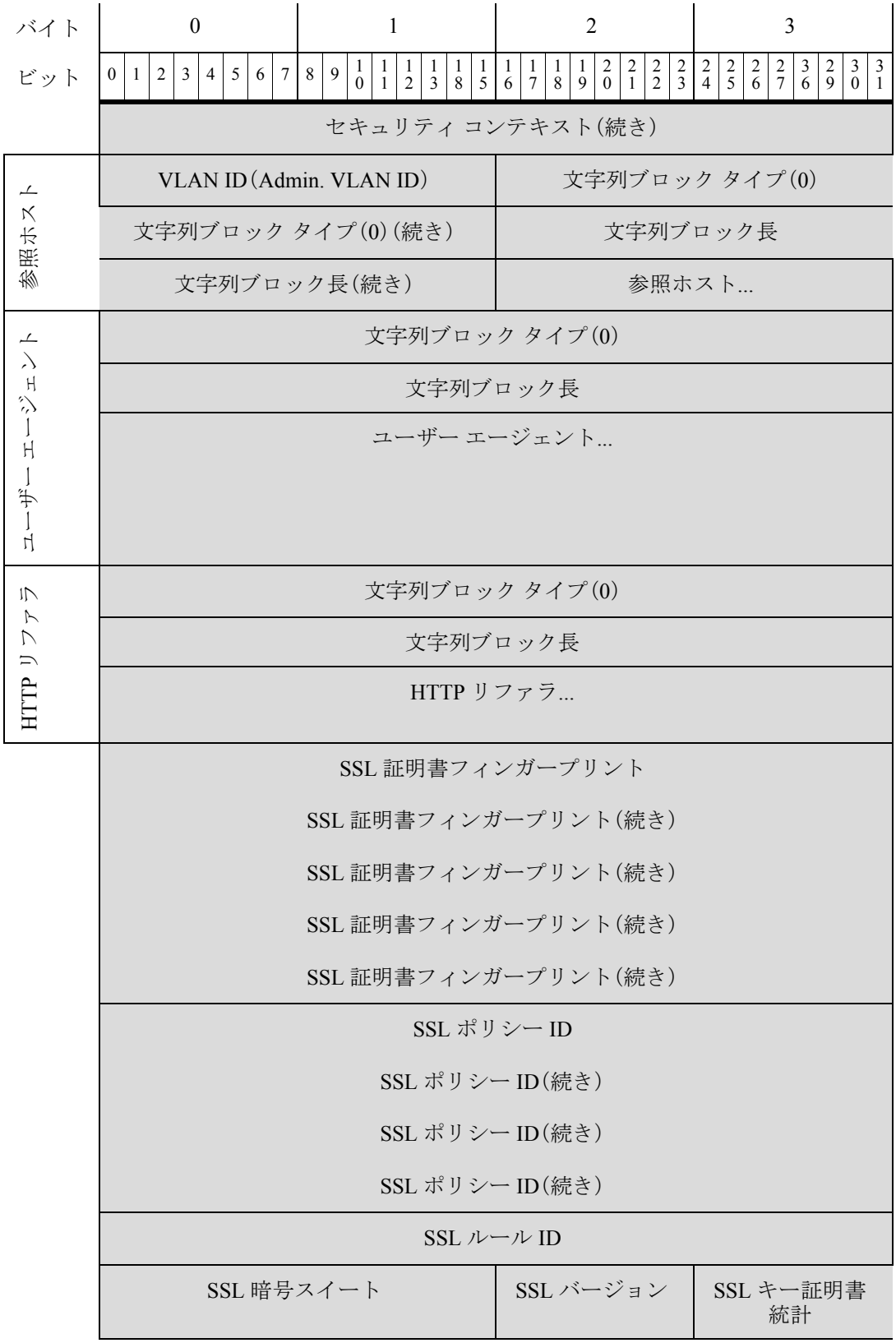


バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
入力ゾーン																																
入力ゾーン（続き）																																
入力ゾーン（続き）																																
入力ゾーン（続き）																																
出力ゾーン	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

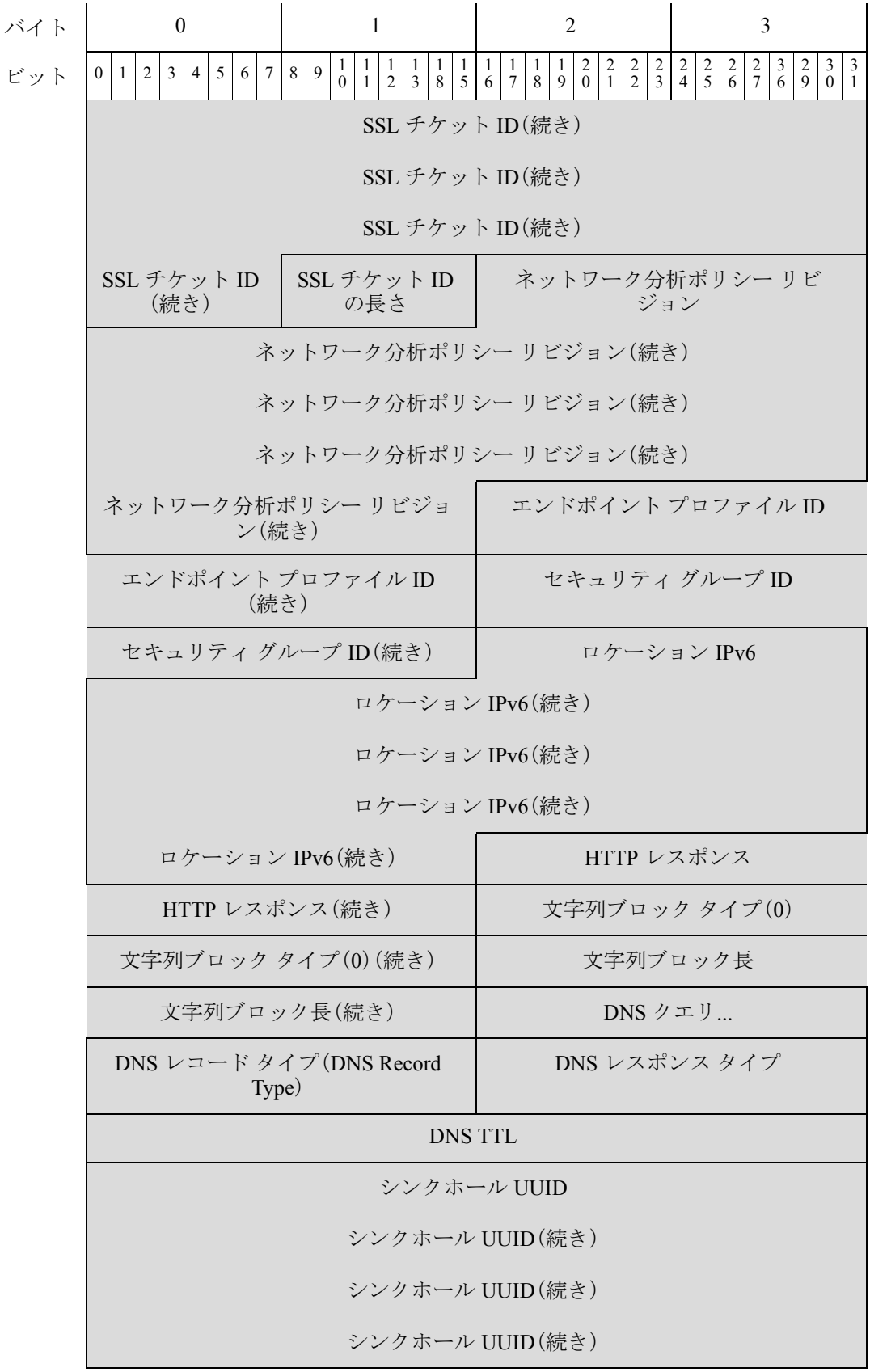

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ルール ID
ルール アクション
ルールの理由
ルールの理由(続き)
イニシエータ ポート
レスポンダ ポート
TCP フラグ
プロトコル
NetFlow ソース
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
インスタンス ID(Instance 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)

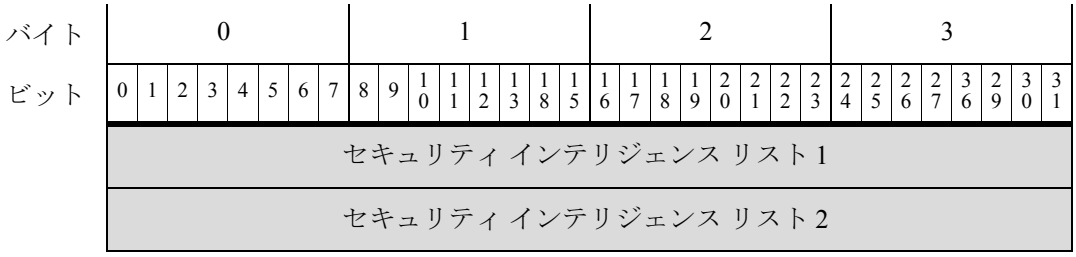

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
イニシエータ送信バイト数（続き）
レスポンダ送信バイト数
レスポンダ送信バイト数（続き）
レスポンダ送信バイト数（続き）
ユーザー ID（User ID）
ユーザー ID（続き）
アプリケーション プロトコル ID
アプリケーション プロトコル ID（続き）
URL カテゴリ
URL カテゴリ（続き）
URLレピュテーション
URL レピュテーション（続き）
クライアント アプリケーション ID
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 [名前（Name）]
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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 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...
モニター ルール 1
モニター ルール 2
モニター ルール 3
モニター ルール 4
モニター ルール 5
モニター ルール 6
モニター ルール 7
モニター 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
セキュリティ コンテキスト(続き)
参照ホスト
VLAN ID(Admin. 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...
ユーザー 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
ユーザー 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


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
SSL キー証明書統計（続き）
実際の SSL アクション
実際の SSL アクション（続き）
予期された SSL アクション
SSL フロー ステータス（SSL Flow Status）
SSL フロー ステータス（続き）
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 Flow Messages）
SSL フローメッセージ（続き）
SSL フローフラグ（SSL Flow Flags）
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）
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 サーバー名...
SSL サーバー名
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）


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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
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)



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-43　　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)。
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ー 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。

表 B-43　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
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。
ユーザー ID（User ID）	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 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 B-43　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
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。
モニター ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニター ルールの ID。
モニター ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニター ルールの ID。
モニター ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニター ルールの ID。
モニター ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニター ルールの ID。
モニター ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニター ルールの ID。
モニター ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニター ルールの ID。
モニター ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニター ルールの ID。
モニター ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニター 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 アドレスが IP ブロックリストに一致しているかどうか。
セキュリティ インテリジェンス層	uint8	IP ブロ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。

表 B-43　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
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（Admin. 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	ユーザー 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	ユーザー 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、およびユーザー エージェント フィールドのバイト数を含む）。
ユーザー エージェント	string	セッションのユーザー 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 サーバー証明書の 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。

表 B-43　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 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 サーバー証明書ステータス	uint32	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）：サーバー証明書のステータスは評価されませんでした。 • 1（不明）：サーバー証明書のステータスは判別できませんでした。 • 2（有効）：サーバー証明書は有効です。 • 4（自己署名済み）：サーバー証明書は自己署名です。 • 16（無効な発行者）：サーバー証明書に無効な発行者があります。 • 32（無効な署名）：サーバー証明書に無効な署名があります。 • 64（期限切れ）：サーバー証明書は期限切れです。 • 128（まだ有効でない）：サーバー証明書はまだ有効ではありません。 • 256（取り消し）：サーバー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-43　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
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-43　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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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-43　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ー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 サーバー名文字列データ 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 サーバー名フィールドのバイト数を含む）。

表 B-43　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 サーバー名	string	SSL Client Hello でサーバー名に指定された名前。
SSL URL カテゴリ	uint32	サーバー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ー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ーがセッション 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 によりユーザーに割り当てられた 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 サーバー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。

表 B-43　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）：サーバー障害 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。

接続統計データ ブロック 6.1.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。6.1.x の接続統計情報データ ブロックに複数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 6.1+ 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-239 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。ブロック タイプ 168 に代わりました（接続統計データ ブロック 7.1+（4-125 ページ））。

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 13 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（2-15 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。

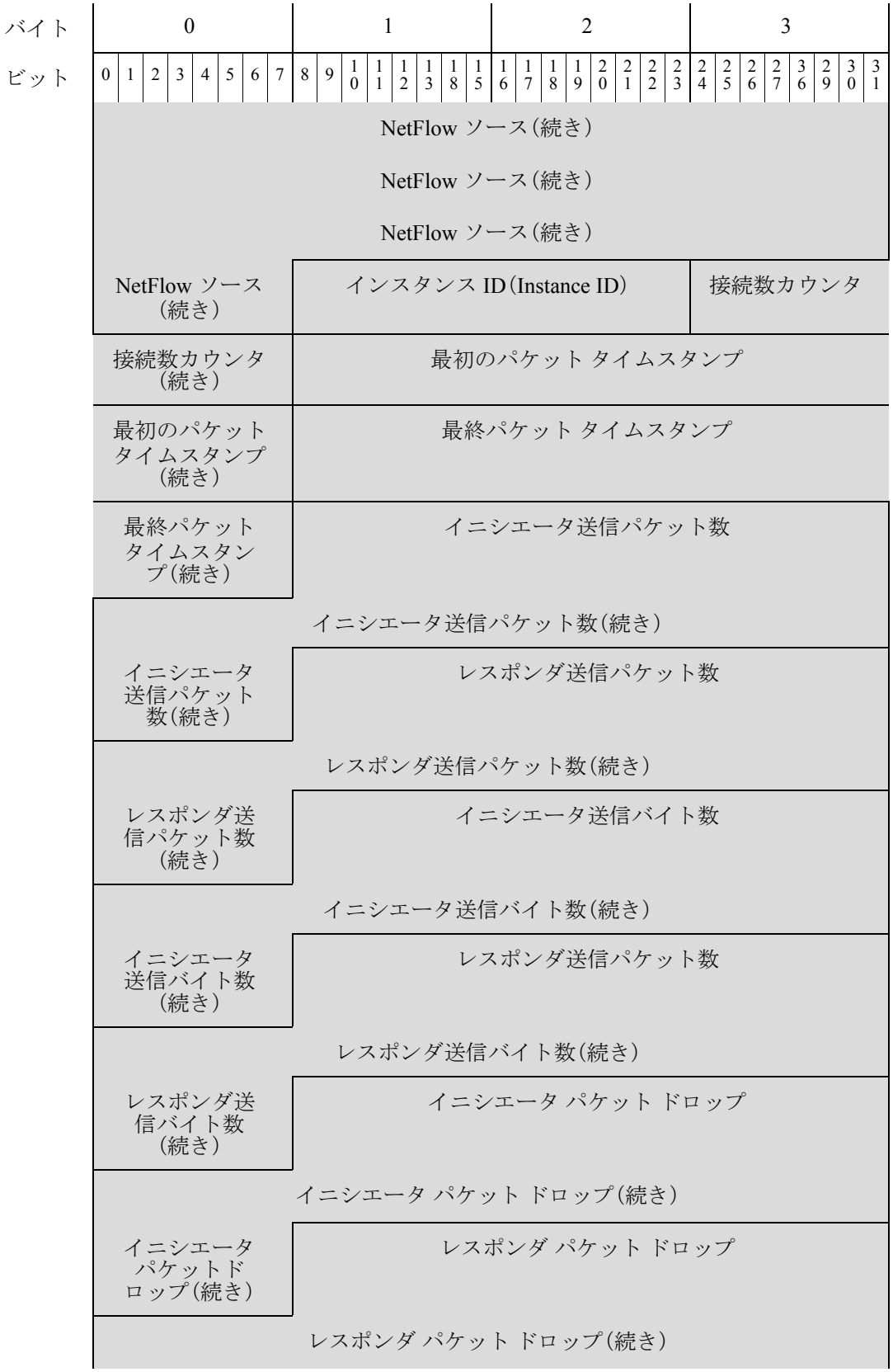
接続統計データ メッセージの詳細については、接続統計データ メッセージ（4-56 ページ）を参照してください。

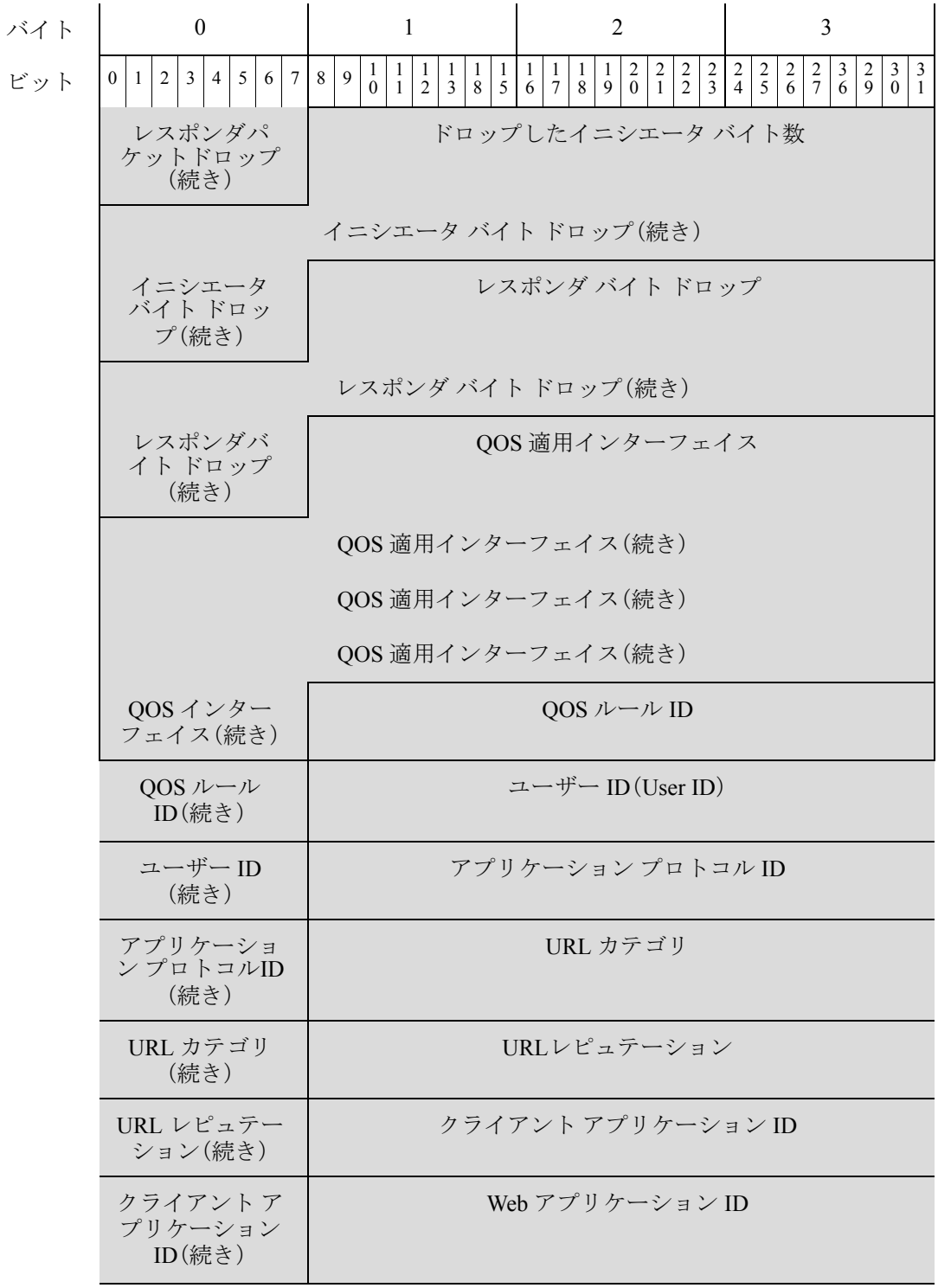
次の図は、6.1+ の接続統計データ ブロックの形式です。

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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（Device 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																																

