



Firepower eStreamer 統合ガイド

バージョン 6.3

2019 年 4 月 10 日

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報と推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任になります。

Cisco Systems, Inc.

www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。

所在地、電話番号、FAX 番号

は以下のシスコ Web サイトをご覧ください。

(www.cisco.com/go/offices) をご覧ください。

**【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。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルとソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図とその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2018 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

はじめに	1-1
eStreamer バージョン 6.3 の主要な変更点	1-1
このガイドの使用方法	1-2
前提条件	1-2
Firepower システム リリース向け製品バージョン	1-3
表記法	1-5
ベストプラクティス	1-5

CHAPTER 2

eStreamer アプリケーションプロトコルについて	2-1
接続の仕様	2-1
eStreamer 通信段階について	2-2
認証された接続の確立	2-2
eStreamer からのデータの要求	2-3
eStreamer からのデータの受け取り	2-5
接続の終了	2-6
eStreamer メッセージタイプについて	2-6
eStreamer メッセージヘッダー (Message Header)	2-8
ヌルメッセージの形式	2-9
エラーメッセージの形式	2-10
イベントストリーム要求メッセージの形式	2-11
最初のタイムスタンプ	2-12
要求フラグ	2-13
イベントデータメッセージの形式	2-19
イベントデータメッセージの構成について	2-20
侵入イベントとメタデータメッセージの形式	2-21
検出イベントメッセージの形式	2-22
接続イベントメッセージの形式	2-24
相関イベントメッセージの形式	2-24
イベント追加データメッセージの形式	2-26
データブロックヘッダー	2-28
ホスト要求メッセージの形式	2-29
ルールドキュメンテーションのメッセージ形式	2-33

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	2-35
ストリーミング情報メッセージの形式	2-36
ストリーミング要求メッセージの形式	2-37
ストリーミングサービス要求の構造	2-38
ドメインストリーミング要求メッセージの形式	2-39
ストリーミングイベントタイプの構造	2-40
拡張要求メッセージの例	2-43
ストリーミング情報メッセージ	2-43
ストリーミング要求メッセージ	2-44
メッセージバンドルの形式	2-44
メタデータについて	2-45
メタデータの伝送	2-46

CHAPTER 3

侵入および関連データ構造の概要 3-1

侵入イベントとメタデータのレコードタイプ	3-1
パケットレコード 4.8.0.2 以上	3-7
プライオリティレコード	3-8
侵入イベントレコード 6.0 以上	3-9
侵入の影響アラートデータ 5.3 以上	3-18
ユーザレコード	3-21
4.6.1 以上のルールメッセージのレコード	3-22
4.6.1 以上の分類レコード	3-23
関連ポリシーレコード	3-25
関連ルールレコード	3-26
侵入イベント追加データレコード	3-28
侵入イベント追加データのメタデータ	3-30
セキュリティゾーン名レコード	3-31
インターフェイス名レコード	3-33
アクセスコントロールポリシー名のレコード	3-34
アクセスコントロールルールIDレコードのメタデータ	3-35
管理対象 Device レコードのメタデータ	3-37
マルウェアイベントレコード 5.1.1 以上	3-38
Cisco Advanced Malware Protection クラウド名のメタデータ	3-39
マルウェアイベントタイプのメタデータ	3-40
マルウェアイベントサブタイプのメタデータ	3-41
エンドポイント向け AMP ディテクタタイプのメタデータ	3-42
エンドポイント向け AMP ファイルタイプのメタデータ	3-43
セキュリティコンテキスト名	3-44
5.4 以上の関連イベント	3-45

シリーズ2のデータブロックの概要	3-58	
シリーズ2のプリミティブデータブロック	3-62	
文字列データブロック	3-63	
BLOBデータブロック	3-63	
リストデータブロック	3-64	
汎用リストのデータブロック	3-65	
UUID文字列マッピングのデータブロック	3-66	
名前説明マッピングのデータブロック	3-67	
アクセスコントロールポリシールールIDのメタデータブロック	3-68	
ICMPタイプのデータブロック	3-70	
ICMPコードのデータブロック	3-71	
5.4.1以上のセキュリティインテリジェンスカテゴリのメタデータ	3-72	
6.0以上のレルムのメタデータ	3-73	
6.0以上のエンドポイントプロファイルのデータブロック	3-74	
6.0以上のセキュリティグループのメタデータ	3-76	
6.0以上のDNSレコードタイプのメタデータ	3-77	
6.0以上のDNSレスポンスタイプのメタデータ	3-78	
6.0以上のシンクホールのメタデータ	3-80	
6.0以上のNetmapドメインのメタデータ	3-81	
6.0以上のアクセスコントロールポリシー理由データブロック	3-82	
アクセスコントロールポリシー名のデータブロック	3-83	
IPレピュテーションカテゴリのデータブロック	3-85	
6.0以上のファイルイベント	3-86	
マルウェアイベントのデータブロック 6.0以上	3-97	
5.3以上のファイルイベントSHAハッシュ	3-108	
5.3以上のファイルタイプIDのメタデータ	3-110	
5.2以上のルールドキュメントのデータブロック	3-111	
6.0以上のFilelogストレージのメタデータ	3-115	
6.0以上のFilelogサンドボックスのメタデータ	3-116	
6.0以上のFilelog Speroのメタデータ	3-117	
6.0以上のFilelogアーカイブのメタデータ	3-118	
6.0以上のFilelogスタティック分析のメタデータ	3-118	
5.2以上の位置情報のデータブロック	3-119	
6.0以上のファイルポリシー名	3-120	
SSLポリシー名	3-122	
SSLルールID	3-123	
SSL暗号スイート	3-124	
SSLバージョン	3-125	
SSLサーバ証明書ステータス	3-126	
実際のSSLアクション	3-127	

予期された SSL アクション	3-128
SSL フロー ステータス	3-129
SSL URL カテゴリ	3-130
5.4 以上の SSL 証明書の詳細のデータ ブロック	3-131
ネットワーク分析ポリシー レコード	3-135

CHAPTER 4

検出と接続データ構造の概要 4-1

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
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
ディスカバリ イベントのメタデータ	4-8
ディスカバリ イベント ヘッダー 5.2+	4-42
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	4-44
イベントタイプ別ホスト ディスカバリ 構造	4-46
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	4-63
ホスト IOC セット メッセージ	4-63
イベントタイプ別のユーザ データ 構造	4-64
ディスカバリ (シリーズ 1) ブロック	4-65
シリーズ 1 データ ブロック ヘッダー シリーズ	4-65
シリーズ 1 プリミティブ データ ブロック	4-66
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
文字列 データ ブロック	4-75
BLOB データ ブロック	4-76
リスト データ ブロック	4-77
汎用 リスト ブロック	4-78
サブサーバ データ ブロック	4-78
プロトコル データ ブロック	4-80
整数型 (INT32) データ ブロック	4-81
VLAN データ ブロック	4-82
サーバ バナー データ ブロック	4-82
文字列 情報 データ ブロック	4-83
属性 アドレス データ ブロック 5.2+	4-84
ユーザ IOC の変更 データ ブロック 5.3+	4-85
属性 リスト 項目 データ ブロック	4-87
属性 値 データ ブロック	4-88
フル サブサーバ データ ブロック	4-89
オペレーティング システム データ ブロック 3.5+	4-92
ポリシー エンジン 制御 メッセージ データ ブロック	4-93
4.7+ の定義 属性 データ ブロック	4-94

ユーザプロトコルデータブロック	4-97	
5.1.1+のユーザクライアントアプリケーションデータブロック		4-98
ユーザクライアントアプリケーションリストデータブロック		4-100
5.2+のIPアドレス範囲データブロック	4-101	
属性指定データブロック	4-102	
ホストIPアドレスデータブロック	4-104	
MACアドレス指定データブロック	4-105	
アドレス指定データブロック	4-105	
6.1+の接続チャックデータブロック	4-107	
フィックスリストデータブロック	4-109	
ユーザサーバデータブロック	4-109	
ユーザサーバリストデータブロック	4-111	
ユーザホストデータブロック 4.7+	4-112	
ユーザ脆弱性変更データブロック 4.7+	4-114	
ユーザ重要度変更データブロック 4.7+	4-115	
ユーザ属性値データブロック 4.7+	4-117	
ユーザプロトコルリストデータブロック 4.7+	4-118	
ホスト脆弱性データブロック 4.9.0+	4-120	
アイデンティティデータブロック	4-121	
ホストMACアドレス 4.9+	4-122	
セカンダリホストの更新	4-123	
5.0+のWebアプリケーションデータブロック	4-125	
接続統計データブロック 6.2+	4-126	
スキャン結果データブロック 5.2+	4-143	
ホストサーバデータブロック 4.10.0+	4-146	
フルホストサーバデータブロック 4.10.0+	4-148	
4.10.x、5.0～5.0.2のサーバ情報データブロック	4-152	
フルサーバ情報データブロック	4-154	
4.10.0+の汎用スキャン結果データブロック	4-157	
4.10.0+のスキャン脆弱性データブロック	4-159	
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+	4-162	
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	4-164	
ユーザ脆弱性データブロック 5.0+	4-166	
オペレー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+	4-169	
5.1+のモバイルDevice情報データブロック	4-171	
ホストプロファイルデータブロック 5.2+	4-172	
ユーザ製品データブロック 5.1+	4-180	
ユーザデータブロック	4-188	
ユーザアカウント更新メッセージデータブロック	4-189	
6.0+の情報データユーザブロック	4-198	

6.2+のVPNセッションデータブロック	4-201
ユーザログイン情報データブロック 6.2+	4-204
ディスクバリ/接続イベントシリーズ2データブロック	4-209
アクセスコントロールルールデータブロック	4-209
アクセスコントロールルール理由データブロック 5.1+	4-211
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+	4-213
ユーザデータブロック	4-214

CHAPTER 5

ホストデータ構造の概要 5-1

全ホストプロファイルデータブロック 5.3+	5-1
------------------------	-----

CHAPTER 6

eStreamer の設定 6-1

eStreamer サーバでの eStreamer の設定	6-1
eStreamer イベントタイプの設定	6-2
eStreamer クライアントの認証の追加	6-3
eStreamer サービスの管理	6-4
eStreamer サービスの開始および停止	6-4
eStreamer サービスのオプション	6-5
eStreamer 参照クライアントの設定	6-6
eStreamer Perl 参照クライアントの設定	6-6
eStreamer Perl 参照クライアントの実行	6-12

APPENDIX A

データ構造の例 A-1

侵入イベントのデータ構造の例	A-1
Management Center 5.4+ の侵入イベントの例	A-1
侵入影響アラートの例	A-7
パケットレコードの例	A-9
分類レコードの例	A-10
優先度レコードの例	A-12
ルールメッセージレコードの例	A-13
6.1.x の接続統計データブロックの例	A-15
バージョン 5.1+ ユーザイベントの例	A-28
ディスクバリ データ構造の例	A-32
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
新しい TCP サーバメッセージの例	A-33

APPENDIX B

レガシー データ構造の概要 B-1

レガシー侵入データ構造	B-1
侵入イベント (IPv4) レコード 5.0.x ~ 5.1	B-2

侵入イベント (IPv6) レコード 5.0.x ~ 5.1	B-8
侵入イベント レコード 5.2.x	B-14
侵入イベント レコード 5.3	B-20
侵入イベント レコード 5.1.1.x	B-26
侵入イベント レコード 5.3.1	B-32
侵入イベント レコード 5.4.x	B-39
侵入影響アラート データ	B-48
レガシー マルウェア イベントのデータ構造	B-51
マルウェア イベントのデータ ブロック 5.1	B-51
マルウェア イベント データ ブロック 5.1.1.x	B-55
マルウェア イベント データ ブロック 5.2.x	B-61
マルウェア イベントのデータ ブロック 5.3	B-68
マルウェア イベント データ ブロック 5.3.1	B-76
マルウェア イベント データ ブロック 5.4.x	B-83
レガシー ディスカバリ データ構造	B-94
レガシー ディスカバリ イベント ヘッダー	B-94
レガシー サーバ データ ブロック	B-96
属性 アドレス データ ブロック 5.0 ~ 5.1.1.x	B-96
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	B-97
レガシー スキャン 結果 データ ブロック	B-99
レガシー ユーザ ログイン データ ブロック	B-108
ユーザ ログイン 情報 データ ブロック 6.1.x	B-119
レガシー ホスト プロファイル データ ブロック	B-126
レガシー OS フィンガープリント データ ブロック	B-133
レガシー 接続 データ 構造	B-135
接続 統計 データ ブロック 5.0 ~ 5.0.2	B-135
接続 統計 データ ブロック 5.1	B-140
接続 統計 データ ブロック 5.2.x	B-146
接続 チャンク データ ブロック 5.0 ~ 5.1	B-153
接続 チャンク データ ブロック 5.1.1 ~ 6.0.x	B-154
接続 統計 データ ブロック 5.1.1.x	B-156
接続 統計 データ ブロック 5.3	B-163
接続 統計 データ ブロック 5.3.1	B-170
接続 統計 データ ブロック 5.4	B-177
接続 統計 データ ブロック 5.4.1	B-191
接続 統計 データ ブロック 6.0.x	B-205
接続 統計 データ ブロック 6.1.x	B-222
レガシー ファイル イベントのデータ 構造	B-240
ファイル イベント 5.1.1.x	B-240

ファイルイベント 5.2.x	B-244
ファイルイベント 5.3	B-249
ファイルイベント 5.3.1	B-256
ファイルイベント 5.4.x	B-262
ファイルイベント SHA ハッシュ 5.1.1 ~ 5.2.x	B-273
レガシー関連イベントのデータ構造	B-274
関連イベント 5.0 ~ 5.0.2	B-275
関連イベント 5.1 ~ 5.3.x	B-283
レガシー ホスト データ構造	B-291
フルホストプロファイルデータ ブロック 5.0 ~ 5.0.2	B-291
フルホストプロファイルデータ ブロック 5.1.1	B-301
フルホストプロファイルデータ ブロック 5.2.x	B-312
ホストプロファイルデータ ブロック 5.1.x	B-326
IP 範囲仕様データ ブロック 5.0 ~ 5.1.1.x	B-332
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-333



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 Firepower システム イベントをストリーミングできます。Management Center からのホストデータ、検出データ、相関データ、コンプライアンスのホワイトリストデータ、侵入データ、ユーザアクティビティデータ、ファイルデータ、マルウェアデータ、接続データをストリーミングでき、また、7000 および 8000 シリーズのデバイスからの侵入データをストリーミングできます。

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

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

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

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

このガイドでは、eStreamer バージョン 6.3 クライアントアプリケーションを正常に作成し、実行するのに必要な情報を提供します。

eStreamer バージョン 6.3 の主要な変更点

[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](#)に、失敗したユーザのログイン、VPN ユーザのログイン、および VPN ユーザのログオフの各イベントを追加しました。

[「ベストプラクティス」](#)のセクションを追加しました。

このガイドの使用方法

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

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

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

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

前提条件

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

Firepower システム リリース向け製品バージョン

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

表 1-1 Firepower システム 製品バージョン

リリース	Management Center バージョン	マスター Management Center バー ジョン	侵入センサー バージョン	センサー バー ジョン	管理対象 Device のバージョン
IMS 3.0	管理コンソール 3.0	該当なし	ネットワーク センサー 3.0	該当なし	該当なし
IMS 3.1	管理コンソール 3.1	該当なし	ネットワーク センサー 3.1	無応答(RNA) センサー 1.0	該当なし
IMS 3.2	管理コンソール 3.2	該当なし	ネットワーク センサー 3.2	無応答(RNA) センサー 2.0	該当なし
3D システム 4.0	Management Center 4.0	該当なし	侵入センサー 4.0	無応答(RNA) センサー 3.0	該当なし
3D システム 4.5	Management Center 4.5	該当なし	侵入センサー 4.5	無応答(RNA) センサー 3.5	該当なし
3D システム 4.6.1	Management Center 4.6.1	マスター Management Center 4.6.1	該当なし	該当なし	4.6.1
3D システム 4.7	Management Center 4.7	マスター Management Center 4.7	該当なし	該当なし	4.7
3D システム 4.8	Management Center 4.8	マスター Management Center 4.8	該当なし	該当なし	4.8
3D システム 4.8.0.2	Management Center 4.8.0.2	マスター Management Center 4.8.0.2	該当なし	該当なし	4.8.0.2
3D システム 4.9	Management Center 4.9	マスター Management Center 4.9	該当なし	該当なし	4.9
3D システム 4.9.1	Management Center 4.9.1	マスター Management Center 4.9.1	該当なし	該当なし	4.9.1
3D システム 4.10	Management Center 4.10	マスター Management Center 4.10	該当なし	該当なし	4.10
3D システム 4.10.1	Management Center 4.10.1	マスター Management Center 4.10.1	該当なし	該当なし	4.10.1

表 1-1 Firepower システム 製品バージョン(続き)

リリース	Management Center バージョン	マスター Management Center バー ジョン	侵入センサー バージョン	センサー バー ジョン	管理対象 Device のバージョン
3D システム 4.10.2	Management Center 4.10.2	マスター Management Center 4.10.2	該当なし	該当なし	4.10.2
3D システム 4.10.3	Management Center 4.10.3	マスター Management Center 4.10.3	該当なし	該当なし	4.10.3
3D システム 5.0	Management Center 5.0	該当なし	該当なし	該当なし	5.0
3D システム 5.1	Management Center 5.1	該当なし	該当なし	該当なし	5.1
3D システム 5.1.1	Management Center 5.1.1	該当なし	該当なし	該当なし	5.1.1
3D システム 5.2	Management Center 5.2	該当なし	該当なし	該当なし	5.2
3D システム 5.3	Management Center 5.3	該当なし	該当なし	該当なし	5.3
Firepower システム 5.3.1	Management Center 5.3.1	該当なし	該当なし	該当なし	5.3.1
Firepower システム 5.4	Management Center 5.4	該当なし	該当なし	該当なし	5.4
Firepower システム 6.0	Management Center 6.0	該当なし	該当なし	該当なし	6.0
Firepower システム 6.1	Management Center 6.1	該当なし	該当なし	該当なし	6.1
Firepower システム 6.2	Management Center 6.2	該当なし	該当なし	該当なし	6.2
Firepower システム 6.2.1	Management Center 6.2.1	該当なし	該当なし	該当なし	6.2.1
Firepower システム 6.2.2	Management Center 6.2.2	該当なし	該当なし	該当なし	6.2.2
Firepower システム 6.2.2	Management Center 6.2.3	該当なし	該当なし	該当なし	6.2.3
Firepower システム 6.3.0	Management Center 6.3.0	該当なし	該当なし	該当なし	6.3.0

- 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関し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

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

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

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

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

接続の仕様

eStreamer サービス：

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

eStreamer 通信段階について

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

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

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

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

イベント データを要求するための 2 つの要求モードを使用できます。

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

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

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

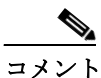
詳細については、[eStreamer からのデータの受け取り \(2-5 ページ\)](#) を参照してください。

4. 接続が終了します。

詳細については、[接続の終了 \(2-6 ページ\)](#) を参照してください。

認証された接続の確立

クライアントが eStreamer からデータを要求できるようになるには、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 チャンネル構成を強制しないため、接続用のインターフェイスを選択する場合は構成を無視できます。クライアントが接続を開始すると、eStreamer サーバが応答し、クライアントとの SSL ハンドシェイクを開始します。SSL ハンドシェイクの一部として、eStreamer サーバはクライアントの認証証明書を要求し、証明書が有効である (eStreamer サーバで内部認証局 (内部 CA) によって署名されている) ことを確認します。



コメント

Cisco は、クライアントが eStreamer サーバによって提示された証明書が信頼できる認証局によって署名されていることを確認するように要求することを推奨しています。これは PKCS # 12 ファイルに含まれる内部 CA 証明書で、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 サーバは証明書の追加の接続後検証を実行します。この検証では、クライアント接続が証明書で指定されたホストから始まり、証明書のサブジェクト名に適切な値が含まれているか確認されます。いずれかの接続後のチェックが失敗すると、eStreamer サーバは接続を閉じます。必要に応じて、クライアント ホスト名のチェックを実行しないように eStreamer サービスを設定できます(詳細については、[eStreamer サービスのオプション\(6-5 ページ\)](#)を参照)。

クライアントは接続後の検証を実行する必要はありませんが、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 サーバはクライアントからのデータ要求を待ちます。

eStreamer からのデータの要求

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

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

セッションの確立

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

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



コメント

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

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

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

イベントストリーム要求の送信

イベントストリーム要求は単純なプロセスを使用します。

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

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

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

拡張要求の送信

イベントストリーム要求メッセージの要求フラグフィールドにビット30を設定すると、拡張要求が開始され、サーバとのネゴシエーションが開始されます。このビットが設定されている場合は、拡張要求フラグを送信する必要があります。拡張要求で使用可能なイベントタイプについては、[表 2-22\(2-41 ページ\)](#)を参照してください。

拡張要求の手順は次のとおりです。

- クライアントは、イベントストリーミング要求メッセージを、要求フラグビット30を1に設定(拡張要求を示す)して eStreamer に送信します。メッセージ形式の詳細については、[イベントストリーム要求メッセージの形式\(2-11 ページ\)](#)を参照してください。
- eStreamer は、クライアントが使用可能なサービスのリストをアドバタイズするストリーミング情報メッセージで応答します。ストリーミング情報メッセージの詳細については、[ストリーミング情報メッセージの形式\(2-36 ページ\)](#)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\(2-43 ページ\)](#)を参照してください。
- eStreamer は、クライアントのストリーミング要求メッセージを処理し、メッセージで指定された時刻にデータのストリーミングを開始します。ストリーミングプロトコルについては、[eStreamer からのデータの受け取り\(2-5 ページ\)](#)を参照してください。

ホストデータの要求

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

要求の変更

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

eStreamer からのデータの受け取り



コメント

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

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

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

イベントストリーム要求

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

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

拡張要求

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

クライアントは各バンドルをメッセージごとに解凍し、レコードとブロックの長さを使用して各メッセージを解析します。各メッセージヘッダーのメッセージ全体の長さを使用して、各メッセージの終わりに達した時点进行計算し、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\(2-44 ページ\)](#)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\(2-9 ページ\)](#)を参照してください。

接続の終了

eStreamer サーバは、接続を閉じる前にエラー メッセージの送信を試行します。エラー メッセージについては、[エラー メッセージの形式\(2-10 ページ\)](#)を参照してください。

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

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

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

eStreamer メッセージタイプについて

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

表 2-2 eStreamer メッセージタイプ

メッセージタイプ	名前	説明
0	ヌル メッセージ	eStreamer サーバとクライアントの両方が、データフローを制御するためのヌル メッセージを送信します。詳細については、 ヌル メッセージの形式(2-9 ページ) を参照してください。
1	エラー メッセージ	eStreamer サーバとクライアントの両方がエラー メッセージを使用して、接続が閉じた理由を示します。詳細については、 エラー メッセージの形式(2-10 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(2-11 ページ) を参照してください。
4	イベント データ	eStreamer サービスは、このメッセージタイプを使用して、イベント データとメタデータをクライアントに送信します。詳細については、 イベント データ メッセージの形式(2-19 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(2-29 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(2-35 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(2-35 ページ) を参照してください。
2049	ストリーミング要求	クライアントは、このメッセージタイプを拡張要求で使用して、希望するストリーム情報メッセージからアドバタイズされたイベントを指定します。詳細については、 拡張要求メッセージの例(2-43 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
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(2-36 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(2-44 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。

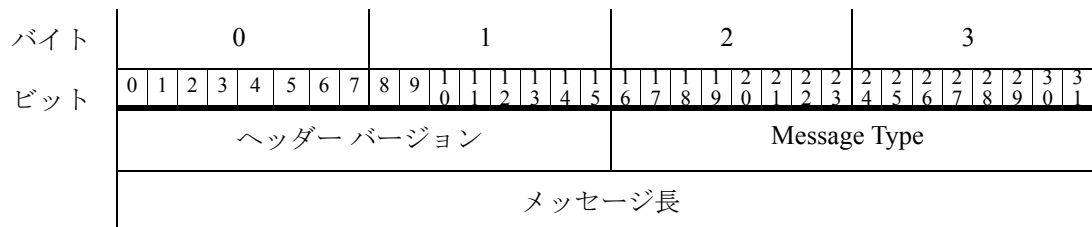


表 2-3 標準の eStreamer メッセージヘッダー フィールド

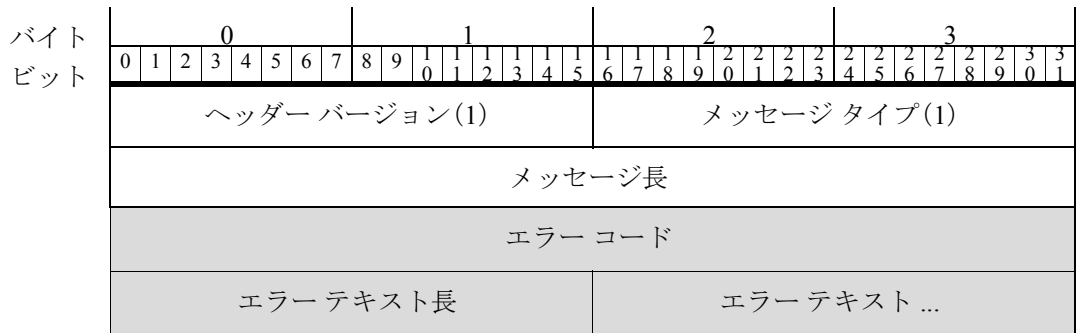
フィールド	データタイプ	説明
ヘッダーバージョン	uint16	メッセージで使用されるヘッダーのバージョンを示します。eStreamer の現在のバージョンの場合、この値は常に 1 となります。
Message Type	uint16	送信されるメッセージのタイプを示します。現在の値のリストについては、 表 2-2(2-7 ページ) を参照してください。
メッセージ長	uint32	後続のコンテンツの長さを示し、メッセージヘッダー自体のバイトを除外します。ヘッダーがありデータのないメッセージのメッセージ長はゼロです。

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。

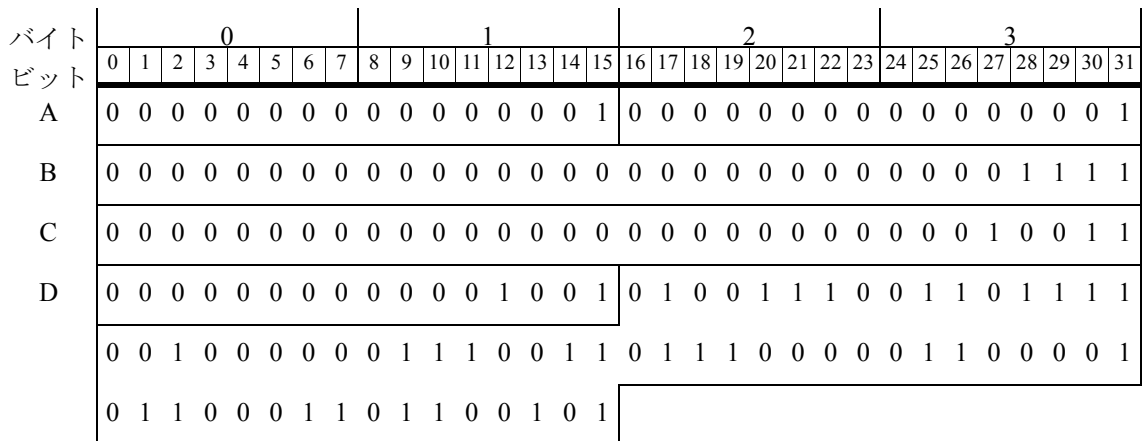


次の表では、エラーコードメッセージの各フィールドについて説明します。

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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(2)															
	メッセージ長																															
	最初のタイムスタンプ																															
	要求フラグ																															

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： <ul style="list-style-type: none"> クライアントが eStreamer に接続するときを開始するには、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。 特定の日に開始するには、UNIX タイムスタンプ (1970 年 1 月 1 日以降の秒数) を指定します。 詳細については、以下の 最初のタイムスタンプ (2-12 ページ) を参照してください。
要求フラグ	bits[32]	イベントストリーム要求で返されるイベントとメタデータのタイプとバージョンを指定します。フラグの定義については、 要求フラグ (2-13 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



コメント

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

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

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

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

要求フラグ

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

[要求フラグ(Request Flags)] フィールドのビット設定の定義については、[表 2-6\(2-13 ページ\)](#)を参照してください。異なるフラグは、異なるバージョンのイベント データを要求します。たとえば、4.10 形式ではなく Firepower システム 4.9 形式でデータを取得するには、異なるフラグ ビットを設定します。特定の製品バージョンのデータを要求するとき使用するフラグの固有情報については、[表 2-7\(2-17 ページ\)](#)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\(2-13 ページ\)](#)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。

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

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(2-45 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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
ビット 3	<p>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。</p> <p>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。</p>
ビット 4	<p>関連データ 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、関連データ バージョン 1 は送信されません。</p>
ビット 5	<p>影響関連イベント(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。</p> <p>侵入影響アラートの詳細については、侵入の影響アラート データ 5.3 以上(3-18 ページ)を参照してください。</p>
ビット 6	<p>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(2-14 ページ)を参照してください。</p>
ビット 7	<p>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。</p>
ビット 8	<p>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。</p>
ビット 9	<p>関連データ 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、関連ポリシー データ バージョン 2 は送信されません。</p>
ビット 10	<p>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。</p> <p>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-94 ページ)を参照してください。</p>
ビット 11	<p>イベントの送信を無効にします。</p>
ビット 12	<p>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。</p>
ビット 13	<p>関連データ 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、関連データ バージョン 3 は送信されません。</p>

表 2-6 要求フラグ(続き)

ビットフィールド	説明
ビット 14	<p>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。</p> <p>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 (2-45 ページ) を参照してください。</p>
ビット 15	<p>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。</p> <p>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 (2-45 ページ) を参照してください。</p>
ビット 16	未使用 (Unused)
ビット 17	<p>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。</p>
ビット 18	<p>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 (4-57 ページ) を参照してください。</p>
ビット 19	<p>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。</p> <p>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-274 ページ) を参照してください。</p>

表 2-6 要求フラグ(続き)

ビット フィールド	説明
ビット 20	<p>侵入、検出、ユーザ アクティビティ、相関、および接続イベントに関連するバージョン 4 メタデータの送信を要求します。1 に設定すると、バージョン 4 のメタデータがイベントとともに送信されます。0 に設定すると、バージョン 4 のメタデータは送信されません。</p> <p>バージョン 4 のメタデータには、次のものが含まれます。</p> <ul style="list-style-type: none"> • 相関(コンプライアンス)ルールの情報 • 相関(コンプライアンス)ポリシーの情報 • フィンガープリント レコード • クライアント アプリケーション レコード • クライアント アプリケーション タイプのレコード • 脆弱性レコード • ホストの重要度レコード • ネットワーク プロトコル レコード • ホストの属性レコード • スキャン タイプのレコード • ユーザ レコード • サービス検出デバイス(バージョン 2)のレコード • イベント分類(バージョン 2)のレコード • 優先順位レコード • ルール情報(バージョン 2) • マルウェアの情報 <p>ビット 22 を使用してビット 20 を要求すると、ユーザのメタデータも送信されます。</p> <p>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(2-45 ページ)を参照してください。</p>
ビット 21	<p>バージョン 1 ユーザ イベントの送信を要求します。ユーザ イベントの詳細については、ユーザ レコード(4-21 ページ)を参照してください。</p>
ビット 22	<p>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。</p> <p>ビット 22 を使用してビット 20 を要求すると、ユーザのメタデータも送信されます。</p> <p>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-274 ページ)を参照してください。</p>
ビット 23	<p>拡張イベント ヘッダーを要求します。1 に設定すると、イベントは、eStreamer サーバが処理するためにイベントがアーカイブされたときに適用されたタイムスタンプと、将来の使用のために予約された 4 バイトが付いて送信されます。このフィールドが 0 に設定されている場合、イベントは、レコードタイプとレコード長のみを含む標準のイベント ヘッダーが付いて送信されます。</p> <p>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) (2-8 ページ)を参照してください。</p>

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、 接続チャックメッセージ(4-57 ページ) を参照してください。
ビット 27	追加データ レコード内の侵入イベントに関連するイベント追加データを要求します。 イベント データの詳細については、 表 3-11 侵入イベント追加データのデータ ブロック フィールド(3-29 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	関連データバージョン 6 (Management Center 4.10 ~ 4.10.x) の送信を要求します。0 に設定すると、関連ポリシー データバージョン 6 は送信されません。 ビット 29 を使用してビット 20 を要求すると、ユーザのメタデータも送信されます。 関連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
関連イベント	ビット 22	ビット 22	ビット 29	ビット 30	ビット 30	ビット 30

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+
イベント追加データ	—	—	ビット ト 27	ビット ト 27	ビット ト 27	ビット ト 27
影響イベントアラート	ビット ト 5	ビット ト 5	ビット ト 5	ビット ト 5	ビット ト 5	ビット ト 5
接続データ	ビット ト 18	ビット ト 26	ビット ト 26	ビット ト 30	ビット ト 30	ビット ト 30
ユーザ イベント	ビット ト 21	ビット ト 21	ビット ト 21	ビット ト 30	ビット ト 30	ビット ト 30
マルウェア イベント	—	—	—	—	—	ビット ト 30
ファイル イベント	—	—	—	—	—	ビット ト 30



注意

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

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

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

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

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



コメント

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。

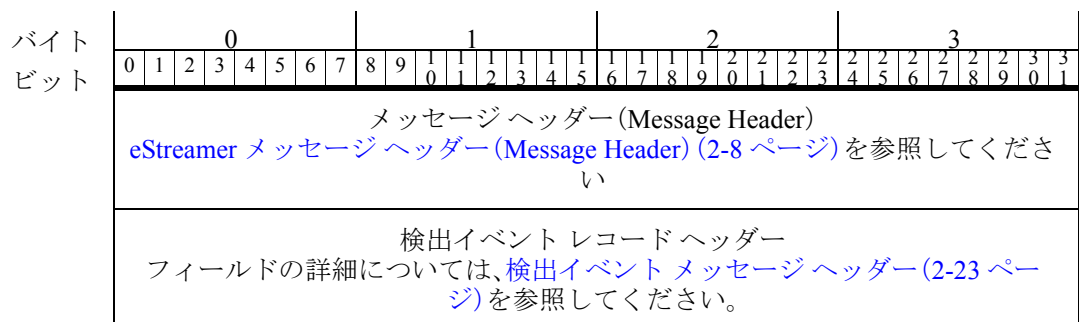
- 侵入イベント データ レコードとすべてのメタデータ レコードについては[侵入イベントとメタデータ メッセージの形式\(2-21 ページ\)](#)。これらのメッセージは固定長フィールドを持ちます。
- 検出イベントまたはユーザ イベント データを含むメッセージについては[検出イベントメッセージの形式\(2-22 ページ\)](#)。標準の eStreamer メッセージ ヘッダーおよび侵入イベントメッセージに類似したレコード ヘッダーに加えて、検出メッセージには、イベント タイプとサブタイプ フィールドが含まれた独特の検出イベント ヘッダーがあります。検出イベントメッセージ内のデータ レコードは、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\(2-24 ページ\)](#)。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。
- 関連(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[関連イベントメッセージの形式\(2-24 ページ\)](#)。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\(2-26 ページ\)](#)。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\(2-26 ページ\)](#)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\(2-28 ページ\)](#)を参照してください。

表 2-8 侵入イベントとメタデータ レコードヘッダー フィールド

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

検出イベントメッセージの形式

次の図に、検出イベントメッセージの構造を示します。標準の eStreamer メッセージヘッダーとイベントレコードヘッダーの後には、検出イベントメッセージとユーザイベントメッセージでのみ使用される検出イベントヘッダーが続きます。メッセージの検出イベントヘッダーセクションには、検出イベントタイプおよびサブタイプフィールドが含まれており、これらのフィールドが一緒になって後続のデータブロックへのキーを形成します。現在の検出イベントタイプおよびサブタイプについては、[表 4-29 タイプ/サブタイプ別のディスカバリイベントと接続イベント \(4-44 ページ\)](#) を参照してください。



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

表 2-9 検出イベントメッセージヘッダーのフィールド

フィールド	データタイプ	説明
Netmap ID	uint16	このフィールドの第1ビットは、ヘッダーがアーカイブタイムスタンプを含む拡張ヘッダーであるかどうかを示すフラグです。残りの15ビットは、イベントが検出されたドメインの Netmap ID を含むオプションのフィールドです。このフィールドは、使用されていない場合は空のままです。Netmap ID は、メタデータで提供されるドメインにマップされます。
レコードタイプ	uint16	データレコードのコンテンツタイプを識別します。レコードタイプのリストについては、 表 4-1 ディスカバリ イベントと接続イベントのレコードタイプ (4-3 ページ) を参照してください。
レコード長	uint32	レコードヘッダーの後のメッセージのコンテンツの長さ。レコードヘッダーの8または16バイトは含まれません。(レコード長+レコードヘッダーの長さは、メッセージ長と等しくなります。)
eStreamer サーバタイムスタンプ (eStreamer Server Timestamp)	uint32	イベントが eStreamer サーバによってアーカイブされたときに適用されるタイムスタンプを示します。アーカイブタイムスタンプとも呼ばれます。イベントストリーム要求の要求フラグフィールドにビット23が設定されている場合にのみ存在するフィールド。
将来使用	uint32	今後使用するために予約されています。要求メッセージフラグにビット23が設定されている場合にのみ表示されるフィールド。
検出イベントヘッダー	さまざま	イベントタイプとサブタイプを含む複数のフィールドが含まれており、これらが一緒になって後続のデータ構造への固有キーを形成します。検出イベントヘッダーのフィールドの定義については、 ディスカバリ イベントヘッダー 5.2+ (4-42 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 \(2-22 ページ\)](#) 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。

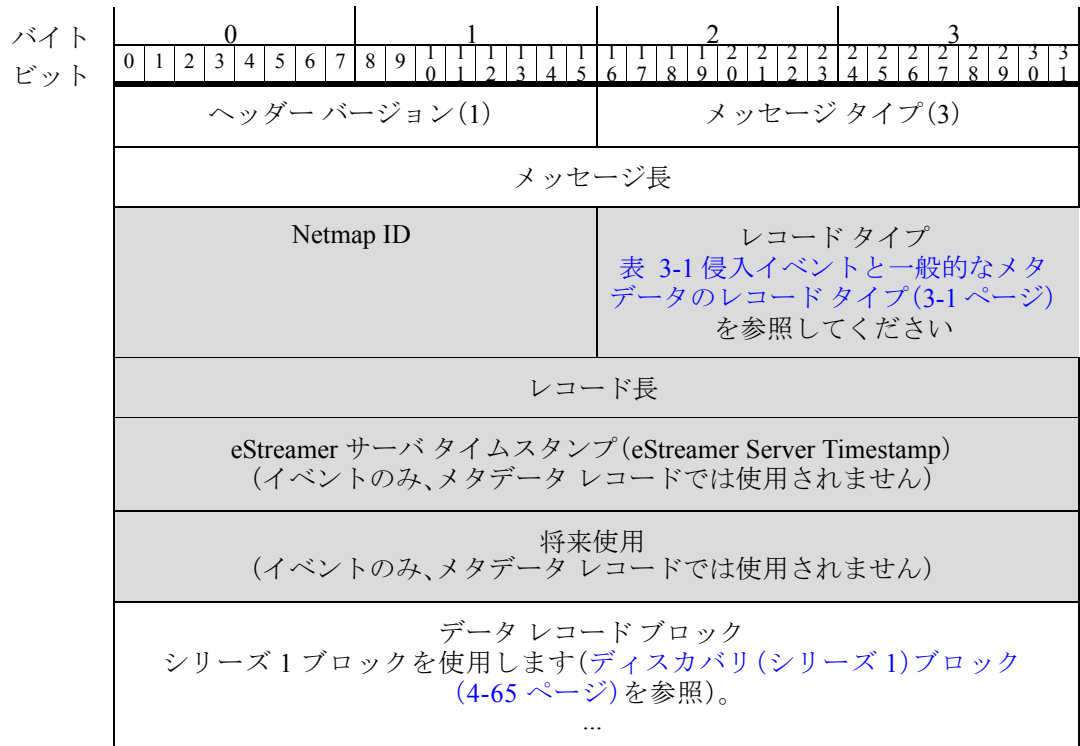
関連イベントメッセージの形式

次の図に、関連(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。関連メッセージは、シリーズ1データブロックを使用します。



関連レコードヘッダー

次の図の網掛け部分は、関連イベント 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。関連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、関連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。



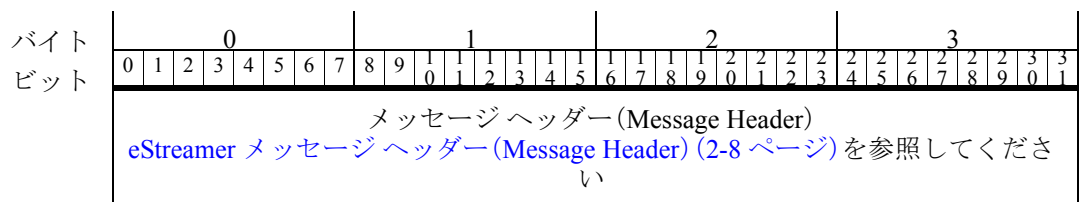
次の表では、関連イベントメッセージのレコードヘッダーの各フィールドについて説明します。

表 2-10 関連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、関連、およびメタデータのレコードタイプのリストについては、表 3-1(3-1 ページ)を参照してください。
レコード長	uint32	レコードヘッダーの後のメッセージのコンテンツの長さ。レコードヘッダーの8または16バイトは含まれません。(レコード長+レコードヘッダーの長さは、メッセージ長と等しくなります。)
eStreamer サーバタイムスタンプ (eStreamer Server Timestamp)	uint32	イベントが eStreamer サーバによってアーカイブされたときに適用されるタイムスタンプを示します。アーカイブタイムスタンプとも呼ばれます。 要求メッセージフラグにビット23が設定されている場合にのみ表示されるフィールド。 ホストプロファイルやメタデータなど、Management Centerによって生成されたデータの場合フィールドはゼロです。
将来使用	uint32	今後使用するために予約されています。 要求メッセージフラグにビット23が設定されている場合にのみ表示されるフィールド。

イベント追加データメッセージの形式

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



レコードヘッダー イベント追加データメッセージのレコードヘッダー(2-27 ページ)を参照してください
データブロック ... 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は、関連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。関連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。

バイト ビット	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;">0</td> <td style="width: 25%;">1</td> <td style="width: 25%;">2</td> <td style="width: 25%;">3</td> </tr> <tr> <td>0</td><td>1</td><td>2</td><td>3</td> </tr> <tr> <td>4</td><td>5</td><td>6</td><td>7</td> </tr> <tr> <td>8</td><td>9</td><td>10</td><td>11</td> </tr> <tr> <td>12</td><td>13</td><td>14</td><td>15</td> </tr> <tr> <td>16</td><td>17</td><td>18</td><td>19</td> </tr> <tr> <td>20</td><td>21</td><td>22</td><td>23</td> </tr> <tr> <td>24</td><td>25</td><td>26</td><td>27</td> </tr> <tr> <td>28</td><td>29</td><td>30</td><td>31</td> </tr> </table>	0	1	2	3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	1	2	3																																		
0	1	2	3																																		
4	5	6	7																																		
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(3)																																					
メッセージ長																																					
Netmap ID	レコードタイプ 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																																					
eStreamer サーバタイムスタンプ(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(Data Record Block) シリーズ2ブロックを使用します(シリーズ2のデータブロックの概要(3-58 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 サーバタイムスタンプ(eStreamer Server Timestamp)	uint32	イベントがeStreamerサーバによってアーカイブされたときに適用されるタイムスタンプを示します。アーカイブタイムスタンプとも呼ばれます。 要求メッセージフラグにビット23が設定されている場合にのみ表示されるフィールド。Management Centerによって生成されたイベントの場合は、フィールドが存在しません。
将来使用	uint32	今後使用するために予約されています。 要求メッセージフラグにビット23が設定されている場合にのみ表示されるフィールド。Management Centerによって生成されたイベントの場合は、フィールドが存在しません。

データブロックヘッダー

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

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

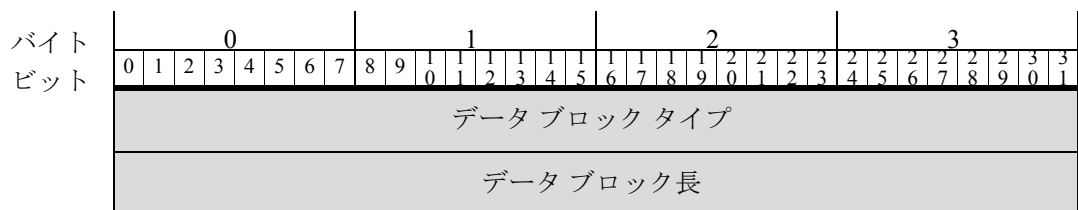


表 2-12

フィールド	データタイプ	説明
データブロックタイプ	uint32	シリーズ 1 ブロックのタイプについては、 ディスカバリ (シリーズ 1) ブロック (4-65 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 3-26 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。

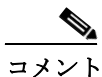
ホスト要求メッセージの形式

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。



コメント

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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 (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。

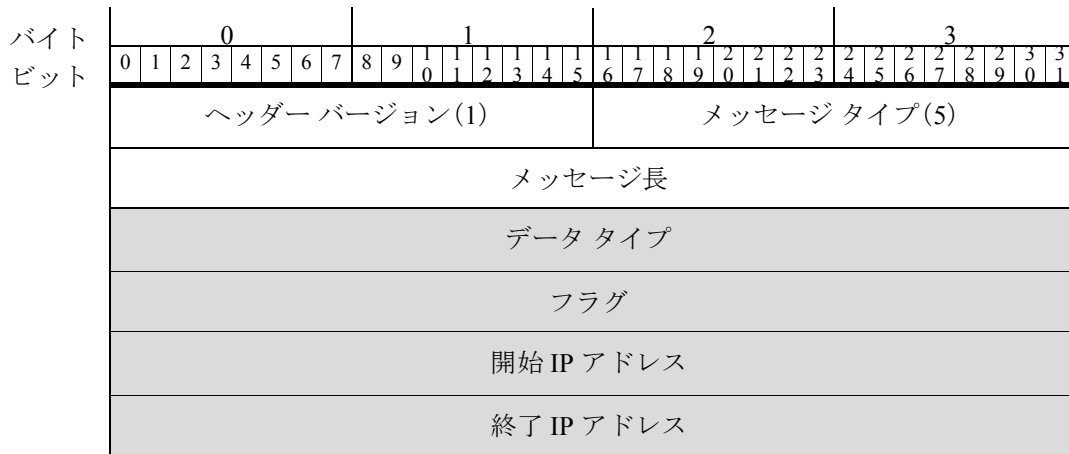
表 2-13 ホスト要求メッセージフィールド

フィールド	データタイプ	説明
データタイプ	uint32	<p>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。</p> <ul style="list-style-type: none"> • 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-291 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-291 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-301 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-301 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 (2-33 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-312 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-312 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)。

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
フラグ	32 ビットフィールド	<ul style="list-style-type: none"> 0x00000001: ホストプロファイルの [注(Notes)] フィールドが (Firepower システムに格納されているホストに関するユーザ定義の情報を使用して) 読み込まれます。 0x00000002: サービスブロックの [バナー(Banner)] フィールドが (サービスについて検出された最初のパケットの最初の 256 バイトを使用して) 読み込まれます。バナーはデフォルトでは無効になっており、設定されている場合にのみ使用できます。
開始 IP アドレス	uint8[16]	データを返す必要があるホストの IP アドレス (要求が単一ホストに対する場合)、または IP アドレス範囲の開始アドレス (要求が複数のホストに対する場合)。IPv4 または IPv6 アドレスにできます。
終了 IP アドレス	uint8[16]	IP アドレス範囲の終了アドレス (要求が複数のホストに対する場合)、または開始 IP アドレスの値 (要求が単一ホストに対する場合)。IPv4 または IPv6 アドレスにできます。

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



次の表では、メッセージフィールドについて説明します。

表 2-14 ホスト要求メッセージフィールド

フィールド	データタイプ	説明
データタイプ	uint32	次のコードを使用して、単一のホストまたは複数のホストのデータを要求します。 <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 0x00000001: ホストプロファイルの [注(Notes)] フィールドが (Firepower システムに格納されているホストに関するユーザ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 (3-111 ページ) を参照してください。
フラグ	32 ビットフィールド	<ul style="list-style-type: none"> 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 Firepower システムに格納されているホストに関するユーザ定義の情報が読み込まれます。 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。

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(続き)

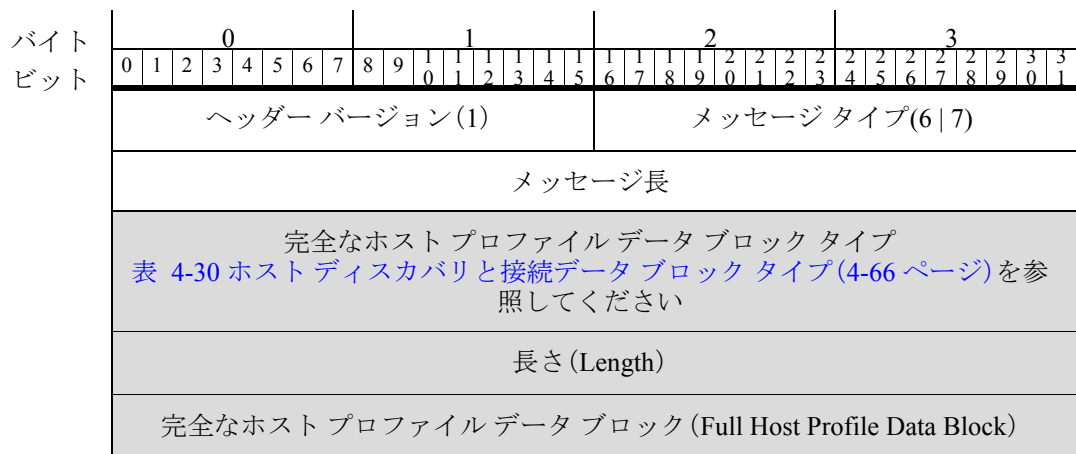
フィールド	データタイプ	説明
シグネチャ ID	uint32	要求したルールの ID 番号。
ジェネレータ ID	uint32	要求したルールの Firepower システム プリプロセッサの ID 番号。
ルールリビジョン	uint32	ルールリビジョン番号。
予約済み	uint8[20]	このフィールドは現在使用されていません。

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。



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。

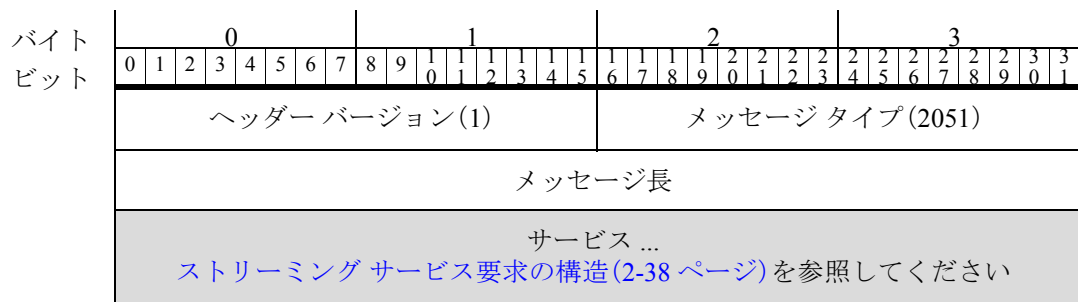
表 2-16

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ます、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\(2-38 ページ\)](#)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、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。

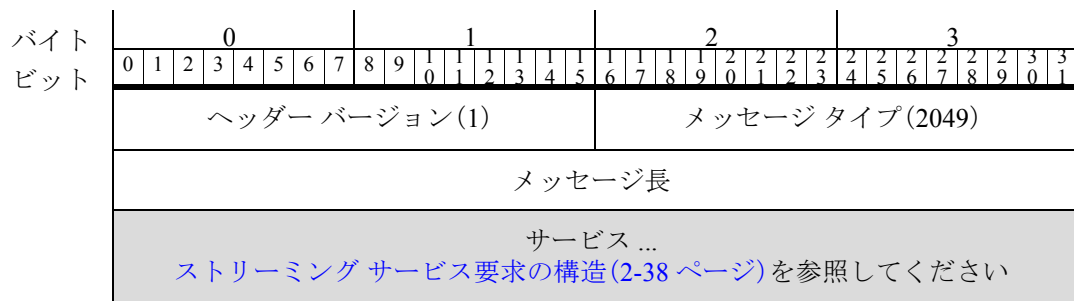
表 2-17 ストリーミング情報メッセージのフィールド(続き)

フィールド	データタイプ	説明
メッセージ長	uint32	メッセージヘッダーの後のメッセージのコンテンツの長さ。[ヘッダーバージョン(Header Version)], [メッセージタイプ(Message Type)], および [メッセージ長(Message Length)] フィールドのバイトは含まれません。
サービス [] (Service[])	アレイ	使用できるサービスのリスト。ストリーミングサービス要求の構造(2-38 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(2-38 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、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。
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(2-38 ページ)を参照してください。

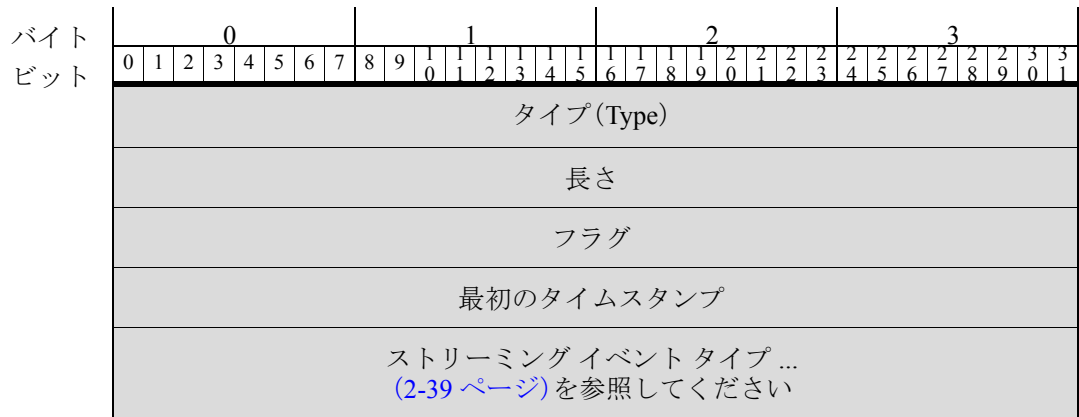
ストリーミング サービス要求の構造

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

クライアントは、eStreamer からのストリーミング サービス要求構造を処理し、サーバに返す応答で同じ構造を使用します。クライアントがサーバに送信するストリーミング サービス要求には、最初に、eStreamer によってアダ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、(2-39 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

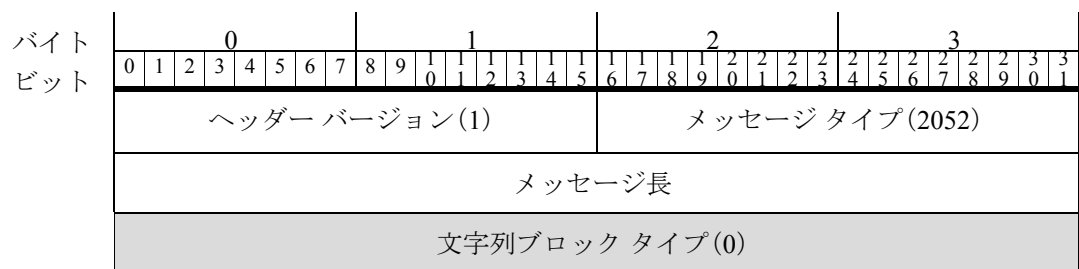
フィールド	データタイプ	説明
タイプ (Type)	uint32	[サービス ID (Service ID)]. eStreamer サーバ メッセージでは、これによって利用可能なサービスがアダバタイズされます。 クライアント メッセージでは、要求されたサービスが指定されます。 現在の有効なオプション: <ul style="list-style-type: none"> 6667 (eStreamer サービスの場合)

表 2-19 ストリーミングサービス要求フィールド(続き)

フィールド	データタイプ	説明
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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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。(2-39 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。(2-39 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、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 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(2-41 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(2-41 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関連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 9:6.0+	12
メタデータ	1:3.2 ~ 4.5.x 2:4.6.0.x 3:4.6.1 ~ 4.6.x 4:4.7+	21
関連およびコンプライアンスのホワイトリストイベント	1:3.2 以前 2:4.0 ~ 4.4.x 3:4.5 ~ 4.6.1 4:4.7 ~ 4.8.0.1 5:4.8.0.2 ~ 4.9.1.x 6:4.10.0 ~ 4.10.x 7:5.0 ~ 5.0.2 8:5.1 ~ 5.3.x 9:5.4+	31

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
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
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 16:6.2+	71
ユーザ イベント	1:4.7 ~ 4.10.x 2:5.0.x 3:5.1 ~ 5.1.x 4:5.2 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 7:6.0+	101
ファイル イベント	1:5.1.1 ~ 5.1.x 2:5.2.x 3:5.3 4:5.3.1 5:5.4.x 6:6.0+	111

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
影響関連イベント	1:5.2.x 以前 2:5.3+	131
リスト内の終了イベントタイプ	0	0

拡張要求メッセージの例

ストリーミング情報メッセージ

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

表 2-23

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	36	/*payload bytes*/
サービス [1]. タイプ	6667	/*eStreamer service ID*/
サービス [1]. 長さ	20	
サービス [1]. フラグ	30	/*original flags value*/
サービス [1]. 最初のタイムスタンプ	0	/*original timestamp*/
サービス [1]. イベント [1]. バージョン	6	/*version 6*/
サービス [1]. イベント [1]. タイプ	71	/*connection events*/
サービス [1]. イベント [2]. バージョン	4	/* version 4*/
サービス [1]. イベント [2]. タイプ	21	/*metadata*/
サービス [1]. イベント [3]. バージョン	0	/*terminate event list*/
サービス [1]. イベント [3]. タイプ	0	/*terminate event list*/

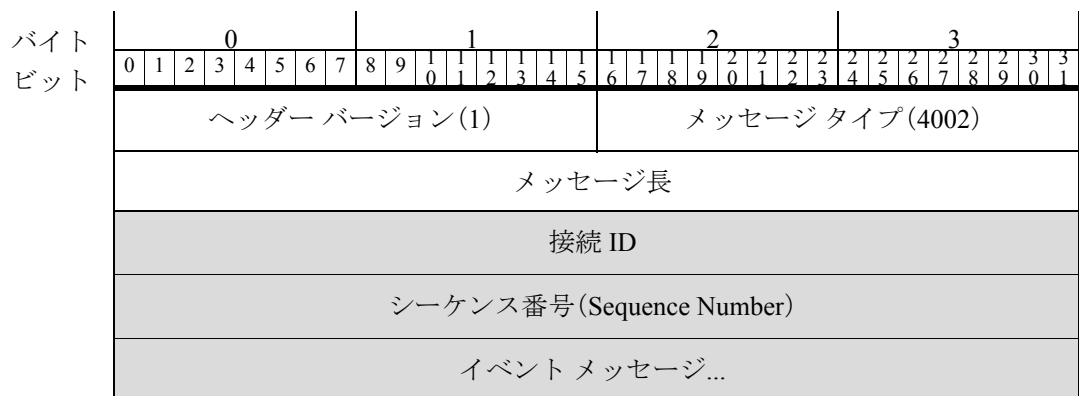
メッセージバンドルの形式

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

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

メッセージバンドルのメッセージタイプは 4002 です。

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

メタデータについて

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

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。



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\(2-19 ページ\)](#)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 つ以上のレベルの変長フィールド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(Block Type)	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(3-7 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)

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(Block Type)	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	20	1	侵入の影響アラート	レガシー	侵入影響アラート データ (B-48 ページ)
9	153	1	侵入の影響アラート	現在 (Current)	侵入の影響アラート データ 5.3 以上 (3-18 ページ)
62	該当なし	2	ユーザ メタデータ	現在 (Current)	ユーザ レコード (3-21 ページ)
66	該当なし	該当なし	ルール メッセージのメタデータ (バージョン 4.6.1 以上)	現在 (Current)	4.6.1 以上のルール メッセージのレコード (3-22 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 (3-23 ページ)
69	該当なし	該当なし	関連ポリシーのメタデータ (バージョン 4.6.1 以上)	現在 (Current)	関連ポリシー レコード (3-25 ページ)
70	該当なし	該当なし	関連ルールのメタデータ (バージョン 4.6.1 以上)	現在 (Current)	関連ルール レコード (3-26 ページ)
104	該当なし	該当なし	侵入イベント (IPv4) レコード 4.9 ~ 4.10.x	レガシー	製品の旧バージョン
105	該当なし	該当なし	侵入イベント (IPv6) レコード 4.9 ~ 4.10.x	レガシー	製品の旧バージョン
110	4	2	侵入イベント追加データ (バージョン 4.10.0 以上)	現在 (Current)	侵入イベント追加データレコード (3-28 ページ)
111	5	2	侵入イベント追加データのメタデータ (バージョン 4.10.0 以上)	現在 (Current)	侵入イベント追加データのメタデータ (3-30 ページ)
112	128	1	5.1 ~ 5.3.x の関連イベント	レガシー	関連イベント 5.1 ~ 5.3.x (B-283 ページ)
112	156	1	5.4 以上の関連イベント	現在 (Current)	5.4 以上の関連イベント (3-45 ページ)
115	18	2	セキュリティゾーン名のメタデータ	現在 (Current)	セキュリティゾーン名レコード (3-31 ページ)
116	18	2	インターフェイス名のメタデータ	現在 (Current)	インターフェイス名レコード (3-33 ページ)
117	18	2	アクセスコントロールポリシー名メタデータ	現在 (Current)	アクセスコントロールポリシー名のレコード (3-34 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)

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 (Block Type)	シリーズ	説明	レコードステータス	データ形式の参照先...
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 (3-35 ページ)
120	該当なし	該当なし	アクセス コントロール ルール アクションのメタデータ	現在 (Current)	アクセス コントロール ルール アクション レコード メタデータ (4-24 ページ)
121	該当なし	該当なし	URL カテゴリのメタデータ	現在 (Current)	URL カテゴリ レコード メタデータ (4-25 ページ)
122	該当なし	該当なし	URL レピュテーション メタデータ	現在 (Current)	URL レピュテーション レコード メタデータ (4-26 ページ)
123	該当なし	該当なし	管理対象 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 (3-37 ページ)
該当なし	64	2	アクセス コントロール 名のデータ ブロック	現在 (Current)	アクセス コントロール ポリシー名のデータ ブロック (3-83 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 (3-82 ページ)
125	該当なし	2	マルウェア イベント レコード (バージョン 5.1.1 以上)	現在 (Current)	マルウェア イベント レコード 5.1.1 以上 (3-38 ページ)
125	24	2	マルウェア イベント (バージョン 5.1.1 以上)	現在 (Current)	マルウェア イベント データ ブロック 5.1.1.x (B-55 ページ)
125	33	2	マルウェア イベント (バージョン 5.2.x)	レガシー	マルウェア イベント データ ブロック 5.2.x (B-61 ページ)
125	35	2	マルウェア イベント (バージョン 5.3)	レガシー	マルウェア イベントのデータ ブロック 5.3 (B-68 ページ)
125	44	2	マルウェア イベント (バージョン 5.3.1)	レガシー	マルウェア イベント データ ブロック 5.3.1 (B-76 ページ)
125	47	2	マルウェア イベント (バージョン 5.4.x)	現在 (Current)	マルウェア イベント データ ブロック 5.4.x (B-83 ページ)
125	62	2	マルウェア イベント (バージョン 6.0 以上)	現在 (Current)	マルウェア イベントのデータ ブロック 6.0 以上 (3-97 ページ)
127	18	2	Cisco Advanced Malware Protection クラウドのメタデータ (バージョン 5.1 以上)	現在 (Current)	Cisco Advanced Malware Protection クラウド名のメタデータ (3-39 ページ)
128	該当なし	該当なし	マルウェア イベント タイプのメタデータ (バージョン 5.1 以上)	現在 (Current)	マルウェア イベント タイプのメタデータ (3-40 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 (Block Type)	シリーズ	説明	レコードステータス	データ形式の参照先...
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 (3-41 ページ)
130	該当なし	該当なし	エンドポイント向け AMP デテクタ 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 デテクタ タイプのメタデータ (3-42 ページ)
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 (3-43 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 (3-44 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 (3-111 ページ)
207	該当なし	該当なし	侵入イベント (IPv4) レコード 5.0.x ~ 5.1	レガシー	侵入イベント (IPv4) レコード 5.0.x ~ 5.1 (B-2 ページ)
208	該当なし	該当なし	侵入イベント (IPv6) レコード 5.0.x ~ 5.1	レガシー	侵入イベント (IPv6) レコード 5.0.x ~ 5.1 (B-8 ページ)
260	19	2	ICMP タイプ データのデータ ブロック	現在 (Current)	ICMP タイプのデータ ブロック (3-70 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 (3-71 ページ)
282	該当なし	2	5.4.1 以上のセキュリティ インテリジェンス カテゴリのメタデータ	現在 (Current)	5.4.1 以上のセキュリティ インテリジェンス カテゴリのメタデータ (3-72 ページ)
300	該当なし	該当なし	6.0 以上のレルムのメタデータ	現在 (Current)	6.0 以上のレルムのメタデータ (3-73 ページ)
301	58	2	6.0 以上のエンドポイント プロファイル	現在 (Current)	6.0 以上のエンドポイント プロファイルのデータ ブロック (3-74 ページ)
302	該当なし	該当なし	6.0 以上のセキュリティ グループのメタデータ	現在 (Current)	6.0 以上のセキュリティ グループのメタデータ (3-76 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 (3-77 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 (Block Type)	シリーズ	説明	レコードステータス	データ形式の参照先...
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 (3-78 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 (3-80 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 (3-81 ページ)
400	34	2	侵入イベント レコード 5.2.x	レガシー	侵入イベント レコード 5.2.x (B-14 ページ)
400	41	2	侵入イベント レコード 5.3	レガシー	侵入イベント レコード 5.3 (B-20 ページ)
400	42	2	侵入イベント レコード 5.3.1	レガシー	侵入イベント レコード 5.3.1 (B-32 ページ)
400	45	2	侵入イベント レコード 5.4.x	レガシー	侵入イベント レコード 5.4.x (B-39 ページ)
400	60	2	侵入イベント レコード 6.0 以上	現在 (Current)	侵入イベント レコード 6.0 以上 (3-9 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	ファイル イベント 5.2.x (B-244 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	ファイル イベント 5.3 (B-249 ページ)
500	43	2	ファイル イベント (バージョン 5.3.1)	レガシー	ファイル イベント 5.3.1 (B-256 ページ)
500	46	2	ファイル イベント (バージョン 5.4 以上)	現在 (Current)	6.0 以上のファイル イベント (3-86 ページ)
502	32	2	ファイル イベント (バージョン 5.2.x)	レガシー	ファイル イベント 5.2.x (B-244 ページ)
502	38	2	ファイル イベント (バージョン 5.3)	レガシー	ファイル イベント 5.3 (B-249 ページ)
502	43	2	ファイル イベント (バージョン 5.3.1)	レガシー	ファイル イベント 5.3.1 (B-256 ページ)
502	46	2	ファイル イベント (バージョン 5.4.x)	現在 (Current)	ファイル イベント 5.4.x (B-262 ページ)
502	56	2	ファイル イベント (バージョン 6.0 以上)	現在 (Current)	6.0 以上のファイル イベント (3-86 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 (3-110 ページ)
511	26	2	5.11 ~ 5.2.x のファイル イベント SHA ハッシュ	レガシー	ファイル イベント SHA ハッシュ 5.1.1 ~ 5.2.x (B-273 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 (Block Type)	シリーズ	説明	レコードステータス	データ形式の参照先...
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 (3-108 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 (3-115 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 (3-116 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 (3-117 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 (3-118 ページ)
519	該当なし	該当なし	6.0 以上の Filelog スタティック分析のメタデータ	現在 (Current)	6.0 以上の Filelog スタティック分析のメタデータ (3-118 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 (3-119 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 (3-120 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 (3-122 ページ)
601	51	2	SSL ルール ID	現在 (Current)	SSL ルール ID (3-123 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 (3-131 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 (3-125 ページ)
605	該当なし	該当なし	SSL サーバ証明書ステータス	現在 (Current)	SSL サーバ証明書ステータス (3-126 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 (3-127 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 (3-128 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 (3-129 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 (3-130 ページ)

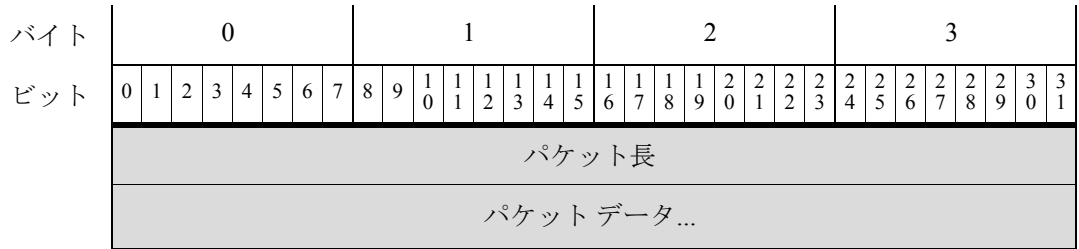
表 3-1 侵入イベントと一般的なメタデータのレコードタイプ(続き)

レコードタイプ	ブロックタイプ (Block Type)	シリーズ	説明	レコードステータス	データ形式の参照先...
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 (3-131 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 (3-135 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 \(2-13 ページ\)](#) を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。メッセージ長フィールドの後に表示されるレコードタイプフィールドにパケット レコードを示す値 2 があることに注意してください。

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



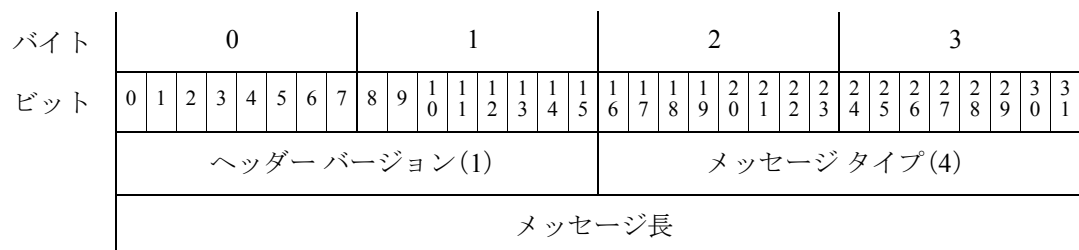
次の表は、パケット レコードのフィールドについての説明です。

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 (3-37 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。
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 \(2-13 ページ\)](#) 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。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Netmap ID																レコードタイプ(4)															
	レコード長																															
	プライオリティ ID																															
	名前の長さ																プライオリティ名...															

