CHAPTER 3

侵入および相関データ構造の概要

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

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

この章の次の項では、イベント メッセージの構造を定義しています。

- 侵入イベントとメタデータのレコード タイプ（3-1 ページ）。

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

侵入イベントとメタデータのレコード タイプ

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

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

表 3-1　侵入イベントと一般的なメタデータのレコード タイプ

レコード タイプ	ブロック タイプ（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（3-6 ページ）
4	該当なし	該当なし	プライオリティのメタデータ	現在（Current）	プライオリティ レコード（3-8 ページ）

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	相関ポリシーのメタデータ(バージョン 4.6.1 以上)	現在 (Current)	相関ポリシー レコード(3-25 ページ)
70	該当なし	該当なし	相関ルールのメタデータ(バージョン 4.6.1 以上)	現在 (Current)	相関ルール レコード(3-26 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 (3-29 ページ)
112	128	1	5.1 ～ 5.3.x の相関イベント	レガシー	相関イベント 5.1 ～ 5.3.x(B-283 ページ)
112	156	1	5.4 以上の相関イベント	現在 (Current)	5.4 以上の相関イベント(3-45 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)
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)

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...
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 デバイス のメタデータ	現在 (Current)	管理対象デバイス レコードのメタデータ (3-36 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 (3-82 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 (3-81 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 (3-37 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 (3-96 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 (3-38 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)
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 ディテクタ タイプのメタデータ(バージョン 5.1 以上)	現在 (Current)	エンドポイント向け AMP ディテクタ タイプのメタデータ (3-42 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...
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 (3-110 ページ)
207	該当なし	該当なし	侵入イベント(IPv4)レコード 5.0.x ～ 5.1	レガシー	侵入イベント(IPv4)レコード 5.0.x ～ 5.1 (B-2 ページ)
208	該当なし	該当なし	侵入イベント(IPv6)レコード 5.0.x ～ 5.1	レガシー	侵入イベント(IPv6)レコード 5.0.x ～ 5.1 (B-8 ページ)
260	19	2	ICMP タイプ データのデータ ブロック	現在 (Current)	ICMP タイプのデータ ブロック (3-69 ページ)
270	20	2	ICMP コードのデータ ブロック	現在 (Current)	ICMP コードのデータ ブロック (3-71 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 (3-75 ページ)
320	該当なし	該当なし	6.0 以上の DNS レコード タイプのメタデータ	現在 (Current)	6.0 以上の DNS レコード タイプのメタデータ (3-76 ページ)
321	該当なし	該当なし	6.0 以上の DNS レスポンス タイプのメタデータ	現在 (Current)	6.0 以上の DNS レスポンス タイプのメタデータ (3-78 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 (3-79 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 (3-80 ページ)
400	34	2	侵入イベント レコード 5.2.x	レガシー	侵入イベント レコード 5.2.x (B-14 ページ)
400	41	2	侵入イベント レコード 5.3	レガシー	侵入イベント レコード 5.3 (B-20 ページ)
400	54	2	侵入イベント レコード 5.3.1	レガシー	侵入イベント レコード 5.3.1 (B-32 ページ)
400	45	2	侵入イベント レコード 5.4.x	レガシー	侵入イベント レコード 5.4.x (B-39 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)

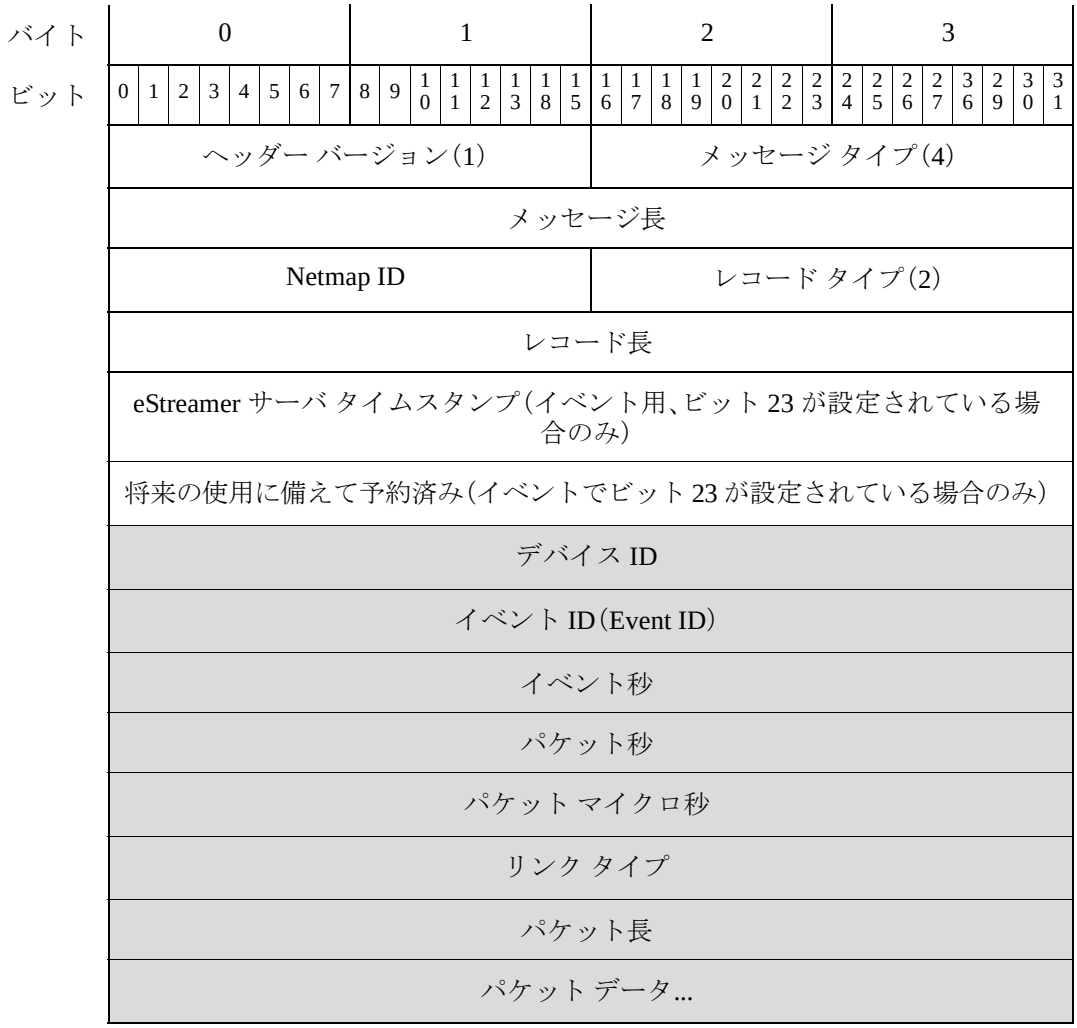
レコード タイプ	ブロック タイプ (Block Type)	シリーズ	説明	レコード ステータス	データ形式の参照先...
400	60	2	侵入イベント レコード 6.0 以上	現在 (Current)	侵入イベント レコード 6.0 以上 (3-9 ページ)
500	32	2	ファイル イベント(バージョン 5.2.x)	レガシー	ファイル イベント 5.2.x (B-244 ページ)
500	38	2	ファイル イベント(バージョン 5.3)	レガシー	ファイル イベント 5.3 (B-249 ページ)
500	43	2	ファイル イベント(バージョン 5.3.1)	レガシー	ファイル 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 (3-85 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	72	2	ファイル イベント(バージョン 6.0 以上)	現在 (Current)	6.0 以上のファイル イベント (3-85 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 (3-109 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)
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 (3-107 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 (3-114 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 (3-115 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 (3-115 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 (3-116 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 (3-117 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 (3-118 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...
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 (3-119 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 (3-120 ページ)
601	51	2	SSL ルール ID	現在 (Current)	SSL ルール ID (3-122 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 (3-129 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 (3-124 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 (3-125 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 (3-125 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 (3-126 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 (3-127 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 (3-128 ページ)
614	50	2	5.4 以上の SSL 証明書の詳細のデータ ブロック	現在 (Current)	5.4 以上の SSL 証明書の詳細のデータ ブロック (3-129 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 (3-133 ページ)

パケット レコード 4.8.0.2 以上

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



次の表は、パケット レコードのフィールドについての説明です。

表 3-2　パケット レコード フィールド

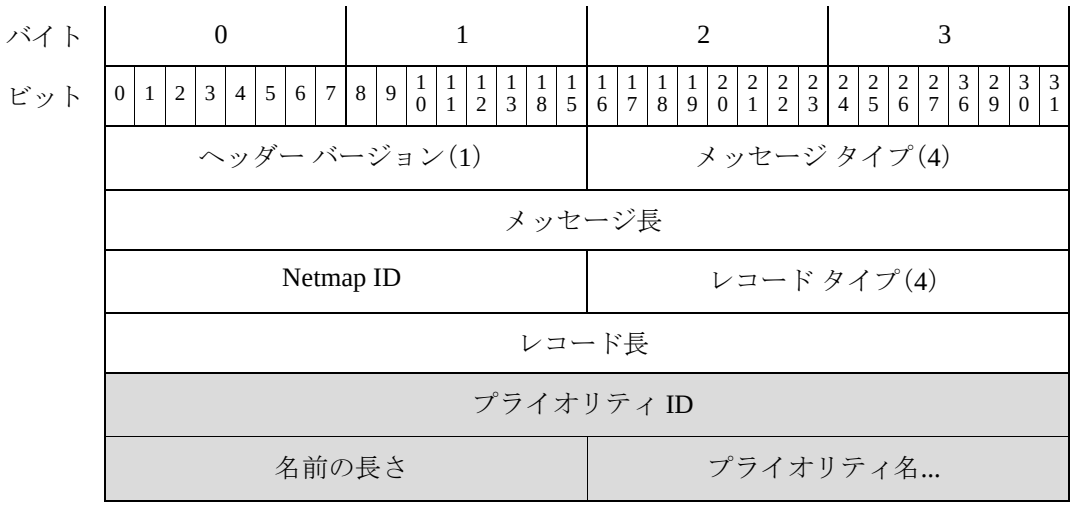
フィールド	データ タイプ	説明
デバイス ID	uint32	デバイス ID 番号。バージョン 3 または 4 のメタデータの要求により関連付けられているデバイス名を取得できます。詳細については、管理対象デバイス レコードのメタデータ (3-36 ページ)を参照してください。
イベント ID (Event ID)	uint32	イベント ID 番号。
イベント秒	uint32	イベントが発生した秒(01/01/1970 以降)。

表 3-2　パケット レコード フィールド(続き)

フィールド	データ タイプ	説明
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(2-12 ページ)を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにプライオリティ レコードを示す値 4 があることに注意してください。



次の表は、各プライオリティ固有のフィールドについての説明です。

表 3-3　プライオリティ レコード フィールド

フィールド	データ タイプ	説明
プライオリティ ID	uint32	プライオリティ ID 番号を表示します。
名前の長さ	uint16	プライオリティ名に含まれるバイト数。
プライオリティ名	変数（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

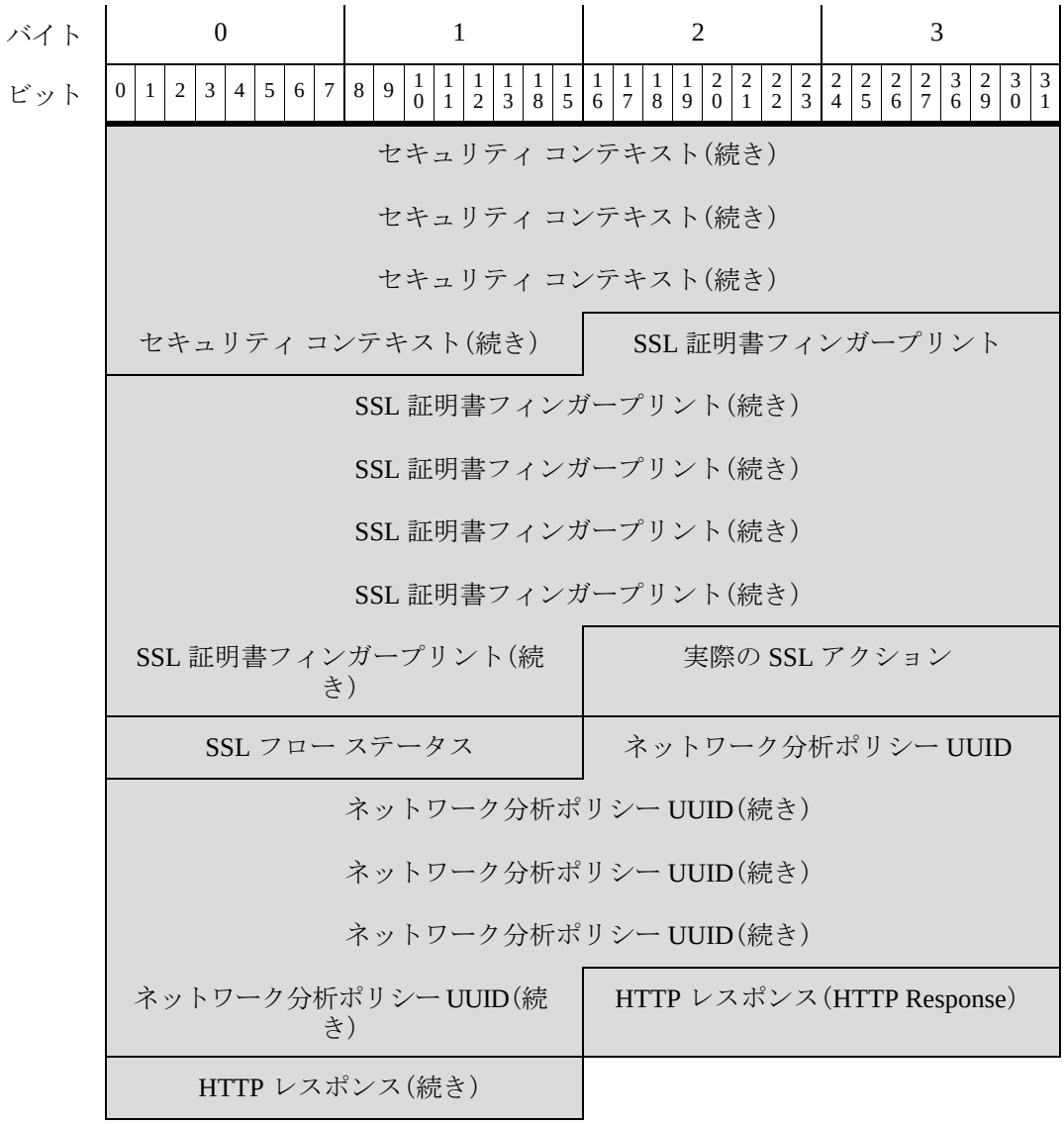
侵入イベント レコードのフィールドは、次の図で網掛けされています。レコード タイプは 400 で、ブロック タイプはシリーズ 2 セットのデータ ブロックの 60 です。これはブロック タイプ 45 に取って代わります。HTTP レスポンス フィールドが追加されました。

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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（400）															
レコード長																																
eStreamer サーバ タイムスタンプ（イベント用、ビット 23 が設定されている場合のみ）																																
将来の使用に備えて予約済み（イベントでビット 23 が設定されている場合のみ）																																
ブロック タイプ（60）																																
ブロック長																																
デバイス ID（Device ID）																																
イベント ID（Event ID）																																
イベント秒																																
イベント マイクロ秒																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ルール 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							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
アクセス コントロール ルール ID																																
アクセス コントロール ポリシー UUID																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
アクセス コントロール ポリシー UUID（続き）																																
インターフェイス入力 UUID																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																
インターフェイス入力 UUID（続き）																																
インターフェイス出力 UUID																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
インターフェイス出力 UUID（続き）																																
セキュリティ ゾーン入力 UUID																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン入力 UUID（続き）																																
セキュリティ ゾーン出力 UUID																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
セキュリティ ゾーン出力 UUID（続き）																																
接続タイムスタンプ																																
接続インスタンス ID																	接続数カウンタ															
送信元の国																	宛先の国															
IOC 番号																	セキュリティ コンテキスト															



次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 3-4　侵入イベント レコード 6.0 以上のフィールド

フィールド	データ タイプ	説明
ブロック タイプ	unint32	侵入イベント データ ブロックを開始します。この値は常に 60 です。
ブロック長	unint32	侵入イベント データ ブロックのバイトの合計数(侵入イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID（Device ID）	unit32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、管理対象デバイス レコードのメタデータ (3-36 ページ)を参照してください。

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

表 3-4　侵入イベント レコード6.0 以上のフィールド(続き)

フィールド	データ タイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 • 0:ブロックされていない • 1:ブロックされた • 2:ブロックされた可能性がある(設定では許可されていない)
MPLS ラベル	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。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 3-4　侵入イベント レコード6.0 以上のフィールド(続き)

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

表 3-4　侵入イベント レコード6.0 以上のフィールド(続き)

フィールド	データ タイプ	説明
ネットワーク分析ポリシー UUID	uint8[16]	侵入イベントを作成したネットワーク分析ポリシーの UUID。
HTTP レスポンス(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(4-63 ページ)を参照してください。)

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(9)															
eStreamer サーバ 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)																																
デバイス ID																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	イベント秒																															
	影響																															
	送信元 IP アドレス 送信元 IP アドレス（続き） 送信元 IP アドレス（続き） 送信元 IP アドレス（続き）																															
	宛先 IP アドレス 宛先 IP アドレス（続き） 宛先 IP アドレス（続き） 宛先 IP アドレス（続き）																															
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。
デバイス ID	uint32	管理対象デバイス ID 番号を表示します。
イベント秒	uint32	イベントが検出された秒（1970 年 1 月 1 日からの経過秒数）を示します。

表 3-5　影響イベント データ フィールド(続き)

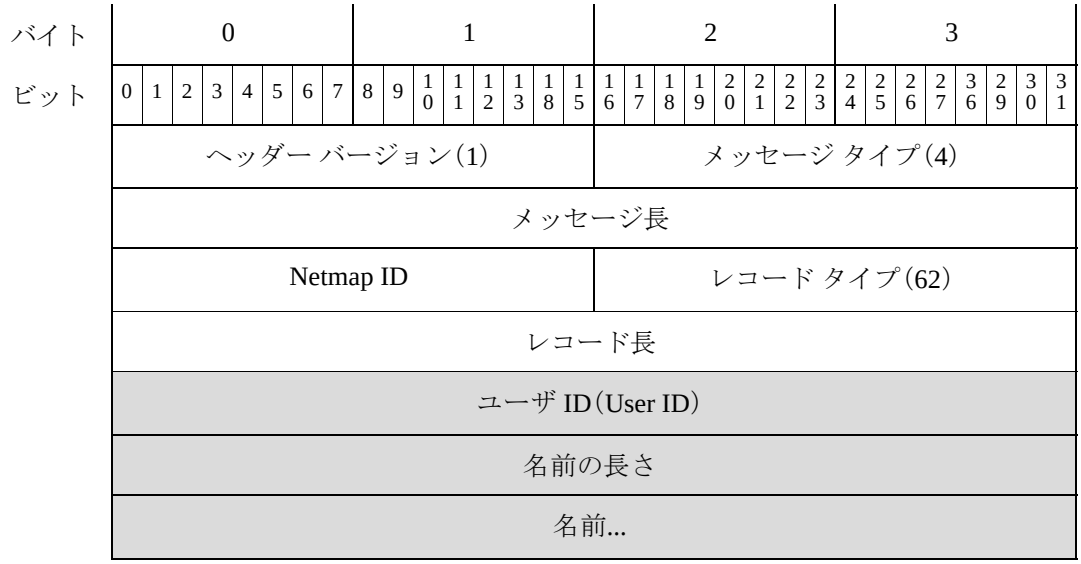
フィールド	データ タイプ	説明
影響	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップさ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

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 (4-73 ページ)を参照してください。
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数。これには文字列ブロック タイプ用の 4 バイト、文字列ブロック長用の 4 バイト、および説明のバイト数が含まれます。
説明	string	影響イベントについての説明。