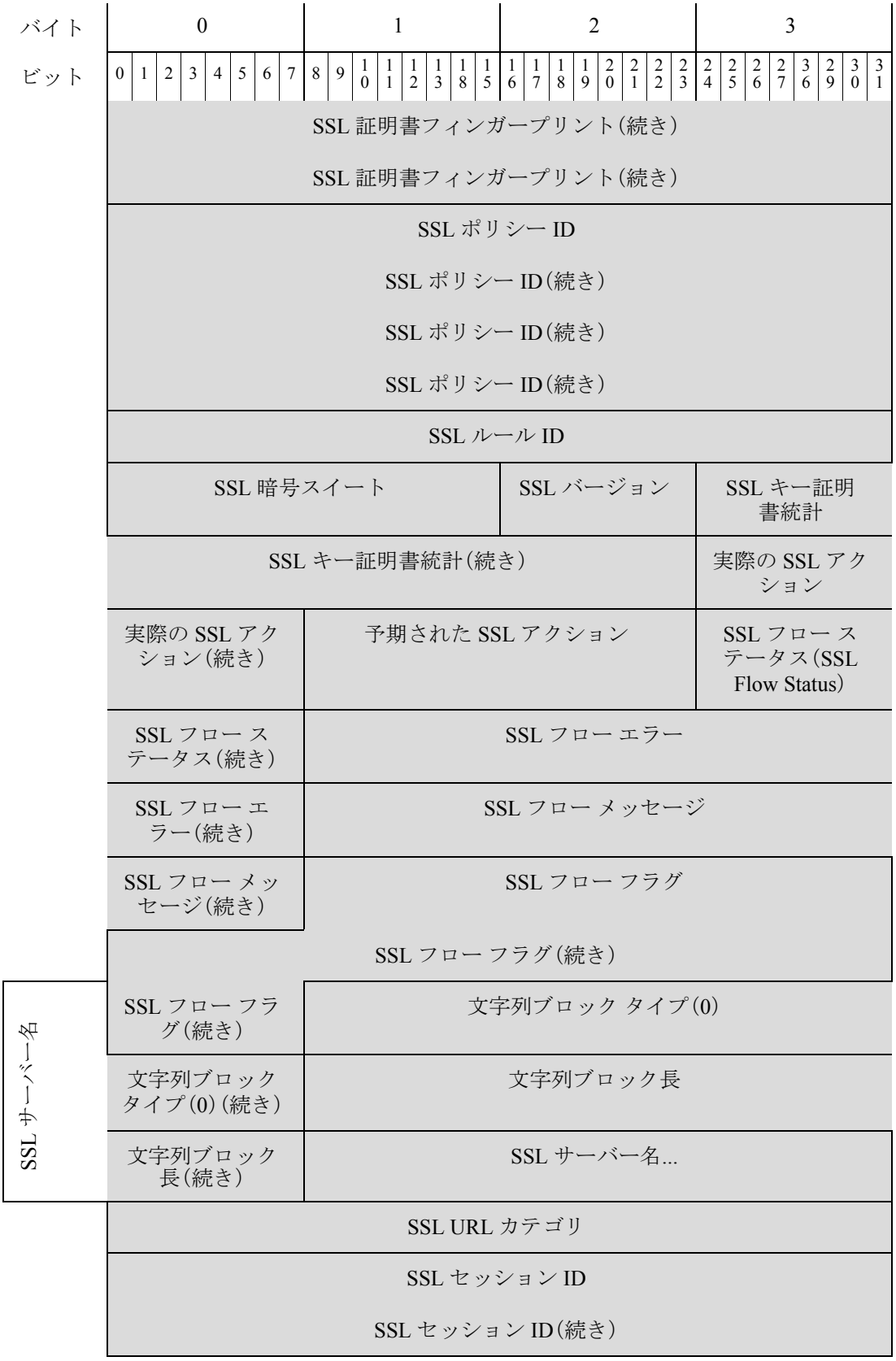
バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
イニシエータ IP アドレス																																
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																																
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																																
トンネル 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																							

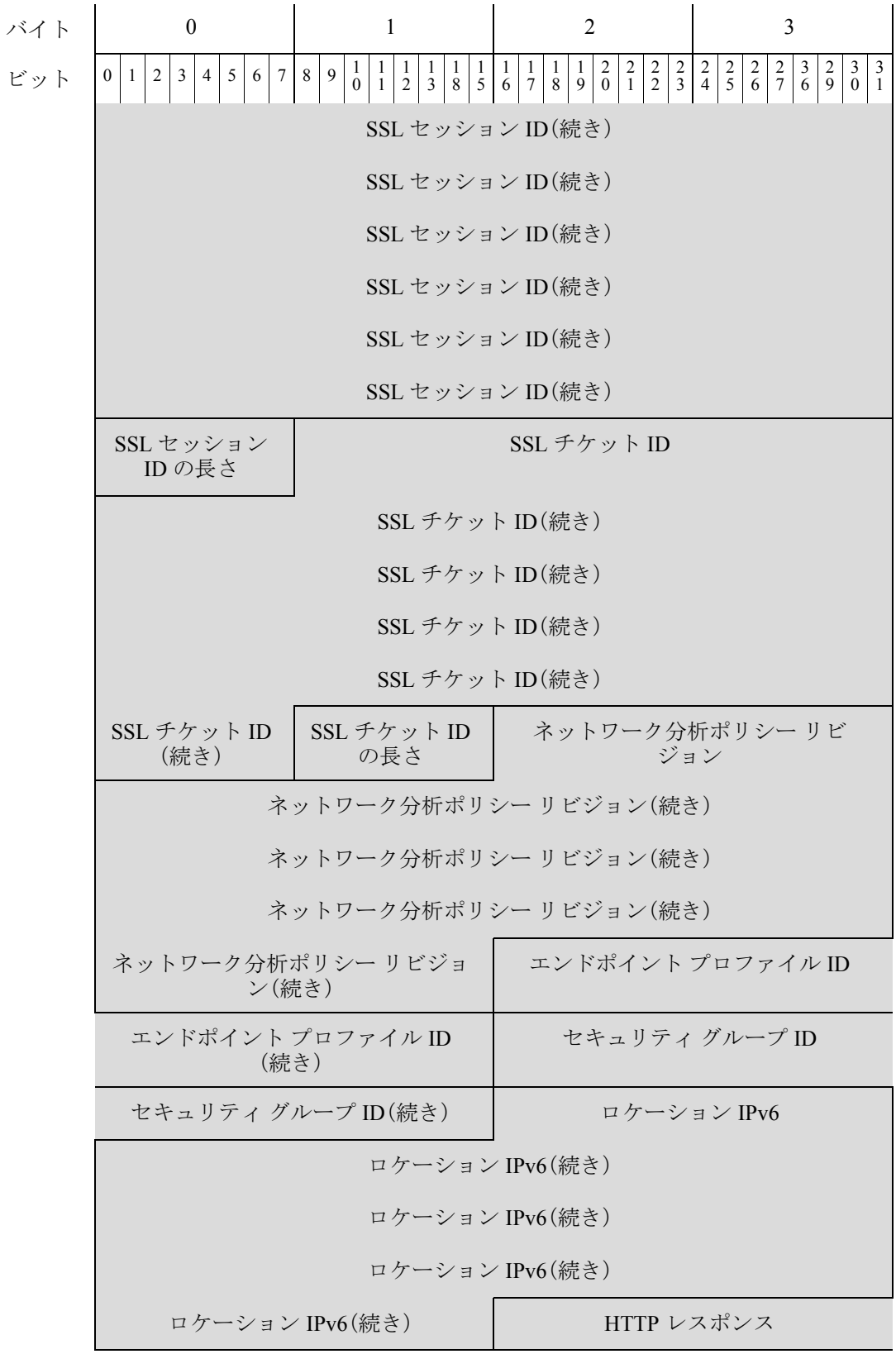

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
NetFlow ソース（続き）
NetFlow ソース（続き）
NetFlow ソース（続き）
NetFlow ソース（続き）
インスタンス ID（Instance ID）
接続数カウンタ
接続数カウンタ（続き）
最初のパケット タイムスタンプ
最初のパケット タイムスタンプ（続き）
最終パケット タイムスタンプ
最終パケット タイムスタンプ（続き）
イニシエータ送信パケット数
イニシエータ送信パケット数（続き）
レスポンダ送信パケット数
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（続き）
イニシエータ送信バイト数
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（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）
イニシエータ パケット ドロップ
レスポンダ送信バイト数（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
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（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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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）
ユーザー ID（User ID）
ユーザー 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 [名前（Name）]		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...																															
		モニター ルール 1																															
		モニター ルール 2																															
		モニター ルール 3																															
		モニター ルール 4																															
		モニター ルール 5																															
		モニター ルール 6																															
		モニター ルール 7																															
		モニター 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															


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
レスポンダの国
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(Admin. 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...
ユーザー 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
ユーザー 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)


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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
実際の SSL アクション(続き)
予期された SSL アクション
SSL フロー ステータス(SSL Flow Status)
SSL フロー ステータス(続き)
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)
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 サーバー名...
SSL サーバー名
SSL URL カテゴリ
SSL セッション ID
SSL セッション ID(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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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
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

次の表は、接続統計データ ブロック 6.1.x のフィールドについての説明です。

表 B-44　　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	接続統計データ ブロック 6.1.x 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（Device 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。

表 B-44　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
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。
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	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	uint16	そのルールに対してユーザー 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（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。
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-44　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
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）。
ユーザー ID（User ID）	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 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。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。

表 B-44　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	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。
モニター ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニター ルールの ID。
モニター ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニター ルールの ID。
モニター ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニター ルールの ID。
モニター ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニター ルールの ID。
モニター ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニター ルールの ID。
モニター ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニター ルールの ID。
モニター ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニター ルールの ID。
モニター ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニター 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 アドレスが IP ブロックリストに一致しているかどうか。
セキュリティ インテリジェンス層	uint8	IP ブロ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。
クライアントのオリジナル国	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。

表 B-44　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
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（Admin. 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	ユーザー 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	ユーザー 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、およびユーザー エージェント フィールドのバイト数を含む）。
ユーザー エージェント	string	セッションのユーザー 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 サーバー証明書の 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。

表 B-44　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 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 サーバー証明書ステータス	uint32	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）：サーバー証明書のステータスは評価されませんでした。 • 1（不明）：サーバー証明書のステータスは判別できませんでした。 • 2（有効）：サーバー証明書は有効です。 • 4（自己署名済み）：サーバー証明書は自己署名です。 • 16（無効な発行者）：サーバー証明書に無効な発行者があります。 • 32（無効な署名）：サーバー証明書に無効な署名があります。 • 64（期限切れ）：サーバー証明書は期限切れです。 • 128（まだ有効でない）：サーバー証明書はまだ有効ではありません。 • 256（取り消し）：サーバー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-44　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
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-44　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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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-44　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ー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。

表 B-44　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 サーバー名文字列データ 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 サーバー名フィールドのバイト数を含む)。
SSL サーバー名	string	SSL Client Hello でサーバー名に指定された名前。
SSL URL カテゴリ	uint32	サーバー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ー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ーがセッション 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 によりユーザーに割り当てられた 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 サーバー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)。

表 B-44　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
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。

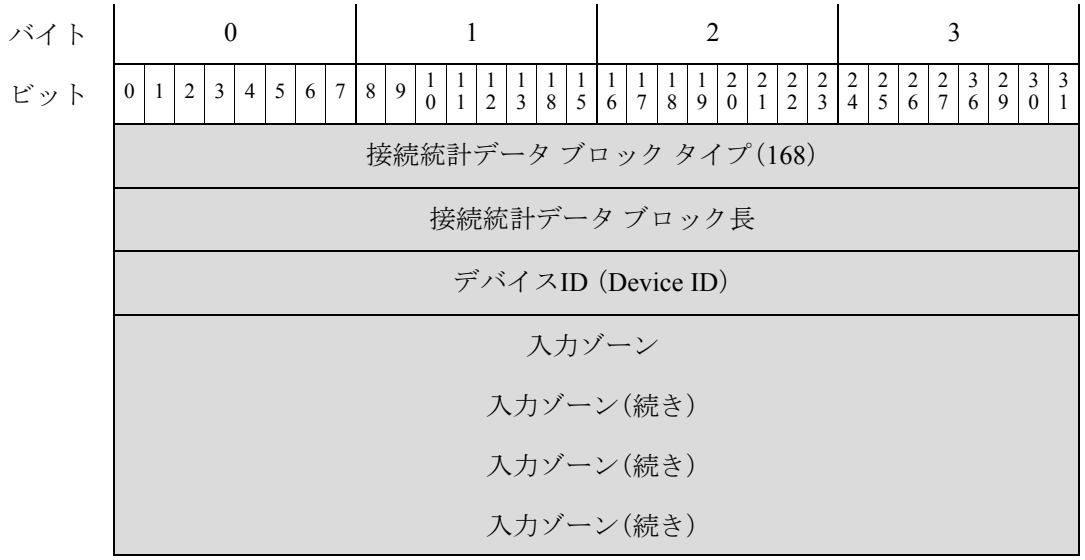
接続統計データブロック 6.2 ～ 6.7.x

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。3 番目のセキュリティ インテリジェンス フィールドが 6.2 ～ 6.7.x の接続統計データブロックに追加されました。バージョン 6.2 ～ 6.7.x の接続統計データブロックには、シリーズ 1 グループのブロックのブロックタイプ 168 が含まれています。これはブロック タイプ163 接続統計データ ブロック 6.1.x（B-257 ページ）に置き換わります。これはブロック タイプ 173 に更新しました。

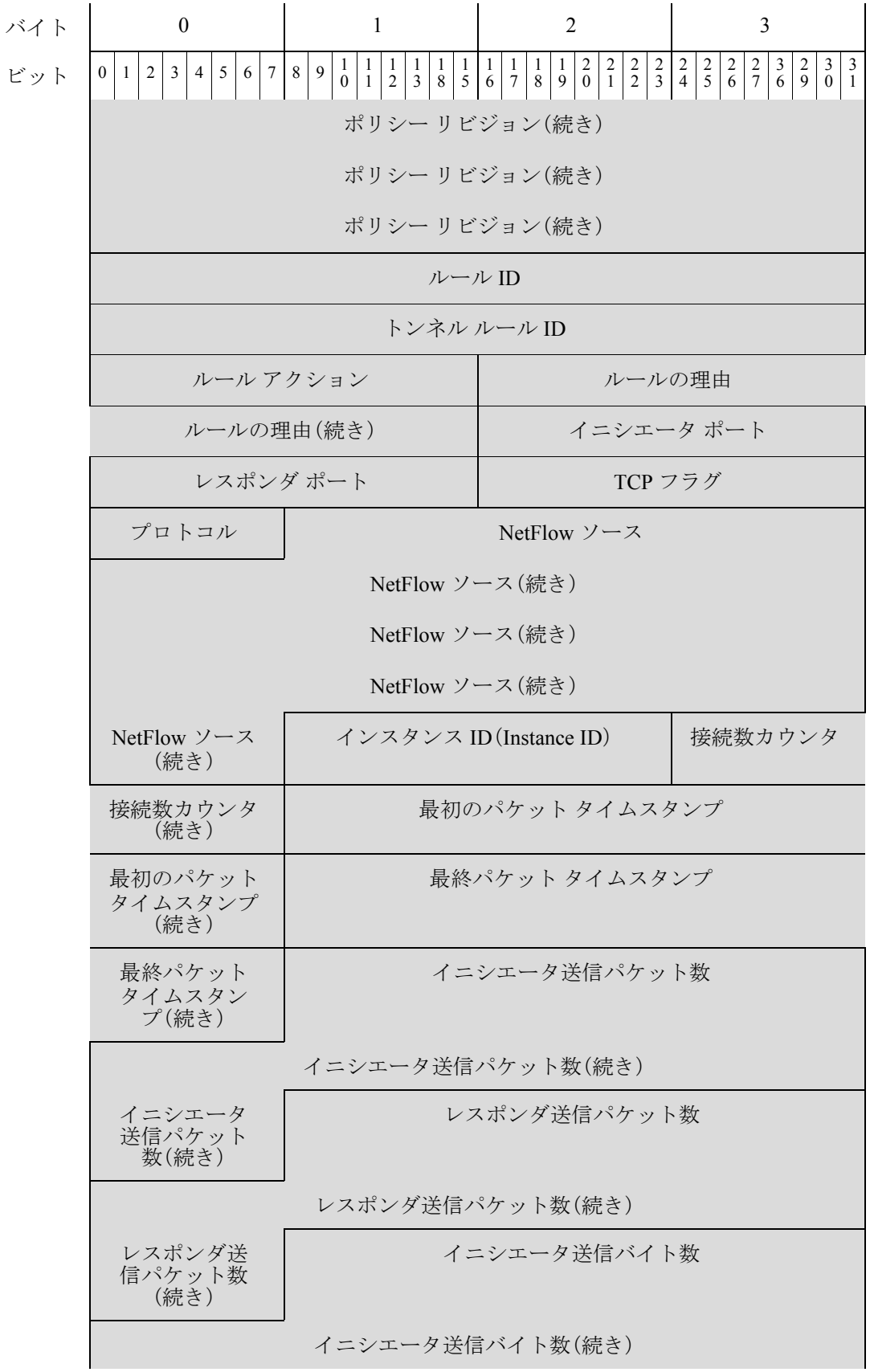
接続イベントレコードを要求するには、イベントバージョン 15 およびイベントコード 71 の要求メッセージ内に、拡張イベントフラグ（要求フラグフィールドのビット 30）を設定します。要求フラグ（2-15 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