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 6.0 以上

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(400)															
	レコード長																															
	eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															

■ 侵入イベントとメタデータのレコードタイプ

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

■ 侵入イベントとメタデータのレコードタイプ

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

次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 3-4 侵入イベント レコード 6.0 以上のフィールド

フィールド	データタイプ	説明
ブロックタイプ	uint32	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	uint32	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)	uint32	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 (3-37 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 Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポートまたは ICMP タイプ	uint16	イベントプロトコルタイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
送信先ポートまたは ICMP コード	uint16	イベントプロトコルタイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル ID	uint8	IANA 指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none"> • 0:IP • 1:ICMP • 6:TCP • 17:UDP

表 3-4 侵入イベント レコード 6.0 以上のフィールド(続き)

フィールド	データタイプ	説明
影響フラグ	bits[8]	<p>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。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) <p>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。</p> <ul style="list-style-type: none"> グレー(0、不明):00x00000 赤(1、脆弱):xxx1xxx, 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	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> 1:レッド(脆弱) 2:オレンジ(脆弱の可能性あり) 3:イエロー(現在は脆弱でない) 4:ブルー(不明なターゲット) 5:グレー(不明なインパクト)

表 3-4 侵入イベントレコード 6.0 以上のフィールド(続き)

フィールド	データタイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 <ul style="list-style-type: none"> 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 ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
インターフェイス入力 UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
インターフェイス出力 UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
セキュリティゾーン入力 UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
セキュリティゾーン出力 UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970年1月1日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。

表 3-4 侵入イベント レコード 6.0 以上のフィールド(続き)

フィールド	データタイプ	説明
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。 <ul style="list-style-type: none"> • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 3-4 侵入イベントレコード 6.0 以上のフィールド(続き)

フィールド	データタイプ	説明
SSL フロース ステータス	uint16	<p>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。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」

表 3-4 侵入イベント レコード 6.0 以上のフィールド(続き)

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

侵入の影響アラート データ 5.3 以上

侵入の影響アラート 5.3 以上のイベントには影響イベントに関する情報が表示されます。これは、侵入イベントがシステム ネットワーク マップ データと比較され、影響が判別されているときに送信されます。レコードタイプ 9 の標準レコードヘッダーを使用します。この後にシリーズ 1 グループのブロックのシリーズ 1 のデータ ブロック タイプが 153 の侵入の影響アラートのデータ ブロックが続きます。(影響アラート データ ブロック タイプは、シリーズ 1 データ ブロックです。シリーズ 1 データ ブロックの詳細については、[ディスカバリ \(シリーズ 1\) ブロック \(4-65 ページ\)](#) 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 \(2-11 ページ\)](#) を参照してください。これらのアラートのバージョン 1 は、IPv4 のみを処理します。5.3 で導入されたバージョン 2 は、IPv4 に加えて IPv6 イベントを処理します。

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

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

次の表は、影響イベントの各データ フィールドについての説明です。

表 3-5 影響イベントデータ フィールド

フィールド	データタイプ	説明
侵入影響アラート ブロック タイプ	uint32	侵入影響アラートデータ ブロックが続くことを示します。このフィールドの値は、常に 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]	<p>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。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれません。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) <p>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。</p> <ul style="list-style-type: none"> 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]	<p>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(1-5 ページ)を参照してください。</p>
宛先 IP アドレス	uint8[16]	<p>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(1-5 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。</p>

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。

ユーザレコード

メタデータを要求すると、Firepower システムのコンポーネントによって生成されたイベントで参照されるユーザに関する情報を取得できます。eStreamer サービスは、ユーザレコード内のイベントのユーザ情報を含むメタデータを送信します。形式は次のとおりです。ユーザレコードには、ユーザ ID と対応する名前が含まれています。ユーザ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 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、ユーザ情報が送信されます。[要求フラグ \(2-13 ページ\)](#) 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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	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(62)																							
	レコード長																																							
	ユーザ ID (User ID)																																							
	名前の長さ																																							
	名前...																																							

次の表は、ユーザレコードのフィールドについての説明です。

表 3-6 ユーザレコードのフィールド

フィールド	データタイプ	説明
[ユーザ ID (User ID)]	uint32	ユーザ 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	ユーザ名に含まれるバイト数。
[名前 (Name)]	string	ユーザの名前。

4.6.1 以上のルールメッセージのレコード

イベントのルールメッセージ情報は、ルールメッセージレコード内で送信されます。形式は次のとおりです。eStreamer サービスは、バージョン 2 またはバージョン 3 のメタデータを要求すると、4.6.1 以上のルールメッセージのレコードを送信します。4.6.1 以上のルールメッセージのレコードには、4.6 以前のルールメッセージのレコードと同じフィールドのほかに、UUID およびリビジョン UUID フィールドが新たに加われました。(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(2-13 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。

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

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

次の表は、各ルール固有のフィールドについての説明です。

表 3-7 ルールメッセージのレコードのフィールド

フィールド	データタイプ	説明
ジェネレータ ID	uint32	ジェネレータ ID 番号。
ルール ID	uint32	ローカル コンピュータのルール ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。これは、すべてのルール メッセージで 0 に現在設定されています。
表示されるシグネチャ ID	uint32	Firepower システム インターフェイスに表示されるルール ID 番号。
メッセージ長	uint16	ルールのテキストに含まれるバイト数。
UUID	uint8[16]	ルールの固有識別子として機能するルール ID 番号。
リビジョン UUID	uint8[16]	リビジョンの固有識別子として機能するルール リビジョン ID 番号。
メッセージ	変数 (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 \(2-13 ページ\)](#) を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに分類バージョン 2 のレコードを示す値 67 があることに注意してください。

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

次の表は、分類レコードのフィールドについての説明です。

表 3-8 分類レコードフィールド

フィールド	データタイプ	説明
分類 ID	uint32	分類 ID 番号。
名前の長さ	uint16	名前に含まれるバイト数。
[名前(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。

関連ポリシーレコード

eStreamer サービスは、関連ポリシーレコード内の関連イベントの関連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、関連ポリシー情報が送信されます。[要求フラグ \(2-13 ページ\)](#)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関連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	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(69)															
	レコード長																															
	関連ポリシー ID																															
	名前の長さ																名前...															
	説明の長さ																説明...															
関連ポリシー UUID	関連ポリシー UUID 関連ポリシー UUID(続き) 関連ポリシー UUID(続き) 関連ポリシー UUID(続き)																															
関連ポリシー リビジョン UUID	関連ポリシー リビジョン UUID 関連ポリシー リビジョン UUID(続き) 関連ポリシー リビジョン UUID(続き) 関連ポリシー リビジョン UUID(続き)																															

次の表は、関連ポリシー レコードのフィールドについての説明です。

表 3-9 関連ポリシー レコードフィールド

フィールド	データタイプ	説明
関連ポリシー ID	uint32	関連ポリシー 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	関連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関連ポリシーの名前。
説明の長さ	uint16	関連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関連ポリシーの説明。
UUID	uint8[16]	関連ポリシーの固有識別子として機能する関連ポリシー ID 番号。
リビジョン UUID	uint8[16]	関連ポリシーの固有識別子として機能する関連ポリシー リビジョン ID 番号。

関連ルール レコード

eStreamer サービスは、関連ルール レコード内の関連イベントをトリガーした関連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、関連ルール情報が送信されます。[要求フラグ\(2-13 ページ\)](#)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関連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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(70)															
	レコード長																															
	関連ルール ID																															
	名前の長さ																名前...															
	名前...																説明の長さ															
	説明...																															
	イベントタイプの長さ																イベントタイプ...															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
関連ルール UUID	イベントタイプ...																関連ルール UUID															
	関連ルール UUID(続き)																関連ルール UUID(続き)															
	関連ルール UUID(続き)																関連ルール UUID(続き)															
関連ルール リビジョン UUID	関連ルール UUID(続き)																関連リビジョン UUID															
	関連ルール リビジョン UUID(続き)																関連ルール リビジョン UUID(続き)															
	関連ルール リビジョン UUID(続き)																関連ルール リビジョン UUID(続き)															
ホワイトリス トルール UUID	関連ルール リビジョン UUID(続き)																ホワイトリストルール UUID															
	ホワイトリストルール UUID(続き)																ホワイトリストルール UUID(続き)															
	ホワイトリストルール UUID(続き)																ホワイトリストルール UUID(続き)															
	ホワイトリストルール UUID(続き)																															

次の表は、関連ルール レコードのフィールドについての説明です。

表 3-10 関連ルール レコードフィールド

フィールド	データタイプ	説明
関連ルール ID	uint32	関連ルール 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	関連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関連ルールの名前。
説明の長さ	uint16	関連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関連ルールの説明。
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	関連ルールをトリガーしたイベントの説明。
UUID	uint8[16]	関連ルールの固有識別子として機能する関連ルール ID 番号。

表 3-10 関連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]	関連ルール リビジョンの固有識別子として機能する関連ルール リビジョン ID 番号。
ホワイトリスト UUID	uint8[16]	ホワイトリスト違反の結果として送信されるイベントの固有識別子として機能する関連 ID 番号。

侵入イベント追加データレコード

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

イベント追加データは、カプセル化されたイベント追加データのデータブロックに表示されます。データブロックタイプの値は常に 4 です。(イベント追加データのデータブロックは、シリーズ 2 のデータブロックです。シリーズ 2 のデータブロックの詳細については、[シリーズ 2 のデータブロックの概要\(3-58 ページ\)](#)を参照してください)。

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

要求メッセージの [要求フラグ (Request Flags)] フィールドにビット 27 を設定すると、各侵入イベントのイベント追加データを受信します。ビット 20 を設定すると、[侵入イベント追加データのメタデータ\(3-30 ページ\)](#)に記載されているイベント追加データのメタデータも受信されます。ビット 23 を有効にすると、eStreamer は拡張イベントヘッダーを表示します。要求フラグの設定方法の詳細については、[要求フラグ\(2-13 ページ\)](#)を参照してください。

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

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

次の表は、侵入イベント追加データ レコードのフィールドについての説明です。

表 3-11 侵入イベント追加データのデータ ブロック フィールド

フィールド	データ タイプ	説明
イベント追加データのデータ ブロック タイプ	uint32	イベント追加データのデータ ブロックを開始します。この値は常に 4 です。ブロック タイプは、シリーズ 2 ブロックです。詳細については、 シリーズ 2 のデータ ブロックの概要 (3-58 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。 <ul style="list-style-type: none"> 2: XFF クライアント (IPv6) 9: HTTP URI
BLOB ブロック タイプ	uint32	追加データを含む BLOB データ ブロックを開始します。この値は常に 1 です。ブロック タイプは、シリーズ 2 ブロックです。
長さ (Length)	uint32	BLOB データ ブロックの合計バイト数。
追加データ	変数 (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。

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 \(2-13 ページ\)](#) を参照してください。ビット 23 を有効にすると、拡張イベントヘッダーがレコードに含まれます。

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

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

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

表 3-12 イベント追加データのメタデータのデータブロック フィールド

フィールド	データタイプ	説明
イベント追加データのメタデータのデータブロックタイプ	uint32	イベント追加データのメタデータのデータブロックを開始します。この値は常に 5 です。このブロックタイプは、シリーズ 2 ブロックです。
イベント追加データのメタデータのデータブロック長	uint32	データブロックの長さ。データのバイト数に 2 つのデータブロックヘッダーフィールドの 8 バイトを加えたバイト数です。
タイプ (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)。

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 \(2-13 ページ\)](#) 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	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(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 3-13 セキュリティゾーンの名のデータブロック フィールド

フィールド	データタイプ	説明
セキュリティゾーン名のデータブロックタイプ	uint32	セキュリティゾーン名のデータブロックを開始します。この値は常に 14 です。ブロックタイプは、シリーズ 2 ブロックです。
セキュリティゾーン名のデータブロック長	uint32	データブロックの長さ。データのバイト数に 2 つのデータブロックヘッダーフィールドの 8 バイトを加えたバイト数です。
セキュリティゾーン UUID	uint8[16]	接続イベントに関連付けられたセキュリティゾーンの固有識別子。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\(2-13 ページ\)](#)を参照してください)。メッセージ長フィールドの後に表示されるレコードタイプフィールドにインターフェイス名レコードを示す値 116 があることに注意してください。シリーズ2セットのデータブロックのブロックタイプ14のUUID文字列データブロックが含まれています。

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

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

表 3-14 インターフェイス名のデータブロックフィールド

フィールド	データタイプ	説明
インターフェイス名のデータブロックタイプ	uint32	インターフェイス名のデータブロックを開始します。この値は常に 14 です。ブロックタイプは、シリーズ2ブロックです。
インターフェイス名のデータブロック長	uint32	データブロックの長さ。データのバイト数に2つのデータブロックヘッダーフィールドの8バイトを加えたバイト数です。
インターフェース 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。

表 3-14 インターフェイス名のデータブロック フィールド(続き)

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

アクセスコントロールポリシー名のレコード

eStreamer サービスは、アクセスコントロールポリシー名レコード内の侵入イベントまたは接続イベントをトリガーしたアクセスコントロールポリシーの名前に関するメタデータを送信します。形式は次のとおりです。(バージョン 4 のメタデータフラグ(要求メッセージの [要求フラグ (Request Flags)] フィールドのビット 20) が設定されていると、アクセスコントロールポリシー名の情報が送信されます。[要求フラグ\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(117)															
	レコード長																															
	アクセスコントロールポリシー名のデータブロック(14)																															
	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																															
	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ポリシー名...																															

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

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

フィールド	データタイプ	説明
アクセス コントロール ポリシー名のデータ ブロック タイプ	uint32	アクセス コントロール ポリシー名のデータ ブロックを開始します。この値は常に 14 です。ブロック タイプは、シリーズ 2 ブロックです。
アクセス コントロール ポリシー名のデータ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
アクセス コントロール ポリシー UUID	uint8[16]	侵入イベントまたは接続イベントに関連付けられたアクセス コントロール ポリシーの固有識別子として機能する ID 番号このフィールドは、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\(2-13 ページ\)](#)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	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(119)															
	レコード長																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	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 3-16 アクセス コントロールルール ID のデータ ブロック フィールド

フィールド	データタイプ	説明
アクセス コントロールルール ID のデータ ブロック タイプ	uint32	アクセス コントロールルール ID のデータ ブロックを開始します。この値は常に 15 です。ブロック タイプは、シリーズ 2 ブロックです。
アクセス コントロールルール ID のデータ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
アクセス コントロールルール UUID	uint8[16]	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。

表 3-16 アクセスコントロールルールID のデータ ブロック フィールド(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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(123)															
	レコード長																															
	Device ID																															
	名前の長さ																															
	名前...																															

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 3-17 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 \(2-13 ページ\)](#) 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	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(125)															
	レコード長																															
	eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
	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 3-18 マルウェア イベントレコードフィールド

フィールド	データタイプ	説明
マルウェア イベントのデータブロック	変数 (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 6.0 以上 (3-97 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 \(2-13 ページ\)](#) 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	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(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)																															
	Cisco Advanced Malware Protection クラウド UUID (続き)																															
	Cisco Advanced Malware Protection クラウド UUID (続き)																															
	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	Cisco Advanced Malware Protection クラウド名前...																															

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 3-19 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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Netmap ID																レコードタイプ(128)															
	レコード長																															
	マルウェア イベント タイプ ID																															
	マルウェア イベント タイプの長さ																															
	マルウェア イベント タイプ...																															

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

表 3-20 マルウェア イベント タイプ レコード フィールド

フィールド	データタイプ	説明
マルウェア イベント タイプ ID	uint32	マルウェア イベント タイプ ID 番号。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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(129)															
	レコード長																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
マルウェア イベント サブタイプ ID																																
マルウェア イベント サブタイプの長さ																																
マルウェア イベント サブタイプ...																																

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

表 3-21 マルウェア イベント サブタイプ レコード フィールド

フィールド	データタイプ	説明
マルウェア イベント サブタイプ ID	uint32	マルウェア イベント サブタイプ ID 番号。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 \(2-13 ページ\)](#) 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(130)																
レコード長																																
エンドポイント向け AMP ディテクタ タイプ ID																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
エンドポイント向け AMP ディテクタ タイプの長さ																																
エンドポイント向け AMP ディテクタ タイプ...																																

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 3-22 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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダーバージョン(1)																メッセージタイプ(4)																
メッセージ長																																
Netmap ID																レコードタイプ(131)																
レコード長																																
エンドポイント向け AMP ファイルタイプ ID																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
エンドポイント向け AMP ファイル タイプの長さ																																
エンドポイント向け AMP ファイル タイプ...																																

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 3-23 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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(132)																
レコード長																																
セキュリティ コンテキスト UUID																																
セキュリティ コンテキスト UUID(続き)																																
セキュリティ コンテキスト UUID(続き)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
セキュリティ コンテキスト 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 コンテキスト名...																																

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

表 3-24 セキュリティ コンテキスト名のレコード フィールド

フィールド	データタイプ	説明
セキュリティ コンテキスト UUID	uint8[16]	セキュリティ コンテキストの UUID。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 以上の関連イベント

関連イベント (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、関連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 の関連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 以上の関連イベントには、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 以上の関連イベントを要求できます (拡張要求の送信の詳細については、[拡張要求の送信 \(2-4 ページ\)](#) を参照してください)。オプションで、最初のイベントストリーム要求メッセージのフラグフィールドでビット 23 を有効にして、拡張イベントヘッダーを含めることができます。また、フラグフィールドでビット 20 を有効にして、ユーザメタデータを含めることもできます。

■ 侵入イベントとメタデータのレコードタイプ

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(112)															
	レコード長																															
	eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
	関連ブロックのタイプ(156)																															
	関連ブロック長																															
	デバイス ID(Device ID)																															
	(関連)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)																イベント 説明															
	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																															
	(トリガー)イベントマイクロ秒																															
	イベント ID(Event 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	
	イベントで定義されたマスク																																
	イベント影響フラグ								IP プロトコル								ネットワーク プロトコル																
	ソース IP																																
	送信元ホストタイプ								送信元 VLAN ID																送信元 OS フィンガープリント UUID								送信元 OS フィンガー プリント UUID
	送信元 OS フィンガープリント UUID (続き)																																
	送信元 OS フィンガープリント UUID (続き)																																
	送信元 OS フィンガープリント UUID (続き)																																
	送信元 OS フィンガープリント UUID (続き)																送信元重要度																
	送信元重要度 (続き)								送信元ユーザ ID																								
	送信元ユーザ ID (続き)								送信元ポート																送信元サーバ ID								
	送信元サーバ ID (続き)																宛先 IP (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 ID (User ID)																																
	接続先ポート																宛先サーバ ID																
	宛先サーバ ID (続き)																影響								ブロック								
	侵入ポリシー (Intrusion Policy)																																

■ 侵入イベントとメタデータのレコードタイプ

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
	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)																																NetBIOS ド メイン (NetBIOS Domain)
	文字列ブロック長																																
	NetBIOS ドメイン...																																
	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)																																URL
	文字列ブロック長																																
	URL...																																
	Client ID																																
	文字列ブロック タイプ(0)																																クライアン ト バージョ ン (Client Version)
	文字列ブロック長																																
	クライアント バージョン...																																
	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)																																
	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)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出力インターフェイス UUID																																
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																																
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)																																

■ 侵入イベントとメタデータのレコードタイプ

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
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 3-25 関連イベント 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
関連ブロック タイプ	uint32	関連イベント 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。
関連ブロック 長	uint32	関連データ ブロック長(関連ブロック タイプと長さの 8 バイト、およびそれに続く関連データを含む)。

表 3-25 関連イベント 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
デバイス ID (Device ID)	uint32	関連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 (3-37 ページ) を参照してください。
(関連) イベント秒	uint32	関連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	関連イベント ID 番号。
ポリシー ID	uint32	違反された関連ポリシーの 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関連ルールの 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	関連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	関連イベントについての説明。
イベントタイプ (Event Type)	uint8	関連イベントが、侵入、ホスト検出、またはユーザ イベントによってトリガーされたかどうかを示します。 <ul style="list-style-type: none"> • 1: 侵入 • 2: ホストの検出 • 3: ユーザ
イベントデバイス ID	uint32	関連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 (3-37 ページ) を参照してください。
シグネチャ ID	uint32	イベントが侵入イベントであった場合、イベントに対応するルール ID 番号を示します。そうでない場合、この値は 0 になります。
シグネチャジェネレータ ID	uint32	イベントが侵入イベントであった場合、イベントを生成した Firepower システム プリプロセッサまたはルールエンジンの ID 番号を示します。
(トリガー) イベント秒	uint32	関連ポリシー 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 3-25 相関イベント 5.4 以上のデータ フィールド(続き)

フィールド	データタイプ	説明
(トリガー)イベントマイクロ秒	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ことを示します。各ビット値のリストの詳細については、表 3-23(3-44 ページ)を参照してください。
イベント影響フラグ	bits[8]	<p>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。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) <p>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。</p> <ul style="list-style-type: none"> 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

表 3-25 関連イベント 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
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(1-5 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: <ul style="list-style-type: none"> 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、ユーザ定義の重要度値: <ul style="list-style-type: none"> 0: なし 1: 低 2: 中 3: 高
送信元ユーザ ID	uint32	システムにより識別される、送信元ホストにログインしたユーザの ID 番号。
送信元ポート	uint16	イベントの送信元ポート。
送信元サーバ ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
宛先 IP アドレス	uint8[4]	このフィールドは予約済みですが、設定されておりません。宛先 IPv4 アドレスは、宛先 IPv6 アドレス フィールドに保存されます。詳細については、 IP アドレス(1-5 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: <ul style="list-style-type: none"> 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 3-25 関連イベント 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 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、ユーザ定義の重要度値: <ul style="list-style-type: none"> • 0:なし • 1:低 • 2:中 • 3:高
宛先ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
接続先ポート	uint16	イベントの宛先ポート。
宛先サービス ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
影響	uint8	イベントの影響フラグ値。値は次のとおりです。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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 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。

表 3-25 関連イベント 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
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 (4-25 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 (4-26 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。
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]	トリガーされた関連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]	関連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]	関連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]	関連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]	関連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。

表 3-25 関連イベント 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 IPv6 アドレス	uint8[16]	IPv6 アドレス オクテットの、イベントの宛先ホストの IP アドレス。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
セキュリティ インテリジェンス UUID	uint8[16]	セキュリティ インテリジェンスに設定されたアクセス コントロール ポリシーの UUID。
セキュリティ コンテキスト	uint8[16]	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL ポリシー ID	uint8[16]	接続を処理した SSL ポリシーの ID 番号。
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルト アクションの ID 番号。
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。 <ul style="list-style-type: none"> • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 3-25 関連イベント 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	<p>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。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。

シリーズ2のデータブロックの概要

バージョン 4.10.0 から、eStreamer サービスは、2 番目のシリーズのデータブロックを使用して、侵入イベント追加データなどの特定のレコードをパッケージしています。このシリーズのすべてのブロックタイプのリストの詳細については、表 3-26(3-58 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を示します。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。

バイト	0								1								2								3											
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	2	2	2	2	2	2	2	2	2	2	2	3	3
	リストデータブロックタイプ(2)																																			
	データブロック長																																			
サーバ フィンガー プリント	オペレーティングシステムフィンガープリントブロックタイプ(87)*																																			
	オペレーティングシステムフィンガープリントブロック長																																			
	オペレーティングシステムサーバフィンガープリントデータ																																			

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

表 3-26 シリーズ2のブロックタイプ

タイプ (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(3-63 ページ) を参照してください。
1	BLOB	現在 (Current)	バイナリデータをカプセル化し、バナー専用として使用します。詳細については、 BLOB データブロック(3-63 ページ) を参照してください。
2	リスト	現在 (Current)	他のデータブロックのリストをカプセル化します。詳細については、 リストデータブロック(3-64 ページ) を参照してください。

表 3-26 シリーズ2のブロックタイプ(続き)

タイプ (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 (3-65 ページ) を参照してください。
4	イベント追加データ	現在 (Current)	侵入イベント追加データが含まれています。詳細については、 侵入イベント追加データレコード (3-28 ページ) を参照してください。
5	追加データタイプ	現在 (Current)	追加データのメタデータが含まれています。詳細については、 侵入イベント追加データのメタデータ (3-30 ページ) を参照してください。
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 (3-66 ページ) を参照してください。
15	アクセスコントロールポリシールール ID のメタデータ	現在 (Current)	アクセスコントロールルールのメタデータが含まれています。 アクセスコントロールポリシールール ID のメタデータブロック (3-68 ページ) を参照してください。
16	マルウェア イベント	レガシー	Cisco Advanced Malware Protection 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-51 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-76 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 (3-70 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 (3-71 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 (3-82 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 (3-83 ページ) を参照してください。

表 3-26 シリーズ2のブロックタイプ(続き)

タイプ (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-240 ページ)を参照してく ださい。これはブロック 32 に取って代わられますアク セス コントロール ポリシー ルール ID のメタデータ ブロック (3-68 ページ)。
24	マルウェア イ ベント	レガシー	Cisco Advanced Malware Protection 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-55 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-51 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-76 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-273 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 (3-108 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 (3-111 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 (3-119 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-244 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-240 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-249 ページ)。

表 3-26 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-61 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-55 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-68 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-68 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-61 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-68 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-249 ページ)を参照してくだ さい。ブロック 32 は廃止予定です。ブロック 43 により 廃止される予定ですマルウェアイベントのデータブ ロック 6.0 以上(3-97 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 (3-108 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-273 ページ)。
41	侵入イベント	レガシー	IOC と侵入イベントを照合するための情報をはじめ として、侵入イベントに関する情報が含まれていま す。侵入イベントレコード 5.3(B-20 ページ)を参照し てください。ブロック 34 は廃止予定です。ブロック 42 により廃止される予定です侵入イベントレコード 5.3.1(B-32 ページ)。

表 3-26 シリーズ2のブロックタイプ(続き)

タイプ (Type)	目次	データブ ロックス テータス	説明
42	侵入イベント	現在 (Current)	IOC と侵入イベントを照合するための情報をはじめとして、侵入イベントに関する情報が含まれています。 侵入イベント レコード 5.3.1 (B-32 ページ) を参照してください。ブロック 41 は廃止予定です 侵入イベント レコード 5.3 (B-20 ページ) 。
43	ファイルイ ベント	レガシー	送信元、SHA ハッシュ、およびファイルの特性などのファイルイベントに関する情報が含まれています。 ファイルイベント 5.3.1 (B-256 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-249 ページ) 。ブロック 46 により廃止される 予定です 6.0 以上のファイルイベント (3-86 ページ) 。
44	マルウェアイ ベント	レガシー	IOC 情報をはじめとするマルウェア イベントに関する情報が含まれています。 マルウェア イベントのデー タブロック 6.0 以上 (3-97 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-68 ページ) 。ブロック 47 によ り廃止される予定です マルウェア イベントのデー タブロック 6.0 以上 (3-97 ページ) 。
46	ファイルイ ベント	現在 (Current)	送信元、SHA ハッシュ、およびファイルの特性などのファイルイベントに関する情報が含まれています。 マル ウェア イベントのデータブロック 6.0 以上 (3-97 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-256 ページ) 。
47	マルウェアイ ベント	現在 (Current)	IOC 情報をはじめとするマルウェア イベントに関する情報が含まれています。 マルウェア イベントのデー タブロック 6.0 以上 (3-97 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-76 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 \(2-28 ページ\)](#)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 \(3-63 ページ\)](#)
- [BLOB データブロック \(3-63 ページ\)](#)
- [リストデータブロック \(3-64 ページ\)](#)
- [汎用リストのデータブロック \(3-65 ページ\)](#)
- [UUID 文字列マッピングのデータブロック \(3-66 ページ\)](#)
- [名前説明マッピングのデータブロック \(3-67 ページ\)](#)

文字列データ ブロック

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

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

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



コメント

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 3-27 文字列ブロック フィールド

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

BLOB データ ブロック

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

次の図に、BLOB データ ブロックの形式を示します。

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

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 3-28 BLOB データ ブロック フィールド

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

リストデータブロック

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

次の図に、リスト データ ブロックの基本的な形式を示します。

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

次の表では、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。

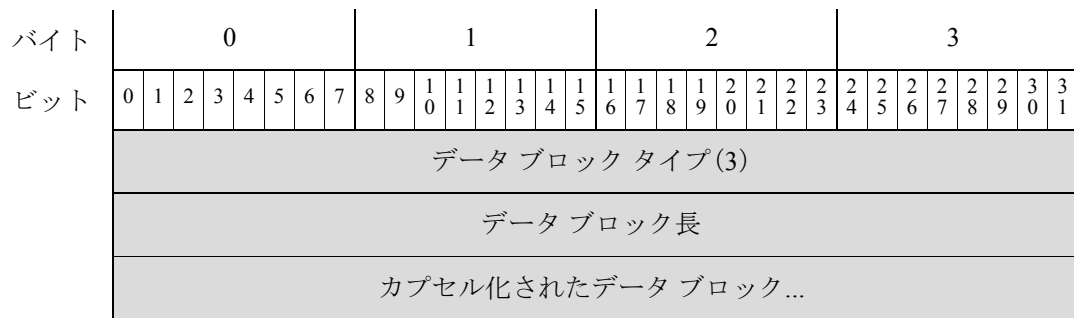
表 3-29 リスト データ フィールド

フィールド	データタイプ	説明
ブロックタイプ (Block Type)	uint32	リスト データ ブロックを開始します。この値は常に 2 です。
ブロック長	uint32	リスト ブロックとカプセル化されたデータのバイト数。たとえば、リスト内に 3 つのサブサーバ データ ブロックがあるとする、この値には、サブサーバ ブロックの合計バイト数とリスト ブロック ヘッダーの 8 バイトが含まれることとなります。
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 3-30 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
UUID 文字列マッピングのブロック タイプ (14)																																
UUID 文字列マッピングのブロック長																																
UUID																																
UUID(続き)																																
UUID(続き)																																
UUID(続き)																																
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、UUID 文字列マッピングのデータ ブロックのフィールドについての説明です。

表 3-31 UUID 文字列マッピングのデータ ブロック フィールド

フィールド	データ タイプ	説明
UUID 文字列マッピングのブロック タイプ	uint32	UUID 文字列マッピングのブロックを開始します。この値は常に 14 です。
UUID 文字列マッピングのブロック長	uint32	UUID 文字列マッピングのブロックの合計バイト数です。UUID 文字列マッピングのブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
UUID	uint8[16]	UUID が識別するイベントまたは他のオブジェクトの固有識別子。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。

表 3-31 UUID 文字列マッピングのデータブロック フィールド(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 3-32 名前説明マッピングのデータブロック フィールド

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

アクセスコントロールポリシールールIDのメタデータブロック

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

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



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	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 3-33 アクセス コントロール ポリシー ルール ID のメタデータ ブロック フィールド

フィールド	データ タイプ	説明
アクセス コントロール ポリシー ルール ID のメタデータ ブロック タイプ	uint32	アクセス コントロール ポリシー ルール ID のメタデータ ブロックを開始します。この値は常に 15 です。
アクセス コントロール ポリシー ルール ID のメタデータのブロック長	uint32	アクセス コントロール ポリシー ルール ID のブロックの合計バイト数です。アクセス コントロール ポリシー ルール ID のメタデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
リビジョン	uint8[16]	トリガーされた関連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 ルールに関連付けられ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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	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(260)																							
	ICMP タイプのデータ ブロック タイプ(19)																																							
	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 3-34 ICMP タイプのデータ ブロック フィールド

フィールド	データ タイプ	説明
ICMP タイプのデータ ブロック タイプ	uint32	ICMP タイプのデータ ブロックを開始します。この値は常に 19 です。
ICMP タイプのデータのブロック長	uint32	ICMP タイプのデータ ブロックの合計バイト数です。ICMP タイプのデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
タイプ(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。 <ul style="list-style-type: none"> 0:IP 1:ICMP 6:TCP 17:UDP

表 3-34 ICMP タイプのデータ 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	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														
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット	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(Type)															
説明	プロトコル																文字列ブロック タイプ(0)															
	文字列ブロック タイプ(0) (続き)																文字列ブロック長															
	文字列ブロック長(続き)																説明...															

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

表 3-35 ICMP コードのデータ ブロック フィールド

フィールド	データタイプ	説明
ICMP コードのデータ ブロックタイプ	uint32	ICMP コードのデータ ブロックを開始します。この値は常に 20 です。
ICMP コードのデータ ブロック長	uint32	ICMP コードのデータ ブロックの合計バイト数です。ICMP コードのデータ ブロックタイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
コード(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。 <ul style="list-style-type: none"> • 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																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
セキュリティ インテリジェンス 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 3-36 セキュリティ コンテキスト名のレコード フィールド

フィールド	データ タイプ	説明
セキュリティ インテリジェンス UUID	uint8[16]	セキュリティ インテリジェンスの UUID。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。
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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(300)															
	レコード長																															
	レルム ID																															
	レルム名の長さ																															
	レルム名...																															

次の表は、レルムのメタデータのレコードのフィールドについての説明です。

表 3-37 レルムのメタデータのレコードフィールド

フィールド	データタイプ	説明
レルム ID	uint32	レルム ID 番号。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)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	エンドポイント プロファイル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 3-38 エンドポイント プロファイルのデータ ブロック フィールド

フィールド	データタイプ	説明
エンドポイント プロファイルのデータ ブロックタイプ	uint32	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。
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。

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

フィールド	データタイプ	説明
文字列ブロック長	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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(302)															
	レコード長																															
	セキュリティグループID																															
	セキュリティグループ名の長さ																															
	セキュリティグループ名...																															

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

表 3-39 セキュリティグループのメタデータのレコードフィールド

フィールド	データタイプ	説明
セキュリティグループID	uint32	セキュリティグループID番号。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 3-40 DNS レコードタイプのメタデータフィールド

フィールド	データタイプ	説明
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。

表 3-40 DNS レコード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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
	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(321)															
	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 応答 ID																															

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
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 3-41 DNS レスポンス タイプのメタデータ フィールド

フィールド	データ タイプ	説明
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。
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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(322)															
	レコード長																															
	UUID 文字列データブロックタイプ(14)																															
	UUID 文字列データブロック長																															
	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)																															
シンクホール名	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	シンクホール名...																															

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

表 3-42 シンクホールのメタデータのレコードフィールド

フィールド	データタイプ	説明
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。

表 3-42 シンクホールのメタデータのレコードフィールド(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	シンクホー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	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	シンクホール名。

6.0 以上の Netmap ドメインのメタデータ

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

バイト	0								1								2								3													
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
	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(350)																					
	レコード長																																					
	Netmap ドメイン ID																																					
	Netmap ドメイン名の長さ																																					
	Netmap ドメイン名...																																					

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

表 3-43 シンクホールのメタデータのレコードフィールド

フィールド	データタイプ	説明
Netmap ドメイン ID	uint32	Netmap ドメイン ID 番号。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 ルールの理由のデータ ブロックを使用して、アクセス コントロール ポリシー ルール ID に関する情報を表示します。このデータ ブロックのレコードタイプは 124 で、シリーズ 2 のブロック タイプ 59 です。これはブロック タイプ 21 に取って代わります。理由フィールドが 16 ビットから 32 ビットに拡張されました。

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

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	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(124)																							
	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(59)																																							
	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																																							
	理由 (Reason)																																							
説明	文字列ブロック タイプ(0)																																							
	文字列ブロック長																																							
	説明...																																							

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

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

フィールド	データ タイプ	説明
アクセス コントロール ポリシー ルール理由データ ブロック タイプ	uint32	アクセス コントロール ポリシー ルール理由データ ブロックを開始します。この値は常に 59 です。
アクセス コントロール ポリシー ルールの理由のデータ ブロックの長さ	uint32	アクセス コントロール ポリシー ルール理由データ ブロックのバイトの合計数(アクセス コントロール ポリシー ルール理由データ ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。

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

フィールド	データタイプ	説明
理由 (Reason)	uint32	<p>イベントをトリガーしたルールの理由の番号。</p> <p>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。</p> <ul style="list-style-type: none"> • 1: IP ブロック • 2: IP モニタ • 4: ユーザ バイパス • 8: ファイル モニタ • 16: ファイル ブロック • 32: 侵入モニタ • 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 • 8192: URL ブロック • 16384: URL モニタ • 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	アクセス コントロール ポリシー名のデータ 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																															
[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 3-45 アクセス コントロール ポリシーのポリシー名のデータ ブロック フィールド

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

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

フィールド	データタイプ	説明
文字列ブロック長	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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IPレピュテーションカテゴリのデータブロックタイプ(22)																															
	IPレピュテーションカテゴリのデータブロックの長さ																															
	ルールID																															
	ポリシーUUID																															
	ポリシーUUID(続き)																															
	ポリシーUUID(続き)																															
	ポリシーUUID(続き)																															
説明	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	カテゴリ名...																															

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

表 3-46 IP レピュテーションカテゴリのデータブロック フィールド

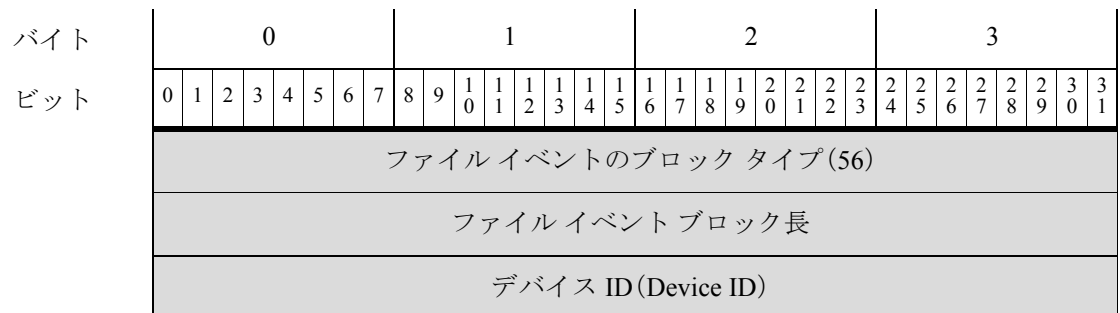
フィールド	データタイプ	説明
IP レピュテーション カテゴリのデータブロックタイプ	uint32	IP レピュテーション カテゴリのデータブロックを開始します。この値は常に 22 です。
IP レピュテーション カテゴリのデータブロックの長さ	uint32	IP レピュテーション カテゴリのデータブロックの合計バイト数です。IP レピュテーション カテゴリのデータブロックタイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID。
ポリシー UUID	uint8[16]	イベントをトリガーしたポリシ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

6.0 以上のファイルイベント

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

ファイルイベントレコードを要求するには、イベントバージョン 5 およびイベントコード 111 の要求メッセージ内に、ファイルイベントフラグ(要求フラグフィールドのビット 30)を設定します。[要求フラグ\(2-13 ページ\)](#)を参照してください。ビット 23 を有効にすると、拡張イベントヘッダーがレコードに含まれます。

次の図は、ファイルイベントデータブロックの構造を示しています。



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

シリーズ2のデータブロックの概要

バイト	0								1							2							3									
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイル名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル名...																															
	ファイル サイズ(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 ID (User ID)																															
URI	ユーザ ID (続き)	文字列ブロック タイプ(0)																														
	文字列ブロック タイプ(0) (続き)	文字列ブロック長																														
	文字列ブロック長 (続き)	URI...																														
シグネチャ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	署名...																															
	送信元ポート (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																															

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
	クライアントアプリケーション ID(続き)								セキュリティ コンテキスト																															
	セキュリティ コンテキスト (続き)								セキュリティ コンテキスト(続き)																															
									セキュリティ コンテキスト(続き)																															
									セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト (続き)								SSL 証明書フィンガープリント																															
									SSL 証明書フィンガープリント(続き)																															
									SSL 証明書フィンガープリント(続き)																															
									SSL 証明書フィンガープリント(続き)																															
	SSL 証明書フィンガープリント(続き)								実際の SSL アクション																SSL フローステータス															
アーカイブ SHA									SSL フローステータス(続き)								文字列ブロック タイプ(0)																							
	文字列ブロックタイプ(続き)								文字列の長さ																															
									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 3-47 6.0 以上のファイル イベントのデータ ブロック フィールド

フィールド	データ タイプ	説明
ファイル イベント ブロック タイプ	uint32	ファイル イベント データ ブロックを開始します。この値は常に 56 です。
ファイル イベント ブロック 長	uint32	ファイル イベント ブロックのバイトの合計数(ファイル イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID (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。 <ul style="list-style-type: none"> • 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 3-47 6.0 以上のファイルイベントのデータブロック フィールド(続き)

フィールド	データ タイプ	説明
ファイル ストレージ ステータス	uint8	ファイルの保存ステータス。値は以下のとおりです。 <ul style="list-style-type: none">• 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、解析結果を入力できません

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

フィールド	データ タイプ	説明
ファイル分析ステータス	uint8	<p>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。</p> <ul style="list-style-type: none"> • 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、解析結果を入力できません • 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ため、ファイル キャパシティが処理されました(センサーに保存) • 25(ファイル送信サーバ制限超過によるキャパシティの処理): サーバの速度制限が原因でファイル キャパシティが処理されました • 26(通信障害): クラウド接続失敗が原因でファイル キャパシティが処理されました • 27(未送信): 設定が原因でファイルは送信されていません。 • 28(事前分類の一致なし): 事前分類でファイル内に埋め込みオブジェクトまたは疑わしいオブジェクトが検出されなかったため、ファイルはダイナミック分析用に送信されませんでした • 29(Transmit Sent Sandbox Private Cloud): ダイナミック分析のためにファイルがプライベートクラウドに送信されました。 • 30(送信ボックスはプライベートクラウドに未送信): ファイルは分析のためにプライベートクラウドに送信されませんでした

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

フィールド	データ タイプ	説明
ローカルのマルウェア分析ステータス	uint8	<p>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。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> 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	<p>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)。</p>
操作	uint8	<p>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。</p> <ul style="list-style-type: none"> 1: 検出 2: ブロック 3: マルウェア クラウドルックアップ 4: マルウェア ブロック 5: マルウェア ホワイトリスト 6: クラウドルックアップのタイムアウト 7: カスタム検出 8: カスタム検出ブロック 9: アーカイブ ブロック (深度超過) 10: アーカイブ ブロック (暗号化されている) 11: アーカイブ ブロック (調査エラー)
SHA ハッシュ	uint8[32]	<p>バイナリ形式の SHA-256 ハッシュのファイル。</p>

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

フィールド	データ タイプ	説明
ファイル タイプ ID	uint32	ファイル タイプにマップされている ID 番号。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、 エンドポイント向け AMP ファイルタイプのメタデータ (3-43 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。 <ul style="list-style-type: none"> 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 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の ID 番号。
URI	string	接続の Uniform Resource Identifier (URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> 1: ICMP 4: IP 6: TCP 17: UDP これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。

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

フィールド	データ タイプ	説明
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト (仮想ファイアウォール) の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 <ul style="list-style-type: none"> • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

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

フィールド	データタイプ	説明
SSL フロー ステータス	uint16	<p>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。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
文字列ブロック タイプ	uint32	<p>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。</p>

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

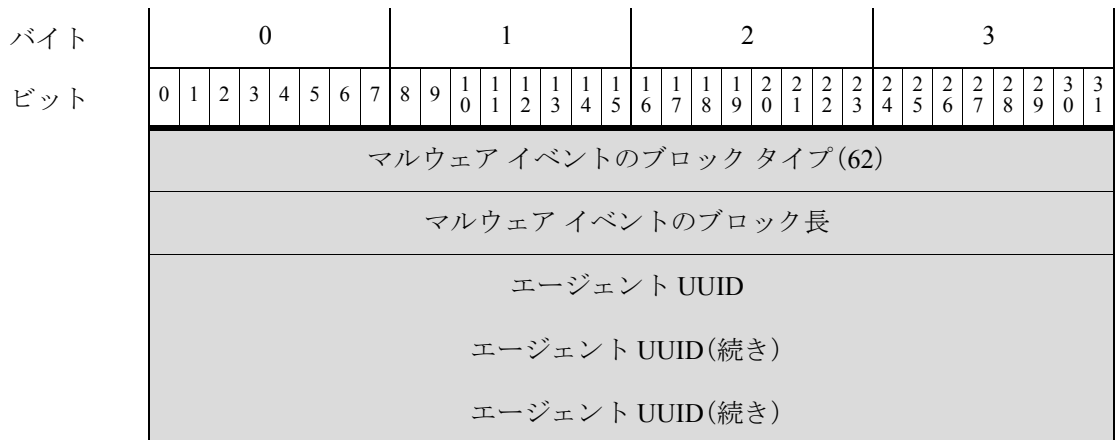
フィールド	データ タイプ	説明
文字列ブロック長	uint32	アーカイブ SHA 文字列データブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および侵入ポリシー名のバイト数を含む)。
アーカイブ SHA	string	ファイルが含まれる親アーカイブの SHA1 ハッシュ。
文字列ブロック タイプ	uint32	アーカイブ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	アーカイブ名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびアーカイブ名のバイト数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

マルウェア イベントのデータブロック 6.0 以上

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

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

次の図に、マルウェア イベントのデータブロックの構造を示します。



バイト	0								1					2				3														
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	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 (User)	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイル名...																															
ファイルパス	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイルパス...																															
ファイル SHA ハッシュ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイル サイズ (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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ファイル タイプ																															
	ファイルのタイムスタンプ																															
親ファイル [名前(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 ID(User ID)																															
ユーザ ID(続き)	アクセス コントロール ポリシー UUID																															

■ シリーズ2のデータブロックの概要

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	アクセスコントロールポリシー UUID(続き)																															
	アクセスコントロールポリシー UUID(続き)																															
	アクセスコントロールポリシー UUID(続き)																															
URI	アクセスコントロールポリシー UUID(続き)								傾向								レトロスペクティブ傾向								文字列ブロックタイプ(0)							
	文字列ブロックタイプ(0)(続き)																文字列ブロック長															
	文字列ブロック長(続き)																URI...															
	送信元ポート (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)																															
	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							

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
アーカイブ 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)																								
HTTP レスポンス (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 3-48 6.0 以上のマルウェア イベントのデータブロック フィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 62 です。
マルウェア イベント のブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする 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。

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

フィールド	データタイプ	説明
文字列ブロック長	uint32	検出名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロックタイプ	uint32	ユーザ名を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ユーザ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびユーザフィールドのバイト数を含む)。
ユーザ(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。これらのユーザはユーザディスカバリには関係ないことに注意してください。
文字列ブロックタイプ	uint32	ファイル名を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ファイル名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロックタイプ	uint32	ファイルパスを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ファイルパス文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびファイルパスフィールドのバイト数を含む)。
ファイルパス	string	検出または検疫されたファイルのファイルパス。ファイル名は含まれません。
文字列ブロックタイプ	uint32	ファイルSHAハッシュを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ファイルSHAハッシュ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびファイルSHAハッシュフィールドのバイト数を含む)。
ファイルSHAハッシュ	string	検出または検疫されたファイルのSHA-256ハッシュ値のレンダリングされた文字列。
ファイルサイズ(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(3-43ページ) を参照してください。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時のUNIXタイムスタンプ(1970年1月1日からの経過秒数)。

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

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	親ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロック タイプ	uint32	親ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル SHA ハッシュフィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロック タイプ	uint32	イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベント タイプに関連付けられている追加イベント情報。
デバイス ID (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。 <ul style="list-style-type: none"> 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 3-48 6.0 以上のマルウェアイベントのデータブロック フィールド(続き)

フィールド	データ タイプ	説明
ユーザ 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。 <ul style="list-style-type: none"> • 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): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
レトロスペクティブ 特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロック タイプ	uint32	URI を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。

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

フィールド	データタイプ	説明
操作	uint8	<p>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。</p> <ul style="list-style-type: none"> • 1:検出 • 2:ブロック • 3:マルウェアクラウドルックアップ • 4:マルウェアブロック • 5:マルウェアホワイトリスト • 6:クラウドルックアップのタイムアウト • 7:カスタム検出 • 8:カスタム検出ブロック • 9:アーカイブブロック(深度超過) • 10:アーカイブブロック(暗号化されている) • 11:アーカイブブロック(調査エラー)
プロトコル	uint8	<p>ユーザが指定した IANA プロトコル数。次に例を示します。</p> <ul style="list-style-type: none"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP <p>これは現時点では TCP のみです。</p>
脅威スコア	uint8	<p>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)。</p>
IOC 番号	uint16	<p>このイベントに関連付けられている侵害 ID 番号。</p>
セキュリティ コンテキスト	uint8(16)	<p>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。</p>
SSL 証明書フィンガープリント	uint8[20]	<p>SSL サーバ証明書の SHA1 ハッシュ。</p>

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

フィールド	データ タイプ	説明
実際の SSL アクション	uint16	<p>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。</p> <ul style="list-style-type: none">0:「不明」1:「復号しない」2:「ブロックする」3:「リセットでブロック」4:「復号(既知のキー)」5:「復号(置換キー)」6:「復号(Resign)」

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

フィールド	データタイプ	説明
SSL フロー ステータス	uint16	<p>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。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
文字列ブロック タイプ	uint32	<p>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。</p>

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

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

5.3 以上のファイルイベント SHA ハッシュ

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

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



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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)																															
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...																															
	傾向																ユーザ定義															

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

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

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

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

フィールド	データタイプ	説明
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> • 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):ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
ユーザ定義	uint8	ファイル名の表示方法を示します。 <ul style="list-style-type: none"> • 0:AMP 定義 • 1:ユーザ定義

5.3 以上のファイルタイプ ID のメタデータ

eStreamer サービスは、ファイルタイプ ID のイベントのファイルタイプ情報を含むメタデータを送信します。形式は次のとおりです。このレコードは、ファイルタイプ名にファイルタイプ ID をマッピングしています。メタデータ フラグのいずれか(要求メッセージの [要求フラグ (Request Flags)] フィールドのビット 1、14、15、または 20) が設定されていると、ファイルタイプ ID の情報が送信されます。[要求フラグ \(2-13 ページ\)](#) を参照してください。メッセージ長フィールドの後に表示されるレコードタイプフィールドにファイルタイプ ID レコードを示す値 510 があることに注意してください。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ヘッダー バージョン (1)																メッセージタイプ (4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ (510)																							
	レコード長																																							
	ファイルタイプ ID																																							

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイルタイプの長さ																																
ファイルタイプ名...																																

次の表は、ファイルタイプIDのレコードのフィールドについての説明です。

表 3-50 ファイルタイプIDのレコードフィールド

フィールド	データタイプ	説明
ファイルタイプID	uint32	ファイルタイプID番号。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\(2-29 ページ\)](#)を参照してください。

次の図に、ルールドキュメントのデータブロックの構造を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ルールドキュメントのブロックタイプ(27)																																
ルールドキュメントのブロック長																																
シグネチャID																																
ジェネレータID																																
リビジョン																																
要約	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	サマリー...																															

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

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

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

表 3-51 ルールドキュメントのデータブロックフィールド

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

表 3-51 ルールドキュメントのデータブロックフィールド(続き)

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

表 3-51 ルールドキュメントのデータブロックフィールド(続き)

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

6.0 以上の Filelog ストレージのメタデータ

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

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	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(515)																							
	レコード長																																							
	Filelog ストレージのステータス																																							

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Filelog ストレージのステータスの説明の長さ																																
Filelog ストレージのステータスの説明...																																

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

表 3-52 Filelog ストレージのメタデータのレコードフィールド

フィールド	データタイプ	説明
Filelog ストレージのステータス	uint32	filelog ストレージのステータスを示す番号。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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(516)																
レコード長																																
Filelog サンドボックスのステータス																																
Filelog サンドボックスのステータスの説明の長さ																																
Filelog サンドボックスのステータスの説明...																																

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

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

フィールド	データタイプ	説明
Filelog サンドボックスのステータス	uint32	filelog サンドボックスのステータスを示す番号。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	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(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 3-54 Filelog Spero のメタデータのレコードフィールド

フィールド	データタイプ	説明
Filelog Spero のステータス	uint32	filelog spero のステータスを示す番号。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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(519)															
	レコード長																															
	Filelog スタティック分析のステータス																															
	Filelog スタティック分析のステータスの説明の長さ																															
	Filelog スタティック分析のステータスの説明...																															

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

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

フィールド	データタイプ	説明
Filelog スタティック分析のステータス	uint32	filelog スタティック分析のステータスを示す番号。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	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																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Netmap ID																レコードタイプ(520)															
	位置情報のブロックタイプ(28)																															
	位置情報のブロック長																															
	国コード(Country Code)																文字列ブロックタイプ(0)															
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 3-57 位置情報のデータブロックフィールド

フィールド	データタイプ	説明
位置情報のデータブロックタイプ	uint32	位置情報のデータブロックを開始します。この値は常に 28 です。
位置情報のデータブロック長	uint32	位置情報のデータブロックの合計バイト数です。位置情報のデータブロックタイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
国コード(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\(2-13 ページ\)](#)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	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(530)															
	レコード長																															
	UUID 文字列ブロック タイプ(14)																															
	UUID 文字列ブロック長																															
	ファイル ポリシー UUID																															
	ファイル ポリシー UUID(続き)																															
	ファイル ポリシー UUID(続き)																															
	ファイル ポリシー UUID(続き)																															
ファイルポリシー名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル ポリシー名...																															

次の表は、ファイルポリシー名のレコードのフィールドについての説明です。

表 3-58 ファイルポリシー名フィールド

フィールド	データタイプ	説明
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。

表 3-58 ファイルポリシー名フィールド(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 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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(600)															
	レコード長																															
	UUID 文字列ブロック タイプ(14)																															
	UUID 文字列ブロック長																															
	SSL ポリシー UUID																															
	SSL ポリシー UUID(続き)																															
	SSL ポリシー UUID(続き)																															
	SSL ポリシー UUID(続き)																															
SSL ポリシー名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	SSL ポリシー名...																															

次の表は、SSL ポリシー名のレコードのフィールドについての説明です。

表 3-59 SSL ポリシー名レコードフィールド

フィールド	データタイプ	説明
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。
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 \(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(601)															
	レコード長																															
	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)																															

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

次の表は、SSL ルール ID レコードのフィールドについての説明です。

表 3-60 SSL ポリシー名レコードフィールド

フィールド	データタイプ	説明
リビジョン	uint8[16]	SSL ルール リビジョンの UUID。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 \(2-13 ページ\)](#) 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(602)															
	レコード長																															
	SSL 暗号 ID																															
	SSL 暗号スイート名の長さ																															
	SSL 暗号スイート名...																															

次の表は、SSL 暗号スイート レコードのフィールドについての説明です。

表 3-61 SSL 暗号スイート フィールド

フィールド	データタイプ	説明
SSL 暗号 ID	uint32	SSL 暗号 ID 番号。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 \(2-13 ページ\)](#) 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(604)															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
レコード長																																
SSL バージョン ID																																
SSL バージョン名の長さ																																
SSL バージョン名...																																

次の表は、SSL バージョン レコードのフィールドについての説明です。

表 3-62 SSL バージョンフィールド

フィールド	データタイプ	説明
SSL バージョン ID	uint32	SSL バージョン ID 番号。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 サーバ証明書ステータス

eStreamer サービスは、SSL サーバ証明書ステータス情報を含むメタデータを送信します。形式は次のとおりです。(メタデータフラグのいずれか(要求メッセージの [要求フラグ (Request Flags)] フィールドのビット 1、14、15、または 20) が設定されていると、SSL サーバ証明書ステータスの情報が送信されます。[要求フラグ \(2-13 ページ\)](#) を参照してください)。メッセージ長フィールドの後に表示されるレコードタイプフィールドに SSL サーバ証明書ステータス レコードを示す値 605 があることに注意してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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 (605)																
レコード長																																
SSL サーバ証明書ステータス																																
SSL サーバ証明書ステータスの説明の長さ																																
SSL サーバ証明書ステータスの説明...																																

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

表 3-63 SSL サーバ証明書ステータス レコードフィールド

フィールド	データタイプ	説明
SSL サーバ証明書ステータス	uint32	SSL サーバ証明書ステータス番号。このフィールドは、このレコードの固有キーです。
SSL サーバ証明書ステータスの説明の長さ	uint32	SSL サーバ証明書ステータスの説明に含まれるバイト数。
SSL サーバ証明書ステータスの説明	string	SSL サーバ証明書ステータスの説明。

実際の SSL アクション

eStreamer は、実際の SSL アクションの情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグのいずれか(要求メッセージの [要求フラグ (Request Flags)] フィールドのビット 1、14、15、または 20) が設定されていると、実際の SSL アクションの情報が送信されます。[要求フラグ \(2-13 ページ\)](#) 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(606)															
	レコード長																															
	実際の SSL アクションの番号																															
	実際の SSL アクションの説明の長さ																															
	実際の SSL アクションの説明...																															

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

表 3-64 実際の SSL アクションフィールド

フィールド	データタイプ	説明
実際の SSL アクションの番号	uint32	実際の SSL アクションを指定する番号。このフィールドは、このレコードの固有キーです。
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 \(2-13 ページ\)](#) を参照してください)。メッセージ長フィールドの後に表示されるレコードタイプフィールドに予期していた SSL アクションレコードを示す値 607 があることに注意してください。

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

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

表 3-65 実際の SSL アクション フィールド

フィールド	データタイプ	説明
予期していた SSL アクションの番号	uint32	予期していた SSL アクションを指定する番号。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 \(2-13 ページ\)](#) を参照してください)。メッセージ長フィールドの後に表示されるレコードタイプフィールドに SSL フロー ステータス レコードを示す値 608 があることに注意してください。

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

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

表 3-66 SSL フロー ステータス フィールド

フィールド	データタイプ	説明
SSL フロー ステータス番号	uint32	SSL フロー ステータスを指定する番号。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 \(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(613)															
	レコード長																															
	SSL URL カテゴリ番号																															
	SSL URL カテゴリの説明の長さ																															
	SSL URL カテゴリの説明...																															

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

表 3-67 SSL URL カテゴリ フィールド

フィールド	データタイプ	説明
SSL URL カテゴリ番号	uint32	SSL URL カテゴリを指定する番号。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 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せん。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、および関連 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。



シリーズ2のデータブロックの概要

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

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
発行者組織	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 3-68 SSL 証明書の詳細のデータブロック フィールド

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

表 3-68 SSL 証明書の詳細のデータ ブロック フィールド(続き)

フィールド	データタイプ	説明
文字列ブロックタイプ	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。
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。

表 3-68 SSL 証明書の詳細のデータブロック フィールド(続き)

フィールド	データタイプ	説明
文字列ブロックタイプ	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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(700)															
	レコード長																															
	UUID 文字列ブロックタイプ(14)																															
	UUID 文字列ブロック長																															
	ネットワーク分析ポリシー UUID																															
	ネットワーク分析 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
	ネットワーク分析 UUID(続き)																															
	ネットワーク分析 UUID(続き)																															
ネットワーク分析 ポリシー名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ネットワーク分析ポリシー名...																															

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

表 3-69 ネットワーク分析ポリシー名レコードフィールド

フィールド	データタイプ	説明
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。
文字列ブロック長	uint32	ネットワーク分析ポリシー名の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとネットワーク分析ポリシー名のバイト数が含まれます。
ネットワーク分析ポリシー名	string	ネットワーク分析ポリシーの名前。



検出と接続データ構造の概要

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

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

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

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

eStreamer サーバからのディスカバリ イベントまたは接続イベントの要求については、[要求フラグ \(2-13 ページ\)](#) 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 \(2-20 ページ\)](#) を参照してください。

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

- [ディスカバリ イベントと接続イベントのデータ メッセージ \(4-2 ページ\)](#) では、eStreamer がホスト ディスカバリ メッセージ、ユーザ メッセージ、接続メッセージに使用する構造の概要を紹介しています。
- [ディスカバリ イベントと接続イベントのレコード タイプ \(4-2 ページ\)](#) では、ディスカバリ イベントと接続イベント レコード タイプについて説明します。
- [ディスカバリ イベントのメタデータ \(4-8 ページ\)](#) では、たとえば、イベント内のユーザ ID をユーザ名に変換するなど、数字データとコード化データをテキストに変換するためのコンテキスト情報を要求できるメタデータ レコードについて説明します。
- [ディスカバリ イベント ヘッダー 5.2+ \(4-42 ページ\)](#) 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 データ構造(4-64 ページ)では、eStreamer が各種ユーザ イベントタイプに使用するデータ レコードの構造について説明します。
- ディスカバリ (シリーズ 1)ブロック(4-65 ページ)では、ディスクバリ 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、関連イベントでも使用します。
- ユーザ脆弱性データ ブロック 5.0+(4-166 ページ)では、複雑なユーザ イベント レコードを伝えるために使用するその他のシリーズ 1 ブロック構造について説明します。



ヒント

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

ディスクバリ イベントと接続イベントのデータ メッセージ

eStreamer は、ディスクバリ 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クバリ 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、[ディスクバリ 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。ディスクバリ 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[ユーザ脆弱性データ ブロック 5.0+\(4-166 ページ\)](#)を参照してください。

ディスクバリ 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、ディスクバリ 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	現在 (Current)	サーバメッセージ(4-48 ページ)
12	103	1	新規 UDP サーバ	現在 (Current)	サーバメッセージ(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 サーバ情報更新	現在 (Current)	サーバメッセージ(4-48 ページ)
17	103	1	UDP サーバ情報更新	現在 (Current)	サーバメッセージ(4-48 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)
28	該当なし	該当なし	ホストの追加 MAC を検出	現在 (Current)	MAC アドレス メッセージ(4-53 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)

表 4-1 ディスカバリ イベントと接続イベントのレコードタイプ(続き)

レコードタイプ	含まれるブロックタイプ	シリーズ	説明	レコードステータス	データ形式の参照先...
31	該当なし	該当なし	ルータ/ブリッジとして識別したホスト	現在 (Current)	ブリッジ/ルータとして識別したホストメッセージ(4-54 ページ)
34	14	1	VLAN タグ情報更新	現在 (Current)	VLAN タグ情報更新メッセージ(4-54 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)
42	35	1	NetBIOS 名変更	現在 (Current)	NetBIOS 名変更メッセージ(4-55 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 サーバ信頼度更新	レガシー	サーバメッセージ(4-48 ページ)
52	103	1	UDP サーバ信頼度更新	レガシー	サーバメッセージ(4-48 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(4-8 ページ)
55	該当なし	該当なし	クライアントアプリケーションメタデータ	現在 (Current)	クライアントアプリケーションレコード(4-10 ページ)
57	該当なし	該当なし	脆弱性メタデータ	現在 (Current)	脆弱性レコード(4-10 ページ)
58	該当なし	該当なし	重要度メタデータ	現在 (Current)	重要度レコード(4-13 ページ)
59	該当なし	該当なし	ネットワークプロトコルメタデータ	現在 (Current)	ネットワークプロトコルレコード(4-13 ページ)
60	該当なし	該当なし	属性メタデータ	現在 (Current)	属性レコード(4-14 ページ)
61	該当なし	該当なし	スキャンタイプメタデータ	現在 (Current)	スキャンタイプレコード(4-15 ページ)
63	該当なし	該当なし	サーバメタデータ	現在 (Current)	サービスレコード(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-146 ページ)

表 4-1 ディスカバリ イベントと接続イベントのレコードタイプ(続き)

レコードタイプ	含まれるブロックタイプ	シリーズ	説明	レコードステータス	データ形式の参照先...
71	152	1	接続統計情報	レガシー	接続統計データ ブロック 5.3(B-163 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-170 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-177 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-191 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-205 ページ)
71	163	1	接続統計情報	現在 (Current)	接続統計データ ブロック 6.2+(4-126 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(4-57 ページ)
74	該当なし	該当なし	ユーザ設定 OS	現在 (Current)	ユーザ サーバ メッセージとオペレーティング システム メッセージ(4-60 ページ)
75	該当なし	該当なし	ユーザ設定サーバ	現在 (Current)	ユーザ サーバ メッセージとオペレーティング システム メッセージ(4-60 ページ)
76	83	1	ユーザ削除プロトコル	現在 (Current)	ユーザ プロトコル メッセージ(4-61 ページ)
77	60	1	ユーザ削除クライアントアプリケーション	現在 (Current)	ユーザ クライアント アプリケーション メッセージ(4-61 ページ)
78	78	1	ユーザ削除アドレス	現在 (Current)	ユーザ追加/削除ホスト メッセージ(4-58 ページ)
79	77	1	ユーザ削除サーバ	現在 (Current)	ユーザ削除サーバ メッセージ(4-58 ページ)
80	80	1	ユーザ設定の有効な脆弱性	現在 (Current)	バージョン4.6.1+ のユーザ設定脆弱性メッセージ(4-57 ページ)
81	80	1	ユーザ設定の無効な脆弱性	現在 (Current)	バージョン4.6.1+ のユーザ設定脆弱性メッセージ(4-57 ページ)
82	81	1	ユーザ設定ホスト重要度	現在 (Current)	ユーザ設定ホスト重要度メッセージ(4-59 ページ)
83	55	1	ユーザ設定属性値	現在 (Current)	属性値メッセージ(4-60 ページ)
84	82	1	ユーザ削除属性値	現在 (Current)	属性値メッセージ(4-60 ページ)
85	78	1	ユーザ追加ホスト	現在 (Current)	ユーザ追加/削除ホスト メッセージ(4-58 ページ)
86	該当なし	該当なし	ユーザ追加サーバ	現在 (Current)	ユーザ サーバ メッセージとオペレーティング システム メッセージ(4-60 ページ)
87	60	1	ユーザ追加クライアントアプリケーション	現在 (Current)	ユーザ クライアント アプリケーション メッセージ(4-61 ページ)
88	83	1	ユーザ追加プロトコル	現在 (Current)	ユーザ プロトコル メッセージ(4-61 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...
89	142	1	ユーザ追加スキャン結果	現在 (Current)	スキャン結果を追加メッセージ(4-62 ページ)
90	該当なし	該当なし	ソース タイプ レコード	現在 (Current)	ソース タイプ レコード(4-17 ページ)
91	該当なし	該当なし	ソース アプリケーション レコード	現在 (Current)	ソース アプリケーション レコード(4-18 ページ)
92	120	1	ユーザ ドロップ変更イベント	現在 (Current)	ユーザ変更メッセージ(4-64 ページ)
93	120	1	ユーザ削除変更イベント	現在 (Current)	ユーザ変更メッセージ(4-64 ページ)
94	120	1	新規ユーザ識別イベント	現在 (Current)	ユーザ変更メッセージ(4-64 ページ)
95	121	1	ユーザ ログイン変更イベント	現在 (Current)	ユーザ情報更新メッセージ ブロック(4-64 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(4-18 ページ)
98	57	2	ユーザ レコード	現在 (Current)	ユーザ レコード(4-21 ページ)
101	該当なし	該当なし	新規 OS イベント	現在 (Current)	新規オペレーティング システム メッセージ(4-62 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(4-63 ページ)
103	94	1	アイデンティティ タイムアウト イベント	現在 (Current)	アイデンティティ競合とアイデンティティ タイムアウトシステムメッセージ(4-63 ページ)
106	該当なし	該当なし	サードパーティ スキャナ脆弱性レコード	現在 (Current)	サードパーティ スキャナの脆弱性レコード(4-19 ページ)
107	122	1	クライアント アプリケーション更新	現在 (Current)	クライアント アプリケーション メッセージ(4-50 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	失敗したユーザのログイン イベント	現在 (Current)	ユーザ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(3-31 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(3-33 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(3-34 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)

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...
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 (3-35 ページ)
120	該当なし	該当なし	アクセス コントロール ルール アクション レコード	現在 (Current)	アクセス コントロール ルール アクション レコードメタデータ (4-24 ページ)
121	該当なし	該当なし	URL カテゴリ統計	現在 (Current)	URL カテゴリ レコードメタデータ (4-25 ページ)
122	該当なし	該当なし	URL レピュテーションメタデータ	現在 (Current)	URL レピュテーション レコードメタデータ (4-26 ページ)
124	21	2	アクセス コントロール ルール理由メタデータ	現在 (Current)	アクセス コントロール ルール理由メタデータ (4-27 ページ)
145	64	2	アクセス コントロール ポリシーメタデータ	現在 (Current)	アクセス コントロール ポリシーメタデータ (4-29 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 (4-30 ページ)
147	21	2	トンネルまたはプレフィルタ ルールメタデータ	現在 (Current)	トンネルまたはプレフィルタのルールのメタデータ (4-32 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)
162	148	1	ユーザ ホスト IOC の削除	Current	ユーザ IOC の変更データ ブロック 5.3+ (4-85 ページ)
163	148	1	ユーザ ホスト IOC の有効化	Current	ユーザ IOC の変更データ ブロック 5.3+ (4-85 ページ)
164	148	1	ユーザ ホスト IOC の無効化	Current	ユーザ IOC の変更データ ブロック 5.3+ (4-85 ページ)
170	95	1	VPN ユーザのログイン イベント	Current	ユーザ情報更新メッセージブロック (4-64 ページ)
171	95	1	VPN ユーザのログオフ イベント	現在 (Current)	ユーザ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。Firepower システム のバージョンに対応するメタデータ バージョンについては、[メタデータについて\(2-45 ページ\)](#)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\(2-46 ページ\)](#)を参照してください。

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

- [フィンガープリント レコード\(4-8 ページ\)](#)
- [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\(4-10 ページ\)](#)
- [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\(4-13 ページ\)](#)
- [属性レコード\(4-14 ページ\)](#)
- [スキャンタイプ レコード\(4-15 ページ\)](#)
- [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\(4-18 ページ\)](#)
- [サードパーティ スキャナの脆弱性レコード\(4-19 ページ\)](#)
- [ユーザ 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\(4-24 ページ\)](#)
- [URL カテゴリ レコード メタデータ\(4-25 ページ\)](#)
- [URL レピュテーション レコード メタデータ\(4-26 ページ\)](#)
- [アクセス コントロール ルール理由メタデータ\(4-27 ページ\)](#)
- [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\(4-35 ページ\)](#)

侵入イベントと関連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\(2-13 ページ\)](#)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	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(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...																															
	OS バージョン長さ																															
	OS バージョン...																															