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 (2-12 ページ)を参照してください)。



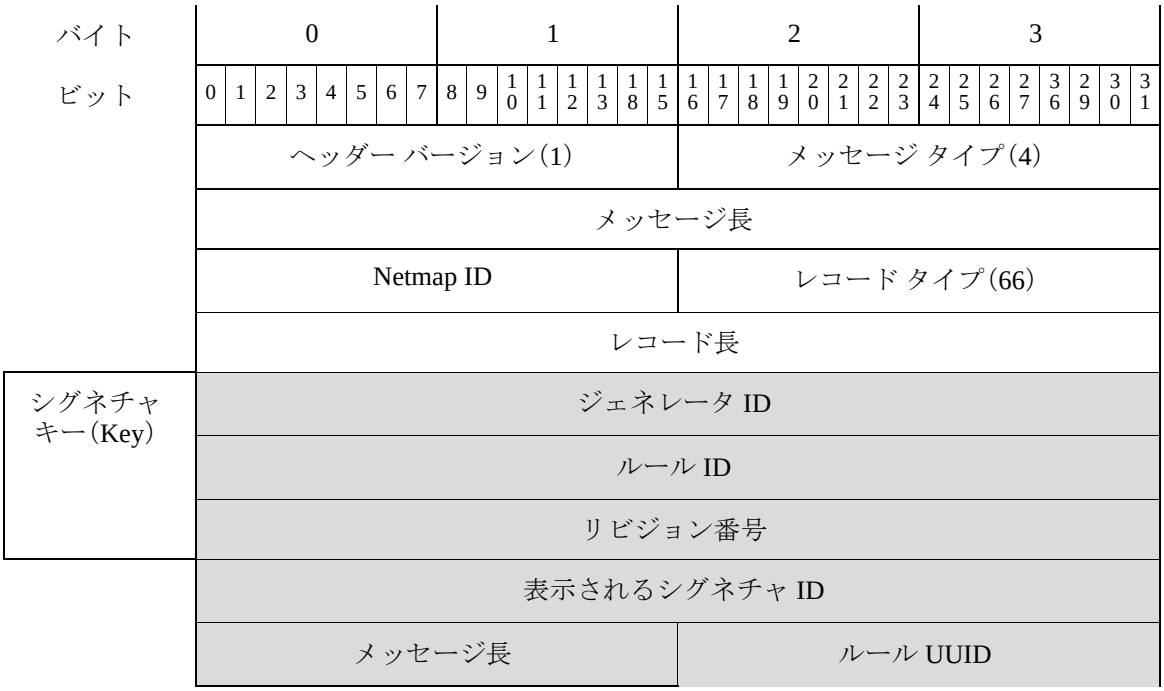
次の表は、ユーザ レコードのフィールドについての説明です。

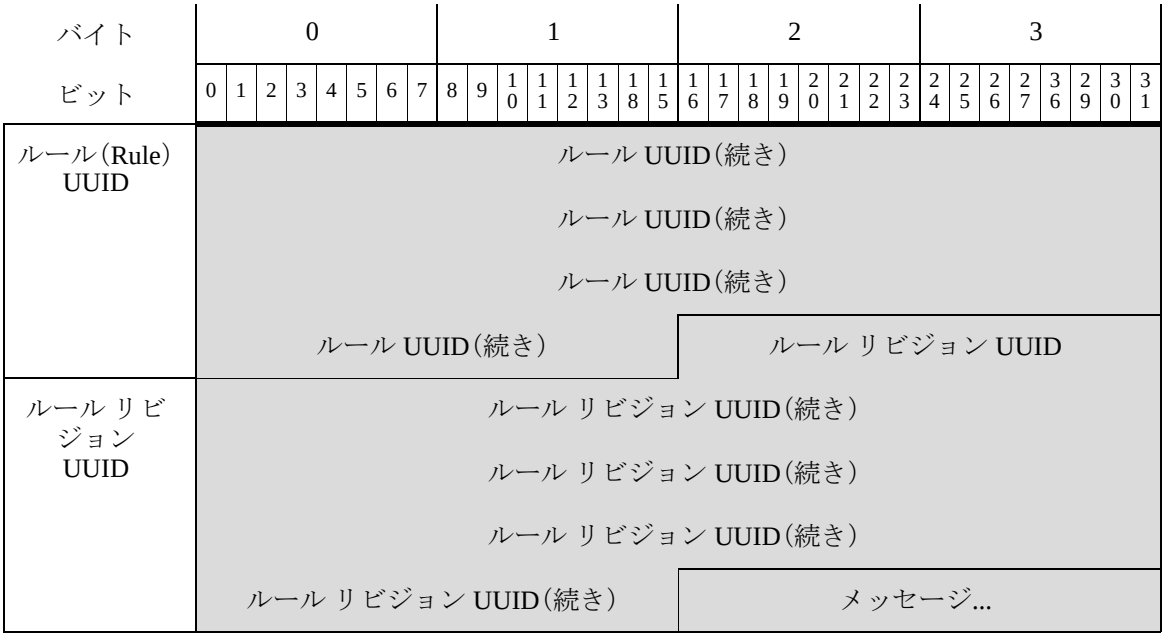
表 3-6　ユーザ レコードのフィールド

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。
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りました。（該当するメタデータ フラグ（要求メッセージの [要求フラグ（Request Flags）] フィールドでバージョン 2 はビット 14、バージョン 3 はビット 15、バージョン 4 はビット 20）が設定されていると、バージョン 2、バージョン 3、またはバージョン 4 のメタデータ情報が送信されます。要求フラグ（2-12 ページ）を参照してください）。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにルール メッセージのバージョン 2 のレコードを示す値 66 があることに注意してください。





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(2-12 ページ)を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに分類バージョン 2 のレコードを示す値 67 があることに注意してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ヘッダー バージョン(1)																メッセージ タイプ(4)															
	メッセージ長																															
	Netmap ID																レコード タイプ(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。

相関ポリシー レコード

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ヘッダー バージョン(1)																メッセージ タイプ(4)																
	メッセージ長																															
	Netmap ID																レコード タイプ(69)															
	レコード長																															
	相関ポリシー ID																															
	名前の長さ																名前...															
	説明の長さ																説明...															
相関ポリシー UUID	相関ポリシー UUID 相関ポリシー UUID(続き) 相関ポリシー UUID(続き) 相関ポリシー UUID(続き)																															
相関ポリシー リビジョン UUID	相関ポリシー リビジョン UUID 相関ポリシー リビジョン UUID(続き) 相関ポリシー リビジョン UUID(続き) 相関ポリシー リビジョン UUID(続き)																															

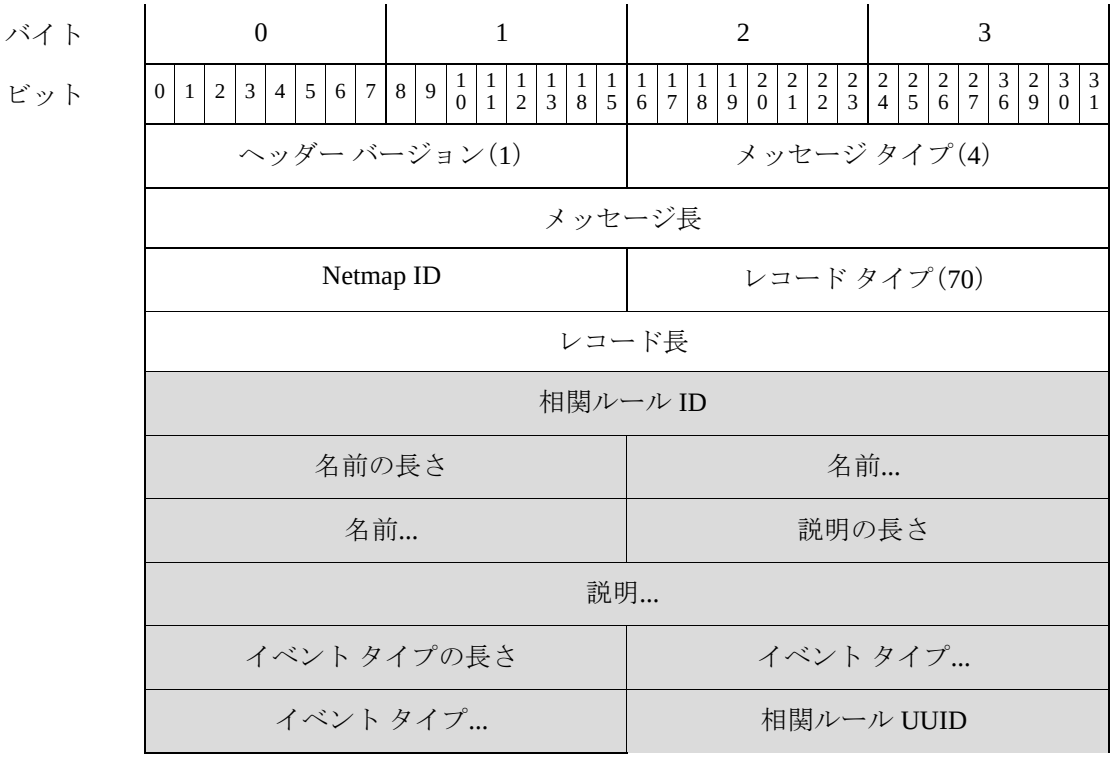
次の表は、相関ポリシー レコードのフィールドについての説明です。

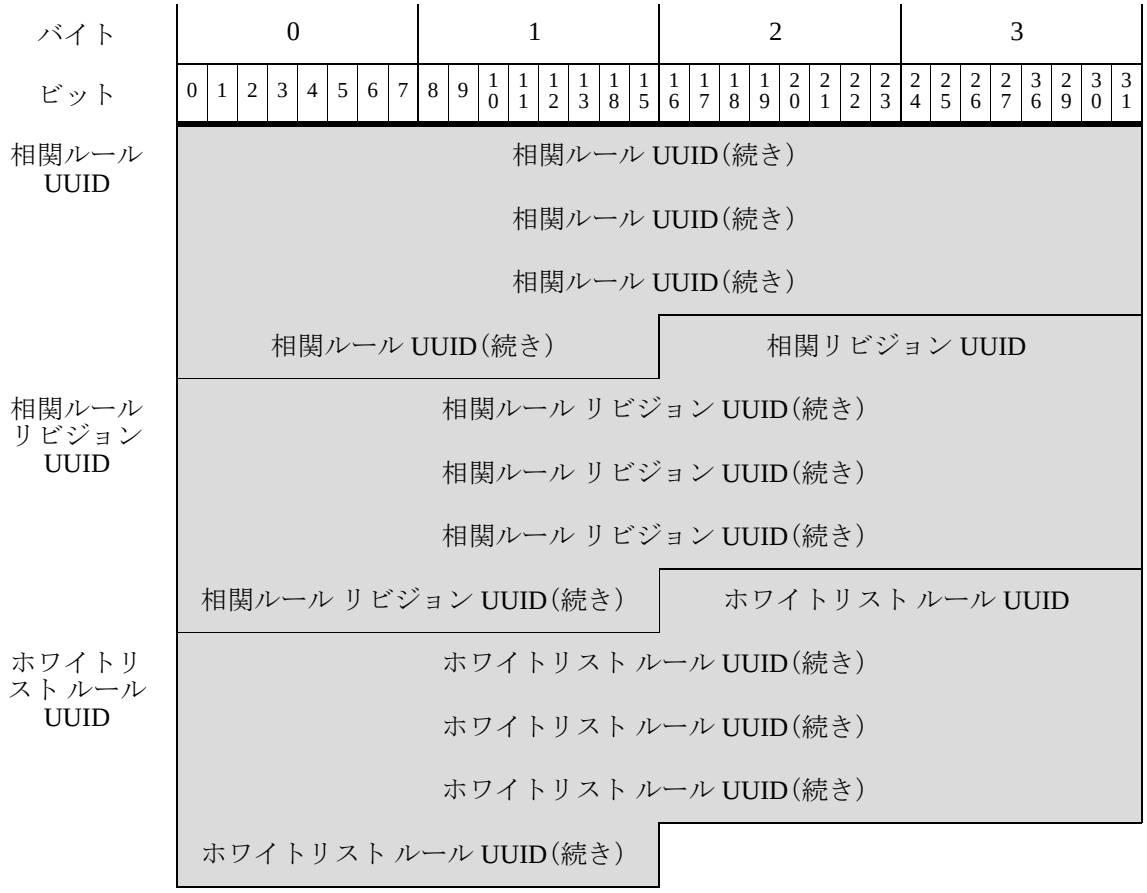
表 3-9　相関ポリシー レコード フィールド

フィールド	データ タイプ	説明
相関ポリシー ID	uint32	相関ポリシー ID 番号。
名前の長さ	uint16	相関ポリシー名に含まれるバイト数。
[名前(Name)]	string	イベントをトリガーした相関ポリシーの名前。
説明の長さ	uint16	相関ポリシーの説明に含まれるバイト数。
説明	string	イベントをトリガーした相関ポリシーの説明。
UUID	uint8[16]	相関ポリシーの固有識別子として機能する相関ポリシー ID 番号。
リビジョン UUID	uint8[16]	相関ポリシーの固有識別子として機能する相関ポリシー リビジョン ID 番号。

相関ルール レコード

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





次の表は、相関ルール レコードのフィールドについての説明です。

表 3-10　相関ルール レコード フィールド

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

侵入イベント追加データ レコード

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

イベント追加データは、カプセル化されたイベント追加データのデータ ブロックに表示されます。データ ブロック タイプの値は常に 4 です。(イベント追加データのデータ ブロックは、シリーズ 2 のデータ ブロックです。シリーズ 2 のデータ ブロックの詳細については、シリーズ 2 のデータ ブロックの概要 (3-58 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 (3-29 ページ)に記載されているイベント追加データのメタデータも受信されます。ビット 23 を有効にすると、eStreamer は拡張イベント ヘッダーを表示します。要求フラグの設定方法の詳細については、要求フラグ (2-12 ページ)を参照してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(110)															
レコード長																																
eStreamer サーバ タイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																																
将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																																
イベント追加データのデータ ブロック タイプ(4)																																
イベント追加データのデータ ブロック長																																
デバイス ID																																
イベント ID(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。
デバイス 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。 • 1：XFF クライアント（IPv4） • 2：XFF クライアント（IPv6） • 9：HTTP URI
BLOB ブロック タイプ	uint32	追加データを含む BLOB データ ブロックを開始します。この値は常に 1 です。ブロック タイプは、シリーズ 2 ブロックです。
長さ（Length）	uint32	BLOB データ ブロックの合計バイト数。
追加データ	変数（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 (2-12 ページ) を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(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。

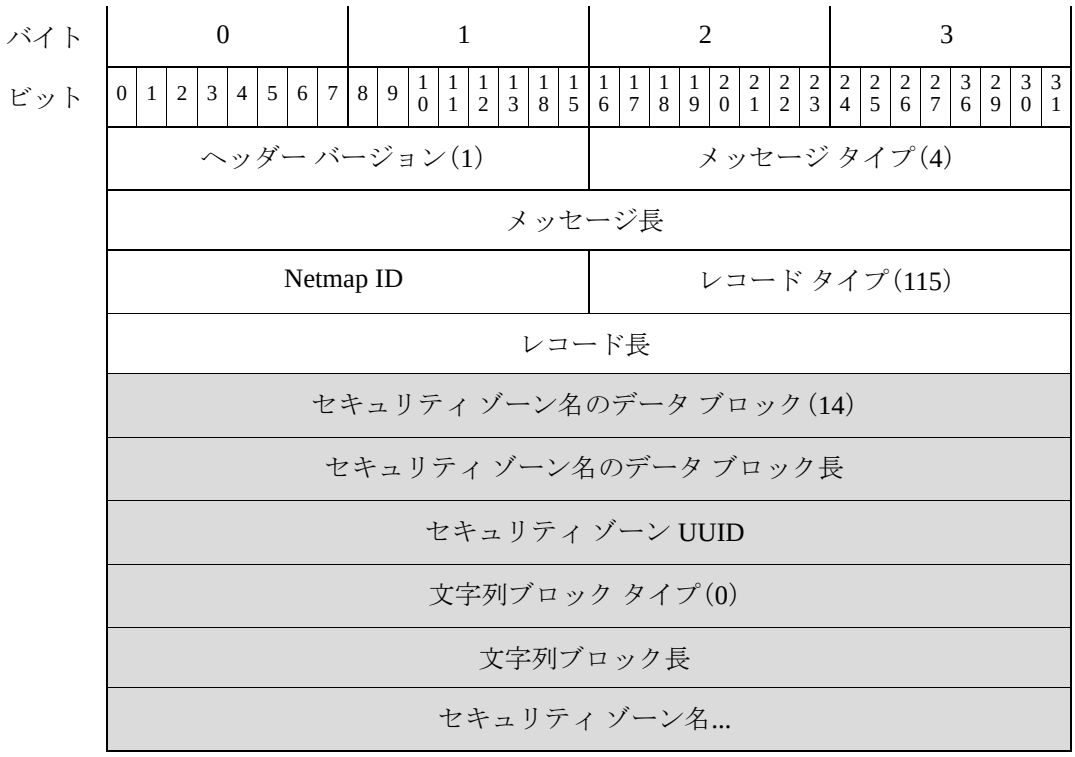
次の表は、イベント追加データのメタデータのレコードのフィールドについての説明です。

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。
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（2-12 ページ）を参照してください）。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにセキュリティ ゾーン名レコードを示す値 115 があることに注意してください。シリーズ 2 セットのデータ ブロックのブロック タイプ 14 の UUID 文字列データ ブロックが含まれています。



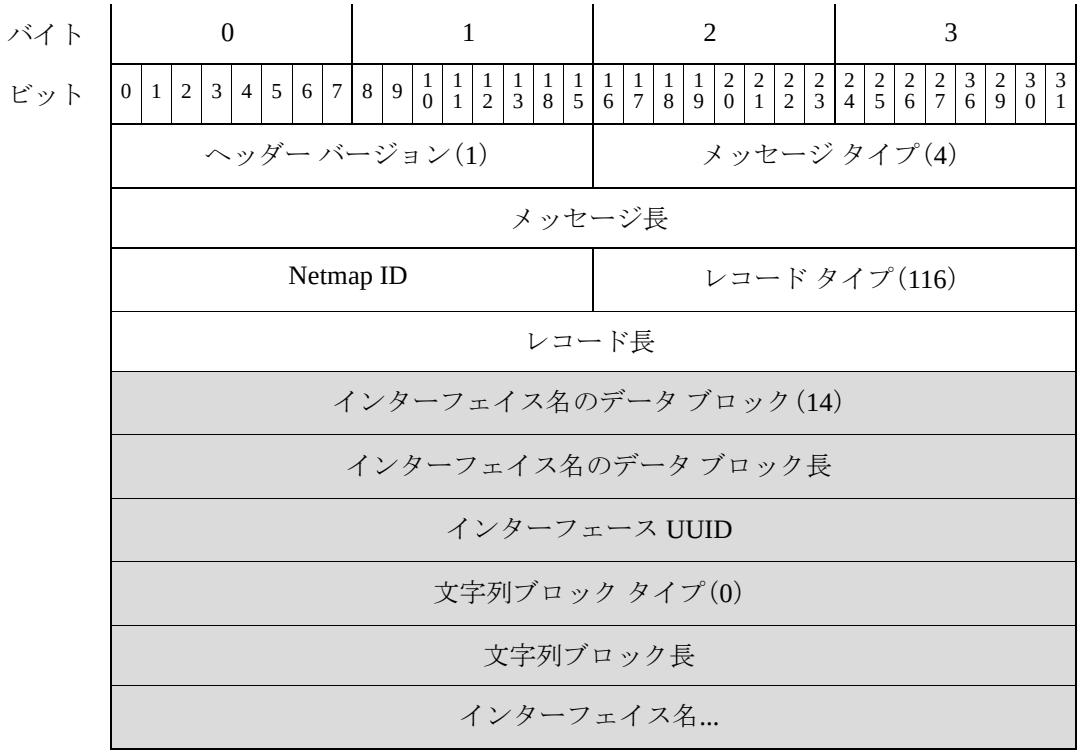
次の表は、セキュリティ ゾーン名のデータ ブロックのフィールドについての説明です。

表 3-13　セキュリティ ゾーンの名のデータ ブロック フィールド

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

インターフェイス名レコード

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



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

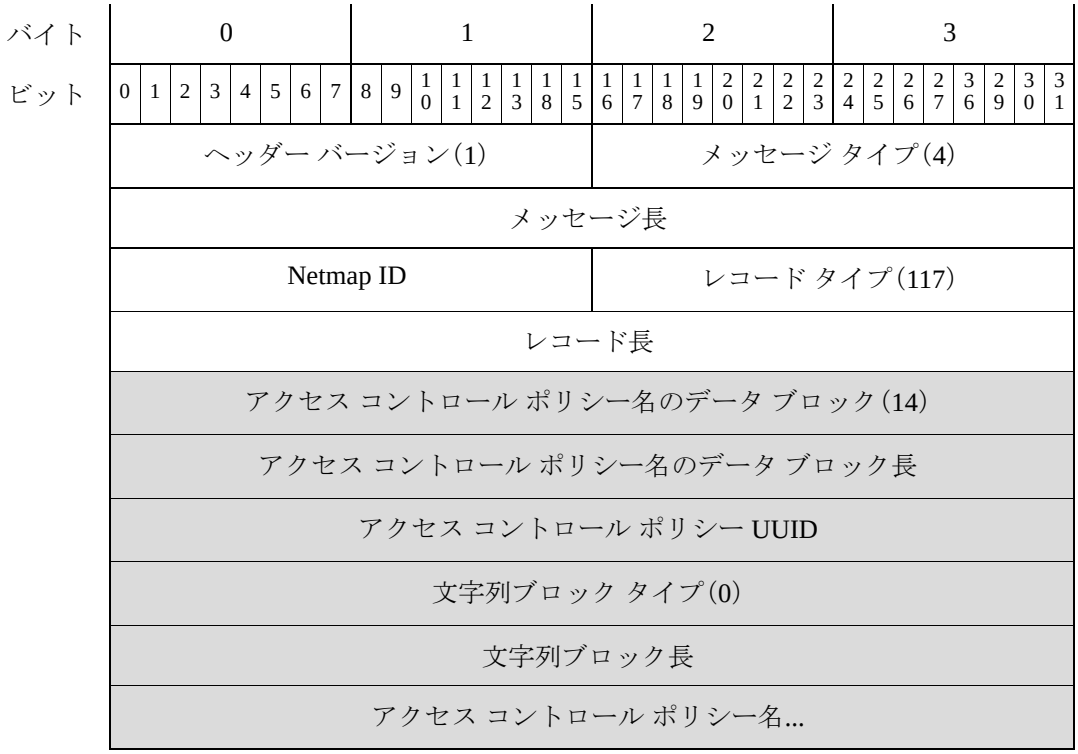
フィールド	データ タイプ	説明
インターフェイス名のデータ ブロック タイプ	uint32	インターフェイス名のデータ ブロックを開始します。この値は常に 14 です。ブロック タイプは、シリーズ 2 ブロックです。
インターフェイス名のデータ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
インターフェース UUID	uint8[16]	接続イベントに関連付けられたインターフェイスの固有識別子として機能するインターフェイス ID 番号。

表 3-14　インターフェイス名のデータ ブロック フィールド(続き)

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

アクセス コントロール ポリシー名のレコード

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



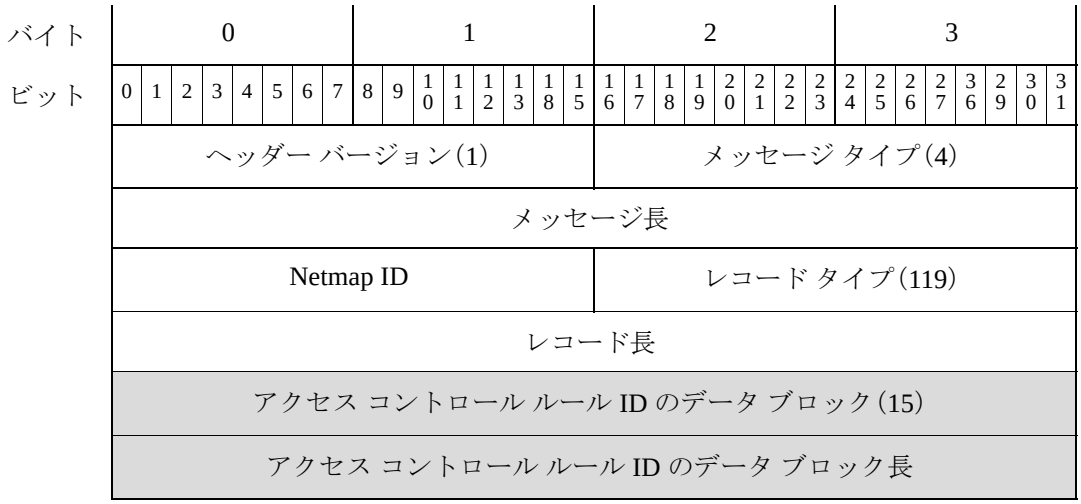
次の表は、アクセス コントロール ポリシー名のデータ ブロックのフィールドについての説明です。