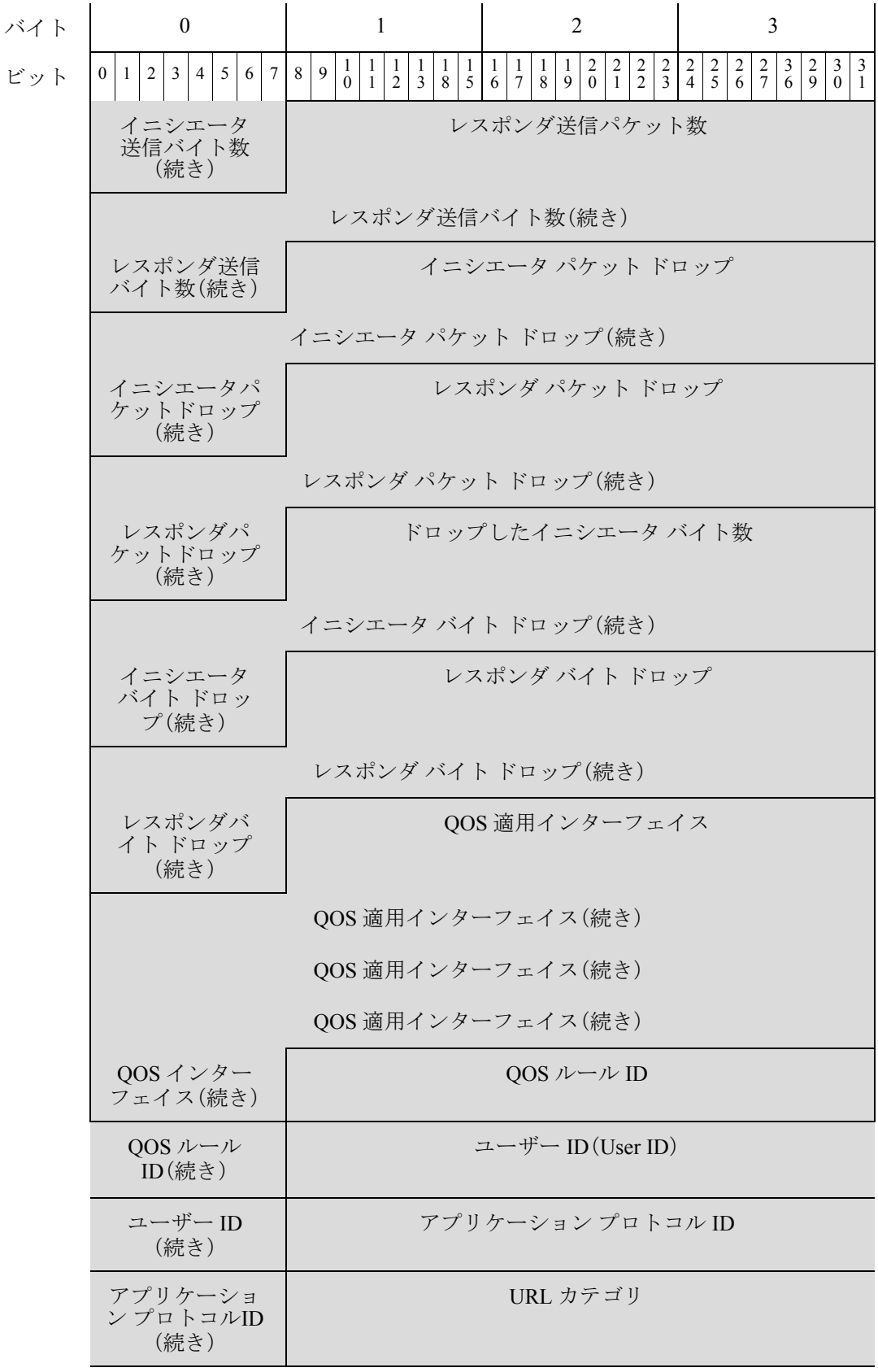
接続統計データ メッセージの詳細については、接続統計データ メッセージ（4-56 ページ）を参照してください。

次の図は、6.2 ～ 6.7.x の接続統計データブロックの形式を示しています。

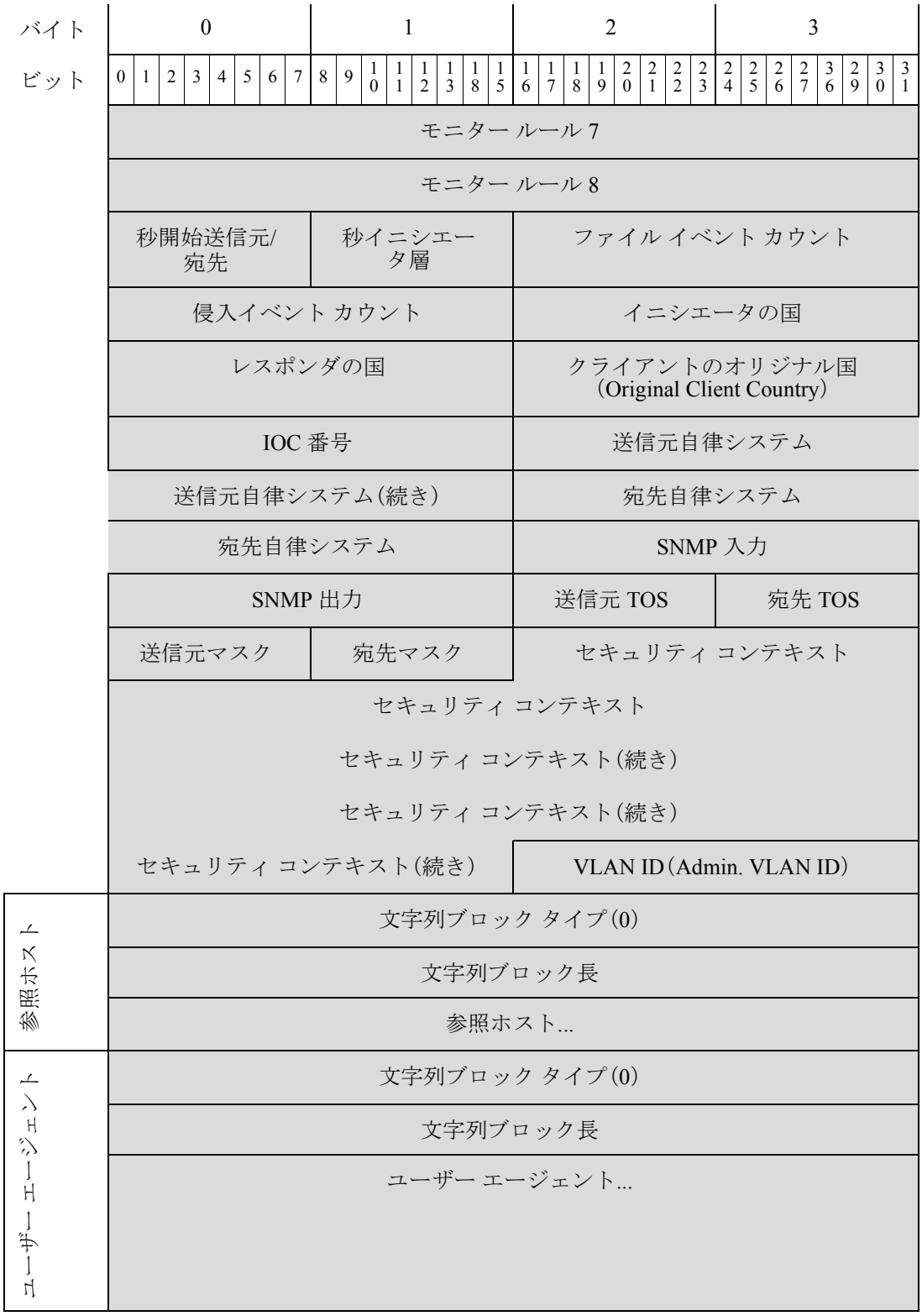


バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
出力ゾーン																																
出力ゾーン(続き)																																
出力ゾーン(続き)																																
出力ゾーン(続き)																																
入力インターフェイス																																
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)																																
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																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 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
トンネル 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(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)

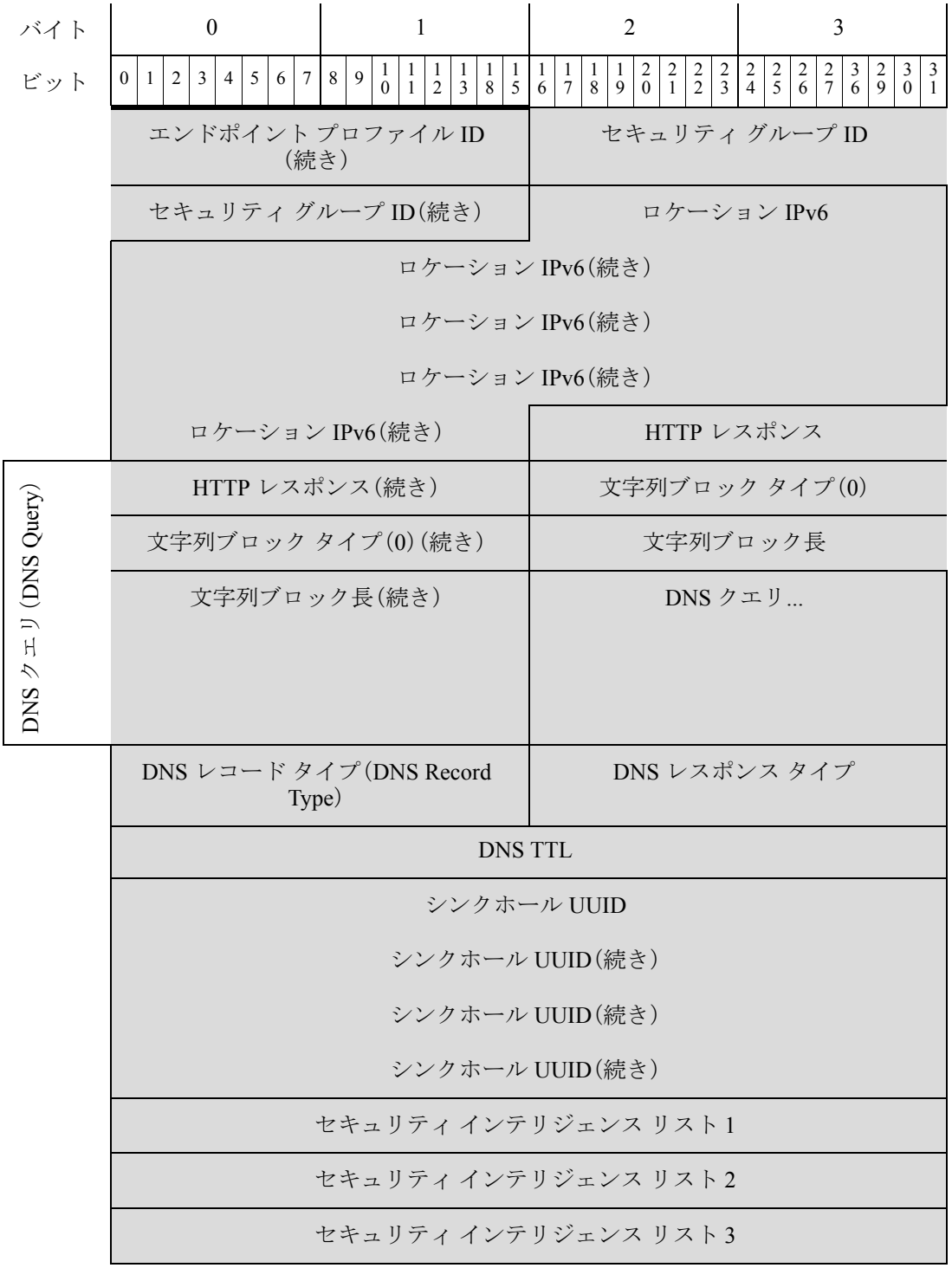

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
イニシエータ送信バイト数（続き）
レスポンダ送信パケット数
レスポンダ送信バイト数(続き)
レスポンダ送信バイト数(続き)
イニシエータ パケット ドロップ
イニシエータ パケット ドロップ(続き)
イニシエータパケットドロップ（続き）
レスポンダ パケット ドロップ
レスポンダ パケット ドロップ(続き)
レスポンダパケットドロップ（続き）
ドロップしたイニシエータ バイト数
イニシエータ 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)
ユーザー ID(User ID)
ユーザー 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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 [名前（Name）]
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...
モニター ルール 1
モニター ルール 2
モニター ルール 3
モニター ルール 4
モニター ルール 5
モニター 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
モニター ルール 7
モニター 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
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（Admin. 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...
ユーザー 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
ユーザー 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 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
実際の SSL アクション(続き)
予期された SSL アクション
SSL フロー ステータス(SSL Flow Status)
SSL フロー ステータス(続き)
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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
SSL サーバー名
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 サーバー名...
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


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 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 クエリ（DNS Query）
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
セキュリティ インテリジェンス リスト 3

次の表は、6.2 ～ 6.7.x の接続統計データブロックのフィールドについての説明です。

表 B-45　接続統計データブロック 6.2 ～ 6.7.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	6.2 ～ 6.7.x の接続統計データブロックを開始します。値は常に 168 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（Device 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。
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	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	uint16	そのルールに対してユーザー 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（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 B-45　接続統計データブロック 6.2 ～ 6.7.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。
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）。
ユーザー ID（User ID）	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 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。

表 B-45　接続統計データブロック 6.2 ～ 6.7.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	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。
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。
モニター ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニター ルールの ID。
モニター ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニター ルールの ID。
モニター ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニター ルールの ID。
モニター ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニター ルールの ID。
モニター ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニター ルールの ID。
モニター ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニター ルールの ID。
モニター ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニター ルールの ID。
モニター ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニター 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 アドレスが IP ブロックリストに一致しているかどうか。
セキュリティ インテリジェンス層	uint8	IP ブロックリストに一致した IP 層。

表 B-45　接続統計データブロック 6.2 ～ 6.7.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 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。
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（Admin. 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	ユーザー 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	ユーザー 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、およびユーザー エージェント フィールドのバイト数を含む）。
ユーザー エージェント	string	セッションのユーザー エージェント ヘッダー フィールドからの情報。

表 B-45　接続統計データブロック 6.2 ～ 6.7.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	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 サーバー証明書の 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。
SSL サーバー証明書ステータス	uint32	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）：サーバー証明書のステータスは評価されませんでした。 • 1（不明）：サーバー証明書のステータスは判別できませんでした。 • 2（有効）：サーバー証明書は有効です。 • 4（自己署名済み）：サーバー証明書は自己署名です。 • 16（無効な発行者）：サーバー証明書に無効な発行者があります。 • 32（無効な署名）：サーバー証明書に無効な署名があります。 • 64（期限切れ）：サーバー証明書は期限切れです。 • 128（まだ有効でない）：サーバー証明書はまだ有効ではありません。 • 256（取り消し）：サーバー証明書は取り消されました。

表 B-45　接続統計データブロック 6.2 ～ 6.7.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)」
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-45　接続統計データブロック 6.2 ～ 6.7.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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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-45　接続統計データブロック 6.2 ～ 6.7.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ー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。

表 B-45　接続統計データブロック 6.2 ～ 6.7.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 サーバー名文字列データ 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 サーバー名フィールドのバイト数を含む）。
SSL サーバー名	string	SSL Client Hello でサーバー名に指定された名前。
SSL URL カテゴリ	uint32	サーバー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ー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ーがセッション 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 によりユーザーに割り当てられた 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 サーバー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 B-45　接続統計データブロック 6.2 ～ 6.7.x 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。接続に関連付けられた 3 つのセキュリティ インテリジェンス リストが存在する場合があります。
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。接続に関連付けられた 3 つのセキュリティ インテリジェンス リストが存在する場合があります。
セキュリティ インテリジェンス リスト 3	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。接続に関連付けられた 3 つのセキュリティ インテリジェンス リストが存在する場合があります。

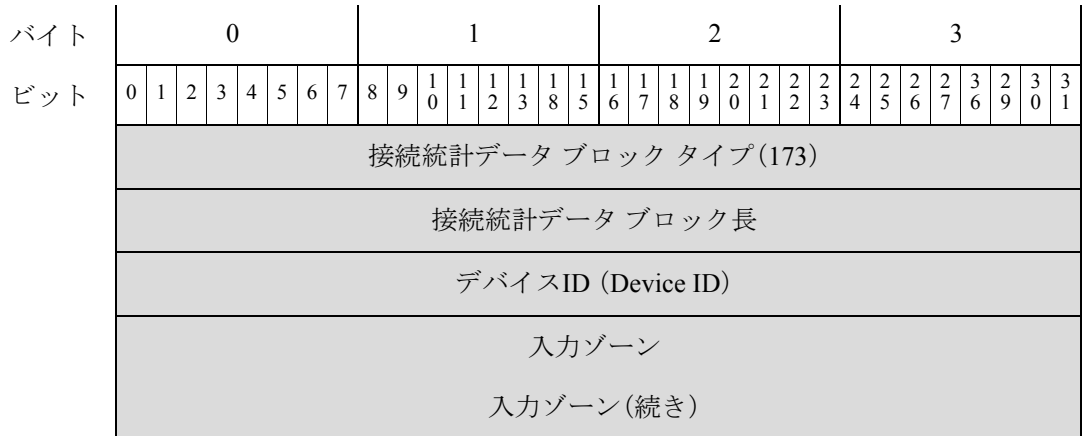
接続統計データ ブロック 7.0

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。セキュリティグループタグ、Virtual Routing and Forwarding、および動的属性のフィールドが 7.0 以降の接続統計データブロックに追加されました。バージョン 7.0 以降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 173 です。これはブロック タイプ168 接続統計データブロック 6.2 ～ 6.7.x（B-275 ページ）に置き換わります。これはブロックタイプ 174 により取って代わられます。