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 システムの一意的 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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(55)															
	レコード長																															
	アプリケーション ID(Application ID)																															
	名前の長さ																															
	名前...																															

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\(2-13 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、脆弱性レコードを示す 57 です。

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

次の表では、脆弱性レコードのフィールドについて説明します。

表 4-4 脆弱性レコードのフィールド

フィールド	データタイプ	説明
脆弱性 ID	uint32	脆弱性 ID 番号このフィールドは、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。 <ul style="list-style-type: none"> 0:はい 1:いいえ
[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。 <ul style="list-style-type: none"> 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 \(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(58)															
	レコード長																															
	重要度 ID																															
	名前の長さ																															
	名前...																															

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 \(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(59)															
	レコード長																															
	ネットワーク プロトコル ID																															
	名前の長さ																															
	名前...																															

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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(60)															
	レコード長																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
属性 ID																																
名前の長さ																																
名前...																																

次の表では、属性レコードのフィールドについて説明します。

表 4-7 属性レコードのフィールド

フィールド	データタイプ	説明
属性 ID	uint32	属性 ID 番号。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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(61)																
レコード長																																
スキャンタイプ ID																																
名前の長さ																																
名前...																																

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 \(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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 (63)															
	レコード長																															
	アプリケーション ID (Application ID)																															
	名前の長さ																															
	名前...																															

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。

表 4-9 サービス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	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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(90)															
	レコード長																															
	ソースタイプ ID																															
	名前の長さ																															
	名前...																															

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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(91)															
	レコード長																															
	ソース アプリケーション ID																															
	名前の長さ																															
	名前...																															

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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(96)															
	レコード長																															
	送信元ディテクタ ID																															
	名前の長さ																															
	名前...																															

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 \(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	レコード長																															
	脆弱性 ID																															
	スキャナ タイプ																															
	タイトル長さ																															
	タイトル...																															
	説明の長さ																															
	説明...																															
	CVE ID 長さ																															
	CVE ID...																															
	BugTraq 長さ																															
	BugTraq ID...																															

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。
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

ユーザレコード

eStreamer サービスは、次の形式のユーザレコードで、システムが検出したユーザに関する情報を格納したメタデータを送信します。(バージョン4メタデータとポリシーイベント要求フラグ(それぞれ要求メッセージの要求フラグフィールドのビット20と22)を設定すると、ユーザ情報が送信されます。[要求フラグ\(2-13ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、ユーザレコードを示す98です。

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

次の表は、ユーザレコードのフィールドについての説明です。

表 4-14 ユーザレコードのフィールド

フィールド	データタイプ	説明
ユーザデータブロックタイプ	uint32	ユーザデータブロックを開始します。この値は常に57です。ブロックタイプは、シリーズ2ブロックです。
ユーザデータブロック長	uint32	データブロックの長さ。データのバイト数に2つのデータブロックヘッダーフィールドの8バイトを加えたバイト数です。
ユーザID(User ID)	uint32	ユーザの固有識別情報。このフィールドは、このレコードの固有キーです。

表 4-14 ユーザレコードのフィールド(続き)

フィールド	データタイプ	説明
プロトコル	uint32	ユーザの検出やレポートに使用するプロトコル。値は以下のとおりです。 <ul style="list-style-type: none"> • 165:FTP • 426:SIP • 547:AOL Instant Messenger • 683:IMAP • 710:LDAP • 767:NTP • 773:Oracle データベース • 788:POP3 • 1755:MDNS
文字列ブロックタイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトにユーザ名フィールドのバイト数を加えたユーザ名文字列データ ブロックのバイト数。
[ユーザ名 (Username)]	string	ユーザの名前

Web アプリケーション レコード

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

eStreamer サービスは、次の形式の Web アプリケーション レコードで、イベントの Web アプリケーション メタデータを送信します。(Web アプリケーション メタデータは、以下のメタデータフラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。[要求フラグ\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(109)															
	レコード長																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
アプリケーション ID (Application ID)																																
名前の長さ																																
名前...																																

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 (Application 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 (Name)]	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 \(2-13 ページ\)](#) 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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 (118)																
レコード長																																
侵入ポリシー名データ ブロック (14)																																
侵入ポリシー名データ ブロック長																																
侵入ポリシー UUID																																

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

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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(120)															
	レコード長																															
	アクセスコントロールルールアクションID																															
	名前の長さ																															
	名前...																															

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。
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。

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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(121)															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	レコード長																															
	URL カテゴリ ID																															
	名前の長さ																															
	名前...																															

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\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(122)															
	レコード長																															
	URL レピュテーション ID																															
	名前の長さ																															
	名前...																															

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 \(2-13 ページ\)](#) を参照してください。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、アクセス コントロール ルール理由レコードを示す 124 です。このメタデータには、アクセス コントロール ルール理由ブロックを格納します ([アクセス コントロール ルール理由データ ブロック 5.1+\(4-211 ページ\)](#) を参照)。アクセス コントロール ルール理由データ ブロックのブロックタイプは、シリーズ 2 のブロックタイプ 21 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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 (124)															
	レコード長																															
	アクセス コントロール ルール理由ブロック タイプ (21)																															
	アクセス コントロール ルール理由ブロック長																															
	アクセス コントロール ルール理由																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...															

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

表 4-20 アクセス コントロール ルール理由メタデータのフィールド

フィールド	データタイプ	説明
アクセス コントロール ルール理由ブロックタイプ	uint32	アクセス コントロール ルール理由ブロックを開始します。この値は常に 21 です。これはシリーズ 2 のデータ ブロックです。
アクセス コントロール ルール理由ブロック長	uint32	アクセス コントロール ルール理由ブロックタイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ルール理由ブロックの合計バイト数。
アクセス コントロール ルール理由	uint16	<p>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。</p> <p>イベントをトリガーしたルールの理由の番号。</p> <p>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。</p> <ul style="list-style-type: none"> • 1: IP ブロック • 2: IP モニタ • 4: ユーザ バイパス • 8: ファイル モニタ • 16: ファイル ブロック • 32: 侵入モニタ • 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 • 8192: URL ブロック • 16384: URL モニタ • 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。

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
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\(2-13 ページ\)](#)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+\(4-215 ページ\)](#)を参照)。アクセスコントロールポリシーメタデータブロックのブロックタイプは、シリーズ2のブロックタイプ64です。

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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。
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\(2-13 ページ\)](#)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+\(4-215 ページ\)](#)を参照)。アクセスコントロールポリシーメタデータブロックのブロックタイプは、シリーズ 2 のブロックタイプ 64 です。

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

表 4-22 プレフィルタ ポリシー メタデータ フィールド(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	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\(2-13 ページ\)](#)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\(4-209 ページ\)](#)を参照)。アクセス コントロール ルール理由データブロックのブロックタイプは、シリーズ 2 のブロックタイプ 15 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(147)															
	レコード長																															
	アクセス コントロール ルール ブロック タイプ(15)																															
	アクセス コントロール ルール 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)																															
	アクセス コントロール ルール ID																															

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

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

表 4-23 トンネルまたはプレフィルタ ルール理由メタデータ フィールド

フィールド	データタイプ	説明
アクセス コントロール ルール ブロック タイプ	uint32	アクセス コントロール ルール ブロックを開始します。この値は常に 15 です。ちなみに、このブロックは、アクセス コントロール ルールだけでなく、トンネル ルールとプレフィルタ ルールにも使用します。
アクセス コントロール ルール ブロック長	uint32	アクセス コントロール ルール ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ルール ブロックの合計 バイト数。
アクセス コントロール ルール UUID	uint8[16]	アクセス コントロール ルールの UUID。このフィールドは、このレコードの固有キーです。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 ID 番号。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となります。
文字列ブロック タイプ	uint32	アクセス コントロール ルール 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。

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\(2-13 ページ\)](#)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+\(4-213 ページ\)](#)を参照)。セキュリティ インテリジェンス データ ブロックのブロック タイプは、シリーズ 2 のブロック タイプ 22 です。

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

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

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

フィールド	データタイプ	説明
セキュリティ インテリジェンス カテゴリ ブロック タイプ	uint32	セキュリティ インテリジェンス カテゴリ のデータ ブロックを開始します。この値は常に 22 です。これはシリーズ 2 のデータ ブロックです。
セキュリティ インテリジェンス カテゴリ のブロック長	uint32	セキュリティ インテリジェンス カテゴリ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたセキュリティ インテリジェンス カテゴリ ブロックの合計バイト数。
セキュリティ インテリジェンス リスト ID	uint32	接続でトリガーがかかる IP ブラックリストまたはホワイトリストの ID。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	接続でトリガーがかかる IP カテゴリ ブラックリストまたはホワイトリストの名前。

セキュリティ インテリジェンス 送信元/宛先レコード

eStreamer サービスは、次の形式のセキュリティ インテリジェンス 送信元/宛先レコードで、セキュリティ インテリジェンス で検出した IP アドレスが、送信元 IP アドレスと宛先 IP アドレスのいずれであるかを示すメタデータを送信します。(送信元/宛先 IP 情報は、以下のメタデータ フラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。[要求フラグ\(2-13 ページ\)](#)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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Netmap ID																レコードタイプ(281)															
	レコード長																															
	セキュリティ インテリジェンス送信元/宛先 ID																															
	セキュリティ インテリジェンス送信元/宛先の長さ																															
	セキュリティ インテリジェンス送信元/宛先...																															

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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IOC ステート ブロック タイプ(150)																															
	IOC ステート ブロック長																															
	IOC ID 番号																															
	無効																最初の確認															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	最初の確認 (続き)								最初のイベント ID																							
	最初のイベント ID(続き)								最初の Device ID																							
	最初の Device ID (続き)								最初のインスタンス ID																最初の接続時間							
	最初の接続時間(続き)																								最初のカウンタ							
	最初のカウンタ (続き)								最後の確認日時																							
	最後の確認日時 (続き)								前回イベント ID																							
	前回イベント ID (続き)								前回 Device ID																							
	前回 Device ID(続き)								前回インスタンス ID																前回接続時間							
	前回接続時間(続き)																								前回カウンタ							
	前回カウンタ (続き)																															

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

表 4-26 IOC ステート データ ブロックのフィールド

フィールド	データタイプ	説明
IOC ステート データ ブロック タイプ	uint32	IOC ステート データ ブロックを開始します。この値は常に 150 です。
IOC ステート データ ブロック の長さ	uint32	IOC ステート データ ブロック タイプ フィールドと長さフィー ルドの 8 バイトに、後続のデータ バイト数を加えた IOC ステ ート データ ブロックの合計バイト数。
IOC ID 番号	uint32	侵害の固有 ID 番号。
無効	uint8	侵害がホストで無効にされているかどうかを示します: <ul style="list-style-type: none"> 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。

表 4-26 IOC ステート データ ブロックのフィールド(続き)

フィールド	データタイプ	説明
最初のイベント 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	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(161)															
	レコード長																															
	IOC 名ブロック タイプ(39)																															
	IOC 名ブロック長																															
	IOC ID 番号																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
カテゴリ (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	<p>侵害のカテゴリ。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • 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	<p>侵害のイベントタイプ。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • Adobe Reader launched shell • Dropper Infection Detected by AMP for Endpoints • Excel Compromise Detected by AMP for Endpoints • Excel launched shell • Impact 1 Intrusion Event - attempted-admin • Impact 1 Intrusion Event - attempted-user • Impact 1 Intrusion Event - successful-admin • Impact 1 Intrusion Event - successful-user • Impact 1 Intrusion Event - web-application-attack • Impact 2 Intrusion Event - attempted-admin • Impact 2 Intrusion Event - attempted-user • Impact 2 Intrusion Event - successful-admin • Impact 2 Intrusion Event - successful-user • Impact 2 Intrusion Event - web-application-attack • Intrusion Event - exploit-kit • Intrusion Event - malware-backdoor • Intrusion Event - malware-cnc • Java Compromise Detected by AMP for Endpoints • Java launched shell • PDF Compromise Detected by AMP for Endpoints • PowerPoint Compromise Detected by AMP for Endpoints • PowerPoint launched shell • QuickTime Compromise Detected by AMP for Endpoints • QuickTime launched shell • Security Intelligence Event - CnC • Security Intelligence Event - DNS CnC • Security Intelligence Event - DNS Malware • Security Intelligence Event - DNS Phishing • Security Intelligence Event - Sinkhole CnC • Security Intelligence Event - Sinkhole Malware • Security Intelligence Event - Sinkhole Phishing • Security Intelligence Event - URL CnC • Security Intelligence Event - URL Malware • Security Intelligence Event - URL Phishing • Suspected Botnet Detected by AMP for Endpoints • Threat Detected by AMP for Endpoints - Executed • Threat Detected by AMP for Endpoints - Not Executed • Threat Detected in File Transfer • Word Compromise Detected by AMP for Endpoints • Word launched shell

ディスカバリ イベント ヘッダー 5.2+

ディスカバリ イベントおよび接続イベントのメッセージには、ディスカバリ イベント ヘッダーが含まれます。これは、イベントのタイプおよびサブタイプ、イベントが発生した時刻、イベントが発生したデバイス、およびメッセージ内のイベント データの構造を伝えます。このヘッダーには、実際のホスト ディスカバリ、ユーザ、または接続イベントのデータが続きます。さまざまなイベントのタイプ/サブタイプ値に関連付けられる構造の詳細については、[イベント タイプ別ホスト ディスカバリ構造\(4-46 ページ\)](#)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\(B-94 ページ\)](#)はサポートを停止しました。

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン(1)																メッセージ タイプ(4)															
	メッセージ長																															
	Netmap ID																レコード タイプ															
	レコード長																															
	eStreamer サーバ タイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
ディスカバリ イベント ヘッダー	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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IPv6 アドレス																																
IPv6 アドレス(続き)																																
IPv6 アドレス(続き)																																
IPv6 アドレス(続き)																																

次の表は、ディスカバリ イベント ヘッダーについての説明です。

表 4-28 ディスカバリ イベント ヘッダーのフィールド

フィールド	データ型	説明
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 (3-37 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 (1-5 ページ) を参照してください。
MAC アドレス	uint86	イベントに関連するホストの MAC アドレス。
IPv6 あり	uint8	ホストに IPv6 アドレスがあることを示すフラグ。
将来の使用に備えて予約済み	uint8	将来の使用に備えて予約済み
イベント秒	uint32	システムがイベントを生成したときの UNIX タイムスタンプ(1970 年 1 月 1 日以降の秒数)。
イベントマイクロ秒	uint32	システムがイベントを生成したときのタイムスタンプの、マイクロ秒(100 万分の 1 秒)の増分。
イベントタイプ (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。
ファイルの位置	byte[4]	シリアル ファイル内のイベントの位置。このフィールドは、シスコ の内部使用のためのものであり、無視してかまいません。
IPv6 アドレス	uin8[16]	IPv6 アドレス。このフィールドは、IPv6 フラグが設定されている場合に存在し、使用されます。

ディスカバリ イベントと接続イベントのタイプとサブタイプ

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

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

表 4-29 タイプ/サブタイプ別のディスカバリ イベントと接続イベント

イベント名	イベントタイプ (Event Type)	イベントサブタイプ
新規ホスト	[1000]	1
新規 TCP サーバ	[1000]	2
新規ネットワーク プロトコル	[1000]	3
新規トランスポート プロトコル	[1000]	4
新規 IP 対 IP トラフィック	[1000]	5
新規 UDP サーバ	[1000]	6
新規クライアント アプリケーション	[1000]	7
新規 OS	[1000]	8
IPv6 トラフィックに新しい IPv6	[1000]	9
ホスト IP アドレスを変更	1001	1
OS 情報の更新	1001	2
ホスト IP アドレスを再利用	1001	3
脆弱性の変更	1001	4
ホップ数の変更	1001	5
TCP サーバ情報更新	1001	6
ホスト タイムアウト	1001	7
TCP ポートクローズ	1001	8
UDP ポートクローズ	1001	9
UDP サーバ情報更新	1001	10
TCP ポート タイムアウト	1001	11
UDP ポート タイムアウト	1001	12
MAC 情報の変更	1001	13
ホストの追加 MAC を検出	1001	14
最終検出時のホスト	1001	15
ルータ/ブリッジとして識別したホスト	1001	16
接続統計情報	1001	17
VLAN タグ情報更新	1001	18
ホストを削除。ホスト上限に到達	1001	19
クライアント アプリケーション タイムアウト	1001	20
NetBIOS 名変更	1001	21

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

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
ユーザ追加ホスト	1002	27
ユーザ追加サーバ	1002	28
ユーザ追加クライアントアプリケーション	1002	29
ユーザ追加プロトコル	1002	30
アプリを再読み込み	1002	31
アカウント削除	1002	32
接続統計情報	1003	1
接続チャック	1003	2
新規ユーザ アイデンティティ	1004	1
ユーザ ログイン	1004	2
ユーザ アイデンティティを削除	1004	3
ユーザ アイデンティティをドロップ。ユーザ上限に到達	1004	4
失敗したユーザのログイン	1004	5
VPN ユーザのログイン	1004	8
VPN ユーザのログオフ	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(4-54 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(4-55 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(4-56 ページ)
- 接続統計データ メッセージ(4-56 ページ)
- 接続チャック メッセージ(4-57 ページ)
- バージョン4.6.1+ のユーザ設定脆弱性メッセージ(4-57 ページ)
- ユーザ追加/削除ホスト メッセージ(4-58 ページ)
- ユーザ削除サーバ メッセージ(4-58 ページ)
- ユーザ設定ホスト重要度メッセージ(4-59 ページ)
- 属性メッセージ(4-59 ページ)
- 属性値メッセージ(4-60 ページ)
- ユーザサーバメッセージとオペレーティング システム メッセージ(4-60 ページ)
- ユーザ プロトコル メッセージ(4-61 ページ)
- ユーザ クライアント アプリケーション メッセージ(4-61 ページ)
- スキャン結果を追加メッセージ(4-62 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(4-63 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+\(4-172 ページ\)](#)を参照)。ホスト プロファイル データ ブロックのブロックタイプは、シリーズ1のブロックタイプ139です。

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



コメント

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\(B-291 ページ\)](#)を参照してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスカバリ イベント ヘッダー																																
ホストプロファイルデータ ブロック																																

サーバメッセージ

次の TCP サーバ イベント メッセージと UDP サーバ イベント メッセージには、標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-42 ページ)参照)があり、サーバ データ ブロック(ホストサーバデータブロック 4.10.0+(4-146 ページ)参照、シリーズ 1 のブロック タイプ 103)がそれに続きます。

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

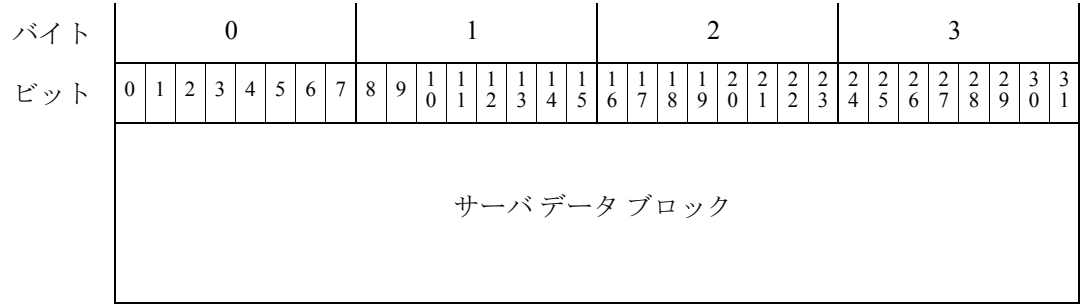


コメント

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

これらのイベントは、それぞれ次の形式を使用します:

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスカバリ イベント ヘッダー																																



新規ネットワークプロトコルメッセージ

新しいネットワークプロトコル 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 \(4-164 ページ\)](#)) 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。



コメント

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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスカバリ イベント ヘッダー																																
クライアント アプリケーション データ ブロック																																

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスカバリ イベント ヘッダー																																
[IP アドレス (IP Address)]																																

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスカバリ イベント ヘッダー																																
[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)																																

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+\(4-92 ページ\)](#)) 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスカバリ イベント ヘッダー																																
オペレーティング システム データ ブロック																																

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

バイト	0								1								2								3																	
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
ディスカバリ イベント ヘッダー																																										

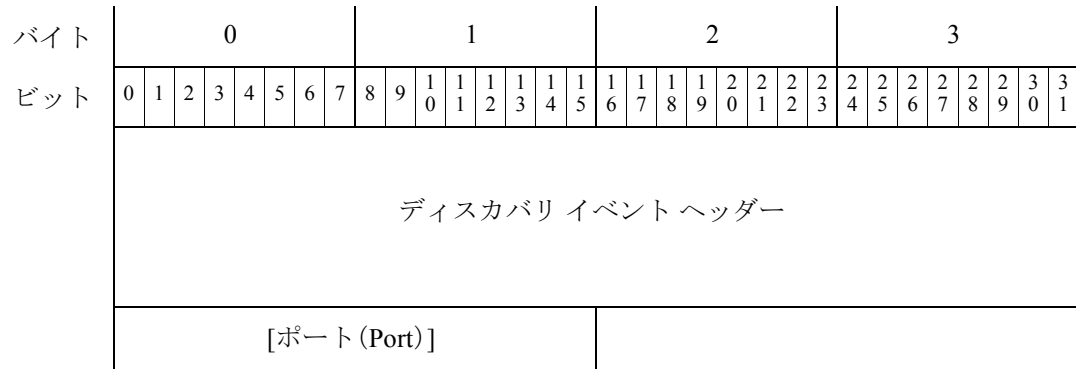
ホップ変更メッセージ

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。

バイト	0								1								2								3																	
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
ディスカバリ イベント ヘッダー																																										
								ホップ																																		

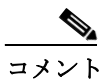
TCP と UDP のポート クローズ メッセージ/タイムアウトメッセージ

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

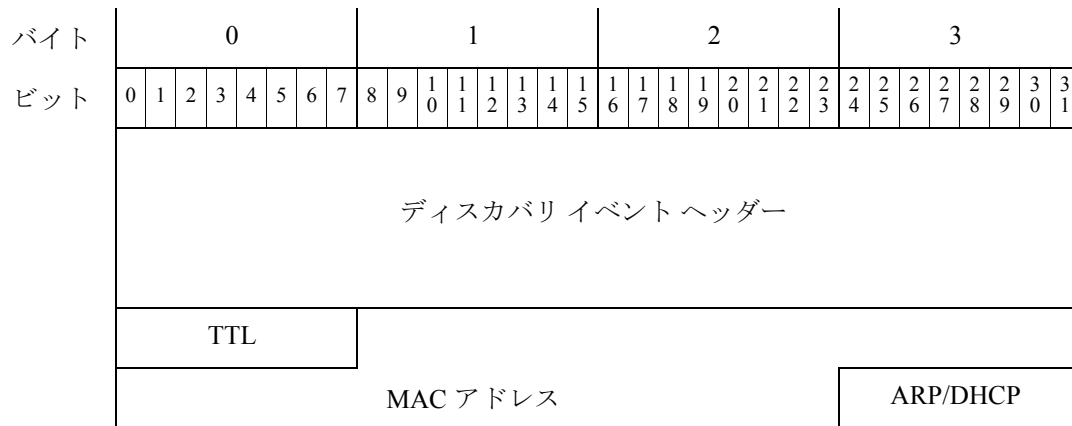
ホストの MAC 情報変更と追加 MAC 検出メッセージには、標準ディスカバリ イベント ヘッダー (ディスカバリ イベント ヘッダー 5.2+(4-42 ページ) を参照)、TTL 値の 1 バイト、MAC アドレスの 6 バイト、ARP/DHCP トラフィックで実際の MAC アドレスとして MAC アドレスを検出したかどうかを示す 1 バイトがあります。



コメント

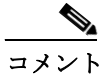
バージョン 4.9.x を実行するシステムから MAC アドレス メッセージを受信したら、MAC アドレスのデータ ブロックの長さを確認し、それに応じて復号してください。データ ブロックの長さが 8 バイト (16 バイトとヘッダー) の場合、MAC アドレス メッセージ (4-53 ページ) を参照してください。データ ブロックの長さが 12 バイト (20 バイトとヘッダー) の場合、ホスト MAC アドレス 4.9+(4-122 ページ) を参照してください。

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。



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。



コメント

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスカバリ イベント ヘッダー																																
文字列情報データ ブロック																																

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 バナーのデータ ブロックがそれに続きます(サーバ バナー データ ブロック (4-82 ページ)を参照)。サーバ バナーのデータ ブロックのブロック タイプは、シリーズ 1 のブロック タイプ 37 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスカバリ イベント ヘッダー																																
サーバ バナー データ ブロック																																

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、標準ディスクバリ イベント ヘッダーがあり ([ディスクバリ 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 \(4-93 ページ\)](#) を参照してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスクバリ イベント ヘッダー																																
ポリシー制御メッセージデータ ブロック																																

接続統計データ メッセージ

接続統計イベントには、標準ディスクバリ イベント ヘッダーがあり ([ディスクバリ 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 6.2+\(4-126 ページ\)](#) を参照してください。



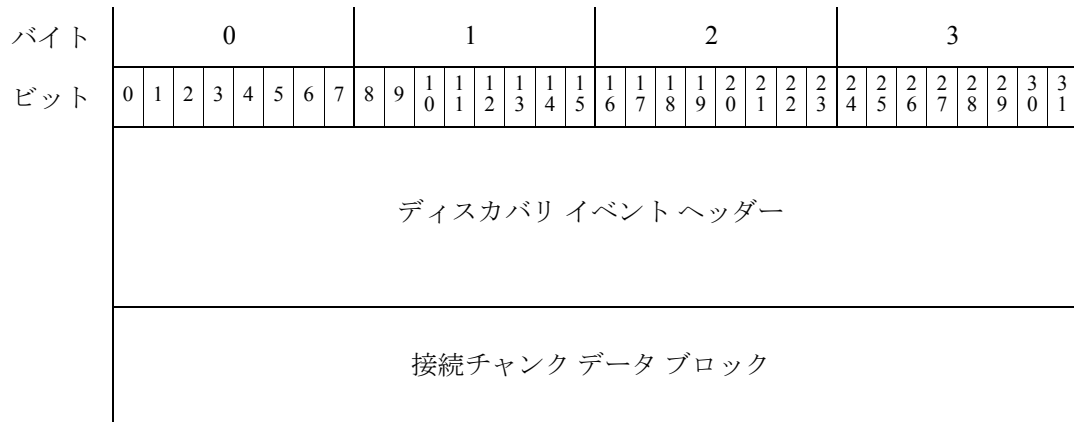
コメント

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 \(B-1 ページ\)](#)。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスクバリ イベント ヘッダー																																
接続統計データ ブロック																																

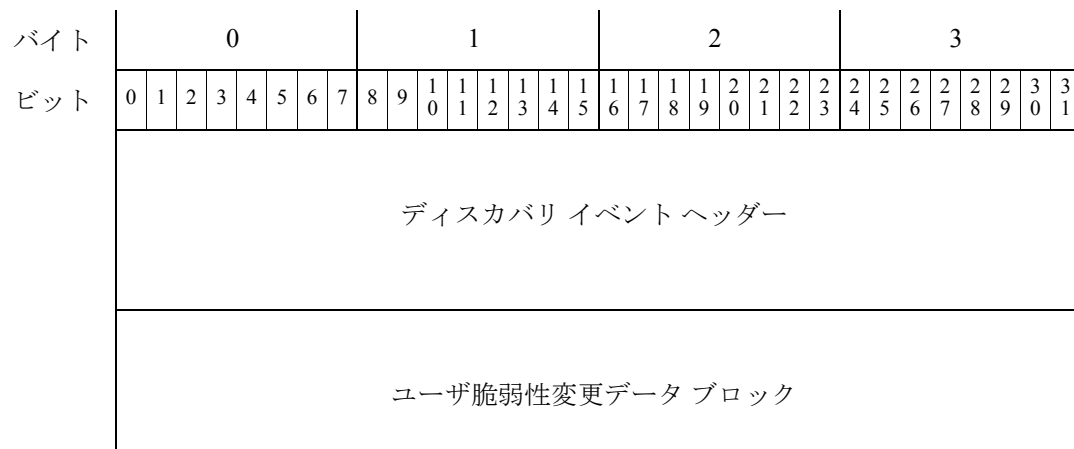
接続チャンク メッセージ

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 (4-107 ページ)を参照してください。接続チャンク データ ブロックのブロック タイプは、シリーズ 1 のブロック タイプ 136 です。



バージョン4.6.1+ のユーザ設定脆弱性メッセージ

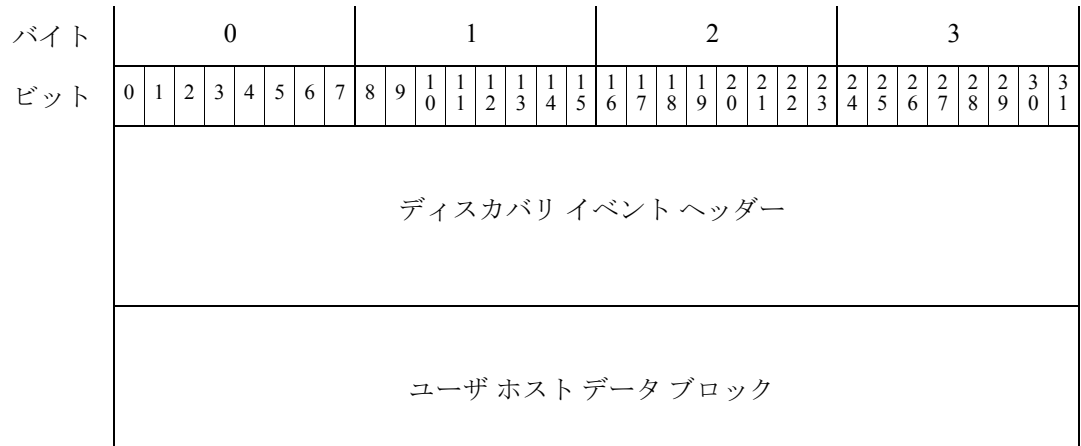
ユーザ設定の有効な脆弱性、ユーザ設定の無効な脆弱性、ユーザ脆弱性資格メッセージは、同じデータ形式を使用します。すなわち、標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-42 ページ)を参照)にユーザ脆弱性変更データ ブロックが続きます(ユーザ脆弱性変更データ ブロック 4.7+(4-114 ページ)を参照。シリーズ 1 のブロック タイプ 80)。これらはレコードタイプ、イベントタイプ、イベント サブタイプで区別します。



ユーザ追加/削除ホストメッセージ

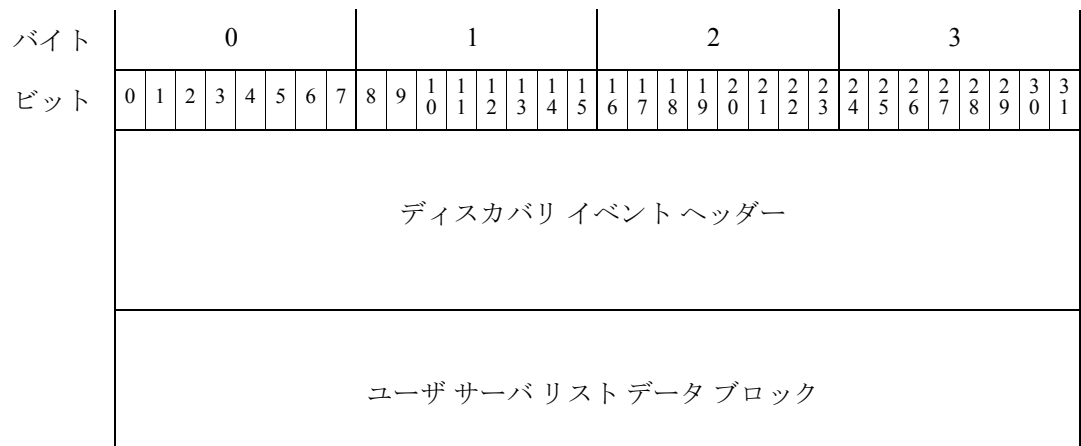
次のホスト入力イベントメッセージには、標準ディスクバリ イベントヘッダーがあり(ディスクバリ イベントヘッダー 5.2+(4-42 ページ)を参照)、ユーザホストデータブロックがそれに続きます(ユーザホストデータブロック 4.7+(4-112 ページ)を参照。シリーズ1のブロックタイプ78)。

- ユーザ削除アドレス
- ユーザ追加ホスト



ユーザ削除サーバメッセージ

ユーザ削除サーバメッセージには、標準ディスクバリ イベントヘッダーがあり(ディスクバリ イベントヘッダー 5.2+(4-42 ページ)を参照)、ユーザサーバリストデータブロックがそれに続きます(ユーザサーバリストデータブロック (4-111 ページ)を参照)。ユーザサーバリストデータブロックはシリーズ1のブロックタイプ77です。



ユーザ設定ホスト重要度メッセージ

ユーザ設定ホスト重要度メッセージには、標準ディスカバリ イベント ヘッダーがあり(ディスカバリ イベント ヘッダー 5.2+(4-42 ページ)を参照)、ユーザ重要度変更データ ブロックがそれに続きます(ユーザ重要度変更データ ブロック 4.7+(4-115 ページ)を参照)。ユーザ重要度変更データ ブロックのブロック タイプは、シリーズ 1 ブロック タイプ 81 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスカバリ イベント ヘッダー																																
ユーザ重要度変更データ ブロック																																

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(4-94 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:

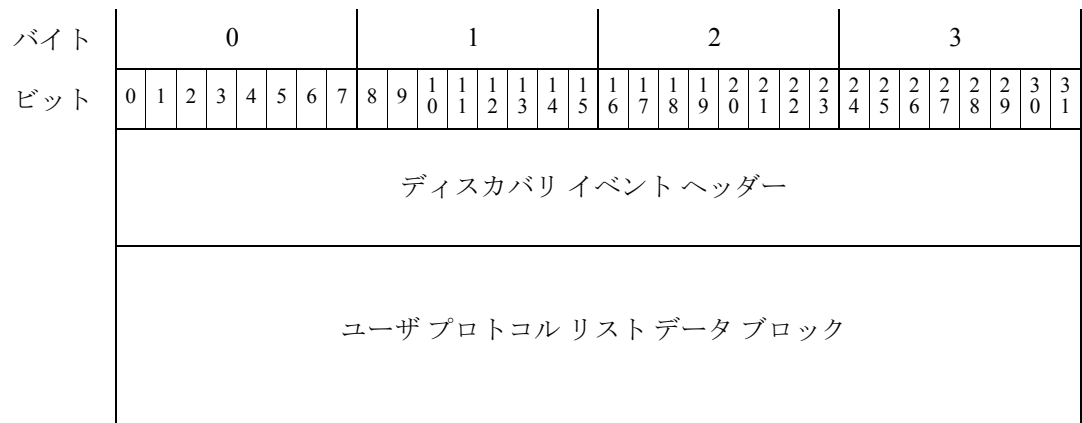
バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスカバリ イベント ヘッダー																																
属性定義データ ブロック																																

ユーザ プロトコル メッセージ

次のイベント メッセージには、標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-42 ページ)を参照)があり、ユーザ プロトコル リスト データ ブロック(ユーザ プロトコル リスト データ ブロック 4.7+(4-118 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:

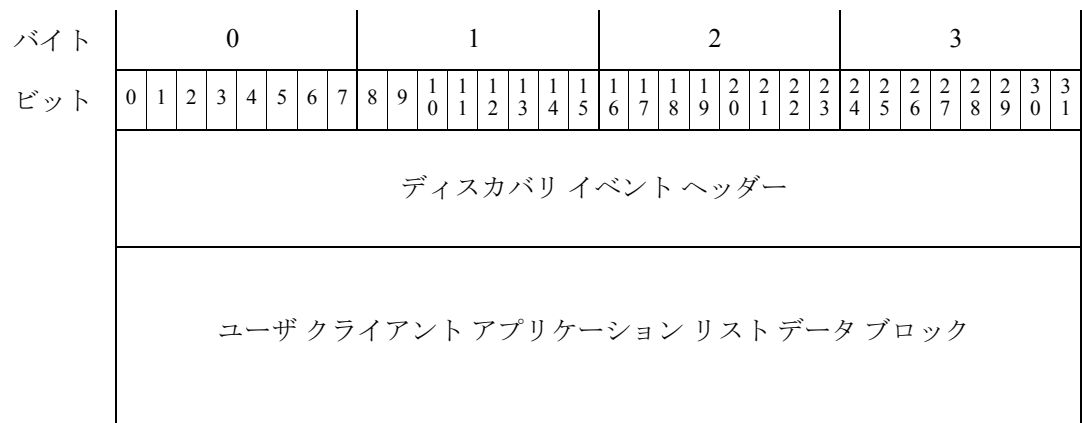


ユーザ クライアント アプリケーション メッセージ

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 クライアント アプリケーション リスト データ ブロック(ユーザ クライアント アプリケーション リスト データ ブロック (4-100 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

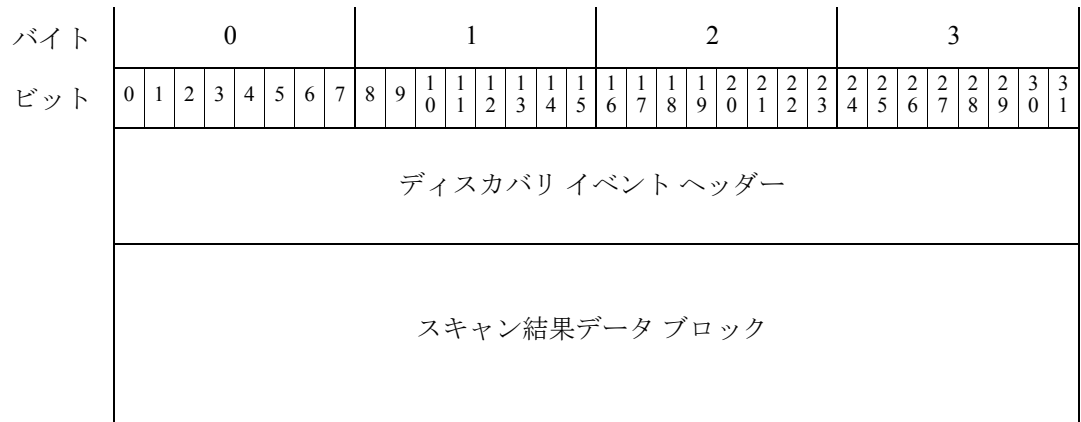
これらのイベントは、それぞれ次の形式を使用します:



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、標準ディスクバリ イベントヘッダー(ディスクバリ 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+(4-143 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。

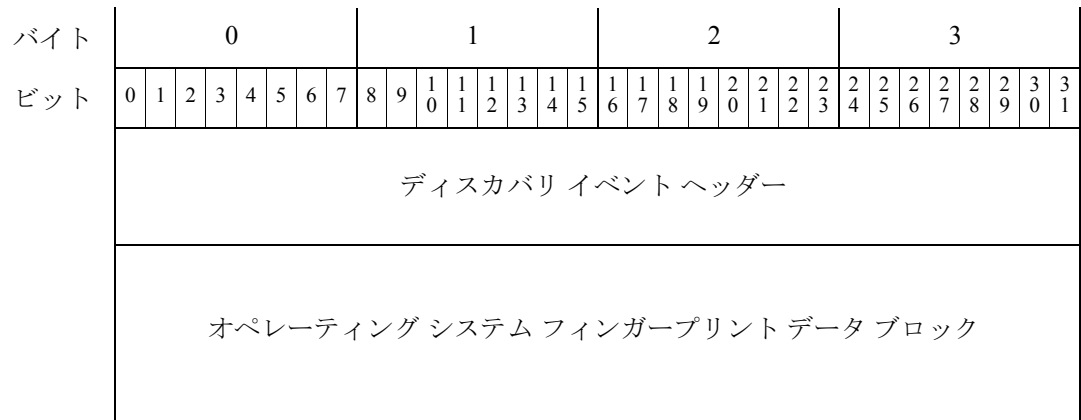
このイベントでは、次の形式を使用します。



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、標準ディスクバリ イベントヘッダー(ディスクバリ 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+(4-169 ページ)を参照)。

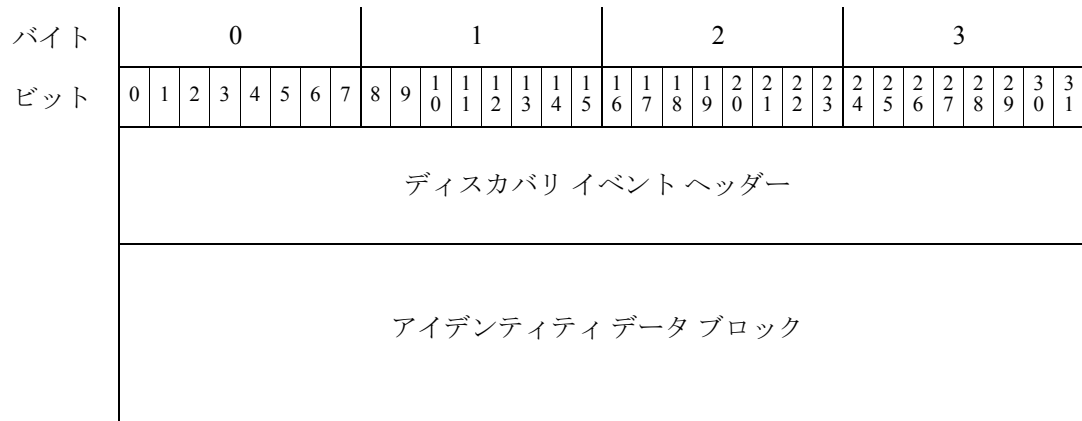
このイベントでは、次の形式を使用します。



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(4-121 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。

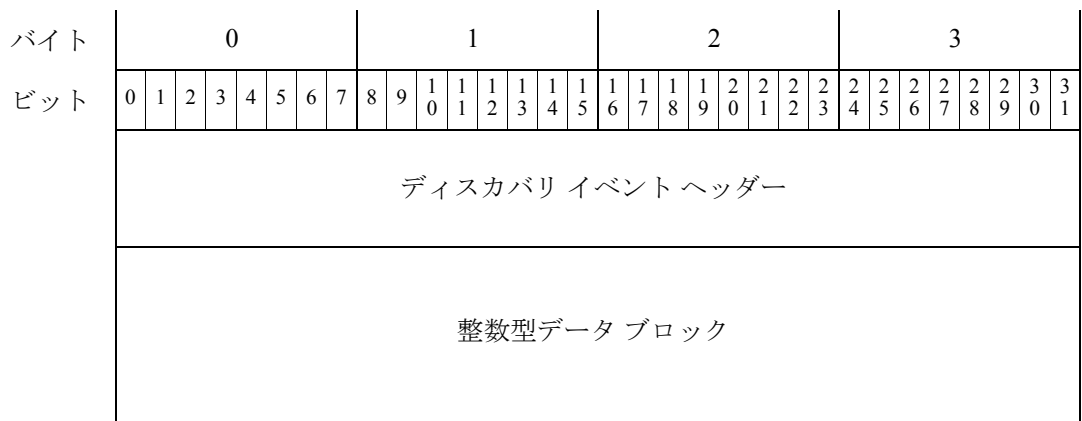
このイベントでは、次の形式を使用します。



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 データ構造

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

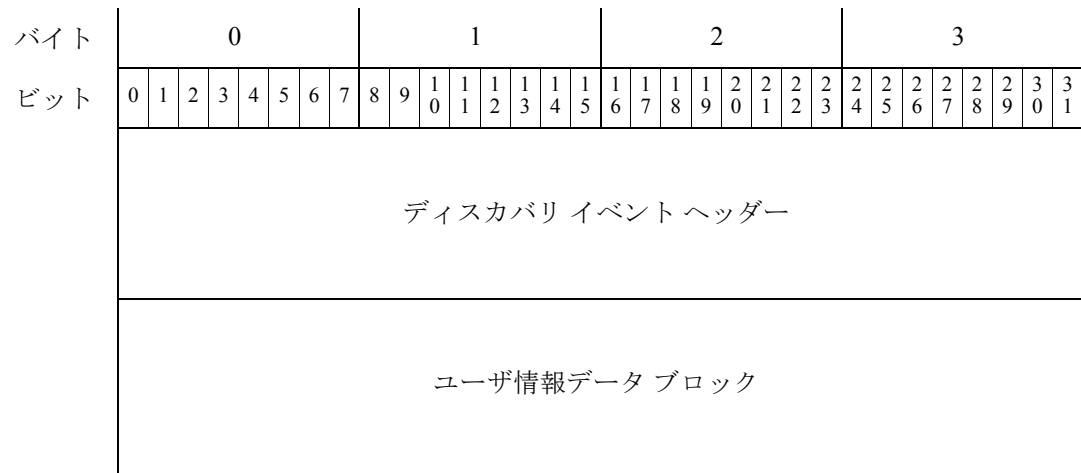
- [ユーザ変更メッセージ\(4-64 ページ\)](#)
- [ユーザ情報更新メッセージブロック\(4-64 ページ\)](#)

ユーザ変更メッセージ

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

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

ユーザ変更イベント メッセージには、標準ディスクバリ イベント ヘッダー([ディスクバリ イベント ヘッダー 5.2+\(4-42 ページ\)](#))を参照)があり、ユーザ情報データ ブロックがそれに続きます([6.0+ の情報データ ユーザ ブロック\(4-198 ページ\)](#)を参照)。ユーザ情報データ ブロックはシリーズ 1 ブロック タイプ 120 です。



ユーザ情報更新メッセージブロック

システムがユーザのログインの変更(ユーザ ログイン イベント — イベント タイプ 1004、サブタイプ2)を検出すると、ユーザ情報更新メッセージが送信されます。このブロックは、ユーザがログインに失敗したとき(失敗したユーザのログイン イベント: イベント タイプ 1004、サブタイプ 5)、VPN ユーザがログインするとき(VPN ユーザのログイン イベント: イベント タイプ 1004、サブタイプ 8)、または VPN ユーザがログオフするとき(VPN ユーザのログオフ 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)とユーザログイン情報データブロックがあります(ユーザログイン情報データブロック 6.2+(4-204 ページ)を参照)。ユーザログイン情報データブロックのブロックタイプは、シリーズ1ブロックタイプ121です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスカバリ イベントヘッダー																																
ユーザログイン情報データブロック																																


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(2-28 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
データブロックタイプ																																
データブロック長																																


コメント

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 イベントブロックタイプについては、[表 4-86 \(4-188 ページ\)](#)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	現在 (Current)	サーバで検出したサブサーバに関する情報を格納します。詳細については、 サブサーバデータブロック (4-78 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。

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
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。
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 (3-18 ページ) を参照してください。
31	汎用リスト	現在 (Current)	たとえば、クライアントアプリケーションブロックなど、カプセル化する汎用リスト情報をブロックリストをホストプロファイルブロックに格納します。詳細については、 汎用リストブロック (4-78 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	サーババナー	現在 (Current)	サーババナーデータを格納します。詳細については、 サーババナー データブロック (4-82 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。
42	ホストクライアントアプリケーション	レガシー	新規クライアントアプリケーションイベントのクライアントアプリケーション情報を格納します(本製品の旧バージョンを参照のこと)。
47	フルホストプロファイル	レガシー	ホストプロファイル情報一式を格納します(本製品の旧バージョンを参照のこと)。
48	属性値 (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 (4-88 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
51	フルサブサーバ	現在(Current)	サーバで検出したサブサーバに関する情報を格納します。フルサーバ情報ブロックとフルホストプロファイルで参照します。各サブサーバの脆弱性情報を格納します。詳細については、 フルサブサーバデータブロック(4-89ページ) を参照してください。
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+(4-92ページ) を参照してください。
54	ポリシーエンジン制御メッセージ	現在(Current)	ユーザポリシー制御の変更に関する情報を格納します。詳細については、 ポリシーエンジン制御メッセージデータブロック(4-93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(4-94ページ) を参照してください。
56	接続統計情報	レガシー	4.7 ~ 4.9.0 の接続統計イベントの情報を格納します(本製品の旧バージョンを参照のこと)。
57	ユーザプロトコル	現在(Current)	ユーザ入力のプロトコル情報を格納します。詳細については、 ユーザプロトコルデータブロック(4-97ページ) を参照してください。
59	ユーザクライアントアプリケーション	レガシー	ユーザ入力クライアントアプリケーションデータを格納します。詳細については、 ユーザクライアントアプリケーションデータブロック 5.0 ~ 5.1(B-97ページ) を参照してください。ブロック 138 に置き換わります。
60	ユーザクライアントアプリケーションリスト	現在(Current)	ユーザクライアントアプリケーションデータブロックのリストを格納します。詳細については、 ユーザクライアントアプリケーションリストデータブロック(4-100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-332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(4-105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
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。
65	ユーザ製品	レガシー	サードパーティ アプリケーション文字列マッピングなど、サードパーティ アプリケーションからインポートしたホスト入力データを格納します。詳細については、 ユーザ製品データブロック 5.0.x (B-102 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-153 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 (4-109 ページ) を参照してください。
71	汎用スキャン結果	レガシー	Nmap スキャンの結果を格納します(本製品の旧バージョンを参照のこと)。
72	スキャン結果	レガシー	サードパーティ スキャンの結果を格納します(本製品の旧バージョンを参照のこと)。
76	ユーザ サーバ	現在 (Current)	ユーザ入力イベントのサーバ情報を格納します。詳細については、 ユーザ サーバ データブロック (4-109 ページ) を参照してください。
77	ユーザ サーバリスト	現在 (Current)	ユーザサーバブロックのリストを格納します。詳細については、 ユーザ サーバリスト データブロック (4-111 ページ) を参照してください。
78	ユーザ ホスト	現在 (Current)	ユーザ ホスト入力イベントからのホスト範囲に関する情報を格納します。詳細については、 ユーザ ホスト データブロック 4.7+(4-112 ページ) を参照してください。
79	ユーザ脆弱性	レガシー	ホスト脆弱性に関する情報を格納します(本製品の旧バージョンを参照のこと)。バージョン 5.0 で導入したサクセサブロックのブロックタイプは 124 です。
80	ユーザ ホスト脆弱性の変更	現在 (Current)	非アクティブ化した脆弱性のリスト、またはアクティブ化した脆弱性のリストを格納します。詳細については、 ユーザ脆弱性変更データブロック 4.7+(4-114 ページ) を参照してください。
81	ユーザ重要度	現在 (Current)	ホストまたはホストの重要度の変更に関する情報を格納します。詳細については、 ユーザ重要度変更データブロック 4.7+(4-115 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	ユーザ属性値	現在(Current)	ホストの属性値の変更を格納します。詳細については、 ユーザ属性値データブロック 4.7+(4-117 ページ) を参照してください。
83	ユーザプロト コル リスト	現在(Current)	ホストのプロトコル リストを示します。詳細については、 ユーザプロトコル リストデータ ブロック 4.7+(4-118 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+(4-120 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-133 ページ) を参 照してください。バージョン 5.1 で導入したサク セサ ブロックのブロック タイプは 130 です。
88	サーバ情報	レガシー	サーバフィンガープリントで使用するサーバ情 報を格納します(本製品の旧バージョンを参照 のこと)。
89	ホスト/サーバ	レガシー	ホスト サーバ情報を格納します(本製品の旧 バージョンを参照のこと)。
90	フル ホスト サーバ	レガシー	ホスト サーバ情報を格納します(本製品の旧 バージョンを参照のこと)。
91	ホストプロ ファイル	レガシー	ホストのプロファイル情報を格納します。詳細 については、 ホストプロファイルデータブロッ ク 5.2+(4-172 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 (4-121 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	レガシー	ホストサーバ情報を格納します(本製品の旧バージョンを参照のこと)。
99	フルホストサーバ	レガシー	ホストサーバ情報を格納します(本製品の旧バージョンを参照のこと)。
100	ホストクライアントアプリケーション	レガシー	新規クライアントアプリケーションイベントのクライアントアプリケーション情報を格納します(本製品の旧バージョンを参照のこと)。バージョン 5.0 で導入したサクセサブロックタイプ 122 には、ブロックタイプ 100 と同じ構造があります。
101	接続統計情報	レガシー	4.9.1+ の接続統計イベントの情報を格納します(本製品の旧バージョンを参照のこと)。
102	スキャン結果	レガシー	脆弱性に関する情報を格納しており、スキャン結果を追加イベントで使用します。 スキャン結果データブロック 5.0 ~ 5.1.1.x (B-99 ページ) を参照してください。
103	ホスト/サーバ	現在 (Current)	ホストサーバ情報を格納します。詳細については、 ホストサーバデータブロック 4.10.0+ (4-146 ページ) を参照してください。
104	フルホストサーバ	現在 (Current)	ホストサーバ情報を格納します。詳細については、 フルホストサーバデータブロック 4.10.0+ (4-148 ページ) を参照してください。
105	サーバ情報	レガシー	サーバフィンガープリントで使用するサーバ情報を格納します。詳細については、 4.10.x, 5.0 ~ 5.0.2 のサーバ情報データブロック (4-152 ページ) を参照してください。5.0 で導入したサクセサブロックタイプ 117 には、ブロックタイプ 105 と同じ構成があります。
106	フルサーバ情報	現在 (Current)	ホストで検出したサーバに関する情報を格納します。詳細については、 フルサーバ情報データブロック (4-154 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 (4-157 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 (4-159 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-291 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+ (4-162 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-135 ページ) を参照してください。バージョン 5.1 で導入したサクセサブロックのブロックタイプは 126 です。
117	サーバ情報	現在 (Current)	サーバフィンガープリントで使用するサーバ情報を格納します。詳細については、 4.10.x, 5.0 ~ 5.0.2 のサーバ情報データブロック (4-152 ページ) を参照してください。
118	ユーザ製品	レガシー	サードパーティアプリケーション文字列マッピングなど、サードパーティアプリケーションからインポートしたホスト入力データを格納します。詳細については、 ユーザ製品データブロック 5.0.x (B-102 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	接続チャック	レガシー	バージョン 4.10.1 ~ 5.1 の接続チャック情報を格納します。詳細については、 接続チャックデータブロック 5.0 ~ 5.1 (B-153 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 (4-164 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 (4-125 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	ユーザ脆弱性	現在 (Current)	ホスト脆弱性に関する情報を格納します。 ユーザ脆弱性データブロック 5.0+(4-166 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-140 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+(4-169 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 (4-171 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-312 ページ) を参照してください。これはブロックタイプ 91 に置き換わります。ブロック 139 に置き換わります。
134	ユーザ製品	現在 (Current)	サードパーティアプリケーション文字列マッピングなど、サードパーティアプリケーションからインポートしたホスト入力データを格納します。詳細については、 ユーザ製品データブロック 5.1+(4-180 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-301 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	接続チャック	現在 (Current)	接続チャック情報を格納します。詳細については、 6.1+ の接続チャックデータブロック (4-107 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-153 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	ユーザクライアントアプリケーション	現在 (Current)	ユーザ入力 of クライアントアプリケーション データを格納します。詳細については、 5.1.1+ のユーザクライアントアプリケーション データブロック (4-98 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+(4-172 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+(4-143 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 (4-104 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-146 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 IOC の変更	Current	ユーザの 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 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-163 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-170 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-177 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-191 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-205 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 6.2+ (4-126 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。

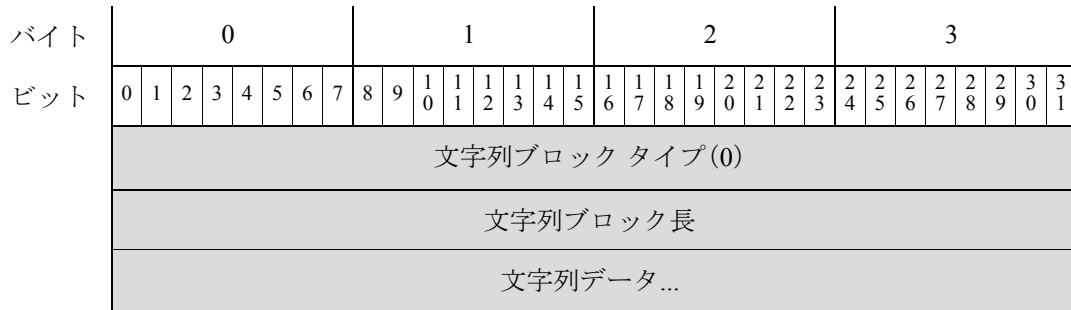
文字列データブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ0です。



コメント

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

次の図に、文字列データ ブロックの形式を示します。



次の表に、文字列データ ブロックのフィールドの説明を示します。

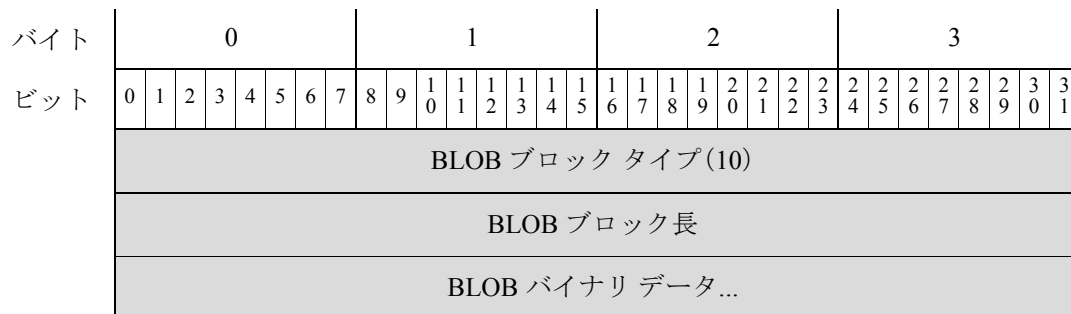
表 4-31 文字列データ ブロックのフィールド

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

BLOB データ ブロック

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

次の図に、BLOB データ ブロックの形式を示します。



次の表に、BLOB データ ブロックのフィールドの説明を示します。

表 4-32 BLOB データ ブロック フィールド

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

リスト データ ブロック

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

次の図に、リスト データ ブロックの基本的な形式を示します。



次の表では、リスト データ ブロックのフィールドについて説明します。

表 4-33 リスト データ ブロックのフィールド

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

サブサーバデータブロック

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

次の図は、サブサーバデータブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	サブサーバブロック タイプ(1)																															
	サブサーバブロック長																															
サブサーバ [名前(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、サブサーバデータブロックのフィールドについて説明します。

表 4-35 サブサーバデータブロックのフィールド

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

表 4-36 プロトコルデータブロックのフィールド(続き)

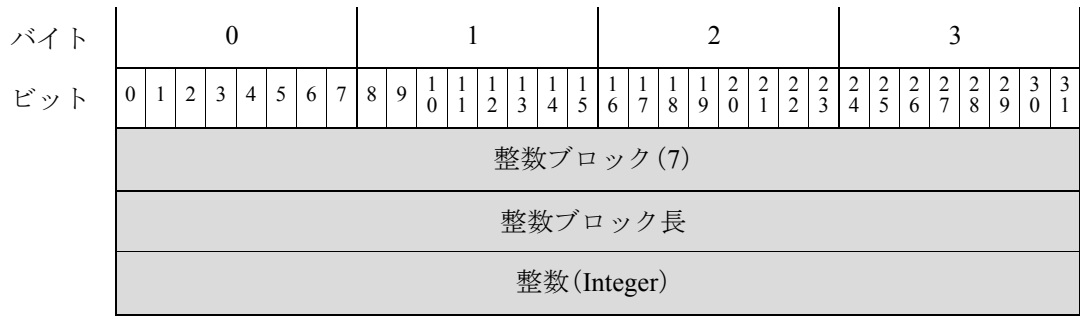
フィールド	データタイプ	説明
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 <ul style="list-style-type: none"> • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 <ul style="list-style-type: none"> • 2048:IP

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。

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
	サーババナー ブロック タイプ (37)																																
	サーババナー ブロック 長																																
	ポート																プロトコル								BLOB ブロック タイプ								サーババナー (BLOB)
	BLOB ブロック タイプ (10) (続き)																BLOB 長																
	BLOB 長 (続き)																サーババナー データ...																
	サーババナー データ (続き).....																																

次の表では、サーババナー データ ブロックのフィールドについて説明します。

表 4-39 サーババナー データ ブロックのフィールド

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

文字列情報データ ブロック

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

次の図は、文字列情報データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	文字列情報ブロック タイプ (35)																															
	文字列情報ブロック長																															
CVE ID	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	値...																															