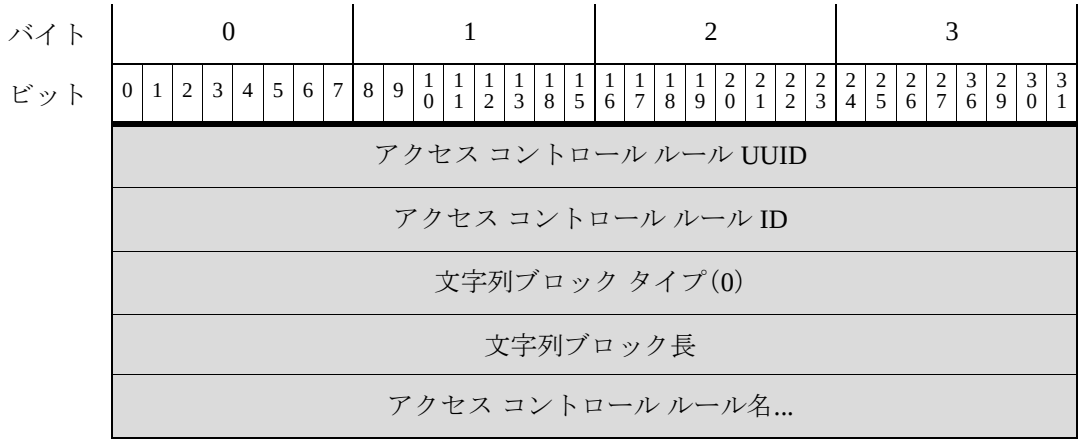
表 3-15　アクセス コントロール ポリシー名のデータ ブロック フィールド

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

アクセス コントロール ルール ID レコードのメタデータ

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





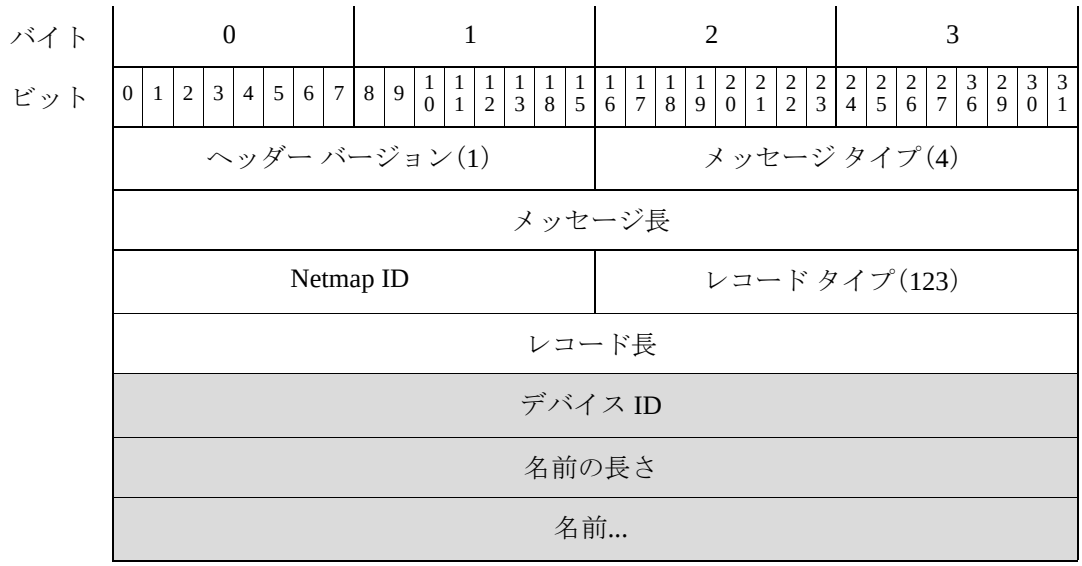
次の表は、アクセス コントロール ルール ID のデータ ブロックのフィールドについての説明です。

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

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

管理対象デバイス レコードのメタデータ

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



次の表は、管理対象 デバイス レコードのフィールドについての説明です。

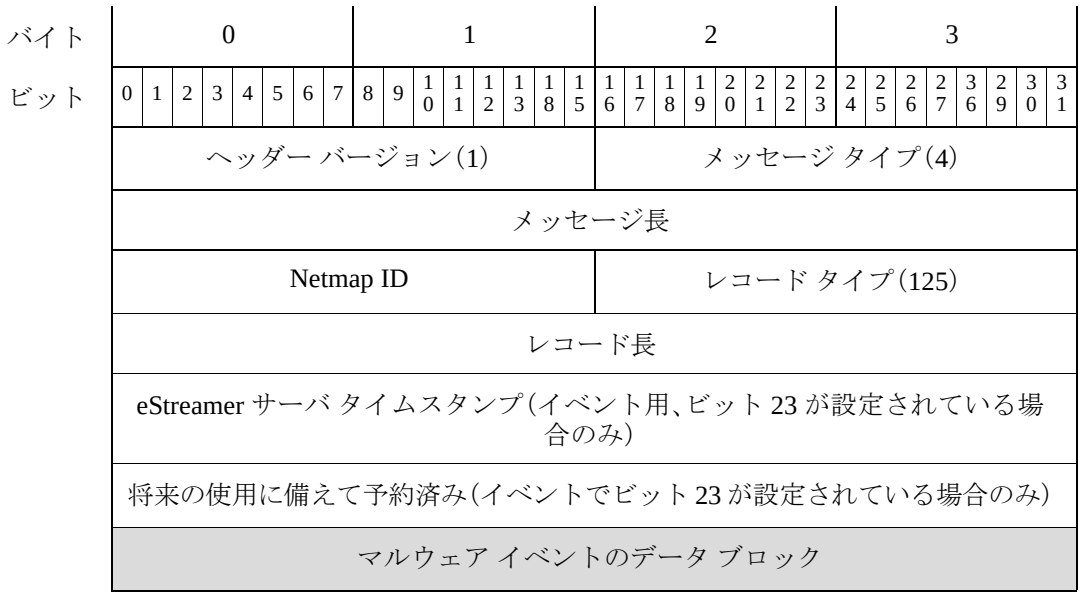
表 3-17　管理対象 デバイス レコード フィールド

フィールド	データ タイプ	説明
デバイス ID	uint32	管理対象デバイス ID 番号。
名前の長さ	uint32	名前に含まれるバイト数。
[名前(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(2-12 ページ)を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。シリーズ 2 セットのデータ ブロックのブロック タイプ 24、33、35、44、47 のいずれかのマルウェア イベントのデータ ブロックが含まれています。



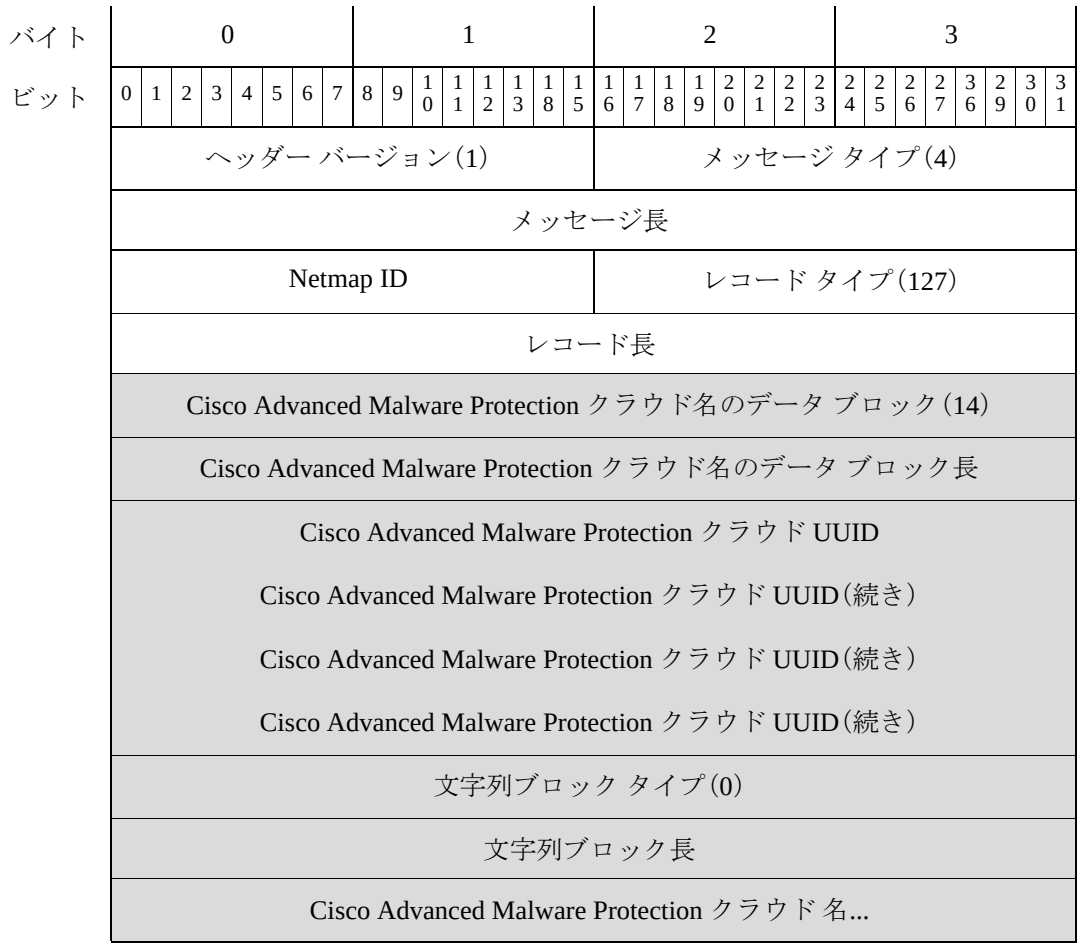
次の表は、各マルウェア イベント レコード データ フィールドについての説明です。

表 3-18　マルウェア イベント レコード フィールド

フィールド	データ タイプ	説明
マルウェア イベントのデータ ブロック	変数(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(3-96 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(2-12 ページ)を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに Cisco Advanced Malware Protection 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。



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

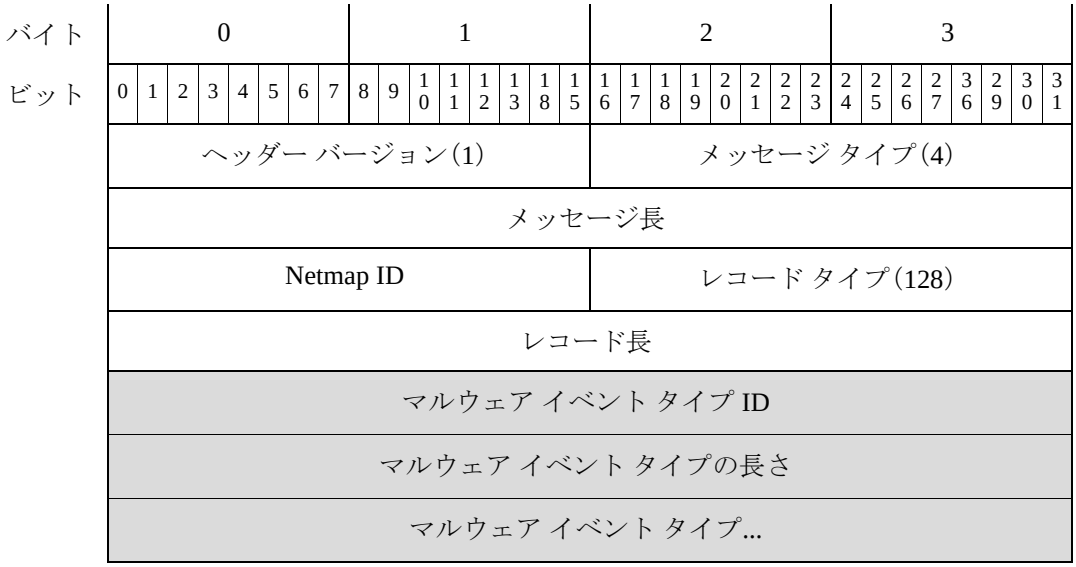
フィールド	データ タイプ	説明
Cisco Advanced Malware Protection クラウド名のデータ ブロック タイプ	uint32	Cisco Advanced Malware Protection クラウド名のデータ ブロックを開始します。この値は常に 14 です。ブロック タイプは、シリーズ 2 ブロックです。
Cisco Advanced Malware Protection クラウド名のデータ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。

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(続き)

フィールド	データ タイプ	説明
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。
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 (2-12 ページ)を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにマルウェア イベント タイプ レコードを示す値 128 があることに注意してください。



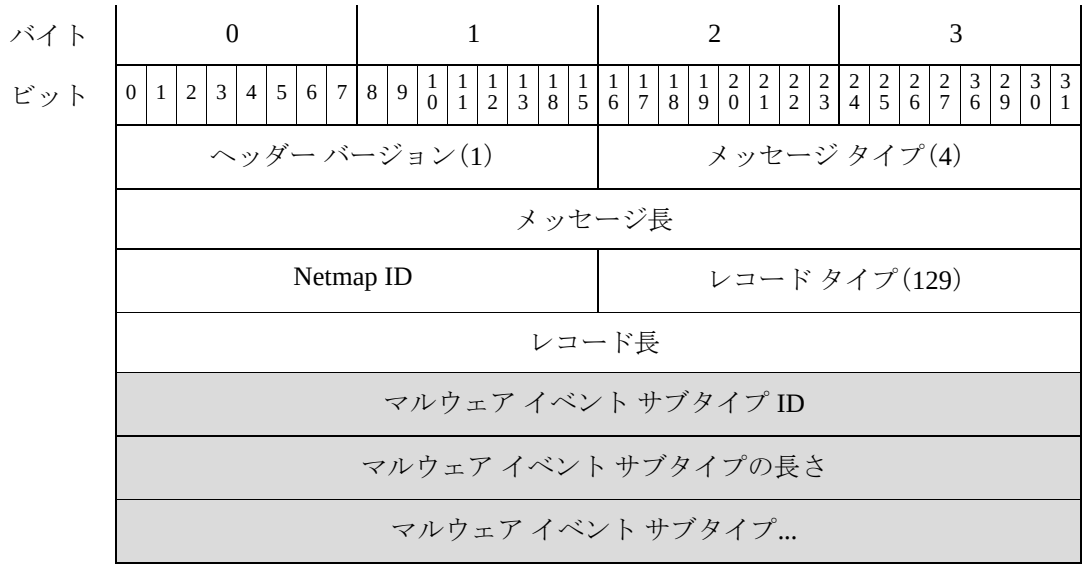
次の表は、マルウェア イベント タイプ レコードのフィールドについての説明です。

表 3-20　マルウェア イベント タイプ レコード フィールド

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

マルウェア イベント サブタイプのメタデータ

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



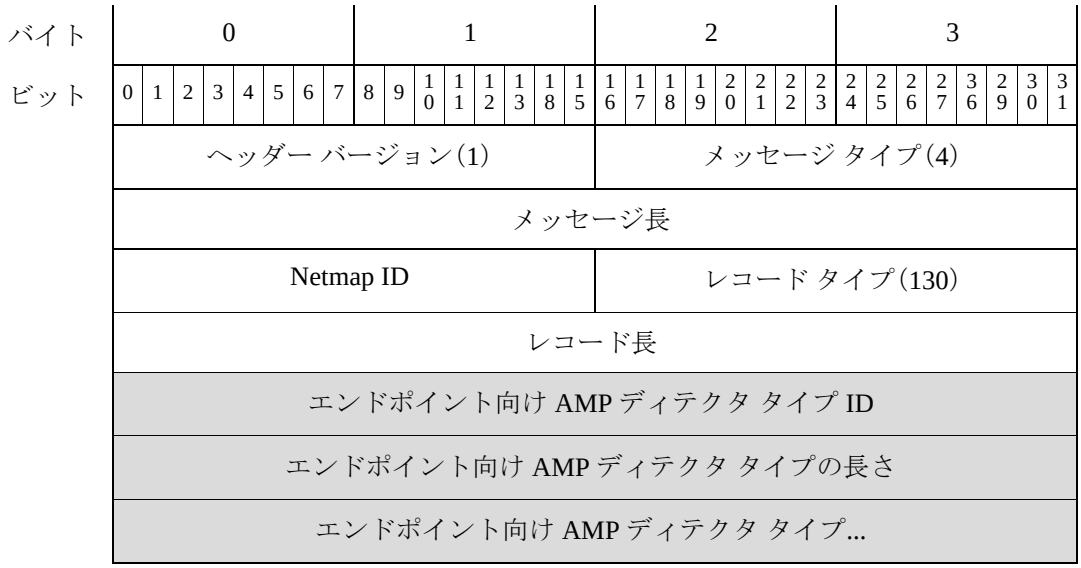
次の表は、マルウェア イベント サブタイプ レコードのフィールドについての説明です。

表 3-21　マルウェア イベント サブタイプ レコード フィールド

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

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(2-12 ページ)を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに エンドポイント向け AMP ディテクタ タイプ レコードを示す値 130 があることに注意してください。



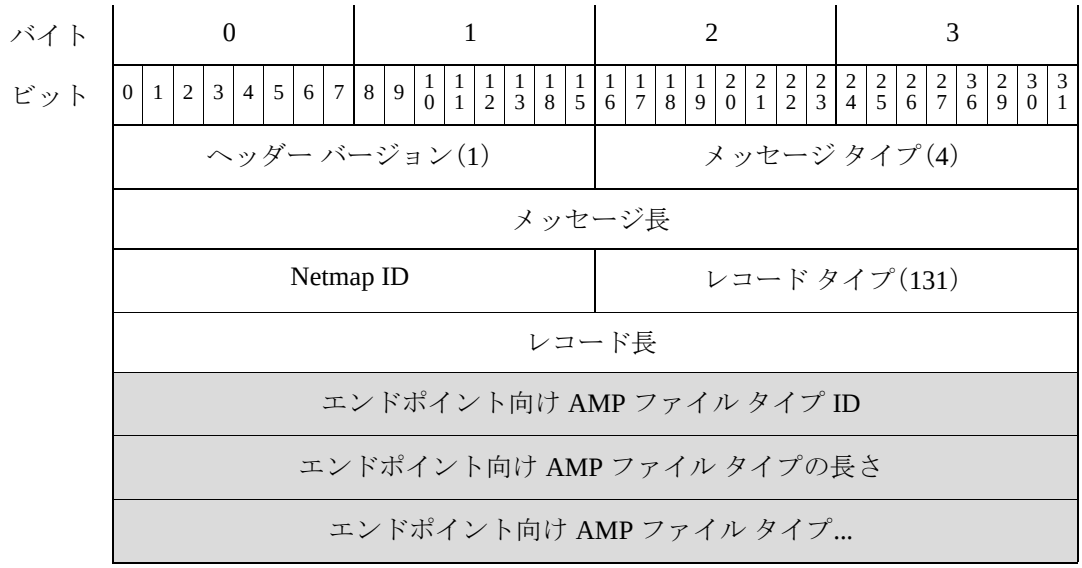
次の表は、エンドポイント向け AMP ディテクタ タイプ レコードのフィールドについての説明です。

表 3-22　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。
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（2-12 ページ）を参照してください）。メッセージ長フィールドの後に表示されるレコード タイプ フィールドに エンドポイント向け AMP ファイル タイプ レコードを示す値 `131` があることに注意してください。



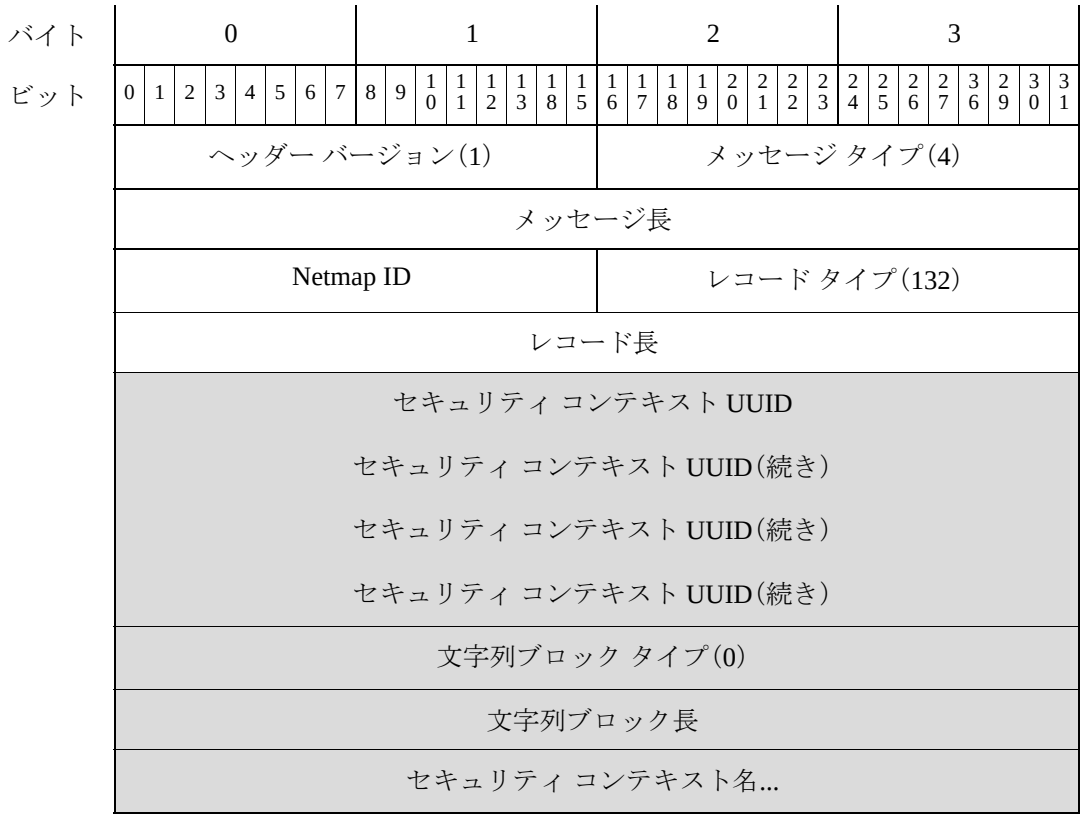
次の表は、エンドポイント向け AMP ファイル タイプ レコードのフィールドについての説明です。

表 3-23　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。
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 (2-12 ページ)を参照してください)。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにセキュリティ コンテキスト名レコードを示す値 132 があることに注意してください。