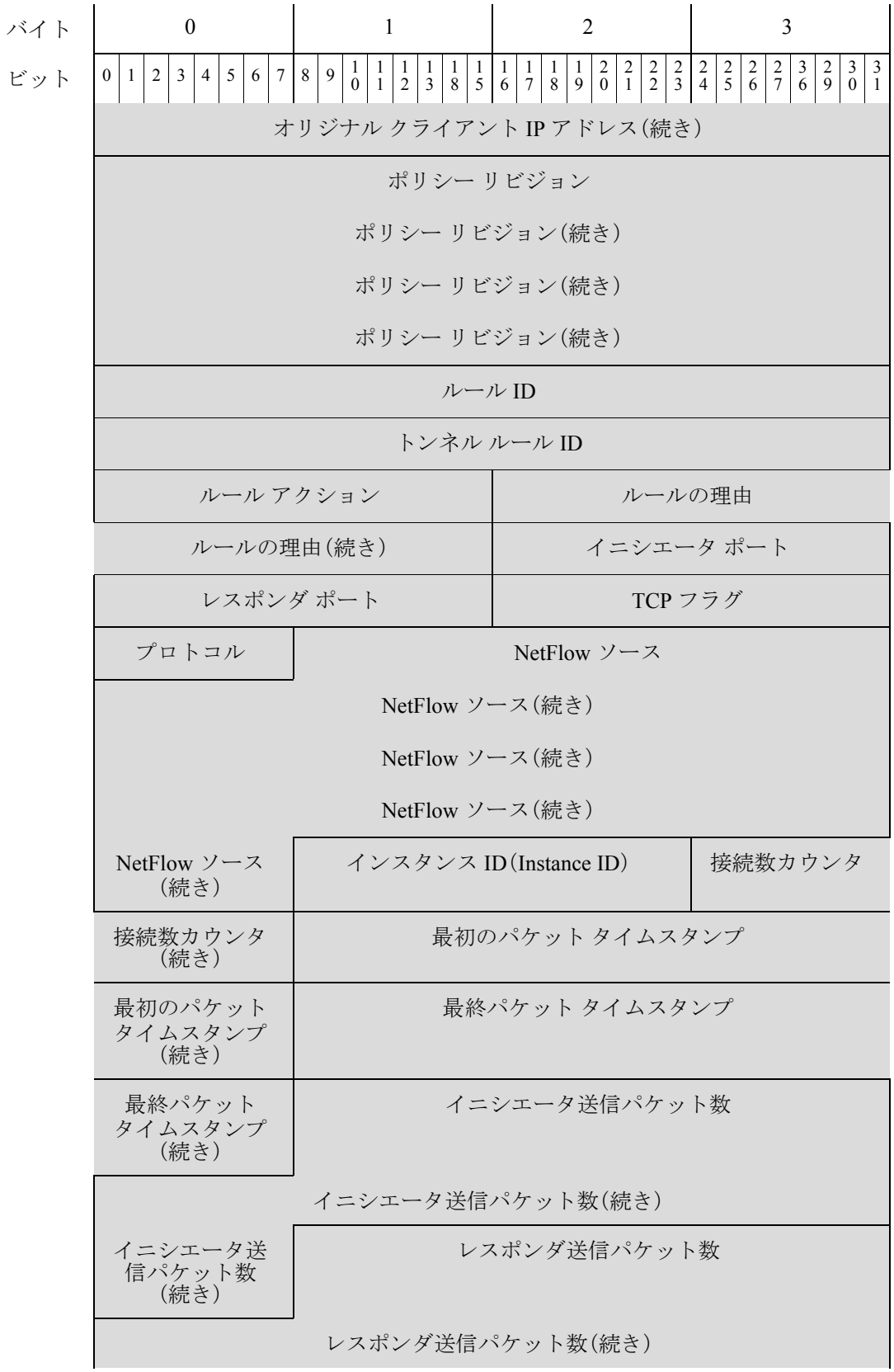
接続イベントレコードを要求するには、イベントバージョン 16 およびイベントコード 71 の要求メッセージ内に、拡張イベントフラグ（要求フラグフィールドのビット 30）を設定します。要求フラグ（2-15 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

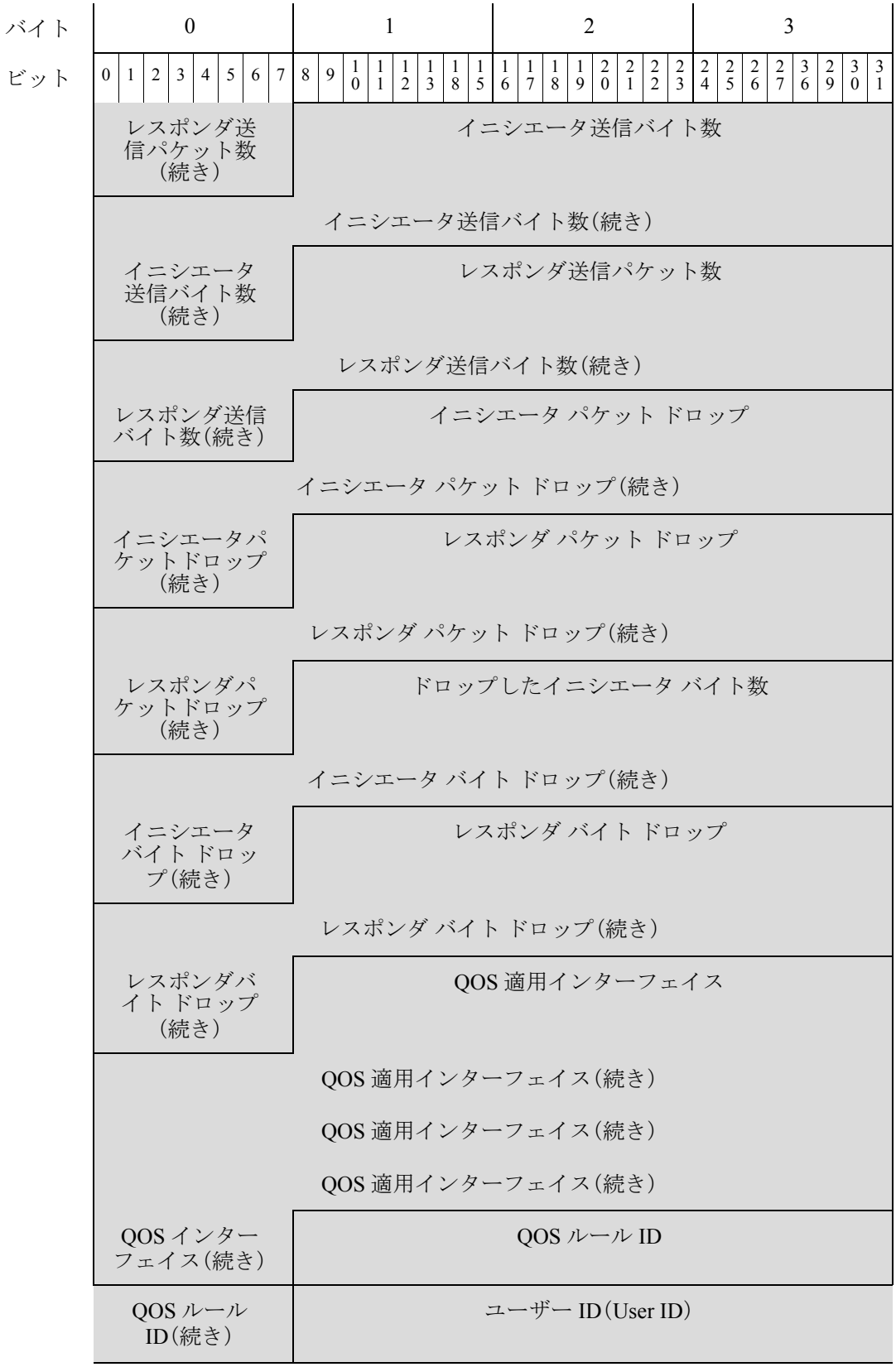
接続統計データ メッセージの詳細については、接続統計データ メッセージ（4-56 ページ）を参照してください。

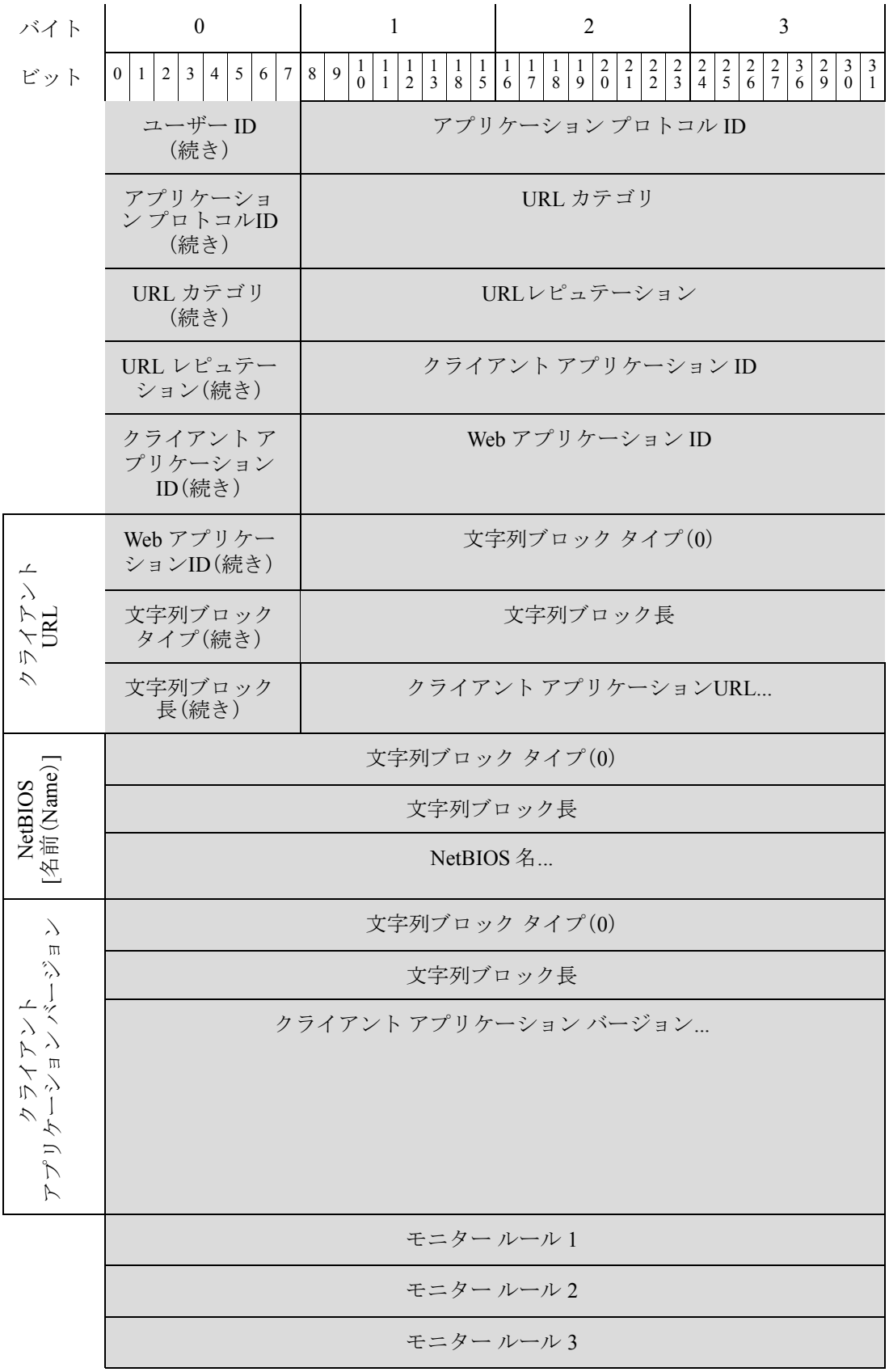
次の図は、接続統計データ ブロック 7.0 の形式を示しています。

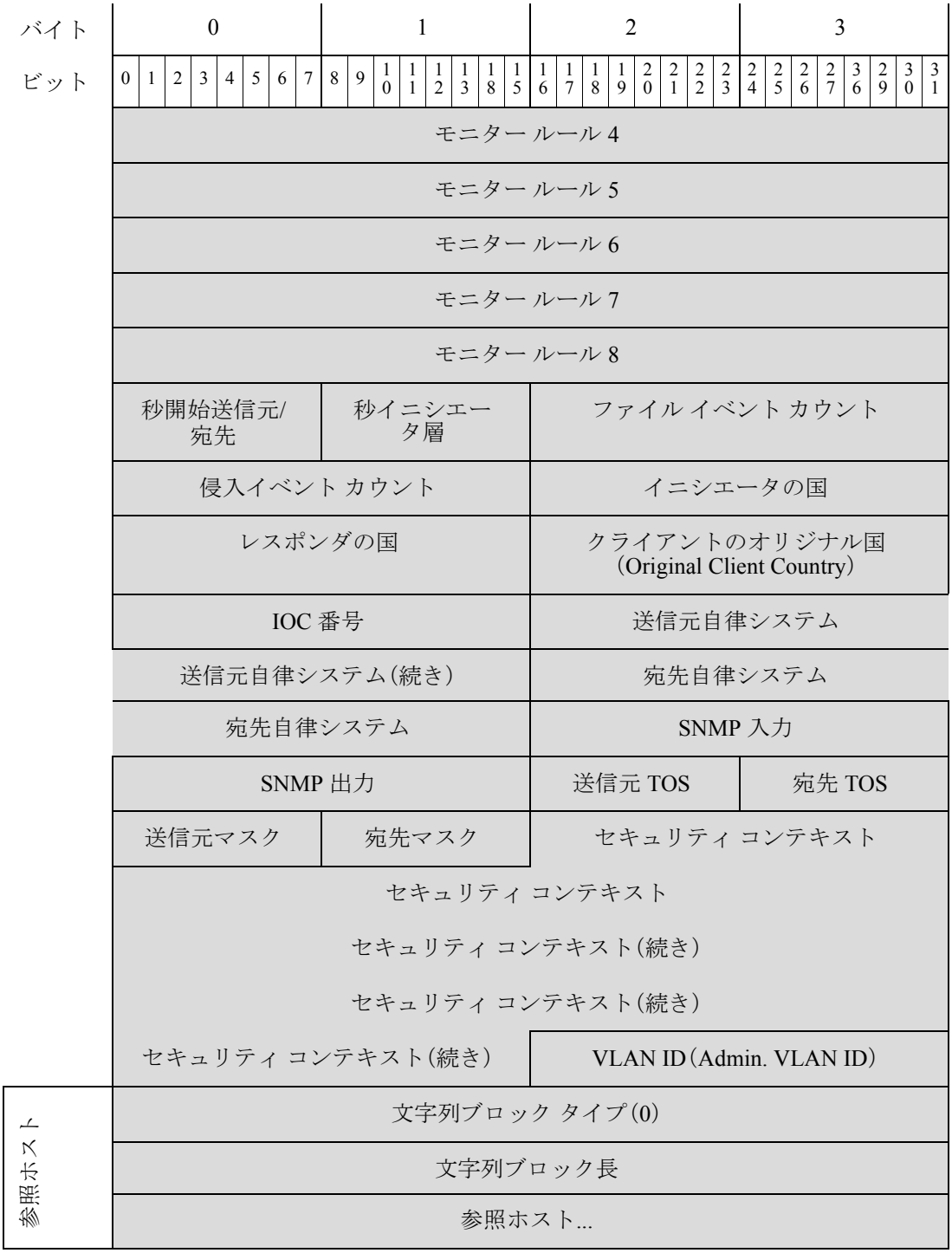


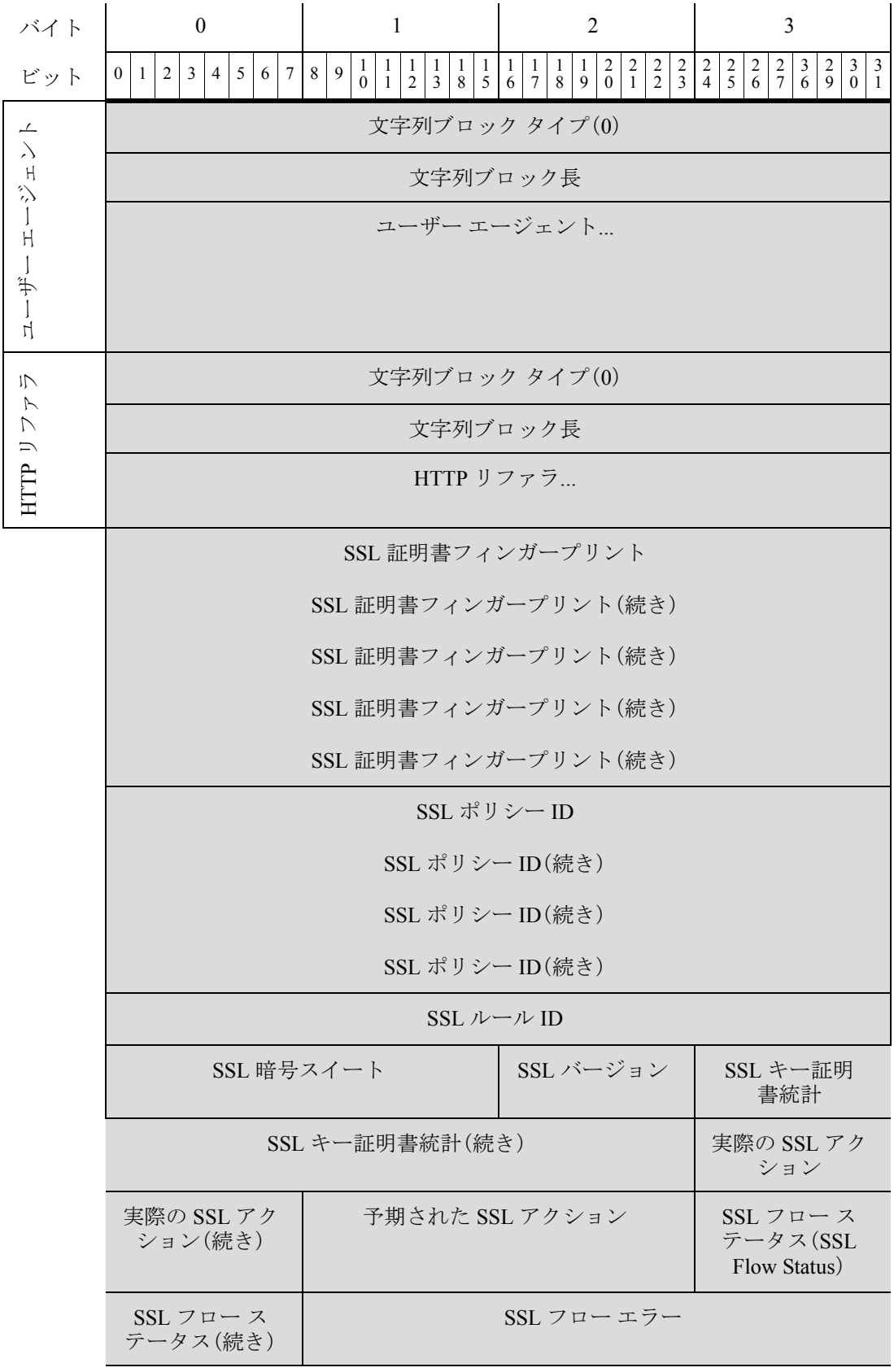
バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
入力ゾーン（続き）																																
入力ゾーン（続き）																																
出力ゾーン																																
出力ゾーン（続き）																																
出力ゾーン（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）																																
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）																																