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

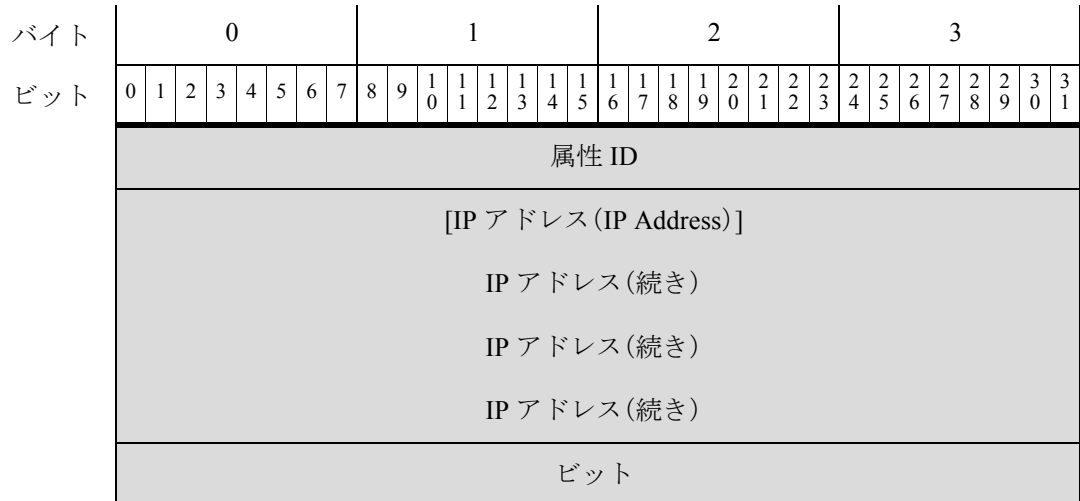
フィールド	データタイプ	説明
文字列情報ブロックタイプ	uint32	文字列情報データ ブロックを開始します。この値は常に 35 です。
文字列情報ブロック長	uint32	文字列情報データ ブロック ヘッダーと文字列情報データを組み合わせた長さ。
文字列ブロックタイプ	uint32	値を含む文字列データ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、値のバイト数を加えた値の文字列データ ブロックのバイト数。
値	string	文字列情報データ ブロックを使用した脆弱性のデータ ブロックの Common Vulnerabilities and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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	属性アドレスブロック タイプ (146)																															
	属性アドレスブロック長																															



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 IOC の変更データ ブロック 5.3+

ユーザ IOC の変更データ ブロックには、ユーザが行った IOC の変更に関する情報が含まれています。これは、ユーザ ホスト IOC の削除、ユーザ ホスト IOC の有効化、およびユーザ 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 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ IOC の変更ブロック タイプ (148)																															
	[ユーザ ID (User ID)]																															
	ソース タイプ																															
[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 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 IOC の変更データ ブロック 5.3+ フィールド

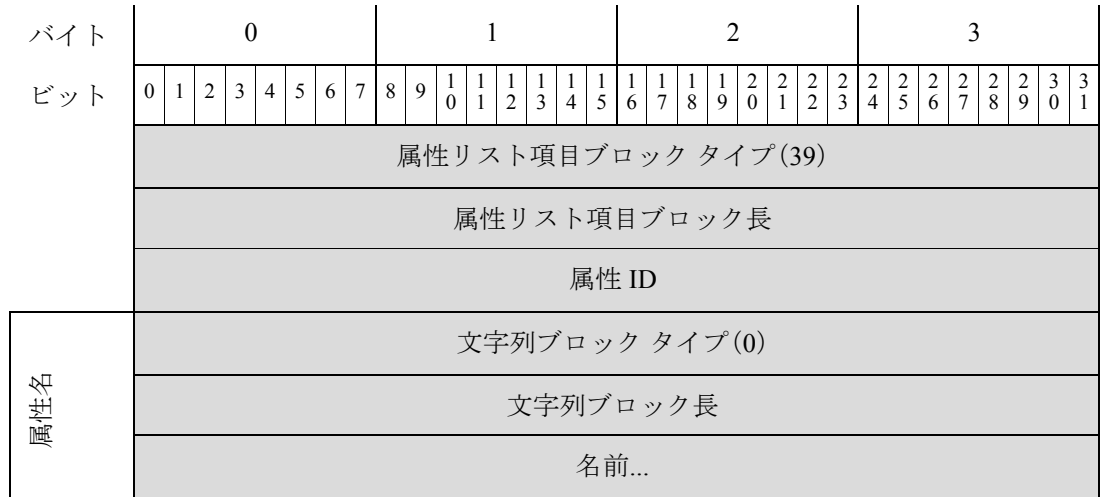
フィールド	データタイプ	説明
ユーザ IOC の変更ブロック タイプ	uint32	ユーザ IOC の変更データブロックを開始します。この値は、常に 148 です。
ユーザ ID (User ID)	uint32	IOC に変更を加えたユーザの ID 番号。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> 無応答 (RNA) がクライアントデータを検出した場合、0 ユーザがクライアントデータを提供した場合、1 サードパーティ スキャナがクライアントデータを検出した場合、2 nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでクライアント データを提供した場合、3
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。

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

フィールド	データタイプ	説明
IOC ID	uint32	変更された IOC の ID 番号。
ターゲット UID	uint32	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。

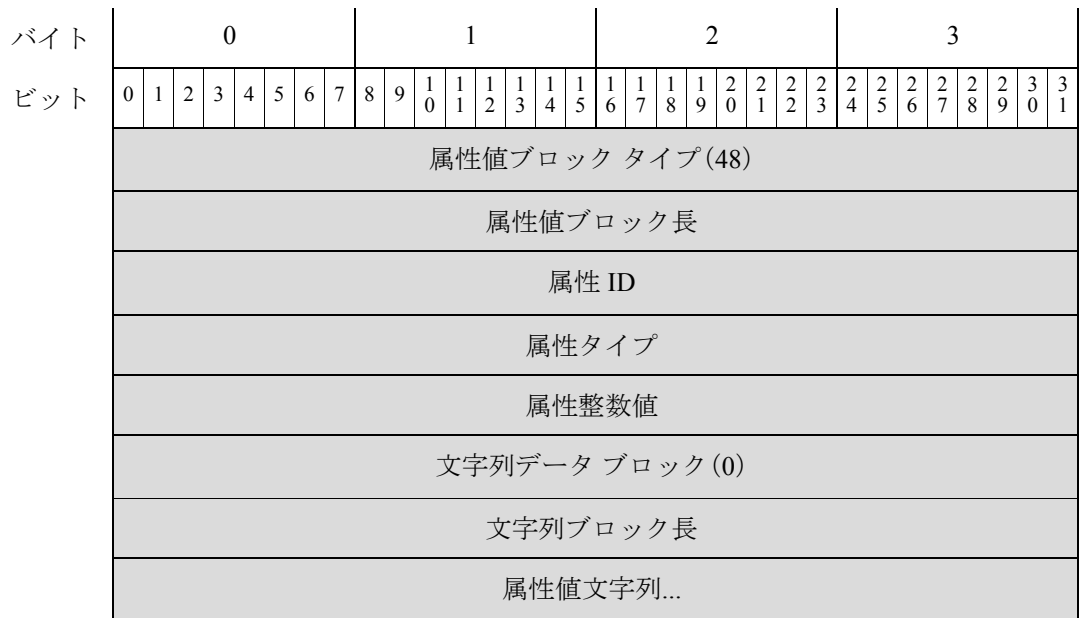
表 4-43 属性リスト項目データブロックのフィールド(続き)

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。

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
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。 <ul style="list-style-type: none"> 0: 値としてのテキストによる属性。文字列データを使用します 1: 範囲の値による属性。整数型データを使用します 2: 使用可能値のリストによる属性。整数型データを使用します 3: 値としての URL による属性。文字列データを使用します 4: 値としてのバイナリ BLOB による属性。文字列データを使用します
属性整数値	uint32	属性に整数値(該当する場合)。
文字列ブロックタイプ	uint32	属性名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロックタイプフィールドと長さフィールドに属性名のバイト数を加えた文字列データブロックのバイト数。
属性値(Attribute Value)	string	属性値。

フルサブサーバデータブロック

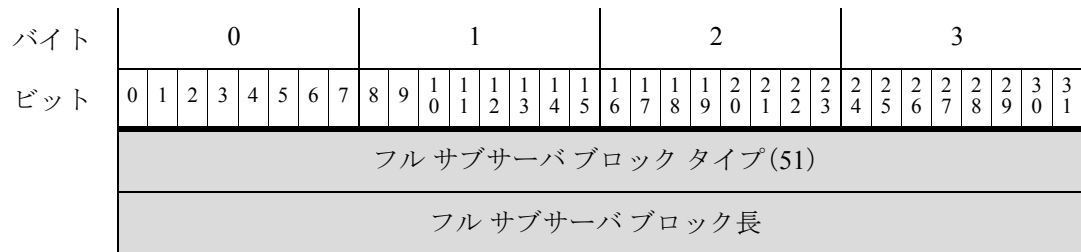
フルサーバデータブロックは、ホストで検出したサーバに関連付けられたサブサーバに関する情報を伝えます。サブサーバに関する情報には、ホスト上のサブサーバのベンダー、バージョン、関連 VDB、サードパーティの脆弱性などがあります。サブサーバは、固有の関連脆弱性があるサーバの読み込み可能なモジュールです。フルホストサーバデータブロックには、ホストで検出した各サーバのフルサブサーバデータブロックが含まれます。フルホストサーバデータブロックのブロックタイプは、シリーズ 1 ブロックグループのブロックタイプ 51 です。



コメント

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

次の図は、フルサブサーバデータブロックの形式です。



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

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

表 4-45 フルサブサーバデータブロックのフィールド

フィールド	データタイプ	説明
フルサブサーバ ブロックタイプ	uint32	フルサブサーバブロックを開始します。この値は常に 51 です。
フルサブサーバ ブロック長	uint32	フルサブサーバブロックタイプフィールドと長さフィールドの 8 バイトに、後続のフルサブサーバブロックのバイト数を加えたフルサブサーバデータブロックの合計バイト数。
文字列ブロック タイプ	uint32	サブサーバ名を格納した文字列データブロックを開始します。この値は常に 0 です。
文字列ブロッ ク長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにサブサーバ名のバイト数を加えたサブサーバ名文字列データブロックのバイト数。

表 4-45 フルサブサーバデータブロックのフィールド(続き)

フィールド	データタイプ	説明
サブサーバ名	string	サブサーバ名。
文字列ブロックタイプ	uint32	サブサーバベンダー名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにサブサーバ名のバイト数を加えたベンダー名文字列データブロックのバイト数。
サブサーバベンダー名	string	サブサーバベンダーの名前。
文字列ブロックタイプ	uint32	サブサーババージョンを格納した文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにサブサーババージョンのバイト数を加えたサブサーババージョン文字列データブロックのバイト数。
サブサーババージョン	string	サブサーバ長
汎用リストブロックタイプ	uint32	VDB 脆弱性データを伝えるホスト脆弱性データブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべてのホスト脆弱性データブロックを含む汎用リストデータブロックのバイト数。
VDB ホスト脆弱性ブロック*	変数 (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+(4-120 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+(4-120 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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	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。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	ポリシー エンジン制御メッセージブロック タイプ (54)																																							
	ポリシー エンジン制御メッセージブロック長																																							
	タイプ (Type)																																							
Control メッセージ	文字列ブロック タイプ (0)																																							
	文字列ブロック長																																							
	制御メッセージ...																																							

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 (Type)	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。

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

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
	属性リスト項目ブロック タイプ(39)																															属性一覧 項目をリスト	
	属性リスト項目ブロック長																																
	リストブロック タイプ(11)																																
項目をリスト	リストブロック長																																
	属性リスト項目...																																
	属性アドレスブロック タイプ(38)																															属性一覧 アドレス	
属性アドレスブロック長																																	
リストブロック タイプ(11)																																	
アドレス一覧	リストブロック長																																
	属性アドレス リスト...																																

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。
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、スキャナ、またはサーブパーティ 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。

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
属性タイプ	uint32	属性のタイプ。値は以下のとおりです。 <ul style="list-style-type: none"> 0: 値としてのテキストによる属性。文字列データを使用します 1: 範囲の値による属性。整数型データを使用します 2: 使用可能値のリストによる属性。整数型データを使用します 3: 値としての URL による属性。文字列データを使用します 4: 値としてのバイナリ BLOB による属性。文字列データを使用します
属性カテゴリ	uint32	属性カテゴリ
範囲の開始値	uint32	定義した属性の整数範囲内の最初の整数。
範囲の終了値	uint32	定義した属性の整数範囲の最後の整数。
自動割り当て IP アドレス フラグ	uint32	属性に基づいて IP アドレスが自動的に割り当てられるかどうかを示すフラグ。
リストブロックタイプ	uint32	属性リスト項目を伝える属性リスト項目データブロックリストで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべての属性リスト項目データブロックを加えた値です。 このフィールドの後にはゼロか、さらに属性リスト項目のデータブロックが続きます。
属性リスト項目ブロックタイプ	uint32	最初の属性リスト項目データブロックを開始します。このデータブロックには、他の属性リスト項目データブロックを、リストブロック長フィールドで定義した上限まで続けることができます。
属性リスト項目ブロック長	uint32	ブロックタイプフィールドとヘッダーフィールドの 8 バイトに属性リスト項目のバイト数を加えた属性リスト項目文字列データブロックのバイト数。
属性リスト項目	変数 (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。

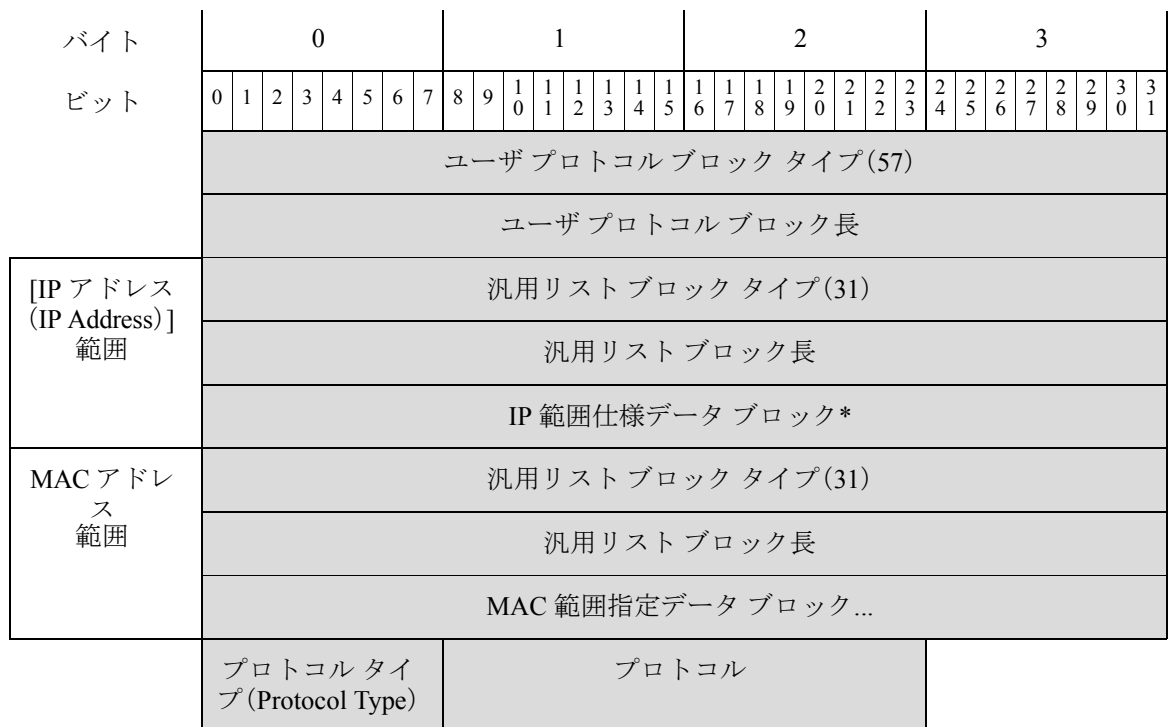
表 4-48 属性定義データブロックのフィールド(続き)

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。

ユーザプロトコルデータブロック

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

次の図は、ユーザプロトコルデータブロックの基本構造です。



次の表では、ユーザプロトコルデータブロックのフィールドについて説明します。

表 4-49 ユーザプロトコルデータブロックのフィールド

フィールド	バイト数	説明
ユーザプロトコルブロックタイプ	uint32	ユーザプロトコルデータブロックを開始します。この値は常に 57 です。
ユーザプロトコルブロック長	uint32	ユーザプロトコルブロックタイプフィールドと長さフィールドの 8 バイトに、後続のユーザプロトコルデータのバイト数を加えたユーザプロトコルデータブロックの合計バイト数。
汎用リストブロックタイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データブロック* で構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべての IP 範囲仕様データブロック* を含む汎用リストデータブロックのバイト数。
IP 範囲仕様データブロック*	変数 (variable)	ユーザ入力 of 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)	ユーザ入力 of 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 (4-105 ページ) を参照してください。
プロトコルタイプ (Protocol Type)	uint8	プロトコルのタイプを示します。プロトコルには、IP などネットワーク層プロトコルの 0、または TCP や UDP などトランスポート層プロトコルの 1 があります。
プロトコル	uint16	データブロックに格納されるデータのプロトコルを示します。

5.1.1+ のユーザクライアントアプリケーションデータブロック

ユーザクライアントアプリケーションデータブロックには、クライアントアプリケーションデータの送信元に関する情報、データを追加したユーザの ID 番号、および IP アドレス範囲データブロックのリストが含まれます。バージョン 6.3 に追加されたペイロード ID は、レコードに関連付けられたアプリケーションインスタンスを指定します。ユーザクライアントアプリケーションデータブロックのブロックタイプは、シリーズ 1 ブロックグループのブロックタイプ 138 です。ブロックタイプ 59 を置換します。

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザクライアントアプリケーションブロック タイプ(138)																															
	ユーザ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 ユーザクライアントアプリケーションデータブロックのフィールド

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

表 4-50 ユーザクライアントアプリケーションデータブロックのフィールド(続き)

フィールド	バイト数	説明
IP 範囲仕様データ ブロック*	変数 (variable)	ユーザ入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データ ブロック。このデータ ブロックの説明の詳細については、 5.2+ の IP アドレス範囲データ ブロック (4-101 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)。

ユーザクライアントアプリケーションリストデータブロック

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

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



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

表 4-51 ユーザクライアント アプリケーション リスト データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ クライアント アプリケーション リスト ブロック タイプ	uint32	ユーザ クライアント アプリケーション リスト データ ブロックを開始します。この値は常に 60 です。
ユーザ クライアント アプリケーション リスト ブロック 長	uint32	ユーザ クライアント アプリケーション リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザ クライアント リスト アプリケーション データのバイト数を加えたユーザ クライアント アプリケーション リスト データ ブロックの合計バイト数。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> 無応答 (RNA) がクライアント データを検出した場合、0 ユーザがクライアント データを提供した場合、1 サードパーティ スキャナがクライアント データを検出した場合、2 nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでクライアント データを提供した場合、3
ソース	uint32	影響を受けるクライアント アプリケーションを追加した送信元にマッピングする ID 番号。送信元タイプによって、これは無応答 (RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
汎用 リスト ブロック タイプ	uint32	汎用 リスト データ ブロックを開始します。この値は常に 31 です。
汎用 リスト ブロック 長	uint32	汎用 リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用 リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
ユーザ クライアント アプリケーション ブロック	変数 (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 クライアント アプリケーション データ ブロック。ユーザ クライアント アプリケーション データ ブロックの詳細については、 5.1.1+ のユーザ クライアント アプリケーション データ ブロック (4-98 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 プロトコル、ユーザ クライアント アプリケーション、アドレス指定、ユーザ 製品、ユーザ サーバ、ユーザ ホスト、ユーザ 脆弱性、ユーザ 重要度、ユーザ 属性値データ ブロックで使用します。IP アドレス範囲データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 141 です。

次の図は、IP アドレス範囲データ ブロックの形式です。

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

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

表 4-52 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。

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

次の表では、属性指定データ ブロックのコンポーネントについて説明します。

表 4-53 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。
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 プロトコル、アドレス指定、ユーザ ホスト データ ブロックで使用します。ホスト IP データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 143 です。

次の図は、ホスト IP アドレス データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ホスト IP アドレス指定ブロック タイプ (143)																																
ホスト IP アドレス 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)																																
最後の確認日時																																

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

次の図は、MAC アドレス指定データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MAC アドレス指定ブロック タイプ (63)																																
MAC アドレス指定ブロック長																																
MAC ブロック 1								MAC ブロック 2								MAC ブロック 3								MAC ブロック 4								
MAC ブロック 5								MAC ブロック 6																								

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。
MAC アドレス指定ブロック長	uint32	MAC アドレス指定ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続の MAC アドレス指定データのバイト数を加えた MAC アドレス指定データ ブロックの合計バイト数。
MAC アドレス ブロック サイズ 1 ~ 6	uint8	順に並んだ MAC アドレス ブロック。

アドレス指定データ ブロック

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

次の図は、アドレス指定データ ブロックの基本構造です。

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

次の表では、アドレス指定データ ブロックのフィールドについて説明します。

表 4-56 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。

表 4-56 アドレス指定データブロックのフィールド(続き)

フィールド	バイト数	説明
汎用リストブロック長	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 (4-105 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。



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

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ドの IP アドレスに使用して、同一の接続を識別します。
レスポンド IP アドレス	uint8(4)	この接続タイプのレスポンドの IP アドレス。このアドレスは、イニシエータとオリジナルクライアントの IP アドレスに使用して、同一の接続を識別します。
オリジナルクライアント IP アドレス	uint8(4)	要求の送信元であるプロキシの背後にあるホストの IP アドレス。これは、イニシエータとレスポンドの 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。
レスポンドポート	uint16	接続チャンクでレスポンドが使用したポート。
プロトコル	uint8	ユーザ情報を含むパケットのプロトコル。
接続タイプ	uint8	接続の種類。
NetFlow ディテクタ IP アドレス	uint8[4]	IP アドレス オクテットの、接続を検出した NetFlow デバイスの IP アドレス。
送信パケット数	uint64	接続チャンクで送信されたパケット数。
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。

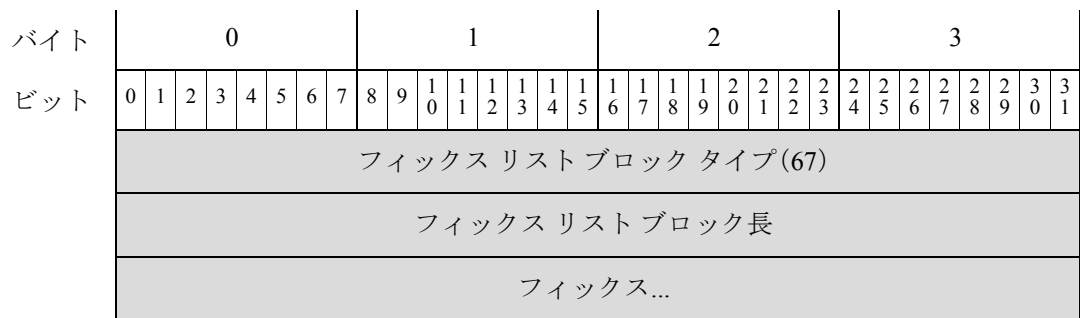
表 4-57 接続チャンク データブロックのフィールド(続き)

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

フィックス リスト データ ブロック

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

次の図は、フィックス リスト データ ブロックの形式です。



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

表 4-58 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 サーバ データ ブロック

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

次の図は、ユーザ サーバ データ ブロックの基本構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザサーバデータブロックタイプ(76)																															
	ユーザサーバブロック長																															
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アドレス範囲の固有ブロック*																															
	ポート																プロトコル															

次の表では、ユーザサーバデータブロックのフィールドについて説明します。

表 4-59 ユーザサーバデータブロックのフィールド

フィールド	バイト数	説明
ユーザサーバデータブロックタイプ	uint32	ユーザサーバデータブロックを開始します。この値は常に 76 です。
ユーザサーバブロック長	uint32	ユーザサーバブロックタイプフィールドと長さフィールドの 8 バイトに、後続のユーザサーバデータのバイト数を加えたユーザサーバデータブロックの合計バイト数。
汎用リストブロックタイプ	uint32	汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストブロックとカプセル化されたデータブロックのバイト数。この値は、汎用リストブロックヘッダーフィールドの 8 バイトに、カプセル化されたすべてのデータブロックのバイト数を加えた値です。
IPアドレス範囲指定データブロック	変数 (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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 2048:IP

ユーザサーバリストデータブロック

ユーザサーバリストデータブロックには、ユーザ入力サーバリストデータブロックを格納します。ユーザサーバリストデータブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ77です。次の図は、ユーザサーバリストデータブロックの基本構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザサーバリストデータブロックタイプ(77)																															
	ユーザサーバリストブロック長																															
	ソースタイプ																															
	ソース																															
ユーザ(User)サーバブロック	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	ユーザサーバデータブロック*																															

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

表 4-60 ユーザサーバリストデータブロックのフィールド

フィールド	バイト数	説明
ユーザサーバリストデータブロックタイプ	uint32	ユーザサーバリストデータブロックを開始します。この値は常に 77 です。
ユーザサーバリストブロック長	uint32	ユーザサーバリストブロックタイプフィールドと長さフィールドの 8 バイトに、後続のユーザサーバリストデータのバイト数を加えたユーザサーバリストデータブロックの合計バイト数。
ソースタイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> 無応答(RNA) がサーバデータを検出した場合、0 ユーザがサーバデータを提供した場合、1 サードパーティ スキャナがサーバデータを検出した場合、2 nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでサーバデータを提供した場合、3
ソース	uint32	サーバデータの送信元にマッピングする ID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
汎用リストブロックタイプ	uint32	汎用リストデータブロックを開始します。この値は常に 31 です。

表 4-60 ユーザサーバリスト 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。
ユーザサーバデータブロック	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サーバデータブロック。

ユーザ ホスト データ ブロック 4.7+

ユーザ ホスト データ ブロックは、[ユーザ追加/削除ホストメッセージ\(4-58 ページ\)](#)で使用し、ホスト範囲、ユーザ ホスト入力イベントから得られるユーザ アイデンティティとソース アイデンティティに関する情報を格納します。ユーザ ホスト データ ブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ78です。

次の図は、ユーザ ホスト データ ブロックの基本構造です。



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

表 4-61 ユーザホストデータブロックのフィールド

フィールド	バイト数	説明
ユーザ ホスト ブロック タイプ	uint32	ユーザ ホストデータブロックを開始します。この値は常に 78 です。
ユーザ ホスト ブロック長	uint32	ユーザ ホストブロックタイプフィールドと長さフィールドの 8 バイトに、後続のユーザホストデータのバイト数を加えたユーザホストデータブロックの合計バイト数。
汎用リストブ ロックタイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データブロック* で構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブ ロック長	uint32	リストヘッダーとカプセル化されたすべての IP 範囲仕様データブロック* を含む汎用リストデータブロックのバイト数。
IP 範囲仕様デー タブロック*	変数 (variable)	ユーザ入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データブロック。このデータブロックの説明の詳細については、 5.2+ の IP アドレス範囲データブロック (4-101 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 (4-105 ページ) を参照してください。
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、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: <ul style="list-style-type: none"> • 無応答 (RNA) がホストデータを検出した場合、0 • ユーザがホストデータを提供した場合、1 • サードパーティ スキャナがホストデータを検出した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでホストデータを提供した場合、3

ユーザ脆弱性変更データ ブロック 4.7+

ユーザ脆弱性変更データ ブロックには、非アクティブ化したホスト脆弱性、脆弱性を非アクティブ化したユーザ、脆弱性変更を提供した送信元に関する情報、重要度値を格納します。ユーザ脆弱性変更データブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ80です。前のユーザ脆弱性変更データブロックからの変更では、新規ソースタイプフィールドが加えられ、リストデータブロックの代わりに、汎用リストデータブロックで脆弱性非アクティブ化を保存するようになりました。このデータブロックは、ユーザ脆弱性変更メッセージで使用します(バージョン4.6.1+のユーザ設定脆弱性メッセージ(4-57 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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	ユーザ脆弱性変更データ ブロック タイプ (80)																																							
	ユーザ脆弱性変更ブロック長																																							
	ソース																																							
	ソースタイプ																																							
Vuln Ack ブロック	汎用リストブロック タイプ (31)																																							
	汎用リストブロック長																																							
	ユーザ脆弱性データ ブロック...*																																							

次の表では、汎用リスト データ ブロックのフィールドについて説明します。

表 4-62 ユーザ脆弱性変更データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ脆弱性変更データ ブロックタイプ	uint32	ユーザ脆弱性変更データ ブロックを開始します。この値は常に 80 です。
ユーザ脆弱性変更ブロック長	uint32	ホスト脆弱性ブロックタイプフィールドと長さフィールドの 8 バイトに、後続のホスト脆弱性データのバイト数を加えたユーザ脆弱性変更データ ブロックの合計バイト数。
ソース	uint32	ホスト脆弱性変更値を更新または追加した送信元にマッピングされるID 番号。送信元タイプによって、これは無応答 (RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。

表 4-62 ユーザ脆弱性変更データブロックのフィールド(続き)

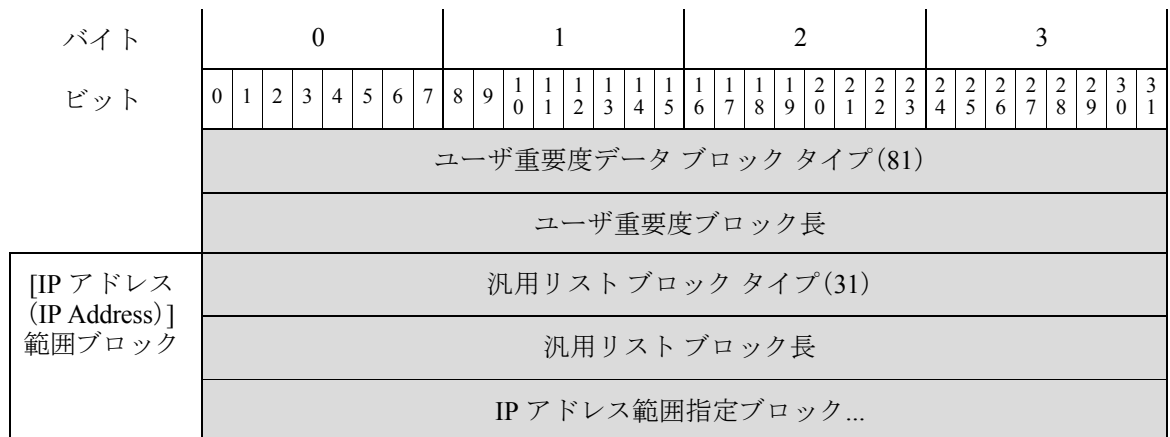
フィールド	バイト数	説明
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> 無応答(RNA) がホスト脆弱性データを検出した場合、0 ユーザがホスト脆弱性データを提供した場合、1 サードパーティ スキャナがホスト脆弱性データを検出した場合、2 nmimport.pl やホスト入力 API クライアントなどのコマンドラインツールでホスト脆弱性データを提供した場合、3
タイプ (Type)	uint32	脆弱性のタイプ。
汎用リストブロック タイプ	uint32	汎用リストデータブロックを開始します。この値は常に 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脆弱性データブロック。詳細については、 ユーザ脆弱性データブロック 5.0+(4-166 ページ) を参照してください。

ユーザ重要度変更データ ブロック 4.7+

ユーザ重要度データ ブロックには、ホスト重要度を変更したホストの IP アドレス範囲指定リスト、重要度値を更新したユーザの ID 番号、重要度値を提供する送信元に関する情報、重要度値を格納します。ユーザ重要度データブロックのブロックタイプは、シリーズ 1 ブロックグループのブロックタイプ 81 です。前のユーザ重要度データブロックからの変更では、新規ソースタイプフィールドが加えられ、リストデータブロックの代わりに、汎用リストデータブロックで IP アドレスを保存するようになりました。

[ユーザ設定ホスト重要度メッセージ\(4-59 ページ\)](#)にあるように、ユーザ設定ホスト重要度メッセージでは、ユーザ重要度データブロックを使用します。

次の図は、ユーザ重要度データブロックの基本構造です。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ソース																															
	ソース タイプ																															
	重要度値...																															

次の表では、ユーザ重要度データブロックのフィールドについて説明します。

表 4-63 ユーザ重要度データブロックのフィールド

フィールド	バイト数	説明
ユーザ重要度データブロックタイプ	uint32	ユーザ重要度データブロックを開始します。この値は常に 81 です。
ユーザ重要度ブロック長	uint32	ユーザ重要度ブロックタイプフィールドと長さフィールドの 8 バイトに、後続のユーザ重要度データのバイト数を加えたユーザ重要度データブロックの合計バイト数。
汎用リストブロックタイプ	uint32	汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストブロックとカプセル化されたデータブロックのバイト数。この値は、汎用リストブロックヘッダーフィールドの 8 バイトに、カプセル化されたすべてのデータブロックのバイト数を加えた値です。
IP アドレス範囲指定データブロック	変数 (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	ユーザ重要度値を更新または追加した送信元にマッピングされる ID 番号。送信元タイプによって、これは無応答 (RNA)、ユーザ、スキャナ、またはサードパーティアプリケーションにマッピングされます。
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: <ul style="list-style-type: none"> 無応答 (RNA) がユーザ重要度値を提供した場合、0 ユーザがユーザ重要度値を提供した場合、1 サードパーティ スキャナがユーザ重要度値を提供した場合、2 nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでユーザ重要度値を提供した場合、3
重要度値	uint32	ユーザの重要度値。

ユーザ属性値データ ブロック 4.7+

ユーザ属性値データ ブロックには、属性値が変更されたホストを示す IP アドレス範囲のリストが、ユーザの ID 番号、属性値、その属性値を提供した送信元に関する情報、その属性値を格納した BLOB データブロックとともに格納されます。ユーザ属性値データ ブロックのブロックタイプは、シリーズ 1 ブロック グループのブロックタイプ 82 です。前のユーザ属性値データ ブロックからの変更では、新規送信元タイプ フィールドが加えられ、リスト データ ブロックの代わりに、汎用リスト データ ブロックで IP アドレスを保存するようになりました。

次の図は、ユーザ属性値データ ブロックの構造です。

バイト	0								1								2								3											
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	2	2	2	2	2	2	2	2	2	2	2	3	3
	ユーザ属性値データ ブロック タイプ(82)																																			
	ユーザ属性値ブロック長																																			
[IP アドレス (IP Address)] 範囲ブロック	汎用リストブロック タイプ(31)																																			
	汎用リストブロック長																																			
	IP アドレス範囲指定ブロック...																																			
	ソース																																			
	ソース タイプ																																			
	属性 ID																																			
値	BLOB ブロック タイプ(10)																																			
	BLOB ブロック長																																			
	値...																																			

次の表では、ユーザ属性値データ ブロックのフィールドについて説明します。

表 4-64 ユーザ属性値データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ属性値データ ブロック タイプ	uint32	ユーザ属性値データ ブロックを開始します。この値は常に 82 です。
ユーザ属性値ブロック長	uint32	ユーザ属性値ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザ属性ブロック データのバイト数を加えた属性値データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。

表 4-64 ユーザ属性値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。
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、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: <ul style="list-style-type: none"> • 無応答(RNA)がユーザ属性を提供した場合、0 • ユーザが属性値を提供した場合、1 • サードパーティスキャナがユーザ属性値を提供した場合、2 • nmimport.pl やホスト入力APIクライアントなどのコマンドラインツールでユーザ属性値を提供した場合、3
属性ID	uint32	更新した属性のID番号(該当する場合)。
BLOB ブロックタイプ	uint32	BLOB データブロックを開始します。この値は常に10です。
BLOB ブロック長	uint32	BLOB データブロックのバイト数です。BLOB ブロックタイプとブロック長フィールドの8バイトと後続のバイナリデータの長さが含まれます。
値	変数 (variable)	バイナリ形式でユーザ属性値を格納します。

ユーザプロトコルリストデータブロック 4.7+

ユーザプロトコルリストデータブロックには、プロトコルデータの送信元に関する情報、データを追加したユーザのID番号、プロトコルデータブロックのリストを格納します。ユーザプロトコルリストデータブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ83です。ユーザプロトコルデータブロックの詳細については、[ユーザプロトコルデータブロック\(4-97ページ\)](#)を参照してください。

[ユーザプロトコルメッセージ\(4-61ページ\)](#)にあるように、ユーザプロトコルメッセージでは、ユーザプロトコルリストデータブロックを使用します。

次の図は、ユーザプロトコルリストデータブロックの基本構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザプロトコルリストブロックタイプ(83)																															
	ユーザプロトコルリストブロック長																															
	ソースタイプ																															
	ソース																															
ユーザプロトコルブロック	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	ユーザプロトコルデータブロック...																															

次の表では、汎用リストデータブロックのフィールドについて説明します。

表 4-65 ユーザプロトコルリストデータブロックのフィールド

フィールド	バイト数	説明
ユーザプロトコルリストブロックタイプ	uint32	ユーザプロトコルリストデータブロックを開始します。この値は常に 83 です。
ユーザプロトコルリストブロック長	uint32	ユーザプロトコルリストブロックタイプフィールドと長さフィールドの8バイトに、後続のユーザプロトコルリストデータのバイト数を加えたユーザプロトコルリストデータブロックの合計バイト数。
ソースタイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> • 無応答(RNA) がプロトコルデータを提供した場合、0 • ユーザがプロトコルデータを提供した場合、1 • サードパーティ スキャナがプロトコルデータを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンドラインツールでプロトコルデータを提供した場合、3
ソース	uint32	影響を受けるプロトコルの送信元にマッピングするID番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
汎用リストブロックタイプ	uint32	汎用リストデータブロックを開始します。この値は常に 31 です。

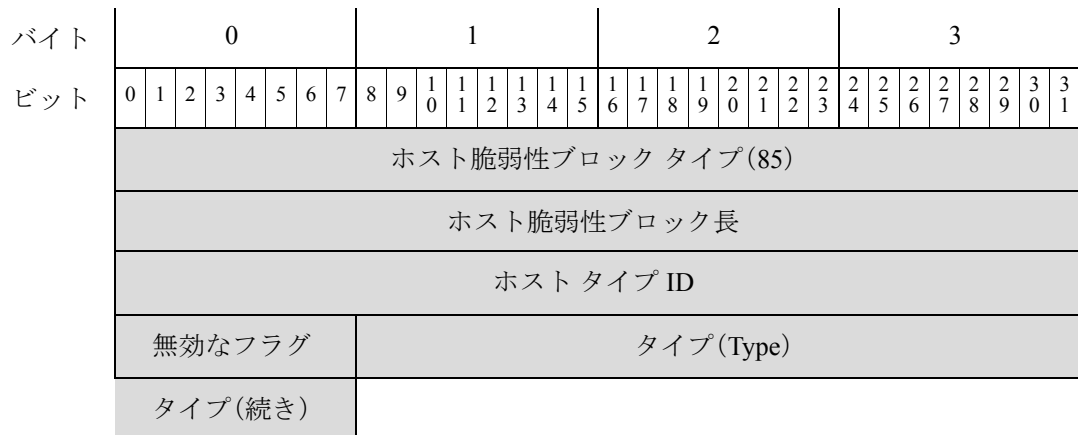
表 4-65 ユーザプロトコル リスト データ ブロックのフィールド(続き)

フィールド	バイト数	説明
汎用リスト ブロック長	uint32	汎用リストブロックとカプセル化されたデータブロックのバイト数。この値は、汎用リストブロックヘッダーフィールドの8バイトに、カプセル化されたすべてのデータブロックのバイト数を加えた値です。
ユーザプロトコルデータブロック	変数 (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プロトコルデータブロック。

ホスト脆弱性データブロック 4.9.0+

ホスト脆弱性データブロックは、ホストに適用する脆弱性を伝えます。ホスト脆弱性データブロックごとに、1回のイベントにおける1つのホストに関する1つの脆弱性について記述します。ホスト脆弱性データブロックは、フルホストプロファイル、フルホストサーバ、フルサブサーバデータブロックで表示されます。ホスト脆弱性データブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ85です。

次の図は、ホスト脆弱性データブロックの形式です。



次の表では、ホスト脆弱性データブロックのコンポーネントについて説明します。

表 4-66 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	脆弱性と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 システムやサーバフィンガープリント送信元のアイデンティティがいつ競合するか、あるいはいつタイムアウトになるかを示すアイデンティティの競合メッセージとアイデンティティ タイムアウトメッセージで使用します。このデータ ブロックは、アクティブ送信元アイデンティティ(ユーザ、スキャナ、またはアプリケーション)と競合中であると報告されたアイデンティティを記述します。詳細については、[アイデンティティ競合とアイデンティティ タイムアウト システム メッセージ\(4-63 ページ\)](#)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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	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)																															
	ポート																プロトコル															
	サーバマップ ID																															

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。

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
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: <ul style="list-style-type: none"> 無応答 (RNA) がフィンガープリント データを提供した場合、0 ユーザがフィンガープリント データを提供した場合、1 サードパーティ スキャナがフィンガープリント データを提供した場合、2 nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでフィンガープリント データを提供した場合、3
アイデンティティ データ送信元 ID	uint32	フィンガープリント データの送信元にマッピングする ID 番号。送信元タイプによって、これは無応答 (RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
UUID	uint8[16]	アイデンティティがオペレーティング システム アイデンティティの場合、フィンガープリントの固有識別子として機能するオクテット形式の ID 番号。
[ポート (Port)]	uint16	アイデンティティがサーバ アイデンティティの場合、サーバ データを含むパケットで使用するポートを示します。
プロトコル	uint16	アイデンティティがサーバ アイデンティティの場合、ネットワーク プロトコルの IANA 番号またはサーバ データを含むパケットが使用する Ethertype を示します。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 2048:IP
サーバマップ ID	uint32	アイデンティティがサーバ アイデンティティの場合、サーバの ID、ベンダー、バージョンの組み合わせを表すサーバ マッピング ID を示します。

ホスト MAC アドレス 4.9+

ホスト MAC アドレス データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 95 です。このブロックには、ホスト データの packets 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ホスト MAC アドレス ブロック タイプ (95)																																
ホスト MAC アドレス ブロック 長																																
TTL								MAC アドレス																								
MAC アドレス (続き)																								プライマリ (Primary)								
最後の確認日時																																

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。

■ 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

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
	セカンダリ ホスト更新ブロック タイプ (96)																																
	セカンダリ ホスト更新ブロック長																																
	[IP アドレス (IP Address)]																																
	リストブロック タイプ (11)																																ホスト MAC アドレス リ スト
	リストブロック長																																
ホスト MAC アドレス一覧	ホスト MAC アドレス ブロック タイプ (95)																																
	ホスト MAC アドレス ブロック長																																
	ホスト MAC アドレス データ ブロック ...																																

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。

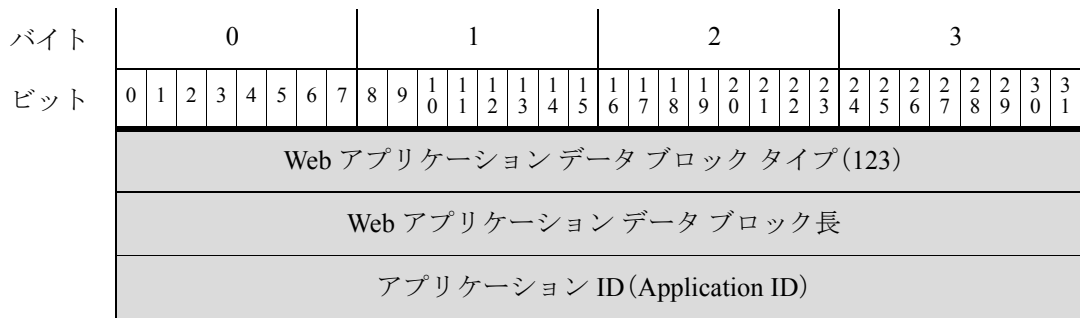
表 4-69 セカンダリ ホスト更新データ ブロックのフィールド(続き)

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 6.2+

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。3 番目の [セキュリティ インテリジェンス (Security Intelligence)] フィールドが 6.2+ 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+ 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 \(B-222 ページ\)](#) に置き換わります。

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 \(2-13 ページ\)](#) 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+ の接続統計データ ブロックの形式です。

7

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続統計データ ブロック タイプ (168)																																
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)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出力インターフェイス(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нда IP アドレス																																
レスポнда IP アドレス(続き)																																
レスポнда IP アドレス(続き)																																
レスポнда 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нда ポート																TCP フラグ																
プロトコル								NetFlow ソース																								
NetFlow ソース(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
	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нда送信パケット数																															
	レスポнда送信パケット数(続き)																															
レスポнда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нда送信パケット数																															
	レスポнда送信バイト数(続き)																															
レスポнда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нда パケット ドロップ																															
	レスポнда パケット ドロップ(続き)																															
レスポнда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																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	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нда バイト ドロップ																															
	レスポнда バイト ドロップ (続き)																															
レスポндаバイトドロップ (続き)	QOS 適用インターフェイス																															
	QOS 適用インターフェイス (続き)																															
	QOS 適用インターフェイス (続き)																															
	QOS 適用インターフェイス (続き)																															
QOS インターフェイス (続き)	QOS ルール ID																															
QOS ルール ID (続き)	ユーザ ID (User ID)																															
ユーザ ID (続き)	アプリケーションプロトコル ID																															
アプリケーションプロトコル ID (続き)	URL カテゴリ																															
URL カテゴリ (続き)	URL レピュテーション																															
URL レピュテーション (続き)	クライアントアプリケーション ID																															
クライアントアプリケーション ID (続き)	Web アプリケーション ID																															
クライアント URL	Web アプリケーション ID (続き)	文字列ブロック タイプ (0)																														
	文字列ブロック タイプ (続き)	文字列ブロック長																														
	文字列ブロック長 (続き)	クライアントアプリケーション URL...																														

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NetBIOS [名前(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 アプリケーションバージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	クライアントアプリケーションバージョン...																															
	モニタ ルール 1																															
	モニタ ルール 2																															
	モニタ ルール 3																															
	モニタ ルール 4																															
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/ 宛先								秒イニシエー タ層								ファイル イベント カウント															
	侵入イベント カウント																イニシエータの国															
	レスポнда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															

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

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	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 サーバ名	SSL フロー フラグ(続き)								文字列ブロック タイプ(0)																							
	文字列ブロック タイプ(0)(続き)																文字列ブロック長															
	文字列ブロック長(続き)																SSL サーバ名...															
	SSL URL カテゴリ																															
	SSL セッション ID																															
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	SSL 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															
DNS クエリ (DNS Query)	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...															

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

次の表では、6.2+ 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 6.2+ 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	6.2+ 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нда IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに回答したホストの IP アドレス。

表 4-71 接続統計データブロック 6.2+ 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]	トリガーされた関連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 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нда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нда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нда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нда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нда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 6.2+ のフィールド(続き)

フィールド	データタイプ	説明
レスポнда バイトドロップ	uint64	レート制限により、セッション レスポндаからドロップしたバイト数。
QOS 適用インターフェイス	uint8[16]	レート制限された接続で、レート制限が適用されるインターフェイスの名前。
QOS ルール ID	uint32	接続に適用される QoS ルールの内部 ID 番号(該当する場合)。
ユーザ ID (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 6.2+ のフィールド(続き)

フィールド	データタイプ	説明
モニタ ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタ ルールの ID。
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス 送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス 層	uint8	IP ブラックリストに一致した IP 層。
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нда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 6.2+ 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	ユーザエージェントを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザエージェント文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびユーザエージェントフィールドのバイト数を含む)。
ユーザエージェント	string	セッションのユーザエージェントヘッダーフィールドからの情報。
文字列ブロックタイプ	uint32	HTTP リファラを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	HTTP リファラ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および HTTP リファラフィールドのバイト数を含む)。
HTTP リファラ	string	ページの発生元のサイト。これは HTTP トラフィック内の参照ヘッダー情報にあります。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
SSL ポリシー ID	uint8[16]	接続を処理した SSL ポリシーの ID 番号。
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルトアクションの ID 番号。
SSL 暗号スイート	uint16	SSL 接続で使用される暗号スイート。値は 10 進形式で保存されます。値により指定されている暗号スイートの詳細については、 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
SSL バージョン	uint8	接続の暗号化に使用された SSL または TLS プロトコルバージョン。

表 4-71 接続統計データブロック 6.2+ のフィールド(続き)

フィールド	データタイプ	説明
SSL サーバ証明書ステータス	uint32	<p>SSL 証明書のステータス。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 1(不明):サーバ証明書のステータスは判別できませんでした。 2(有効):サーバ証明書は有効です。 4(自己署名済み):サーバ証明書は自己署名です。 16(無効な発行者):サーバ証明書に無効な発行者があります。 32(無効な署名):サーバ証明書に無効な署名があります。 64(期限切れ):サーバ証明書は期限切れです。 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 256(取り消し):サーバ証明書は取り消されました。
実際の SSL アクション	uint16	<p>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。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> 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 6.2+ 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	<p>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。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL フロー エラー	uint32	<p>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。</p>

表 4-71 接続統計データブロック 6.2+ 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	<p>SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> 0x00000001 (NSE_FLOW__VALID):他のフィールドを有効にするために設定する必要があります 0x00000002 (NSE_FLOW__INITIALIZED):内部構造が処理可能です 0x00000004 (NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました
文字列ブロックタイプ	uint32	SSL サーバ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	SSL サーバ名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および SSL サーバ名フィールドのバイト数を含む)。

表 4-71 接続統計データブロック 6.2+ のフィールド(続き)

フィールド	データタイプ	説明
SSL サーバ名	string	SSL Client Hello でサーバ名に指定された名前。
SSL URL カテゴリ	uint32	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできます。
SSL チケット ID	uint8[20]	クライアントとサーバがセッション チケットの使用に同意する場合に使用されるセッション チケットのハッシュ。
SSL チケット ID の長さ	uint8	SSL チケット ID の長さ。チケット ID は 20 バイトより長くすることはできませんが、20 バイト未満であってもかまいません。
ネットワーク分析ポリシー リビジョン	uint8[16]	接続イベントに関連付けられているネットワーク分析ポリシーのリビジョン。
エンドポイントプロファイル ID	uint32	ISE により識別される、接続エンドポイントで使用されるデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
セキュリティグループ ID	uint32	ポリシーに基づいて ISE によりユーザに割り当てられた ID 番号。
ロケーション IPv6	uint8[16]	ISE と通信するインターフェイスの IP アドレス。IPv4 または IPv6 のアドレスを使用できます。
HTTP レスポンス	uint32	HTTP 要求の応答コード。
文字列ブロックタイプ	uint32	DNS クエリを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数(文字列ブロックタイプと長さのフィールド用の 8 バイト、および DNS クエリ文字列のバイト数を含む)。
DNS クエリ (DNS Query)	string	DNS サーバに送信されたクエリの内容。
DNS レコードタイプ (DNS Record Type)	uint16	DNS レコードタイプの数値。
DNS レスポンスタイプ	uint16	DNS 応答タイプの数値。
DNS TTL	uint32	DNS レスポンスの存続期間(秒単位)。
シンクホール UUID	uint8[16]	このシンクホール オブジェクトに関連付けられているリビジョン UUID。

表 4-71 接続統計データブロック 6.2+ 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。

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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
スキャン結果ブロック タイプ (142)																																
スキャン結果ブロック長																																
ユーザ ID (User ID)																																
スキャン タイプ																																
[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)																																
ポート																プロトコル																

■ 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

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
脆弱性 リスト	フラグ(Flag)																リストブロック タイプ(11)																脆弱性スキャン リスト
	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...																
スキャン結果 リスト	リストブロック タイプ(11)																																汎用スキャン 結果リスト
	リストブロック長																																
	汎用スキャン結果ブロック タイプ(108)																																
ユーザ(User) 製品リスト	汎用スキャン結果ブロック長																																
	汎用スキャン結果...																																
	汎用リストブロック タイプ(31)																																
ユーザ製品リスト	汎用リストブロック長																																
	ユーザ製品データ ブロック*																																

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 ID (User ID)	uint32	スキャン結果をインポートしたユーザ、またはスキャン結果を生成したスキャンを実行したユーザのユーザ ID 番号が含まれます。
スキャンタイプ	uint32	結果がシステムに追加された方法を示します。
[IP アドレス (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)

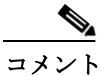
フィールド	データタイプ	説明
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 <ul style="list-style-type: none"> • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 <ul style="list-style-type: none"> • 2048:IP
フラグ(Flag)	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製品データブロックを含む)。
ユーザ製品データブロック*	変数 (variable)	ホスト入力データを含むユーザ製品データブロック。このデータブロックの説明の詳細については、 ユーザ製品データブロック 5.1+(4-180 ページ) を参照してください。

ホストサーバデータブロック 4.10.0+

ホストサーバデータブロックは、ホストで検出したサーバに関する情報を伝えます。ここには、検出したサーバごとにブロックとともに、サーバが実行している Web アプリケーションの Web アプリケーションデータブロックのリストも格納します。ホストサーバデータブロックは、新規と変更された TCP サーバと UDP サーバのメッセージに含まれます。詳細については、[サーバメッセージ\(4-48 ページ\)](#)を参照してください。ホストサーバデータブロックのブロックタイプは、シリーズ 1 ブロックグループのブロックタイプ 103 です。



コメント

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

次の図は、ホストサーバデータブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	サーバブロックタイプ(103)																															
	サーバブロック長																															
	[ポート (Port)]																ヒット															
	ヒット(続き)																前回の使用 (Last Used)															
サブサーバ情報	前回の使用(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)																サーバ情報ブロックタイプ(117)*															
	信頼度																															
	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																															
Web Application	Web アプリケーションブロック タイプ(123)*																															
	Web アプリケーションブロック長																															
	Web アプリケーション データ...																															

次の表では、ホスト サーバデータ ブロックのフィールドについて説明します。

表 4-73 ホストサーバデータブロックのフィールド

フィールド	データタイプ	説明
ホストサーバブロックタイプ	uint32	ホストサーバデータブロックを開始します。この値は常に 103 です。
ホストサーバブロック長	uint32	ホストサーバブロックタイプフィールドと長さフィールドの 8 バイトに、後続のデータバイト数を加えたホストサーバデータブロックの合計バイト数。
[ポート (Port)]	uint16	サーバが実行しているポート番号。
ヒット	uint32	サーバが受信したヒット数。
前回の使用 (Last Used)	uint32	システムが使用中のサーバを検出した前回時刻を表す UNIX タイムスタンプ。
汎用リストブロックタイプ	uint32	汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストブロックとカプセル化されたサブサーバ情報データブロックのバイト数。この値は、汎用リストブロックヘッダーフィールドの 8 バイトに、カプセル化されたすべてのデータブロックのバイト数を加えた値です。
サーバ情報データブロック*	変数 (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情報データブロック。詳細は、 4.10.x、5.0 ~ 5.0.2 のサーバ情報データブロック (4-152 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 (4-125 ページ) を参照してください。

フルホストサーバデータブロック 4.10.0+

フルホストサーバデータブロックは、サーバポート、使用頻度と最新の更新、データ正確性の信頼度、シスコそのホストのサーバに関するサードパーティ脆弱性などサーバに関する情報を伝えます。フルホストサーバデータブロックには、そのサーバの各サブサーバのフルサブサーバ情報データブロックを格納します。各フルホストプロファイルデータブロックには、ホスト上の各TCPサーバとUDPサーバのフルホストサーバデータブロックを格納します。フルホストサーバデータブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ104です。



コメント

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

次の図は、フルサーバデータブロックの形式です。

バイト	0								1							2							3									
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	フルサーバブロックタイプ(104)																															
	フルサーバブロック長																															
	[ポート (Port)]																ヒット															
サブサーバ-シスコ	ヒット(続き)																汎用リストブロックタイプ(31)															
	汎用リストブロックタイプ(続き)																汎用リストブロック長															
	汎用リストブロック長(続き)																フルサーバ情報データブロック(106)*															
サブサーバ-ユーザ (User)	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	フルサーバ情報データブロックタイプ(106)*																															
サブサーバ-スキャナ	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	フルサーバ情報データブロック(106)*																															
サブサーバ-Application	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	フルサーバ情報データブロック(106)*																															
	信頼度																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
サーババナー	BLOB ブロック タイプ (10)																															
	BLOB ブロック長																															
	サーババナー 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 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 フルホストサーバデータブロック 4.10.0+ のフィールド

フィールド	データタイプ	説明
フルサーバブロックタイプ	uint32	フルサーバデータブロックを開始します。この値は常に104です。
フルサーバブロック長	uint32	フルサーバブロックタイプフィールドと長さフィールドの8バイトに、後続のフルサーバデータのバイト数を加えたフルサーバデータブロックの合計バイト数。
[ポート (Port)]	uint16	サーバポート番号。
ヒット	uint32	サーバが受信したヒット数。
汎用リストブロックタイプ	uint32	検出したサブサーバデータでデータブロックを構成する汎用リストデータブロックを開始します。この値は常に31です。

表 4-74 フルホストサーバデータブロック 4.10.0+ のフィールド(続き)

フィールド	データタイプ	説明
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべてのサブサーバ情報データブロックを含む汎用リストデータブロックのバイト数。
サブサーバ情報 - シスコデータブロック *	変数 (variable)	シスコが検出したホストサーバのサブサーバに関する情報を含むフルサーバ情報データブロック。このデータブロックの説明の詳細については、 フルサーバ情報データブロック (4-154 ページ) を参照してください。
汎用リストブロックタイプ	uint32	ユーザが追加したサブサーバデータを伝えるサブサーバ情報データブロックで構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべてのサーバ情報データブロックを含む汎用リストデータブロックのバイト数。
サブサーバ情報 - ユーザが追加したデータブロック *	変数 (variable)	ユーザが検出したホストサーバのサブサーバに関する情報を含むフルサーバ情報データブロック。このデータブロックの説明の詳細については、 フルサーバ情報データブロック (4-154 ページ) を参照してください。
汎用リストブロックタイプ	uint32	スキャナが追加したサブサーバデータを伝えるサブサーバ情報データブロックで構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべてのサブサーバ情報データブロックを含む汎用リストデータブロックのバイト数。
サブサーバ情報 - スキャナ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のサブサーバに関する情報を含むフルサーバ情報データブロック。このデータブロックの説明の詳細については、 フルサーバ情報データブロック (4-154 ページ) を参照してください。
汎用リストブロックタイプ	uint32	アプリケーションが追加したサブサーバデータを伝えるサブサーバ情報データブロックで構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべてのサブサーバ情報データブロックを含む汎用リストデータブロックのバイト数。
サブサーバ情報 - アプリケーションが追加したデータブロック *	変数 (variable)	アプリケーションが検出したホストサーバのサブサーバに関する情報を含むフルサーバ情報データブロック。このデータブロックの説明の詳細については、 フルサーバ情報データブロック (4-154 ページ) を参照してください。
信頼度	uint32	フルサーバデータの正しい識別におけるシスコの信頼度のパーセンテージ。
BLOB ブロックタイプ	uint32	バナーデータを含む BLOB データブロックを開始します。この値は常に 10 です。
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。

表 4-74 フルホストサーバデータブロック 4.10.0+ のフィールド(続き)

フィールド	データタイプ	説明
サーババナー データ	byte[n]	パケットの最初の n バイトがサーバイベントに関わるバイトであり、 n は 256 以下です。
汎用リストブロックタイプ	uint32	シスコ 脆弱性データを搬送するホスト脆弱性データブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべてのホスト脆弱性データブロックを含む汎用リスト データ ブロックのバイト数。
(VDB)ホスト脆弱性データブロック*	変数 (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+(4-120 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+(4-120 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。
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+(4-120 ページ) を参照してください。
汎用リストブロックタイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。

表 4-74 フルホストサーバデータブロック 4.10.0+ のフィールド(続き)

フィールド	データタイプ	説明
汎用リストブロック長	uint32	汎用リストブロックとカプセル化された Web アプリケーションデータブロックのバイト数。この値は、汎用リストブロックヘッダーフィールドの 8 バイトに、カプセル化されたすべてのデータブロックのバイト数を加えた値です。
Web アプリケーションデータブロック*	変数 (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 のサーバ情報データブロック

サーバ情報データブロックは、サーバ ID、サーバベンダーとバージョン、送信元情報など、サーバに関する情報を伝えます。サーバ情報データブロックのブロックタイプは、4.10.x のシリーズ 1 ブロックグループのブロックタイプ 105 と、5.0 ~ 5.0.2 のシリーズ 1 ブロックグループのブロックタイプ 117 です。サーバ情報データブロックは、ホストサーバブロックとフルホストサーバデータブロックのリストで搬送されます。詳細については、[ホストサーバデータブロック 4.10.0+\(4-146 ページ\)](#)と[フルホストサーバデータブロック 4.10.0+\(4-148 ページ\)](#)を参照してください。

次の図は、サーバ情報データブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	サーバ情報ブロック タイプ (105 117)																															
	サーバ情報ブロック長																															
	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																															
	サーババージョン文字列...																															
	前回の使用 (Last Used)																															
	ソースタイプ																															
	ソース																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	リストブロックタイプ(11)																															
	リストブロック長																															
サブサーバ	サブサーバブロックタイプ(1)*																															
	サブサーバブロック長																															
	サブサーバデータ...																															

次の表では、サーバ情報データブロックのコンポーネントについて説明します。

表 4-75 サーバ情報データブロックのフィールド

フィールド	データタイプ	説明
サーバ情報ブロックタイプ	uint32	サーバ情報データブロックを開始します。ブロックタイプは 4.10.x の場合、105、5.0+ の場合、117 です。
サーバ情報ブロック長	uint32	サーバ情報データブロックの合計バイト数。サーバ情報ブロックタイプフィールドと長さフィールドの 8 バイト、サーバ ID の 4 バイト、ベンダー名ブロックタイプと長さの 8 バイト、ベンダー名にさらに 4 バイト、バージョン文字列ブロックタイプと長さに 8 バイト、バージョン文字列にさらに 4 バイト、最後に使用する送信元タイプと送信元 ID フィールドごとに 4 バイトで構成します。
アプリケーション ID (Application ID)	uint32	検出したサーバで実行しているアプリケーションプロトコルのアプリケーション ID。
文字列ブロックタイプ	uint32	サーバベンダー名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにサーバベンダー名のバイト数を加えたベンダー名文字列データブロックのバイト数。
サーバベンダー名	string	サーバベンダーの名前。
文字列ブロックタイプ	uint32	サーババージョンを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにサーババージョンのバイト数を加えたサーババージョン文字列データブロックのバイト数。
サーババージョン	string	サーババージョン
前回使用時刻	uint32	トラフィックで前回サーバ情報を使用した時刻を示します。

表 4-75 サーバ情報データ ブロックのフィールド(続き)

フィールド	データタイプ	説明
ソースタイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> • 無応答(RNA) がサーバ データを提供した場合、0 • ユーザがサーバ データを提供した場合、1 • サードパーティ スキャナがサーバ データを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでサーバ データを提供した場合、3
ソース	uint32	サーバ データの送信元にマッピングする ID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
リストブロックタイプ	uint32	サブサーバデータ ブロック リストを開始します。この値は常に 11 です。
リストブロック長	uint32	リストブロックタイプ フィールドと長さフィールドの 8 バイトに、後続のカプセル化されたサブサーバデータブロックのバイト数を加えたリストデータブロックの合計バイト数。
サブサーバブロックタイプ	uint32	最初のサブサーバデータ ブロックを開始します。このデータブロックには、他のサブサーバデータブロックを、リストブロック長フィールドで定義した上限まで続けることができます。
サブサーバブロック長	uint32	サブサーバブロックタイプ フィールドと長さフィールドの 8 バイトに、後続のデータバイト数を加えた各サブサーバデータブロックの合計バイト数。
サブサーバデータ	変数 (variable)	サブサーバデータ ブロック (4-78 ページ) に記載のサブサーバデータ。

フルサーバ情報データ ブロック

フルサーバ情報データブロックは、サブサーバのアプリケーションプロトコル、ベンダー、バージョン、関連サブサーバなど、ホストで検出したサーバに関する情報を伝えます。サブサーバごとに、情報は、フルサブサーバデータブロックに格納します([フルサブサーバデータブロック \(4-89 ページ\)](#)を参照)。フルサーバ情報データブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ 106 です。



コメント

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

次の図は、フルサーバ情報データブロックの形式です。

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	フル サーバブロック タイプ(106)																															
	フル サーバブロック長																															
アプリケーションプロトコル ID																																
ベンダー	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ベンダー名文字列...																															
バージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	バージョン文字列...																															
	前回の使用 (Last Used)																															
	ソース タイプ																															
	ソース																															
	リストブロック タイプ(11)																															
	リストブロック長																															
サブサーバ	フル サブサーバブロック タイプ(51)*																															
	フル サブサーバブロック長																															
	フル サブサーバデータ...																															

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

表 4-76 フル サーバ情報データ ブロックのフィールド

フィールド	データタイプ	説明
フル サーバ情報 ブロック タイプ	uint32	フル サーバ情報データ ブロックを開始します。この値は常に106です。
フル サーバ情報 ブロック長	uint32	フル サーバブロック タイプ フィールドと長さフィールドの8バイトに、後続のフル サーバデータのバイト数を加えたフル サーバ情報データ ブロックの合計バイト数。

表 4-76 フルサーバ情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
アプリケーションプロトコル ID	uint32	サーバで実行しているアプリケーションプロトコルのアプリケーション ID。
文字列ブロックタイプ	uint32	アプリケーションプロトコルベンダー名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにベンダー名のバイト数を加えたベンダー名文字列データブロックのバイト数。
ベンダー名 (Vendor Name)	string	サーバベンダーの名前。
文字列ブロックタイプ	uint32	アプリケーションプロトコルバージョンを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにバージョンのバイト数を加えた文字列データブロックのバイト数。
バージョン	string	サーバのバージョン。
前回の使用 (Last Used)	uint32	システムが使用中のサーバを検出した前回時刻を表す UNIX タイムスタンプ。
ソースタイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> • 無応答 (RNA) がサーバデータを提供した場合、0 • ユーザがサーバデータを提供した場合、1 • サードパーティスキャナがクライアントデータを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンドラインツールでサーバデータを提供した場合、3
ソース	uint32	サーバデータの送信元にマッピングする ID 番号。送信元タイプによって、これは無応答 (RNA)、ユーザ、スキャナ、またはサードパーティアプリケーションにマッピングされます。
リストブロックタイプ	uint32	サブサーバデータを伝えるフルサーバ情報データブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのフルサブサーバデータブロックを加えた値です。 このフィールドの後にはゼロか、さらにフルサブサーバデータブロックが続きます。
フルサブサーバブロックタイプ	uint32	最初のフルサブサーバデータブロックを開始します。このデータブロックには、他のフルサブサーバデータブロックを、リストブロック長フィールドで定義した上限まで続けることができます。

表 4-76 フルサーバ情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
フルサブサーバブロック長	uint32	フルサブサーバブロックタイプフィールドと長さフィールドの8バイトに、後続のデータバイト数を加えた各フルサブサーバデータブロックの合計バイト数。
フルサブサーバデータブロック*	uint32	このサーバのサブサーバを含むフルサブサーバデータブロック。このデータブロックの説明の詳細については、 フルサブサーバデータブロック(4-89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+\(4-143ページ\)](#)で使用します。汎用スキャン結果データブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ108です。

次の図は、汎用スキャン結果データブロックの基本構造です。

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
ビット																																
	汎用スキャン結果データブロックタイプ(108)																															
	汎用スキャン結果ブロック長																															
	ポート																プロトコル															
スキャン結果サブサーバ	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	スキャン結果サブサーバ文字列...																															
スキャン結果値	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	スキャン結果値...																															
スキャン結果サブサーバ	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	スキャン結果サブサーバ(不定様式)文字列...																															

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

次の表では、汎用スキャン結果データブロックのフィールドについて説明します。

表 4-77 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)] プロトコル	uint16	結果の脆弱性による影響を受けたサーバが使用するポート。 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 2048:IP
文字列ブロックタイプ	uint32	サブサーバを格納した文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにサブサーバのバイト数を加えたサブサーバ文字列データブロックのバイト数。
スキャン結果サブサーバ	string	サブサーバ。
文字列ブロックタイプ	uint32	値を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに値のバイト数を加えた値文字列データブロックのバイト数。
スキャン結果値	string	スキャン結果値。
文字列ブロックタイプ	uint32	サブサーバを格納した文字列データブロックを開始します。この値は常に 0 です。

表 4-77 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バイトにサブサーバのバイト数を加えたサブサーバ文字列データブロックのバイト数。
スキャン結果サブサーバ	string	サブサーバ(不定様式)。
文字列ブロックタイプ	uint32	値を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトに値のバイト数を加えた値文字列データブロックのバイト数。
スキャン結果値	string	スキャン結果値(不定様式)。

4.10.0+のスキャン脆弱性データブロック

スキャン脆弱性データブロックは、脆弱性を記述し、スキャン結果データブロックで使用します。そのスキャン結果データブロックは、追加スキャン結果イベント(イベントタイプ1002、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+\(4-143 ページ\)](#) および [スキャン結果を追加メッセージ\(4-62 ページ\)](#) 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									
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	説明...																															
名前クリーン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	脆弱性名クリーン...																															
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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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)。
リストブロックタイプ	uint32	Bugtraq ID 番号のリストのリストデータブロックを開始します。

表 4-78 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	フルホストクライアントアプリケーションブロックタイプ (112)																															
	フルホストクライアントアプリケーションブロック長																															
	ヒット																															
	前回の使用 (Last Used)																															
	アプリケーション ID (Application ID)																															
バージョン	文字列ブロックタイプ (0)																															
	文字列ブロック長																															
	バージョン...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
Web 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)。
文字列ブロックタイプ	uint32	クライアントアプリケーションバージョンの文字列データブロックを開始します。この値は常に 0 です。

表 4-79 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)で使われます。4.10.2+ のホストクライアントアプリケーションデータブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ122です。

次の図は、5.0+ のホストクライアントアプリケーションデータブロックの基本構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ホストクライアントアプリケーションブロックタイプ(122)																																
ホストクライアントアプリケーションブロック長																																
ヒット																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	前回の使用 (Last Used)																															
	ID																															
	アプリケーションプロトコル ID																															
バージョン	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	バージョン...																															
	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
Web 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(4-125 ページ) を参照してください。

ユーザ脆弱性データブロック 5.0+

ユーザ脆弱性データブロックは、脆弱性について記述し、ユーザ脆弱性変更ブロック内で使用します。さらに、ユーザ脆弱性変更ブロックはユーザ設定有効脆弱性イベントとユーザ設定無効脆弱性イベントで使用します。5.0+ のユーザ脆弱性データブロックのブロックタイプは、シリーズ 1 ブロックグループのブロックタイプ 124 です。これはブロックタイプ 79 に置き換わります。ユーザ脆弱性変更データブロックの詳細については、[ユーザ脆弱性変更データブロック 4.7+\(4-114 ページ\)](#)を参照してください。

次の図は、ユーザ脆弱性変更データブロックの形式です。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	ユーザ脆弱性ブロックタイプ(124)																																							
	ユーザ脆弱性ブロック長																																							
IP Range 指定ブロック	汎用リストブロックタイプ(31)																																							
	汎用リストブロック長																																							
	IP 範囲仕様データブロック...*																																							
	ポート																プロトコル																							

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	脆弱性 ID																															
サードパーティ脆弱性 UUID	サードパーティ脆弱性 UUID UUID(続き) UUID(続き) UUID(続き)																															
	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	脆弱性文字列...																															
	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																															
	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...																															