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

表 3-24　セキュリティ コンテキスト名のレコード フィールド

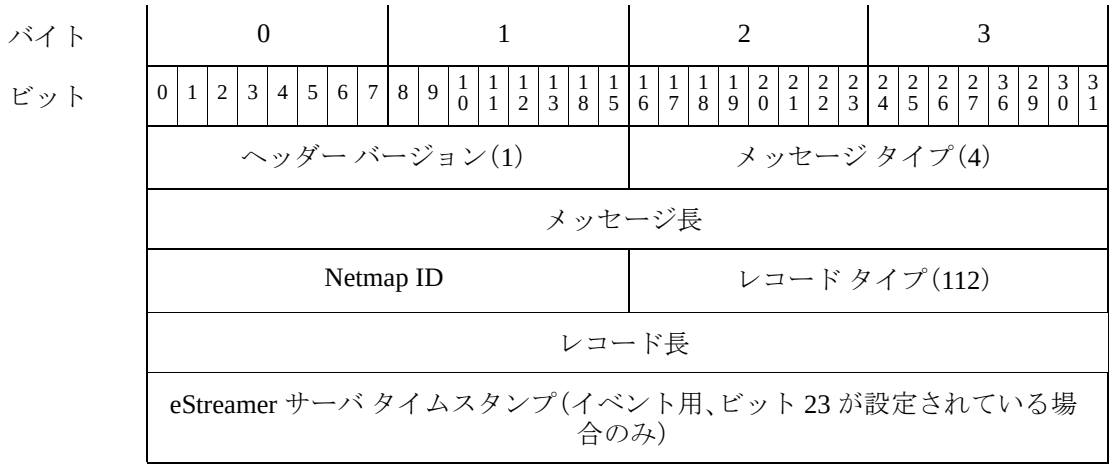
フィールド	データ タイプ	説明
セキュリティ コンテキスト UUID	uint8[16]	セキュリティ コンテキストの UUID
文字列ブロック タイプ	uint32	セキュリティ コンテキストの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	セキュリティ コンテキスト名の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとセキュリティ コンテキスト名のバイト数が含まれます。
セキュリティ コンテキスト名	string	セキュリティ コンテキスト名。

5.4 以上の相関イベント

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

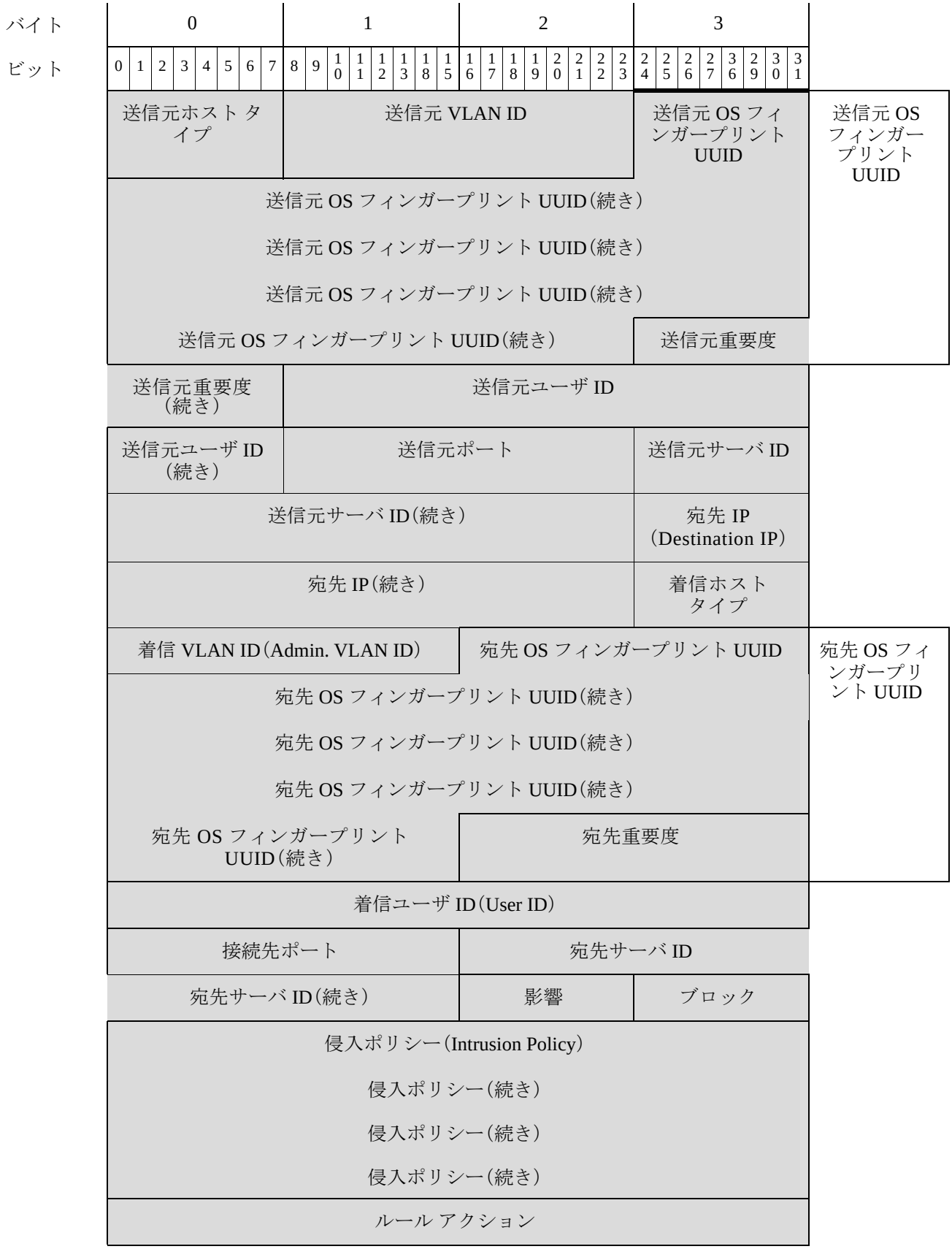
バージョン 5.4 以上の相関イベントには、位置情報、セキュリティ インテリジェンス、および SSL サポートのフィールド新たに加わります。

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



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																																
相関ブロックのタイプ(156)																																
相関ブロック長																																
デバイス ID(Device ID)																																
(相関)イベント秒																																
イベント ID(Event ID)																																
ポリシー ID																																
ルール ID																																
[プライオリティ(Priority)]																																
文字列ブロック タイプ(0)																																
文字列ブロック長																																
説明...																									イベント タイプ (Event Type)							
イベント デバイス ID																																
シグネチャ ID																																
シグネチャ ジェネレータ ID																																
(トリガー)イベント秒																																
(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																																

イベント説明


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

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
セキュリティ コンテキスト(続き)																																
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(4-63 ページ)を参照してください。

表 3-25　相関イベント 5.4 以上のデータ フィールド

フィールド	データ タイプ	説明
相関ブロック タイプ	uint32	相関イベント データ ブロックが続くことを示します。このフィールドの値は常に 156 です。ディスカバリ(シリーズ 1)ブロック(4-63 ページ)を参照してください。
相関ブロック長	uint32	相関データ ブロック長(相関ブロック タイプと長さの 8 バイト、およびそれに続く相関データを含む)。
デバイス ID(Device ID)	uint32	相関イベントを生成した管理対象デバイスまたは Management Center の内部 ID 番号。ゼロ値は Management Center を示します。バージョン 3 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、管理対象デバイス レコードのメタデータ(3-36 ページ)を参照してください。
(相関)イベント秒	uint32	相関イベントが生成された時刻を示す UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。

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
イベント ID（Event ID）	uint32	相関イベント ID 番号。
ポリシー ID	uint32	違反された相関ポリシーの ID 番号。データベースからのポリシー ID 番号を入手する方法の詳細については、サーバ レコード（4-16 ページ）を参照してください。
ルール ID	uint32	トリガーしてポリシー違反となった相関ルールの ID 番号。データベースからのポリシー ID 番号を入手する方法の詳細については、サーバ レコード（4-16 ページ）を参照してください。
[プライオリティ（Priority）]	uint32	イベントに割り当てられた優先順位。これは、0 ～ 5 の整数値です。
文字列ブロック タイプ	uint32	相関違反イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、文字列データ ブロック（4-73 ページ）を参照してください。
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数（文字列のブロック タイプのための 4 バイト、文字列ブロック長のための 4 バイト、説明のバイト数を含む）。
説明	string	相関イベントについての説明。
イベント タイプ（Event Type）	uint8	相関イベントが、侵入、ホスト検出、またはユーザ イベントによってトリガーされたかどうかを示します。 • 1：侵入 • 2：ホストの検出 • 3：ユーザ
イベント デバイス ID	uint32	相関イベントをトリガーしたイベントを生成したデバイスの ID 番号。バージョン 3 メタデータを要求するとデバイス名を入手できます。詳細については、管理対象デバイス レコードのメタデータ（3-36 ページ）を参照してください。
シグネチャ ID	uint32	イベントが侵入イベントであった場合、イベントに対応するルール ID 番号を示します。そうでない場合、この値は 0 になります。
シグネチャ ジェネレータ ID	uint32	イベントが侵入イベントであった場合、イベントを生成した Firepower システム プリプロセッサまたはルール エンジンの ID 番号を示します。
（トリガー）イベント秒	uint32	相関ポリシー ルールをトリガーしたイベントの時刻を示す UNIX タイムスタンプ（1970 年 1 月 1 日からの秒数）。
（トリガー）イベント マイクロ秒	uint32	イベントが検出されたタイムスタンプの、マイクロ秒（100 万分の 1 秒）の増分。
イベント ID（Event ID）	uint32	Cisco デバイスによって生成されたイベントの ID 番号。
イベントで定義されたマスク	bits[32]	このフィールドに設定されたビットは、メッセージ内の続くどのフィールドが有効であるかを示します。各ビット値のリストの詳細については、表 3-23（3-44 ページ）を参照してください。

表 3-25　相関イベント 5.4 以上のデータ フィールド(続き)

フィールド	データ タイプ	説明
イベント影響フラグ	bits[8]	イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。 • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 • 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) 次の影響レベル値は、Management Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。 • グレー(0、不明):`00X00000` • 赤(1、脆弱):`xxxx1xxx`, `xxx1xxxx`, `x1xxxxxx`, `1xxxxxxx`(バージョン 5.0+ のみ) • オレンジ(2、潜在的に脆弱):`00X0011X` • 黄(3、現在は脆弱でない):`00X0001X` • 青(4、不明なターゲット):`00X00001`
IP プロトコル	uint8	イベントに関連付けられている IP プロトコルの ID(該当する場合)。
ネットワーク プロトコル	uint16	イベントに関連付けられているネットワーク プロトコル(該当する場合)。
送信元 IP アドレス	uint8[4]	このフィールドは予約済みですが、設定されておりません。送信元 IPv4 アドレスは、送信元 IPv6 アドレス フィールドに保存されます。詳細については、IP アドレス (1-5 ページ) を参照してください。

表 3-25　相関イベント 5.4 以上のデータ フィールド（続き）

フィールド	データ タイプ	説明
送信元ホスト タイプ	uint8	送信元ホストのタイプ: • 0:ホスト • 1:ルータ • 2:ブリッジ
送信元 VLAN ID	uint16	送信元ホストの VLAN ID 番号（該当する場合）。
送信元 OS フィンガープリント UUID	uint8[16]	送信元ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID。 フィンガープリント ID にマップする値の取得の詳細については、サーバ レコード（4-16 ページ）を参照してください。
送信元重要度	uint16	送信元ホストの、ユーザ定義の重要度値: • 0:なし • 1:低 • 2:中 • 3:高
送信元ユーザ ID	uint32	システムにより識別される、送信元ホストにログインしたユーザの ID 番号。
送信元ポート	uint16	イベントの送信元ポート。
送信元サーバ ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
宛先 IP アドレス	uint8[4]	このフィールドは予約済みですが、設定されておりません。宛先 IPv4 アドレスは、宛先 IPv6 アドレス フィールドに保存されます。詳細については、IP アドレス（1-5 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: • 0:ホスト • 1:ルータ • 2:ブリッジ
宛先 VLAN ID	uint16	宛先ホストの VLAN ID 番号（該当する場合）。
宛先 OS フィンガープリント UUID	uint8[16]	宛先ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID 番号。 フィンガープリント ID にマップする値の取得の詳細については、サーバ レコード（4-16 ページ）を参照してください。
宛先重要度	uint16	宛先ホストの、ユーザ定義の重要度値: • 0:なし • 1:低 • 2:中 • 3:高

表 3-25　相関イベント 5.4 以上のデータ フィールド(続き)

フィールド	データ タイプ	説明
宛先ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
接続先ポート	uint16	イベントの宛先ポート。
宛先サービス ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
影響	uint8	イベントの影響フラグ値。値は次のとおりです。 • 1:レッド(脆弱) • 2:オレンジ(脆弱の可能性あり) • 3:イエロー(現在は脆弱でない) • 4:ブルー(不明なターゲット) • 5:グレー(不明なインパクト)
ブロック	uint8	侵入イベントをトリガーしたパケットの処理を示す値。 • 0:侵入イベントがドロップされていない • 1:侵入イベントがドロップされている(展開がインライン型、スイッチ型、またはルーティング型である場合はドロップ) • 2:侵入ポリシーが、インライン型、スイッチ型、またはルーティング型展開のデバイスに適用されている場合は、イベントをトリガーしたパケットがドロップされている可能性がある。
侵入ポリシー(Intrusion Policy)	uint8[16]	イベントに関連付けられた侵入ポリシーの UUID。
ルール アクション	uint32	イベントをトリガーしたルールのユーザ 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 (4-73 ページ)を参照してください。
文字列ブロック長	uint32	イベント説明の文字列ブロックのバイト数。これには、文字列ブロック タイプ用の 4 バイト、文字列ブロック長用の 4 バイト、および NetBIOS ドメイン内のバイト数が含まれます。
NetBIOS ドメイン(NetBIOS Domain)	string	NetBIOS ドメインの名前。
URL カテゴリ	uint32	URL カテゴリを指定する番号。詳細については、URL カテゴリ レコード メタデータ (4-25 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 (4-73 ページ)を参照してください。

表 3-25　相関イベント 5.4 以上のデータ フィールド（続き）

フィールド	データ タイプ	説明
文字列ブロック長	uint32	イベント説明の文字列ブロックのバイト数。これには、文字列ブロック タイプ用の 4 バイト、文字列ブロック長用の 4 バイト、および URL のバイト数が含まれます。
URL	string	関連イベントをトリガーした URL です。
Client ID	uint32	イベントを検出したクライアントの ID 番号。
文字列ブロック タイプ	uint32	クライアント バージョンを含む文字列データ ブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、文字列データ ブロック (4-73 ページ)を参照してください。
文字列ブロック長	uint32	イベント説明の文字列ブロックのバイト数。これには、文字列ブロック タイプ用の 4 バイト、文字列ブロック長用の 4 バイト、およびクライアント バージョン内のバイト数が含まれます。
クライアント バージョン（Client Version）	string	イベントを検出したクライアントのバージョン。
アクセス制御ポリシーのリビジョン	uint8[16]	トリガーされた相関イベントに関連付けられたルールのリビジョン番号。
アクセス コントロール ルール ID	uint32	イベントをトリガーしたルールの内部 ID。
入力インターフェイス UUID	uint8[16]	相関イベントに関連付けられている入力インターフェイスの固有識別子として機能するインターフェイス ID。
出力インターフェイス UUID	uint8[16]	相関イベントに関連付けられている出力インターフェイスの固有識別子として機能するインターフェイス ID。
入力ゾーン UUID	uint8[16]	相関イベントに関連付けられている入力セキュリティ ゾーンの固有識別子として機能するゾーン ID。
出力ゾーン UUID	uint8[16]	相関イベントに関連付けられている出力セキュリティ ゾーンの固有識別子として機能するゾーン ID。
送信元 IPv6 アドレス	uint8[16]	IPv6 アドレス オクテットの、イベントの送信元ホストの IP アドレス。
宛先 IPv6 アドレス	uint8[16]	IPv6 アドレス オクテットの、イベントの宛先ホストの IP アドレス。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
セキュリティ インテリジェンス UUID	uint8[16]	セキュリティ インテリジェンスに設定されたアクセス コントロール ポリシーの UUID。

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
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。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

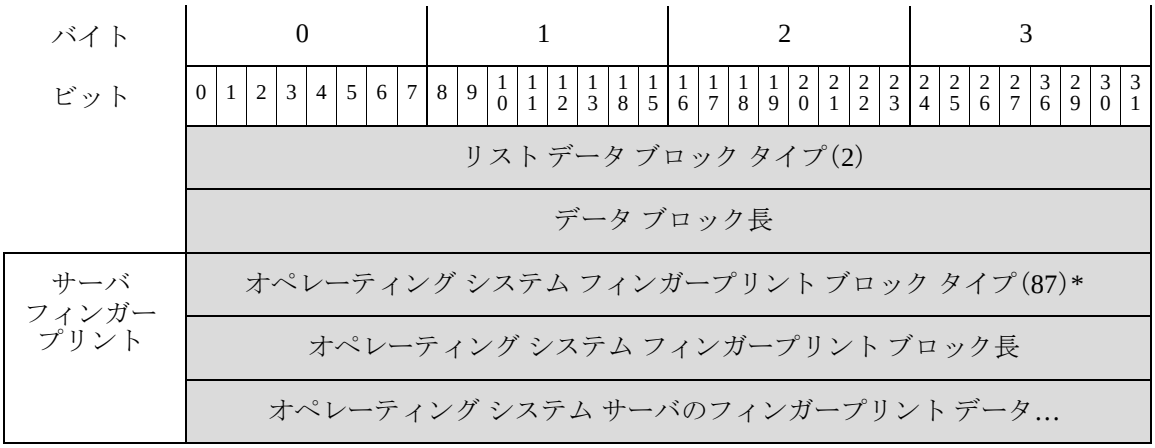
表 3-25　相関イベント 5.4 以上のデータ フィールド(続き)

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

シリーズ 2 のデータ ブロックの概要

バージョン 4.10.0 から、eStreamer サービスは、2 番目のシリーズのデータ ブロックを使用して、侵入イベント追加データなどの特定のレコードをパッケージしています。このシリーズのすべてのブロック タイプのリストの詳細については、表 3-26（3-58 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示します。リスト データ ブロック（シリーズ 2 のブロック タイプ 31）は、多数のオペレーティング システムのフィンガープリントを定義しています（各データ ブロック自体が可変長のタイプ 87 のブロックです）。一般的なタイプ 31 のデータ ブロックの長さは、データ ブロック長フィールドによる自己記述的です。ブロック タイプとブロック長フィールドの 8 バイトを除いた、メッセージのデータ部分の長さが含まれています。



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

表 3-26　シリーズ 2 のブロック タイプ

タイプ（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 (3-29 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 (3-69 ページ) を参照してください。
20	ICMP コードのデータ ブロック	現在（Current）	ICMP コードを示すメタデータが含まれています。ICMP コードのデータ ブロック (3-71 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 (3-81 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 (3-82 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（3-107 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（3-110 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（3-118 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（3-96 ページ）。
39	IOC 名のデータ ブロック	現在（Current）	IOC に関する情報が含まれています。5.3+ の IOC 名データ ブロック（4-37 ページ）を参照してください
40	ファイル イベント SHA ハッシュ	現在（Current）	マルウェアが含まれていると認識されたファイルの SHA ハッシュと名前が含まれています。5.3 以上のファイル イベント SHA ハッシュ（3-107 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（3-85 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（3-96 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（3-96 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（3-96 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（3-96 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（2-26 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

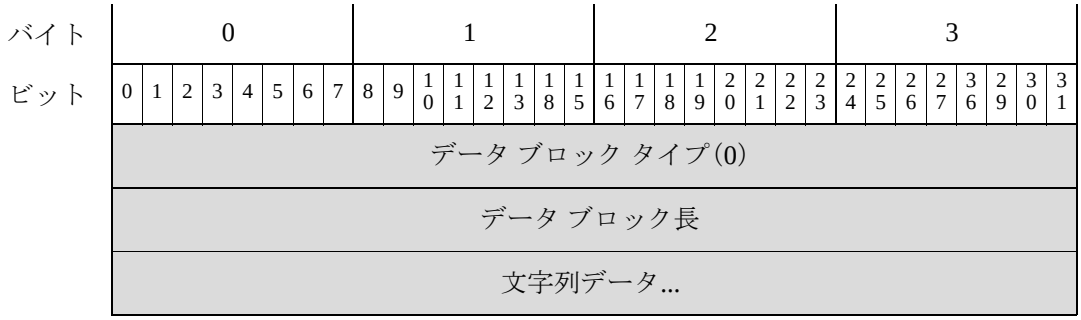
eStreamer サービスは、文字列データ ブロックを使用してメッセージの文字列データを送信します。通常、これらのブロックは、オペレーティング システムやサーバ名などを識別するために他のデータ ブロック内に表示されます。

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。

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

次の図に、文字列データ ブロックの形式を示します。



次の表は、文字列データ ブロックのフィールドについての説明です。

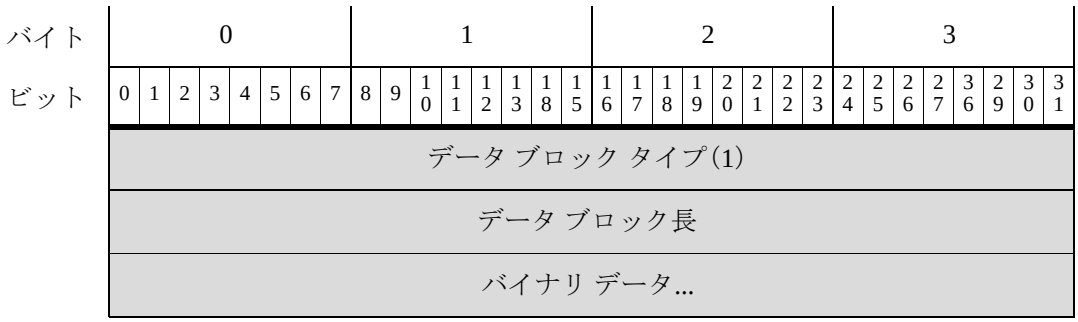
表 3-27　文字列ブロック フィールド

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

BLOB データ ブロック

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

次の図に、BLOB データ ブロックの形式を示します。



次の表は、BLOB データ ブロックのフィールドについての説明です。

表 3-28　BLOB データ ブロック フィールド

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

次の表は、リスト データ ブロックのフィールドについての説明です。

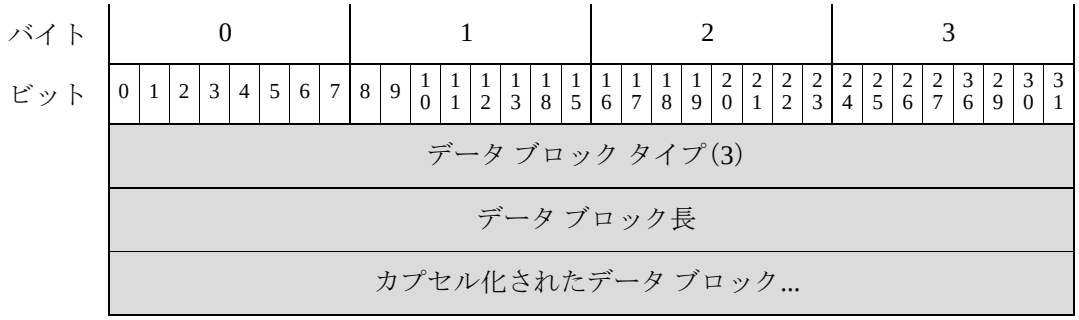
表 3-29　リスト データ フィールド

フィールド	データ タイプ	説明
ブロック タイプ（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と、この値には、サブサーバ ブロックの合計バイト数とリスト ブロック ヘッダーの 8 バイトが含まれることになります。
カプセル化されたデータ ブロック	変数（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。