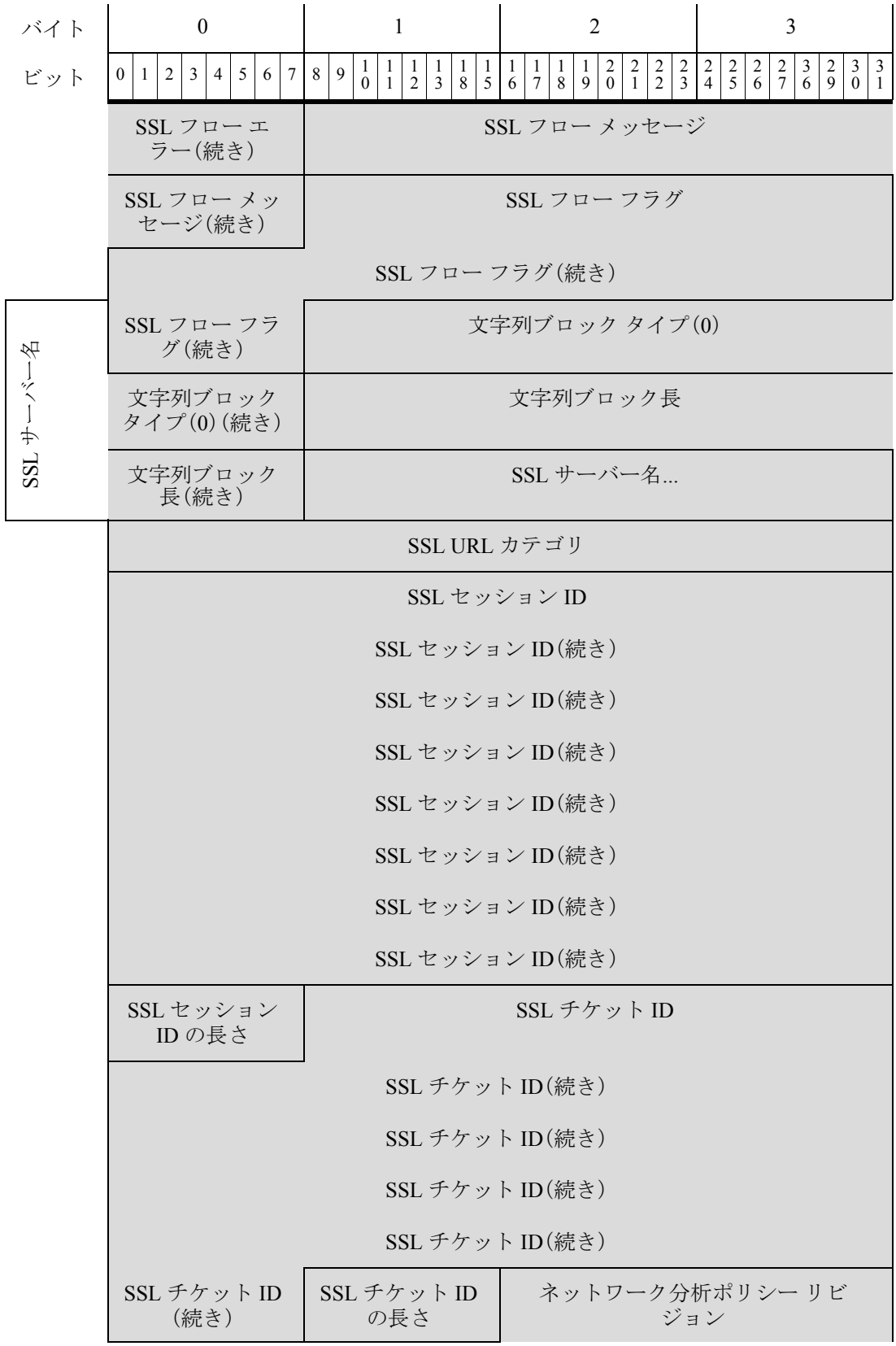

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
オリジナル クライアント IP アドレス(続き)
ポリシー リビジョン
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ポリシー リビジョン(続き)
ルール ID
トンネル ルール ID
ルール アクション
ルールの理由
ルールの理由(続き)
イニシエータ ポート
レスポンダ ポート
TCP フラグ
プロトコル
NetFlow ソース
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
NetFlow ソース(続き)
インスタンス ID(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)
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)


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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）
レスポンダ送信パケット数
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)
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)
ユーザー ID(User 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 18 15
16 17 18 19 20 21 22 23
24 25 26 27 36 29 30 31
ユーザー 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 [名前（Name）]
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...
モニター ルール 1
モニター ルール 2
モニター 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
モニター ルール 4
モニター ルール 5
モニター ルール 6
モニター ルール 7
モニター 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
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（Admin. 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...


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
ユーザー 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
ユーザー 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
実際の SSL アクション(続き)
予期された SSL アクション
SSL フロー ステータス(SSL Flow Status)
SSL フロー ステータス(続き)
SSL フロー エラー


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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 サーバー名
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 サーバー名...
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


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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
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)
送信元セキュリティグループタグ
Src. 秒グループ タグタイプ
宛先セキュリティグループタグ
宛先の秒グループタグタイプ
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)
HTTP レスポンス
DNS クエリ (DNS Query)
文字列ブロック タイプ(0)
文字列ブロック長
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)

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	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																															
	脅威インテリジェンスカテゴリ																															
入力 VRF	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	入力 VRF 名																															
出力 VRF	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	出力 VRF 名																															
送信元属性	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	送信元 IP の動的属性																															
着信属性	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	宛先 IP の動的属性																															

次の表は、接続統計データ ブロック 7.0 のフィールドについての説明です。

表 B-46　　接続統計データ ブロック 7.0 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	7.0+ の接続統計データ ブロックを開始します。値は常に 173 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（Device 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-46　接続統計データ ブロック 7.0 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。
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	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	uint16	そのルールに対してユーザー 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（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。
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。

表 B-46　接続統計データ ブロック 7.0 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。
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）。
ユーザー ID（User ID）	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 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 B-46　接続統計データ ブロック 7.0 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。
モニター ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニター ルールの ID。
モニター ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニター ルールの ID。
モニター ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニター ルールの ID。
モニター ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニター ルールの ID。
モニター ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニター ルールの ID。
モニター ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニター ルールの ID。
モニター ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニター ルールの ID。
モニター ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニター 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 アドレスが IP ブロックリストに一致しているかどうか。
セキュリティ インテリジェンス層	uint8	IP ブロ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。
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。

表 B-46　接続統計データ ブロック 7.0 のフィールド（続き）

フィールド	データタイプ	説明
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（Admin. 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	ユーザー 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	ユーザー 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、およびユーザー エージェント フィールドのバイト数を含む）。
ユーザー エージェント	string	セッションのユーザー 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 サーバー証明書の 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-46　接続統計データ ブロック 7.0 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.xhtm1 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 サーバー証明書ステータス	uint32	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）：サーバー証明書のステータスは評価されませんでした。 • 1（不明）：サーバー証明書のステータスは判別できませんでした。 • 2（有効）：サーバー証明書は有効です。 • 4（自己署名済み）：サーバー証明書は自己署名です。 • 16（無効な発行者）：サーバー証明書に無効な発行者があります。 • 32（無効な署名）：サーバー証明書に無効な署名があります。 • 64（期限切れ）：サーバー証明書は期限切れです。 • 128（まだ有効でない）：サーバー証明書はまだ有効ではありません。 • 256（取り消し）：サーバー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-46　接続統計データ ブロック 7.0 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-46　接続統計データ ブロック 7.0 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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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-46　接続統計データ ブロック 7.0 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ー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。

表 B-46　接続統計データ ブロック 7.0 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	SSL サーバー名文字列データ 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 サーバー名フィールドのバイト数を含む)。
SSL サーバー名	string	SSL Client Hello でサーバー名に指定された名前。
SSL URL カテゴリ	uint32	サーバー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ー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ーがセッション 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 によりユーザーに割り当てられた ID 番号。
送信元セキュリティグループタグ	uint16	接続の送信元のセキュリティグループタグ。
送信元セキュリティ グループ タグ タイプ	uint8	送信元セキュリティグループタグの割り当て方法: • 0:不明 • 1:インライン • 2:セッションディレクトリ • 3:Security Group Tag Exchange Protocol(SXP)
宛先セキュリティグループタグ	uint16	接続の宛先のセキュリティグループタグ。
宛先セキュリティ グループ タグ タイプ	uint8	宛先セキュリティグループタグの割り当て方法: • 0:不明 • 1:インライン • 2:セッションディレクトリ • 3:Security Group Tag Exchange Protocol(SXP)
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。

表 B-46　接続統計データ ブロック 7.0 のフィールド（続き）

フィールド	データタイプ	説明
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 サーバー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。
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。接続に関連付けられた 3 つのセキュリティ インテリジェンス リストが存在する場合があります。
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。接続に関連付けられた 3 つのセキュリティ インテリジェンス リストが存在する場合があります。
脅威インテリジェンスカテゴリ	uint32	イベントに関連付けられた脅威インテリジェンスカテゴリ。これは、関連メタデータの脅威インテリジェンスリストにマップされます。
文字列ブロックタイプ	uint32	入力 VRF 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。ブロックタイプとヘッダーフィールドの 8 バイト、および入力 VRF 名フィールドのバイト数が含まれています。
入力 VRF 名	文字列	トラフィックがネットワークに入るときに通過する仮想ルータ。
文字列ブロックタイプ	uint32	出力 VRF 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。ブロックタイプとヘッダーフィールドの 8 バイト、および出力 VRF 名フィールドのバイト数が含まれています。

表 B-46　接続統計データ ブロック 7.0 のフィールド（続き）

フィールド	データタイプ	説明
出力 VRF 名	文字列	トラフィックがネットワークから出るときに通過する仮想ルータの名前。
文字列ブロック タイプ	uint32	送信元 IP の動的属性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。ブロックタイプとヘッダーフィールドの 8 バイト、および送信元 IP の動的属性フィールドのバイト数が含まれています。
送信元 IP の動的属性	文字列	送信元 IP アドレスに関連付けられた動的属性。
文字列ブロック タイプ	uint32	宛先 IP の動的属性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。ブロックタイプとヘッダーフィールドの 8 バイト、および宛先 IP の動的属性フィールドのバイト数が含まれています。
宛先 IP の動的属性	文字列	宛先 IP アドレスに関連付けられた動的属性。

レガシー ファイル イベントのデータ構造

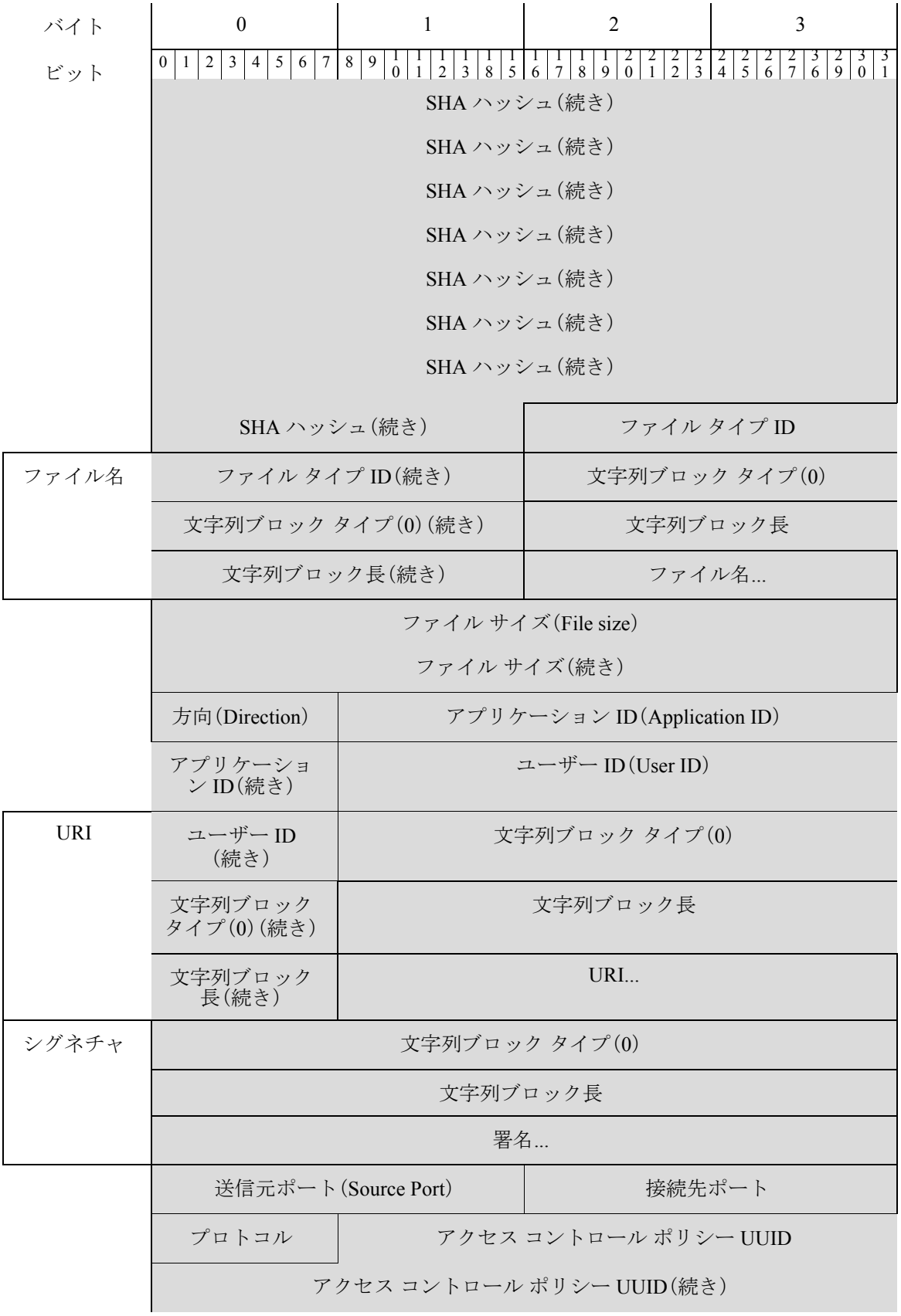
続くいくつかのトピックでは、他のレガシー ファイル イベント データの構造について説明します。

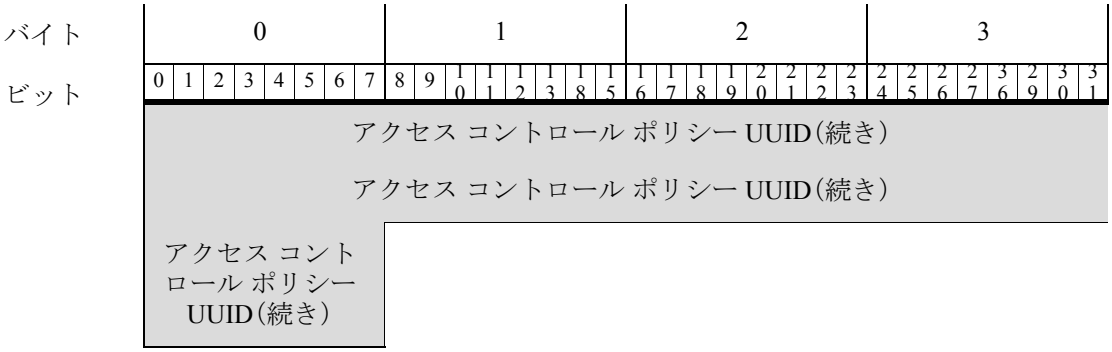
- ファイル イベント 5.1.1.x（B-314 ページ）
- ファイル イベント 5.2.x（B-318 ページ）
- ファイル イベント 5.3（B-322 ページ）
- ファイル イベント 5.3.1（B-329 ページ）
- ファイル イベント 5.4.x（B-335 ページ）
- ファイル イベント SHA ハッシュ 5.1.1 ～ 5.2.x（B-357 ページ）

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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 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（File size）
ファイル サイズ（続き）
方向（Direction）
アプリケーション ID（Application ID）
アプリケーション ID（続き）
ユーザー ID（User ID）
URI
ユーザー 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（Source Port）
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）



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-47　　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）。
Device 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。

表 B-47　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：マルウェア許可リスト
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（File size）	uint64	ファイルのサイズ（バイト単位）。
方向（Direction）	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（Application 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。
ユーザー ID（User 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ーの 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。

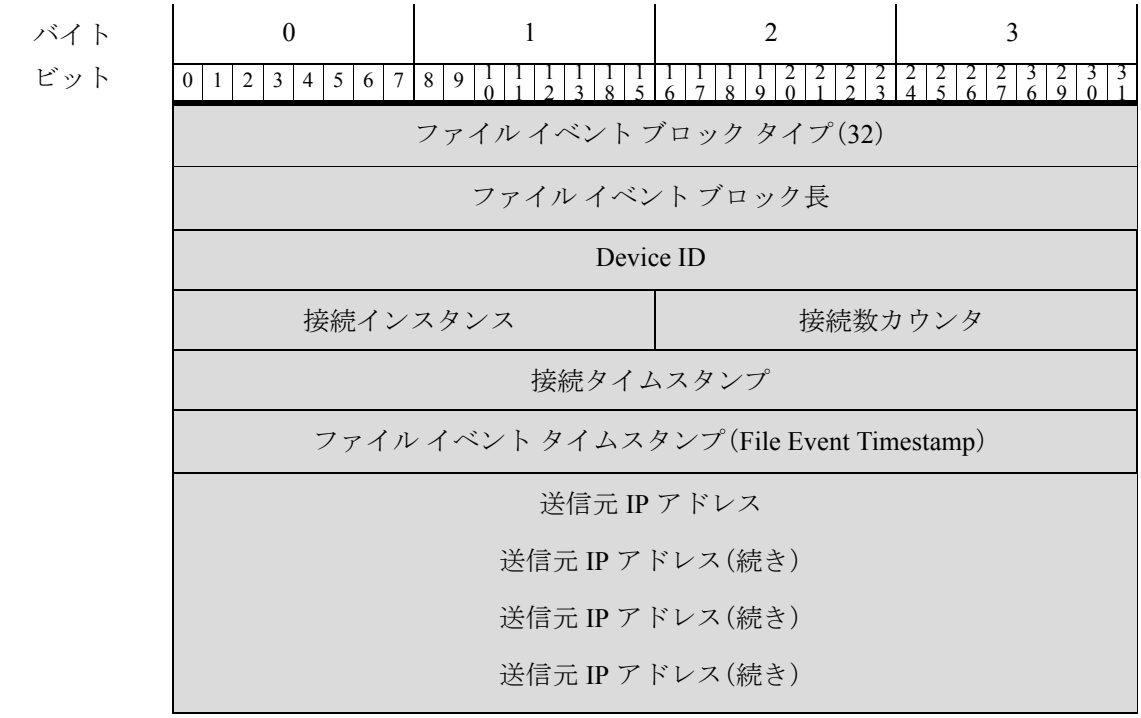
表 B-47　　ファイル イベント データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
プロトコル	uint8	ユーザーが指定した 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。

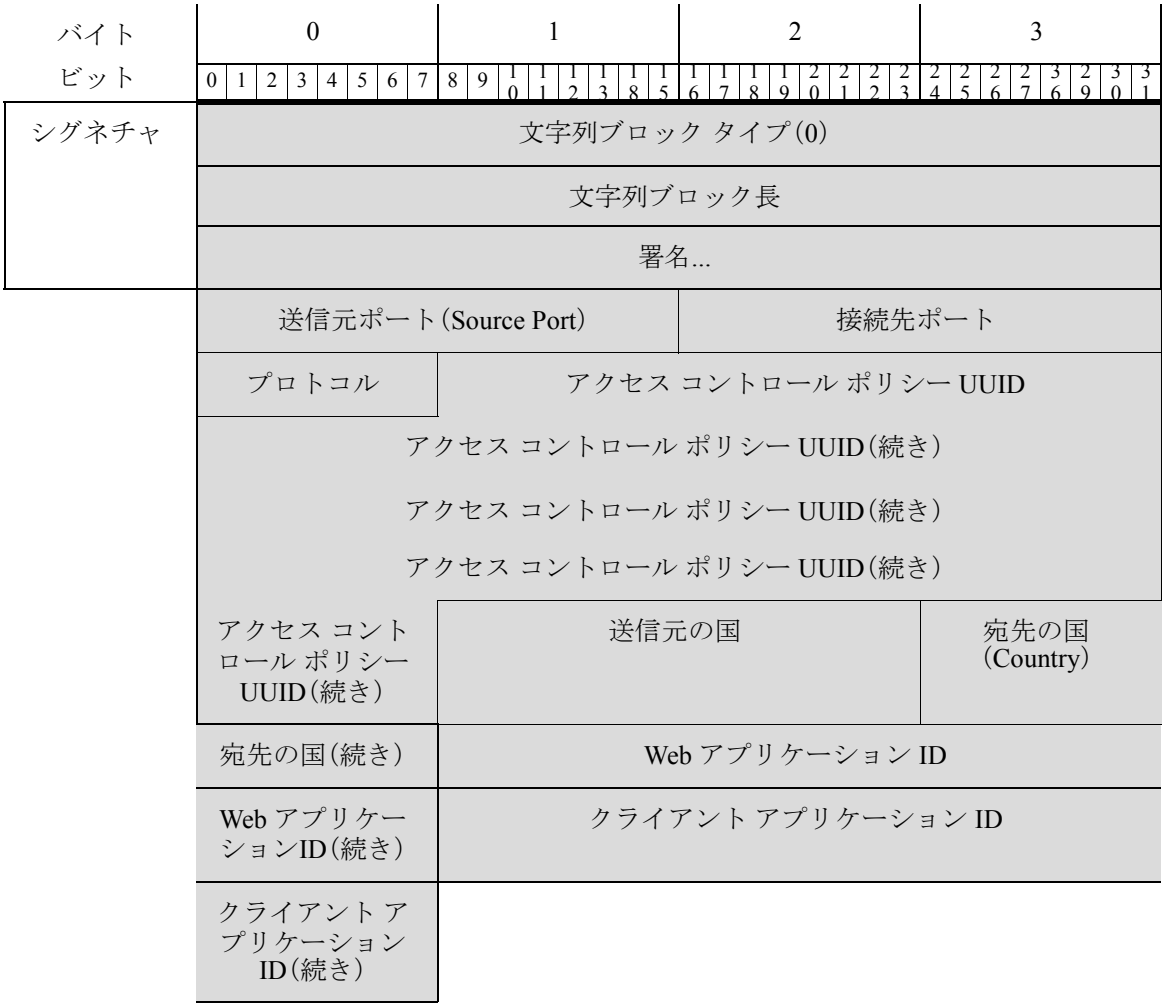
ファイル イベント 5.2.x

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 18 15	16 17 18 19 20 21 22 23	24 25 26 27 36 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（File size）			
	ファイル サイズ（続き）			
	方向（Direction）	アプリケーション ID（Application ID）		
	アプリケーション ID（続き）	ユーザー ID（User ID）		
URI	ユーザー 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...		