次の表では、ユーザ脆弱性データ ブロックのフィールドについて説明します。

表 4-81 ユーザ脆弱性データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザ脆弱性ブロックタイプ	uint32	ユーザ脆弱性データ ブロックを開始します。この値は常に 124 です。
ユーザ脆弱性ブロック長	uint32	ユーザ脆弱性ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザ脆弱性データのバイト数を加えたユーザ脆弱性データ ブロックの合計バイト数。
汎用リストブロックタイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データブロック* で構成された汎用リストデータ ブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リストデータ ブロックのバイト数。
IP 範囲仕様データ ブロック*	変数 (variable)	ユーザ入力からの IP アドレス範囲。このデータ ブロックの説明の詳細については、 5.2+ の IP アドレス範囲データ ブロック (4-101 ページ) を参照してください。

表 4-81 ユーザ脆弱性データブロックのフィールド(続き)

フィールド	データタイプ	説明
[ポート (Port)]	uint16	脆弱性の影響を受けるサーバで使用するポート。クライアントアプリケーション脆弱性の場合、値は 0 です。
プロトコル	uint16	このブロックには、フィンガープリント Universally Unique Identifier (UUID) の他、フィンガープリントタイプ、フィンガープリント送信元タイプ、フィンガープリント送信元 ID を格納します。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	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(ユーザやスキャナ)を示します。
フィンガープリント ソース ID	uint32	ID 番号。オペレーティング システム フィンガープリントを提供したユーザのログイン名にマップします。
最後の確認日時	uint32	トラフィックで前回フィンガープリントを確認した時刻を示します。
TTL 差異	uint8	フィンガープリントの TTL 値とホストにフィンガープリントを実行するとき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 (4-171 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	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。

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(続き)

フィールド	データタイプ	説明
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。



コメント

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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	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)																																							
サーバフィンガープリント	ホップ								プライマリ/セカンダリ								汎用リスト ブロック タイプ (31)																							
	汎用リスト ブロック タイプ (続き)																汎用リスト ブロック 長																							
	汎用リスト ブロック 長 (続き)																サーバフィンガープリント データ ブロック*																							

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
クライアント フィンガー プリント	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	クライアントフィンガープリント データブロック*																															
SMB フィンガー プリント	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	SMB フィンガープリント データブロック*																															
DHCP フィンガー プリント	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	DHCP フィンガープリント データブロック*																															
モバイル 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 フィンガー プリント	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	Ipv6 サーバフィンガープリント データブロック*																															
IPv6 クライ アント フィンガー プリント	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	IPv6 クライアントフィンガープリント データブロック*																															
IPv6 DHCP フィンガー プリント	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	IPv6 DHCP フィンガープリント データブロック*																															
ユーザエー ジェント フィンガー プリント	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	ユーザ エージェント フィンガープリント データ ブロック*																															

■ 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

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
TCP サーバ ブロック*	リストブロック タイプ(11)																																TCP のリス ト サーバ
	リストブロック長																																
	TCP サーバデータ ブロック																																
UDP サーバ ブロック*	リストブロック タイプ(11)																																UDP のリス ト サーバ
	リストブロック長																																
	UDP サーバデータ ブロック																																
ネットワー クプロトコ ルブロック*	リストブロック タイプ(11)																																ネットワー クのリス ト プロトコ ル
	リストブロック長																																
	ネットワーク プロトコルデータ ブロック																																
トランス ポート (Transport) プロトコ ル ブロック*	リストブロック タイプ(11)																																トランスポー トリス ト プロトコ ル
	リストブロック長																																
	トランスポート プロトコルデータ ブロック																																
MAC アドレ ス ブロック*	リストブロック タイプ(11)																																MAC のリス ト アドレス
	リストブロック長																																
	ホスト MAC アドレス データ ブロック																																
最終検出時のホスト																																	
ホストタイプ																																	
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																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NetBIOS [名前(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。 <ul style="list-style-type: none"> 0: ホストはプライマリ ネットワークにあります。 1: ホストはセカンダリ ネットワークにあります。
汎用リスト ブロック タイプ	uint32	サーバフィンガープリントを使用して特定されたフィンガープリントデータを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント (サーバ フィンガープリント) データ ブロック*	変数 (variable)	サーバフィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの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+(4-169 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。

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	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(クライアントフィンガープリント)データブロック*	変数(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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	SMB フィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。
オペレーティングシステムフィンガープリント(SMB フィンガープリント)データブロック*	変数(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+(4-169 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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	モバイルデバイスフィンガープリントで識別するフィンガープリントデータを搬送するオペレーティングシステムフィンガープリントデータブロックで構成される汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。

表 4-84 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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	IPv6 サーバフィンガープリントを使用して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)データブロック*	変数 (variable)	IPv6 サーバフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	IPv6 DHCP フィンガープリントで識別するフィンガープリントデータを搬送するオペレーティングシステムフィンガープリントデータブロックで構成される汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。

表 4-84 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(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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	ユーザエージェントフィンガープリントで識別するフィンガープリントデータを搬送するオペレーティングシステムフィンガープリントデータブロックで構成される汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。
オペレーティングシステムフィンガープリント(ユーザエージェントフィンガープリント)データブロック*	変数(variable)	ユーザエージェントフィンガープリントで識別したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-169 ページ) を参照してください。
リストブロックタイプ	uint32	TCP サーバデータを伝えるサーバデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバデータブロックを加えた値です。 このフィールドには、ゼロ以上のサーバデータブロックが続きます。
TCP サーバデータブロック	変数(variable)	TCP サーバを記述するホストサーバデータブロック。このデータブロックの説明の詳細については、 ホストサーバデータブロック 4.10.0+(4-146 ページ) を参照してください。
リストブロックタイプ	uint32	UDP サーバデータを伝えるサーバデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバデータブロックを加えた値です。 このフィールドには、ゼロ以上のサーバデータブロックが続きます。
UDP サーバデータブロック	uint32	UDP サーバを記述するホストサーバデータブロック。このデータブロックの説明の詳細については、 ホストサーバデータブロック 4.10.0+(4-146 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
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)。
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。 <ul style="list-style-type: none"> • 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。

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
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。 <ul style="list-style-type: none"> 0:はい 1:いいえ
VLAN ID (Admin. VLAN ID)	uint16	ホストがいずれの VLAN メンバーであることを示す 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。
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+(4-162 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。

ユーザ製品データブロック 5.1+

ユーザ製品データブロックは、サードパーティアプリケーション文字列マッピングを含む、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+\(4-143 ページ\)](#)と[ユーザサーバメッセージとオペレーティングシステムメッセージ\(4-60 ページ\)](#)で使用します。ユーザ製品データブロックのブロックタイプのブロックタイプは、4.7 ~ 4.10.1 のシリーズ 1 ブロックグループのブロックタイプ 65 と、4.10.2 ~ 5.0.x のブロックタイプ 118、そして 5.1+ のシリーズ 1 ブロックグループのブロックタイプ 134 です。ブロックタイプ 65 と 118 の構造は同じです。



コメント

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

次の図は、ユーザ製品データブロックの形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ製品データブロックタイプ(134)																															
	ユーザ製品ブロック長																															
	ソース																															
	ソースタイプ																															
[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															
	ドロップユーザ製品																															
カスタム (Custom) ベンダー文 字列	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	カスタムベンダー文字列...																															
カスタム (Custom) 製品文字列	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	カスタム製品文字列...																															
カスタム (Custom) バージョン 文字列	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	カスタムバージョン文字列...																															
	ソフトウェアID																															
	サーバID																															
	ベンダーID																															
	製品ID																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
メジャーバージョン 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	メジャーバージョン文字列...																															
マイナーバージョン 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	マイナー用バージョン文字列...																															
リビジョン 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	リビジョン文字列...																															
メジャー用 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	メジャー用バージョン文字列...																															
マイナー用 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	マイナー用バージョン文字列...																															
リビジョン用 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	リビジョン用文字列...																															
ビルド文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ビルド文字列...																															
パッチ文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	パッチ文字列...																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	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)																															
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 ユーザ製品データブロックのフィールド

フィールド	データタイプ	説明
ユーザ製品データブロックタイプ	uint32	ユーザ製品データブロックを開始します。5.1+ の場合、この値は 134 です。
ユーザ製品ブロック長	uint32	ユーザ製品データブロックのバイトの合計数(ユーザ製品ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ製品データのバイト数を含む)。
ソース	uint32	データをインポートした送信元にマッピングするID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティアプリケーションにマッピングされます。

表 4-85 ユーザ製品データブロックのフィールド(続き)

フィールド	データタイプ	説明
ソースタイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> • 無応答(RNA)がデータを提供した場合、0 • ユーザがデータを提供した場合、1 • サードパーティ スキャナがデータを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンドラインツールでデータを提供した場合、3
汎用リストブロックタイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データブロック*で構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべての IP 範囲仕様データブロック*を含む汎用リストデータブロックのバイト数。
IP 範囲仕様データブロック*	変数(variable)	ユーザ入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データブロック。このデータブロックの説明の詳細については、5.2+ の IP アドレス範囲データブロック (4-101 ページ) を参照してください。
[ポート (Port)]	uint16	ユーザが指定するポート。
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 2048:IP
ドロップ ユーザ製品	uint32	ユーザ OS 定義がホストから削除されたかどうかを示します: <ul style="list-style-type: none"> • 0:いいえ • 1:はい
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタムベンダー名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタムベンダー文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびベンダー名のバイト数を含む)。
カスタムベンダー名	string	ユーザ入力で指定されたカスタムベンダー名。
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタム製品名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタム製品文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および製品名のバイト数を含む)。

表 4-85 ユーザ製品データブロックのフィールド(続き)

フィールド	データタイプ	説明
カスタム製品名	string	ユーザ入力に指定されたカスタム製品名。
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタムバージョンを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタムバージョン文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
カスタムバージョン	string	ユーザ入力に指定されたカスタムバージョン。
ソフトウェア ID	uint32	データベースのサーバまたはオペレーティングシステムの特定のリビジョンの識別子。
サーバ ID	uint32	ユーザ入力に指定したホストサーバのアプリケーションプロトコルの Firepower システムアプリケーション識別子。
ベンダー ID	uint32	サードパーティオペレーティングシステムを Firepower システム OS 定義にマッ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 Firepower 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	ユーザ入力のサードパーティオペレーティングシステム文字列をマップする Firepower システムオペレーティングシステム定義のメジャーバージョン番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	メジャー文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
メジャーバージョン	string	サードパーティ OS 文字列をマップする Firepower システムオペレーティングシステム定義のメジャーバージョン。
文字列ブロックタイプ	uint32	サードパーティ OS 文字列をマップする Firepower システムオペレーティングシステム定義のマイナーバージョン番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	マイナー文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
マイナーバージョン	string	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システムオペレーティングシステム定義のマイナーバージョン番号。
文字列ブロックタイプ	uint32	ユーザ入力のサードパーティオペレーティングシステム文字列をマップする Firepower システムオペレーティングシステム定義の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)。

表 4-85 ユーザ製品データブロックのフィールド(続き)

フィールド	データタイプ	説明
リビジョン	string	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システム定義のリビジョン番号。
文字列ブロックタイプ	uint32	サードパーティ オペレーティング システム文字列をマップする Firepower システム オペレーティング システム定義の最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。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにバージョンのバイト数を加えた移行先メジャー文字列データブロックのバイト数。
移行先メジャー	string	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システム定義のメジャーバージョン番号の範囲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 Firepower 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	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システム定義のマイナーバージョン番号の範囲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 Firepower 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	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システム定義のリビジョン番号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 Firepower システム オペレーティング システムのビルド番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
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	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システムのビルド番号。
文字列ブロックタイプ	uint32	サードパーティ OS 文字列をマップする Firepower システム オペレーティング システムのパッチ番号を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 4-85 ユーザ製品データブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	パッチ文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の8バイト、およびパッチ番号のバイト数を含む)。
パッチ	string	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システムのパッチ番号。
文字列ブロックタイプ	uint32	サードパーティ オペレーティング システム文字列をマップする Firepower システム 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	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システムの拡張番号。
UUID	uint8 [x16]	オペレーティング システム用の固有 ID 番号が含まれます。
文字列ブロックタイプ	uint32	ユーザ入力に指定されたデバイス ハードウェア情報を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ビルド文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の8バイト、およびビルド番号のバイト数を含む)。
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 (4-109 ページ) を参照してください。

ユーザデータブロック

ユーザデータブロックはユーザ イベントメッセージに表示されます。これらはシリーズ1データブロックのサブセットです。シリーズ1データブロックの一般的な形式については、[ディスカバリ\(シリーズ1\)ブロック\(4-65 ページ\)](#)を参照してください。



コメント

ユーザデータブロックヘッダーのデータブロック長フィールドには、2つのデータブロックヘッダーフィールドの8バイトを含む、そのデータブロックのバイト数を格納します。

次の表は、ユーザ イベントメッセージに表示される可能性のあるユーザデータブロックの一覧です。一覧のデータブロックはデータブロックタイプ別に分かれています。現在のデータブロックは最新バージョンです。レガシーブロックはサポート対象ですが、Firepower システムの現行バージョンによる作成対象ではありません。

表 4-86 ユーザ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 ログイン情報	レガシー	システムが検出したユーザのログイン情報の変更を格納します。詳細については、 ユーザ ログイン情報データブロック 5.0 ~ 5.0.2(B-108 ページ) を参照してください。バージョン 5.0 で導入したサクセサブロックタイプは、ブロックタイプ 73 と同じ構造ですが、そのフィールド内のデータは異なります。
74	ユーザ アカウント更新メッセージ	現在 (Current)	ユーザ アカウント情報の変更を格納します。詳細については、 ユーザ アカウント更新メッセージデータブロック(4-189 ページ) を参照してください。
75	4.7 ~ 4.10.x のユーザ情報	レガシー	システムが検出したユーザの情報の変更を格納します。詳細については、 ユーザ情報データブロック 5.x (B-123 ページ) を参照してください。バージョン 6.0 で導入したサクセサブロックのブロックタイプは 158 です。
120	5.x のユーザ情報	現在 (Current)	システムが検出したユーザの情報の変更を格納します。詳細については、 ユーザ情報データブロック 5.x (B-123 ページ) を参照してください。ブロックタイプ 75 に置き換わります。これはブロックタイプ 158 に更新しました。
121	ユーザ ログイン情報	レガシー	システムが検出したユーザのログイン情報の変更を格納します。詳細については、 ユーザ ログイン情報データブロック 5.0 ~ 5.0.2(B-108 ページ) を参照してください。プロトコルフィールドの内容であるブロック 73 とは異なります。ここには、イベントで検出したアプリケーションプロトコル ID のバージョン 5.0+ アプリケーション ID を保存します。バージョン 5.1 で導入したサクセサブロックのブロックタイプは 127 です。

表 4-86 ユーザ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
127	ユーザ ログイン情報	レガシー	システムが検出したユーザのログイン情報の変更を格納します。詳細については、 ユーザ ログイン情報 データブロック 5.1 ~ 5.4.x (B-110 ページ) を参照してください。これはブロック タイプ 121 に置き換わります。6.0 で導入したサクセサ ブロックのブロック タイプは 159 です。
150	IOC 状態	現在 (Current)	侵害に関する情報を格納します。詳細については、 5.3+ の IOC ステート データ ブロック (4-36 ページ) を参照してください。
158	6.0+ のユーザ 情報	現在 (Current)	システムが検出したユーザの情報の変更を格納します。詳細については、 6.0+ の情報データ ユーザ ブロック (4-198 ページ) を参照してください。ブロック タイプ 120 に置き換わります。
159	ユーザ ログイン情報	レガシー	システムが検出したユーザのログイン情報の変更を格納します。詳細については、 ユーザ ログイン情報 データブロック 6.0.x (B-112 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。
165	ユーザ ログイン情報	レガシー	システムが検出したユーザのログイン情報の変更を格納します。詳細については、 ユーザ ログイン情報 データブロック 6.1.x (B-119 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 (4-201 ページ) を参照してください。
167	ユーザ ログイン情報	現在 (Current)	システムが検出したユーザのログイン情報の変更を格納します。詳細については、 ユーザ ログイン情報 データブロック 6.2+ (4-204 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 アカウント更新メッセージデータ ブロック

ユーザ アカウント更新メッセージデータ ブロックは、更新に関する情報をユーザのアカウント情報に伝えます。

ユーザ アカウント 更新データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 74 です。

次の図は、ユーザ アカウント更新メッセージデータ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザアカウント更新メッセージブロック タイプ (74)																															
	ユーザアカウント更新メッセージブロック長																															
ユーザ (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...																															
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...																															
名 [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...																															

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

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

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	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 1	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ 1...																															
ユーザ 2	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ 2...																															
ユーザ 3	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ 3...																															
ユーザ 4	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ 4...																															
電子メール エイリアス 1	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール エイリアス 1...																															
電子メール エイリアス 2	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール エイリアス 2...																															
電子メール エイリアス 3	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール エイリアス 3...																															

次の表では、ユーザアカウント更新メッセージデータブロックのコンポーネントについて説明します。

表 4-87 ユーザアカウント更新メッセージのデータブロックのフィールド

フィールド	データタイプ	説明
ユーザアカウント更新メッセージブロックタイプ	uint32	ユーザアカウント更新メッセージのデータブロックを開始します。この値は常に 74 です。
ユーザアカウント更新メッセージブロック長	uint32	ユーザアカウント更新メッセージブロックタイプフィールドと長さフィールドの 8 バイトに、後続のユーザアカウント更新メッセージデータのバイト数を加えたユーザアカウント更新メッセージデータブロックの合計バイト数。
文字列ブロックタイプ	uint32	ユーザのユーザ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
文字列ブロックタイプ	uint32	ユーザの名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに名のバイト数を加えた名文字列データブロックのバイト数。
名	string	ユーザの名前。
文字列ブロックタイプ	uint32	ユーザのミドルネームイニシャルを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにミドルネームイニシャルのバイト数を加えたミドルネームイニシャル文字列データブロックのバイト数。
ミドルネームイニシャル	string	ユーザのミドルネームイニシャル。
文字列ブロックタイプ	uint32	ユーザの姓を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに姓のバイト数を加えた姓文字列データブロックのバイト数。
姓	string	ユーザの姓。
文字列ブロックタイプ	uint32	ユーザの姓名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに姓名のバイト数を加えた姓名文字列データブロックのバイト数。
正式名称	string	ユーザの姓名。
文字列ブロックタイプ	uint32	ユーザの役職を含む文字列データブロックを開始します。この値は常に 0 です。

表 4-87 ユーザアカウント更新メッセージのデータブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトに役職のバイト数を加えた役職文字列データブロックのバイト数。
役職(Title)	string	ユーザの役職。
文字列ブロックタイプ	uint32	ユーザのスタッフの識別子を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトにスタッフアイデンティティのバイト数を加えたスタッフアイデンティティ文字列データブロックのバイト数。
スタッフアイデンティティ	string	ユーザのスタッフアイデンティティ。
文字列ブロックタイプ	uint32	ユーザのアドレスを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトにアドレスのバイト数を加えたアドレス文字列データブロックのバイト数。
アドレス(Address)	string	ユーザの住所。
文字列ブロックタイプ	uint32	ユーザの住所から得た市町村郡を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトに市町村郡のバイト数を加えた市町村郡文字列データブロックのバイト数。
市区町村郡(City)	string	ユーザの住所から得た市町村郡。
文字列ブロックタイプ	uint32	ユーザの住所から得た県を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトに県のバイト数を加えた県文字列データブロックのバイト数。
県	string	ユーザの県。
文字列ブロックタイプ	uint32	ユーザの住所から得た国または地域を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトに国または地域のバイト数を加えた国または地域文字列データブロックのバイト数。
国/地域	string	ユーザの住所から得た国または地域。
文字列ブロックタイプ	uint32	ユーザの住所から得た郵便番号を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトに郵便番号のバイト数を加えた郵便番号文字列データブロックのバイト数。
郵便番号	string	ユーザの住所から得た郵便番号。

表 4-87 ユーザアカウント更新メッセージのデータブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロックタイプ	uint32	ユーザの住所から得た建物を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに建物名のバイト数を加えた建物文字列データブロックのバイト数。
建物	string	ユーザの住所から得た建物。
文字列ブロックタイプ	uint32	ユーザの住所から得た場所を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに場所名のバイト数を加えた場所文字列データブロックのバイト数。
参照先	string	ユーザの住所から得た場所。
文字列ブロックタイプ	uint32	ユーザの住所から得たルームを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにルームのバイト数を加えたルーム文字列データブロックのバイト数。
会議室(Room)	string	ユーザの住所から得たルーム。
文字列ブロックタイプ	uint32	ユーザの住所から得た会社を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに会社名のバイト数を加えた会社文字列データブロックのバイト数。
会社	string	ユーザの住所から得た会社。
文字列ブロックタイプ	uint32	ユーザの住所から得た部門を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに部門名のバイト数を加えた部門文字列データブロックのバイト数。
部門(Division)	string	ユーザの住所から得た部門。
文字列ブロックタイプ	uint32	ユーザの住所から得た部署を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	部署文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および部署のバイト数を含む)。
部署名 (Department)	string	ユーザの住所から得た部署。
文字列ブロックタイプ	uint32	ユーザの住所から得たオフィスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにオフィスのバイト数を加えたオフィス文字列データブロックのバイト数。
オフィス (Office)	string	ユーザの住所から得たオフィス。
文字列ブロックタイプ	uint32	ユーザの住所から得た郵便配達先を含む文字列データブロックを開始します。この値は常に 0 です。

表 4-87 ユーザアカウント更新メッセージのデータブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトに郵便配達先のバイト数を加えた郵便配達先文字列データブロックのバイト数。
郵便配達先	string	ユーザの住所から得た郵便配達先。
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
Eメール	string	ユーザの電子メールアドレス。
文字列ブロックタイプ	uint32	ユーザの電話番号を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトに電話番号のバイト数を加えた電話番号文字列データブロックのバイト数。
電話	string	ユーザの電話番号。
文字列ブロックタイプ	uint32	ユーザのインターネット電話番号を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトにインターネット電話番号のバイト数を加えたインターネット電話番号文字列データブロックのバイト数。
インターネット電話	string	ユーザのインターネット電話番号。
文字列ブロックタイプ	uint32	ユーザの代替ユーザ名を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトにユーザ名のバイト数を加えたユーザ文字列データブロックのバイト数。
ユーザ1	string	ユーザの代替ユーザ名。
文字列ブロックタイプ	uint32	ユーザの代替ユーザ名を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトにユーザ名のバイト数を加えたユーザ文字列データブロックのバイト数。
ユーザ2	string	ユーザの代替ユーザ名。
文字列ブロックタイプ	uint32	ユーザの代替ユーザ名を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトにユーザ名のバイト数を加えたユーザ文字列データブロックのバイト数。
ユーザ3	string	ユーザの代替ユーザ名。

表 4-87 ユーザアカウント更新メッセージのデータブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロックタイプ	uint32	ユーザの代替ユーザ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにユーザ名のバイト数を加えたユーザ文字列データブロックのバイト数。
ユーザ 4	string	ユーザの代替ユーザ名。
文字列ブロックタイプ	uint32	ユーザの電子メールエイリアスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールエイリアスのバイト数を加えた電子メールエイリアス文字列データブロックのバイト数。
電子メールエイリアス 1	string	ユーザの電子メールアドレス。
文字列ブロックタイプ	uint32	ユーザの電子メールエイリアスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールエイリアスのバイト数を加えた電子メールエイリアス文字列データブロックのバイト数。
電子メールエイリアス 2	string	ユーザの電子メールアドレス。
文字列ブロックタイプ	uint32	ユーザの電子メールエイリアスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールエイリアスのバイト数を加えた電子メールエイリアス文字列データブロックのバイト数。
電子メールエイリアス 3	string	ユーザの電子メールアドレス。

6.0+ の情報データ ユーザブロック

ユーザ情報データブロックはユーザ変更メッセージで使用され、検出、削除、またはドロップされたユーザの情報を伝えます。詳細については、[ユーザ変更メッセージ\(4-64 ページ\)](#)を参照してください。

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

ユーザ情報データブロックのブロックタイプは、4.7 ~ 4.10.x のシリーズ 1 ブロックグループのブロックタイプ 75 と、5.x のシリーズ 1 ブロックグループのブロックタイプ 120 です。詳細については、[ユーザ情報データブロック 5.x\(B-123 ページ\)](#)を参照してください。

次の図は、ユーザ情報データブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ情報ブロック タイプ(158)																															
	ユーザ情報ブロック長																															
	ユーザ ID (User ID)																															
ユーザ (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																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
セキュリティグループ ID																																
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)																																

次の表は、ユーザ情報データブロックのコンポーネントについての説明です。

表 4-88 ユーザ情報データブロックのフィールド

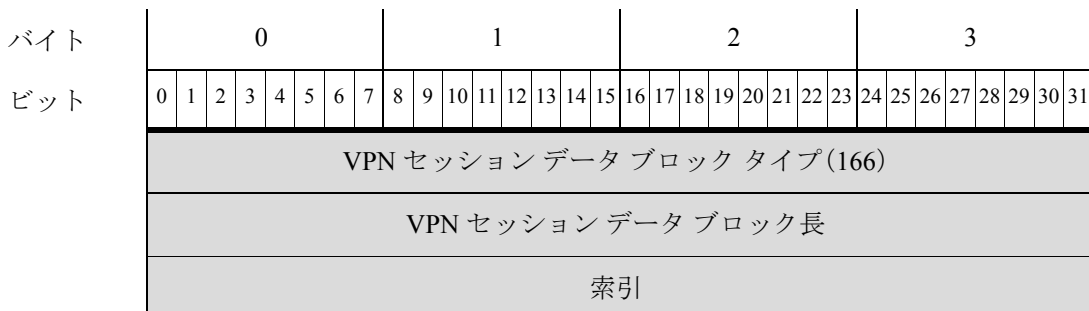
フィールド	データタイプ	説明
ユーザ情報ブロックタイプ	uint32	ユーザ情報データブロックを開始します。この値は 158 です。
ユーザ情報ブロック長	uint32	ユーザ情報データブロックのバイトの合計数(ユーザログイン情報ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ情報データのバイト数を含む)。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。
文字列ブロックタイプ	uint32	ユーザのユーザ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
レルム ID	uint32	アイデンティティレルムに対応する整数 ID。
プロトコル	uint32	ユーザ情報を含むパケットのプロトコル。
文字列ブロックタイプ	uint32	ユーザの名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および名のバイト数を含む)。
名	string	ユーザの名前。
文字列ブロックタイプ	uint32	ユーザの姓を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	姓文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および姓のバイト数を含む)。
姓	string	ユーザの姓。

表 4-88 ユーザ情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。
文字列ブロックタイプ	uint32	ユーザの部署を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	部署文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および部署のバイト数を含む)。
部署名 (Department)	string	ユーザの部署名。
文字列ブロックタイプ	uint32	ユーザの電話番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電話番号のバイト数を加えた電話番号文字列データブロックのバイト数。
電話	string	ユーザの電話番号。
エンドポイントプロファイル ID	uint32	接続エンドポイントが使用するデバイスのタイプの ID 番号。この番号は防御センターごとに固有であり、メタデータで解決します。
セキュリティグループ ID	uint32	ネットワークトラフィックグループの ID 番号。
ロケーション IPv6 アドレス	uint16[8]	ISE と通信するインターフェイスの IP アドレス。IPv4 または IPv6 のアドレスを使用できます。

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							
	0	1	2	3	4	5	6	7	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...																															
クライアントオペレーティングシステム	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。 <ul style="list-style-type: none"> 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。

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。
文字列ブロック長	uint32	ユーザ名文字列のデータ 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 ログイン情報データ ブロック 6.2+

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

バージョン 6.2+ では、ユーザ 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 ログイン情報データ ブロック 6.1.x \(B-116 ページ\)](#)を参照してください。

次の図は、ユーザ ログイン情報データ ブロックの形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ ログイン情報ブロック タイプ (167)																															
	ユーザ ログイン情報ブロック長																															
	Timestamp																															
	IPv4 アドレス (IPv4 Address)																															
ユーザ (User) [名前 (Name)]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザ名...																															
ドメイン	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ドメイン...																															
	ユーザ ID (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)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ロケーション IPv6 アドレス																															
	ロケーション IPv6 アドレス(続き)																															
	ロケーション IPv6 アドレス(続き)																															
	ロケーション IPv6 アドレス(続き)																															
レポート基準	ログインタイプ								承認タイプタイプ(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 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 ログイン情報データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザ ログイン情報ブロック タイプ	uint32	ユーザ ログイン情報データ ブロックを開始します。バージョン 6.2+ の場合、この値は 167 です。
ユーザ ログイン情報ブロック長	uint32	ユーザ ログイン情報データ ブロックのバイトの合計数 (ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ ログイン情報データのバイト数を含む)。
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(1-5 ページ) を参照してください。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 4-90 ユーザログイン情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	ユーザ名文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の8バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
文字列ブロックタイプ	uint32	ドメインを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトにドメインのバイト数を加えたユーザ名文字列データブロックのバイト数。
ドメイン	string	ユーザがログインしているドメイン。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。
レルム ID	uint32	アイデンティティレルムに対応する整数 ID。
エンドポイントプロファイル ID	uint32	接続エンドポイントが使用するデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
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。 <ul style="list-style-type: none"> • 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	ユーザを検出したポート番号。
範囲の開始	uint16	TS エージェントが使用するポート範囲の開始ポート
開始ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の開始ポート。
終了ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の最終ポート。
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に0です。

表 4-90 ユーザログイン情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
Eメール	string	ユーザの電子メールアドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IPv6 アドレス。
ロケーション IPv6 アドレス	uint8[16]	ユーザがログインした最新の IP アドレス。IPv4 または IPv6 のどちらかのアドレスになります。
ログインタイプ	uint8	検出されたユーザログインのタイプ。
認証タイプ (Authentication Type)	uint8	ユーザが使用する認証のタイプ。値は次のとおりです。 <ul style="list-style-type: none"> 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)のいずれであることを示します。

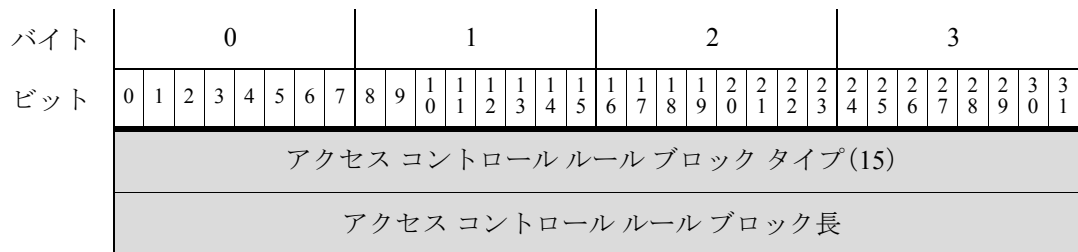
表 4-91 ディスカバリ/接続イベントシリーズ2ブロックタイプ

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 (4-209 ページ) を参照してください。
21	アクセスコントロールルール理由	現在 (Current)	アクセスコントロールルールのメタデータメッセージが、アクセスコントロールルール理由を記述文字列にマップするときに使用します。 アクセスコントロールルール理由データブロック 5.1+(4-211 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+(4-213 ページ) を参照してください。
57	ユーザデータ (User Data)	現在 (Current)	ユーザレコードメタデータメッセージが、ユーザを検出したユーザ ID 番号、プロトコル、そしてユーザ名を提供するために使用します。 ユーザデータブロック (4-214 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。



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

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。
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 5.1+

eStreamer サービスでは、アクセスコントロールルール理由データブロックをアクセスコントロールルール理由メタデータメッセージで使用して、アクセス制御原因を記述文字列にマッピングします。アクセスコントロールルール理由データブロックのブロックタイプは、シリーズ2ブロックグループのブロックタイプ21です。

次の図は、アクセスコントロールルール理由データブロックの構造です。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	アクセスコントロールルール理由ブロックタイプ(21)																																							
	アクセスコントロールルールブロック長																																							
説明	アクセスコントロールルール理由																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 21 です。
アクセスコントロールルール理由ブロック長	uint32	アクセスコントロールルール理由ブロックタイプフィールドと長さフィールドの 8 バイトに、後続のデータバイト数を加えたアクセスコントロールルール理由ブロックの合計バイト数。

表 4-93 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	uint16	<p>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。</p> <p>イベントをトリガーしたルールの理由の番号。</p> <p>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、複数の理由があります。ビット値は次のとおりです。</p> <ul style="list-style-type: none"> • 1: IP ブロック • 2: IP モニタ • 4: ユーザ バイパス • 8: ファイル モニタ • 16: ファイル ブロック • 32: 侵入モニタ • 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 • 8192: URL ブロック • 16384: URL モニタ • 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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	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	接続でトリガーがかかる IP ブラックリストまたはホワイトリストの ID。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。

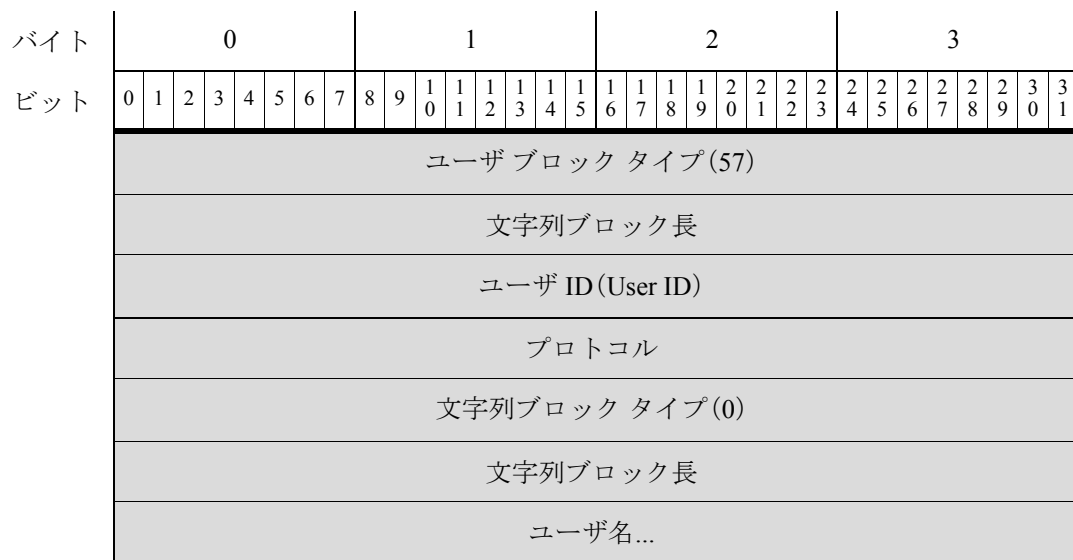
表 4-94 セキュリティ インテリジェンス カテゴリ データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
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	接続でトリガーがかかるセキュリティ インテリジェンス カテゴリ IP カテゴリ ブラックリストまたはホワイトリストの名前。

ユーザ データ ブロック

eStreamer サービスは、ユーザ レコード メタデータ メッセージのユーザデータ ブロックで、ユーザ ID 番号、ユーザを検出したプロトコル、そしてユーザ名を提供します。ユーザ データ ブロックのブロック タイプは、シリーズ 2 ブロック グループのブロック タイプ 57 です。

次の図は、ユーザ データ ブロックの構造です。



次の表では、ユーザ データ ブロックのフィールドについて説明します。

表 4-95 ユーザデータブロックのフィールド

フィールド	データタイプ	説明
ユーザ ブロックタイプ	uint32	ユーザ ブロックを開始します。この値は常に 57 です。
文字列ブロック長	uint32	ユーザ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータのバイト数を加えたユーザ ブロックの合計バイト数。
ユーザ ID (User ID)	uint32	ユーザの固有識別情報。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。 <ul style="list-style-type: none"> • 165:FTP • 426:SIP • 547:AOL Instant Messenger • 683:IMAP • 710:LDAP • 767:NTP • 773:Oracle データベース • 788:POP3 • 1755:MDNS
文字列ブロックタイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトにユーザ名フィールドのバイト数を加えたユーザ名文字列データブロックのバイト数。
[ユーザ名 (Username)]	string	ユーザの名前

アクセス コントロール ポリシー メタデータ ブロック 6.0+

eStreamer サービスはアクセス制御ポリシー メタデータ メッセージのアクセス制御ポリシー メタデータ データ ブロックでアクセス制御情報を提供します。アクセス コントロール ルール ポリシー メタデータ ブロックのブロック タイプは、シリーズ 2 ブロック グループのブロック タイプ 64 です。

次の図は、アクセス コントロール ポリシー メタデータ ブロックの構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	アクセスコントロールポリシーのメタデータブロックタイプ(64)																															
	アクセスコントロールポリシーのメタデータブロック長																															
ACポリシー UUID	アクセスコントロールポリシー UUID アクセスコントロールポリシー UUID(続き) アクセスコントロールポリシー UUID(続き) アクセスコントロールポリシー UUID(続き)																															
	センサー ID (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 4-96 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

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\(2-35 ページ\)](#)を参照してください。

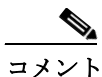
eStreamer では、シリーズ 1 データ ブロック構造を使用して、これらの全ホスト プロファイル ブロックをパッケージ化します。シリーズ 1 ブロックの一般的な構造については、[シリーズ 1 データ ブロック ヘッダー シリーズ\(4-65 ページ\)](#)を参照してください。全ホスト プロファイル データ ブロックには、[検出と接続データ構造の概要\(4-1 ページ\)](#)で定義されているサブセクションにそれぞれ記述されているいくつかのカプセル化されたブロックを含みます。

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\(B-291 ページ\)](#)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。



コメント

次の図において、ブロック名の横にあるアスタリスク(*)は、データ ブロックのインスタンスが複数発生する可能性があることを示しています。

次の図は、全ホスト プロファイル データ ブロック 5.3+ の形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	全ホストプロファイルデータブロック (149)																															
	データブロック長																															
	ホスト ID (Host ID) ホスト ID(続き) ホスト ID(続き) ホスト ID(続き)																															
IP アドレス	リストブロック タイプ (11)																															
	リストブロック長																															
	IP アドレス データ ブロック (143)*																															
	ホップ								汎用リストブロック タイプ (31)																							
	汎用リストブ ロック タイプ (続き)								汎用リストブロック長																							
OS から取得 した フィンガー プリント	汎用リストブ ロック長(続き)								オペレーティング システムフィンガープリントブロック タイプ (130)*																							
	OS フィンガー プリントブ ロック タイプ (130)*(続き)								オペレーティング システム フィンガープリントブロック長																							
	OS フィンガーブ プリントブロッ ク長(続き)								オペレーティング システムから取得したフィンガープリ ントデータ...																							
	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
サーバ フィンガー プリント	オペレーティング システム フィンガープリントブロック タイプ (130)*																															
	オペレーティング システム フィンガープリントブロック長																															
	オペレーティング システム サーバフィンガープリント データ																															
	汎用リストブロック タイプ (31)																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	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(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 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
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 フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム IPv6 サーバフィンガープリント データ...																															
	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Ipv6 クライアントフィンガープリント	オペレーティング システム フィンガープリントブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム Ipv6 クライアント フィンガープリント データ...																															
	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
IPv6 DHCP フィンガープリント	オペレーティング システム フィンガープリントブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム IPv6 DHCP フィンガープリント データ...																															
	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
ユーザエージェントフィンガープリント	オペレーティング システム フィンガープリントブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム ユーザ エージェント フィンガープリント データ...																															
(TCP)全サーバデータ	リストブロック タイプ(11)...																															
	リストブロック長...																															
	(TCP)全サーバデータ ブロック (104)*																															
(UDP)全サーバデータ	リストブロック タイプ(11)																															
	リストブロック長																															
	(UDP)全サーバデータ ブロック (104)*																															
ネットワークプロトコルデータ	リストブロック タイプ(11)																															
	リストブロック長																															
	(ネットワーク)プロトコルデータ ブロック (4)*																															

バイト	0								1							2							3									
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
トランスポート (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							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
サードパーティ スキャン Host Vulns	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	(サードパーティ スキャン)元の Vuln ID によるホスト脆弱性データ ブロック (85) *																															
属性 (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 (4-104 ページ) を参照してください。
ホップ	uint8	ホストからデバイスへのネットワーク ホップ数。
汎用リストブロック タイプ	uint32	ホストの既存のフィンガープリントから取得したフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。

表 5-1 全ホストプロフィールレコード 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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	サーバフィンガープリントを使用して特定されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(サーバフィンガープリント)データブロック*	変数 (variable)	サーバフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	クライアントフィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(クライアントフィンガープリント)データブロック*	変数 (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+(4-169 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	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。

表 5-1 全ホストプロファイルレコード 5.3+ フィールド(続き)

フィールド	データタイプ	説明
オペレーティングシステムフィンガープリント(VDB)ネイティブフィンガープリント1)データブロック*	変数 (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+(4-169 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	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(VDB)ネイティブフィンガープリント2)データブロック*	変数 (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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	ユーザが追加したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(ユーザフィンガープリント)データブロック*	変数 (variable)	ユーザが追加したホストのオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	脆弱性スキャナによって追加されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。

表 5-1 全ホストプロフィールレコード 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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	アプリケーションによって追加されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(アプリケーションフィンガープリント)データブロック*	変数(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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	フィンガープリント競合解決から選択したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(競合フィンガープリント)データブロック*	変数(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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	モバイルデバイスフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。

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+(4-169 ページ) を参照してください。
汎用リストブロック タイプ	uint32	IPv6 サーバ フィンガープリントを使用して特定されたフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティングシステムフィンガープリント(IPv6 サーバフィンガープリント)データブロック*	変数 (variable)	IPv6 サーバ フィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの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+(4-169 ページ) を参照してください。
汎用リストブロック タイプ	uint32	IPv6 クライアント フィンガープリントを使用して特定されたフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティングシステムフィンガープリント(IPv6 クライアントフィンガープリント)データブロック*	変数 (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+(4-169 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	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。

表 5-1 全ホストプロファイルレコード 5.3+ フィールド(続き)

フィールド	データタイプ	説明
オペレーティングシステムフィンガープリント(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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	ユーザエージェントフィンガープリントで識別するフィンガープリントデータを搬送するオペレーティングシステムフィンガープリントデータブロックで構成される汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(ユーザエージェント)データブロック*	変数(variable)	ユーザエージェントフィンガープリントで識別したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-169 ページ) を参照してください。
リストブロックタイプ	uint32	TCP サービスデータを伝送する全サーバデータブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リストブロックタイプフィールド、リストブロック長フィールド、すべてのカプセル化全サーバデータブロック長から成る 8 バイトを含みます。
(TCP)全サーバデータブロック*	変数(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データブロックのリスト。このデータブロックの説明の詳細については、 フルホストサーバデータブロック 4.10.0+(4-148 ページ) を参照してください。
リストブロックタイプ	uint32	UDP サービスデータを伝送する全サーバデータブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リストブロックタイプフィールド、リストブロック長フィールド、すべてのカプセル化全サーバデータブロック長から成る 8 バイトを含みます。
(UDP)全サーバデータブロック*	変数(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データブロックのリスト。このデータブロックの説明の詳細については、 フルホストサーバデータブロック 4.10.0+(4-148 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。 <ul style="list-style-type: none"> • 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	ホストがいずれの VLAN メンバーであるかを示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグ内でカプセル化されるパケットのタイプ。
VLAN プライオリティ	uint8	VLAN タグに含まれるプライオリティ値。
汎用リストブロックタイプ	uint32	クライアントアプリケーションデータを伝送するホスト脆弱性データブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。

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+(4-162 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+(4-120 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+(4-120 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。

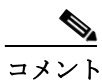
表 5-1 全ホストプロファイルレコード 5.3+ フィールド(続き)

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+(4-120 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 (4-88 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、ユーザはそれを eStreamer サーバに接続し、eStreamer サービスを開始して、データのやりとりを始めることができます。



コメント

eStreamer サーバとは、eStreamer サービスが実行されている Management Center または管理対象デバイス(バージョン 4.9 以降)です。

eStreamer とクライアントのインタラクションを管理するには、次のタスクを実行します。

1. eStreamer サーバで eStreamer を有効にします。
eStreamer サーバへのアクセス許可、クライアントの追加、および認証された接続を確立するための認証クレデンシャルの生成の詳細については、「[eStreamer サーバでの eStreamer の設定 \(6-1 ページ\)](#)」を参照してください。
2. 必要に応じて、手動で eStreamer サービス (eStreamer) を実行します。サービスのステータスを停止、開始、および表示できます。また、コマンドライン オプションを使用して、クライアント/サーバ通信をデバッグできます。
詳細については、[eStreamer サービスの管理 \(6-4 ページ\)](#) を参照してください。
3. オプションとして、eStreamer 参照クライアントを使用して接続またはデータ ストリームをトラブルシューティングするには、クライアントの実行を予定しているコンピュータで参照クライアントを設定します。
[eStreamer 参照クライアントの設定 \(6-6 ページ\)](#) を参照してください。

eStreamer サーバでの eStreamer の設定

ライセンス:任意 (Any)

eStreamer サーバとして使用する Management Center または管理対象デバイスが、クライアントアプリケーションへのイベントのストリームを開始する前に、クライアントにイベントを送信するように eStreamer サーバを設定し、クライアントに関する情報を指定して、通信を確立するときに使用する認証クレデンシャルを生成する必要があります。これらのタスクはすべて、Management Center または管理対象デバイスのユーザ インターフェイスから実行できます。

詳細については、次の各項を参照してください。

- [eStreamer イベント タイプの設定 \(6-2 ページ\)](#)
- [eStreamer クライアントの認証の追加 \(6-3 ページ\)](#)

eStreamer イベント タイプの設定

ライセンス:任意 (Any)

eStreamer サーバはどのタイプのイベントを要求するクライアント アプリケーションに送信できるかを制御できます。

管理対象デバイスまたは Management Center で使用可能なイベント タイプは、以下のとおりです。

- 侵入イベント
- 侵入イベント パケット データ
- 侵入イベント追加データ

次のものを含む Management Center で使用可能なイベントのタイプ:

- 検出イベント(これも、接続イベントを有効にします)
- 相関およびホワイトリスト イベント
- 影響フラグ アラート
- ユーザ アクティビティ イベント
- マルウェア イベント
- ファイル イベント

スタック構成 3D9900 ペアのプライマリとセカンダリは、それらが別の管理対象デバイスであるかのように、Management Center に侵入イベントを報告することに注意してください。3D9900 スタックのプライマリで eStreamer クライアントとの通信を設定する場合は、セカンダリでもクライアントを設定する必要があります。クライアント設定は複製されません。同様に、クライアントを削除する場合は、両方で削除します。スタック構成で 3D9900 を管理する Management Center に eStreamer クライアントを設定する場合は、同じイベントが両方によって報告されても、両方の管理対象デバイスから受信するすべてのイベントは Management Center が報告することに注意してください。

高可用性の構成の Management Center で eStreamer クライアントを設定する場合は、クライアントの設定は、プライマリの Management Center からセカンダリの Management Center に複製されません。

eStreamer によってキャプチャされるイベントのタイプを設定する方法:

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 サーバに接続しているクライアントの発信元 IP アドレスに関連付けられている URL など、侵入イベントに関連付けられた追加データを送信します。

Management Center で、次のいずれかまたはすべてを選択できます。

- [検出イベント (Discovery Events)]: ホスト検出イベントを送信します。
- [相関イベント (Correlation Events)]: 相関イベントおよびホワイトリスト イベントを送信します。
- [影響フラグアラート (Impact Flag Alerts)]: Management Center によって生成される影響アラートを送信します。
- [ユーザ アクティビティ イベント (User Activity Events)]: ユーザ イベントを送信します。
- [侵入イベント追加データ (Intrusion Event Extra Data)]: HTTP プロキシまたはロードバランサ経由で Web サーバに接続しているクライアントの発信元 IP アドレスに関連付けられている URL など、侵入イベントの追加データを送信します。



コメント

これは、eStreamer サーバが送信できるイベントを制御することに注意してください。クライアントアプリケーションは、ユーザが受信する必要が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 \(2-13 ページ\)](#) を参照してください。

ステップ 4 [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 サーバのピア データベースにクライアントを追加しておく必要があります。また、eStreamer サーバによって生成された認証証明書をクライアントにコピーする必要があります。

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。



コメント

ホスト名を使用する場合は、ホスト入力サーバはホストを IP アドレスに解決できる必要があります。DNS 解決を設定していない場合、最初に設定するか、IP アドレスを使用する必要があります。

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 [保存 (Save)] をクリックします。

eStreamer サーバはクライアント コンピュータから Management Center 上のポート 8302 へのアクセスを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。新しいクライアントが [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 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
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 ログで eStreamer を実行します。エラーは <code>syslog</code> 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。エラーは画面に表示されます。
--nohostcheck	<p>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 <code>subjectAltName:dNSName</code> 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。</p> <p> 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。</p>

最初に eStreamer サービスを停止し、次に必要なオプションでサービスを実行し、最後にサービスを再開して、上記のオプションを使用します。たとえば、eStreamer の機能をデバッグするには、[デバッグ モードでの eStreamer サービスの実行\(6-6 ページ\)](#)に記載されている手順に従うことができます。

デバッグモードでの eStreamer サービスの実行

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および Perl モジュールのセットです。これらを実行して eStreamer の出力に習熟したり、これらを使用してカスタム設計クライアントのインストールの問題をデバッグしたりできます。

参照クライアントのセットアップの詳細については、以降の各項を参照してください。

- [eStreamer Perl 参照クライアントの設定 \(6-6 ページ\)](#)
- [eStreamer Perl 参照クライアントの実行 \(6-12 ページ\)](#)

eStreamer Perl 参照クライアントの設定

eStreamer Perl 参照クライアントを使用するには、まず環境と要件に合うようにサンプルスクリプトを設定する必要があります。

詳細については、次の項を参照してください。

- [eStreamer Perl 参照クライアントについて \(6-7 ページ\)](#)
- [eStreamer 参照クライアントの通信の設定 \(6-7 ページ\)](#)
- [Perl 参照クライアントのための一般的な前提条件のロード \(6-8 ページ\)](#)
- [Perl SNMP 参照クライアントのための前提条件のロード \(6-8 ページ\)](#)
- [テストスクリプトで要求されるデータについて \(6-8 ページ\)](#)
- [テストスクリプトで要求されるデータタイプの変更 \(6-10 ページ\)](#)
- [Perl 参照クライアントのための証明書の作成 \(6-11 ページ\)](#)

eStreamer Perl 参照クライアントについて

eStreamer Perl 参照クライアントを含む 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 サーバに接続できるようにします。

- SFRNABlocks.pm

この Perl モジュールには、検出データのブロックの定義が含まれています。

- ssl_test.pl

この Perl スクリプトは、SSL 接続を介した侵入イベント要求をテストするために使用できます。

- OutputPlugins/csv.pm

この Perl モジュールは、侵入イベントをカンマ区切り値の (CSV) の形式に出力します。

- OutputPlugins/print.pm

この Perl モジュールは、人間が解読可能な形式でイベントを出力します。

- OutputPlugins/snmp.pm

この Perl モジュールは、特定の SNMP サーバにイベントを送信します。

- OutputPlugins/pcap.pm

この Perl モジュールは、パケット キャプチャを pcap ファイルとして保存します。

- OutputPlugins/syslog.pm

この Perl モジュールは、ローカルの syslog サーバにイベントを送信します。

eStreamer 参照クライアントの通信の設定

参照クライアントは、データ通信にセキュア ソケット レイヤ (SSL) を使用します。クライアントとして使用する予定のコンピュータに OpenSSL をインストールし、環境に合わせて適切に設定する必要があります。



コメント

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。
-

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。



コメント

クライアント コンピュータに Net::SSLeay モジュールがインストールされていない場合は、そのモジュールも同様にインストールします。Net::SSLeay は OpenSSL との通信に必要です。

eStreamer サーバへの SSL 接続をサポートするためには、OpenSSL もインストールし、設定する必要があります。詳細については、[eStreamer 参照クライアントの通信の設定 \(6-7 ページ\)](#) を参照してください。

Perl SNMP 参照クライアントのための前提条件のロード

Perl 参照クライアントの eStreamer SNMP モジュールを実行する前に、クライアント コンピュータのクライアント オペレーティング システムで使用可能な最新の net-snmp Perl モジュールをインストールする必要があります。

Perl 参照クライアントのダウンロードと展開

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

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
<code>./ssl_test.pl eStreamerServerName -h HostIPAddresses</code>	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 (2-35 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
<code>./ssl_test.pl eStreamerServerName -d "Global \ domain \ subdomain"</code>	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(2-39 ページ)を参照してください。)
<code>./ssl_test.pl eStreamerServerName -o print -f TextFile</code>	OutputPlugins/print.pm	イベントストリーム要求、メッセージタイプ 2、ビット 2 および 20 ~ 24 を 1 に設定	イベントデータ(イベントストリーム要求メッセージの形式(2-11 ページ)、関連ポリシーレコード(3-25 ページ)、関連ルールレコード(3-26 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データ構造(4-64 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。
<code>./ssl_test.pl eStreamerServerName -o pcap -f TargetPCAPFile</code>	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(2-19 ページ)およびパケットレコード 4.8.0.2 以上(3-7 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。
<code>./ssl_test.pl eStreamerServerName -o csv -f CSVFile</code>	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(2-19 ページ)および侵入イベントレコード 6.0 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。
<code>./ssl_test.pl eStreamerServerName -o snmp -f SNMPServer</code>	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(2-19 ページ)および侵入イベントレコード 6.0 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。
<code>./ssl_test.pl eStreamerServerName -o syslog</code>	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(2-19 ページ)および侵入イベントレコード 6.0 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。

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 \(2-13 ページ\)](#) 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 の関連イベント
\$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 の関連イベント
\$FLAG_RNA_EVENTS_3	10	バージョン 3 の検出イベント
\$FLAG_HOST_ONLY	11	\$FLAG_HOST_SINGLE (1 台のホスト用) または \$FLAG_HOST_MULTI (複数のホスト用) とともに送信される場合は、イベント データのないホスト データのみ
\$FLAG_RNA_FLOW_3	12	バージョン 3 の接続データ
\$FLAG_POLICY_EVENTS_3	13	バージョン 3 の関連イベント
\$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 の関連イベント
\$FLAG_METADATA_4	20	バージョン 4 のメタデータ
\$FLAG_RUA	21	ユーザ アクティビティ イベント
\$FLAG_POLICY_EVENTS_5	22	バージョン 5 の関連イベント
\$FLAGS_SEND_ARCHIVE_TIMESTAMP	23	タイムスタンプを含む拡張されたイベント ヘッダーは、eStreamer サーバでの処理のためにイベントがアーカイブされたときに適用されます
\$FLAG_RNA_EVENTS_5	24	バージョン 5 の検出イベント
\$FLAG_RNA_EVENTS_6	25	バージョン 6 の検出イベント

表 6-4 サンプル スクリプトで使用される要求フラグ変数(続き)

変数	設定する要求フラグ	要求するデータ
\$FLAG_RNA_FLOW_5	26	バージョン 5 の接続データ
\$FLAG_EXTRA_DATA	27	侵入イベント追加データレコード
\$FLAG_RNA_EVENTS_7	36	バージョン 7 の検出イベント
\$FLAG_POLICY_EVENTS_6	29	バージョン 6 の関連イベント
\$FLAG_DETAIL_REQUEST	30	eStreamer に対する拡張された要求



注意

バージョン 5.x より前は、すべてのイベントタイプでは、参照クライアントは detection engine ID フィールドを sensor ID としてラベル付けしています。

Perl 参照クライアントのための証明書の作成

ライセンス:任意(Any)

Perl 参照クライアントを使用する前に、Management Center または管理対象デバイスで、クライアントを実行するコンピュータ用に証明書を作成する必要があります。次に、証明書ファイルをクライアント コンピュータにダウンロードし、それを使用して証明書(server.crt)および RSA キーファイル(server.key)を作成します。

Perl 参照クライアントのための証明書の作成:

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。
- コメント** ホスト名を使用する場合は、ホスト入力サーバはホストを IP アドレスに解決できる必要があります。DNS 解決を設定していない場合、最初に設定するか、IP アドレスを使用する必要があります。
- 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** [保存(Save)] をクリックします。

eStreamer サーバはクライアント コンピュータから Management Center 上のポート 8302 へのアクセスを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。新しいクライアントが [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 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設計されていますが、クライアント マシンが [eStreamer Perl 参照クライアントの設定 \(6-6 ページ\)](#) で定義されている前提条件を満たしていれば、任意の POSIX ベースの 64 ビットのオペレーティングシステムでも機能します。

詳細については、次の項を参照してください。

- [ホストの要求を使用した SSL 上のクライアント接続のテスト \(6-12 ページ\)](#)
- [参照クライアントを使用した PCAP のキャプチャ \(6-13 ページ\)](#)
- [参照クライアントを使用した CSV レコードのキャプチャ \(6-13 ページ\)](#)
- [参照のクライアントを使用した SNMP サーバへのレコードの送信 \(6-13 ページ\)](#)
- [参照クライアントを使用した Syslog へのイベントのロギング \(6-13 ページ\)](#)
- [IPv6 アドレスへの接続 \(6-14 ページ\)](#)

ホストの要求を使用した SSL 上のクライアント接続のテスト

ssl_test.pl スクリプトを使用すると、eStreamer サーバおよび eStreamer クライアント間で接続をテストできます。ssl_test.pl スクリプトはどのレコードタイプも処理し、STDOUT または指定する出力プラグインにこれを出力します。出力オプションを使用せずに -h オプションを使用すると、指定したホストのホストデータが端末にストリームされます。



コメント

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 サーバからストリームされたイベントを使用して、`test.csv` という名前の CSV ファイルを作成するには、次の構文を使用します。

```
./ssl_test.pl 10.10.0.4 -o csv -f test.csv
```

参照のクライアントを使用した SNMP サーバへのレコードの送信

侵入イベントデータを SNMP サーバにストリームする場合も、参照クライアントを使用できます。`-f` オプションを使用して、イベントを受信する SNMP トラップサーバの名前を示します。この出力方法では、パスに `snmptrapd` という名前のバイナリが必須であるため、UNIX のようなシステムでのみ機能することに注意してください。

SNMP サーバに侵入イベントを送信するには、次の構文を使用します。

```
./ssl_test.pl eStreamerServerIPAddress -o snmp  
-f SNMPServerName
```

たとえば、10.10.0.4 の IP アドレスの eStreamer サーバからストリームされたイベントを使用して、10.10.0.3 で SNMP サーバにイベントを送信するには、次の構文を使用します。

```
./ssl_test.pl 10.10.0.4 -o snmp -f 10.10.0.3
```

参照クライアントを使用した Syslog へのイベントのロギング

クライアントのローカル syslog サーバに侵入イベントをストリームする場合も、参照クライアントを使用できます。

Syslog にイベントを送信するには、次の構文を使用します。

```
./ssl_test.pl eStreamerServerIPAddress -o syslog
```

たとえば、10.10.0.4 の IP アドレスの eStreamer サーバからストリームされたイベントを記録するには、次の構文を使用します。

```
./ssl_test.pl 10.10.0.4 -o syslog
```

IPv6 アドレスへの接続

プライマリ管理インターフェイスを介して IPv6 アドレスの Management Center に接続する場合も、参照クライアントを使用できます。クライアントのマシンには **Socket6** および **IO::Socket::INET6 Perl** モジュールがインストールしてある必要があり、`-ipv6` オプションまたは短縮形式の `-i` を使用します。

`ssl_test.pl` スクリプトを使用して IPv6 アドレスを指定するには、次の構文を使用します。

```
./ssl_test.pl -ipv6 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
```



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 \(A-32 ページ\)](#)

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 \(A-13 ページ\)](#)
- [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 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	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	0	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	0	0	1	1

■ 侵入イベントのデータ構造の例

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

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

■ 侵入イベントのデータ構造の例

バイト	0								1								2								3									
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
34	0	0	1	0	1	1	0	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	0	1	1	0	0	1	1	0	0	0	
	1	1	1	1	1	1	1	0	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	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	0	0	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	0	1	0	0	0	0	0	0	1	0	1	1	0	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	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	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	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
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
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
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
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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

上記の例では、次のイベント情報を確認できます。

番号 (Number)	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。

番号 (Number)	説明
21	この行の最初のバイトは、TCP(6)がイベントで使用されているプロトコルであることを示しています。2番目のバイトは影響フラグであり、2番目のビットが1であるため、イベントがレッド(脆弱)であることを示します。また、送信元または宛先ホストはシステムによってモニタされているネットワーク内にあること、送信元または宛先ホストがネットワークマップにあること、送信元または宛先ホストがイベント発生ポートでサーバを実行していることを示します。さらに、2番目と3番目のフラグが1であるため、これがオレンジ(脆弱の可能性あり)のイベントであることを示しています。この行の3番目のバイトは影響フラグです。2であるため、イベントがオレンジ(脆弱の可能性あり)であることを示しています。最後のバイトはイベントがブロックされなかったことを示しています。
22	この行には、MPLS ラベルが含まれます(存在する場合)。
23	この行の最初の2バイトはVLAN IDが0であることを示しています。最後の2バイトは、予約されており、0に設定されています。
24	この行には、侵入ポリシーの一意のID番号が含まれます。
25	この行には、ユーザの内部ID番号が含まれます。該当のユーザが存在しないため、すべてゼロになっています。
26	この行にはWebアプリケーションの内部ID番号が含まれ、この場合は847となっています。
27	この行にはクライアントアプリケーションの内部ID番号が含まれ、この場合は2000000676となっています。
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。

番号 (Number)	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 サーバ証明書の SHA1 ハッシュの残りの部分が含まれます。
42	この行の最初の 2 バイトには、SSL サーバ証明書の SHA1 ハッシュの最後の 2 バイトが含まれます。2 番目の 2 バイトには、実際に実行された SSL アクションが含まれます。この接続では SSL が使用されなかったため、0 になっています。
43	この行の最初の 2 バイトには、SSL フロー ステータスが含まれます。この接続では SSL が使用されなかったため、0 になっています。2 番目の 2 バイトには、このイベントに関連付けられているネットワーク分析ポリシーの UUID の最初の 2 バイトが含まれます。
44	この行には、このイベントに関連付けられているネットワーク分析ポリシーの UUID の残りの部分が含まれます。

侵入影響アラートの例

次の図に、侵入影響アラート レコードの例を示します。

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	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	0	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	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	0	0	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	1	0	1	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
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	1	0	0	0	1	0	1	0	0	
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
9	0	1	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	1
11	1	0	1	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	
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

■ 侵入イベントのデータ構造の例

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

上記の例では、次の情報を確認できます。

番号 (Number)	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 (3-63 ページ) を参照してください。

番号 (Number)	説明
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	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	0	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	0	0	1	0	
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	1	0	1		
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	0	1	1	1	0	0	1	0	1	0	
8	0	0	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	1	0	0	
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	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	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	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	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0
	0	0	1	1	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	1	0	0	0	0

上記の例では、次のパケット情報を確認できます。

番号 (Number)	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。

番号 (Number)	説明
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。
8	この行は、パケットが 10572380 秒で収集されたことを示しています。
9	この行は、パケットが 254365 マイクロ秒で収集されたことを示しています。
10	この行は、リンクタイプが 1(イーサネット層)であることを示しています。
11	この行は、後続のパケットデータの長さが 953 バイトであることを示しています。
12	この行と次の行は、実際のペイロードデータを示します。実際のデータは 953 バイトであり、この例では切り捨てられていることに注意してください。

分類レコードの例

次の図に、分類レコードの例を示します。

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

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

上記の例では、次のイベント情報を確認できます。

番号 (Number)	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。

番号 (Number)	説明
8	この行は、分類の一意の ID としての役割を果たす分類 ID 番号を示します。
9	この行は、分類のリビジョンの一意の ID としての役割を果たす分類リビジョン ID 番号を示し、この場合、分類のリビジョンがないため、Null です。

優先度レコードの例

次に、優先度レコードの例を示します。

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

上記の例では、次のイベント情報を確認できます。

番号 (Number)	説明
1	この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータメッセージ(メッセージタイプ 4)であることを示しています。
2	この行は、後続のメッセージが 16 バイトであることを示しています。
3	この行は、レコードタイプの値 4 を示し、優先度レコードを表します。
4	この行は、後続の優先度レコードの長さが 8 バイトであることを示しています。
5	この行は、優先度 ID が 1 であることを示しています。
6	この行の最初の 2 バイトは、優先度名に 4 バイトが含まれていることを示しています。2 番目の 2 バイトと次の行の 2 バイトは、優先度名自体(「high(高)」)を示しています。

ルールメッセージレコードの例

次に、ルールメッセージレコードの例を示します。

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

■ 侵入イベントのデータ構造の例

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

上記の例では、次のイベント情報を確認できます。

番号 (Number)	説明
1	この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ(つまり、メッセージ タイプ 4)であることを示しています。
2	この行は、後続のメッセージが 129 バイトであることを示しています。
3	この行の先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーではないことを示すフラグです。後続の 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプション フィールドです。行の残りの部分は、レコード タイプの値 66 を示し、ルール メッセージ レコードを表します。
4	この行は、後続のルール メッセージ レコードの長さが 121 バイトであることを示しています。
5	この行は、ジェネレータ ID 番号が 1(ルール エンジン)であることを示しています。
6	この行は、ルール ID 番号が 28069 であることを示しています。
7	この行は、ルールのリビジョン番号が 1 であることを示しています。
8	この行は、Firepower システム に渡されたルール ID 番号が 28069 であることを示しています。
9	この行の最初の 2 バイトは、ルール テキスト名に 71 バイトが含まれていることを示しています。2 番目の 2 バイトは、ルールの一意の ID 番号で始まります。

番号 (Number)	説明
10	この行の最初の2バイトは、ルールの一意的 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的 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的 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	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	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	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	1	0	0	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	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	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	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	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	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	0
10	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	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	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	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	0	0
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	1
16	0	0	0	0	1	0	0	0	1	0	1	1	1	0	1	0	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

■ 侵入イベントのデータ構造の例

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

■ 侵入イベントのデータ構造の例

バイト	0							1							2							3										
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
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
42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	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
	0	0	0	0	0	0	0	0	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
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	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
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
	0	0	0	0	0	0	0	0	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
	0	0	0	0	0	0	0	0	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	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
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
	0	0	0	0	0	0	0	0	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

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
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	
56	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	
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	
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	
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	
60	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	1	0	0	0
61	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	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	
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	
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	
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	
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	
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	
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	
69	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	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	
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	
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	
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	
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	
75	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	
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	
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	

■ 侵入イベントのデータ構造の例

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

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

■ 侵入イベントのデータ構造の例

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

上記の例では、次のイベント情報を確認できます。

番号 (Number)	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せん。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。

番号 (Number)	説明
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。
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、開始ホストに回答したホストの 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、トリガーされた関連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、レスポンス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。

番号 (Number)	説明
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。
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нда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нда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нда送信バイトが開始します(0)。
42	最初のバイトはレスポнда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нда 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нда 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нда 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нда 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の ID 番号です(16466)。
49	この行の最初のバイトは、ユーザ 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。

番号 (Number)	説明
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。
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。
56	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、この行の残りはブロック 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)。