次の表は、汎用リストのデータ ブロックのフィールドについての説明です。

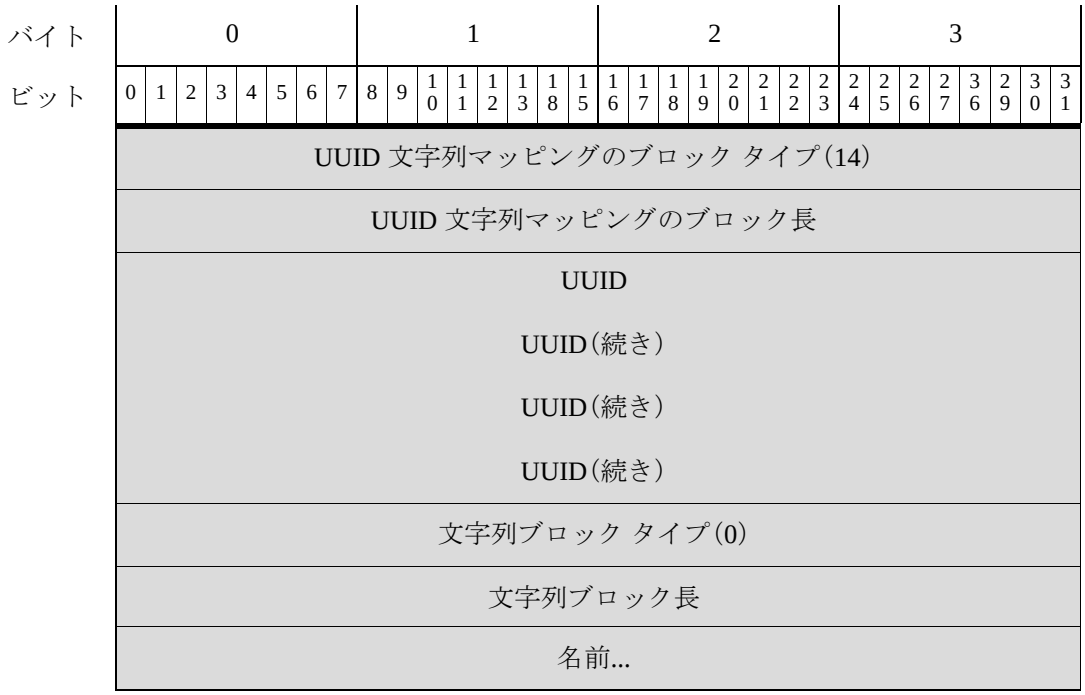
表 3-30　汎用リストのデータ ブロック フィールド

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

UUID 文字列マッピングのデータ ブロック

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

次の図に、UUID 文字列マッピングのデータ ブロックの構造を示します。



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

表 3-31　UUID 文字列マッピングのデータ ブロック フィールド

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

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	unit32	ID が識別するイベントまたは他のオブジェクトの固有識別子。
文字列ブロック タイプ	uint32	ID に関連付けられた名前を含む文字列のデータ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
[名前(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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	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。

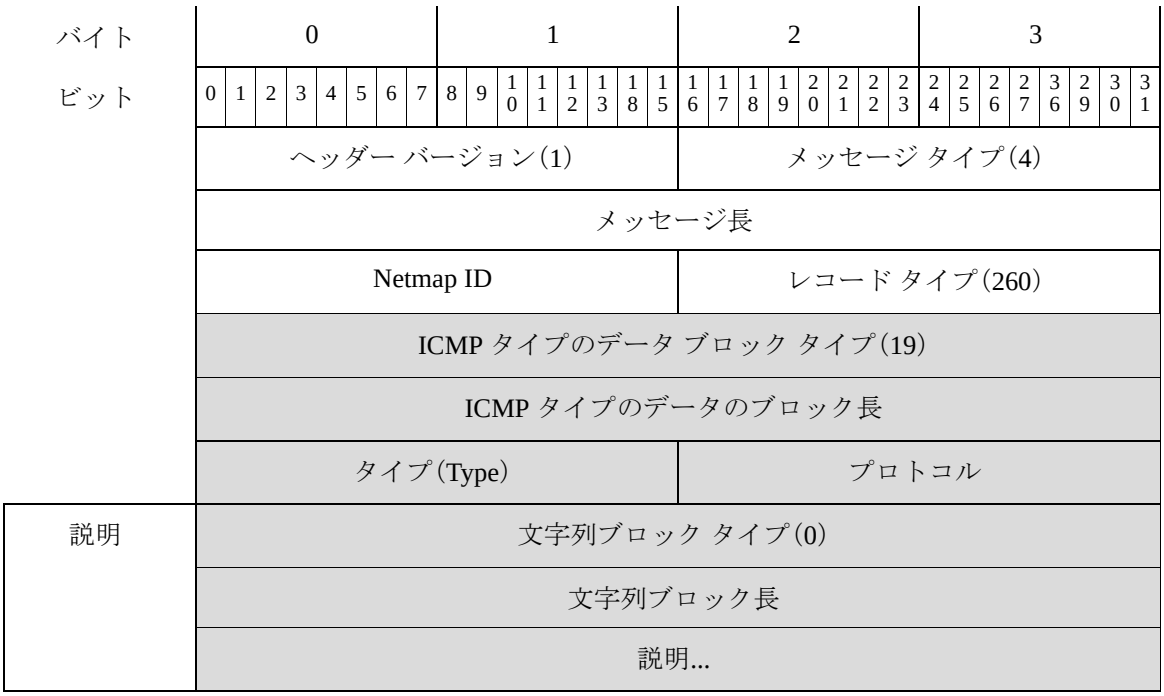
表 3-33　　アクセス コントロール ポリシー ルール ID のメタデータ ブロック フィールド

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

ICMP タイプのデータ ブロック

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

次の図に、ICMP タイプのデータ ブロックの構造を示します。



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。 • 0:IP • 1:ICMP • 6:TCP • 17:UDP
文字列ブロック タイプ	uint32	ICMP タイプの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	イベントの ICMP タイプの説明。

ICMP コードのデータ ブロック

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ヘッダー バージョン(1)																メッセージ タイプ(4)															
	メッセージ長																															
	Netmap ID																レコード タイプ(270)															
	ICMP コードのデータ ブロック タイプ(20)																															
	ICMP コードのデータ ブロック長																															
	コード(Code)																タイプ(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

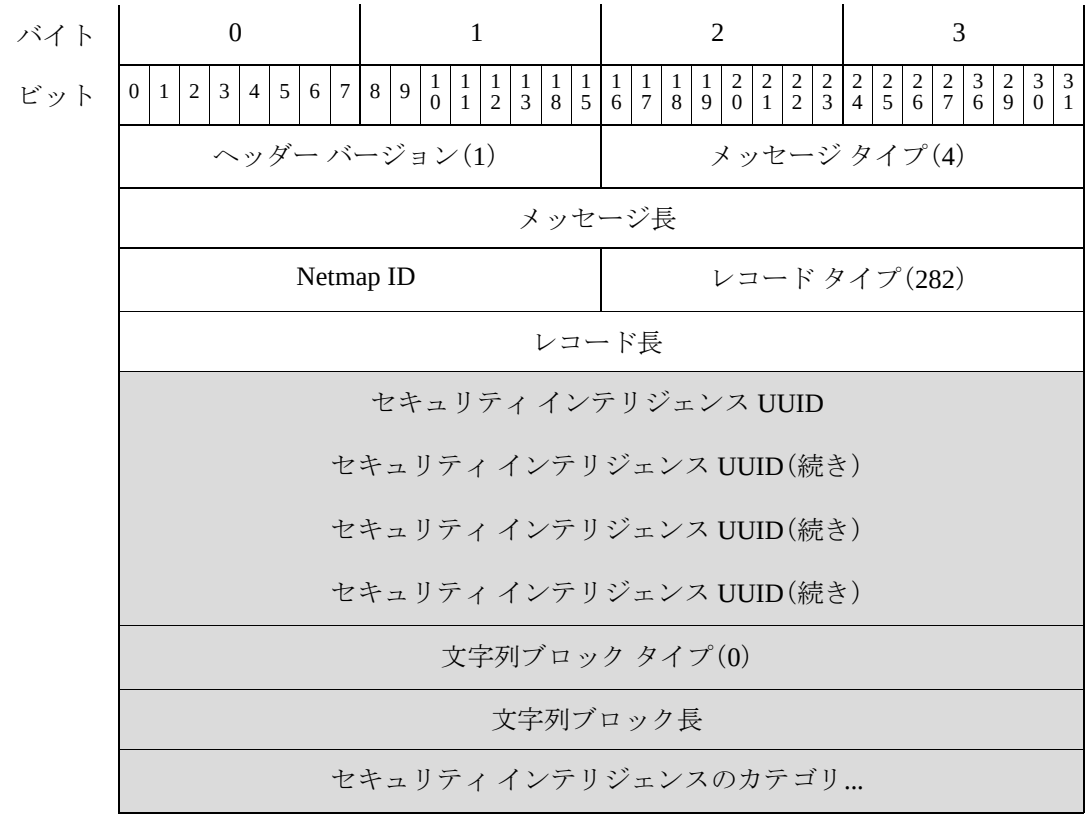
フィールド	データ タイプ	説明
ICMP コードのデータ ブロック タイプ	uint32	ICMP コードのデータ ブロックを開始します。この値は常に 20 です。
ICMP コードのデータ ブロック長	uint32	ICMP コードのデータ ブロックの合計バイト数です。ICMP コードのデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
コード(Code)	uint16	イベントの ICMP コード。
タイプ(Type)	uint16	イベントの ICMP タイプ。

表 3-35　ICMP コードのデータ ブロック フィールド(続き)

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

5.4.1 以上のセキュリティ インテリジェンス カテゴリのメタデータ

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



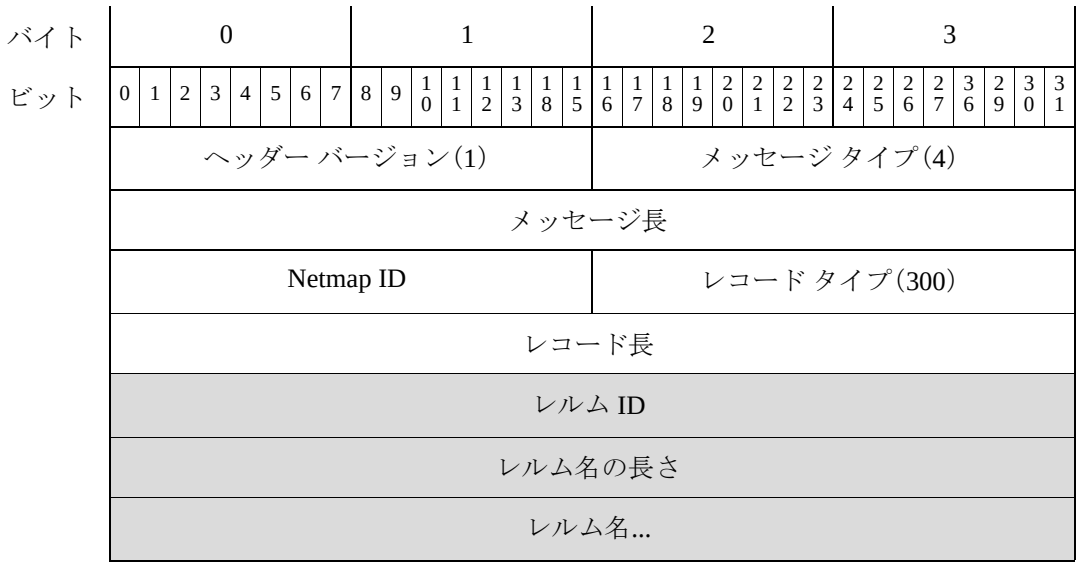
次の表は、セキュリティ コンテキスト名のレコードのフィールドについての説明です。

表 3-36　セキュリティ コンテキスト名のレコード フィールド

フィールド	データ タイプ	説明
セキュリティ インテリジェンス UUID	uint8[16]	セキュリティ インテリジェンスの UUID。
文字列ブロック タイプ	uint32	セキュリティ インテリジェンス カテゴリを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	セキュリティ インテリジェンス カテゴリの文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとプロファイル名フィールドのバイト数が含まれます。
セキュリティ インテリジェンスのカテゴリ（Security Intelligence Category）	string	セキュリティ インテリジェンスのカテゴリ。

6.0 以上のレルムのメタデータ

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



次の表は、レルムのメタデータのレコードのフィールドについての説明です。

表 3-37　レルムのメタデータのレコード フィールド

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

6.0 以上のエンドポイント プロファイルのデータ ブロック

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

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

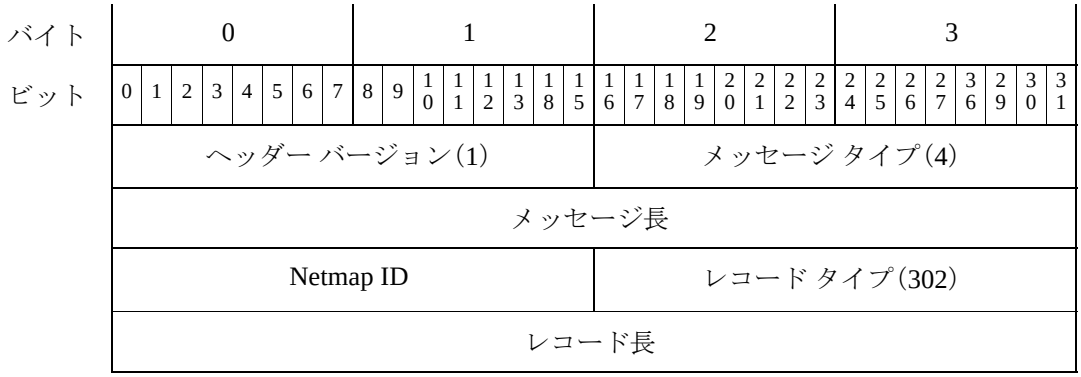
次の表は、エンドポイント プロファイルのデータ ブロックのフィールドについての説明です。

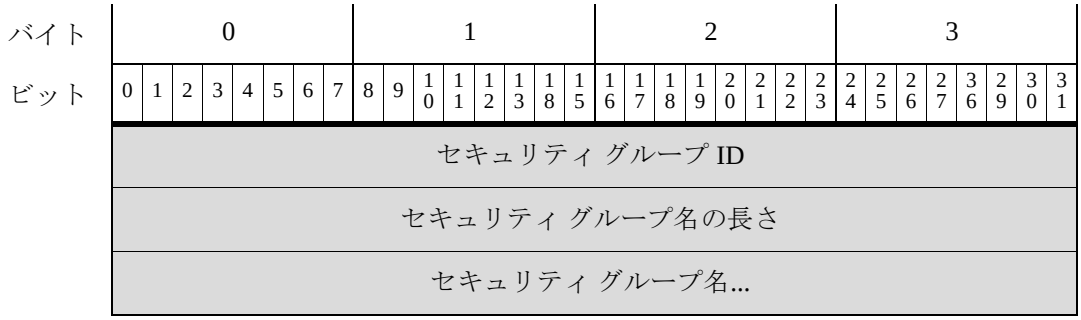
表 3-38　エンドポイント プロファイルのデータ ブロック フィールド

フィールド	データ タイプ	説明
エンドポイント プロファイルのデータ ブロック タイプ	uint32	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。
文字列ブロック長	uint32	正式名称の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと正式名称フィールドのバイト数が含まれます。
正式名称	string	プロファイルの完全修飾名。エンドポイントのタイプの関係階層を示します。

6.0 以上のセキュリティ グループのメタデータ

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





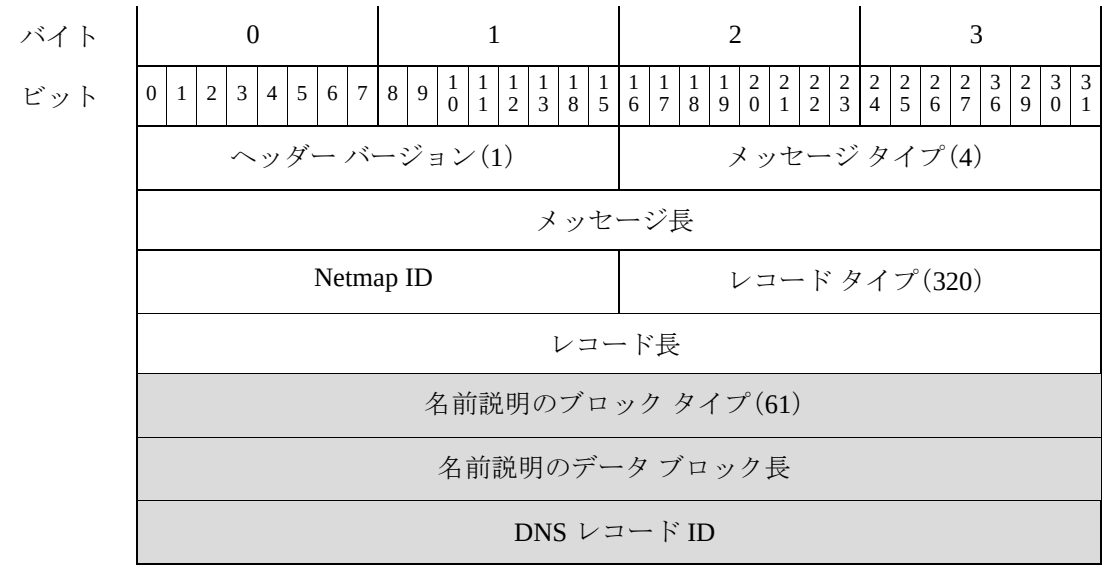
次の表は、セキュリティ グループのメタデータのレコードのフィールドについての説明です。

表 3-39　セキュリティ グループのメタデータのレコード フィールド

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

6.0 以上の DNS レコード タイプのメタデータ

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



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
DNS 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。
文字列ブロック タイプ	uint32	DNS レコード タイプの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	DNS レコード タイプ名文字列のデータ ブロック内に含まれるバイト数。これには、ブロック タイプ フィールドおよびヘッダー フィールド用の 8 バイトと、DNS レコード タイプ名フィールド内のバイト数が含まれます。
DNS レコード タイプ名	string	DNS レコード タイプの名前。
文字列ブロック タイプ	uint32	DNS レコード タイプの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	DNS レコード タイプ説明文字列のデータ ブロック内に含まれるバイト数。これには、ブロック タイプ フィールドおよびヘッダー フィールド用の 8 バイトと、DNS レコード タイプ説明フィールド内のバイト数が含まれます。
DNS レコード タイプの説明	string	DNS レコード タイプの説明。

6.0 以上の DNS レスポンス タイプのメタデータ

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

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	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(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																															
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

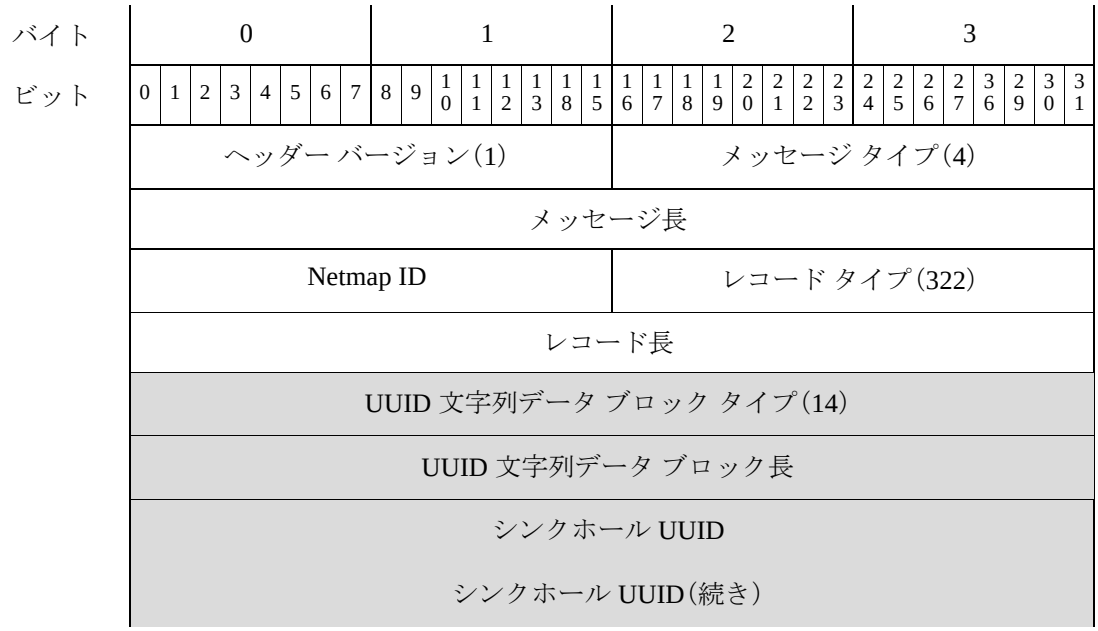
フィールド	データ タイプ	説明
名前説明のデータ ブロック タイプ	uint32	名前説明のデータ ブロックを開始します。この値は常に 61 です。
名前説明のデータ ブロック長	uint32	名前説明のデータ ブロック内の総バイト数。これには、名前説明のデータ ブロックのタイプ フィールドおよび長さフィールド用の 8 バイトと、その後のデータのバイト数が含まれます。
DNS 応答 ID	uint32	DNS レスポンス ID 番号。

表 3-41　DNS レスポンス タイプのメタデータ フィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック 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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	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。

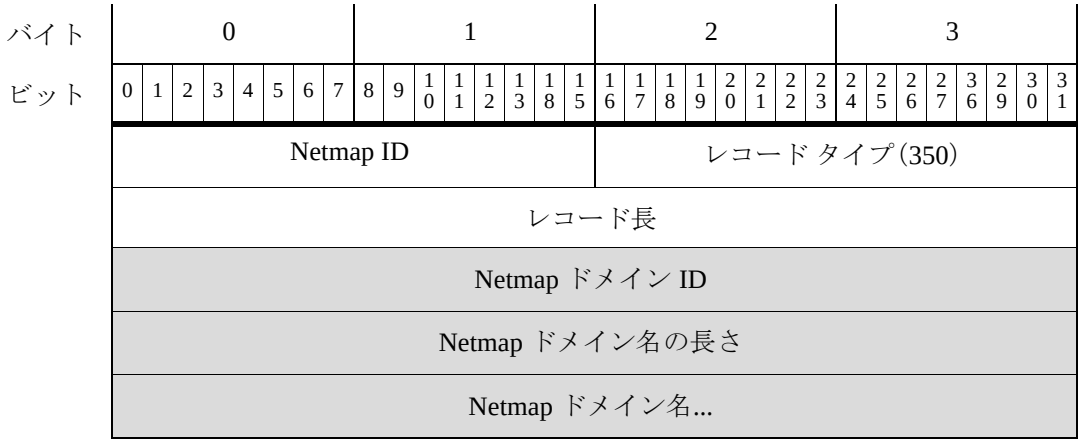
表 3-42　シンクホールのメタデータのレコード フィールド

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。
文字列ブロック タイプ	uint32	シンクホールの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	シンクホール名文字列のデータ ブロック内に含まれるバイト数。これには、ブロック タイプ フィールドおよびヘッダー フィールド用の 8 バイトと、シンクホール名フィールド内のバイト数が含まれます。
シンクホール名	string	シンクホールの名前。

6.0 以上の Netmap ドメインのメタデータ

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

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



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

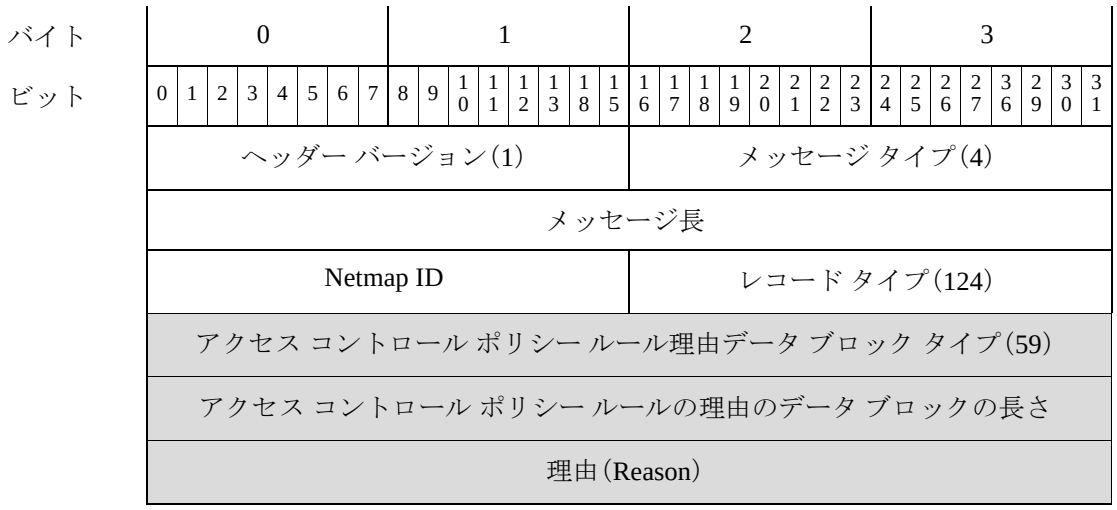
表 3-43　　シンクホールのメタデータのレコード フィールド

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

6.0 以上のアクセス コントロール ポリシー ルール理由データ ブロック

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

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



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	説明...																															