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-48　　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)。
Device 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-48　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（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（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：マルウェア許可リスト
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（File size）	uint64	ファイルのサイズ（バイト単位）。
方向（Direction）	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）。

表 B-48　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
アプリケーション ID（Application 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。
ユーザー ID（User 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ーの 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	ユーザーが指定した 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

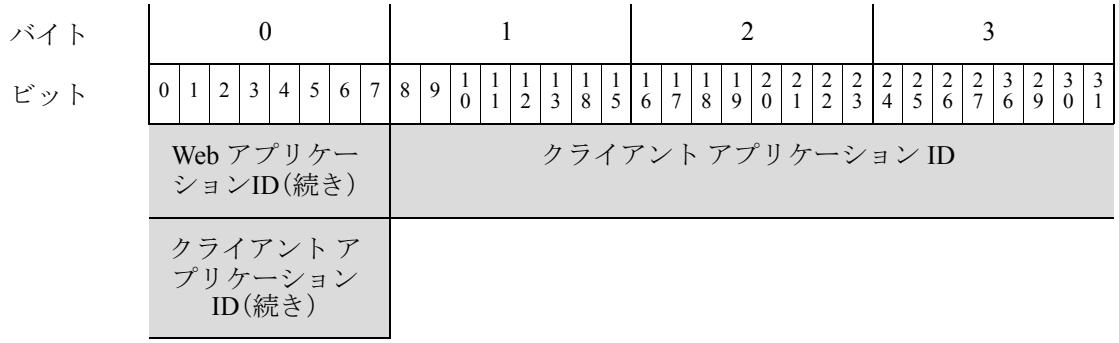
ファイル イベントには、ネットワークを介して送信されるファイルに関する情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントのブロック タイプは、シリーズ 2 グループのブロックの、ブロック タイプ 38 です。これはブロック タイプ 32 に取って代わります。新しいフィールドは、ダイナミック ファイル分析とファイル ストレージを追跡するために追加されました。

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（2-15 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ファイル イベント ブロック タイプ(38)																																
ファイル イベント ブロック長																																
Device 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(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							
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)																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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（File size）
ファイル サイズ（続き）
方向（Direction）
アプリケーション ID（Application ID）
アプリケーション ID（続き）
ユーザー ID（User ID）
URI
ユーザー 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（Source Port）
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（Country）
宛先の国（続き）
Web アプリケーション ID



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-49　　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)。
Device 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。

表 B-49　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（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）：ファイルがユーザー定義のハッシュと一致するため、ユーザー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-49　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:マルウェア許可リスト
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-49　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、エンドポイント向け AMP 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（File size）	uint64	ファイルのサイズ（バイト単位）。
方向（Direction）	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（Application 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。
ユーザー ID（User 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ーの 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	ユーザーが指定した 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

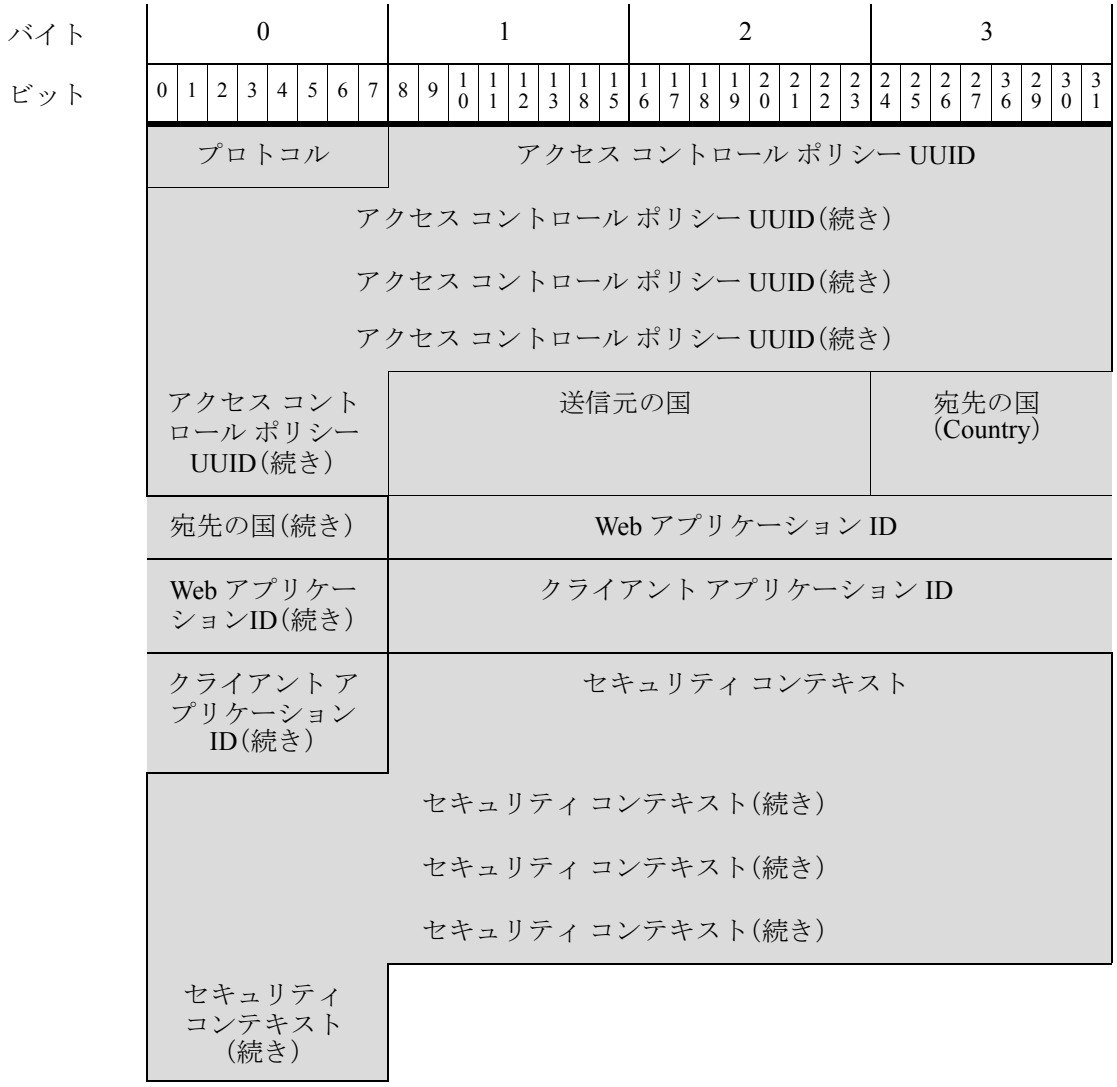
ファイル イベントには、ネットワークを介して送信されるファイルに関する情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントのブロック タイプは、シリーズ 2 グループのブロックの、ブロック タイプ 43 です。これはブロック タイプ 38 に取って代わります。セキュリティ コンテキスト フィールドが追加されました。

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（2-15 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（Device 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（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							
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							


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
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（File size）
ファイル サイズ（続き）
方向（Direction）
アプリケーション ID（Application ID）
アプリケーション ID（続き）
ユーザー ID（User ID）
URI
ユーザー 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（Source Port）
接続先ポート



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-50　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 (Device 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。

表 B-50　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 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）：ファイルがユーザー定義のハッシュと一致するため、ユーザー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-50　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ー制限超過によるキャパシティの処理):サーバー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-50　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：マルウェア許可リスト
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、エンドポイント向け AMP 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（File size）	uint64	ファイルのサイズ（バイト単位）。
方向（Direction）	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（Application 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。
ユーザー ID（User 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ーの 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-50　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	ユーザーが指定した 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

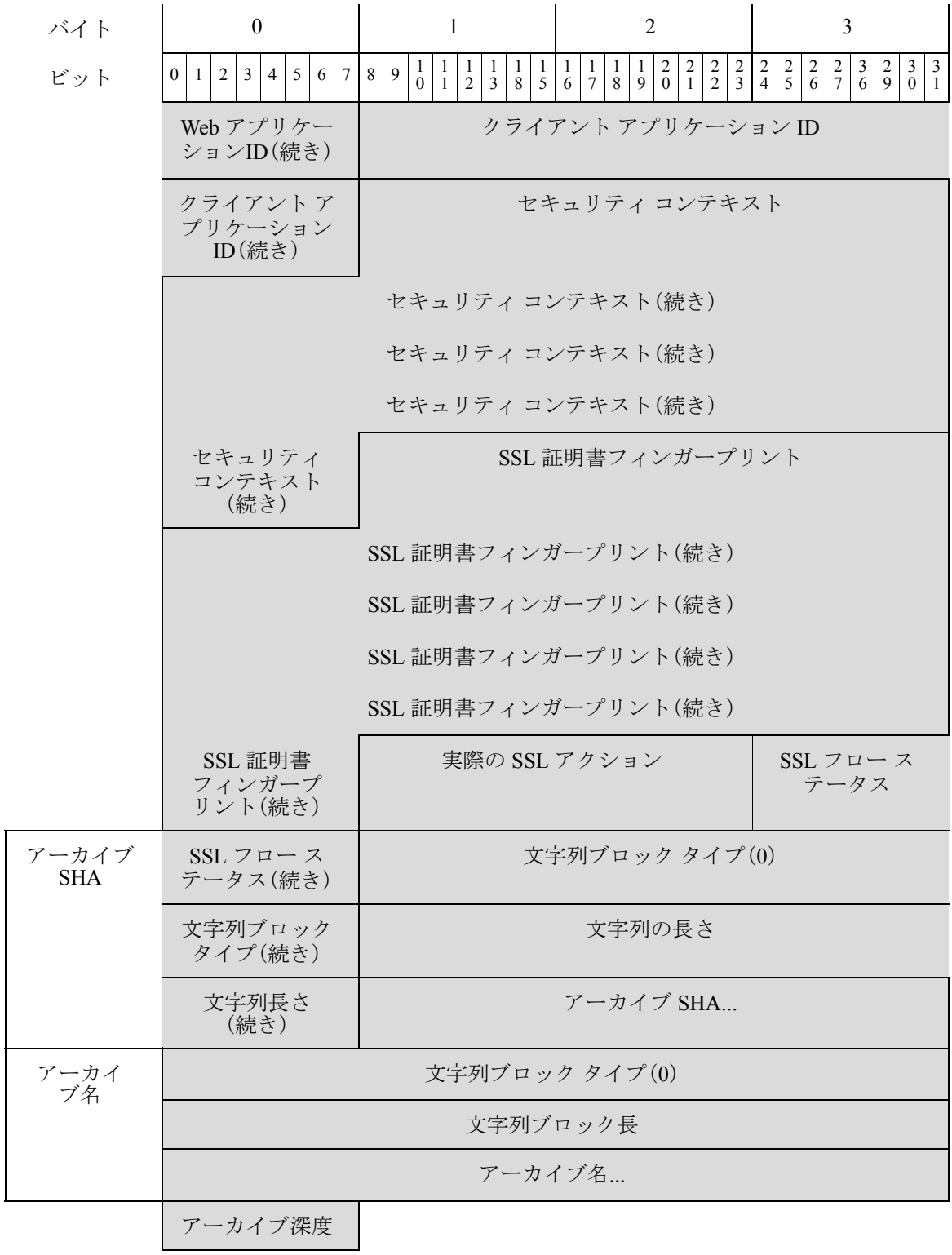
ファイル イベントには、ネットワークを介して送信されるファイルに関する情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントのブロック タイプは、シリーズ 2 グループのブロックの、ブロック タイプ 46 です。これはブロック タイプ 43 に取って代わります。SSL とファイル アーカイブ サポート用のフィールドが追加されました。

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（2-15 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ファイル イベント ブロック タイプ(46)																																
ファイル イベント ブロック長																																
デバイスID（Device 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(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							
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)																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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（File size）
ファイル サイズ（続き）
方向（Direction）
アプリケーション ID（Application ID）
アプリケーション ID（続き）
ユーザー ID（User ID）
URI
ユーザー 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（Source Port）
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（Country）
宛先の国（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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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)
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-51　　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（Device 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 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）：ファイルがユーザー定義のハッシュと一致するため、ユーザー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-51　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-51　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-51　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:マルウェア許可リスト • 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、エンドポイント向け AMP 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-51　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（File size）	uint64	ファイルのサイズ（バイト単位）。
方向（Direction）	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（Application 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。
ユーザー ID（User 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ーの 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	ユーザーが指定した 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 サーバー証明書の SHA1 ハッシュ。

表 B-51　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-51　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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー証明書の検証エラー」 • 28:「無効な操作」

表 B-51　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）

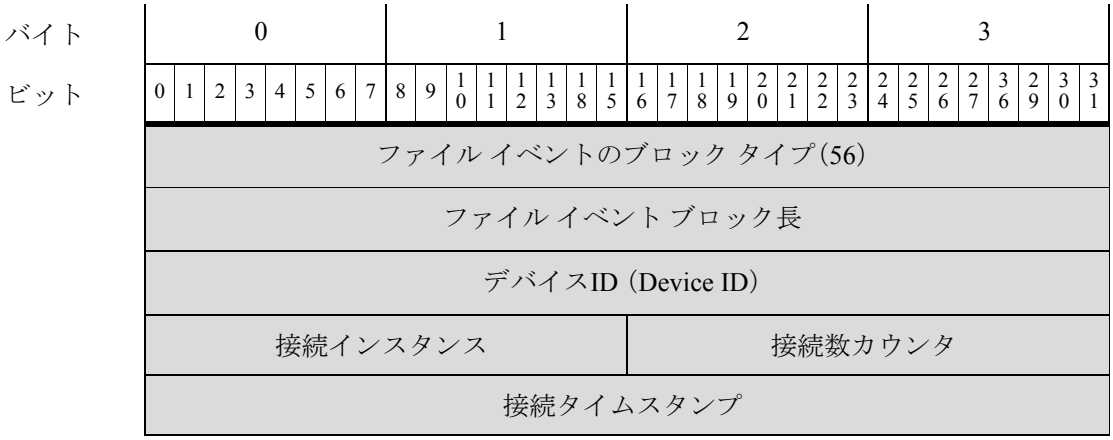
フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	アーカイブ SHA を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	アーカイブ SHA 文字列データ ブロックに含まれるバイト数（ブロック タイプとヘッダー フィールド用の 8 バイト、および侵入ポリシー名のバイト数を含む）。
アーカイブ SHA	string	ファイルが含まれる親アーカイブの SHA1 ハッシュ。
文字列ブロック タイプ	uint32	アーカイブ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	アーカイブ名文字列データ 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。

6.x 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、ブロックタイプ 79 により取って代わられます。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。