番号 (Number)	説明
67	この行には、8 番目のモニターールの 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 アドレスを IP ブラックリストに突き合わせ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 ブラックリストの一致した 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、レスポンスの国です (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。
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: 0000-0000000000000000 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 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 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。

番号 (Number)	説明
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)。
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_NULL_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)。

番号 (Number)	説明
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)。
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 イベントの例

次の図に、ユーザ イベント レコードの例を示します。

バイト	0								1								2								3											
	0	1	2	3	4	5	6	7	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	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	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	0	1	0	1	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	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	1	1	1	1	1	0	0	0	0	1	0	1	0	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	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	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	0	0	0	0

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

■ 侵入イベントのデータ構造の例

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
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	0	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 (Number)	説明
1	この行の最初の 2 バイトは、標準ヘッダー値 1 を示しています。2 番目の 2 バイトは、メッセージがデータ メッセージ(つまり、メッセージ タイプ 4)であることを示しています。
2	この行は、後続のメッセージの長さが 153 バイトであることを示しています。
3	この先頭ビットは、ヘッダーがアーカイブのタイムスタンプを含む拡張ヘッダーであることを示すフラグです。後続の 15 ビットは、イベントが検出されたドメインの Netmap ID を含むオプションフィールドです。行の残りの部分は、レコードタイプの値 95 を示し、ユーザ情報更新メッセージを表します。
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。

番号 (Number)	説明
12	この行には、システムがイベントを生成した時刻をマイクロ秒(100 万分の 1 秒)単位で表した値が含まれます。
13	この行には、イベントタイプが含まれます。ユーザ変更メッセージを示す値 1004 が含まれています。
14	この行には、イベント サブタイプが含まれます。ユーザ ログイン イベントを示す値 2 が含まれています。
15	この行には、シリアル ファイル番号が含まれます。このフィールドは、内部使用向けであり、無視してかまいません。
16	この行には、シリアル ファイル内のイベントの位置が含まれます。このフィールドは、内部使用向けであり、無視してかまいません。
17	この行には、IPv6 アドレスが含まれます。このフィールドは、IPv6 フラグが設定されている場合に存在し、使用されます。ただし、この場合は IPv4 アドレス 10.4.15.120 が含まれています。
18	この行は、ブロック タイプ 127 で示されるユーザ ログイン情報データ ブロックで始まります。
19	この行は、後続のブロックの長さが 81 バイトであることを示しています。
20	この行は、ユーザ ログインのタイムスタンプが 1,391,456,7 であることを示しています。これは、2014 年 10 月 3 日(月)の 19 時 43 分 47 秒(GMT)に生成されたことを意味します。
21	この行は、レガシー IP(IPv4)アドレス用です。事前に設定されていないため、すべてゼロになっており、IPv4 アドレスは IPv6 フィールドに保存されます。
22	この行は、文字列ブロックの長さでテキスト文字列を含む文字列ブロックが続くことを示します。この場合、テキスト文字列はユーザ名です。文字列ブロックの詳細については、 文字列データ ブロック (3-63 ページ) を参照してください。
23	この行は、文字列ブロック内のデータの長さが 16 バイトであることを示しています。
24	この行は、ユーザ名が「301@10.4.11.175」であることを示しています。
25	この行は、ユーザの ID 番号を示します。
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で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 (3-63 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、このユーザに関連付けられている電子メールアドレスがないためです。
29	この行には、ユーザのログインが検出されたホストの IP アドレスが含まれます。

番号 (Number)	説明
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してテキスト文字列を含む文字列ブロックが続くことを示します。この場合、テキスト文字列は、ログインを報告した Active Directory サーバの名前です。文字列ブロックの詳細については、 文字列データ ブロック (3-63 ページ) を参照してください。
31	この行の先頭バイトで、文字列データ ブロックの開始が完了します。この行の残りの部分は、文字列ブロック内のデータの長さが 0 バイトであることを示しています。なぜならば、このログインに関連付けられている Active Directory サーバがないためです。

ディスカバリ データ構造の例

このセクションでは、ディスカバリ イベントに関して eStreamer で送信されることがあるデータ構造の例を紹介いたします。ここでは、次の例を示します。

- [新しいネットワークング プロトコル メッセージの例 \(A-32 ページ\)](#)
- [新しい TCP サーバ メッセージの例 \(A-33 ページ\)](#)

新しいネットワークング 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												
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
ヘッダーバージョン 1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	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	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	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	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	0	0	0	0	1	0	

バイト	0								1								2								3										
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
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	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	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	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	0	0	1	1	1	1	1	0	1	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	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	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	0	0	標準メッセー ジヘッダーの 終了
プロトコル (6—TCP)	0	0	0	0	0	1	1	0																											

新しい TCP サーバメッセージの例

次の図に、3.0+ の新しい TCP サーバメッセージの例を示します。

バイト	0								1								2								3									
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
ヘッダーバー ジョン 1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	1	0	0	0	0	0	0	0	0	

■ ディスカバリ データ構造の例

バイト	0								1								2								3												
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
新しい TCP サーバ メッ セージ(11)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	1	1	1	1	
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	0	0	0	0	0	1	
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	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	
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	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	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	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	0	0	0	0	0	0	0	0	0	0	標準メッ セージヘッ ダーの終了	
サーバブロッ ク ヘッダー (12)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	サーバデー タブロック の開始		
サーバ長 (208 バイト)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0				
サーバポート (80)	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	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		

バイト	0								1								2								3																																	
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	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	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	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブ ロック長				
文字列ブ ロック長 (15バイト)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	0	0	0	0	1																
サーバベン 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	1	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	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブ ロック長			
文字列長(8- 製品なし)	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	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	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	0	1	1	0	0	1	0	0	0	1	1	0	1	1	0	0	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	0	1	1	0	1	1	0		
	0	1	1	0	1	0	0	1	0	1	1	1	1	0	0	0	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	0	1	1	0	1	0	0	1	0	0	1	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	サブサーバリ ストの開始	

■ ディスカバリ データ構造の例

バイト	0								1								2								3															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
リストブロック 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	0	0	0	0	1	0	1	1	1	1	0	
サブサーバ ヘッダー(1)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	サブサーバブ ロックの開始
サブサーバ長 (46 バイト)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	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	0	0	0	0	1	0	0	0	0			
サブサーバ名 - mod_ssl	0	1	1	0	1	1	0	1	0	1	1	0	1	1	1	1	0	1	1	0	0	1	0	0	0	1	0	1	1	1	1	1	1							
文字列ブ ロックヘッ ダー(0)	0	1	1	1	0	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	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	0	0	0	0	0	1	0	0	0	(サブタイプペ 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	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	0	0	0	0	0	1	1	1	0			
サブサーバ バージョン - 2.8.9 + Null 文 字	0	0	1	1	0	0	1	0	0	0	1	0	1	1	1	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	サブサーバブ ロックの終了		
	0	0	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	サブサーバブ ロックの開始
サブサーバ ヘッダー(1)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	サブサーバ長
サブサーバ長 (48 バイト)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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																											
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	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	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	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	0	1	1	1	0	0	0	0	0					
サブサーバ名 -OpenSSL	0	1	1	0	0	1	0	1	0	1	0	1	1	0	1	1	0	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	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	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	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	文字列ブ ロック長	
文字列ブ ロック長 (16バイト)	0	0	0	0	0	0	0	0	0	0	0	0	0	1	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	0	0	1	0	1	1	1	1	0		
サブサーバ バージョン- 0.9.6.d+Null 文字	0	0	1	1	1	0	0	1	0	0	1	0	1	1	1	0	0	0	1	1	0	1	1	0	0	0	1	0	1	1	1	0	0	0	1	1	0	1	1	0	0	0	1	0	1	1	1	0	0	0	0	サブサーバブ ロックの終了
信頼性(%)	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	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	1	1	0	0	1	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	1	1	0	1	0	1	0	1	1	1	前回の使用	
前回の使用 (1047242787)	1	0	1	0	1	0	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	0	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	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	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	0	1	0	1	1	0	0	1	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0	0	1	0	0	0	0	1	0	1	0	1	0	1	0	0	0		

■ ディスカバリ データ構造の例

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
サーバ ナー (HTTP/1.1 414 要求)- 短縮された サーバ 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	1	0	1	1	1	1	0	0	1	1	0	0	0	1	サーバデータ ブロックの終了	
	0	0	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	1	0	1	0		0
	0	0	1	1	0	0	0	1	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	0	1		0
	0	1	1	0	0	1	0	1	0	1	1	1	0	0	0	1	0	1	1	1	0	1	0	1	0	1	1	0	0	1	0		1

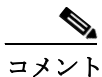


レガシー データ構造の概要

この付録には、旧バージョンの Firepower システム 製品の eStreamer によってサポートされるデータ構造に関する情報を記載しています。

クライアントが、旧バージョン形式でデータを要求するようにビットが設定されているイベントストリーム要求を使用する場合、この付録の情報を使用して、受け取るデータ メッセージのデータ構造を識別できます。

バージョン 5.0 より前は、検出エンジンに個別に ID が割り当てられていたことに注意してください。バージョン 5.0 では、デバイスに ID が割り当てられます。この点は、バージョンに基づいてデータ構造に反映されます。



コメント

この付録では、Firepower システム のバージョン 4.9 以降からのデータ構造のみを説明します。以前のデータ構造バージョンによる構造向けの資料が必要な場合は、シスコ 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 \(B-1 ページ\)](#)
- [レガシー マルウェア イベントのデータ構造 \(B-51 ページ\)](#)
- [レガシー ディスカバリ データ構造 \(B-94 ページ\)](#)
- [レガシー接続データ構造 \(B-135 ページ\)](#)
- [レガシー関連イベントのデータ構造 \(B-274 ページ\)](#)
- [レガシー ホスト データ構造 \(B-291 ページ\)](#)

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 \(B-2 ページ\)](#)
- [侵入イベント \(IPv6\) レコード 5.0.x ~ 5.1 \(B-8 ページ\)](#)
- [侵入イベント レコード 5.2.x \(B-14 ページ\)](#)
- [侵入イベント レコード 5.3 \(B-20 ページ\)](#)
- [侵入イベント レコード 5.1.1.x \(B-26 ページ\)](#)
- [侵入イベント レコード 5.3.1 \(B-32 ページ\)](#)
- [侵入イベント レコード 5.4.x \(B-39 ページ\)](#)
- [侵入影響アラート データ \(B-48 ページ\)](#)

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 \(2-13 ページ\)](#) および [拡張要求の送信 \(2-4 ページ\)](#) を参照してください。

バージョン 5.0.x ~ 5.1 の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (207)															
	レコード長																															
	eStreamer サーバ タイムスタンプ (イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み (イベントでビット 23 が設定されている場合のみ)																															
	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 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															

バイト	0							1							2							3										
ビット	0	1	2	3	4	5	6	7	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 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 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)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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	uint32	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 (3-37 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 Firepower システム プリプロセッサの ID 番号。
ルールリビジョン	uint32	ルールリビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IPv4 アドレス	uint8[4]	アドレス オクテットの、イベントで使用される送信元 IPv4 アドレス。

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
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。 <ul style="list-style-type: none">• 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]	<p>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。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。 <p>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。</p> <ul style="list-style-type: none"> (0、不明):00x00000 赤(1、脆弱):xxx1xxx, 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	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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 ID (User ID)	uint32	ユーザの内部 ID 番号 (該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号 (該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号 (該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号 (該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。

侵入イベント (IPv6) レコード 5.0.x ~ 5.1

侵入イベント (IPv6) レコードのフィールドは、次の図では網掛けされています。レコードの種類は 208 です。

侵入イベント レコードは、要求メッセージに侵入イベント フラグまたは拡張要求フラグを設定して要求します。[要求フラグ \(2-13 ページ\)](#) および [拡張要求の送信 \(2-4 ページ\)](#) を参照してください。

バージョン 5.0.x ~ 5.1 の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(208)															
	レコード長																															
	eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
	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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
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 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	インターフェイス入力 UUID(続き)																															
	インターフェイス入力 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	uint32	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 (3-37 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 Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 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。 <ul style="list-style-type: none"> • 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]	<p>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。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。 <p>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。</p> <ul style="list-style-type: none"> (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	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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 ID (User ID)	uint32	ユーザの内部 ID 番号 (該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号 (該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号 (該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号 (該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。

侵入イベント レコード 5.2.x

侵入イベントレコードのフィールドは、次の図で網掛けされています。レコードタイプは400であり、ブロックタイプはシリーズ2セットのデータブロックの34です。

eStreamer からの 5.2.x 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベントタイプコード12およびバージョン5を要求します(拡張要求の送信の詳細については、[拡張要求の送信\(2-4 ページ\)](#)を参照してください)。

バージョン 5.2.x の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。接続の秒、接続インスタンス、および接続数カウンタは、侵入イベントに関連付けられた接続イベントの、1つの固有識別子を形成します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(400)															
	レコード長																															
	eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
	ブロックタイプ(34)																															
	ブロック長																															
	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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
送信元 IP アドレス																																
送信元 IP アドレス(続き)																																
送信元 IP アドレス(続き)																																
送信元 IP アドレス(続き)																																
宛先 IP アドレス																																
宛先 IP アドレス(続き)																																
宛先 IP アドレス(続き)																																
宛先 IP アドレス(続き)																																
送信元ポートまたは ICMP タイプ																送信先ポートまたは ICMP コード																
IP プロトコル ID								影響フラグ								影響								ブロック								
MPLS ラベル																																
VLAN ID (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 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
インターフェイス入力 UUID																																
インターフェイス入力 UUID (続き)																																
インターフェイス入力 UUID (続き)																																
インターフェイス入力 UUID (続き)																																
インターフェイス出力 UUID																																
インターフェイス出力 UUID (続き)																																
インターフェイス出力 UUID (続き)																																
インターフェイス出力 UUID (続き)																																
セキュリティゾーン入力 UUID																																
セキュリティゾーン入力 UUID (続き)																																
セキュリティゾーン入力 UUID (続き)																																
セキュリティゾーン入力 UUID (続き)																																
セキュリティゾーン出力 UUID																																
セキュリティゾーン出力 UUID (続き)																																
セキュリティゾーン出力 UUID (続き)																																
セキュリティゾーン出力 UUID (続き)																																
接続タイムスタンプ																																
接続インスタンス ID																接続数カウンタ																
送信元の国																宛先の国																

次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 B-3 侵入イベント レコード 5.2.x のフィールド

フィールド	データタイプ	説明
ブロックタイプ	uint32	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	uint32	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	uint32	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 (3-37 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 Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポートまたは ICMP タイプ	uint16	イベントプロトコルタイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
送信先ポートまたは ICMP コード	uint16	イベントプロトコルタイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none"> • 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]	<p>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。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) <p>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。</p> <ul style="list-style-type: none"> (0、不明):00x00000 赤(1、脆弱):xxx1xxx, 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	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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 ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970年1月1日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。

表 B-3 侵入イベント レコード 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。

侵入イベント レコード 5.3

侵入イベント レコードのフィールドは、次の図で網掛けされています。レコードタイプは 400 であり、ブロックタイプはデータブロックのシリーズ 2 セットの 41 です。

eStreamer からの 5.3 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベントタイプコード 12 およびバージョン 6 を要求します(拡張要求の送信の詳細については、[拡張要求の送信 \(2-4 ページ\)](#) を参照してください)。

バージョン 5.3 の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。接続の秒、接続インスタンス、および接続数カウンタは、侵入イベントに関連付けられた接続イベントの、1 つの固有識別子を形成します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(400)															
	レコード長																															
	eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
	ブロックタイプ(41)																															
	ブロック長																															
	Device ID																															
	イベント ID(Event ID)																															
	イベント秒																															
	イベントマイクロ秒																															

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
ビット																																	
	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)																																
	ポリシー UUID (続き)																																
	ポリシー UUID (続き)																																
	ユーザ 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																																

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
アクセスコントロールルール ID																																
アクセスコントロールポリシー UUID																																
アクセスコントロールポリシー UUID(続き)																																
アクセスコントロールポリシー UUID(続き)																																
アクセスコントロールポリシー UUID(続き)																																
インターフェイス入力 UUID																																
インターフェイス入力 UUID(続き)																																
インターフェイス入力 UUID(続き)																																
インターフェイス入力 UUID(続き)																																
インターフェイス出力 UUID																																
インターフェイス出力 UUID(続き)																																
インターフェイス出力 UUID(続き)																																
インターフェイス出力 UUID(続き)																																
セキュリティゾーン入力 UUID																																
セキュリティゾーン入力 UUID(続き)																																
セキュリティゾーン入力 UUID(続き)																																
セキュリティゾーン入力 UUID(続き)																																
セキュリティゾーン出力 UUID																																
セキュリティゾーン出力 UUID(続き)																																
セキュリティゾーン出力 UUID(続き)																																
セキュリティゾーン出力 UUID(続き)																																
接続タイムスタンプ																																
接続インスタンス ID																接続数カウンタ																
送信元の国																宛先の国																
IOC 番号																																

次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 B-4 侵入イベント レコード 5.3 のフィールド

フィールド	データタイプ	説明
ブロックタイプ	uint32	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	uint32	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	uint32	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 (3-37 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 Firepower システム プリプロセッサの ID 番号。
ルールリビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポートまたは ICMP タイプ	uint16	イベントプロトコルタイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
送信先ポートまたは ICMP コード	uint16	イベントプロトコルタイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none"> • 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]	<p>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。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) <p>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。</p> <ul style="list-style-type: none"> (0、不明):00x00000 赤(1、脆弱):xxx1xxx, 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	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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 ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970年1月1日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。

表 B-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
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。

侵入イベント レコード 5.1.1.x

侵入イベント レコードのフィールドは、次の図で網掛けされています。レコードタイプは 400 で、ブロックタイプは 25 です。

eStreamer からの 5.1.1 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベントタイプコード 12 およびバージョン 4 を要求します(拡張要求の送信の詳細については、[拡張要求の送信 \(2-4 ページ\)](#)を参照してください)。

バージョン 5.1.1.x の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。接続の秒、接続インスタンス、および接続数カウンタは、侵入イベントに関連付けられた接続イベントの、1 つの固有識別子を形成します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(400)															
	レコード長																															
	eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
	ブロックタイプ(25)																															
	ブロック長																															
	Device ID																															
	イベント ID(Event ID)																															
	イベント秒																															
	イベントマイクロ秒																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ルール ID (シグネチャ ID)																															
	ジェネレータ ID																															
	ルール リビジョン																															
	分類 ID																															
	プライオリティ ID																															
	送信元 IP アドレス																															
	送信元 IP アドレス (続き)																															
	送信元 IP アドレス (続き)																															
	送信元 IP アドレス (続き)																															
	宛先 IP アドレス																															
	宛先 IP アドレス (続き)																															
	宛先 IP アドレス (続き)																															
	宛先 IP アドレス (続き)																															
	送信元ポート/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 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																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	アクセス コントロール ルール ID																															
	アクセス コントロール ポリシー UUID																															
	アクセス コントロール ポリシー UUID (続き)																															
	アクセス コントロール ポリシー UUID (続き)																															
	アクセス コントロール ポリシー UUID (続き)																															
	インターフェイス入力 UUID																															
	インターフェイス入力 UUID (続き)																															
	インターフェイス入力 UUID (続き)																															
	インターフェイス入力 UUID (続き)																															
	インターフェイス出力 UUID																															
	インターフェイス出力 UUID (続き)																															
	インターフェイス出力 UUID (続き)																															
	インターフェイス出力 UUID (続き)																															
	セキュリティゾーン入力 UUID																															
	セキュリティゾーン入力 UUID (続き)																															
	セキュリティゾーン入力 UUID (続き)																															
	セキュリティゾーン入力 UUID (続き)																															
	セキュリティゾーン出力 UUID																															
	セキュリティゾーン出力 UUID (続き)																															
	セキュリティゾーン出力 UUID (続き)																															
	セキュリティゾーン出力 UUID (続き)																															
	接続タイムスタンプ																															
	接続インスタンス ID																接続数カウンタ															

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	uint32	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	uint32	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	uint32	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 (3-37 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 Firepower システム プリプロセッサの ID 番号。
ルールリビジョン	uint32	ルールリビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポート/ICMP タイプ	uint16	イベントプロトコルタイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
宛先ポート/ICMP コード	uint16	イベントプロトコルタイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none"> • 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]	<p>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。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。 <p>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。</p> <ul style="list-style-type: none"> (0、不明):00x00000 赤(1、脆弱):xxx1xxx, 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	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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 ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970年1月1日からの経過秒数)。

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 インスタンスの数值 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。

侵入イベント レコード 5.3.1

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

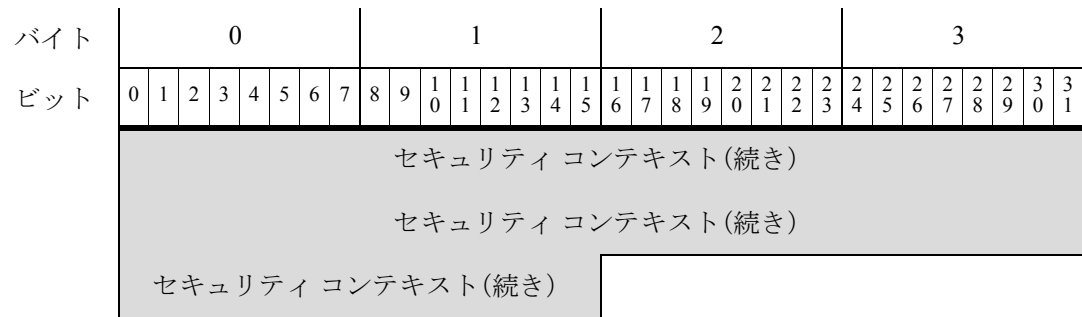
eStreamer からの 5.3.1 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベントタイプコード 12 およびバージョン 7 を要求します(拡張要求の送信の詳細については、[拡張要求の送信 \(2-4 ページ\)](#) を参照してください)。

バージョン 5.3.1 の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。接続の秒、接続インスタンス、および接続数カウンタは、侵入イベントに関連付けられた接続イベントの、1 つの固有識別子を形成します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(400)															
	レコード長																															
	eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
	ブロックタイプ(42)																															
	ブロック長																															
	デバイス ID(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)																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	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 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
アクセスコントロールポリシー UUID																																
アクセスコントロールポリシー UUID(続き)																																
アクセスコントロールポリシー UUID(続き)																																
アクセスコントロールポリシー UUID(続き)																																
インターフェイス入力 UUID																																
インターフェイス入力 UUID(続き)																																
インターフェイス入力 UUID(続き)																																
インターフェイス入力 UUID(続き)																																
インターフェイス出力 UUID																																
インターフェイス出力 UUID(続き)																																
インターフェイス出力 UUID(続き)																																
インターフェイス出力 UUID(続き)																																
セキュリティゾーン入力 UUID																																
セキュリティゾーン入力 UUID(続き)																																
セキュリティゾーン入力 UUID(続き)																																
セキュリティゾーン入力 UUID(続き)																																
セキュリティゾーン出力 UUID																																
セキュリティゾーン出力 UUID(続き)																																
セキュリティゾーン出力 UUID(続き)																																
セキュリティゾーン出力 UUID(続き)																																
接続タイムスタンプ																																
接続インスタンス ID																接続数カウンタ																
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	uint32	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	uint32	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)	uint32	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 (3-37 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 Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。

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。 <ul style="list-style-type: none"> • 0:IP • 1:ICMP • 6:TCP • 17:UDP

表 B-6 侵入イベントレコード 5.3.1 のフィールド(続き)

フィールド	データタイプ	説明
影響フラグ	bits[8]	<p>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。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) <p>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。</p> <ul style="list-style-type: none"> (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	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> 1:レッド(脆弱) 2:オレンジ(脆弱の可能性あり) 3:イエロー(現在は脆弱でない) 4:ブルー(不明なターゲット) 5:グレー(不明なインパクト)

表 B-6 侵入イベント レコード 5.3.1 のフィールド(続き)

フィールド	データタイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 <ul style="list-style-type: none"> 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 ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970年1月1日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。

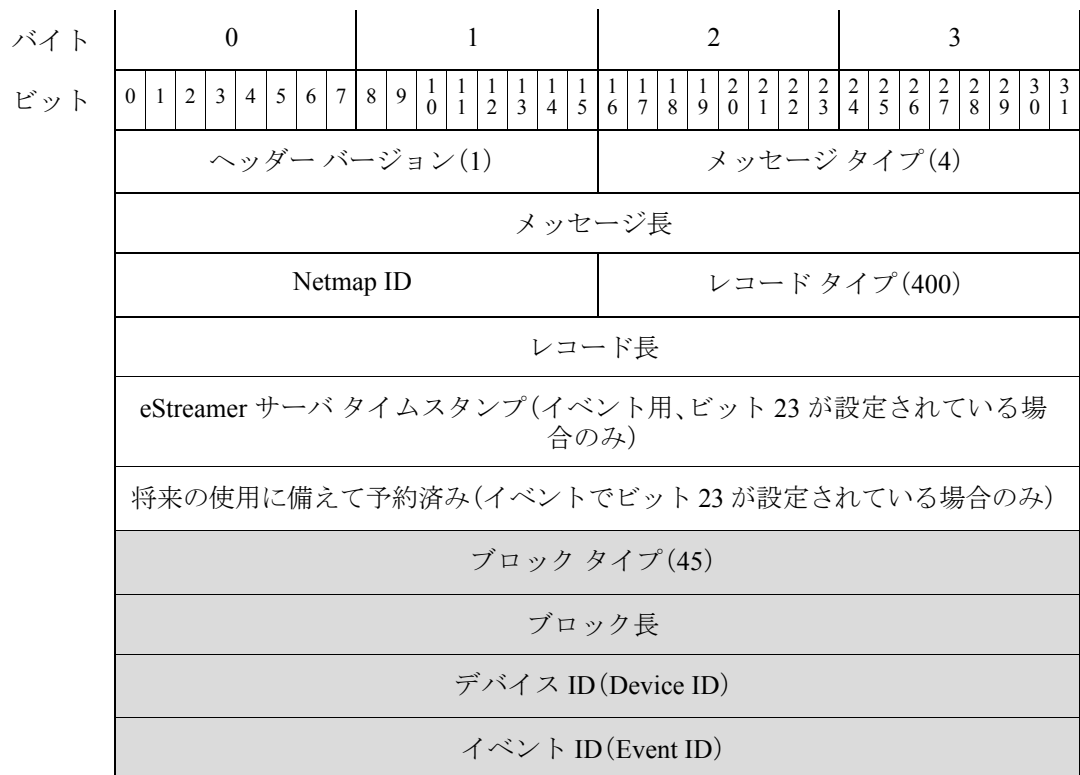
表 B-6 侵入イベントレコード 5.3.1 のフィールド(続き)

フィールド	データタイプ	説明
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	uint16	宛先ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティコンテキスト	uint8(16)	トラフィックが通過したセキュリティコンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキストモードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

侵入イベントレコード 5.4.x

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

eStreamer からの 5.4.x 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベントタイプコード 12 およびバージョン 8 を要求します(拡張要求の送信の詳細については、[拡張要求の送信 \(2-4 ページ\)](#) を参照してください)。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
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)																																
ポリシー UUID (続き)																																
ポリシー UUID (続き)																																
ユーザ ID (User ID)																																
Web アプリケーション ID																																

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	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																															
	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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	接続インスタンス 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	uint32	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	uint32	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)。

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
デバイス ID (Device ID)	uint32	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 (3-37 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 Firepower システム プリプロセッサの ID 番号。
ルールリビジョン	uint32	ルールリビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポート または ICMP タイプ	uint16	イベントプロトコルタイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
送信先ポート または ICMP コード	uint16	イベントプロトコルタイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル 番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none"> • 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]	<p>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。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) <p>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。</p> <ul style="list-style-type: none"> グレー(0、不明):00x00000 赤(1、脆弱):xxx1xxx, 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	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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 ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970年1月1日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。

表 B-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。 <ul style="list-style-type: none"> • 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	<p>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。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
ネットワーク分析ポリシー UUID	uint8[16]	侵入イベントを作成したネットワーク分析ポリシーの UUID。

侵入影響アラート データ

侵入影響アラート イベントには、影響イベントに関する情報が含まれます。これは、侵入イベントがシステム ネットワーク マップ データと比較され、影響が判別されているときに送信されます。これはレコードタイプ 9 の標準レコードヘッダーを使用し、シリーズ 1 グループのブロックの、データブロックタイプが 20 である侵入影響アラートデータブロックが続きます。(影響アラートデータブロックタイプは、シリーズ 1 データブロックです。シリーズ 1 データブロックの詳細については、[ディスカバリ \(シリーズ 1\) ブロック \(4-65 ページ\)](#)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 \(2-11 ページ\)](#)を参照してください。これらのアラートのバージョン 1 は、IPv4 のみを処理します。5.3 で導入されたバージョン 2 は、IPv4 に加えて IPv6 イベントを処理します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(9)															
	レコード長																															
	侵入影響アラートブロックタイプ(20)																															
	侵入影響アラートブロック長																															
	イベント ID (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-8 影響イベントデータ フィールド

フィールド	データタイプ	説明
侵入影響アラート ブロックタイプ	uint32	侵入影響アラートデータブロックが続くことを示します。このフィールドの値は、常に 20 です。 侵入イベントとメタデータのレコードタイプ(3-1 ページ) を参照してください。
侵入影響アラート ブロック長	uint32	侵入の影響アラートのブロックタイプの長さを示します。後続のすべてのデータ、および侵入の影響アラートのブロックタイプと長さの 8 バイトを含みます。
イベント ID (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-8 影響イベント データ フィールド(続き)

フィールド	データタイプ	説明
影響	bits[8]	<p>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。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれません。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) <p>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。</p> <ul style="list-style-type: none"> (0、不明):00x00000 赤(1、脆弱):xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx (バージョン 5.0+ のみ) オレンジ(2、潜在的に脆弱):00x0011x 黄(3、現在は脆弱でない):00x0001x 青(4、不明なターゲット):00x00001
送信元 IP アドレス	uint8[4]	IP アドレス オクテットの、影響イベントに関連付けられているホストの IP アドレス。
宛先 IP アドレス	uint8[4]	IP アドレス オクテットの、影響イベントに関連付けられている宛先 IP アドレスの IP アドレス(該当する場合)。宛先 IP アドレスがない場合、この値は 0 です。

表 B-8 影響イベントデータフィールド(続き)

フィールド	データタイプ	説明
文字列ブロックタイプ	uint32	影響名を含む文字列データのブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、 文字列データブロック (4-75 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。

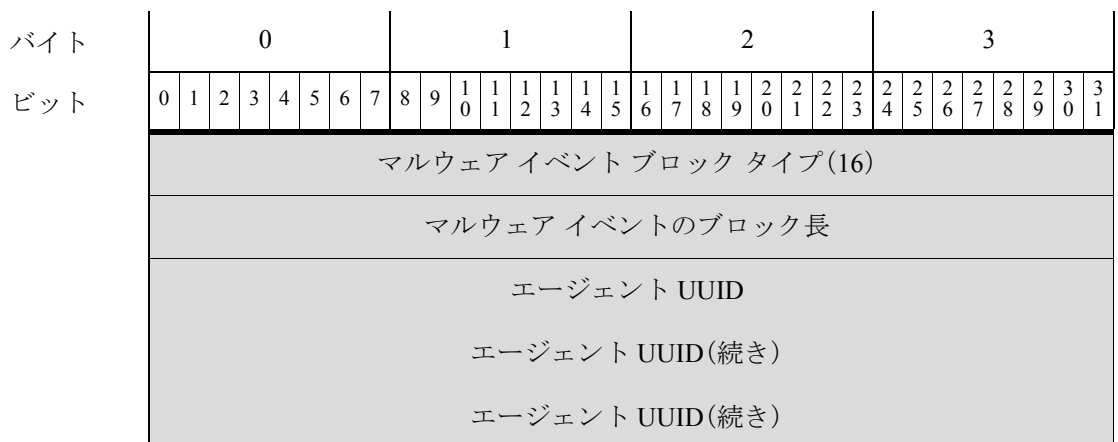
レガシーマルウェアイベントのデータ構造

- [マルウェアイベントのデータブロック 5.1 \(B-51 ページ\)](#)
- [マルウェアイベントデータブロック 5.1.1.x \(B-55 ページ\)](#)
- [マルウェアイベントデータブロック 5.2.x \(B-61 ページ\)](#)
- [マルウェアイベントのデータブロック 5.3 \(B-68 ページ\)](#)
- [マルウェアイベントデータブロック 5.3.1 \(B-76 ページ\)](#)
- [マルウェアイベントデータブロック 5.4.x \(B-83 ページ\)](#)

マルウェアイベントのデータブロック 5.1

eStreamer サービスは、マルウェアイベントに関する情報を保存するために、マルウェアイベントデータブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェアイベントデータブロックのブロックタイプは、シリーズ 2 グループの 16 です。マルウェアイベントレコードの一部としてイベントを要求するには、イベントバージョン 1 およびイベントコード 101 の要求メッセージ内に、マルウェアイベントフラグ (要求フラグフィールドのビット 30) を設定します。

次の図は、マルウェアイベントデータブロックの構造を示しています。



レガシーマルウェアイベントのデータ構造

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	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)																															
	Timestamp																															
	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 (User)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル名...																															
ファイルパス	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイルパス...																															
ファイル SHA ハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイルサイズ (File size)																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ファイルタイプ								ファイルのタイムスタンプ																							
親ファイル [名前(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...																															

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-9 マルウェア イベント データ ブロックのフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 16 です。
マルウェア イベント のブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数 (マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする 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。

表 B-9 マルウェアイベントデータブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロックタイプ	uint32	検出名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	検出名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロックタイプ	uint32	ユーザ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびユーザフィールドのバイト数を含む)。
ユーザ (User)	string	シスコ Agent がインストールされ、マルウェアイベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリー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。

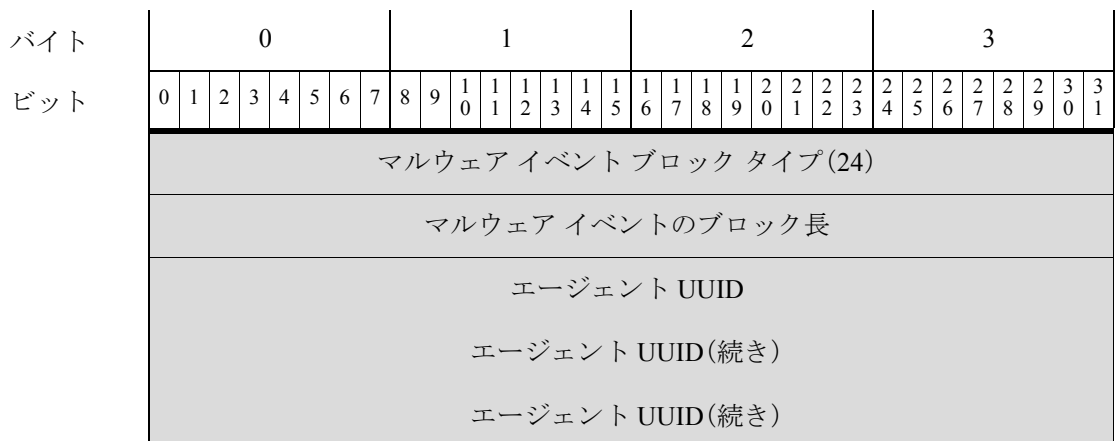
表 B-9 マルウェアイベントデータブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	親ファイル名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロックタイプ	uint32	親ファイルSHAハッシュを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	親ファイルSHAハッシュ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、および親ファイルSHAハッシュフィールドのバイト数を含む)。
親ファイルSHAハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルのSHA-256のハッシュ値。
文字列ブロックタイプ	uint32	イベントの説明を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	イベントの説明文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベントタイプに関連付けられている追加イベント情報。

マルウェアイベントデータブロック 5.1.1.x

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

次の図は、マルウェアイベントデータブロックの構造を示しています。



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

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-10 マルウェア イベント データ ブロック 5.1.1.x のフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 24 です。
マルウェア イベントのブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする 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-10 マルウェアイベントデータブロック 5.1.1.x のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	検出名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロックタイプ	uint32	ユーザ名を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ユーザ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびユーザフィールドのバイト数を含む)。
ユーザ(User)	string	シスコ Agent がインストールされ、マルウェアイベントが発生したコンピュータのユーザ。これらのユーザはユーザディスカバリには関係ないことに注意してください。
文字列ブロックタイプ	uint32	ファイル名を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ファイル名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロックタイプ	uint32	ファイルパスを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ファイルパス文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびファイルパスフィールドのバイト数を含む)。
ファイルパス	string	検出または検疫されたファイルのファイルパス。ファイル名は含まれません。
文字列ブロックタイプ	uint32	ファイル SHA ハッシュを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびファイル SHA ハッシュフィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値のレンダリングされた文字列。
ファイルサイズ (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-10 マルウェアイベントデータブロック 5.1.1.x のフィールド(続き)

フィールド	データタイプ	説明
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。 <ul style="list-style-type: none"> 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 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の ID 番号。

表 B-10 マルウェアイベントデータブロック 5.1.1.x のフィールド(続き)

フィールド	データタイプ	説明
ア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。 <ul style="list-style-type: none"> • 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):ソフトウェアはシスコ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):シスコクラウドサービスが要求に応答しませんでした。
レトロスペクティブ特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロックタイプ	uint32	URI を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。

マルウェアイベントデータブロック 5.2.x

eStreamer サービスは、マルウェアイベントに関する情報を保存するために、マルウェアイベントデータブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェアイベントデータブロックのブロックタイプは、シリーズ 2 グループの 33 です。マルウェアイベントレコードの一部として、イベントバージョン 3 およびイベントコード 101 の要求メッセージ内にマルウェアイベントフラグ(要求フラグフィールドのビット 30)を設定して、イベントを要求します。

次の図は、マルウェアイベントデータブロックの構造を示しています。

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

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイル SHA ハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイル サイズ (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									
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	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 ID(User ID)																							
	ユーザ ID(続き)								アクセスコントロールポリシー UUID																							
	アクセスコントロールポリシー UUID(続き)																															
	アクセスコントロールポリシー UUID(続き)																															
	アクセスコントロールポリシー UUID(続き)																															
URI	アクセスコントロールポリシー UUID(続き)								傾向							レトロスペクティブ傾向							文字列ブロックタイプ(0)									
	文字列ブロックタイプ(0)(続き)															文字列ブロック長																
	文字列ブロック長(続き)															URI...																
	送信元ポート(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-11 マルウェアイベントデータブロック 5.2.x のフィールド

フィールド	データタイプ	説明
マルウェアイベントブロックタイプ	uint32	マルウェアイベントデータブロックを開始します。この値は常に 33 です。
マルウェアイベントのブロック長	uint32	マルウェアイベントデータブロックのバイトの合計数(マルウェアイベントブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。

表 B-11 マルウェアイベントデータブロック 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
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	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびユーザフィールドのバイト数を含む)。
ユーザ (User)	string	シスコ Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイルパスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイルパス文字列データ ブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびファイルパスフィールドのバイト数を含む)。
ファイルパス	string	検出または検疫されたファイルのファイルパス。ファイル名は含まれません。
文字列ブロック タイプ	uint32	ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-11 マルウェアイベントデータブロック 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	ファイル 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。
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。

表 B-11 マルウェアイベントデータブロック 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
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。 <ul style="list-style-type: none"> 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 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。 <ul style="list-style-type: none"> 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):ソフトウェアからシスコクラウドに対して、特性を確認する要求を送信できなかったか、またはシスコ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。
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。

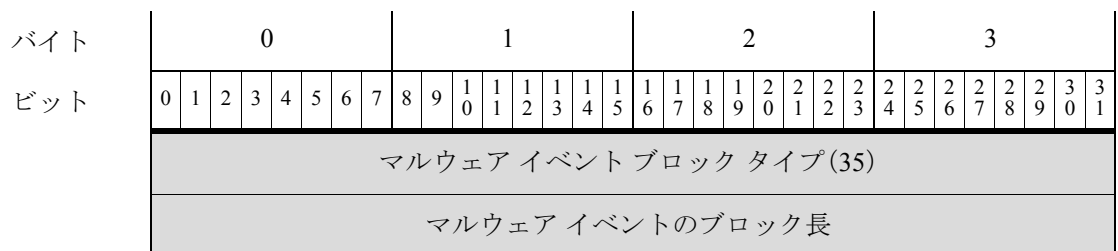
表 B-11 マルウェアイベントデータブロック 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
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。 <ul style="list-style-type: none"> • 1:検出 • 2:ブロック • 3:マルウェアクラウドルックアップ • 4:マルウェアブロック • 5:マルウェアホワイトリスト
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。

マルウェアイベントのデータブロック 5.3

eStreamer サービスは、マルウェアイベントに関する情報を保存するために、マルウェアイベントデータブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェアイベントデータブロックのブロックタイプは、シリーズ 2 グループの 35 です。マルウェアイベントレコードの一部として、イベントバージョン 4 およびイベントコード 101 の要求メッセージ内にマルウェアイベントフラグ(要求フラグフィールドのビット 30)を設定して、イベントを要求します。

次の図は、マルウェアイベントデータブロックの構造を示しています。



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

バイト	0								1							2							3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
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...																														
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							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット	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 ID (User ID)																							
	ユーザ ID(続き)								アクセス コントロール ポリシー UUID																							
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
URI	アクセス コントロール ポリシー UUID(続き)								傾向								レトロスペクティブ傾向								文字列ブロックタイプ(0)							
	文字列ブロックタイプ(0)(続き)																文字列ブロック長															
	文字列ブロック長(続き)																URI...															
	送信元ポート (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-12 マルウェア イベント データ ブロック 5.3 のフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 35 です。
マルウェア イベントのブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする 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	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ フィールドのバイト数を含む)。
ユーザ (User)	string	シスコ Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリーには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイルパスを含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-12 マルウェアイベントデータブロック 5.3 のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	ファイルパス文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびファイルパスフィールドのバイト数を含む)。
ファイルパス	string	検出または検疫されたファイルのファイルパス。ファイル名は含まれません。
文字列ブロックタイプ	uint32	ファイルSHAハッシュを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ファイルSHAハッシュ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびファイルSHAハッシュフィールドのバイト数を含む)。
ファイルSHAハッシュ	string	検出または検疫されたファイルのSHA-256ハッシュ値のレンダリングされた文字列。
ファイルサイズ (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(3-43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)。

表 B-12 マルウェアイベントデータブロック 5.3 のフィールド(続き)

フィールド	データタイプ	説明
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	<p>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。</p> <ul style="list-style-type: none"> 1:ダウンロード 2:アップロード <p>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)。</p>
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 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	<p>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。</p> <ul style="list-style-type: none"> 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):ソフトウェアからシスコクラウドに対して、特性を確認する要求を送信できなかったか、またはシスコクラウドサービスが要求に応答しませんでした。 5(CUSTOM SIGNATURE):ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。

表 B-12 マルウェアイベントデータブロック 5.3 のフィールド(続き)

フィールド	データタイプ	説明
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。 <ul style="list-style-type: none"> • 1:検出 • 2:ブロック • 3:マルウェアクラウドルックアップ • 4:マルウェアブロック • 5:マルウェアホワイトリスト
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ~ 100)。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。

マルウェア イベント データ ブロック 5.3.1

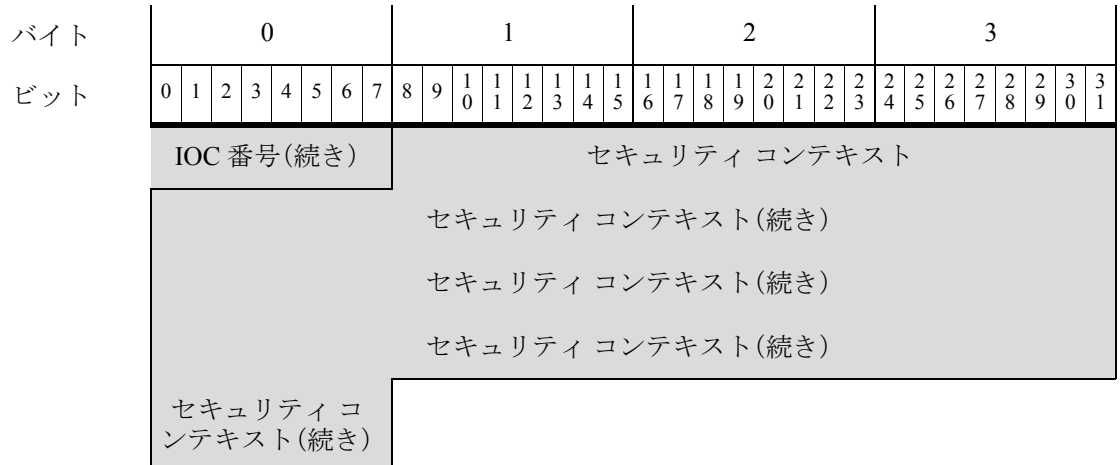
eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 44 です。これはブロック 35 に取って代わります。マルウェア イベント レコードの一部として、イベントバージョン 5 およびイベント コード 101 の要求メッセージ内にマルウェア イベント フラグ(要求フラグ フィールドのビット 30)を設定して、イベントを要求します。

次の図は、マルウェア イベント データ ブロックの構造を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	マルウェア イベント ブロック タイプ (44)																															
	マルウェア イベントのブロック長																															
	エージェント UUID																															
	エージェント UUID (続き)																															
	エージェント UUID (続き)																															
	エージェント UUID (続き)																															
	クラウド UUID																															
	クラウド UUID (続き)																															
	クラウド UUID (続き)																															
	クラウド UUID (続き)																															
	マルウェア イベント タイムスタンプ																															
	イベント タイプ ID																															
	イベント サブタイプ ID																															
検出名	ディテクタ ID								文字列ブロック タイプ (0)																							
	文字列ブロック タイプ (0) (続き)								文字列ブロック長																							
	文字列ブロック長 (続き)								検出名...																							

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	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 (User)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル名...																															
ファイルパス	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイルパス...																															
ファイル SHA ハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイル サイズ (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)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	接続インスタンス																接続数カウンタ															
	接続イベント 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)																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 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 ID (User ID)																							
	ユーザ ID (続き)								アクセス コントロール ポリシー UUID																							
	アクセス コントロール ポリシー UUID (続き)																アクセス コントロール ポリシー UUID (続き)															
	アクセス コントロール ポリシー UUID (続き)																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								



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 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	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ フィールドのバイト数を含む)。

表 B-13 マルウェアイベントデータブロック 5.3.1 のフィールド(続き)

フィールド	データタイプ	説明
ユーザ (User)	string	シスコ Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリー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 (3-43 ページ) を参照してください。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ (1970 年 1 月 1 日からの経過秒数)。
文字列ブロックタイプ	uint32	親ファイル名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル名文字列データブロックに含まれるバイト数 (ブロックタイプとヘッダーフィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロックタイプ	uint32	親ファイル SHA ハッシュを含む文字列データブロックを開始します。この値は常に 0 です。

表 B-13 マルウェアイベントデータブロック 5.3.1 のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および親ファイル SHA ハッシュフィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロックタイプ	uint32	イベントの説明を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベントタイプに関連付けられている追加イベント情報。
デバイス ID(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。 <ul style="list-style-type: none"> • 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 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の ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	イベントをトリガーしたアクセスコントロールポリシーの固有識別子として機能する ID 番号。

表 B-13 マルウェアイベントデータブロック 5.3.1 のフィールド(続き)

フィールド	データタイプ	説明
傾向	uint8	<p>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。</p> <ul style="list-style-type: none"> 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): ソフトウェアからシスコクラウドに対して、特性を確認する要求を送信できなかったか、またはシスコクラウドサービスが要求に応答しませんでした。 5(CUSTOM SIGNATURE): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
レトロスペクティブ特性	uint8	<p>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。</p>
文字列ブロックタイプ	uint32	<p>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。</p>
文字列ブロック長	uint32	<p>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)。</p>
URI	string	<p>接続のURI。</p>
送信元ポート	uint16	<p>接続の送信元のポート番号。</p>
接続先ポート	uint16	<p>接続の宛先のポート番号。</p>
送信元の国	uint16	<p>送信元ホストの国のコード。</p>
宛先の国	uint16	<p>宛先ホストの国のコード。</p>
WebアプリケーションID	uint32	<p>専用Webアプリケーションの内部ID番号(該当する場合)。</p>
クライアントアプリケーションID	uint32	<p>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)。</p>
操作	uint8	<p>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。</p> <ul style="list-style-type: none"> 1: 検出 2: ブロック 3: マルウェアクラウドルックアップ 4: マルウェアブロック 5: マルウェアホワイトリスト

表 B-13 マルウェア イベント データ ブロック 5.3.1 のフィールド(続き)

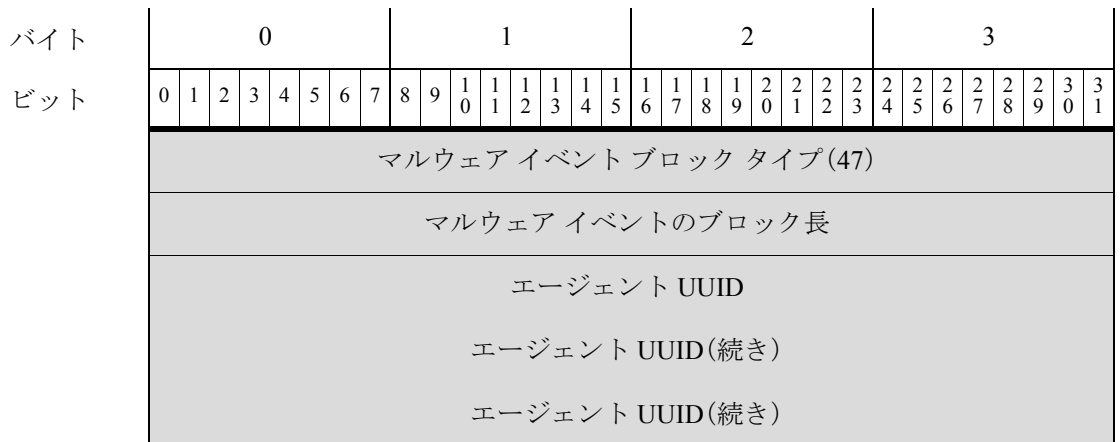
フィールド	データタイプ	説明
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ~ 100)。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト (仮想ファイアウォール) の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

マルウェア イベント データ ブロック 5.4.x

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

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

次の図は、マルウェア イベント データ ブロックの構造を示しています。



レガシーマルウェアイベントのデータ構造

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	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 (User)	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイル名...																															
ファイルパス	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイルパス...																															
ファイル SHA ハッシュ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイルサイズ (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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ファイル タイプ																															
	ファイルのタイムスタンプ																															
親ファイル [名前(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 ID(User ID)																															
ユーザ ID(続き)	アクセス コントロール ポリシー UUID																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	アクセスコントロールポリシー UUID(続き)																															
	アクセスコントロールポリシー UUID(続き)																															
	アクセスコントロールポリシー UUID(続き)																															
URI	アクセスコントロールポリシー UUID(続き)								傾向								レトロスペクティブ傾向								文字列ブロックタイプ(0)							
	文字列ブロックタイプ(0)(続き)																文字列ブロック長															
	文字列ブロック長(続き)																URL...															
	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)																															
	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							

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

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 5.4.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。
文字列ブロック長	uint32	検出名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。

表 B-14 マルウェアイベントデータブロック 5.4.x のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロックタイプ	uint32	ユーザ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびユーザフィールドのバイト数を含む)。
ユーザ (User)	string	シスコ Agent がインストールされ、マルウェアイベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリー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 (3-43 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。

表 B-14 マルウェアイベントデータブロック 5.4.x のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	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。 <ul style="list-style-type: none"> • 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 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の ID 番号。

表 B-14 マルウェアイベントデータブロック 5.4.x のフィールド(続き)

フィールド	データタイプ	説明
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。 <ul style="list-style-type: none"> • 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): ソフトウェアからシスコクラウドに対して、特性を確認する要求を送信できなかったか、またはシスコクラウドサービスが要求に応答しませんでした。 • 5(CUSTOM SIGNATURE): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
レトロスペクティブ特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロックタイプ	uint32	URI を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。

表 B-14 マルウェアイベントデータブロック 5.4.x のフィールド(続き)

フィールド	データタイプ	説明
操作	uint8	<p>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。</p> <ul style="list-style-type: none"> • 1:検出 • 2:ブロック • 3:マルウェアクラウドルックアップ • 4:マルウェアブロック • 5:マルウェアホワイトリスト • 6:クラウドルックアップのタイムアウト • 7:カスタム検出 • 8:カスタム検出ブロック • 9:アーカイブブロック(深度超過) • 10:アーカイブブロック(暗号化されている) • 11:アーカイブブロック(調査エラー)
プロトコル	uint8	<p>ユーザが指定した IANA プロトコル数。次に例を示します。</p> <ul style="list-style-type: none"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP <p>これは現時点では TCP のみです。</p>
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0～100)。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティコンテキスト	uint8(16)	トラフィックが通過したセキュリティコンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキストモードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。

表 B-14 マルウェアイベントデータブロック 5.4.x のフィールド(続き)

フィールド	データタイプ	説明
実際の SSL アクション	uint16	<p>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。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 B-14 マルウェアイベントデータブロック 5.4.x のフィールド(続き)

フィールド	データタイプ	説明
SSL フロー ステータス	uint16	<p>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。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
文字列ブロック タイプ	uint32	<p>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。</p>

表 B-14 マルウェアイベントデータブロック 5.4.x のフィールド(続き)

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

レガシーディスカバリデータ構造

- [レガシーディスカバリ イベントヘッダー \(B-94 ページ\)](#)
- [レガシーサーバデータブロック \(B-96 ページ\)](#)
- [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 \(B-97 ページ\)](#)
- [レガシースキャン結果データブロック \(B-99 ページ\)](#)
- [レガシーホストプロファイルデータブロック \(B-126 ページ\)](#)
- [レガシー OS フィンガープリントデータブロック \(B-133 ページ\)](#)

レガシーディスカバリ イベントヘッダー

ディスカバリ イベントヘッダー 5.0 ~ 5.1.1.x

ディスカバリ イベントおよび接続イベントのメッセージには、ディスカバリ イベントヘッダーが含まれます。これは、イベントのタイプおよびサブタイプ、イベントが発生した時刻、イベントが発生したデバイス、およびメッセージ内のイベントデータの構造を伝えます。このヘッダーには、実際のホストディスカバリ、ユーザ、または接続イベントのデータが続きます。さまざまなイベントのタイプ/サブタイプ値に関連付けられる構造の詳細については、[イベントタイプ別ホストディスカバリ構造 \(4-46 ページ\)](#)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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ															
	レコード長																															
	eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
ディスカバリイベントヘッダー	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-15 ディスカバリ イベントヘッダーのフィールド

フィールド	データ型	説明
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 (3-37 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	uint86	イベントに関連するホストの MAC アドレス。

[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-16 属性アドレス データ ブロックのフィールド

フィールド	データタイプ	説明
属性アドレスブロックタイプ	uint32	属性アドレスブロック データを開始します。この値は常に 38 です。
属性アドレスブロック長	uint32	属性アドレス データ ブロックのバイト数(属性アドレスブロックタイプと長さ用の 8 バイト、およびそれに続く属性アドレスデータのバイト数を含む)。
属性 ID	uint32	影響を受ける属性の ID 番号(該当する場合)。
[IP アドレス (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

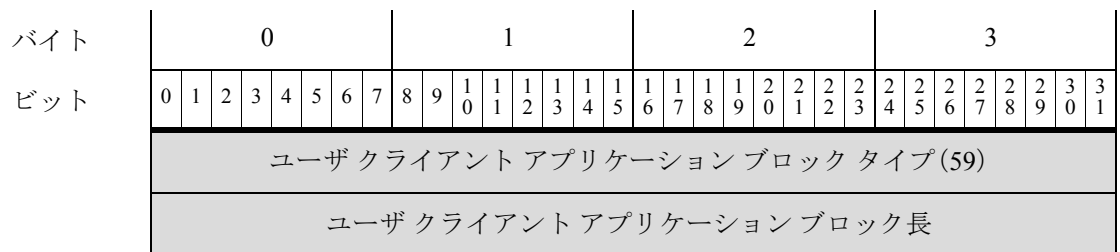
詳細については、次の項を参照してください。

- [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\(B-97 ページ\)](#)

ユーザクライアントアプリケーションデータブロック 5.0 ~ 5.1

ユーザクライアントアプリケーションデータブロックには、クライアントアプリケーションデータの送信元に関する情報、データを追加したユーザの ID 番号、および IP アドレス範囲データブロックのリストが含まれます。ユーザクライアントアプリケーションデータブロックのブロックタイプは 59 です。

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



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

表 B-17 ユーザクライアントアプリケーションデータブロックのフィールド

フィールド	バイト数	説明
ユーザクライアントアプリケーションブロックタイプ	uint32	ユーザクライアントアプリケーションデータブロックを開始します。この値は常に 0 です。
ユーザクライアントアプリケーションブロック長	uint32	ユーザクライアントアプリケーションデータブロックのバイトの合計数(ユーザクライアントアプリケーションブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザクライアントアプリケーションデータのバイト数を含む)。
汎用リストブロックタイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データブロック* で構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべての IP 範囲仕様データブロック* を含む汎用リストデータブロックのバイト数。
IP 範囲仕様データブロック*	変数 (variable)	ユーザ入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データブロック。このデータブロックの説明の詳細については、 表 4-59 ユーザサーバデータブロックのフィールド(4-110 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。

表 B-17 ユーザクライアントアプリケーションデータブロックのフィールド(続き)

フィールド	バイト数	説明
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 \(B-99 ページ\)](#)
- [ユーザ製品データ ブロック 5.0.x \(B-102 ページ\)](#)
- [ユーザ情報データ ブロック 5.x \(B-123 ページ\)](#)

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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	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 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																
	フラグ (Flag)																リストブロック タイプ(11)																脆弱性スキャン リスト
	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...																

レガシーディスカバリデータ構造

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
	リストブロックタイプ(11)																															汎用スキャン 結果リスト	
	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...																																
ユーザ(User) 製品リスト	汎用リストブロックタイプ(31)																																
	汎用リストブロック長																																
	ユーザ製品データブロック*																																

次の表は、スキャン結果データブロックのフィールドについての説明です。

表 B-18 スキャン結果データブロックのフィールド

フィールド	データタイプ	説明
スキャン結果ブロックタイプ	uint32	スキャン結果データブロックを開始します。この値は常に 102 です。
スキャン結果ブロック長	uint32	スキャン脆弱性データブロックのバイト数(接続統計ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン脆弱性データのバイト数を含む)。
ユーザ ID (User ID)	uint32	スキャン結果をインポートしたユーザ、またはスキャン結果を生成したスキャンを実行したユーザのユーザ ID 番号が含まれます。
スキャンタイプ	uint32	結果がシステムに追加された方法を示します。
[IP アドレス (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。 <ul style="list-style-type: none"> 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。

表 B-18 スキャン結果データブロックのフィールド(続き)

フィールド	データタイプ	説明
リストブロック長	uint32	リスト内のバイト数。この数には、リストブロックタイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのスキャン脆弱性データブロックが含まれています。 このフィールドには、ゼロ以上のスキャン脆弱性データブロックが続きます。
スキャン脆弱性ブロックタイプ	uint32	スキャン中に検出された脆弱性を記述するスキャン脆弱性データブロックを開始します。この値は常に 109 です。
スキャン脆弱性ブロック長	uint32	スキャン脆弱性データブロックのバイト数(接続統計ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン脆弱性データのバイト数を含む)。
脆弱性データ	string	各脆弱性に関する情報。
リストブロックタイプ	uint32	トランスポートスキャン脆弱性データを伝えるスキャン脆弱性データブロックで構成されるリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数には、リストブロックタイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのスキャン脆弱性データブロックが含まれています。 このフィールドには、ゼロ以上のスキャン脆弱性データブロックが続きます。
汎用スキャン結果ブロックタイプ	uint32	スキャン中に検出されたサーバおよびオペレーティングシステムを記述する汎用スキャン結果データブロックを開始します。この値は常に 108 です。
汎用スキャン結果ブロック長	uint32	汎用スキャン結果データブロックのバイト数(汎用スキャン結果ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン結果データのバイト数を含む)。
汎用スキャン結果データ	string	各スキャン結果に関する情報。
汎用リストブロックタイプ	uint32	サードパーティアプリケーションからのホスト入力データを伝えるユーザ製品データブロックを構成する、汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのユーザ製品データブロックを含む)。
ユーザ製品データブロック*	変数(variable)	ホスト入力データを含むユーザ製品データブロック。このデータブロックの説明の詳細については、 ユーザ製品データブロック 5.1+(4-180 ページ) を参照してください。

ユーザ製品データ ブロック 5.0.x

ユーザ製品データ ブロックは、サードパーティアプリケーション文字列マッピングを含む、サードパーティアプリケーションからインポートされたホスト入力データを伝えます。このデータブロックは [接続統計データブロック 6.0.x \(B-205 ページ\)](#) と [ユーザ サーバ メッセージとオペレーティング システム メッセージ \(4-60 ページ\)](#) で使用します。ユーザ製品データ ブロックは、4.10.x の場合はブロック タイプ 65、5.0 ~ 5.0.x の場合はブロック タイプ 118 です。それぞれのブロック タイプは同じ構造を持ちます。



コメント

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

次の図は、ユーザ製品データ ブロックの形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ製品データ ブロック タイプ (65 118)																															
	ユーザ製品ブロック長																															
	ソース																															
	ソース タイプ																															
[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...																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
カスタム (Custom) バージョン 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	カスタム バージョン文字列...																															
	ソフトウェア ID																															
	サーバ ID																															
	ベンダー ID																															
	製品 ID																															
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...																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビルド文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ビルド文字列...																															
パッチ文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	パッチ文字列...																															
内線番号 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	拡張文字列...																															
OS UUID	オペレーティング システム UUID																															
	オペレーティング システム UUID(続き)																															
	オペレーティング システム UUID(続き)																															
	オペレーティング システム UUID(続き)																															
修正のリスト	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	修正リストデータブロック*																															

次の表では、ユーザ製品データブロックのコンポーネントについて説明します。

表 B-19 ユーザ製品データブロック 4.10.x、5.0 ~ 5.0.x のフィールド

フィールド	データタイプ	説明
ユーザ製品データブロックタイプ	uint32	ユーザ製品データブロックを開始します。この値はバージョン 4.10.x の場合は 65、バージョン 5.0 ~ 5.0.x の場合は 118 です。
ユーザ製品ブロック長	uint32	ユーザ製品データブロックのバイトの合計数(ユーザ製品ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ製品データのバイト数を含む)。
ソース	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。

表 B-19 ユーザ製品データブロック 4.10.x, 5.0 ~ 5.0.x のフィールド(続き)

フィールド	データタイプ	説明
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	ユーザが指定するポート。
プロトコル	uint16	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP
ドロップ ユーザ製品	uint32	ユーザ OS 定義がホストから削除されたかどうかを示します。 <ul style="list-style-type: none"> • 0:いいえ • 1:はい
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタムベンダー名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタムベンダー文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびベンダー名のバイト数を含む)。
カスタムベンダー名	string	ユーザ入力に指定されたカスタムベンダー名。
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタム製品名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタム製品文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および製品名のバイト数を含む)。
カスタム製品名	string	ユーザ入力に指定されたカスタム製品名。
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタムバージョンを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタムバージョン文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
カスタムバージョン	string	ユーザ入力に指定されたカスタムバージョン。
ソフトウェア ID	uint32	シスコデータベースの特定のレビジョンのサーバまたはオペレーティングシステムの ID。

表 B-19 ユーザ製品データブロック 4.10.x、5.0 ~ 5.0.x のフィールド(続き)

フィールド	データタイプ	説明
サーバ ID	uint32	ユーザ入力に指定したホストサーバのアプリケーションプロトコルのシスコ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シスコ 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シスコ 3D オペレーティングシステム定義にマップされるときに指定される、サードパーティオペレーティングシステム文字列の製品 ID 文字列。
文字列ブロックタイプ	uint32	ユーザ入力内のサードパーティオペレーティングシステム文字列がマップされるシスコ 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シスコ 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シスコ 3D オペレーティングシステム定義のマイナーバージョン番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	マイナー文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
マイナーバージョン	string	ユーザ入力内のサードパーティオペレーティングシステム文字列がマップされるシスコ 3D オペレーティングシステム定義のマイナーバージョン。
文字列ブロックタイプ	uint32	ユーザ入力内のサードパーティオペレーティングシステム文字列がマップされるシスコ 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シスコ 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シスコ 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。

表 B-19 ユーザ製品データブロック 4.10.x, 5.0 ~ 5.0.x のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトにバージョンのバイト数を加えた移行先メジャー文字列データブロックのバイト数。
移行先メジャー	string	ユーザ入力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シスコ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シスコ3Dオペレーティングシステム定義の最終マイナーバージョン番号を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトにバージョンのバイト数を加えたマイナー用文字列データブロックのバイト数。
マイナー用	string	ユーザ入力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シスコ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シスコ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りビジョン用文字列データブロックのバイト数。
リビジョン用	string	ユーザ入力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シスコ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シスコ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シスコ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シスコ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)。

表 B-19 ユーザ製品データブロック 4.10.x、5.0 ~ 5.0.x のフィールド(続き)

フィールド	データタイプ	説明
パッチ	string	ユーザ入力内のサードパーティオペレーティングシステム文字列がマップされる シスコ 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 シスコ 3D オペレーティング システムの拡張番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	拡張文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および拡張番号のバイト数を含む)。
内線番号	string	ユーザ入力内のサードパーティオペレーティングシステム文字列がマップされる シスコ 3D オペレーティング システムの拡張番号。
UUID	uint8 [x16]	オペレーティングシステム用の固有 ID 番号が含まれます。
汎用リストブロックタイプ	uint32	どの修正が特定の IP アドレス範囲内のホストに適用されているかに関するユーザ入力データを伝える修正リストデータブロックで構成される、汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべての修正リストデータブロックを含む)。
修正リストデータブロック*	変数(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(4-109 ページ) を参照してください。

レガシーユーザログインデータブロック

詳細については、次の各項を参照してください。

- [ユーザログイン情報データブロック 5.0 ~ 5.0.2\(B-108 ページ\)](#)
- [ユーザログイン情報データブロック 5.1 ~ 5.4.x\(B-110 ページ\)](#)
- [ユーザログイン情報データブロック 6.0.x\(B-112 ページ\)](#)
- [ユーザログイン情報データブロック 6.1.x\(B-116 ページ\)](#)
- [ユーザ情報データブロック 5.x\(B-123 ページ\)](#)

ユーザログイン情報データブロック 5.0 ~ 5.0.2

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

ユーザログイン情報データブロックは、バージョン 5.0 ~ 5.0.2 の場合は、ブロックタイプ 121 です。

次の図は、ユーザログイン情報データブロックの形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ ログイン情報ブロック タイプ (121)																															
	ユーザ ログイン情報ブロック長																															
	Timestamp																															
	[IP アドレス (IP Address)]																															
ユーザ (User) [名前 (Name)]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザ名...																															
	ユーザ 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 ログイン情報データ ブロックのコンポーネントについての説明です。

表 B-20 ユーザ ログイン情報データ ブロック 5.0 ~ 5.0.2 のフィールド

フィールド	データタイプ	説明
ユーザ ログイン情報ブロック タイプ	uint32	ユーザ ログイン情報データ ブロックを開始します。この値は、バージョン 5.0 ~ 5.0.2 の場合は 121 です。
ユーザ ログイン情報ブロック長	uint32	ユーザ ログイン情報データ ブロックのバイトの合計数(ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ ログイン情報データのバイト数を含む)。
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、ユーザのログインが検出されたホストからの IP アドレス。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。

表 B-20 ユーザログイン情報データブロック 5.0 ~ 5.0.2 のフィールド(続き)

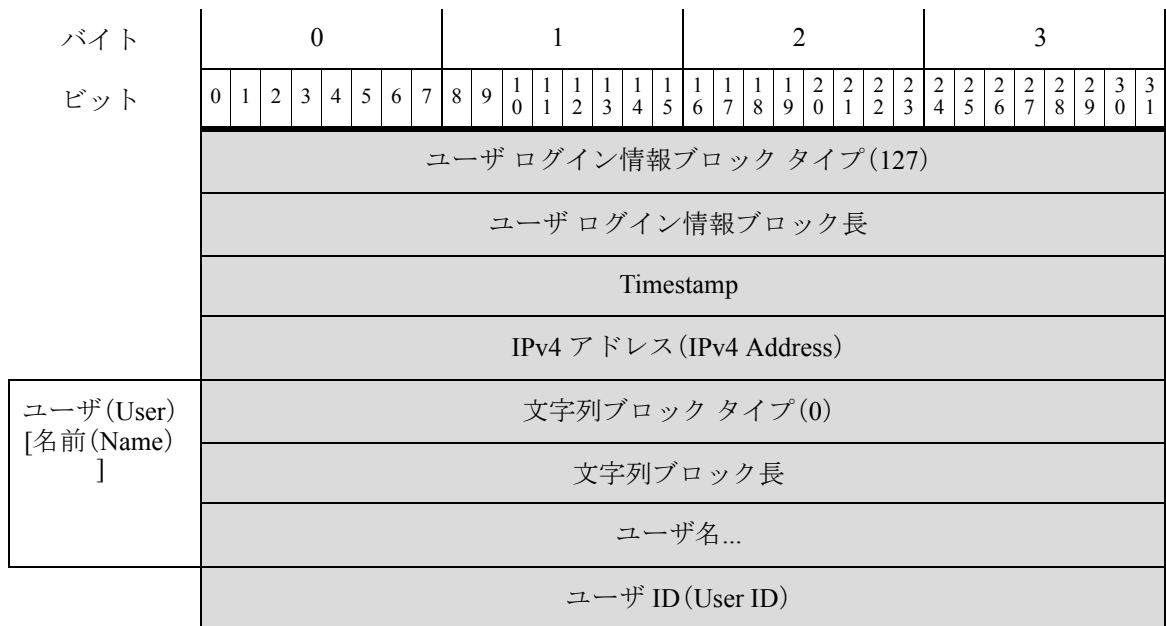
フィールド	データタイプ	説明
[ユーザ名 (Username)]	string	ユーザのユーザ名。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。
アプリケーション ID (Application ID)	uint32	ログイン情報の取得元の、接続に使用されたアプリケーションプロトコルのアプリケーション ID。
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。

ユーザログイン情報データブロック 5.1 ~ 5.4.x

ユーザログイン情報データブロックは、ユーザ情報更新メッセージで使用され、検出されたユーザのログイン情報の変更を伝えます。詳細については、[ユーザアカウント更新メッセージデータブロック \(4-189 ページ\)](#) を参照してください。

ユーザログイン情報データブロックは、バージョン 4.7 ~ 4.10.x の場合はブロックタイプ 73、バージョン 5.0 ~ 5.0.2 の場合はシリーズ 1 グループのブロックのブロックタイプ 121、バージョン 5.1 ~ 5.4.x の場合はシリーズ 1 グループのブロックのブロックタイプ 127 です。

次の図は、ユーザログイン情報データブロックの形式を示しています。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	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																															
	IPv6 アドレス(続き)																															
	IPv6 アドレス(続き)																															
	IPv6 アドレス(続き)																															
レポート基準	ログインタイプ	文字列ブロック タイプ(0)																														
	文字列ブロックタイプ(0)(続き)	文字列ブロック長																														
	文字列ブロック長	レポート基準...																														