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

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

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

アクセス コントロール ポリシー名のデータ ブロック

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	アクセス コントロール ポリシー名のデータ ブロック タイプ（64）																															
	アクセス コントロール ポリシー名のデータ ブロック長 アクセス コントロール ポリシー UUID アクセス コントロール ポリシー UUID（続き） アクセス コントロール ポリシー UUID（続き） アクセス コントロール ポリシー UUID（続き）																															
	センサー ID																															
[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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	IP レピュテーション カテゴリのデータ ブロック タイプ(22)																															
	IP レピュテーション カテゴリのデータ ブロックの長さ																															
	ルール ID																															
	ポリシー UUID ポリシー UUID(続き) ポリシー UUID(続き) ポリシー UUID(続き)																															
説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	カテゴリ名...																															

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

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

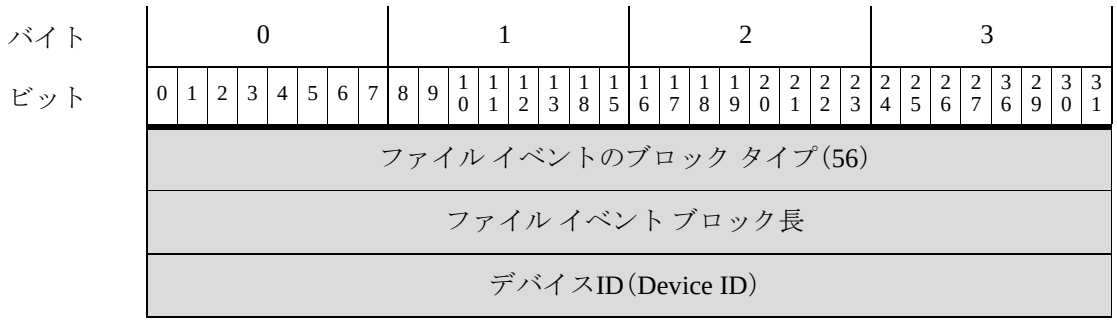
フィールド	データ タイプ	説明
IP レピュテーション カテゴリのデータ ブロック タイプ	uint32	IP レピュテーション カテゴリのデータ ブロックを開始します。この値は常に 22 です。
IP レピュテーション カテゴリのデータ ブロックの長さ	uint32	IP レピュテーション カテゴリのデータ ブロックの合計バイト数です。IP レピュテーション カテゴリのデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID。
ポリシー UUID	uint8[16]	イベントをト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

6.0 以上のファイル イベント

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

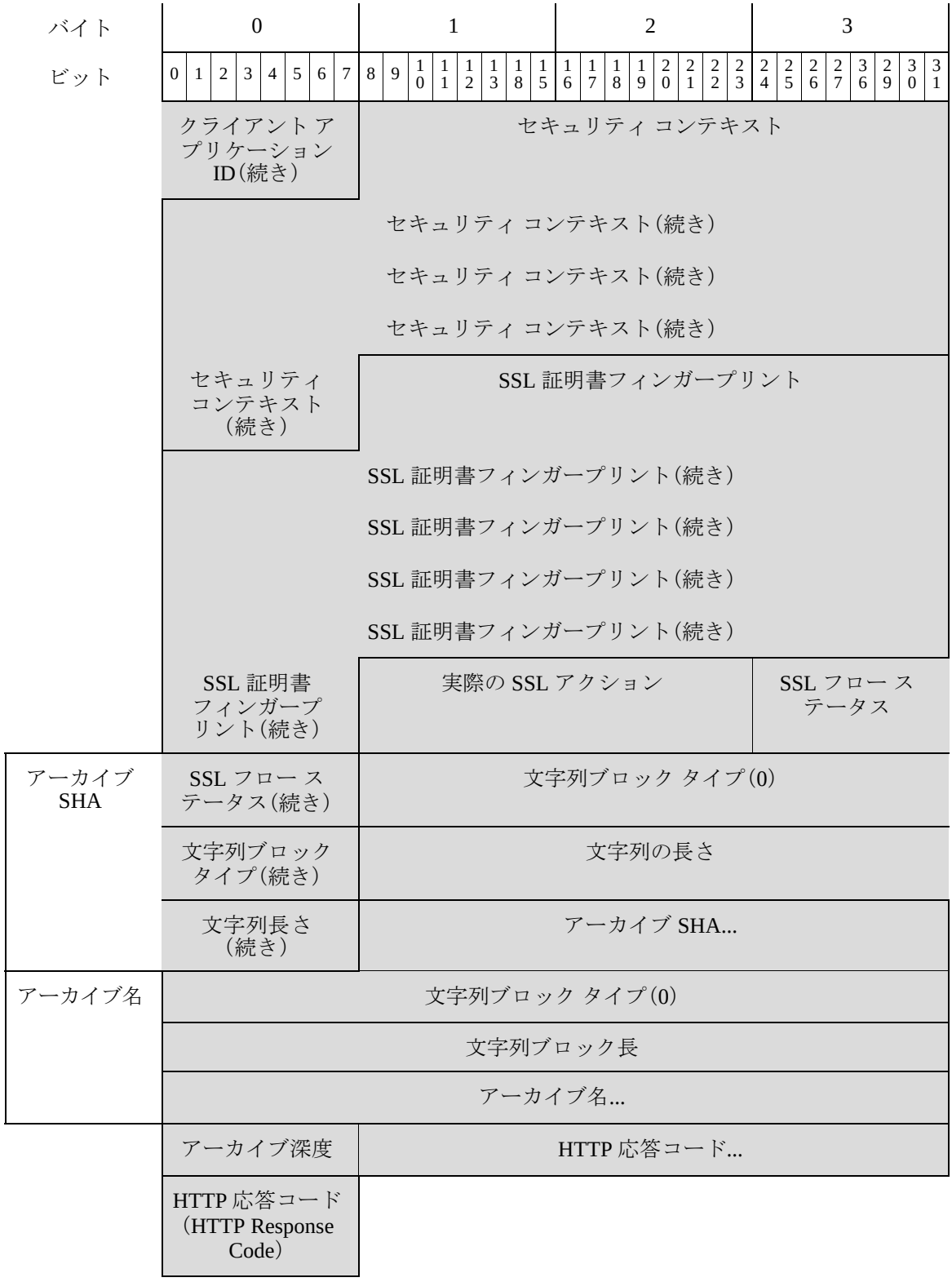
ファイル イベント レコードを要求するには、イベント バージョン 5 およびイベント コード 111 の要求メッセージ内に、ファイル イベント フラグ（要求フラグ フィールドのビット 30）を設定します。要求フラグ（2-12 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

次の図は、ファイル イベント データ ブロックの構造を示しています。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
接続インスタンス																	接続数カウンタ															
接続タイムスタンプ																																
ファイル イベント タイムスタンプ（File Event Timestamp）																																
送信元 IP アドレス 送信元 IP アドレス（続き） 送信元 IP アドレス（続き） 送信元 IP アドレス（続き）																																
宛先 IP アドレス 宛先 IP アドレス（続き） 宛先 IP アドレス（続き） 宛先 IP アドレス（続き）																																
傾向									SPERO 解析結果								ファイル ストレージ ステータス								ファイル分析ステータス							
ローカルのマルウェア分析のステータス									アーカイブ ファイル ステータス								脅威スコア								操作							
SHA ハッシュ SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き） SHA ハッシュ（続き）																																
ファイル タイプ ID																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ファイル名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル名...																															
	ファイル 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																							



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。 • 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。
SPERO 解析結果	uint8	SPERO 署名がファイル分析で使用されたかどうかを示します。値が 1、2、または 3 であれば、SPERO 分析は使用されました。それ以外の値であれば、SPERO 分析は使用されませんでした。

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

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

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

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

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

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

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

フィールド	データ タイプ	説明
ファイル タイプ ID	uint32	ファイル タイプにマップされている ID 番号。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、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。 • 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。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。

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

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

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

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

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

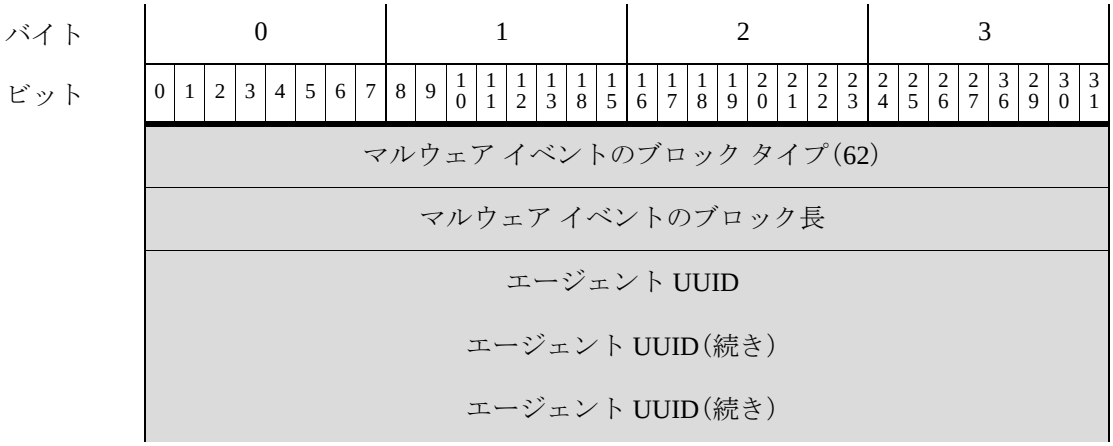
フィールド	データ タイプ	説明
文字列ブロック長	uint32	アーカイブ SHA 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および侵入ポリシー名のバイト数を含む)。
アーカイブ SHA	string	ファイルが含まれる親アーカイブの SHA1 ハッシュ。
文字列ブロック タイプ	uint32	アーカイブ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	アーカイブ名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびアーカイブ名のバイ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

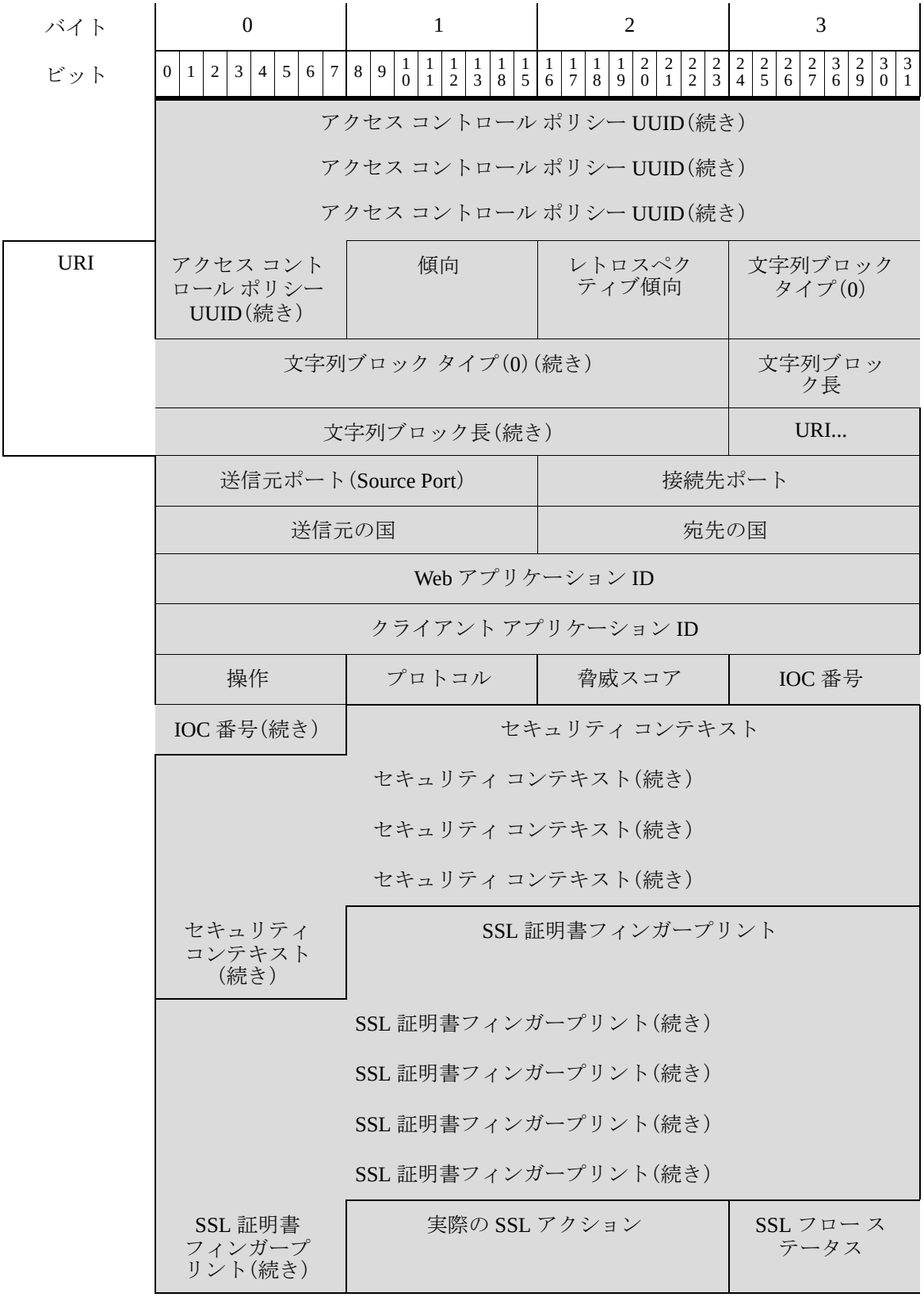
イベント バージョンが 7 でイベント コードが 101 の要求メッセージでマルウェア イベント フラグ([要求フラグ(Request Flags)] フィールドのビット 30)を設定することで、マルウェア イベント レコードの一部としてイベントを要求します。

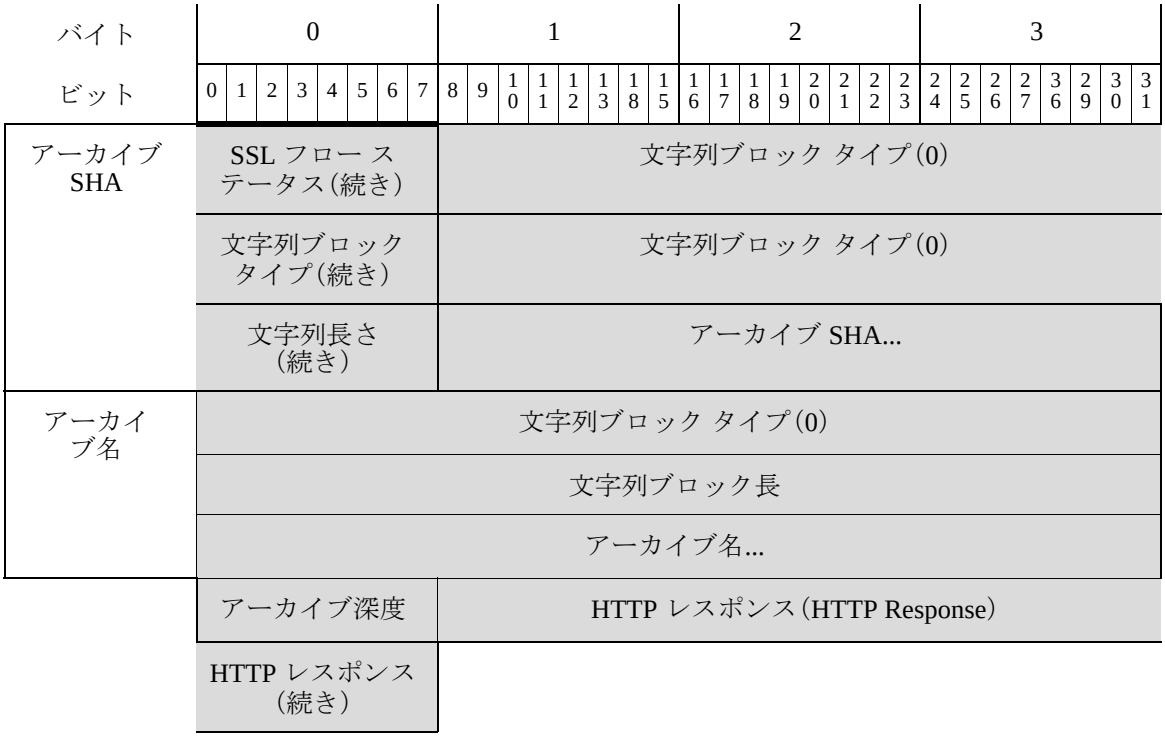
次の図に、マルウェア イベントのデータ ブロックの構造を示します。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	エージェント UUID（続き）																															
	クラウド UUID クラウド UUID（続き） クラウド UUID（続き） クラウド UUID（続き）																															
	マルウェア イベント タイムスタンプ																															
	イベント タイプ ID																															
	イベント サブタイプ ID																															
検出名	ディテクタ ID								文字列ブロック タイプ（0）																							
	文字列ブロック タイプ（0）（続き）								文字列ブロック長																							
	文字列ブロック長（続き）								検出名...																							
ユーザ（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	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ファイル タイプ																															
	ファイルのタイムスタンプ																															
親ファイル [名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル名...																															
親ファイル SHA ハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル SHA ハッシュ...																															
イベント 説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	イベントの説明...																															
	デバイス ID(Device ID)																															
	接続インスタンス																接続数カウンタ															
	接続イベント タイムスタンプ																															
	方向(Direction)								送信元 IP アドレス																							
	送信元 IP アドレス(続き)																															
	送信元 IP アドレス(続き)																															
	送信元 IP アドレス(続き)																															
	送信元 IP(続き)								宛先IPアドレス																							
	宛先 IP アドレス(続き)																															
	宛先 IP アドレス(続き)																															
	宛先 IP アドレス(続き)																															
	宛先 IP(続き)								アプリケーション ID(Application ID)																							
	アプリケーション ID(続き)								ユーザ 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 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
アクセス コントロール ポリシー UUID(続き)
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



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。 • 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。 • 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	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト • 6:クラウド ルックアップのタイムアウト • 7:カスタム検出 • 8:カスタム検出ブロック • 9:アーカイブ ブロック(深度超過) • 10:アーカイブ ブロック(暗号化されている) • 11:アーカイブ ブロック(調査エラー)
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ～ 100)。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

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 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