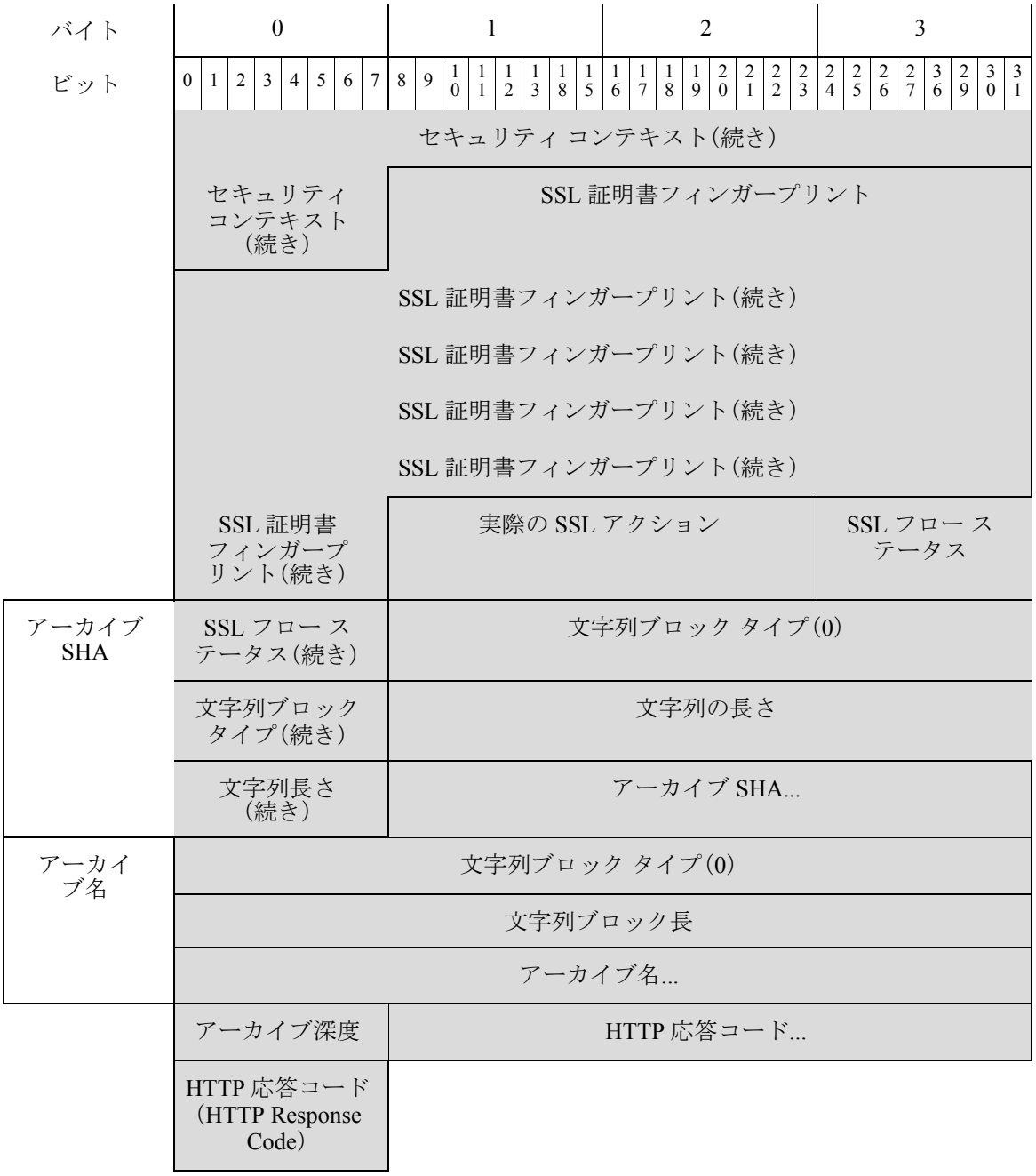
ファイル イベント レコードを要求するには、イベント バージョン 5 およびイベント コード 111 の要求メッセージ内に、ファイル イベント フラグ（要求フラグ フィールドのビット 30）を設定します。要求フラグ（2-15 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	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																															
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 サイズ(File size)																															
	ファイル サイズ(続き)																															
	方向(Direction)								アプリケーション ID(Application ID)																							
	アプリケーション ID(続き)								ユーザー ID(User ID)																							
URI	ユーザー 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(Source Port)																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(Country)							
	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)								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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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
HTTP 応答コード...
HTTP 応答コード(HTTP Response Code)

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-52　ファイル イベント データ ブロック 6.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 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（Device 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 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 AMP クラウド サービスが要求に応答しなかった。 • 5（CUSTOM SIGNATURE）：ファイルがユーザー定義のハッシュと一致するため、ユーザー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-52　ファイル イベント データ ブロック 6.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-52　ファイル イベント データ ブロック 6.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(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ー制限超過によるキャパシティの処理):サーバー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-52　ファイル イベント データ ブロック 6.x のフィールド（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:マルウェア許可リスト • 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、エンドポイント向け AMP 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-52　ファイル イベント データ ブロック 6.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（File size）	uint64	ファイルのサイズ（バイト単位）。
方向（Direction）	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（Application 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。
ユーザー ID（User 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ーの 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	ユーザーが指定した 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。

表 B-52　ファイル イベント データ ブロック 6.x のフィールド（続き）

フィールド	データタイプ	説明
SSL 証明書フィンガープリント	uint8[20]	SSL サーバー証明書の 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-52　ファイル イベント データ ブロック 6.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:「保留中のサーバー名カテゴリ 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:「無効なサーバーの証明書の処理」 • 16:「サーバー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:「サーバー証明書の検証が使用できません」 • 27:「サーバー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。

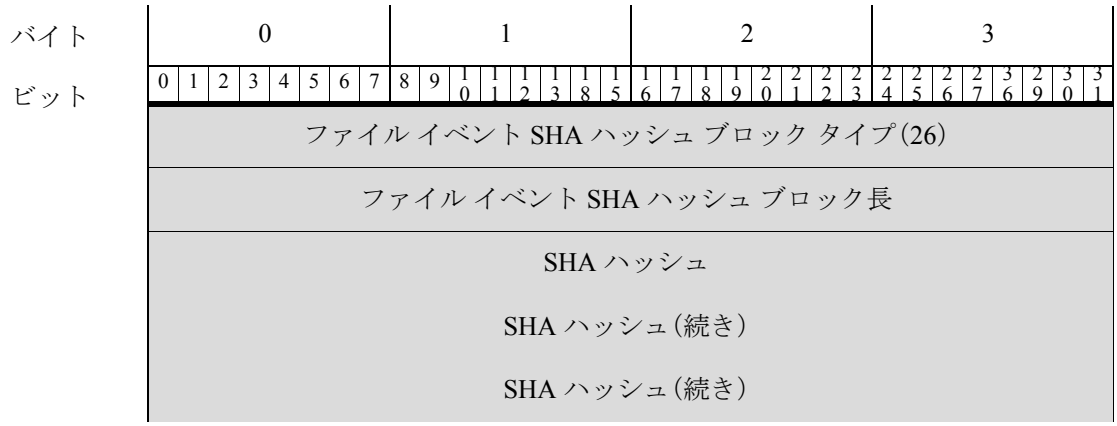
表 B-52　ファイル イベント データ ブロック 6.x のフィールド（続き）

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。
HTTP 応答コード（HTTP Response Code）	uint32	HTTP 応答コード（HTTP Response Code）

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。



	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-53　　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-359 ページ）
- 相関イベント 5.1 ～ 5.3.x（B-367 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、ユーザー 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（4-65 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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																																
Device ID																																
（相関）イベント秒																																
イベント ID（Event ID）																																
ポリシー ID																																
ルール ID																																
[プライオリティ（Priority）]																																


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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 (Event Type)
イベント Device 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(Event 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
送信元重要度 (続き)
送信元ユーザー ID
送信元ユーザー ID(続き)
送信元ポート
送信元サーバー ID
送信元サーバー ID(続き)
宛先 IP (Destination IP)
宛先 IP(続き)
着信ホスト タイプ
イベント説明
送信元 OS フィンガープリント 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
着信VLAN ID（Admin. 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
着信ユーザー ID（User ID）
接続先ポート
宛先サーバー ID
宛先サーバー 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）

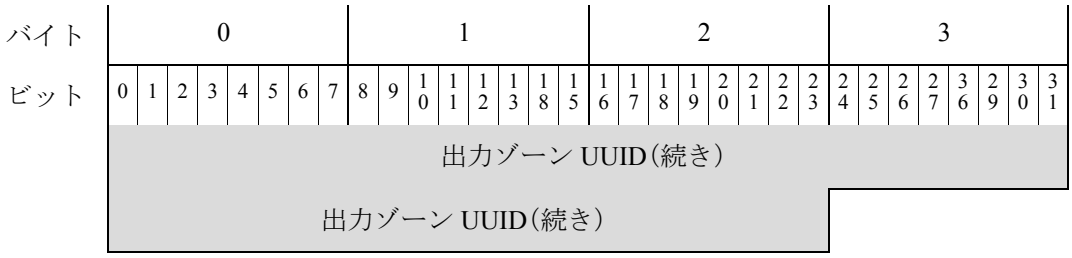


表 B-54　　相関イベント データ 5.0 ～ 5.0.2 のフィールド

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（4-65 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）。
Device 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Device 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（Event 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、サービス 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、サービス 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（Priority）]	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（4-75 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。

表 B-54　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 タイプ（Event Type）	uint8	相関イベントが、侵入、ホスト検出、またはユーザー 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：ユーザー
イベント Device 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Device 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 Cisco Secure Firewall 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（Event 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-55（B-366 ページ）を参照してください。

表 B-54　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ー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ーを実行しているか（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ー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）。Cisco Secure Firewall 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。

表 B-54　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、サービス 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、ユーザー定義の重要度値: • 0:なし • 1:低 • 2:中 • 3:高
送信元ユーザー 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ーの ID 番号。
送信元ポート	uint16	イベントの送信元ポート。
送信元サーバー ID	uint32	送信元ホスト上で実行するサーバーの 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、サービス 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、ユーザー定義の重要度値: • 0:なし • 1:低 • 2:中 • 3:高

表 B-54　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
宛先ユーザー 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ーの 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ーの 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。

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-55　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
送信元サーバー	0x00000200
宛先 IP（Destination IP）	0x00000400
宛先ホスト タイプ	0x00000800

表 B-55　　イベントで定義された値（続き）

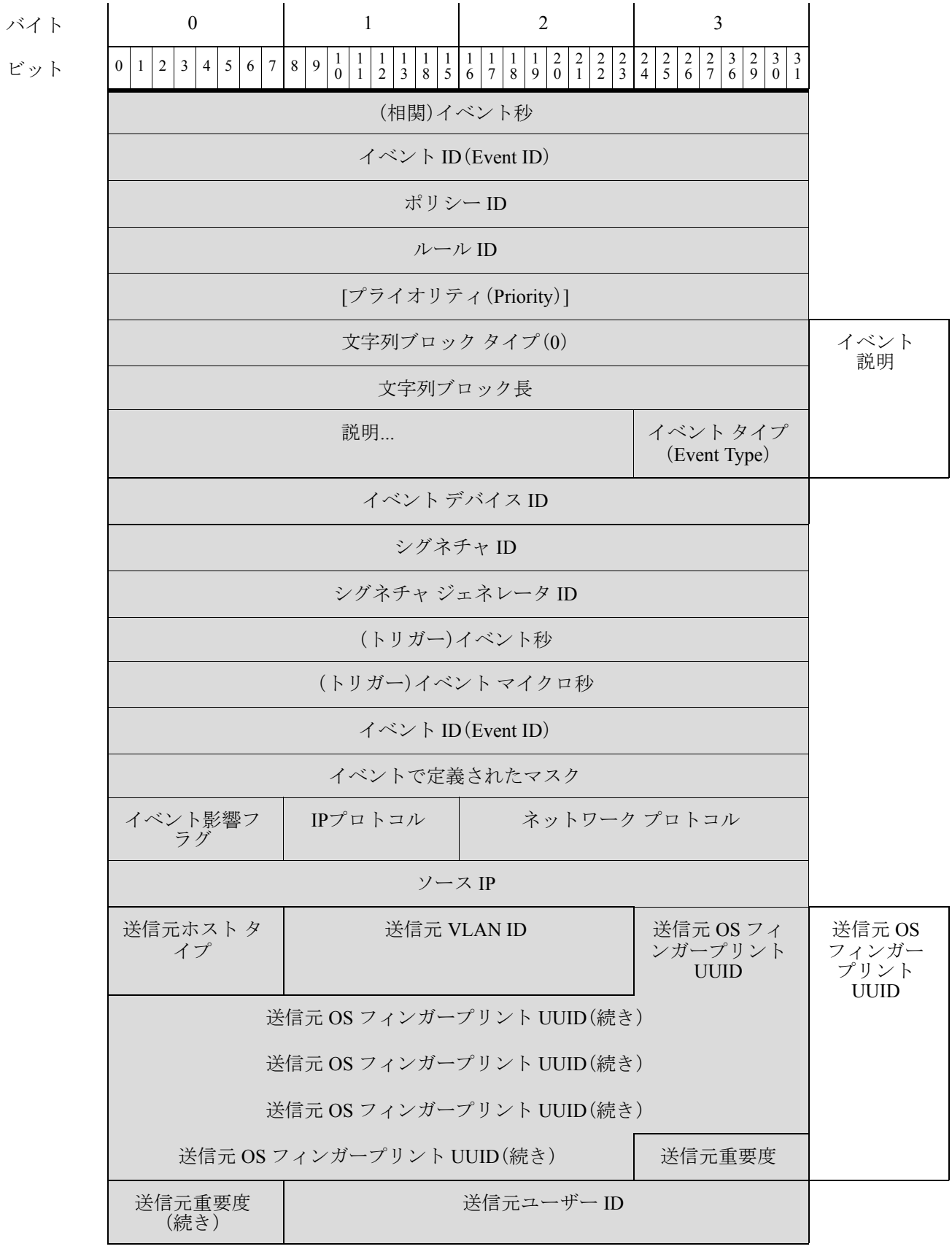
説明	マスク値
宛先 VLAN ID	0x00001000
宛先フィンガープリント ID	0x00002000
宛先重要度	0x00004000
接続先ポート	0x00008000
宛先サーバー	0x00010000
送信元ユーザー	0x00020000
宛先ユーザー	0x00040000

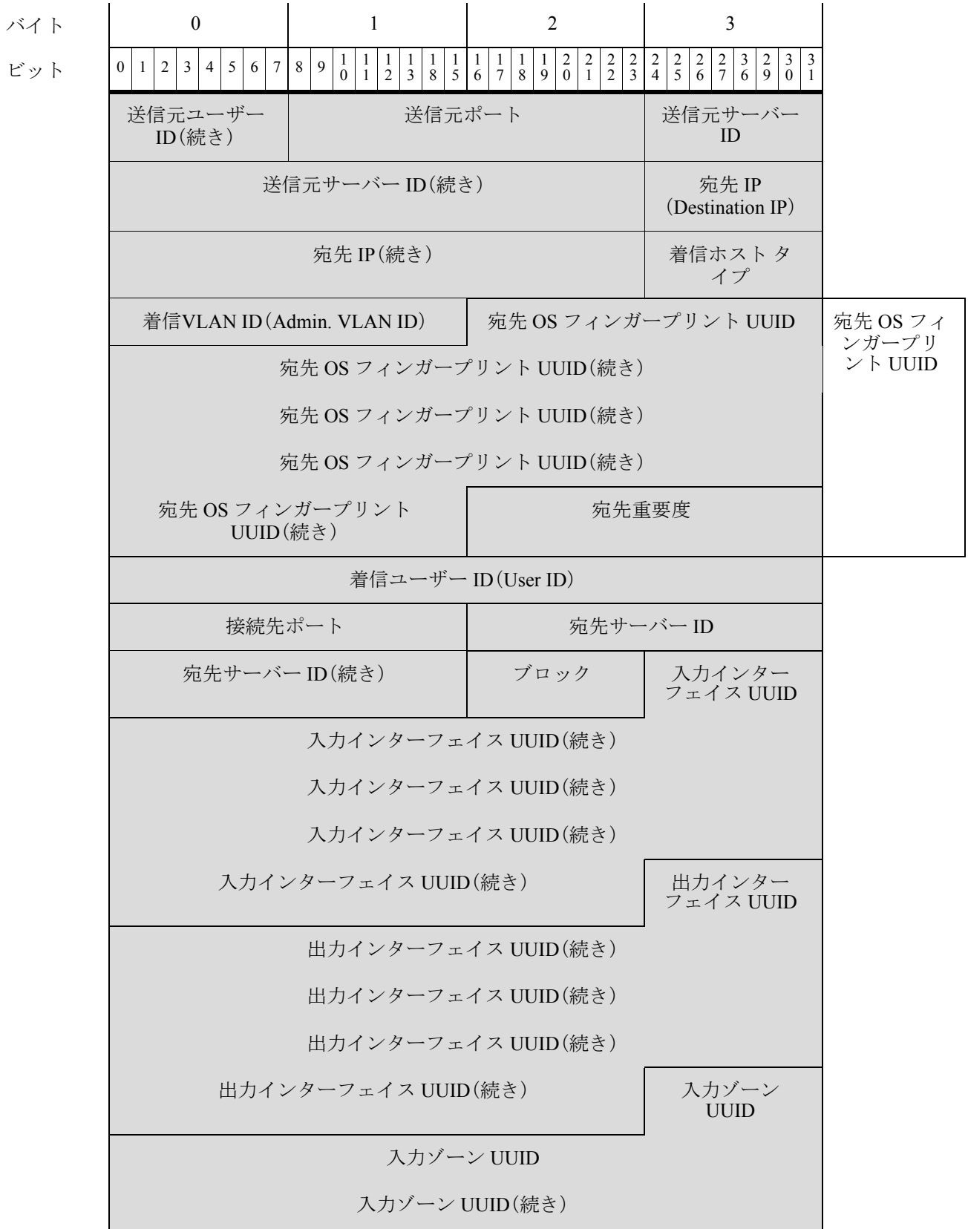
相関イベント 5.1 ～ 5.3.x

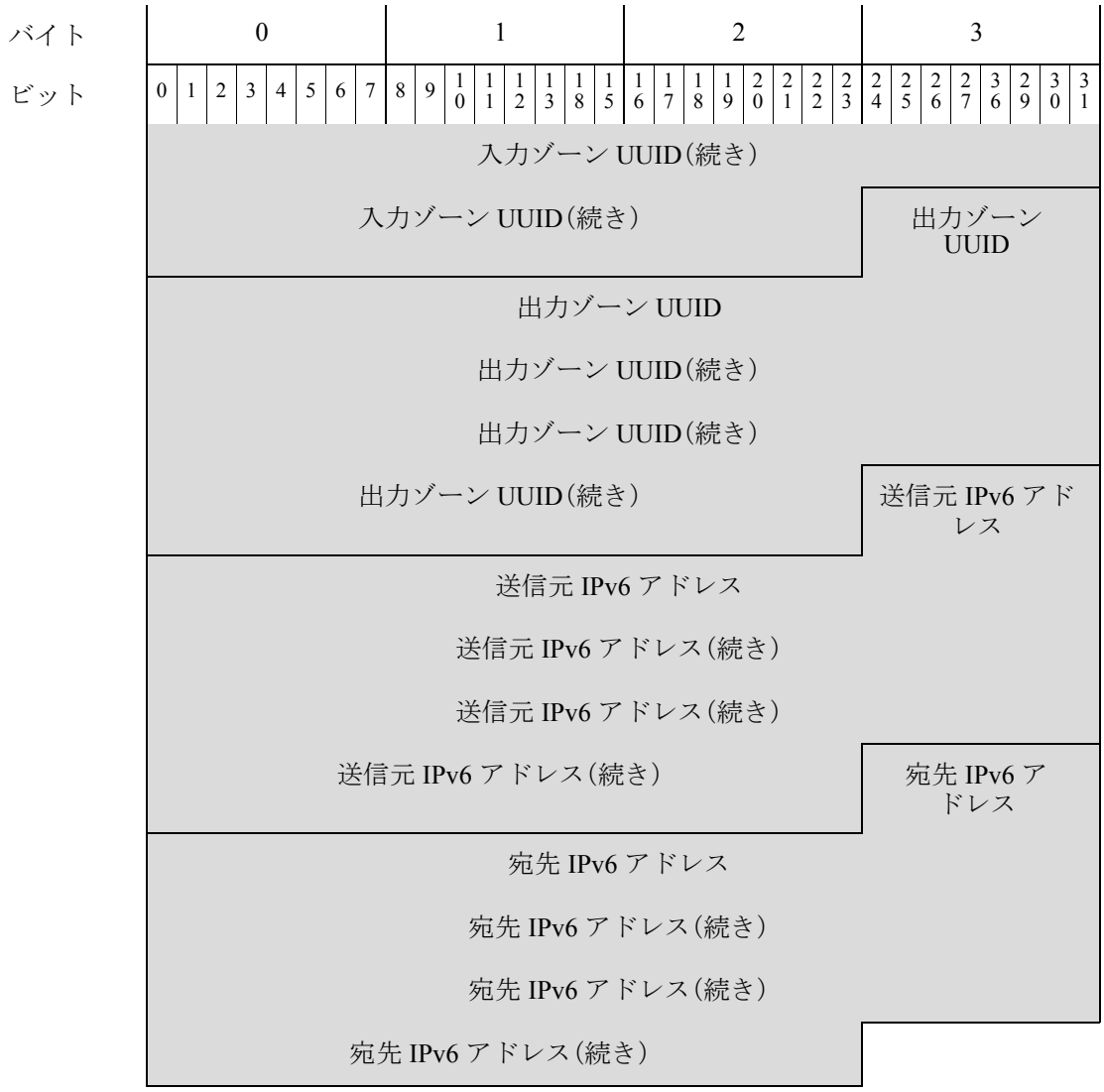
相関イベント（5.0 よりも前のバージョンではコンプライアンス イベントと呼ばれていた）には、相関ポリシー違反に関する情報が含まれます。このメッセージは、標準 eStreamer メッセージ ヘッダーを使用し、レコード タイプ 112 を指定し、それにシリーズ 1 セットのデータ ブロックの相関データ ブロック タイプ 128 が続きます。データ ブロック タイプ 128 は、IPv6 サポートが含まれるという点で、その先行するもの（ブロック タイプ 116）とは異なります。