次の表は、ユーザ ログイン情報データ ブロックのコンポーネントについての説明です。

表 B-21 ユーザ ログイン情報データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザ ログイン情報ブロックタイプ	uint32	ユーザ ログイン情報データ ブロックを開始します。この値は、バージョン 5.1+ の場合は 127 です。
ユーザ ログイン情報ブロック長	uint32	ユーザ ログイン情報データ ブロックのバイトの合計数 (ユーザ ログイン情報ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ ログイン情報データのバイト数を含む)。
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せん。詳細については、 IP アドレス (1-5 ページ) を参照してください。
文字列ブロックタイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。

表 B-21 ユーザログイン情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
[ユーザ名 (Username)]	string	ユーザのユーザ名。
ユーザ ID (User ID)	uint32	ユーザの 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	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IPv6 アドレス。
ログインタイプ	uint8	検出されたユーザログインのタイプ。
文字列ブロックタイプ	uint32	レポート基準値を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	レポート基準文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびレポート基準フィールドのバイト数を含む)。
レポート基準	string	ログインをレポートする Active Directory サーバの名前。

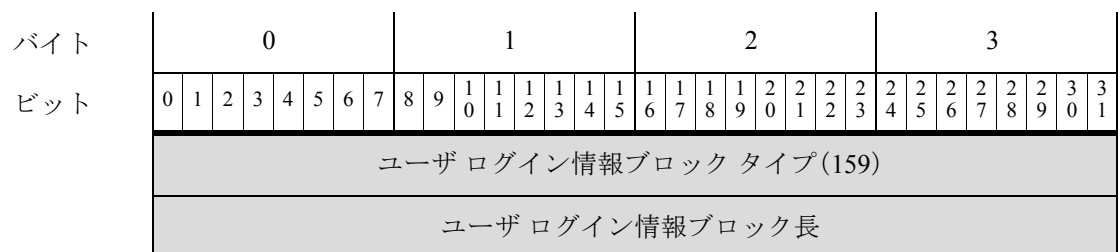
ユーザログイン情報データブロック 6.0.x

ユーザログイン情報データブロックは、ユーザ情報更新メッセージで使用され、検出されたユーザのログイン情報の変更を伝えます。詳細については、[ユーザアカウント更新メッセージデータブロック \(4-189 ページ\)](#)を参照してください。

ユーザログイン情報データブロックは、バージョン 6.0.x の場合は、ブロックタイプ 159 です。これには新しい ISE 統合エンドポイントプロファイル、セキュリティインテリジェンスのフィールドがあります。

ユーザログイン情報データブロックは、バージョン 4.7 ~ 4.10.x の場合はブロックタイプ 73、バージョン 5.0 ~ 5.0.2 の場合はシリーズ 1 グループのブロックのブロックタイプ 121、バージョン 5.1+ の場合はシリーズ 1 グループのブロックのデータタイプ 127 です。詳細については、[ユーザログイン情報データブロック 5.1 ~ 5.4.x \(B-110 ページ\)](#)を参照してください。

次の図は、ユーザログイン情報データブロックの形式を示しています。



バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	Timestamp																															
	IPv4 アドレス (IPv4 Address)																															
ユーザ (User) [名前 (Name)]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザ名...																															
ドメイン	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ドメイン...																															
	ユーザ ID (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							
	0	1	2	3	4	5	6	7	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 ログイン情報データ ブロックのコンポーネントについての説明です。

表 B-22 ユーザ ログイン情報データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザ ログイン情報ブロック タイプ	uint32	ユーザ ログイン情報データ ブロックを開始します。この値は、バージョン 6.0.x の場合は 159 です。
ユーザ ログイン情報ブロック長	uint32	ユーザ ログイン情報データ ブロックのバイトの合計数 (ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ ログイン情報データのバイト数を含む)。
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 (1-5 ページ) を参照してください。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数 (ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
文字列ブロック タイプ	uint32	ドメインを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにドメインのバイト数を加えたユーザ名文字列データ ブロックのバイト数。
ドメイン	string	ユーザがログインしているドメイン。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。
レルム ID	uint32	アイデンティティ レルムに対応する整数 ID。
エンドポイントプロファイル ID	uint32	接続エンドポイントが使用するデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。

表 B-22 ユーザログイン情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
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。 <ul style="list-style-type: none"> • 165:FTP • 426:SIP • 547:AOL Instant Messenger • 683:IMAP • 710:LDAP • 767:NTP • 773:Oracle データベース • 788:POP3 • 1755:MDNS
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IPv6 アドレス。
ロケーション IPv6 アドレス	uint8[16]	ユーザがログインした最新の IP アドレス。IPv4 または IPv6 のどちらかのアドレスになります。
ログインタイプ	uint8	検出されたユーザログインのタイプ。
認証タイプ (Authentication Type)	uint8	ユーザが使用する認証のタイプ。値は次のとおりです。 <ul style="list-style-type: none"> • 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 サーバの名前。

ユーザ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、[ユーザログイン情報データブロック 6.0.x \(B-112 ページ\)](#) を参照してください。これはブロックタイプ 167 に更新しました。

次の図は、ユーザログイン情報データブロックの形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザログイン情報ブロックタイプ(165)																															
	ユーザログイン情報ブロック長																															
	Timestamp																															
	IPv4 アドレス (IPv4 Address)																															
ユーザ (User) [名前 (Name)]	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	ユーザ名...																															
ドメイン	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	ドメイン...																															
	ユーザ ID (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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IPv6 アドレス																															
	IPv6 アドレス(続き)																															
	IPv6 アドレス(続き)																															
	IPv6 アドレス(続き)																															
	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 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-23 ユーザ ログイン情報データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザ ログイン情報ブロック タイプ	uint32	ユーザ ログイン情報データ ブロックを開始します。バージョン 6.1+ の場合、この値は 165 です。
ユーザ ログイン情報ブロック長	uint32	ユーザ ログイン情報データ ブロックのバイトの合計数 (ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ ログイン情報データのバイト数を含む)。
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せん。詳細については、 IP アドレス (1-5 ページ) を参照してください。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。

表 B-23 ユーザログイン情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
[ユーザ名 (Username)]	string	ユーザのユーザ名。
文字列ブロックタイプ	uint32	ドメインを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにドメインのバイト数を加えたユーザ名文字列データブロックのバイト数。
ドメイン	string	ユーザがログインしているドメイン。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。
レルム ID	uint32	アイデンティティレルムに対応する整数 ID。
エンドポイントプロファイル ID	uint32	接続エンドポイントが使用するデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
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。 <ul style="list-style-type: none"> • 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	ユーザを検出したポート番号。
範囲の開始	uint16	TS エージェントが使用するポート範囲の開始ポート
開始ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の開始ポート。
終了ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の最終ポート。
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。

表 B-23 ユーザログイン情報データブロックのフィールド(続き)

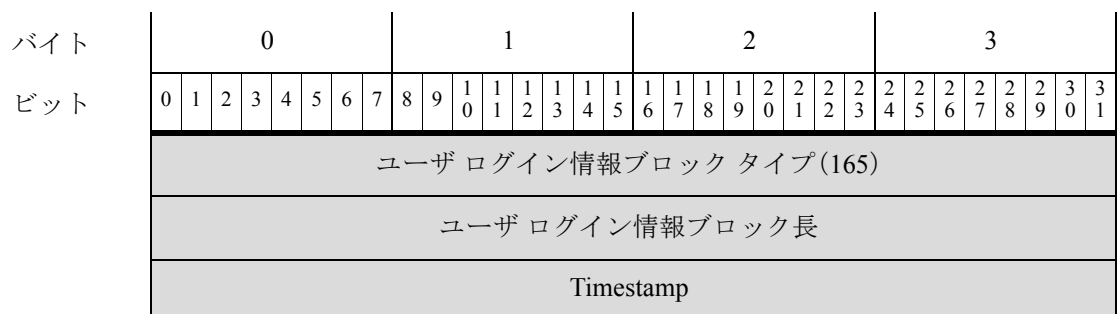
フィールド	データタイプ	説明
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IPv6 アドレス。
ロケーション IPv6 アドレス	uint8[16]	ユーザがログインした最新の IP アドレス。IPv4 または IPv6 のどちらかのアドレスになります。
ログインタイプ	uint8	検出されたユーザ ログインのタイプ。
認証タイプ (Authentication Type)	uint8	ユーザが使用する認証のタイプ。値は次のとおりです。 <ul style="list-style-type: none"> 0: 認証は不要 1: 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 サーバの名前。

ユーザログイン情報データブロック 6.1.x

ユーザログイン情報データブロックは、ユーザ情報更新メッセージで使用され、検出されたユーザのログイン情報の変更を伝えます。詳細については、[ユーザ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、[ユーザログイン情報データブロック 6.0.x \(B-112 ページ\)](#)を参照してください。

次の図は、ユーザログイン情報データブロックの形式を示しています。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IPv4 アドレス (IPv4 Address)																															
ユーザ (User) [名前 (Name)]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザ名...																															
ドメイン	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ドメイン...																															
	ユーザ ID (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							
	0	1	2	3	4	5	6	7	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-24 ユーザログイン情報データブロックのフィールド

フィールド	データタイプ	説明
ユーザログイン情報ブロックタイプ	uint32	ユーザログイン情報データブロックを開始します。バージョン 6.2+ の場合、この値は 165 です。
ユーザログイン情報ブロック長	uint32	ユーザログイン情報データブロックのバイトの合計数 (ユーザログイン情報ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザログイン情報データのバイト数を含む)。
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せん。詳細については、 IP アドレス (1-5 ページ) を参照してください。
文字列ブロックタイプ	uint32	ユーザのユーザ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データブロックのバイト数 (ブロックタイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
文字列ブロックタイプ	uint32	ドメインを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにドメインのバイト数を加えたユーザ名文字列データブロックのバイト数。
ドメイン	string	ユーザがログインしているドメイン。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。

表 B-24 ユーザログイン情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
レルム ID	uint32	アイデンティティレルムに対応する整数 ID。
エンドポイントプロファイル ID	uint32	接続エンドポイントが使用するデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
セキュリティグループ ID	uint32	ネットワークトラフィックグループの ID 番号。
プロトコル	uint32	ユーザの検出やレポートに使用するプロトコル。値は以下のとおりです。 <ul style="list-style-type: none"> • 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	ユーザを検出したポート番号。
範囲の開始	uint16	TS エージェントが使用するポート範囲の開始ポート
開始ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の開始ポート。
終了ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の最終ポート。
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IPv6 アドレス。
ロケーション IPv6 アドレス	uint8[16]	ユーザがログインした最新の IP アドレス。IPv4 または IPv6 のどちらかのアドレスになります。
ログインタイプ	uint8	検出されたユーザログインのタイプ。

表 B-24 ユーザログイン情報データブロックのフィールド(続き)

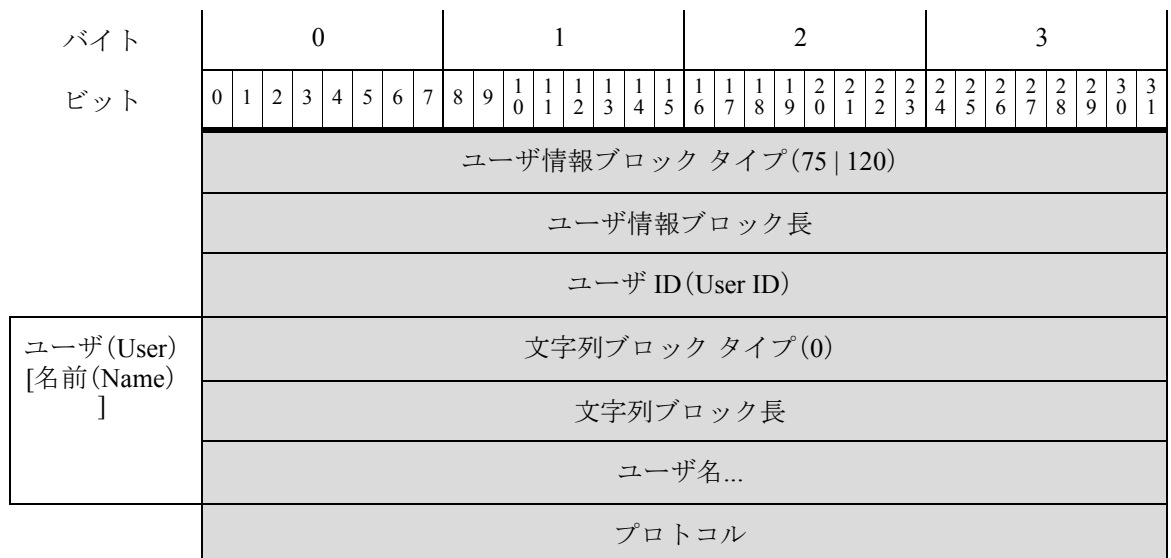
フィールド	データタイプ	説明
認証タイプ (Authentication Type)	uint8	ユーザが使用する認証のタイプ。値は次のとおりです。 <ul style="list-style-type: none"> 0: 認証は不要 1: パッシブ認証、AD エージェント、または ISE セッション 2: キャプティブ ポータルの正常な認証 3: キャプティブ ポータルのゲスト認証 4: キャプティブ ポータルの失敗認証
文字列ブロックタイプ	uint32	レポート基準値を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	レポート基準文字列デ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 サーバの名前。

ユーザ情報データブロック 5.x

ユーザ情報データブロックはユーザ変更メッセージで使用され、検出、削除、またはドロップされたユーザの情報を伝えます。詳細については、[ユーザ変更メッセージ\(4-64 ページ\)](#)を参照してください。

ユーザ情報データブロックのブロックタイプは、4.7 ~ 4.10.x のシリーズ 1 ブロックグループのブロックタイプ 75 と、5.x のシリーズ 1 ブロックグループのブロックタイプ 120 です。構成は、ブロックタイプ 75 と 120 で同じです。

次の図は、ユーザ情報データブロックの形式を示しています。



バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	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 ユーザ情報データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザ情報ブロックタイプ	uint32	ユーザ情報データ ブロックを開始します。この値は、バージョン 4.7 ~ 4.10.x の場合は 75、5.0 以降の場合は 120 です。
ユーザ情報ブロック長	uint32	ユーザ情報データ ブロックのバイトの合計数(ユーザ ログイン情報ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ情報データのバイト数を含む)。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。
文字列ブロックタイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-25 ユーザ情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	ユーザ名文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
プロトコル	uint32	ユーザ情報を含むパケットのプロトコル。
文字列ブロックタイプ	uint32	ユーザの名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および名のバイト数を含む)。
名	string	ユーザの名前。
文字列ブロックタイプ	uint32	ユーザの姓を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	姓文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および姓のバイト数を含む)。
姓	string	ユーザの姓。
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。
文字列ブロックタイプ	uint32	ユーザの部署を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	部署文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および部署のバイト数を含む)。
部署名 (Department)	string	ユーザの部署名。
文字列ブロックタイプ	uint32	ユーザの電話番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電話番号のバイト数を加えた電話番号文字列データブロックのバイト数。
電話	string	ユーザの電話番号。

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 \(B-126 ページ\)](#)

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。



コメント

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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	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)]																																							
サーバフィンガープリント	ホップ								プライマリ/セカンダリ								汎用リストブロックタイプ(31)																							
	汎用リストブロックタイプ(続き)																汎用リストブロック長																							
	汎用リストブロック長(続き)																サーバフィンガープリントデータブロック*																							
クライアントフィンガープリント	汎用リストブロックタイプ(31)																																							
	汎用リストブロック長																																							
	クライアントフィンガープリントデータブロック*																																							
SMBフィンガープリント	汎用リストブロックタイプ(31)																																							
	汎用リストブロック長																																							
	SMBフィンガープリントデータブロック*																																							

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
DHCP フィンガー プリント	汎用リストブロックタイプ(31)																																
	汎用リストブロック長																																
	DHCP フィンガープリント データブロック*																																
TCP サーバ ブロック*	リストブロックタイプ(11)																																TCP サーバ のリスト
	リストブロック長																																
	サーバブロックタイプ(36)																																
TCP サーバ ブロック*	サーバブロック長																																
	TCP サーバ データ...																																
	リストブロックタイプ(11)																																UDP サーバ のリスト
リストブロック長																																	
サーバブロックタイプ(36)*																																	
UDP サーバ ブロック*	サーバブロック長																																
	UDP サーバ 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																																	
プロトコルブロックタイプ(4)*																																	
ネットワーク プロトコルブ ロック*	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																																	
プロトコルブロックタイプ(4)*																																	
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長																																
	トランスポート プロトコル データ...																																

レガシーディスカバリデータ構造

バイト	0								1								2								3															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
ビット																																	MACアドレスのリスト							
	リストブロックタイプ(11)																																							
																																MACアドレスブロック*								
リストブロック長																																								
MACアドレスブロックタイプ(95)*																																								
																																最終検出時のホスト								
MACアドレスブロック長																																								
																																ホストタイプ								
MACアドレスデータ...																																								
																																クライアントアプリケーションのリスト								
VLANの有無								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)																																
汎用リストブロックタイプ(続き)								汎用リストブロック長																																
クライアントアプリケーションデータ	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ブロックタイプ(112)*																															
	クライアントアプリケーションブロックタイプ(29)*(続き)								クライアントアプリケーションブロック長																															
	クライアントアプリケーションブロック長(続き)								クライアントアプリケーションデータ...																															
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-26 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。 <ul style="list-style-type: none"> 0: ホストはプライマリ ネットワークにあります。 1: ホストはセカンダリ ネットワークにあります。
汎用リストブロックタイプ	uint32	サーバフィンガープリントを使用して特定されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(サーバフィンガープリント)データブロック*	変数 (variable)	サーバフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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-133 ページ) を参照してください。
汎用リストブロックタイプ	uint32	クライアントフィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。

表 B-26 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
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-133 ページ) を参照してください。
汎用リストブロックタイプ	uint32	SMB フィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。
オペレーティングシステムフィンガープリント(SMB フィンガープリント)データブロック*	変数(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-133 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-133 ページ) を参照してください。
リストブロックタイプ	uint32	TCP サーバデータを伝えるサーバデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバデータブロックを加えた値です。 このフィールドには、ゼロ以上のサーバデータブロックが続きます。
サーバブロックタイプ	uint32	サーバデータブロックを開始します。この値は常に 89 です。

表 B-26 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
サーバブロック長	uint32	サーバデータブロックのバイト数(サーバブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く TCP サーバデータのバイト数を含む)。
TCP サーバデータ	変数 (variable)	TCP サーバを記述するデータフィールド(旧バージョンの製品で説明)。
リストブロックタイプ	uint32	UDP サーバデータを伝えるサーバデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバデータブロックを加えた値です。 このフィールドには、ゼロ以上のサーバデータブロックが続きます。
サーバブロックタイプ	uint32	UDP サーバを記述するサーバデータブロックを開始します。この値は常に 89 です。
サーバブロック長	uint32	サーバデータブロックのバイト数(サーバブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く UDP サーバデータのバイト数を含む)。
UDP サーバデータ	変数 (variable)	UDP サーバを記述するデータフィールド(旧バージョンの製品で説明)。
リストブロックタイプ	uint32	ネットワークプロトコルデータを伝えるプロトコルデータブロック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。

表 B-26 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
プロトコルブロックタイプ	uint32	トランスポートプロトコルを記述するプロトコルデータブロックを開始します。この値は常に 4 です。
プロトコルブロック長	uint32	プロトコルデータブロックのバイト数(プロトコルブロックタイプと長さ用の 8 バイト、およびそれに続くプロトコルデータのバイト数を含む)。
トランスポートプロトコルデータ	変数 (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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 0:はい • 1:いいえ
VLAN ID (Admin. VLAN ID)	uint16	ホストがいずれの VLAN メンバーであることを示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグ内でカプセル化されるパケットのタイプ。
VLAN プライオリティ	uint8	VLAN タグに含まれるプライオリティ値。

表 B-26 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	クライアントアプリケーションデータを伝えるクライアントアプリケーションデータブロックで構成される汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのクライアントアプリケーションデータブロックを含む)。
クライアントアプリケーションブロックタイプ	uint32	クライアントアプリケーションブロックを開始します。この値は常に 5 です。
クライアントアプリケーションブロック長	uint32	クライアントアプリケーションブロックのバイト数(クライアントアプリケーションブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くクライアントアプリケーションデータのバイト数を含む)。
クライアントアプリケーションデータ	変数 (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(4-164 ページ)で説明)。
文字列ブロックタイプ	uint32	NetBIOS 名の文字列データブロックを開始します。この値は文字列データを示す 0 に設定されます。
文字列ブロック長	uint32	NetBIOS 名データブロックのバイト数を示します(文字列ブロックタイプと長さのフィールド用の 8 バイト、および NetBIOS 名のバイト数を含む)。
NetBIOS 文字列データ	変数	ホストプロファイルに記述されているホストの NetBIOS 名が含まれます。

レガシー OS フィンガープリントデータブロック

詳細については、次の各項を参照してください。

- [オペレーティングシステムフィンガープリントデータブロック 5.0 ~ 5.0.2 \(B-133 ページ\)](#)

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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	オペレーティングシステムフィンガープリントブロックタイプ(87)																															
	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																															
	フィンガープリントの最終確認値																															
	TTL 差異																															

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-27 オペレー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。

表 B-27 オペレーティングシステム 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 タイプ	uint32	フィンガープリントのタイプを示します。
フィンガープリント ソース タイプ	uint32	オペレーティングシステム フィンガープリントを提供するソースのタイプ(ユーザやスキャナ)を示します。
フィンガープリント ソース ID	uint32	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\(B-135 ページ\)](#)
- [接続統計データ ブロック 5.1\(B-140 ページ\)](#)
- [接続統計データ ブロック 5.2.x\(B-146 ページ\)](#)
- [接続チャンク データ ブロック 5.0 ~ 5.1\(B-153 ページ\)](#)
- [接続チャンク データ ブロック 5.1.1 ~ 6.0.x\(B-154 ページ\)](#)
- [接続統計データ ブロック 5.1.1.x\(B-156 ページ\)](#)
- [接続統計データ ブロック 5.3\(B-163 ページ\)](#)
- [接続統計データ ブロック 5.3.1\(B-170 ページ\)](#)
- [接続統計データ ブロック 5.4\(B-177 ページ\)](#)
- [接続統計データ ブロック 5.4.1\(B-191 ページ\)](#)
- [接続統計データ ブロック 6.0.x\(B-205 ページ\)](#)
- [接続統計データ ブロック 6.1.x\(B-222 ページ\)](#)

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							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	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нда IP アドレス(続き)																															
	レスポнда 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нда 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 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ ID (続き)																アプリケーション プロトコル ID															
	アプリケーションプロトコル ID (続き)																URL カテゴリ															
	URL カテゴリ (続き)																URL レピュテー ション															
	URL レピュテーション (続き)																クライアントア プリケーション ID															
	クライアントアプリケーション ID (続き)																Web アプリケー ション ID															
	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-28 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-28 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нда IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに回答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた関連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ндаポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス
最初のパケットタイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケットタイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
送信パケット数	uint64	開始ホストからの送信パケット数。
受信パケット数	uint64	応答ホストが送信したパケット数。
送信バイト数	uint64	開始ホストからの送信バイト数。
受信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID (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。

表 B-28 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 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。

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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	接続データ ブロック タイプ (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нда IP アドレス																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	レスポンド IP アドレス(続き)																															
	レスポンド IP アドレス(続き)																															
	レスポンド 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																レスポンド 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)																								レスポンド送信パケット数							
	レスポンド送信パケット数(続き)																															
	レスポンド送信パケット数(続き)																								イニシエータ送信バイト数							
	イニシエータ送信バイト数(続き)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	イニシエータ送信バイト数(続き)																レスポнда送信バイト数															
	レスポнда送信バイト数(続き)																ユーザ ID (User ID)															
	レスポнда送信バイト数(続き)																ユーザ ID(続き)															
	ユーザ ID(続き)																アプリケーションプロトコル ID															
	アプリケーションプロトコル ID(続き)																URL カテゴリ															
	URL カテゴリ(続き)																URL レピュテーション															
	URL レピュテーション(続き)																クライアントアプリケーション ID															
	クライアントアプリケーション ID(続き)																Web アプリケーション ID															
	Web アプリケーション ID(続き)																文字列ブロックタイプ(0)															
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 ルール 1																															
	モニタ ルール 2																															
	モニタ ルール 3																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	モニタ ルール 4																															
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/ 宛先																秒開始レビュ ーション層															

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-29 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нда 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]	トリガーされた関連イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アク ション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。

表 B-29 接続統計データブロック 5.1 のフィールド(続き)

フィールド	データタイプ	説明
イニシエータポート	uint16	開始ホストにより使用されるポート。
レスポнда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нда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нда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ 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)。

表 B-29 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 アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティインテリジェンス層	uint8	IP ブラックリストに一致した IP 層。

接続統計データブロック 5.2.x

接続統計データブロックは、接続データメッセージで使用されます。バージョン 5.1.1 と 5.2 の間に加えられた接続データブロックの変更には、地理位置情報をサポートするための新規フィールドの追加が含まれます。バージョン 5.2.x の接続統計データブロックは、シリーズ 1 グループのブロックの、ブロックタイプ 144 です。これにより、ブロックタイプ 137(接続統計データブロック 5.1.1.x(B-156 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							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	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)																															
	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нда IP アドレス(続き)																															
	レスポнда 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нда 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нда Tx Packets							
	レスポнда送信パケット数(続き)																															
	レスポнда送信パケット数(続き)																								イニシエータ送信バイト数							
	イニシエータ送信バイト数(続き)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	イニシエータ送信バイト数(続き)																							レスポндаTx Bytes								
	レスポнда送信バイト数(続き)																							ユーザ ID(User ID)								
	レスポнда送信バイト数(続き)																							ユーザ ID(続き)								
	ユーザ ID(続き)																							アプリケーションプロトコル ID								
	アプリケーションプロトコル ID(続き)																							URL カテゴリ								
	URL カテゴリ(続き)																							URLレピュテーション								
	URLレピュテーション(続き)																							クライアントアプリケーション ID								
	クライアントアプリケーション ID(続き)																							Web アプリケーション ID								
クライアント URL	Web アプリケーション ID(続き)																							文字列ブロックタイプ(0)								
	文字列ブロックタイプ(続き)																							文字列ブロック長								
	文字列ブロック長(続き)																							クライアントアプリケーション URL...								
NetBIOS [名前(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 ルール 1																															
	モニタ ルール 2																															
	モニタ ルール 3																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	モニタ ルール 4																															
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/ 宛先								秒イニシエー タ層								ファイル イベント カウント															
	侵入イベント カウント																イニシエータの国															
	レスポنداの国																															

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-30 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ندا IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに回答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた関連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)。

表 B-30 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
ルールアクション	uint16	そのルールに対してユーザインターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータポート	uint16	開始ホストにより使用されるポート。
レスポнда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нда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нда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ 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-30 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 アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティインテリジェンス層	uint8	IP ブラックリストに一致した IP 層。

表 B-30 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нда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。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	イニシエータ IP アドレス																															
	レスポнда IP アドレス																															
	開始時刻																															
	アプリケーションプロトコル																															
	レスポнда ポート																プロトコル								接続タイプ							
	NetFlow ディテクタ IP アドレス																															
	送信パケット数 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)																															
	送信バイト数 送信バイト数(続き)																															
	受信バイト数 受信バイト数(続き)																															
	接続																															

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-32 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нда 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нда IP アドレス	uint8(4)	この接続タイプのレスポнда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。

表 B-32 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
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ндаポート	uint16	接続チャンクでレスポндаが使用したポート。
プロトコル	uint8	ユーザ情報を含むパケットのプロトコル。
接続タイプ	uint8	接続の種類。
NetFlow ディテクタ IP アドレス	uint8[4]	IP アドレス オクテットの、接続を検出した NetFlow デバイスの IP アドレス。
送信パケット数	uint64	接続チャンクで送信されたパケット数。
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 \(B-140 ページ\)](#)) 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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1			
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)																																			

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ルール ID																															
	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нда 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нда Tx Packets							
	レスポнда送信パケット数 (続き)																															
	レスポнда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нда Tx Bytes							
	レスポнда送信バイト数 (続き)																															
	レスポнда送信バイト数 (続き)																								ユーザ ID (User ID)							
	ユーザ ID (続き)																															
	ユーザ ID (続き)																								アプリケーションプロトコル ID							
	アプリケーションプロトコル ID (続き)																															
	アプリケーションプロトコル ID (続き)																								URL カテゴリ							

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	URL カテゴリ(続き)																URL レピュテーション															
	URL 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...																															
	モニターール 1																															
	モニターール 2																															
	モニターール 3																															
	モニターール 4																															
	モニターール 5																															
	モニターール 6																															
	モニターール 7																															
	モニターール 8																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	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-33 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нда IP ア ドレス	uint8[16]	IP アドレス オクテットの、開始ホストに回答したホストの IP アドレス。
ポリシー リビ ジョン	uint8[16]	トリガーされた関連イベントに関連付けられているルール のリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アク ション	uint16	そのルールに対してユーザ インターフェイスで選択された アクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポнда ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。

表 B-33 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
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нда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нда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ 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-33 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
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。
モニタルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタルールの ID。
モニタルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタルールの ID。
モニタルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタルールの ID。
モニタルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタルールの ID。
モニタルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタルールの ID。
モニタルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタルールの ID。
モニタルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタルールの ID。
モニタルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタルールの ID。
セキュリティインテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティインテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイルイベントカウント	uint16	同じ秒で発生するファイルイベントを区別するために使用される値。
侵入イベントカウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。

接続統計データ ブロック 5.3

接続統計データ ブロックは、接続データ メッセージで使用されます。バージョン 5.2.x と 5.3 の間に加えられた接続データ ブロックの変更には、NetFlow 情報用の新規フィールドの追加が含まれます。バージョン 5.3 の接続統計データ ブロックは、シリーズ 1 グループのブロックの、ブロック タイプ 152 です。これにより、ブロック タイプ 144 (接続統計データ ブロック 5.2.x (B-146 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 (2-13 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続データ ブロック タイプ (152)																																
接続データ ブロック長																																
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)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	出力インターフェイス(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нда IP アドレス																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	レスポнда 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нда 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	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)																レスポнда Tx Packets															
	イニシエータ送信パケット数(続き)																															
	レスポнда送信パケット数(続き)																イニシエータ送信バイト数															
	レスポнда送信パケット数(続き)																															
	イニシエータ送信バイト数(続き)																レスポнда Tx Bytes															
	イニシエータ送信バイト数(続き)																															
	レスポнда送信バイト数(続き)																ユーザ ID (User ID)															
	レスポнда送信バイト数(続き)																															
	ユーザ ID(続き)																アプリケーションプロトコル ID															
	アプリケーションプロトコル ID(続き)																URL カテゴリ															
	URL カテゴリ(続き)																URL レピュテーション															
	URL レピュテーション(続き)																クライアントアプリケーション ID															
	クライアントアプリケーション ID(続き)																Web アプリケーション ID															
クライアント URL	Web アプリケーション ID(続き)																文字列ブロックタイプ(0)															
	文字列ブロックタイプ(続き)																文字列ブロック長															
	文字列ブロック長(続き)																クライアントアプリケーション URL...															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NetBIOS [名前 (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 ルール 1																															
	モニタ ルール 2																															
	モニタ ルール 3																															
	モニタ ルール 4																															
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/ 宛先								秒イニシエー タ層								ファイル イベント カウント															
	侵入イベント カウント																イニシエータの国															
	レスポндаの国																IOC 番号															
	送信元自律システム																															
	宛先自律システム																															
	SNMP 入力																SNMP 出力															
	送信元 TOS								宛先 TOS								送信元マスク								宛先マスク							

次の表は、接続統計データ ブロック 5.3 のフィールドについての説明です。

表 B-34 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。
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нда 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]	トリガーされた関連イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アク ション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポнда 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-34 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нда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нда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ 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-34 接続統計データブロック 5.3+のフィールド(続き)

フィールド	データタイプ	説明
モニタ ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタ ルールの ID。
モニタ ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタ ルールの ID。
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス 送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入イベント カウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータ の国	uint16	開始ホストの国のコード。
レスポнда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 \(B-163 ページ\)](#)) 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 \(2-13 ページ\)](#) 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。

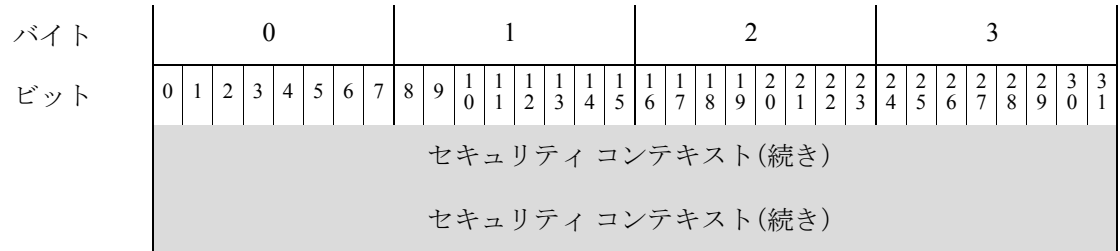
次の図は、接続統計データブロック 5.3.1 の形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	接続データブロックタイプ (154)																															
	接続データブロック長																															
	デバイス ID (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)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	出力インターフェイス(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нда IP アドレス																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	レスポнда 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нда 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 ビット	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	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)																レスポнда Tx Packets															
	イニシエータ送信パケット数(続き)																															
	レスポнда送信パケット数(続き)																イニシエータ送信バイト数															
	レスポнда送信パケット数(続き)																															
	イニシエータ送信バイト数(続き)																レスポнда Tx Bytes															
	イニシエータ送信バイト数(続き)																															
	レスポнда送信バイト数(続き)																ユーザ ID (User ID)															
	レスポнда送信バイト数(続き)																															
	ユーザ ID(続き)																アプリケーションプロトコル ID															
	アプリケーションプロトコル ID(続き)																URL カテゴリ															
	URL カテゴリ(続き)																URL レピュテーション															
	URL レピュテーション(続き)																クライアントアプリケーション ID															
	クライアント アプリケーション ID(続き)																Web アプリケーション ID															
クライアント URL	Web アプリケーション ID(続き)																文字列ブロックタイプ(0)															
	文字列ブロックタイプ(続き)																文字列ブロック長															
	文字列ブロック長(続き)																クライアントアプリケーション URL...															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NetBIOS [名前(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 ルール 1																																
モニタ ルール 2																																
モニタ ルール 3																																
モニタ ルール 4																																
モニタ ルール 5																																
モニタ ルール 6																																
モニタ ルール 7																																
モニタ ルール 8																																
秒開始送信元/ 宛先								秒イニシエー タ層								ファイルイベント カウント																
侵入イベント カウント																イニシエータの国																
レスポнда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)																																



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-35 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。
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нда 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]	トリガーされた関連イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アク ション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポнда ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。

表 B-35 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
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нда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нда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ 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の内部 ID 番号。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URL レピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロックタイプ	uint32	クライアントアプリケーション URL の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーション URL の文字列データブロックのバイト数(文字列ブロックタイプと長さのフィールド用の 8 バイト、およびクライアントアプリケーション URL 文字列のバイト数を含む)。
クライアントアプリケーション URL	string	クライアントアプリケーションがアクセスする URL(該当する場合) (/files/index.html など)。
文字列ブロックタイプ	uint32	ホスト NetBIOS 名の文字列データブロックを開始します。この値は常に 0 です。

表 B-35 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
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。
モニタルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタルールの ID。
モニタルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタルールの ID。
モニタルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタルールの ID。
モニタルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタルールの ID。
モニタルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタルールの ID。
モニタルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタルールの ID。
モニタルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタルールの ID。
モニタルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタルールの ID。
セキュリティインテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティインテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイルイベントカウント	uint16	同じ秒で発生するファイルイベントを区別するために使用される値。
侵入イベントカウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポндаの国	uint16	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。

表 B-35 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
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-170 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(2-13 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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
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																																						

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ポリシー リビジョン(続き)																																
ポリシー リビジョン(続き)																																
ルール ID																																
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нда 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нда Tx Packets								
レスポнда送信パケット数(続き)																																
レスポнда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нда Tx Bytes								
レスポнда送信バイト数(続き)																																
レスポнда送信バイト数(続き)																								ユーザ 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ ID(続き)														アプリケーション プロトコル ID																	
	アプリケーションプロトコル ID(続き)														URL カテゴリ																	
	URL カテゴリ(続き)														URL レピュテー ション																	
	URL レピュテーション(続き)														クライアント アプリケー ション ID																	
	クライアントアプリケーション ID(続き)														Web アプリケー ション ID																	
クライアント URL	Web アプリケーション ID(続き)														文字列ブロック タイプ(0)																	
	文字列ブロック タイプ(続き)														文字列ブロック長																	
	文字列ブロック長(続き)														クライアントア プリケーシ ョン URL...																	
NetBIOS [名前(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 ルール 1																															
	モニタ ルール 2																															
	モニタ ルール 3																															
	モニタ ルール 4																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/ 宛先								秒イニシエー タ層								ファイル イベント カウント															
	侵入イベント カウント																イニシエータの国															
	レスポнда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...															
ト ン ジェ ー ユ ー ザ エ ー ジ ェ ン ト	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ エージェント...																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
HTTP リファラ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	HTTP リファラ...																															
SSL 証明書フィンガープリント																																
SSL 証明書フィンガープリント(続き)																																
SSL 証明書フィンガープリント(続き)																																
SSL 証明書フィンガープリント(続き)																																
SSL 証明書フィンガープリント(続き)																																
SSL ポリシー ID																																
SSL ポリシー ID(続き)																																
SSL ポリシー ID(続き)																																
SSL ポリシー ID(続き)																																
SSL ルール ID																																
SSL 暗号スイート																SSL バージョン								SSL キー証明書 統計								
SSL キー証明書 統計(続き)								実際の SSL アクション																予期された SSL アクション								
予期された SSL アクション(続き)								SSL フロー ステータス																SSL フロー エ ラー								
SSL フロー エラー(続き)																SSL フロー メッ セージ																
SSL フロー メッセージ(続き)																SSL フロー フラ グ																
SSL フロー フラグ(続き)																																

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-36 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нда IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに回答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた関連イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルールアクション	uint16	そのルールに対してユーザインターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータポート	uint16	開始ホストにより使用されるポート。
レスポнда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。

表 B-36 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
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нда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нда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ 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)。

表 B-36 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バージョン	string	クライアントアプリケーションバージョン。
モニタルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタルールの ID。
モニタルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタルールの ID。
モニタルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタルールの ID。
モニタルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタルールの ID。
モニタルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタルールの ID。
モニタルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタルールの ID。
モニタルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタルールの ID。
モニタルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタルールの ID。
セキュリティインテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティインテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイルイベントカウント	uint16	同じ秒で発生するファイルイベントを区別するために使用される値。
侵入イベントカウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポндаの国	uint16	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。

表 B-36 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
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	ユーザエージェントを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザエージェント文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびユーザエージェントフィールドのバイト数を含む)。
ユーザエージェント	string	セッションのユーザエージェントヘッダーフィールドからの情報。
文字列ブロックタイプ	uint32	HTTP リファラを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	HTTP リファラ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および HTTP リファラフィールドのバイト数を含む)。
HTTP リファラ	string	ページの発生元のサイト。これは HTTP トラフィック内の参照ヘッダー情報にあります。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
SSL ポリシー ID	uint8[16]	接続を処理した SSL ポリシーの ID 番号。
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルトアクションの ID 番号。
SSL 暗号スイート	uint16	SSL 接続で使用される暗号スイート。値は 10 進形式で保存されます。値により指定されている暗号スイートの詳細については、 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
SSL バージョン	uint8	接続の暗号化に使用された SSL または TLS プロトコルバージョン。

表 B-36 接続統計データブロック 5.4+のフィールド(続き)

フィールド	データタイプ	説明
SSL サーバ証明書ステータス	uint16	<p>SSL 証明書のステータス。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 1(不明):サーバ証明書のステータスは判別できませんでした。 2(有効):サーバ証明書は有効です。 4(自己署名済み):サーバ証明書は自己署名です。 16(無効な発行者):サーバ証明書に無効な発行者があります。 32(無効な署名):サーバ証明書に無効な署名があります。 64(期限切れ):サーバ証明書は期限切れです。 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 256(取り消し):サーバ証明書は取り消されました。
実際の SSL アクション	uint16	<p>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。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> 0:「不明」 1:「復号しない」 2:「ブロックする」 3:「リセットでブロック」 4:「復号(既知のキー)」 5:「復号(置換キー)」 6:「復号(Resign)」

表 B-36 接続統計データブロック 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	<p>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。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL フロー エラー	uint32	<p>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。</p>

表 B-36 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	<p>SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> 0x00000001 (NSE_FLOW__VALID):他のフィールドを有効にするために設定する必要があります 0x00000002 (NSE_FLOW__INITIALIZED):内部構造が処理可能です 0x00000004 (NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました
文字列ブロックタイプ	uint32	SSL サーバ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	SSL サーバ名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および SSL サーバ名フィールドのバイト数を含む)。

表 B-36 接続統計データ ブロック 5.4+のフィールド(続き)

フィールド	データ タイプ	説明
SSL サーバ名	string	SSL Client Hello でサーバ名に指定された名前。
SSL URL カテゴリ	uint32	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値。
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできます。
SSL チケット ID	uint8[20]	クライアントとサーバがセッション チケットの使用に同意する場合に使用されるセッション チケットのハッシュ。
SSL チケット ID の長さ	uint8	SSL チケット ID の長さ。チケット ID は 20 バイトより長くすることはできませんが、20 バイト未満であってもかまいません。
ネットワーク分析ポリシー リビジョン	uint8[16]	接続イベントに関連付けられているネットワーク分析ポリシーのリビジョン。

接続統計データ ブロック 5.4.1

接続統計データ ブロックは、接続データ メッセージで使用されます。接続統計データ ブロック 5.4 には、いくつかの新しいフィールドが追加されました。SSL 接続、HTTP リダイレクション、およびネットワーク分析ポリシーをサポートするためのフィールドが追加されています。バージョン 5.4+ の接続統計データ ブロックは、シリーズ 1 グループのブロックの、ブロック タイプ 157 です。これにより、ブロック タイプ 155(接続統計データ ブロック 5.3.1(B-170 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(2-13 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続データ ブロック タイプ(157)																																
接続データ ブロック長																																
デバイス ID(Device ID)																																
入力ゾーン																																

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ポリシー リビジョン(続き)																															
	ポリシー リビジョン(続き)																															
	ルール ID																															
	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нда 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нда Tx Packets							
	レスポнда送信パケット数(続き)																															
	レスポнда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нда Tx Bytes							
	レスポнда送信バイト数(続き)																															
	レスポнда送信バイト数(続き)																								ユーザ 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ ID (続き)														アプリケーションプロトコル ID																	
	アプリケーションプロトコル ID (続き)														URL カテゴリ																	
	URL カテゴリ (続き)														URL レピュテーション																	
	URL レピュテーション (続き)														クライアントアプリケーション ID																	
	クライアントアプリケーション ID (続き)														Web アプリケーション ID																	
クライアント URL	Web アプリケーション ID (続き)														文字列ブロックタイプ (0)																	
	文字列ブロックタイプ (続き)														文字列ブロック長																	
	文字列ブロック長 (続き)														クライアントアプリケーション URL...																	
NetBIOS [名前]	文字列ブロックタイプ (0)																															
	文字列ブロック長																															
	NetBIOS 名...																															
クライアントアプリケーションバージョン	文字列ブロックタイプ (0)																															
	文字列ブロック長																															
	クライアントアプリケーションバージョン...																															
	モニタ ルール 1																															
	モニタ ルール 2																															
	モニタ ルール 3																															
	モニタ ルール 4																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/ 宛先								秒イニシエー タ層								ファイルイベント カウント															
	侵入イベント カウント																イニシエータの国															
	レスポнда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...															
ト ン ジェ ー エ コ ユ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ エージェント...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
HTTP リファラ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	HTTP リファラ...																															
	SSL 証明書フィンガープリント																															
	SSL 証明書フィンガープリント(続き)																															
	SSL 証明書フィンガープリント(続き)																															
	SSL 証明書フィンガープリント(続き)																															
	SSL 証明書フィンガープリント(続き)																															
	SSL ポリシー ID																															
	SSL ポリシー ID(続き)																															
	SSL ポリシー ID(続き)																															
	SSL ポリシー ID(続き)																															
	SSL ルール ID																															
	SSL 暗号スイート																SSL バージョン								SSL キー証明書 統計							
SSL キー証明書 統計(続き)								実際の SSL アクション																予期された SSL アクション								
予期された SSL アクション(続き)								SSL フロー ステータス																SSL フロー エ ラー								
SSL フロー エラー(続き)																SSL フロー メッ セージ																
SSL フロー メッセージ(続き)																SSL フロー フラ グ																
SSL フロー フラグ(続き)																																

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-37 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нда IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに回答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた関連イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルールアクション	uint16	そのルールに対してユーザインターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータポート	uint16	開始ホストにより使用されるポート。
レスポнда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。

表 B-37 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
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нда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нда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ 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)。

表 B-37 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バージョン	string	クライアントアプリケーションバージョン。
モニタルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタルールの ID。
モニタルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタルールの ID。
モニタルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタルールの ID。
モニタルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタルールの ID。
モニタルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタルールの ID。
モニタルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタルールの ID。
モニタルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタルールの ID。
モニタルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタルールの ID。
セキュリティインテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティインテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイルイベントカウント	uint16	同じ秒で発生するファイルイベントを区別するために使用される値。
侵入イベントカウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポндаの国	uint16	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。

表 B-37 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
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	ユーザエージェントを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザエージェント文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびユーザエージェントフィールドのバイト数を含む)。
ユーザエージェント	string	セッションのユーザエージェントヘッダーフィールドからの情報。
文字列ブロックタイプ	uint32	HTTP リファラを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	HTTP リファラ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および HTTP リファラフィールドのバイト数を含む)。
HTTP リファラ	string	ページの発生元のサイト。これは HTTP トラフィック内の参照ヘッダー情報にあります。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
SSL ポリシー ID	uint8[16]	接続を処理した SSL ポリシーの ID 番号。
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルトアクションの ID 番号。
SSL 暗号スイート	uint16	SSL 接続で使用される暗号スイート。値は 10 進形式で保存されます。値により指定されている暗号スイートの詳細については、 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
SSL バージョン	uint8	接続の暗号化に使用された SSL または TLS プロトコルバージョン。

表 B-37 接続統計データブロック 5.4+ のフィールド(続き)

フィールド	データタイプ	説明
SSL サーバ証明書ステータス	uint16	<p>SSL 証明書のステータス。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 1(不明):サーバ証明書のステータスは判別できませんでした。 2(有効):サーバ証明書は有効です。 4(自己署名済み):サーバ証明書は自己署名です。 16(無効な発行者):サーバ証明書に無効な発行者があります。 32(無効な署名):サーバ証明書に無効な署名があります。 64(期限切れ):サーバ証明書は期限切れです。 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 256(取り消し):サーバ証明書は取り消されました。
実際の SSL アクション	uint16	<p>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。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> 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-37 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	<p>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。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL フロー エラー	uint32	<p>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。</p>

表 B-37 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	<p>SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> 0x00000001 (NSE_FLOW__VALID):他のフィールドを有効にするために設定する必要があります 0x00000002 (NSE_FLOW__INITIALIZED):内部構造が処理可能です 0x00000004 (NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました
文字列ブロックタイプ	uint32	SSL サーバ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	SSL サーバ名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および SSL サーバ名フィールドのバイト数を含む)。

表 B-37 接続統計データブロック 5.4+ のフィールド(続き)

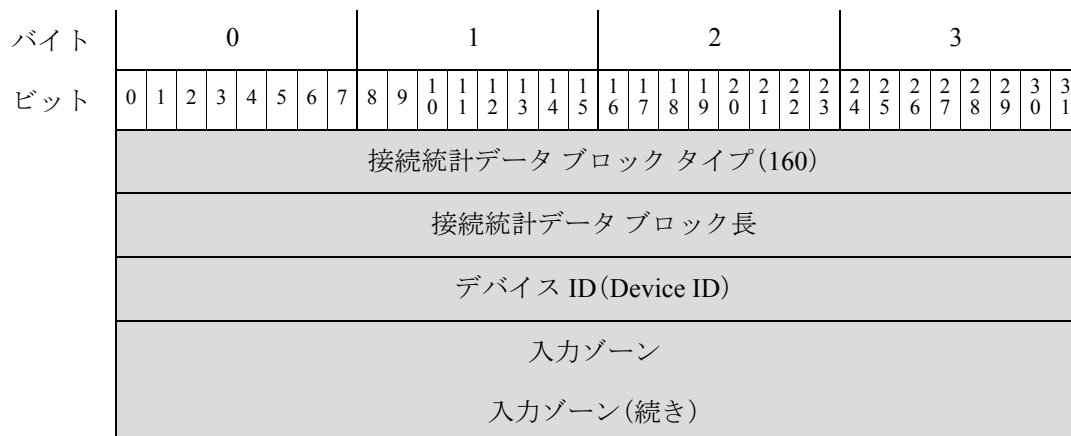
フィールド	データタイプ	説明
SSL サーバ名	string	SSL Client Hello でサーバ名に指定された名前。
SSL URL カテゴリ	uint32	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値。
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできます。
SSL チケット ID	uint8[20]	クライアントとサーバがセッション チケットの使用に同意する場合に使用されるセッション チケットのハッシュ。
SSL チケット ID の長さ	uint8	SSL チケット ID の長さ。チケット ID は 20 バイトより長くすることはできませんが、20 バイト未満であってもかまいません。
ネットワーク分析ポリシー リビジョン	uint8[16]	接続イベントに関連付けられているネットワーク分析ポリシーのリビジョン。

接続統計データブロック 6.0.x

接続統計データブロックは、接続データメッセージで使用されます。接続統計データブロック 6.0 には、いくつかの新しいフィールドが追加されました。ISE 統合および複数ネットワークマップをサポートするために、フィールドが追加されました。バージョン 6.0.x の接続統計データブロックは、シリーズ 1 グループのブロックの、ブロックタイプ 160 です。これはブロックタイプ 157(接続統計データブロック 5.4.1 (B-191 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(2-13 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(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нда IP アドレス																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	ポリシー リビジョン																															
	ポリシー リビジョン(続き)																															
	ポリシー リビジョン(続き)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ポリシー リビジョン(続き)																																
ルール ID																																
ルール アクション																ルールの理由																
ルールの理由(続き)																イニシエータ ポート																
レスポнда 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нда送信パケット数																								
								レスポнда送信パケット数(続き)																								
レスポнда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нда送信バイト数																								
								レスポнда送信バイト数(続き)																								

バイト	0							1							2							3																
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						
	レスポンス送信 バイト数(続き)							ユーザ ID (User ID)																														
	ユーザ ID(続き)							アプリケーションプロトコル ID																														
	アプリケーション プロトコル ID (続き)							URL カテゴリ																														
	URL カテゴリ (続き)							URL レピュテーション																														
	URL レピュテー ション(続き)							クライアントアプリケーション ID																														
	クライアントア プリケーション ID(続き)							Web アプリケーション ID																														
クライアント URL	Web アプリケー ション ID(続き)							String ブロック タイプ(0)																														
	文字列ブロック タイプ(続き)							文字列ブロック長																														
	文字列ブロック 長(続き)							クライアントアプリケーション URL...																														
NetBIOS [名前(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 ルール 1																																					
	モニタ ルール 2																																					

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
モニタ ルール 3																																
モニタ ルール 4																																
モニタ ルール 5																																
モニタ ルール 6																																
モニタ ルール 7																																
モニタ ルール 8																																
秒開始送信元/ 宛先								秒イニシエー タ層								ファイル イベント カウント																
侵入イベント カウント																イニシエータの国																
レスポнда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...															
ト ン シ ェ ー ユ ー ザ コ ー ド	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ エージェント...																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
HTTP リファラ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	HTTP リファラ...																															
SSL 証明書フィンガープリント																																
SSL 証明書フィンガープリント(続き)																																
SSL 証明書フィンガープリント(続き)																																
SSL 証明書フィンガープリント(続き)																																
SSL 証明書フィンガープリント(続き)																																
SSL ポリシー ID																																
SSL ポリシー ID(続き)																																
SSL ポリシー ID(続き)																																
SSL ポリシー ID(続き)																																
SSL ルール ID																																
SSL 暗号スイート																SSL バージョン								SSL キー証明書 統計								
SSL キー証明書 統計(続き)								実際の SSL アクション																予期された SSL アクション								
予期された SSL アクション(続き)								SSL フロー ステータス																SSL フロー エ ラー								
SSL フロー エラー(続き)																SSL フロー メッ セージ																
SSL フロー メッセージ(続き)																SSL フロー フラ グ																
SSL フロー フラグ(続き)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	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)															
	ロケーション IPv6(続き)																HTTP レスポンス															
	HTTP レスポンス(続き)																文字列ブロック タイプ (0)															
	文字列ブロック タイプ (0) (続き)																文字列ブロック長															
	文字列ブロック長(続き)																DNS クエリ...															
	DNS レコードタイプ (DNS Record Type)																DNS レスポンス タイプ															
	DNS TTL																															
	シンクホール UUID																															
	シンクホール UUID(続き)																															
	シンクホール UUID(続き)																															
	シンクホール UUID(続き)																															
	セキュリティインテリジェンス リスト 1																															
	セキュリティインテリジェンス リスト 2																															

次の表は、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-38 接続統計データブロック 6.0.x のフィールド

フィールド	データタイプ	説明
接続統計データブロックタイプ	uint32	接続統計データブロック 6.0+ を開始します。値は常に 160 です。
接続統計データブロック長	uint32	接続統計データブロックのバイト数(接続統計ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。

表 B-38 接続統計データブロック 6.0.x のフィールド(続き)

フィールド	データタイプ	説明
デバイス ID (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нда IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに回答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた相関イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アクション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint32	イベントをトリガーしたルールの理由。
イニシエータポート	uint16	開始ホストにより使用されるポート。
レスポнда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нда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-38 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нда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ 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。

表 B-38 接続統計データブロック 6.0.x のフィールド(続き)

フィールド	データタイプ	説明
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス 送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入イベント カウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータ の国	uint16	開始ホストの国のコード。
レスポンスの国	uint 16	応答ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。
SNMP 出力	uint16	出力インターフェイスの SNMP インデックス
送信元 TOS	uint8	着信インターフェイス用のタイプオブ サービス バイト設定。
宛先 TOS	uint8	発信インターフェイス用のタイプオブ サービス バイト設定。
送信元マスク	uint8	送信元アドレス プレフィックス マスク。
宛先マスク	uint8	宛先アドレス プレフィックス マスク。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキストモードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

表 B-38 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
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 エージェントを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック 長	uint32	ユーザ エージェント文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびユーザ エージェントフィールドのバイト数を含む)。
ユーザ エージェント	string	セッションのユーザ エージェントヘッダーフィールドからの情報。
文字列ブロック タイプ	uint32	HTTP リファラを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック 長	uint32	HTTP リファラ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および HTTP リファラフィールドのバイト数を含む)。
HTTP リファラ	string	ページの発生元のサイト。これは HTTP トラフィック内の参照ヘッダー情報にあります。
SSL 証明書フィン ガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
SSL ポリシー ID	uint8[16]	接続を処理した SSL ポリシーの ID 番号。
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルトアクションの ID 番号。
SSL 暗号スイ ート	uint16	SSL 接続で使用される暗号スイート。値は 10 進形式で保存されます。値により指定されている暗号スイートの詳細については、 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
SSL バージョン	uint8	接続の暗号化に使用された SSL または TLS プロトコルバージョン。

表 B-38 接続統計データブロック 6.0.x のフィールド(続き)

フィールド	データタイプ	説明
SSL サーバ証明書ステータス	uint16	<p>SSL 証明書のステータス。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 1(不明):サーバ証明書のステータスは判別できませんでした。 2(有効):サーバ証明書は有効です。 4(自己署名済み):サーバ証明書は自己署名です。 16(無効な発行者):サーバ証明書に無効な発行者があります。 32(無効な署名):サーバ証明書に無効な署名があります。 64(期限切れ):サーバ証明書は期限切れです。 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 256(取り消し):サーバ証明書は取り消されました。
実際の SSL アクション	uint16	<p>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。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> 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-38 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	<p>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。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL フロー エラー	uint32	<p>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。</p>

表 B-38 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	<p>SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> 0x00000001 (NSE_FLOW__VALID):他のフィールドを有効にするために設定する必要があります 0x00000002 (NSE_FLOW__INITIALIZED):内部構造が処理可能です 0x00000004 (NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました
文字列ブロックタイプ	uint32	SSL サーバ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	SSL サーバ名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および SSL サーバ名フィールドのバイト数を含む)。

表 B-38 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 サーバ名	string	SSL Client Hello でサーバ名に指定された名前。
SSL URL カテゴリ	uint32	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできます。
SSL チケット ID	uint8[20]	クライアントとサーバがセッション チケットの使用に同意する場合に使用されるセッション チケットのハッシュ。
SSL チケット ID の長さ	uint8	SSL チケット ID の長さ。チケット ID は 20 バイトより長くすることはできませんが、20 バイト未満であってもかまいません。
ネットワーク分析ポリシー リビジョン	uint8[16]	接続イベントに関連付けられているネットワーク分析ポリシーのリビジョン。
エンドポイントプロファイル ID	uint32	ISE により識別される、接続エンドポイントで使用されるデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
セキュリティグループ ID	uint32	ポリシーに基づいて ISE によりユーザに割り当てられた ID 番号。
ロケーション IPv6	uint8[16]	ISE と通信するインターフェイスの IP アドレス。IPv4 または IPv6 のアドレスを使用できます。
HTTP レスポンス	uint32	HTTP 要求の応答コード。
文字列ブロックタイプ	uint32	DNS クエリを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データブロックのバイト数(文字列ブロックタイプと長さのフィールド用の 8 バイト、および DNS クエリ文字列のバイト数を含む)。
DNS クエリ (DNS Query)	string	DNS サーバに送信されたクエリの内容。
DNS レコードタイプ (DNS Record Type)	uint16	DNS レコードタイプの数値。

表 B-38 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	<p>0(NoError): エラーなし</p> <p>1(FormErr): フォーマット エラー</p> <p>2(ServFail): サーバ障害</p> <p>3(NXDomain): 存在していないドメイン</p> <p>4(NotImp): 未実装</p> <p>5(Refused): クエリ拒否</p> <p>6(YXDomain): 名前が存在してはならない状況で存在している</p> <p>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</p> <p>8(NXRRSet): 存在しているべき RR セットが存在していない</p> <p>9(NotAuth): 未承認</p> <p>10(NotZone): 名前がゾーンに含まれていない</p> <p>16(BADSIG): TSIG 署名失敗</p> <p>17(BADKEY): キーが認識されない</p> <p>18(BADTIME): 時間範囲外の署名</p> <p>19(BADMODE): 不適切な TKEY モード</p> <p>20(BADNAME): 重複するキー名</p> <p>21(BADALG): サポートされていないアルゴリズム</p> <p>22(BADTRUNC): 不適切な切り捨て</p> <p>3841(NXDOMAIN): ファイアウォールからの NXDOMAIN 応答</p> <p>3842(SINKHOLE): ファイアウォールからのシンクホール応答</p>
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 \(B-205 ページ\)](#) 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 6.2+\(4-126 ページ\)](#))。

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 \(2-13 ページ\)](#) 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続統計データ ブロック タイプ (163)																																
接続統計データ ブロック 長																																
デバイス ID (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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出力インターフェイス(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нда IP アドレス																																
レスポнда IP アドレス(続き)																																
レスポнда IP アドレス(続き)																																
レスポнда 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нда ポート																TCP フラグ																
プロトコル								NetFlow ソース																								

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	NetFlow ソース(続き)																															
	NetFlow ソース(続き)																															
	NetFlow ソース(続き)																															
NetFlow ソース(続き)	インスタンス ID(Instance ID)																接続数カウンタ															
接続数カウンタ(続き)	最初の packets タイムスタンプ																															
最初の packets タイムスタンプ(続き)	最終 packets タイムスタンプ																															
最終 packets タイムスタンプ(続き)	イニシエータ送信 packets 数																															
	イニシエータ送信 packets 数(続き)																															
イニシエータ送信 packets 数(続き)	レスポнда送信 packets 数																															
	レスポнда送信 packets 数(続き)																															
レスポнда送信 packets 数(続き)	イニシエータ送信 bytes 数																															
	イニシエータ送信 bytes 数(続き)																															
イニシエータ送信 bytes 数(続き)	レスポнда送信 packets 数																															
	レスポнда送信 bytes 数(続き)																															
レスポнда送信 bytes 数(続き)	イニシエータ packets ドロップ																															
	イニシエータ packets ドロップ(続き)																															
イニシエータ packets ドロップ(続き)	レスポнда packets ドロップ																															
	レスポнда packets 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
レスポンスパケットドロップ (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)																															
レスポンスバイトドロップ (続き)									レスポンス バイト ドロップ																															
レスポンスバイトドロップ (続き)									レスポンス バイト ドロップ (続き)																															
QOS インターフェイス (続き)									QOS 適用インターフェイス																															
QOS ルール ID (続き)									QOS 適用インターフェイス (続き)																															
ユーザ ID (続き)									QOS 適用インターフェイス (続き)																															
アプリケーションプロトコル ID (続き)									QOS 適用インターフェイス (続き)																															
URL カテゴリ (続き)									QOS ルール ID																															
URL カテゴリ (続き)									ユーザ ID (User ID)																															
URL レピュテーション (続き)									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 (続き)									URL カテゴリ																															
									URL レピュテーション																															
									クライアント アプリケーション ID																															
									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 ルール 1																																									
モニタ ルール 2																																									
モニタ ルール 3																																									
モニタ ルール 4																																									
モニタ ルール 5																																									
モニタ ルール 6																																									
モニタ ルール 7																																									
モニタ ルール 8																																									
秒開始送信元/ 宛先							秒イニシエー タ層							ファイル イベント カウント																											
侵入イベント カウント														イニシエータの国																											

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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нда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 エージェント	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ エージェント...																															
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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	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 サーバ名	SSL フロー フラグ (続き)								文字列ブロック タイプ (0)																							
	文字列ブロック タイプ (0) (続き)								文字列ブロック長																							
	文字列ブロック長 (続き)								SSL サーバ名...																							
	SSL URL カテゴリ																															
	SSL セッション ID																															
	SSL セッション ID (続き)																															

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
DNS クエリ (DNS Query)	HTTP レスポンス (続き)																文字列ブロック タイプ (0)															
	文字列ブロック タイプ (0) (続き)																文字列ブロック長															
	文字列ブロック長 (続き)																DNS クエリ...															
	DNS レコード タイプ (DNS Record Type)																DNS レスポンス タイプ															
	DNS TTL																															
	シンクホール UUID シンクホール UUID (続き) シンクホール UUID (続き) シンクホール UUID (続き)																															
	セキュリティ インテリジェンス リスト 1																															
セキュリティ インテリジェンス リスト 2																																

次の表では、6.1+ の接続統計データ ブロックのフィールドについて説明します。

表 B-39 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-39 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нда 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]	トリガーされた関連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нда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нда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-39 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нда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нда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нда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ндаバイ トドロップ	uint64	レート制限により、セッションレスポндаからドロップしたバイト数。
QoS 適用イン ターフェイス	uint8[16]	レート制限された接続で、レート制限が適用されるインターフェイスの名前。
QoS ルール ID	uint32	接続に適用される QoS ルールの内部 ID 番号(該当する場合)。
ユーザ ID (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-39 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 アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティインテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイルイベントカウント	uint16	同じ秒で発生するファイルイベントを区別するために使用される値。
侵入イベントカウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポンドの国	uint16	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)	uint16	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。

表 B-39 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
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 エージェントを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ エージェント文字列データ ブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびユーザ エージェント フィールドのバイト数を含む)。
ユーザ エージェント	string	セッションのユーザ エージェント ヘッダー フィールドからの情報。
文字列ブロックタイプ	uint32	HTTP リファラを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	HTTP リファラ文字列データ ブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および HTTP リファラ フィールドのバイト数を含む)。
HTTP リファラ	string	ページの発生元のサイト。これは HTTP トラフィック内の参照ヘッダー情報にあります。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
SSL ポリシー ID	uint8[16]	接続を処理した SSL ポリシーの ID 番号。
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルトアクションの ID 番号。