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

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

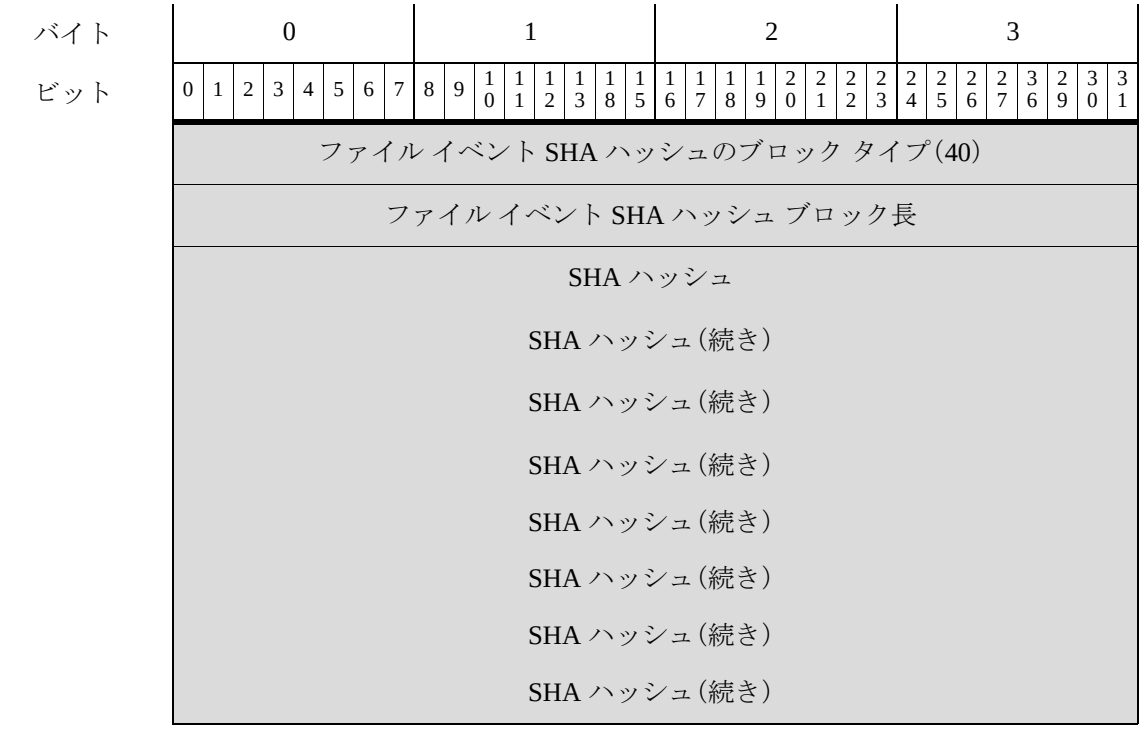
表 3-48　6.0 以上のマルウェア イベントのデータ ブロック フィールド(続き)

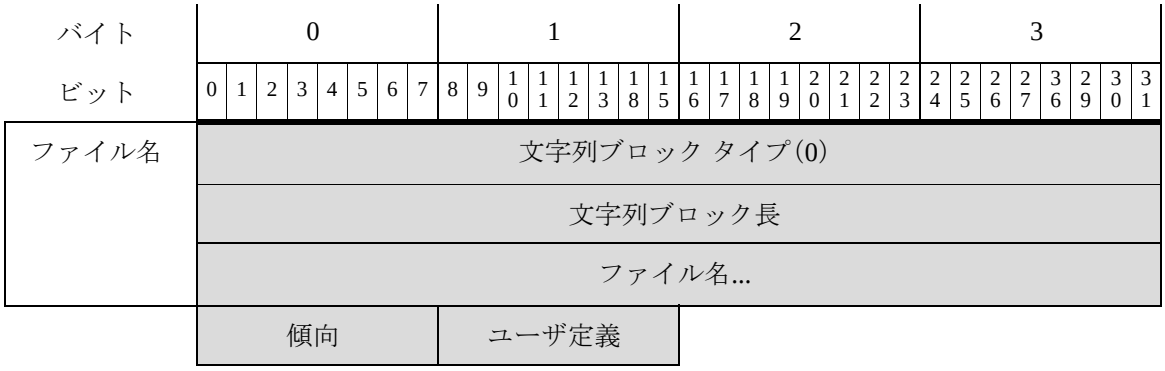
フィールド	データ タイプ	説明
文字列ブロック長	uint32	アーカイブ SHA 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および侵入ポリシー名のバイト数を含む)。
アーカイブ SHA	string	ファイルが含まれる親アーカイブの SHA1 ハッシュ。
文字列ブロック タイプ	uint32	アーカイブ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	アーカイブ名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびアーカイブ名のバイ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





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

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

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

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

フィールド	データ タイプ	説明
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4:UNAVAILABLE。ソフトウェアから AMP 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。 • 0:AMP 定義 • 1:ユーザ定義

5.3 以上のファイル タイプ ID のメタデータ

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ヘッダー バージョン(1)																	メッセージ タイプ(4)															
メッセージ長																																
Netmap ID																	レコード タイプ(510)															
レコード長																																
ファイル タイプ ID																																
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。
ファイル タイプの長さ	uint32	ファイル タイプ名に含まれるバイト数。
ファイル タイプ名	string	ファイル タイプ名の記述名。

5.2 以上のルール ドキュメントのデータ ブロック

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

次の図に、ルール ドキュメントのデータ ブロックの構造を示します。

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
影響を受けるシステム	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...																															
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。
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。

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)

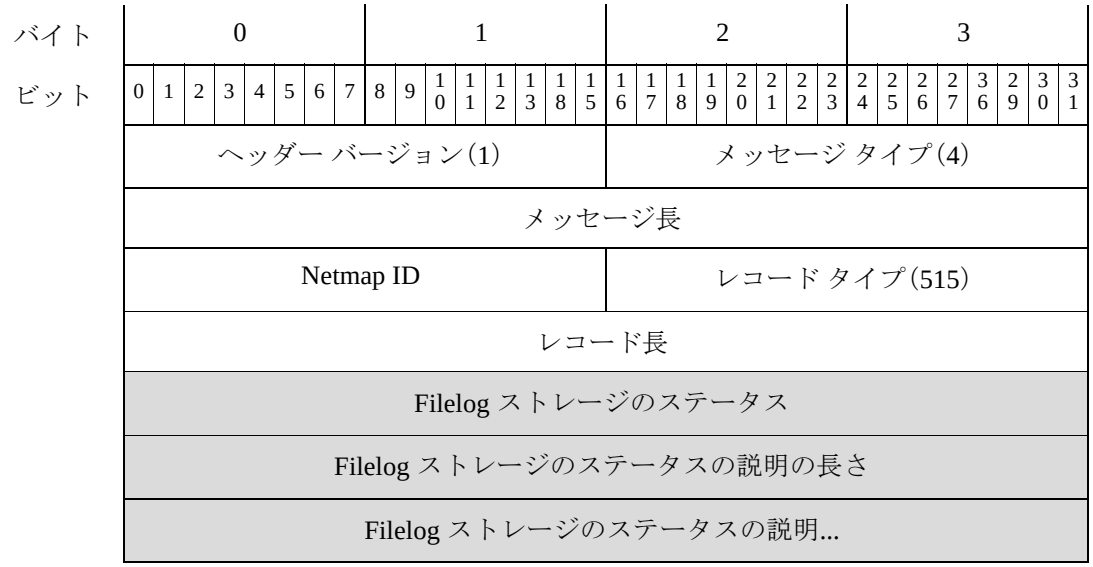
フィールド	データ タイプ	説明
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと攻撃のシナリオ フィールドのバイト数が含まれます。
攻撃のシナリオ	string	潜在的な攻撃の例。
文字列ブロック タイプ	uint32	ルールに関連付けられた攻撃のしやすさを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと攻撃のしやすさフィールドのバイト数が含まれます。
攻撃のしやすさ	string	攻撃の難易度(simple、medium、hard、または difficult)と、その攻撃がスクリプトを使用して実行できるものであるかどうか。
文字列ブロック タイプ	uint32	ルールに関連付けられた潜在的な誤検出を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと誤検出フィールドのバイト数が含まれます。
誤検出	string	誤検出となる可能性のある例。デフォルト値は None Known です。
文字列ブロック タイプ	uint32	ルールに関連付けられた潜在的な検出漏れを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと検出漏れフィールドのバイト数が含まれます。
検出漏れ	string	検出漏れとなる可能性のある例。デフォルト値は None Known です。
文字列ブロック タイプ	uint32	ルールに関連付けられた修正処置を含む文字列データ ブロックを開始します。この値は常に 0 です。
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。

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
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとその他の参考資料フィールドのバイト数が含まれます。
その他の参考資料	string	その他の情報およびリファレンス。

6.0 以上の Filelog ストレージのメタデータ

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



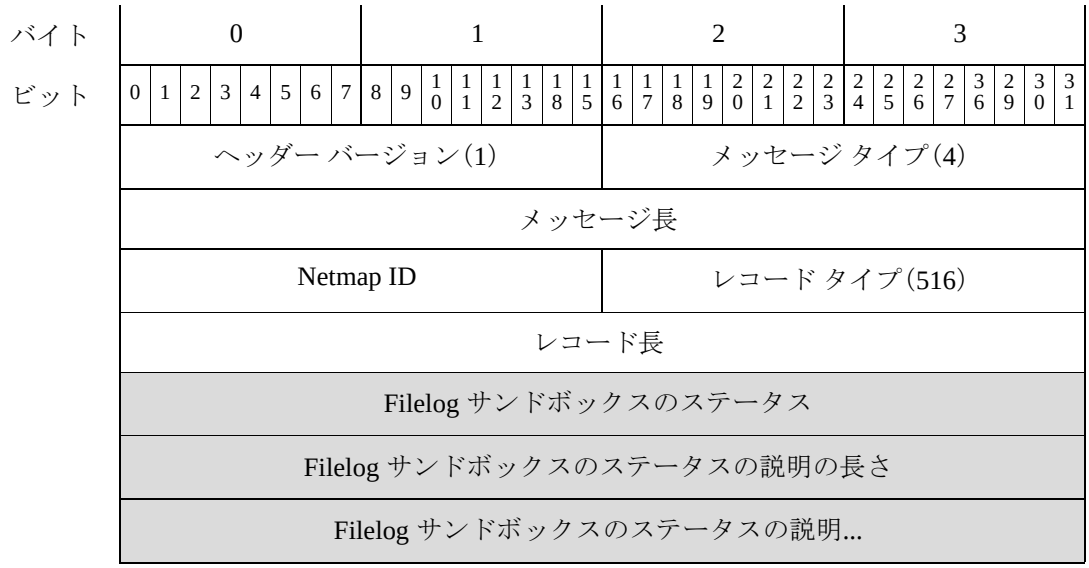
次の表は、Filelog ストレージのメタデータのレコードのフィールドについての説明です。

表 3-52　Filelog ストレージのメタデータのレコード フィールド

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

6.0 以上の Filelog サンドボックスのメタデータ

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



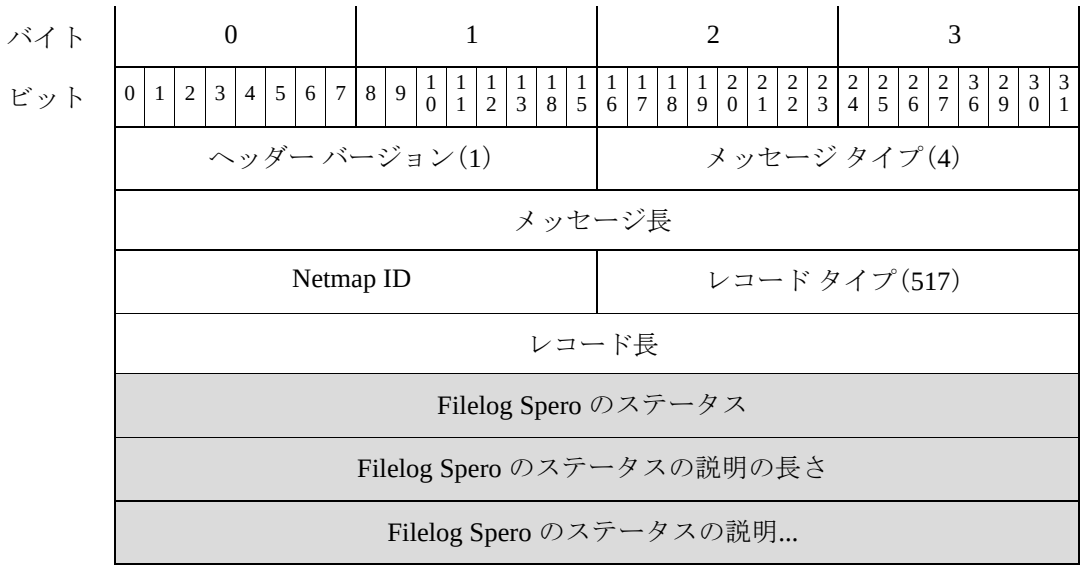
次の表は、Filelog サンドボックスのメタデータのレコードのフィールドについての説明です。

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

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

6.0 以上の Filelog Spero のメタデータ

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



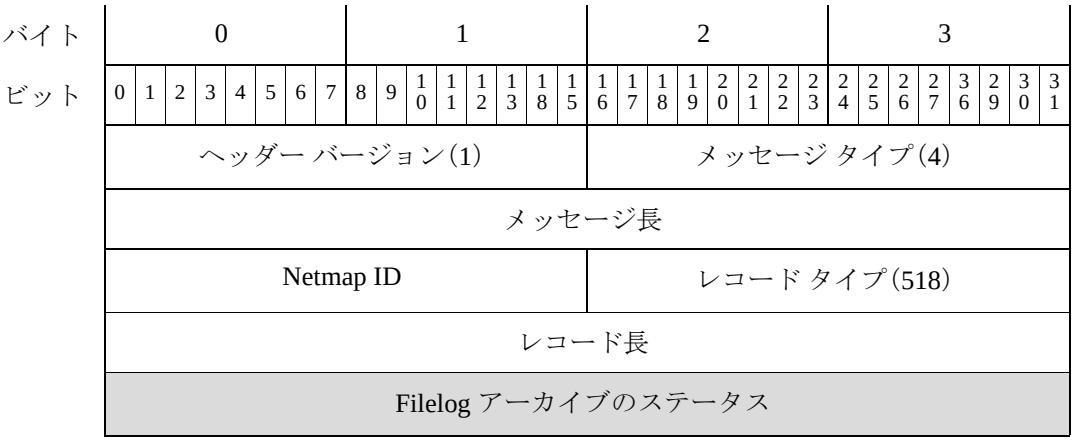
次の表は、Filelog Spero のメタデータのレコードのフィールドについての説明です。

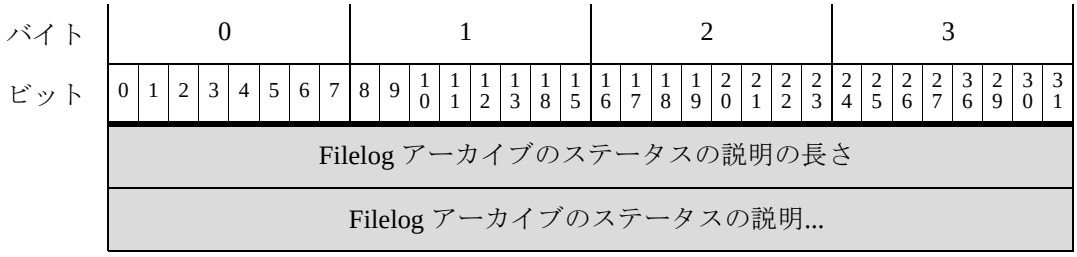
表 3-54　Filelog Spero のメタデータのレコード フィールド

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

6.0 以上の Filelog アーカイブのメタデータ

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





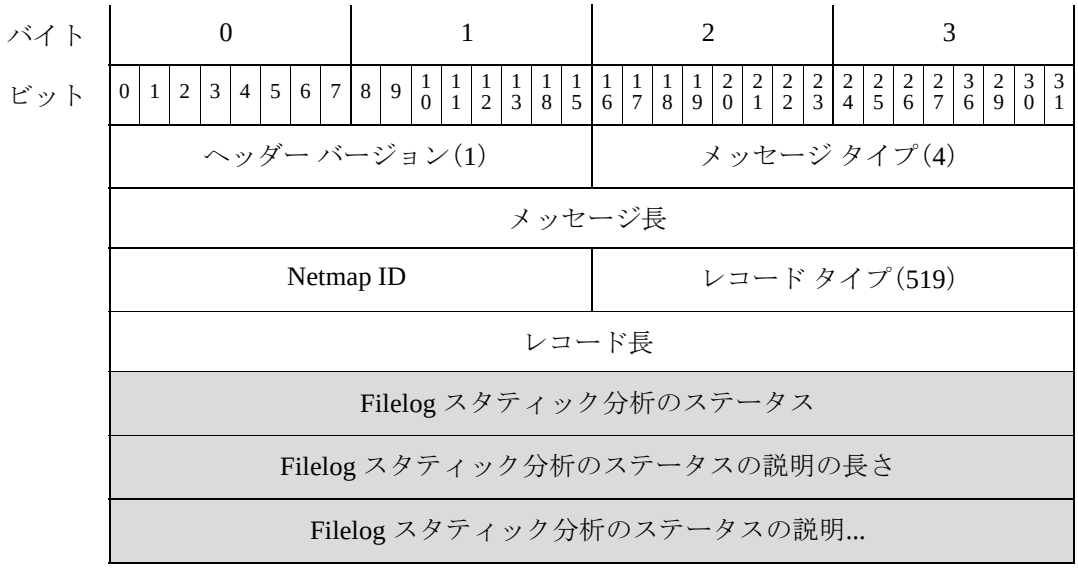
次の表は、Filelog アーカイブのメタデータのレコードのフィールドについての説明です。

表 3-55　Filelog アーカイブのメタデータのレコード フィールド

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

6.0 以上の Filelog スタティック分析のメタデータ

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



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

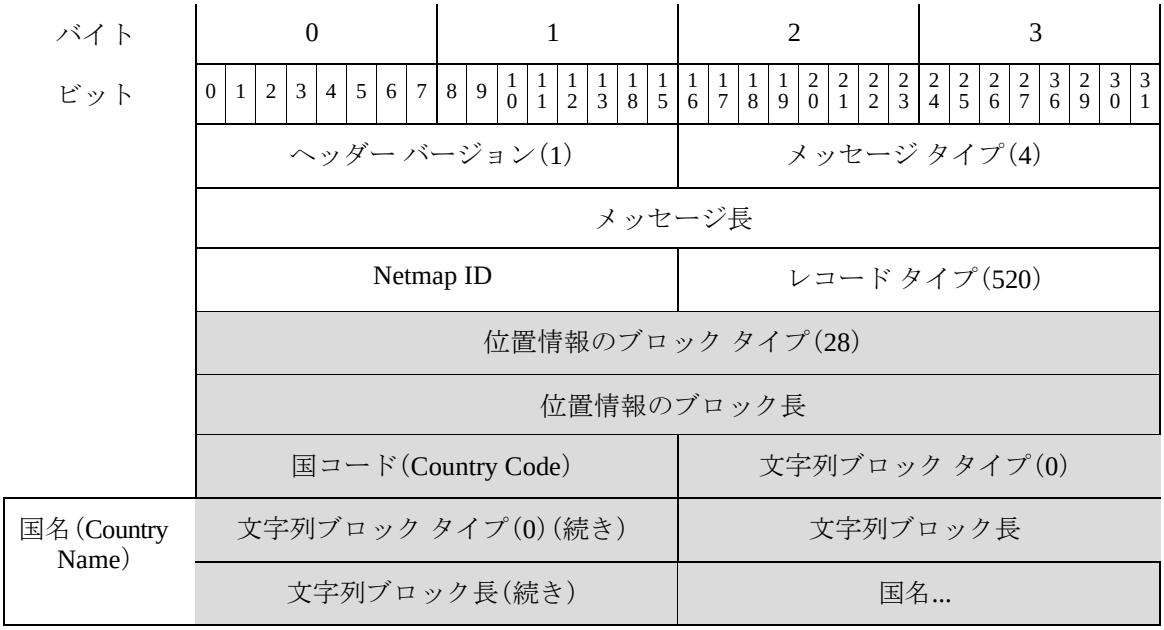
表 3-56　Filelog スタティック分析のメタデータのレコード フィールド

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

5.2 以上の位置情報のデータ ブロック

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

次の図に、位置情報のデータ ブロックの構造を示します。



次の表は、位置情報のデータ ブロックのフィールドについての説明です。

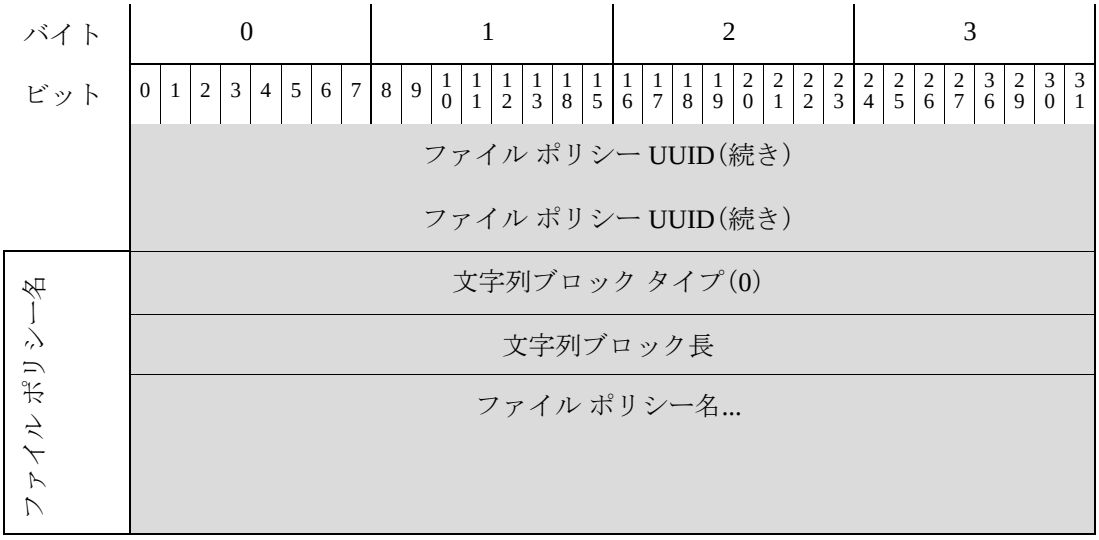
表 3-57　位置情報のデータ ブロック フィールド

フィールド	データ タイプ	説明
位置情報のデータ ブロック タイプ	uint32	位置情報のデータ ブロックを開始します。この値は常に 28 です。
位置情報のデータ ブロック長	uint32	位置情報のデータ ブロックの合計バイト数です。位置情報のデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
国コード（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（2-12 ページ）を参照してください）。メッセージ長フィールドの後に表示されるレコード タイプ フィールドにファイル ポリシー名レコードを示す値 530 があることに注意してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（530）															
レコード長																																
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）																																



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

SSL ポリシー名

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

次の表は、SSL ポリシー名のレコードのフィールドについての説明です。

表 3-59　SSL ポリシー名レコード フィールド

フィールド	データ タイプ	説明
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
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。

表 3-59　SSL ポリシー名レコード フィールド(続き)