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、ユーザー 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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 サーバー 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（Device 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
(相関)イベント秒
イベント ID(Event ID)
ポリシー ID
ルール ID
[プライオリティ(Priority)]
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 (Event Type)
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(Event 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
送信元ユーザー ID（続き）
送信元ポート
送信元サーバー ID
送信元サーバー ID（続き）
宛先 IP（Destination IP）
宛先 IP（続き）
着信ホスト タイプ
着信VLAN ID（Admin. 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
着信ユーザー ID（User ID）
接続先ポート
宛先サーバー ID
宛先サーバー 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）



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（4-65 ページ）を参照してください。

表 B-56　　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（4-65 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）。

表 B-56　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
デバイスID（Device 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Device 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（Event 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、サービス 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、サービス 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(Priority)]	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 (4-75 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(Event Type)	uint8	相関イベントが、侵入、ホスト検出、またはユーザー 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:ユーザー
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Device 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 Cisco Secure Firewall 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)。

表 B-56　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
(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（Event 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-55(B-366 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ー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ーを実行しているか(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ー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)。Cisco Secure Firewall 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`

表 B-56　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
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（1-4 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、サービス 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、ユーザー定義の重要度値: • 0:なし • 1:低 • 2:中 • 3:高
送信元ユーザー 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ーの ID 番号。
送信元ポート	uint16	イベントの送信元ポート。
送信元サーバー ID	uint32	送信元ホスト上で実行するサーバーの 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（1-4 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）。

表 B-56　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 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、サービス 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、ユーザー定義の重要度値: • 0:なし • 1:低 • 2:中 • 3:高
宛先ユーザー 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ーの 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ーの 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(2-30 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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（IP Address）]																																
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																							

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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																															
サーバー 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 サーバー 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																															
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																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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																															
ユーザー（User）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 ユーザー 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（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																															
Application 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…																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
(TCP) 全サーバー データ	リスト ブロック タイプ (11)…																															
	リスト ブロック長…																															
	(TCP) 全サーバー データ ブロック (104)*																															
(UDP) 全サーバー データ	リスト ブロック タイプ (11)																															
	リスト ブロック長																															
	(UDP) 全サーバー 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 (Transport) 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 (Admin. 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 [名前 (Name)]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	NetBIOS 名文字列																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
注記(Notes)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)*																															
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(Attribute)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-57　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	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-57　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 システムから取得したフィンガープリント データ ブロック*	変数（variable）	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+（4-172 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	サーバー 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	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（サーバー フィンガープリント）データ ブロック*	変数（variable）	サーバー 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+（4-172 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	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（variable）	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+（4-172 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	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-57　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 1)データ ブロック*	変数(variable)	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+(4-172 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	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 2)データ ブロック*	変数(variable)	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+(4-172 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	ユーザー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	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(ユーザー フィンガープリント)データ ブロック*	変数(variable)	ユーザー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+(4-172 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	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-57　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（スキャン フィンガープリント）データ ブロック*	変数（variable）	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+（4-172 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	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（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（variable）	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+（4-172 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	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（variable）	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+（4-172 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ー 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ー データ ブロック長から成る 8 バイトを含みます。
（TCP）全サーバー データ ブロック*	変数（variable）	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ー 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 サーバー データ ブロック 4.10.0+（4-151 ページ）を参照してください。

表 B-57　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 タイプ	uint32	UDP サービス データを伝送する全サーバー 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ー データ ブロック長から成る 8 バイトを含みます。
(UDP) 全サーバー データ ブロック*	変数（variable）	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ー 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 サーバー データ ブロック 4.10.0+（4-151 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（variable）	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 ブロックの説明の詳細については、プロトコル データ ブロック（4-80 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。
(トランスポート) プロトコル データ ブロック*	変数（variable）	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 ブロックの説明の詳細については、プロトコル データ ブロック（4-80 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（variable）	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+（4-122 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 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。

表 B-57　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
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（Admin. 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（variable）	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+（4-165 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。
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（Notes）	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。

表 B-57　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
(VDB) ホスト脆弱性データ ブロック*	変数 (variable)	Cisco 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+ (4-119 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 (variable)	サードパーティの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+ (4-119 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 (variable)	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、Cisco 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+ (4-119 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。
属性値データ ブロック*	変数 (variable)	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 (4-87 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	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(IP Address)]																																
	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																																
サーバー 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 サーバー 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																																
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																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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																															
ユーザー（User）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 ユーザー 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（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																															
Application 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)																															

	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																																
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…																																
(TCP)全サーバー データ	リスト ブロック タイプ(11)…																																
	リスト ブロック長…																																
	(TCP)全サーバー データ ブロック(104)*																																
(UDP)全サーバー データ	リスト ブロック タイプ(11)																																
	リスト ブロック長																																
	(UDP)全サーバー 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(Transport)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(Admin. 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)														

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	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 [名前(Name)]	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(Notes) 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)*																															
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(Attribute) 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*																															
	Mobile								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-58　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	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 システムから取得したフィンガープリント データ ブロック*	変数（variable）	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+（4-172 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	サーバー 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	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（サーバー フィンガープリント）データ ブロック*	変数（variable）	サーバー 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+（4-172 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	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（variable）	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+（4-172 ページ）を参照してください。

表 B-58　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 タイプ	uint32	Cisco 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	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（variable）	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+（4-172 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	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 2）データ ブロック*	変数（variable）	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+（4-172 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	ユーザー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	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（ユーザー フィンガープリント）データ ブロック*	変数（variable）	ユーザー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+（4-172 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。

表 B-58　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オペレーティング 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（variable）	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+(4-172 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	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(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（variable）	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+(4-172 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	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（variable）	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+(4-172 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ー 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ー データ ブロック長から成る 8 バイトを含みます。

表 B-58　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
(TCP) 全サーバー データ ブロック*	変数 (variable)	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ー 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 サーバー データ ブロック 4.10.0+ (4-151 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ー 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ー データ ブロック長から成る 8 バイトを含みます。
(UDP) 全サーバー データ ブロック*	変数 (variable)	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ー 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 サーバー データ ブロック 4.10.0+ (4-151 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 (variable)	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 ブロックの説明の詳細については、プロトコル データ ブロック (4-80 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。
(トランスポート) プロトコル データ ブロック*	変数 (variable)	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 ブロックの説明の詳細については、プロトコル データ ブロック (4-80 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 (variable)	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+ (4-122 ページ) を参照してください。

表 B-58　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
最後の確認日時	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（Admin. 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（variable）	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+（4-165 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。
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（Notes）	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。

表 B-58　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	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(variable)	Cisco 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+(4-119 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(variable)	サードパーティの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+(4-119 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(variable)	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、Cisco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+(4-119 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。
属性値データ ブロック*	変数(variable)	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(4-87 ページ)を参照してください。
Mobile	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。
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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	フル ホスト プロファイル データ ブロック（140）																															
	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																								

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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																															
サーバー 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 サーバー 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																															
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																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
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																															
ユーザー（User）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 ユーザー 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（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																															
Application 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)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	汎用リスト ブロック長																															
Mobile 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 サーバー 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 サーバー 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 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																															
ユーザー 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 ユーザー エージェント 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
(TCP)全サーバー データ	リスト ブロック タイプ(11)…																															
	リスト ブロック長…																															
	(TCP)全サーバー データ ブロック(104)*																															
(UDP)全サーバー データ	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	(UDP)全サーバー 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(Transport)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(Admin. 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 [名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	NetBIOS 名文字列																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
注記（Notes）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）*																															
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（Attribute）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*																															
	Mobile								改造																							

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-59　　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（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。

表 B-59　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
[IPアドレス(IP Address)]	変数(variable)	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(4-103 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	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 システムから取得したフィンガープリント データ ブロック*	変数(variable)	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+(4-172 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	サーバー 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	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(サーバー フィンガープリント)データ ブロック*	変数(variable)	サーバー 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+(4-172 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	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(variable)	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+(4-172 ページ) を参照してください。

表 B-59　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
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	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（variable）	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+（4-172 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	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 2）データ ブロック*	変数（variable）	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+（4-172 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	ユーザー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	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（ユーザー フィンガープリント）データ ブロック*	変数（variable）	ユーザー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+（4-172 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。

表 B-59　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
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(variable)	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+(4-172 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	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(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(variable)	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+(4-172 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	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(variable)	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+(4-172 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	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-59　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(モバイル)データ ブロック*	変数(variable)	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+(4-172 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 サーバー 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	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 サーバー フィンガープリント)データ ブロック*	変数(variable)	IPv6 サーバー 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+(4-172 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	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(variable)	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+(4-172 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)。
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(variable)	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+(4-172 ページ) を参照してください。

表 B-59　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
汎用リスト ブロック タイプ	uint32	ユーザー 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（ユーザー エージェント）データ ブロック*	変数（variable）	ユーザー 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+（4-172 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ー 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ー データ ブロック長から成る 8 バイトを含みます。
（TCP）全サーバー データ ブロック*	変数（variable）	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ー 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 サーバー データ ブロック 4.10.0+（4-151 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ー 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ー データ ブロック長から成る 8 バイトを含みます。
（UDP）全サーバー データ ブロック*	変数（variable）	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ー 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 サーバー データ ブロック 4.10.0+（4-151 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（variable）	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 ブロックの説明の詳細については、プロトコル データ ブロック（4-80 ページ）を参照してください。

表 B-59　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	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。
(トランスポート)プロトコル データ ブロック*	変数（variable）	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 ブロックの説明の詳細については、プロトコル データ ブロック (4-80 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（variable）	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+ (4-122 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（Admin. 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。

表 B-59　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
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（variable）	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+（4-165 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。
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（Notes）	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（variable）	Cisco 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+（4-119 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（variable）	サードパーティの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+（4-119 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。

表 B-59　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）

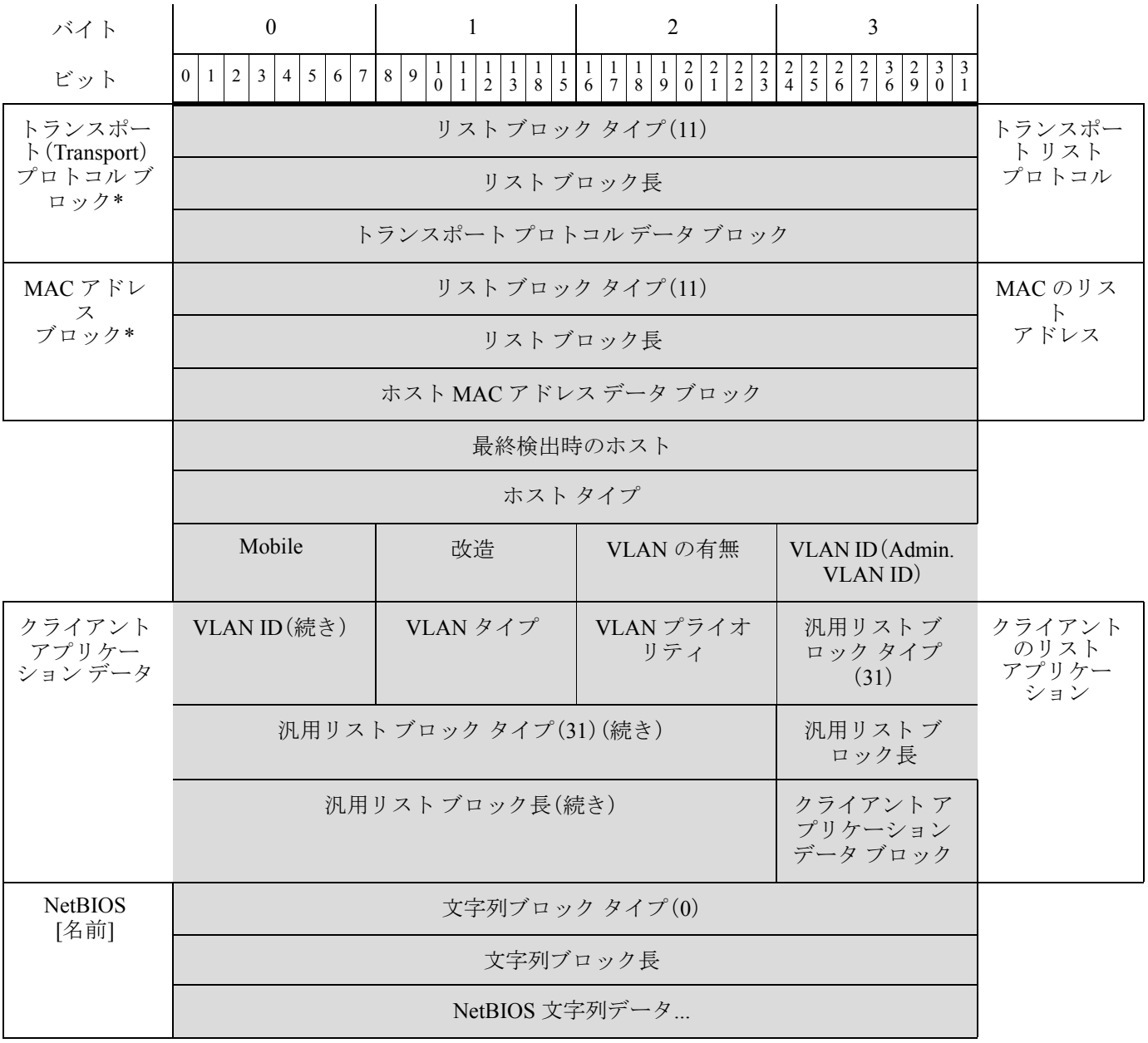
フィールド	データタイプ	説明
(サードパーティスキャン)ホスト脆弱性データ ブロック*	変数（variable）	サードパーティのスキャナから送信されたホスト脆弱性データ ブロック。これらのデータ ブロックのホスト脆弱性 ID は、サードパーティのスキャナ ID であり、Ciscoによって検出された ID ではない点にご注意ください。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+（4-119 ページ）を参照してください。
リスト ブロック タイプ	uint32	属性データを伝送する属性値データ ブロックを含むリスト データ ブロックを表示します。この値は常に 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。
属性値データ ブロック*	変数（variable）	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（4-87 ページ）を参照してください。
Mobile	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。

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 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
サーバー 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)																サーバー 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*																															
モバイル Device 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Device フィンガープリント データ ブロック*																															
TCP サーバー ブロック*	リスト ブロック タイプ(11)																															TCP のリスト サーバー
	リスト ブロック長																															
	TCP サーバー データ ブロック																															
UDP サーバー ブロック*	リスト ブロック タイプ(11)																															UDP のリスト サーバー
	リスト ブロック長																															
	UDP サーバー 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																															


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
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)
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
トランスポート リスト プロトコル
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
MAC のリスト アドレス
最終検出時のホスト
ホスト タイプ
Mobile
改造
VLAN の有無
VLAN ID(Admin. 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 プライオリティ
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)
クライアント アプリケーション データ ブロック
クライアント のリスト アプリケーション
NetBIOS [名前]
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-60　　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（IP Address）]	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	サーバー 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	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（サーバー フィンガープリント）データ ブロック*	変数（variable）	サーバー 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+（4-172 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	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（variable）	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+（4-172 ページ）を参照してください。

表 B-60　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
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（variable）	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+（4-172 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（variable）	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+（4-172 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 Device フィンガープリント）データ ブロック*	変数（variable）	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+（4-172 ページ）を参照してください。
リストブロック タイプ	uint32	TCP サーバー データを伝えるサーバー 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。

表 B-60　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ー データ ブロックを加えた値です。 このフィールドには、ゼロ以上のサーバー データ ブロックが続きます。
TCP サーバー データ ブロック	変数（variable）	TCP サーバーを記述するホスト サーバー 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 サーバー データを伝えるサーバー 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ー データ ブロックを加えた値です。 このフィールドには、ゼロ以上のサーバー データ ブロックが続きます。
UDP サーバー データ ブロック	uint32	UDP サーバーを記述するホスト サーバー 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 (4-80 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 (4-80 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）。

表 B-60　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
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+(4-122 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)
Mobile	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。
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（Admin. 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+(4-165 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表す 0 に設定されます。

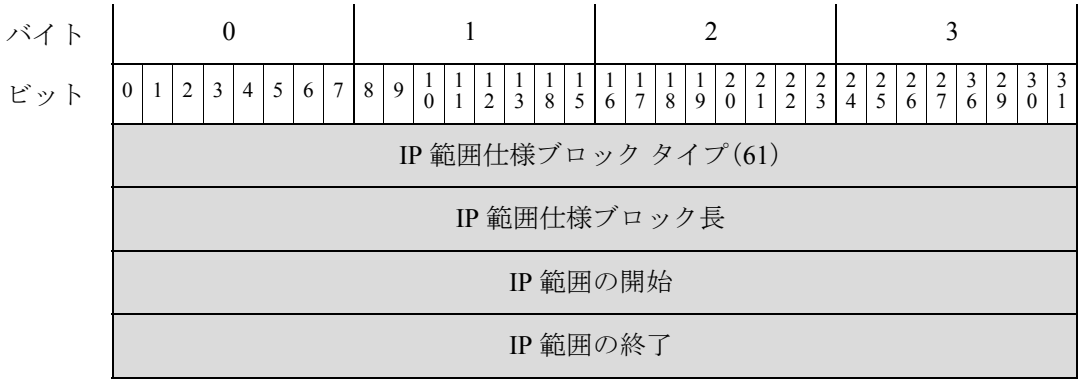
表 B-60　　ホスト プロファイル データ ブロック 5.1.x のフィールド（続き）

フィールド	データタイプ	説明
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、ユーザー プロトコル、ユーザー クライアント アプリケーション、アドレス指定、ユーザー製品、ユーザー サーバー、ユーザー ホスト、ユーザー脆弱性、ユーザー重要度、およびユーザー属性値の各データ 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-61　　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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	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 タイプ(21)																															
	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																															
説明	理由(Reason)																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-62　　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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。