表 B-39 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。 <ul style="list-style-type: none"> 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 1(不明):サーバ証明書のステータスは判別できませんでした。 2(有効):サーバ証明書は有効です。 4(自己署名済み):サーバ証明書は自己署名です。 16(無効な発行者):サーバ証明書に無効な発行者があります。 32(無効な署名):サーバ証明書に無効な署名があります。 64(期限切れ):サーバ証明書は期限切れです。 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 256(取り消し):サーバ証明書は取り消されました。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 <ul style="list-style-type: none"> 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-39 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。 <ul style="list-style-type: none">• 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-39 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	<p>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。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL フロー エラー	uint32	<p>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。</p>

表 B-39 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	<p>SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> 0x00000001 (NSE_FLOW__VALID):他のフィールドを有効にするために設定する必要があります 0x00000002 (NSE_FLOW__INITIALIZED):内部構造が処理可能です 0x00000004 (NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました
文字列ブロックタイプ	uint32	SSL サーバ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	SSL サーバ名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および SSL サーバ名フィールドのバイト数を含む)。

表 B-39 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 サーバ名	string	SSL Client Hello でサーバ名に指定された名前。
SSL URL カテゴリ	uint32	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値。
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできます。
SSL チケット ID	uint8[20]	クライアントとサーバがセッション チケットの使用に同意する場合に使用されるセッション チケットのハッシュ。
SSL チケット ID の長さ	uint8	SSL チケット ID の長さ。チケット ID は 20 バイトより長くすることはできませんが、20 バイト未満であってもかまいません。
ネットワーク分析ポリシー リビジョン	uint8[16]	接続イベントに関連付けられているネットワーク分析ポリシーのリビジョン。
エンドポイントプロファイル ID	uint32	ISE により識別される、接続エンドポイントで使用されるデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
セキュリティグループ ID	uint32	ポリシーに基づいて ISE によりユーザに割り当てられた ID 番号。
ロケーション IPv6	uint8[16]	ISE と通信するインターフェイスの IP アドレス。IPv4 または IPv6 のアドレスを使用できます。
HTTP レスポンス	uint32	HTTP 要求の応答コード。
文字列ブロックタイプ	uint32	DNS クエリを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データブロックのバイト数(文字列ブロックタイプと長さのフィールド用の 8 バイト、および DNS クエリ文字列のバイト数を含む)。
DNS クエリ (DNS Query)	string	DNS サーバに送信されたクエリの内容。
DNS レコードタイプ (DNS Record Type)	uint16	DNS レコードタイプの数値。
DNS レスポンスタイプ	uint16	DNS 応答タイプの数値。
DNS TTL	uint32	DNS レスポンスの存続期間(秒単位)。
シンクホール UUID	uint8[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-39 接続統計データブロック 6.1+ のフィールド(続き)

フィールド	データタイプ	説明
セキュリティインテリジェンスリスト 1	uint32	イベントに関連付けられているセキュリティインテリジェンスリスト。これは、関連メタデータのセキュリティインテリジェンスリストにマップされます。接続には、2つのセキュリティインテリジェンスリストが関連付けられている場合があります。
セキュリティインテリジェンスリスト 2	uint32	イベントに関連付けられているセキュリティインテリジェンスリスト。これは、関連メタデータのセキュリティインテリジェンスリストにマップされます。接続には、2つのセキュリティインテリジェンスリストが関連付けられている場合があります。

レガシーファイルイベントのデータ構造

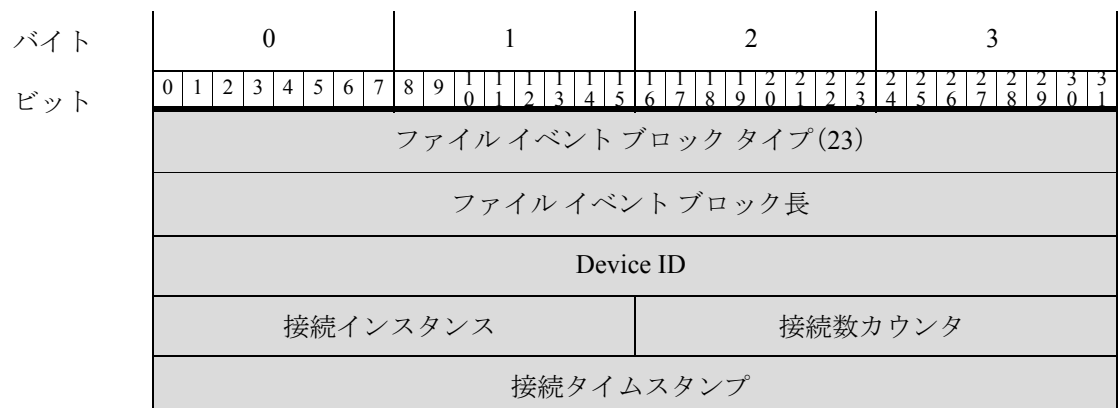
続くいくつかのトピックでは、他のレガシーファイルイベントデータの構造について説明します。

- [ファイルイベント 5.1.1.x \(B-240 ページ\)](#)
- [ファイルイベント 5.2.x \(B-244 ページ\)](#)
- [ファイルイベント 5.3 \(B-249 ページ\)](#)
- [ファイルイベント 5.3.1 \(B-256 ページ\)](#)
- [ファイルイベント 5.4.x \(B-262 ページ\)](#)
- [ファイルイベント SHA ハッシュ 5.1.1 ~ 5.2.x \(B-273 ページ\)](#)

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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
	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	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)																																				

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7		
	アプリケーション ID (続き)								ユーザ ID (User ID)																															
URI	ユーザ ID (続き)								文字列ブロック タイプ (0)																															
	文字列ブロック タイプ (0) (続き)								文字列ブロック長																															
	文字列ブロック長 (続き)								URI...																															
シグネチャ	文字列ブロック タイプ (0)																																							
	文字列ブロック長																																							
	署名...																																							
	送信元ポート (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)																																								

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

表 B-40 ファイルイベントデータブロックのフィールド

フィールド	データ タイプ	説明
ファイル イベント ブロック タイプ	uint32	ファイル イベント データ ブロックを開始します。この値は常に 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。

表 B-40 ファイルイベントデータブロックのフィールド(続き)

フィールド	データタイプ	説明
接続数カウンタ	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	<p>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。</p> <ul style="list-style-type: none"> 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): ソフトウェアはシスコ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): シスコクラウドサービスが要求に応答しませんでした。
操作	uint8	<p>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。</p> <ul style="list-style-type: none"> 1: 検出 2: ブロック 3: マルウェアクラウドルックアップ 4: マルウェアブロック 5: マルウェアホワイトリスト
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
ファイルタイプ ID	uint32	ファイルタイプにマップされている ID 番号。
ファイル名	string	ファイルの名前。
ファイルサイズ(File size)	uint64	ファイルのサイズ(バイト単位)。

表 B-40 ファイルイベントデータブロックのフィールド(続き)

フィールド	データタイプ	説明
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。 <ul style="list-style-type: none"> 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 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の ID 番号。
URI	string	接続の Uniform Resource Identifier (URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> 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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
ファイルイベントブロックタイプ(32)																																								
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								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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
	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 ID (User ID)																											
URI	ユーザ ID (続き)								文字列ブロック タイプ (0)																											
	文字列ブロック タイプ (0) (続き)								文字列ブロック長																											
	文字列ブロック長 (続き)								URI...																											
シグネチャ	文字列ブロック タイプ (0)																																			
	文字列ブロック長																																			
	署名...																																			
	送信元ポート (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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	Web アプリケーション ID(続き)								クライアント アプリケーション ID																															
	クライアント アプリケーション ID(続き)																																							

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

表 B-41 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-41 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	<p>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。</p> <ul style="list-style-type: none"> • 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 シスコ 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 シスコ クラウド サービスが要求に応答しませんでした。
操作	uint8	<p>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。</p> <ul style="list-style-type: none"> • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
ファイルタイプ ID	uint32	ファイルタイプにマップされている ID 番号。
ファイル名	string	ファイルの名前。
ファイルサイズ (File size)	uint64	ファイルのサイズ(バイト単位)。
方向 (Direction)	uint8	<p>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。</p> <ul style="list-style-type: none"> • 1:ダウンロード • 2:アップロード <p>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)。</p>
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 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。

表 B-41 ファイルイベント データ ブロックのフィールド(続き)

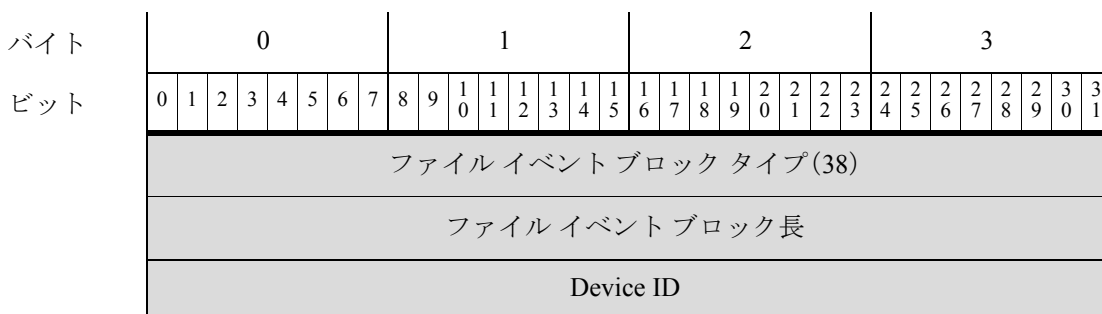
フィールド	データ タイプ	説明
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション 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\(2-13 ページ\)](#)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。



レガシーファイルイベントのデータ構造

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ファイル サイズ (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 ID (User ID)																							
URI	ユーザ ID (続き)								文字列ブロック タイプ (0)																							
	文字列ブロック タイプ (0) (続き)								文字列ブロック長																							
	文字列ブロック長 (続き)								URI...																							
シグネチャ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	署名...																															
	送信元ポート (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)																															

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-42 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。
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。 <ul style="list-style-type: none"> 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 シスコ 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 シスコ クラウド サービスが要求に応答しませんでした。 5 (CUSTOM SIGNATURE): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
SPERO 解析結果	uint8	SPERO 署名がファイル分析で使用されたかどうかを示します。値が 1、2、または 3 であれば、SPERO 分析は使用されました。それ以外の値であれば、SPERO 分析は使用されませんでした。

表 B-42 ファイルイベントデータブロックのフィールド(続き)

フィールド	データタイプ	説明
ファイルストレージステータス	uint8	ファイルの保存ステータス。値は以下のとおりです。 <ul style="list-style-type: none">• 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、解析結果を入力できません

表 B-42 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	<p>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。</p> <ul style="list-style-type: none"> • 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、解析結果を入力できません • 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	<p>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。</p> <ul style="list-style-type: none"> • 1: 検出 • 2: ブロック • 3: マルウェア クラウドルックアップ • 4: マルウェア ブロック • 5: マルウェア ホワイトリスト
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。

表 B-42 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 (3-43 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。 <ul style="list-style-type: none"> 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 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の ID 番号。
URI	string	接続の Uniform Resource Identifier (URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> 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\(2-13 ページ\)](#)を参照してください。ビット 23 を有効にすると、拡張イベントヘッダーがレコードに含まれます。

次の図は、ファイルイベントデータブロックの構造を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイルイベントブロックタイプ(43)																																
ファイルイベントブロック長																																
デバイス ID (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 ID (User ID)																							
URI	ユーザ ID (続き)								文字列ブロック タイプ(0)																							
	文字列ブロック タイプ(0) (続き)								文字列ブロック長																							
	文字列ブロック長 (続き)								URI...																							
シグネチャ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	署名...																															
	送信元ポート (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																							

レガシーファイルイベントのデータ構造

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	アクセスコントロールポリシー UUID(続き)																															
	アクセスコントロールポリシー UUID(続き)																															
	アクセスコントロールポリシー UUID(続き)																															
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)																															
	セキュリティコンテキスト(続き)																															
セキュリティコンテキスト(続き)																																

次の表は、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-43 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。
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-43 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	<p>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。</p> <ul style="list-style-type: none"> • 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 シスコ 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 シスコ クラウド サービスが要求に応答しませんでした。 • 5 (CUSTOM SIGNATURE): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
SPERO 解析結果	uint8	SPERO 署名がファイル分析で使用されたかどうかを示します。値が 1、2、または 3 であれば、SPERO 分析は使用されました。それ以外の値であれば、SPERO 分析は使用されませんでした。
ファイル ストレージ ステータス	uint8	<p>ファイルの保存ステータス。値は以下のとおりです。</p> <ul style="list-style-type: none"> • 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-43 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	<p>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。</p> <ul style="list-style-type: none"> • 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、解析結果を入力できません • 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ため、ファイル キャパシティが処理されました(センサーに保存) • 25(ファイル送信サーバ制限超過によるキャパシティの処理): サーバの速度制限が原因でファイル キャパシティが処理されました • 26(通信障害): クラウド接続失敗が原因でファイル キャパシティが処理されました • 27(未送信): 設定が原因でファイルは送信されていません。

表 B-43 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
		<ul style="list-style-type: none"> 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
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	<p>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。</p> <ul style="list-style-type: none"> 1:検出 2:ブロック 3:マルウェアクラウドルックアップ 4:マルウェアブロック 5:マルウェアホワイトリスト
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
ファイルタイプID	uint32	ファイルタイプにマップされている ID 番号。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、 エンドポイント向け AMP ファイルタイプのメタデータ (3-43 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	<p>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。</p> <ul style="list-style-type: none"> 1:ダウンロード 2:アップロード <p>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)。</p>
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の ID 番号。
URI	string	接続の Uniform Resource Identifier (URI)。

表 B-43 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
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> • 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\(2-13 ページ\)](#)を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

次の図は、ファイル イベント データ ブロックの構造を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイルイベントブロック タイプ (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)																																
SHA ハッシュ (続き)																								ファイル タイプ ID								

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイル名	ファイルタイプ ID(続き)																								文字列ブロックタイプ(0)							
	文字列ブロックタイプ(0)(続き)																								文字列ブロック長							
	文字列ブロック長(続き)																								ファイル名...							
	ファイルサイズ(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 ID(User ID)																							
URI	ユーザ ID(続き)								文字列ブロックタイプ(0)																							
	文字列ブロックタイプ(0)(続き)								文字列ブロック長																							
	文字列ブロック長(続き)								URI...																							
シグネチャ	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	署名...																															
	送信元ポート(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																							

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

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

表 B-44 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。 <ul style="list-style-type: none"> 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 シスコ 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 シスコ クラウド サービスが要求に応答しませんでした。 5 (CUSTOM SIGNATURE): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
SPERO 解析結果	uint8	SPERO 署名がファイル分析で使用されたかどうかを示します。値が 1、2、または 3 であれば、SPERO 分析は使用されました。それ以外の値であれば、SPERO 分析は使用されませんでした。

表 B-44 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。 <ul style="list-style-type: none">• 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、解析結果を入力できません

表 B-44 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	<p>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。</p> <ul style="list-style-type: none"> • 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、解析結果を入力できません • 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-44 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	<p>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。</p> <ul style="list-style-type: none"> 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	<p>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)。</p>
操作	uint8	<p>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。</p> <ul style="list-style-type: none"> 1:検出 2:ブロック 3:マルウェア クラウドルックアップ 4:マルウェア ブロック 5:マルウェア ホワイトリスト 6:クラウドルックアップのタイムアウト 7:カスタム検出 8:カスタム検出ブロック 9:アーカイブ ブロック(深度超過) 10:アーカイブ ブロック(暗号化されている) 11:アーカイブ ブロック(調査エラー)
SHA ハッシュ	uint8[32]	<p>バイナリ形式の SHA-256 ハッシュのファイル。</p>
ファイルタイプ ID	uint32	<p>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(3-43 ページ)を参照してください。</p>
ファイル名	string	<p>ファイルの名前。</p>

表 B-44 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。 <ul style="list-style-type: none"> 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 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の ID 番号。
URI	string	接続の Uniform Resource Identifier (URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> 1: ICMP 4: IP 6: TCP 17: UDP これは現時点では TCP のみです。
アクセスコントロールポリシー UUID	uint8[16]	イベントをトリガーするアクセスコントロールポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号 (該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号 (該当する場合)。
セキュリティコンテキスト	uint8(16)	トラフィックが通過したセキュリティコンテキスト (仮想ファイアウォール) の ID 番号。マルチコンテキストモードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。

表 B-44 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	<p>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。</p> <ul style="list-style-type: none">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 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	<p>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。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブモードで復号不可のセッション」 • 9:「ハンドシェイクエラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
文字列ブロックタイプ	uint32	<p>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。</p>

表 B-44 ファイルイベント データ ブロック 5.4.x のフィールド(続き)

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

ファイルイベント SHA ハッシュ 5.1.1 ~ 5.2.x

eStreamer サービスは、ファイルの SHA ハッシュとそのファイル名とのマッピングのメタデータを含む、ファイル イベント SHA ハッシュ データ ブロックを使用します。ブロック タイプは、シリーズ 2 リストのデータ ブロックの 26 です。これは、ファイル ログ イベントが拡張要求(イベント コード 111)で要求されており、ビット 20 が設定されているかまたはメタデータがイベントバージョン 4 およびイベント コード 21 で要求されているか、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-45 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。

レガシー関連イベントのデータ構造

続くいくつかのトピックでは、他のレガシー関連(コンプライアンス)データの構造について説明します。

- [関連イベント 5.0 ~ 5.0.2 \(B-275 ページ\)](#)
- [関連イベント 5.1 ~ 5.3.x \(B-283 ページ\)](#)

関連イベント 5.0 ~ 5.0.2

関連イベント(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、関連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、それに関連データ 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 関連イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベント タイプ コード 31 およびバージョン 7 を要求します(拡張要求の送信の詳細については、[拡張要求の送信\(2-4 ページ\)](#)を参照してください)。オプションで、最初のイベントストリーム要求メッセージのフラグフィールドでビット 23 を有効にして、拡張イベントヘッダーを含めることができます。また、フラグフィールドでビット 20 を有効にして、ユーザメタデータを含めることもできます。

レコード構造には、シリーズ 1 のブロックである、文字列ブロック タイプが含まれることに注目してください。シリーズ 1 ブロックの詳細については、[ディスカバリ\(シリーズ 1\)ブロック\(4-65 ページ\)](#)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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン(1)																メッセージ タイプ(4)															
	メッセージ長																															
	Netmap ID																レコード タイプ(112)															
	レコード長																															
	eStreamer サーバ タイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
	関連ブロック タイプ(116)																															
	関連ブロック長																															
	Device ID																															
	(関連)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)]																															

レガシー関連イベントのデータ構造

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
文字列ブロック タイプ(0)																																イベント 説明	
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	
送信元 OS フィンガープリント UUID(続き)																																	
送信元 OS フィンガープリント UUID(続き)																																	
送信元 OS フィンガープリント UUID(続き)																																	
送信元 OS フィンガープリント UUID(続き)																								送信元重要度									
送信元重要度(続き)								送信元ユーザ ID																									
送信元ユーザ ID(続き)								送信元ポート																送信元サーバ ID									
送信元サーバ ID(続き)																								宛先 IP (Destination IP)									
宛先 IP(続き)																								着信ホストタイプ									

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
	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 ID (User ID)																																
	接続先ポート																宛先サーバ ID																
	宛先サーバ ID (続き)																ブロック								入力インターフェイス UUID								
	入力インターフェイス UUID (続き)																出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)																出力インターフェイス UUID																
	出力インターフェイス UUID (続き)																入力ゾーン 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																出力ゾーン 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)																																

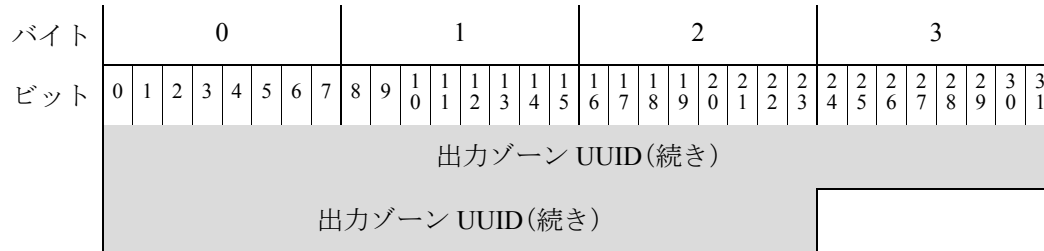


表 B-46 関連イベント データ 5.0 ~ 5.0.2 のフィールド

フィールド	データタイプ	説明
関連ブロックタイプ	uint32	関連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。
関連ブロック長	uint32	関連データブロック長(関連ブロックタイプと長さの 8 バイト、およびそれに続く関連データを含む)。
Device ID	uint32	関連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 (3-37 ページ) を参照してください。
(関連) イベント秒	uint32	関連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	関連イベント ID 番号。
ポリシー ID	uint32	違反された関連ポリシーの 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関連ルールの 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	関連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	関連イベントについての説明。

表 B-46 関連イベントデータ 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	<p>関連イベントが、侵入、ホスト検出、またはユーザ イベントによってトリガーされたかどうかを示します。</p> <ul style="list-style-type: none"> • 1: 侵入 • 2: ホストのディスカバリ • 3: ユーザ
イベント Device ID	uint32	<p>関連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 (3-37 ページ) を参照してください。</p>
シグネチャ ID	uint32	<p>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。</p>
シグネチャジェネレータ ID	uint32	<p>イベントが侵入イベントであった場合、イベントを生成した Firepower システム プリプロセッサまたはルール エンジンの ID 番号を示します。</p>
(トリガー) イベント秒	uint32	<p>関連ポリシー 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)。</p>
(トリガー) イベント マイクロ秒	uint32	<p>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。</p>
イベント ID (Event ID)	uint32	<p>デバイスによって生成されたイベントの ID 番号。</p>
イベントで定義されたマスク	bits[32]	<p>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-47 (B-282 ページ) を参照してください。</p>

表 B-46 関連イベント 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]	<p>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。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40:このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます(ビット 6)。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。 <p>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。</p> <ul style="list-style-type: none"> (0、不明):00x00000 赤(1、脆弱):xxx1xxx, 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-46 関連イベントデータ 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: <ul style="list-style-type: none"> 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、ユーザ定義の重要度値: <ul style="list-style-type: none"> 0: なし 1: 低 2: 中 3: 高
送信元ユーザ ID	uint32	システムにより識別される、送信元ホストにログインしたユーザの ID 番号。
送信元ポート	uint16	イベントの送信元ポート。
送信元サーバ ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
宛先 IP アドレス	uint8[4]	ポリシー違反に関連付けられた宛先ホストの IP アドレス(該当する場合)。宛先 IP アドレスがない場合、この値は 0 になります。
宛先ホストタイプ	uint8	宛先ホストのタイプ: <ul style="list-style-type: none"> 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、ユーザ定義の重要度値: <ul style="list-style-type: none"> 0: なし 1: 低 2: 中 3: 高

表 B-46 関連イベント 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 ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
接続先ポート	uint16	イベントの宛先ポート。
宛先サービス ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
ブロック	uint8	侵入イベントをトリガーしたパケットの処理を示す値。 <ul style="list-style-type: none"> 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]	関連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]	関連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]	関連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]	関連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-47 イベントで定義された値

説明	マスク値
イベント影響フラグ	0x00000001
IP プロトコル	0x00000002
ネットワーク プロトコル	0x00000004
ソース IP	0x00000008
送信元ホスト タイプ	0x00000010
送信元 VLAN ID	0x00000020
送信元フィンガープリント ID	0x00000040
送信元重要度	0x00000080
送信元ポート	0x00000100
送信元サーバ	0x00000200
宛先 IP (Destination IP)	0x00000400
宛先ホスト タイプ	0x00000800

表 B-47 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	0x00010000
送信元ユーザ	0x00020000
宛先ユーザ	0x00040000

関連イベント 5.1 ~ 5.3.x

関連イベント(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、
 関連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
 関連データブロック 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 の関連イベントは、拡張要求によってのみ要求できます。これに対
 してはストリーム要求メッセージでイベントタイプコード 31 およびバージョン 8 を要求しま
 す(拡張要求の送信の詳細については、[拡張要求の送信\(2-4 ページ\)](#)を参照してください)。オプ
 ションで、最初のイベントストリーム要求メッセージのフラグフィールドでビット 23 を有効に
 して、拡張イベントヘッダーを含めることができます。また、フラグフィールドでビット 20 を有
 効にして、ユーザメタデータを含めることもできます。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(112)															
	レコード長																															
	eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場 合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
	関連ブロック タイプ(128)																															
	関連ブロック長																															
	デバイス ID (Device ID)																															

レガシー関連イベントのデータ構造

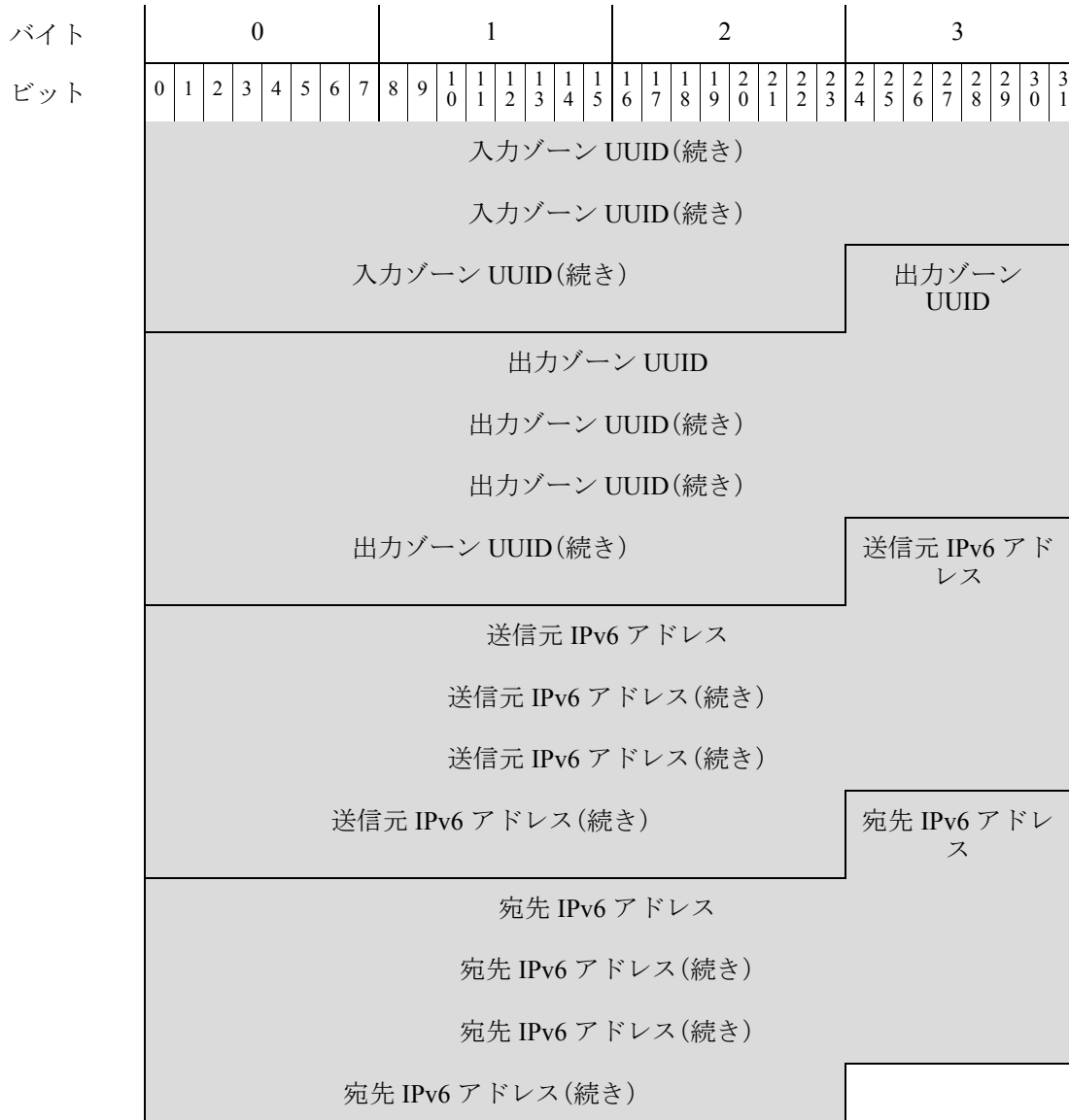
バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	(関連)イベント秒																															
	イベント ID (Event ID)																															
	ポリシー ID																															
	ルール ID																															
	[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																															
	(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							

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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	送信元重要度 (続き)								送信元ユーザ ID																							
	送信元ユーザ ID (続き)								送信元ポート																送信元サーバ ID							
	送信元サーバ ID (続き)																宛先 IP (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 ID (User ID)																															
	接続先ポート																宛先サーバ ID															
	宛先サーバ ID (続き)																ブロック								入力インターフェイス UUID							
	入力インターフェイス UUID (続き)																															
	入力インターフェイス UUID (続き)																															
	入力インターフェイス UUID (続き)																															
	入力インターフェイス UUID (続き)																出力インターフェイス UUID															
	出力インターフェイス UUID (続き)																															
	出力インターフェイス UUID (続き)																															
	出力インターフェイス UUID (続き)																入力ゾーン UUID															
	入力ゾーン UUID																															

レガシー関連イベントのデータ構造



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-48 関連イベント 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
関連ブロックタイプ	uint32	関連イベント 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。
関連ブロック長	uint32	関連データ ブロック長(関連ブロック タイプと長さの 8 バイト、およびそれに続く関連データを含む)。

表 B-48 関連イベントデータ 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	関連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 (3-37 ページ) を参照してください。
(関連) イベント秒	uint32	関連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	関連イベント ID 番号。
ポリシー ID	uint32	違反された関連ポリシーの 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関連ルールの 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	関連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	関連イベントについての説明。
イベントタイプ (Event Type)	uint8	関連イベントが、侵入、ホスト検出、またはユーザ イベントによってトリガーされたかどうかを示します。 <ul style="list-style-type: none"> • 1: 侵入 • 2: ホストのディスクバリエーション • 3: ユーザ
イベントデバイス ID	uint32	関連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 (3-37 ページ) を参照してください。
シグネチャ ID	uint32	イベントが侵入イベントであった場合、イベントに対応するルール ID 番号を示します。そうでない場合、この値は 0 になります。
シグネチャジェネレータ ID	uint32	イベントが侵入イベントであった場合、イベントを生成した Firepower システム プリプロセッサまたはルールエンジンの ID 番号を示します。
(トリガー) イベント秒	uint32	関連ポリシー 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-48 関連イベント 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	シスコ デバイスによって生成されたイベントの ID 番号。
イベントで定義されたマスク	bits[32]	このフィールドに設定されたビットは、メッセージ内の続くどのフィールドが有効であるかを示します。各ビット値のリストの詳細については、表 B-47(B-282 ページ)を参照してください。
イベント影響フラグ	bits[8]	<p>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。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) <p>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。</p> <ul style="list-style-type: none"> (0、不明):00x00000 赤(1、脆弱):xxx1xxx, 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-48 関連イベントデータ 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(1-5 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: <ul style="list-style-type: none"> • 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、ユーザ定義の重要度値: <ul style="list-style-type: none"> • 0: なし • 1: 低 • 2: 中 • 3: 高
送信元ユーザ ID	uint32	システムにより識別される、送信元ホストにログインしたユーザの ID 番号。
送信元ポート	uint16	イベントの送信元ポート。
送信元サーバ ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
宛先 IP アドレス	uint8[4]	このフィールドは予約済みですが、設定されておりません。宛先 IPv4 アドレスは、宛先 IPv6 アドレスフィールドに保存されます。詳細については、 IP アドレス(1-5 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: <ul style="list-style-type: none"> • 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-48 関連イベント 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、ユーザ定義の重要度値: <ul style="list-style-type: none"> • 0:なし • 1:低 • 2:中 • 3:高
宛先ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
接続先ポート	uint16	イベントの宛先ポート。
宛先サービス ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
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。 <ul style="list-style-type: none"> • 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]	関連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]	関連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]	関連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]	関連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

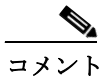
これらの構造を要求するには、ホスト要求メッセージを使用する必要があります。レガシー構造を要求するには、古い形式のホスト要求メッセージを使用する必要があります。詳細については、[ホスト要求メッセージの形式\(2-29 ページ\)](#)を参照してください。

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\(B-291 ページ\)](#)
- [フルホストプロファイルデータブロック 5.1.1\(B-301 ページ\)](#)
- [フルホストプロファイルデータブロック 5.2.x\(B-312 ページ\)](#)
- [ホストプロファイルデータブロック 5.1.x\(B-327 ページ\)](#)
- [IP 範囲仕様データブロック 5.0 ~ 5.1.1.x\(B-333 ページ\)](#)
- [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\(B-334 ページ\)](#)

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。



コメント

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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
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																

レガシーホストデータ構造

バイト	0								1								2								3														
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	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																																							
サーバフィンガープリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																																						
	オペレーティングシステムフィンガープリントブロック長																																						
	オペレーティングシステムサーバフィンガープリントデータ																																						
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 ネットワーク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							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	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(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のフィンガープリントデータ...																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
(TCP)フルサーバデータ	リストブロックタイプ(11)...																															
	リストブロック長...																															
	(TCP)全サーバデータブロック(104)*																															
(UDP)全サーバデータ	リストブロックタイプ(11)																															
	リストブロック長																															
	(UDP)全サーバデータブロック(104)*																															
ネットワークプロトコルデータ	リストブロックタイプ(11)																															
	リストブロック長																															
	(ネットワーク)プロトコルデータブロック(4)*																															
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)																フルホストクライアントアプリケーションデータブロック(112)*															
NetBIOS [名前(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							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	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-49 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 (IP Address)]	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 データを送信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-49 フルホストプロファイルレコード 5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステム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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	サーバフィンガープリントを使用して特定されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(サーバフィンガープリント)データブロック*	変数 (variable)	サーバフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	クライアントフィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(クライアントフィンガープリント)データブロック*	変数 (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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。

表 B-49 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)	シスコ脆弱性データベース(VDB)のフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(VDB)ネイティブフィンガープリント2)データブロック*	変数(variable)	シスコ脆弱性データベース(VDB)のフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	ユーザが追加したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(ユーザフィンガープリント)データブロック*	変数(variable)	ユーザが追加したホストのオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	脆弱性スキャナによって追加されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。

表 B-49 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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	アプリケーションによって追加されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(アプリケーションフィンガープリント)データブロック*	変数 (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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	フィンガープリント競合解決から選択したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(競合フィンガープリント)データブロック*	変数 (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+(4-169 ページ) を参照してください。
リストブロックタイプ	uint32	TCP サービスデータを伝送する全サーバデータブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リストブロックタイプフィールド、リストブロック長フィールド、すべてのカプセル化全サーバデータブロック長から成る 8 バイトを含みます。
(TCP)全サーバデータブロック*	変数 (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データブロックのリスト。このデータブロックの説明の詳細については、 フルホストサーバデータブロック 4.10.0+(4-148 ページ) を参照してください。

表 B-49 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データブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リストブロックタイプフィールド、リストブロック長フィールド、すべてのカプセル化全サーバデータブロック長から成る 8 バイトを含みます。
(UDP)全サーバデータブロック*	変数 (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データブロックのリスト。このデータブロックの説明の詳細については、 フルホストサーバデータブロック 4.10.0+(4-148 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-49 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)

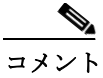
フィールド	データタイプ	説明
ホストタイプ	uint32	ホストのタイプを示します。次の値を指定します。 <ul style="list-style-type: none"> 0 — ホスト 1 — ルータ 2 — ブリッジ 3 — NAT(ネットワークアドレス変換デバイス) 4 — LB(ロードバランサー)
ビジネス上の重要度	uint16	ビジネスに対するホストの重要度を示します。
VLAN ID (Admin. VLAN ID)	uint16	ホストがいずれの VLAN メンバーであることを示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグ内でカプセル化されるパケットのタイプ。
VLAN プライオリティ	uint8	VLAN タグに含まれるプライオリティ値。
汎用リストブロックタイプ	uint32	クライアントアプリケーションデータを伝送するホスト脆弱性データブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化クライアントアプリケーションデータブロックを含む汎用リストデータブロック内のバイト数。
全ホストクライアントアプリケーションデータブロック*	変数 (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+(4-162 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-49 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)	シスコ脆弱性データベース(VDB)で特定された脆弱性に関するホスト脆弱性データブロックのリスト。このデータブロックの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+(4-120 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ナから送信され、シスコ脆弱性データベース(VDB)でカタログされているホストの脆弱性に関する情報を含むホスト脆弱性データブロック。このデータブロックの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+(4-120 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ナ ID であり、シスコによって検出された ID ではない点にご注意ください。このデータブロックの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+(4-120 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 (4-88 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。



コメント

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							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット	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																															
サーバフィンガープリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムサーバフィンガープリントデータ																															
	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...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
VDB ネイ ティブフィン 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 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 (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 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																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
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のフィンガープリントデータ...																															
(TCP)フル サーバデータ	リストブロックタイプ(11)...																															
	リストブロック長...																															
	(TCP)全サーバデータブロック(104)*																															
(UDP)全 サーバデー タ	リストブロックタイプ(11)																															
	リストブロック長																															
	(UDP)全サーバデータブロック(104)*																															
ネットワーク プロトコル データ	リストブロックタイプ(11)																															
	リストブロック長																															
	(ネットワーク)プロトコルデータブロック(4)*																															
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																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	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)																フルホストクライアントアプリケーションデータブロック(112)*															
NetBIOS [名前(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)*																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
属性 (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-50 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 (IP Address)]	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	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステム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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	サーバフィンガープリントを使用して特定されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(サーバフィンガープリント)データブロック*	変数 (variable)	サーバフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。

表 B-50 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	クライアントフィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(クライアントフィンガープリント)データブロック*	変数(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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(VDB)ネイティブフィンガープリント1)データブロック*	変数(variable)	シスコ脆弱性データベース(VDB)のフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(VDB)ネイティブフィンガープリント2)データブロック*	変数(variable)	シスコ脆弱性データベース(VDB)のフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。

表 B-50 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	ユーザが追加したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(ユーザフィンガープリント)データブロック*	変数(variable)	ユーザが追加したホストのオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	脆弱性スキャナによって追加されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	アプリケーションによって追加されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(アプリケーションフィンガープリント)データブロック*	変数(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+(4-169 ページ) を参照してください。

表 B-50 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	フィンガープリント競合解決から選択したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(競合フィンガープリント)データブロック*	変数(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+(4-169 ページ) を参照してください。
リストブロックタイプ	uint32	TCP サービスデータを伝送する全サーバデータブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リストブロックタイプフィールド、リストブロック長フィールド、すべてのカプセル化全サーバデータブロック長から成る 8 バイトを含みます。
(TCP)全サーバデータブロック*	変数(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データブロックのリスト。このデータブロックの説明の詳細については、 フルホストサーバデータブロック 4.10.0+(4-148 ページ) を参照してください。
リストブロックタイプ	uint32	UDP サービスデータを伝送する全サーバデータブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リストブロックタイプフィールド、リストブロック長フィールド、すべてのカプセル化全サーバデータブロック長から成る 8 バイトを含みます。
(UDP)全サーバデータブロック*	変数(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データブロックのリスト。このデータブロックの説明の詳細については、 フルホストサーバデータブロック 4.10.0+(4-148 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-50 フルホストプロファイルレコード 5.1.1 のフィールド(続き)

フィールド	データタイプ	説明
リストブロックタイプ	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。 <ul style="list-style-type: none"> • 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	ホストがいずれの VLAN メンバーであるかを示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグ内でカプセル化されるパケットのタイプ。
VLAN プライオリティ	uint8	VLAN タグに含まれるプライオリティ値。
汎用リストブロックタイプ	uint32	クライアントアプリケーションデータを伝送するホスト脆弱性データブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化クライアントアプリケーションデータブロックを含む汎用リストデータブロック内のバイト数。

表 B-50 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)

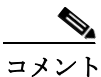
フィールド	データタイプ	説明
全ホストクライアントアプリケーションデータブロック*	変数 (variable)	クライアントアプリケーションデータブロックのリスト。このデータブロックの説明の詳細については、 フルクライアントアプリケーションデータブロック 5.0+(4-162 ページ) を参照してください。
文字列ブロックタイプ	uint32	ホスト NetBIOS 名の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロックタイプフィールドおよび文字列ブロック長フィールドの 8 バイトを含む文字列データブロック内のバイト数と NetBIOS 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)	シスコ脆弱性データベース (VDB) で特定された脆弱性に関するホスト脆弱性データブロックのリスト。このデータブロックの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+(4-120 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ナから送信され、シスコ脆弱性データベース (VDB) でカタログされているホストの脆弱性に関する情報を含むホスト脆弱性データブロック。このデータブロックの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+(4-120 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-50 フルホストプロファイルレコード 5.1.1 のフィールド(続き)

フィールド	データタイプ	説明
(サードパーティスキャン)ホスト脆弱性データブロック*	変数 (variable)	サードパーティのスキ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ナ ID であり、シスコによって検出された ID ではない点にご注意ください。このデータブロックの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+(4-120 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 (4-88 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。 <ul style="list-style-type: none"> 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。



コメント

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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
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																																								

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット	ホスト ID (Host ID)																															
	ホスト ID (続き)																															
	ホスト ID (続き)																															
	ホスト ID (続き)																															
IP アドレス	リストブロック タイプ (11)																															
	リストブロック長																															
	IP アドレス データブロック (143)*																															
	ホップ								汎用リストブロック タイプ (31)																							
	汎用リストブロック タイプ (続き)								汎用リストブロック長																							
OS から取得したフィンガープリント	汎用リストブロック長 (続き)								オペレーティングシステムフィンガープリントブロック タイプ (130)*																							
	OS フィンガープリントブロック タイプ (130)* (続き)								オペレーティングシステムフィンガープリントブロック長																							
	OS フィンガープリントブロック長 (続き)								オペレーティングシステムから取得したフィンガープリントデータ...																							
	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
サーバフィンガープリント	オペレーティングシステムフィンガープリントブロック タイプ (130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムサーバフィンガープリントデータ																															
	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							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
クライアント フィンガー プリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムクライアント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 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 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(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)																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	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																															
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 フィンガー プリント	オペレーティング システム フィンガープリントブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム IPv6 サーバ フィンガープリント データ...																															
	汎用リストブロック タイプ(31)																															
	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...																															

レガシーホストデータ構造

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
IPv6 DHCP フィンガー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム IPv6 DHCP フィンガープリント データ...																															
	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
ユーザ エ ジェント フィンガ ー プリント	オペレーティング システム フィンガープリント ブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム ユーザ エージェント フィンガープリント データ...																															
(TCP)全サー バデー タ	リストブロック タイプ(11)...																															
	リストブロック長...																															
	(TCP)全サーバデータブロック (104)*																															
(UDP)全 サーバデー タ	リストブロック タイプ(11)																															
	リストブロック長																															
	(UDP)全サーバデータブロック (104)*																															
ネットワー ク プロトコ ル デー タ	リストブロック タイプ(11)																															
	リストブロック長																															
	(ネットワーク)プロトコルデータブロック (4)*																															
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)*																															

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
MAC アドレス データ	リストブロックタイプ(11)																																
	リストブロック長																																
	ホストMACアドレスデータブロック(95)*																																
	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							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
サードパーティ ディスクスキャン 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-51 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。
[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 (4-104 ページ) を参照してください。
ホップ	uint8	ホストからデバイスへのネットワークホップ数。
汎用リストブロックタイプ	uint32	ホストの既存のフィンガープリントから取得したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	サーバフィンガープリントを使用して特定されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(サーバフィンガープリント)データブロック*	変数 (variable)	サーバフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。

表 B-51 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	クライアントフィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(クライアントフィンガープリント)データブロック*	変数(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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(VDB)ネイティブフィンガープリント1)データブロック*	変数(variable)	シスコ脆弱性データベース(VDB)のフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(VDB)ネイティブフィンガープリント2)データブロック*	変数(variable)	シスコ脆弱性データベース(VDB)のフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。

表 B-51 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	ユーザが追加したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(ユーザフィンガープリント)データブロック*	変数(variable)	ユーザが追加したホストのオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	脆弱性スキャナによって追加されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	アプリケーションによって追加されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(アプリケーションフィンガープリント)データブロック*	変数(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+(4-169 ページ) を参照してください。

表 B-51 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	フィンガープリント競合解決から選択したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(競合フィンガープリント)データブロック*	変数(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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	モバイルデバイスフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(モバイル)データブロック*	変数(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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	IPv6 サーバフィンガープリントを使用して特定されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(IPv6 サーバフィンガープリント)データブロック*	変数(variable)	IPv6 サーバフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 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。

表 B-51 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	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(IPv6クライアントフィンガープリント)データブロック*	変数(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+(4-169 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	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(IPv6 DHCP)データブロック*	変数(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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	ユーザエージェントフィンガープリントで識別するフィンガープリントデータを搬送するオペレーティングシステムフィンガープリントデータブロックで構成される汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(ユーザエージェント)データブロック*	変数(variable)	ユーザエージェントフィンガープリントで識別したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-169 ページ) を参照してください。
リストブロックタイプ	uint32	TCP サービスデータを伝送する全サーバデータブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リストブロックタイプフィールド、リストブロック長フィールド、すべてのカプセル化全サーバデータブロック長から成る 8 バイトを含みます。
(TCP)全サーバデータブロック*	変数(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データブロックのリスト。このデータブロックの説明の詳細については、 フルホストサーバデータブロック 4.10.0+(4-148 ページ) を参照してください。

表 B-51 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	UDP サービス データを伝送する全サーバデータブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リストブロックタイプフィールド、リストブロック長フィールド、すべてのカプセル化全サーバデータブロック長から成る 8 バイトを含みます。
(UDP)全サーバデータブロック*	変数 (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データブロックのリスト。このデータブロックの説明の詳細については、フルホストサーバデータブロック 4.10.0+(4-148 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-51 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)

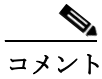
フィールド	データタイプ	説明
ホストタイプ	uint32	ホストのタイプを示します。次の値を指定します。 <ul style="list-style-type: none"> • 0 — ホスト • 1 — ルータ • 2 — ブリッジ • 3 — NAT(ネットワークアドレス変換デバイス) • 4 — LB(ロードバランサー)
ビジネス上の重要度	uint16	ビジネスに対するホストの重要度を示します。
VLAN ID (Admin. VLAN ID)	uint16	ホストがいずれの VLAN メンバーであるかを示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグ内でカプセル化されるパケットのタイプ。
VLAN プライオリティ	uint8	VLAN タグに含まれるプライオリティ値。
汎用リストブロックタイプ	uint32	クライアントアプリケーションデータを伝送するホスト脆弱性データブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化クライアントアプリケーションデータブロックを含む汎用リストデータブロック内のバイト数。
全ホストクライアントアプリケーションデータブロック*	変数 (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+(4-162 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-51 フルホストプロフィールレコード 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
(VDB)ホスト脆弱性データブロック*	変数 (variable)	シスコ脆弱性データベース(VDB)で特定された脆弱性に関するホスト脆弱性データブロックのリスト。このデータブロックの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+ (4-120 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ナから送信され、シスコ脆弱性データベース(VDB)でカタログされているホストの脆弱性に関する情報を含むホスト脆弱性データブロック。このデータブロックの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+ (4-120 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ナ ID であり、シスコによって検出された ID ではない点にご注意ください。このデータブロックの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+ (4-120 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 (4-88 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。



コメント

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を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ホストプロファイルブロックタイプ(132)																															
	ホストプロファイルブロック長																															
	[IPアドレス(IP Address)]																															
サーバフィンガープリント	ホップ								プライマリ/セカンダリ								汎用リストブロックタイプ(31)															
	汎用リストブロックタイプ(続き)																汎用リストブロック長															
	汎用リストブロック長(続き)																サーバフィンガープリントデータブロック*															
クライアントフィンガープリント	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	クライアントフィンガープリントデータブロック*																															
SMBフィンガープリント	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	SMBフィンガープリントデータブロック*																															
DHCPフィンガープリント	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	DHCPフィンガープリントデータブロック*																															

レガシーホストデータ構造

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
モバイル 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 ブロック*	リストブロック タイプ(11)																																TCP のリス ト サーバ
	リストブロック長																																
	TCP サーバデータ ブロック																																
UDP サーバ ブロック*	リストブロック タイプ(11)																																UDP のリス ト サーバ
	リストブロック長																																
	UDP サーバデータ ブロック																																
ネットワーク プロトコルブ ロック*	リストブロック タイプ(11)																																ネットワー クのリス ト プロトコル
	リストブロック長																																
	ネットワーク プロトコルデータ ブロック																																
トランス ポート (Transport) プロトコル ブロック*	リストブロック タイプ(11)																																トランスポー トリス ト プロトコル
	リストブロック長																																
	トランスポート プロトコルデータ ブロック																																
MAC アドレ ス ブロック*	リストブロック タイプ(11)																																MAC のリス ト アドレス
	リストブロック長																																
	ホスト MAC アドレス データ ブロック																																
最終検出時のホスト																																	
ホストタイプ																																	
Mobile								改造								VLAN の有無								VLAN ID (Admin. VLAN ID)									

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
クライアントアプリケーションデータ	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-52 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。 <ul style="list-style-type: none"> 0: ホストはプライマリ ネットワークにあります。 1: ホストはセカンダリ ネットワークにあります。
汎用リストブロックタイプ	uint32	サーバフィンガープリントを使用して特定されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。

表 B-52 ホストプロファイルデータブロック 5.1.x のフィールド(続き)

フィールド	データタイプ	説明
オペレーティングシステムフィンガープリント(サーバフィンガープリント)データブロック*	変数(variable)	サーバフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	クライアントフィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(クライアントフィンガープリント)データブロック*	変数(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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	SMB フィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。
オペレーティングシステムフィンガープリント(SMB フィンガープリント)データブロック*	変数(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+(4-169 ページ) を参照してください。
汎用リストブロックタイプ	uint32	DHCP フィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。

表 B-52 ホストプロファイルデータブロック 5.1.x のフィールド(続き)

フィールド	データタイプ	説明
オペレーティングシステムフィンガープリント(DHCPフィンガープリント)データブロック*	変数(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+(4-169 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+(4-169 ページ) を参照してください。
リストブロックタイプ	uint32	TCPサーバデータを伝えるサーバデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバデータブロックを加えた値です。 このフィールドには、ゼロ以上のサーバデータブロックが続きます。
TCPサーバデータブロック	変数(variable)	TCPサーバを記述するホストサーバデータブロック(旧バージョンの製品で説明)。
リストブロックタイプ	uint32	UDPサーバデータを伝えるサーバデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバデータブロックを加えた値です。 このフィールドには、ゼロ以上のサーバデータブロックが続きます。
UDPサーバデータブロック	uint32	UDPサーバを記述するホストサーバデータブロック(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。

表 B-52 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)。
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。 <ul style="list-style-type: none"> • 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。

表 B-52 ホストプロファイルデータブロック 5.1.x のフィールド(続き)

フィールド	データタイプ	説明
VLAN の有無	uint8	VLAN が存在するかどうかを示します。 <ul style="list-style-type: none"> 0: はい 1: いいえ
VLAN ID (Admin. VLAN ID)	uint16	ホストがいずれの VLAN メンバーであるかを示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグ内でカプセル化されるパケットのタイプ。
VLAN プライオリティ	uint8	VLAN タグに含まれるプライオリティ値。
汎用リストブロックタイプ	uint32	クライアントアプリケーションデータを伝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+(4-162 ページ) を参照してください。
文字列ブロックタイプ	uint32	NetBIOS 名の文字列データブロックを開始します。この値は文字列データを示す 0 に設定されます。
文字列ブロック長	uint32	NetBIOS 名データブロックのバイト数を示します(文字列ブロックタイプと長さのフィールド用の 8 バイト、および NetBIOS 名のバイト数を含む)。
NetBIOS 文字列データ	変数	ホストプロファイルに記述されているホストの NetBIOS 名が含まれます。

IP 範囲仕様データブロック 5.0 ~ 5.1.1.x

IP 範囲仕様データブロックは、一定範囲内の IP アドレスを伝えます。IP 範囲仕様データブロックは、ユーザプロトコル、ユーザクライアントアプリケーション、アドレス指定、ユーザ製品、ユーザサーバ、ユーザホスト、ユーザ脆弱性、ユーザ重要度、およびユーザ属性値の各データブロックで使用されます。IP 範囲仕様データブロックのブロックタイプは 61 です。

次の図は、IP 範囲仕様データブロックの形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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 範囲仕様ブロック タイプ (61)																															
	IP 範囲仕様ブロック長																															
	IP 範囲の開始																															
	IP 範囲の終了																															

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-53 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	アクセスコントロールポリシールール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-54 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 (Reason)	uint16	イベントをトリガーしたルールの理由の番号。
文字列ブロックタイプ	uint32	アクセスコントロールポリシールール理由の説明を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	ルールの理由の説明。



数値

- 5.1.1+ のユーザクライアントアプリケーションデータブロック [4-98](#)
- 5.2 以上のルールドキュメントのデータブロック [3-111](#)
- 5.2+ の IP 範囲仕様データブロック* [4-101](#)
- 6.0 以上のアクセスコントロールポリシーの理由データブロック [3-82](#)
- 6.0+ の情報データユーザブロック [4-198](#)

B

- BLOB データブロック
- シリーズ 1 [4-76](#)
 - シリーズ 2 [3-63](#)

E

- eStreamer メッセージヘッダー形式 [2-8](#)

I

- ICMP コードのデータブロック [3-71](#)
- ICMP タイプのデータブロック [3-70](#)
- IP アドレス変更メッセージ [4-50](#)
- IP 範囲仕様データブロック 5.0 ~ 5.1.1.x [B-332](#)
- IP レピュテーションカテゴリのデータブロック [3-85](#)

M

- MAC アドレスメッセージ [4-53](#)
- MAC アドレス指定データブロック [4-105](#)
- MAC 情報変更メッセージ [4-53](#)

N

- NetBIOS 名を変更メッセージ [4-55](#)

O

- OS 情報更新メッセージ [4-51](#)
- OS 信頼度更新メッセージ [4-51](#)

T

- TCP サーバ情報更新メッセージ [4-48](#)
- TCP サーバ信頼度更新メッセージ [4-48](#)
- TCP ポートクローズメッセージ [4-52](#)
- TCP ポートタイムアウトメッセージ [4-52](#)

U

- UDP サーバ情報更新メッセージ [4-48](#)
- UDP サーバ信頼度更新メッセージ [4-48](#)
- UDP ポートクローズメッセージ [4-52](#)
- UDP ポートタイムアウトメッセージ [4-52](#)
- URL カテゴリ統計 [4-25](#)
- URL レピュテーションレコード [4-26](#)
- UUID 文字列マッピングのデータブロック [3-66](#)

V

- VLAN タグ情報更新メッセージ [4-54](#)
- VLAN データブロック [4-82](#)

W

Web アプリケーション データ ブロック

5.0+ [4-125](#)

Web アプリケーション レコード [4-22](#)

あ

アイデンティティ タイムアウト メッセージ [4-63](#)

アイデンティティ データ ブロック [4-121](#)

アイデンティティ 競合 メッセージ [4-63](#)

アクセス コントロール ポリシー ルール ID のメタ
データ ブロック [3-68](#)

アクセス コントロール ポリシー ルール ID マッピング
のデータ ブロック [3-68](#)

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-333](#)

アクセス コントロール ポリシー名のデータ
ブロック [3-83](#)

アクセス コントロール ポリシー名のレコード [3-34](#)

アクセス コントロール ルール ID レコード [3-35](#)

アクセス コントロール ルール アクション レコー
ド [4-24](#)

アクセス コントロール ルール データ ブロッ
ク [4-209](#)、[4-214](#)

アクセス コントロール ルール理由データ
ブロック 5.1+ [4-211](#)、[4-215](#)

アクセス コントロール ルール理由レコード [4-27](#)、
[4-29](#)、[4-30](#)、[4-32](#)

アドレス指定データ ブロック [4-105](#)

い

イベント ストリーム 要求メッセージの形式 [2-11](#)

イベント データ メッセージの形式 [2-19](#)

イベント 追加データ メッセージの形式 [2-26](#)

インターフェイス名レコード [3-33](#)

え

エラー メッセージの形式 [2-10](#)

エンドポイント プロファイルのデータ ブロック [3-74](#)

お

オペレーティング システム データ ブロック
3.5+ [4-92](#)

オペレーティング 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-133](#)

5.1+ [4-169](#)

オペレーティング システム フィンガープリント デー
タ ブロック 5.1+ [4-169](#)

か

管理対象デバイス レコードのメタデータ [3-37](#)

く

クライアント アプリケーション メッセージ [4-50](#)

クライアント アプリケーション メッセージの
削除 [4-61](#)

クライアント アプリケーション メッセージの
追加 [4-61](#)

クライアント アプリケーション レコード [4-10](#)

け

検出 イベント メッセージ ヘッダー [2-23](#)

検出 イベント メッセージの形式 [2-22](#)

こ

更新 バナー メッセージ [4-55](#)

さ

- サードパーティ スキャナ脆弱性レコード **4-19**
- サーババナー データ ブロック **4-82**
- サーバ メッセージ **4-48**
- サーバ レコード **4-16**
- サーバ情報データ ブロック
4.10.x、5.0 ～ 5.0.2 **4-152**
- 最後の確認日時ホスト メッセージ **4-47**
- サブサーバ データ ブロック **4-78**

し

- 集合型セキュリティ インテリジェンス クラウド名のレコード **3-39**
- 重要度レコード データ構造 **4-13**
- 新規 IP 対 IP トラフィック メッセージ **4-50**
- 新規 TCP サーバ メッセージ **4-48**
- 新規 UDP サーバ メッセージ **4-48**
- 新規ネットワーク プロトコル メッセージ **4-49**
- 新規ホスト メッセージ **4-47**
- 侵入イベント メッセージの形式 **2-21**
- 侵入イベント レコード
 - 5.0.w.x **B-14**
 - 5.0.x ～ 5.1 (IPv4) **B-2**
 - 5.0.x ～ 5.1 (IPv6) **B-8**
 - 5.1.1.x **B-26**
 - 5.3 **B-20**
 - 5.3.1 **B-32**
 - 5.4.x **B-39**
- 侵入イベント レコード 5.2.x **B-14**
- 侵入イベント レコード 5.3 **B-20**
- 侵入イベント レコード 5.3.1 **B-32**
- 侵入イベント レコード 6.0 以上 **3-9**
- 侵入イベント追加データのメタデータレコード **330**
- 侵入イベント追加データレコード **3-28**
- 侵入影響アラート レコード **B-48**
- 侵入の影響アラート レコード 5.3 以上 **3-18**
- 侵入ポリシー名レコード **4-23**

す

- スキャン タイプ レコード **4-15**
- スキャン結果データ ブロック
5.0 ～ 5.1.1.x **B-99**
5.2+ **4-143**
- スキャン結果を追加メッセージ **4-62**
- スキャン脆弱性データ ブロック
4.10.0+ **4-159**
- ストリーミング イベント タイプ **2-40**
- ストリーミング サービス要求 **2-38**
- ストリーミング サービス要求のデータ構造 **2-38**
- ストリーミング情報メッセージの形式 **2-36**
- ストリーミング要求メッセージの形式 **2-37**

せ

- 脆弱性レコード **4-10**
- 整数型 (INT32) データ ブロック **4-81**
- セカンダリ ホスト更新データ ブロック **4-123**
- 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+ **4-213**
- セキュリティ インテリジェンス カテゴリレコード **4-34**
- 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**
- セキュリティ ゾーン名レコード **3-31**
- 接続イベント メッセージの形式 **2-24**
- 接続チャンク データ ブロック 5.0 ～ 5.1 **B-153**
- 接続チャンク データ ブロック 5.1.1+ **4-107、B-154**
- 接続チャンク メッセージ **4-57**
- 接続統計データ ブロック
5.0 ～ 5.0.2 **B-135**
5.1.1.x **B-156**
5.1+ **B-140**
5.2.x **B-146**
5.3 **B-163**
5.3.1 **B-170**
5.4 **B-177**
5.4.1 **B-191**

6.0+ [4-126](#), [B-205](#), [B-222](#)接続統計データ メッセージ [4-56](#)

そ

ソース アプリケーション レコード [4-18](#)ソース タイプ レコード [4-17](#)ソース ディテクタ レコード [4-18](#)関連イベント メッセージの形式 [2-24](#)

関連イベント レコード

5.0 ~ 5.0.2 [B-275](#)5.1 ~ 5.3.x [B-283](#)5.4+ [3-45](#)関連ポリシー レコード [3-25](#)関連ルール レコード [3-26](#)関連レコード ヘッダーの形式 [2-25](#)属性値データ ブロック [4-88](#)属性アドレス データ ブロック [4-84](#)属性指定データ ブロック [4-102](#)

属性定義データ ブロック

4.7+ [4-94](#)属性リスト項目データ ブロック [4-87](#)属性レコード [4-14](#)

て

データ ブロック ヘッダーの形式 [2-28](#)ディスカバリ イベント ヘッダー 5.0 ~ 5.1.1.x [B-94](#)ディスカバリ イベント ヘッダー 5.2+ [4-42](#)

な

名前説明マッピングのデータ ブロック [3-67](#)

ぬ

ヌル メッセージの形式 [2-9](#)

ね

ネットワーク プロトコル レコード [4-13](#)

は

パケット レコードのデータ構造

4.8.0.2+ [3-7](#)

汎用スキャン結果データ ブロック

4.10.0+ [4-157](#)

汎用リストのデータ ブロック

シリーズ 1 [4-78](#)シリーズ 2 [3-65](#)

ふ

ファイル イベント 5.3 [B-249](#)フィックス リスト データ ブロック [4-109](#)フィンガープリント レコード [4-8](#)プライオリティ レコード [3-8](#)ブリッジ/ルータとして識別したホスト
メッセージ [4-54](#)フル サーバ情報データ ブロック [4-154](#)フル サブサーバ データ ブロック [4-89](#)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+ [4-162](#)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+ [4-162](#)フル ホスト サーバ データ ブロック 4.10.0+ [4-148](#)

フル ホスト プロファイル データ ブロック

5.0 ~ 5.0.2 [B-291](#)5.1.1 [B-301](#)5.2.x [B-312](#)5.3+ [5-1](#)プロトコル データ ブロック [4-80](#)プロトコル メッセージの削除 [4-61](#)プロトコル メッセージの追加 [4-61](#)

分類レコード

4.6.1+ [3-23](#)

ほ

- ホスト IP アドレス データ ブロック [4-104](#)
- ホスト IP アドレス変更メッセージ [4-50](#)
- ホスト IP アドレスを再利用メッセージ [4-52](#)
- ホスト MAC アドレス データ ブロック 4.9+ [4-122](#)
- 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+ [4-164](#)
- ホスト サーバ データ ブロック
 - 4.10.0+ [4-146](#)
- ホスト タイムアウト メッセージ [4-52](#)
- ホスト データ メッセージの形式 [2-35](#)
- ホスト プロファイル データ ブロック 5.1.x [B-326](#)
- ホスト プロファイル データ ブロック 5.2+ [4-172](#)
- ホスト 脆弱性 データ ブロック
 - 4.9.0+ [4-120](#)
- ホスト 属性地 メッセージ [4-60](#)
- ホスト 属性 メッセージ [4-59](#)
- ホスト 属性 メッセージの更新 [4-59](#)
- ホスト 属性 メッセージの削除 [4-59](#)
- ホスト 属性 メッセージの追加 [4-59](#)
- ホストの追加 MAC を検出メッセージ [4-53](#)
- ホスト 要求 メッセージの形式 [2-29](#)
- ホストを削除
 - ホスト 上限に到達メッセージ [4-52](#)
- ホストをドロップ
 - ホスト 上限に到達メッセージ [4-52](#)
- ホップ変更メッセージ [4-52](#)
- ポリシー エンジン制御メッセージ データ ブロック [4-93](#)
- ポリシー制御の概要 [4-56](#)

ま

- マルウェア イベント データ ブロック 5.2.x [B-61](#)
- マルウェア イベント データ ブロック 5.3.1 [B-76](#)
- マルウェア イベント データ ブロック 5.4.x [B-83](#)
- マルウェア イベント レコード 5.1.1 以上 [3-38](#)

- マルウェア イベントのデータ ブロック 5.1 [B-51](#)
- マルウェア イベントのデータ ブロック 5.1.1.x [B-55](#)
- マルウェア イベントのデータ ブロック 5.3 [B-68](#)
- マルウェア イベントのデータ ブロック 6.0以上 [3-97](#)
- マルチ ホスト データ メッセージの形式 [2-35](#)

め

- メタデータ メッセージの形式 [2-21](#)
- メッセージ バンドルの形式 [2-44](#)

も

- 文字列情報 データ ブロック [4-83](#)
- 文字列 データ ブロック
 - シリーズ 1 [4-75](#)
 - シリーズ 2 [3-63](#)
- モバイル デバイス 情報 データ ブロック 5.1+ [4-171](#)

ゆ

- ユーザ アカウント更新メッセージ データ ブロック [4-189](#)
- ユーザ クライアント アプリケーション データ ブロック 5.0 ~ 5.1 [B-97](#)
- ユーザ クライアント アプリケーション リスト データ ブロック [4-100](#)
- ユーザ サーバ データ ブロック [4-109](#)
- ユーザ サーバ リスト データ ブロック [4-111](#)
- ユーザ データ ブロック [4-188](#)
- ユーザ プロトコル データ ブロック [4-97](#)
- ユーザ プロトコル リスト データ ブロック 4.7+ [4-118](#)
- ユーザ ホスト データ ブロック 4.7+ [4-112](#)
- ユーザ レコード [3-21](#)、[4-21](#)
- ユーザ ログイン 情報 データ ブロック
 - 5.0 ~ 5.0.2 [B-108](#)
 - 5.1 ~ 5.4.x [B-110](#)
 - 6.0+ [4-204](#)、[B-112](#)、[B-116](#)、[B-119](#)
- ユーザ 削除 アドレス メッセージ [4-58](#)

- ユーザ削除サーバ メッセージ [4-58](#)
- ユーザ重要度変更データ ブロック 4.7+ [4-115](#)
- ユーザ情報更新メッセージ [4-64](#)
- ユーザ情報データ ブロック 5.x [B-123](#)
- ユーザ脆弱性資格メッセージ 4.6.1+ [4-57](#)
- ユーザ脆弱性データ ブロック
5.0+ [4-166](#)
- ユーザ脆弱性変更データ ブロック 4.7+ [4-114](#)
- ユーザ製品データ ブロック
5.0.x [B-102](#)
5.1+ [4-180](#)
- ユーザ設定の無効な脆弱性メッセージ 4.6.1+ [4-57](#)
- ユーザ設定の有効な脆弱性メッセージ 4.6.1+ [4-57](#)
- ユーザ設定ホスト重要度メッセージ [4-59](#)
- ユーザ属性値データ ブロック 4.7+ [4-117](#)
- ユーザ追加ホスト メッセージ [4-58](#)
- ユーザ変更メッセージ [4-64](#)
- エラー メッセージの形式 [2-10](#)
- 侵入イベント レコード 5.4+ [A-1、A-15](#)
- 侵入影響アラート レコード [A-7](#)
- ストリーミング サービス要求メッセージ [2-44](#)
- ストリーミング情報メッセージの形式 [2-43](#)
- パケット レコード [A-9](#)
- 分類レコード [A-10](#)
- ユーザ イベント レコード 5.1+ [A-28](#)
- 優先度レコード [A-12](#)
- ルール メッセージ レコード [A-13](#)

よ

- 要求フラグの形式 [2-13](#)

り

- リスト データ ブロック
シリーズ 1 [4-77](#)
シリーズ 2 [3-64](#)

る

- ルール メッセージのレコード データ構造 4.6.1
以上 [3-22](#)

れ

例

- Null メッセージの形式 [2-9](#)
- 新しい TCP サーバ メッセージ [A-33](#)
- 新しいネットワークプロトコルメッセージ [A-32](#)