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

SSL ルール ID

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

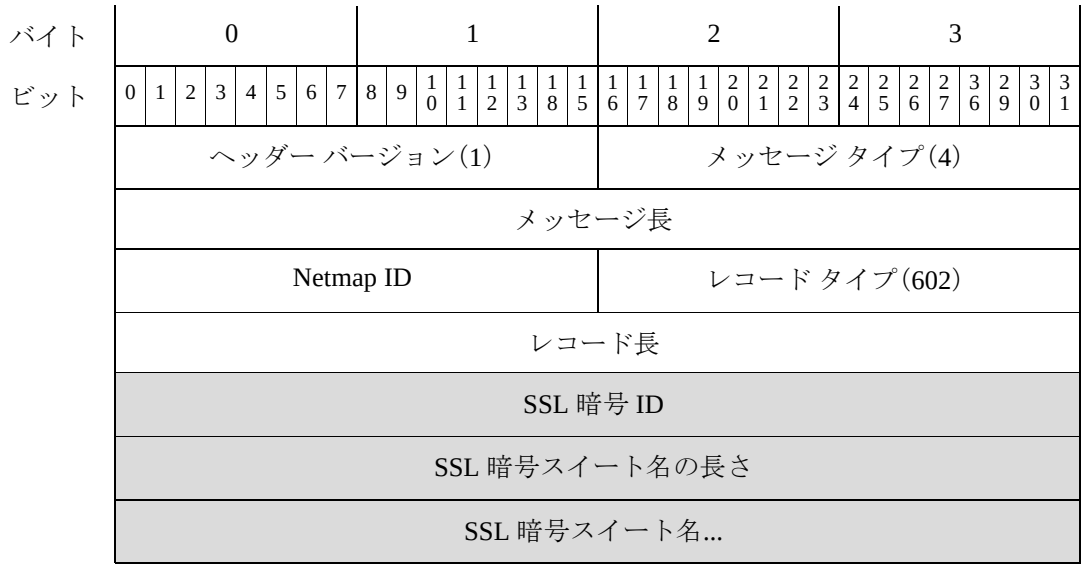
次の表は、SSL ルール ID レコードのフィールドについての説明です。

表 3-60　SSL ポリシー名レコード フィールド

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

SSL 暗号スイート

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



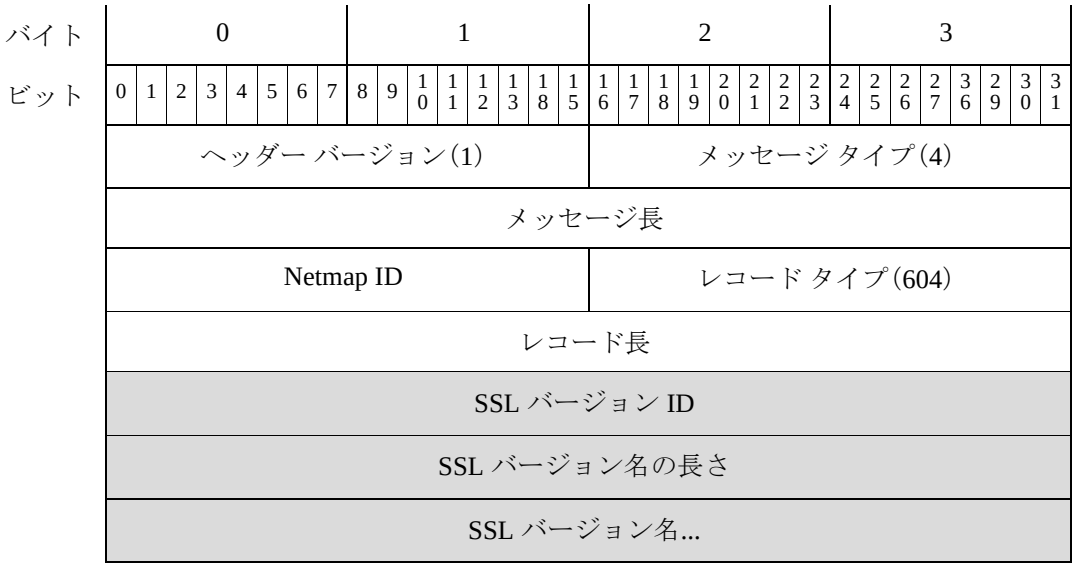
次の表は、SSL 暗号スイート レコードのフィールドについての説明です。

表 3-61　SSL 暗号スイート フィールド

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

SSL バージョン

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



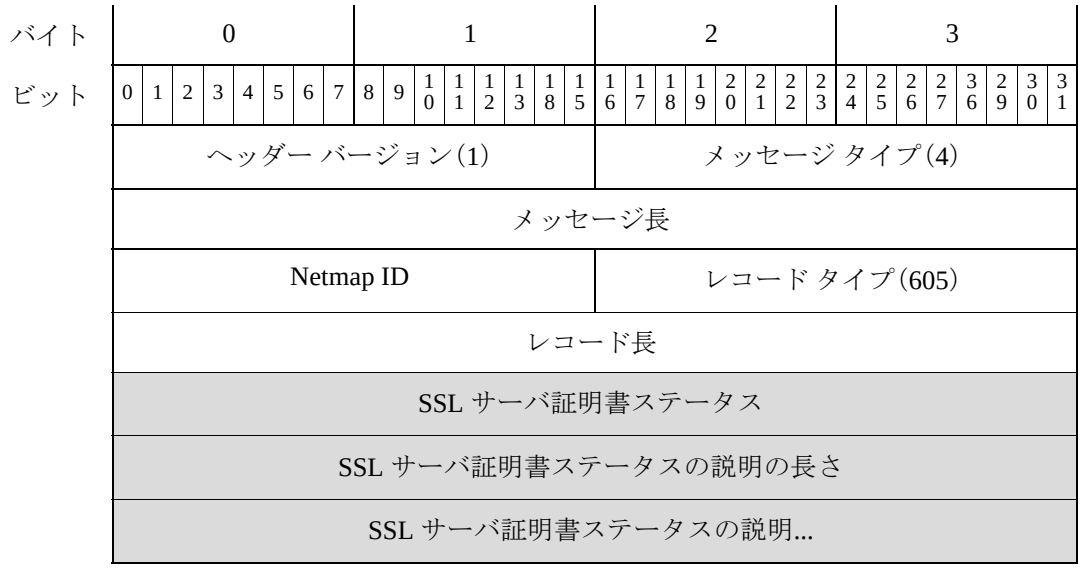
次の表は、SSL バージョン レコードのフィールドについての説明です。

表 3-62　SSL バージョン フィールド

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

SSL サーバ証明書ステータス

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



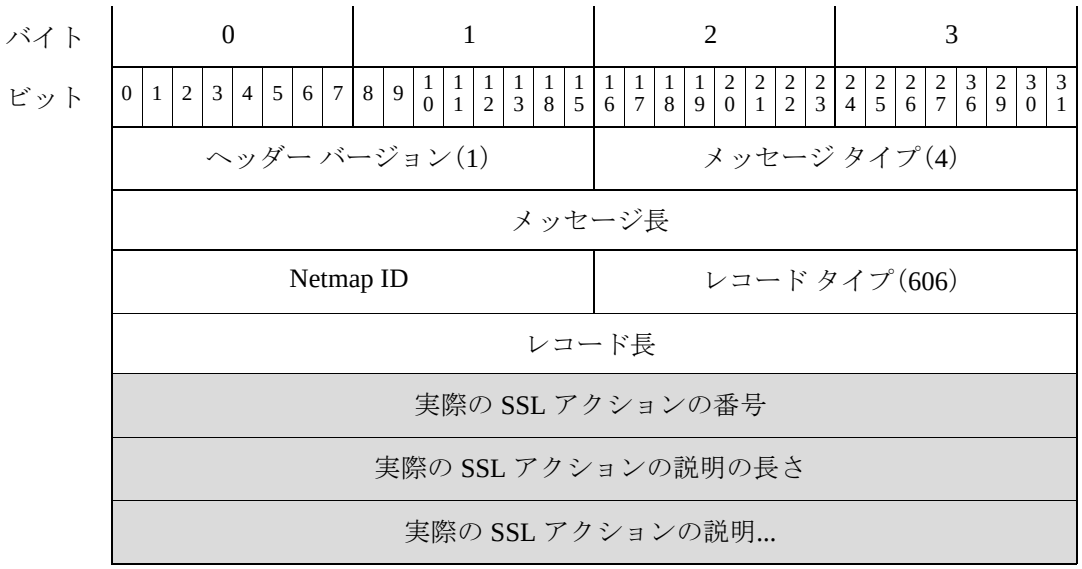
次の表は、SSL サーバ証明書ステータス レコードのフィールドについての説明です。

表 3-63　　SSL サーバ証明書ステータス レコード フィールド

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

実際の SSL アクション

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



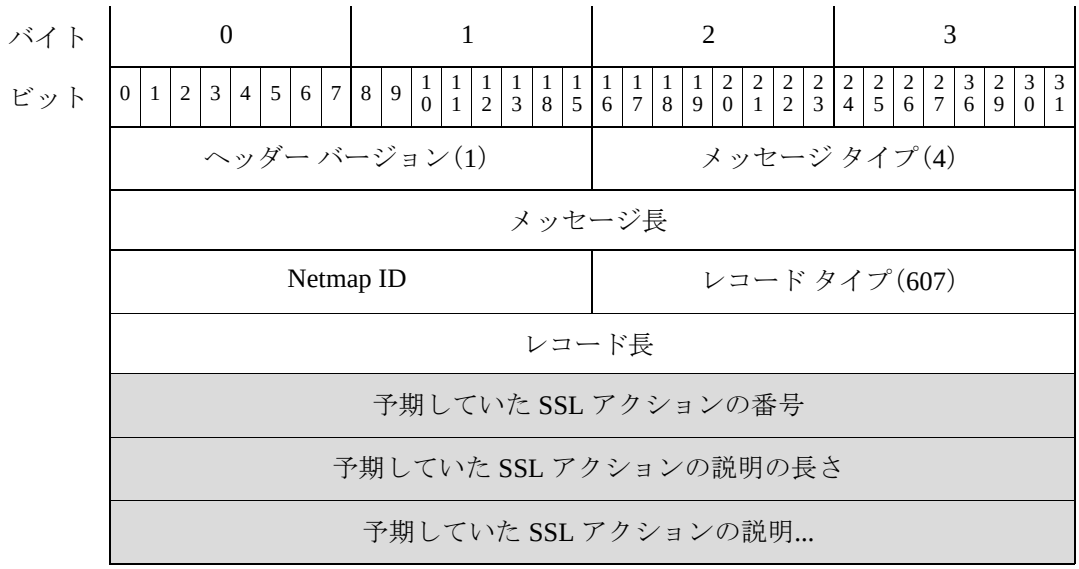
次の表は、実際の SSL アクション レコードのフィールドについての説明です。

表 3-64　　実際の SSL アクション フィールド

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

予期された SSL アクション

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



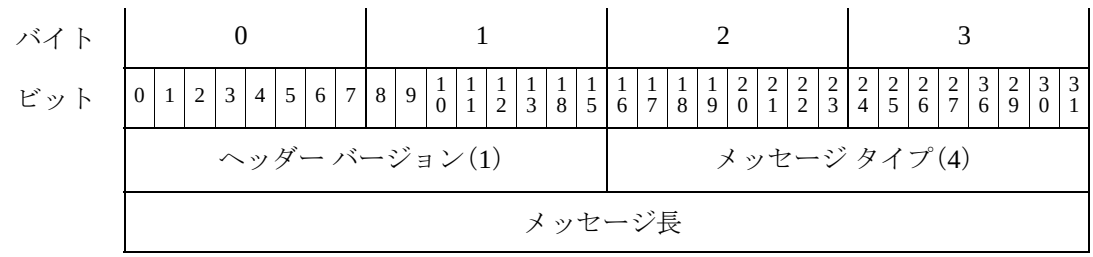
次の表は、予期していた SSL アクション レコードのフィールドについての説明です。

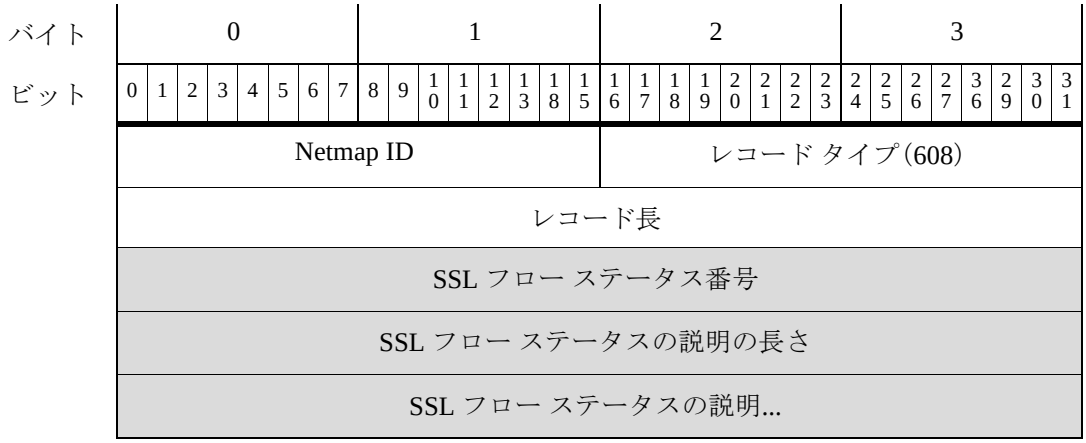
表 3-65　実際の SSL アクション フィールド

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

SSL フロー ステータス

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





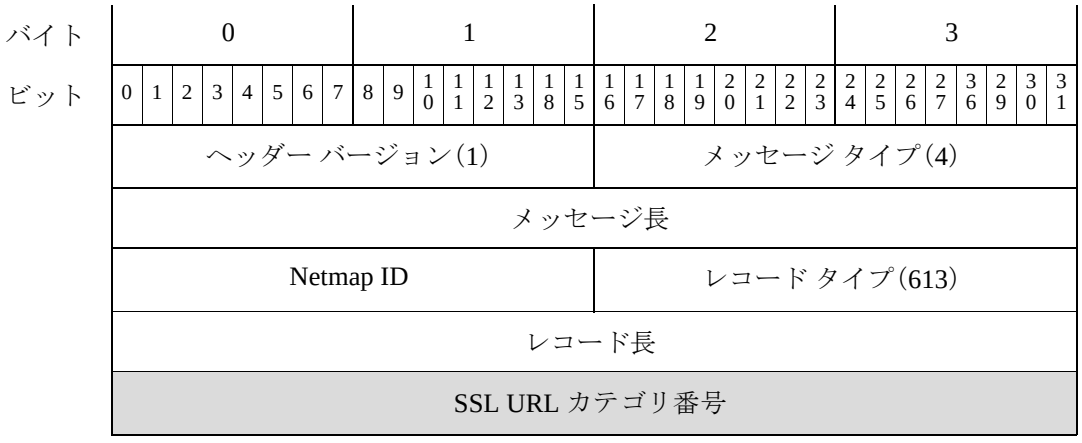
次の表は、SSL フロー ステータス レコードのフィールドについての説明です。

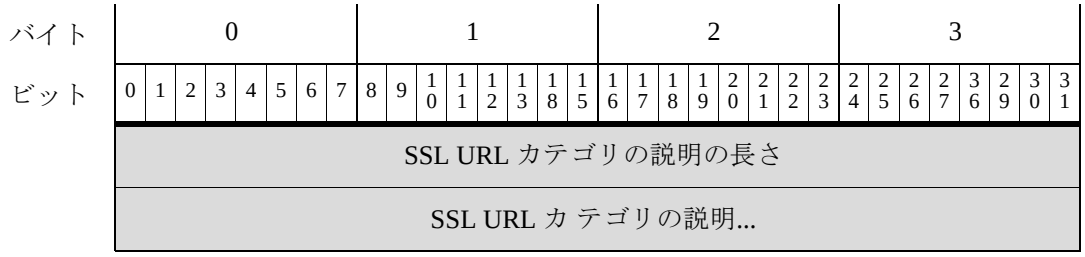
表 3-66　SSL フロー ステータス フィールド

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

SSL URL カテゴリ

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





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

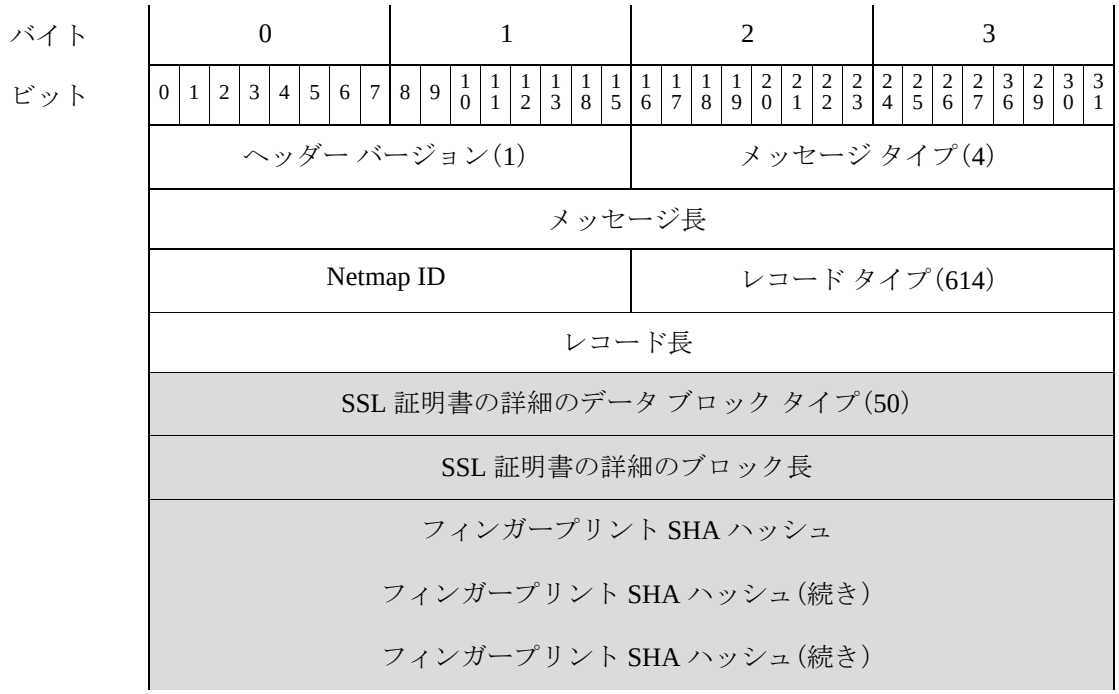
表 3-67　SSL URL カテゴリ フィールド

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

5.4 以上の SSL 証明書の詳細のデータ ブロック

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

次の図に、SSL 証明書の詳細のデータ ブロックの構造を示します。



	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
		フィンガープリント SHA ハッシュ（続き）																															
		フィンガープリント SHA ハッシュ（続き）																															
		公開キーの SHA ハッシュ																															
		公開キーの SHA ハッシュ（続き）																															
		公開キーの SHA ハッシュ（続き）																															
		公開キーの SHA ハッシュ（続き）																															
		公開キーの SHA ハッシュ（続き）																															
		シリアル番号（Serial Number）																															
		シリアル番号（続き）																															
		シリアル番号（続き）																															
		シリアル番号（続き）																															
		シリアル番号（続き）																															
		シリアル番号の長さ																															
	サブジェクトの共通名	文字列ブロック タイプ（0）																															
		文字列ブロック長																															
		サブジェクトの共通名...																															
	サブジェクト組織	文字列ブロック タイプ（0）																															
		文字列ブロック長																															
		サブジェクト組織...																															
	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...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
発行元の共通名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	発行元の共通名...																															
発行者組織	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	発行者組織...																															
発行者の組織単位	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	発行者の組織単位...																															
発行者の国	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	発行者の国...																															
	有効な開始日																															
	有効な終了日																															

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

表 3-68　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。

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)

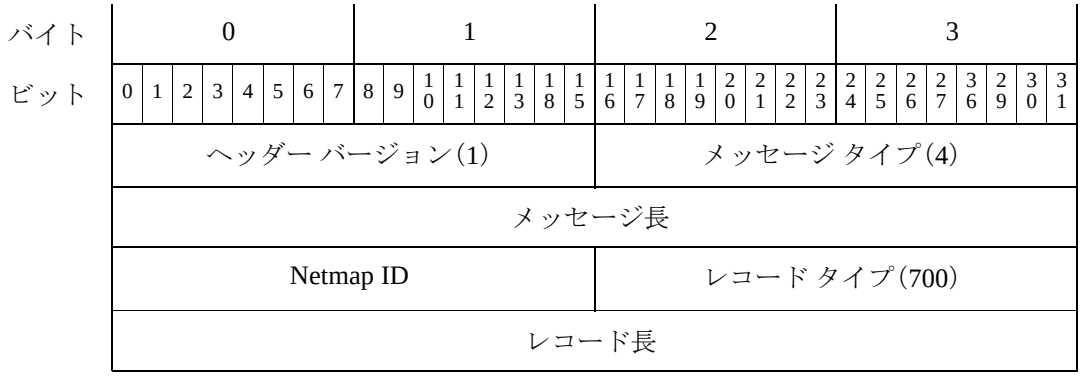
フィールド	データ タイプ	説明
シリアル番号（Serial Number）	uint8[20]	発行元 CA によって割り当てられたシリアル番号。この番号は 20 バイトを超えない長さにする必要があります。シリアル番号の長さフィールドの指定どおりに 20 バイト未満にすることができます。
シリアル番号の長さ	uint32	シリアル番号の長さ(バイト単位)。
文字列ブロック タイプ	uint32	侵害に関連付けられたカテゴリを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとカテゴリ フィールドのバイト数が含まれます。
サブジェクトの共通名	string	SSL 証明書のサブジェクトの共通名。これは通常、証明書のサブジェクトのホストとドメイン名ですが、他の情報が含まれていることもあります。
文字列ブロック タイプ	uint32	侵害に関連付けられたイベント タイプを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとイベント タイプ フィールドのバイト数が含まれます。
サブジェクト組織	string	証明書のサブジェクトの組織。
文字列ブロック タイプ	uint32	侵害に関連付けられたイベント タイプを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとイベント タイプ フィールドのバイト数が含まれます。
サブジェクトの組織単位	string	証明書のサブジェクトの組織単位。
文字列ブロック タイプ	uint32	侵害に関連付けられたイベント タイプを含む文字列データ ブロックを開始します。この値は常に 0 です。
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。

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。
発行者組織	string	証明書の発行者の組織。
文字列ブロック タイプ	uint32	侵害に関連付けられたイベント タイプを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとイベント タイプ フィールドのバイト数が含まれます。
発行者の組織単位	string	証明書の発行者の組織単位。
文字列ブロック タイプ	uint32	侵害に関連付けられたイベント タイプを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとイベント タイプ フィールドのバイト数が含まれます。
発行者の国	string	証明書の発行者の国。
有効な開始日	uint32	証明書が発行された時刻の Unix タイムスタンプ。
有効な終了日	uint32	証明書が有効でなくなる時刻の Unix タイムスタンプ。

ネットワーク分析ポリシー レコード

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



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