



侵入および相関データ構造の概要

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

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

この章の次の項では、イベント メッセージの構造を定義しています。

- [侵入イベントとメタデータのレコードタイプ\(3-1 ページ\)](#)。

データ レコードを送信する eStreamer のメッセージ形式の概要の詳細については、[イベント データ メッセージの形式\(2-21 ページ\)](#)を参照してください。

侵入イベントとメタデータのレコードタイプ

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

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

表 3-1 侵入イベントと一般的なメタデータのレコードタイプ

レコードタイプ	ブロックタイプ	シリーズ	説明	レコードステータス	データ形式の参照先...
2	該当なし	該当なし	パケット データ(バージョン 4.8.0.2 以上)	現在 (Current)	パケット レコード 4.8.0.2 以上(3-6 ページ)
4	該当なし	該当なし	プライオリティのメタデータ	現在 (Current)	プライオリティ レコード(3-8 ページ)
9	20	1	侵入の影響アラート	レガシー (Legacy)	侵入影響アラート データ(B-66 ページ)

表 3-1 侵入イベントと一般的なメタデータのレコードタイプ (続き)

レコードタイプ	ブロックタイプ	シリーズ	説明	レコードステータス	データ形式の参照先...
9	153	1	侵入の影響アラート	現在 (Current)	侵入の影響アラート データ 5.3 以上 (3-22 ページ)
62	該当なし	2	ユーザ メタデータ	現在 (Current)	ユーザー レコード (3-26 ページ)
66	該当なし	該当なし	ルール メッセージのメタデータ (バージョン 4.6.1 以上)	現在 (Current)	4.6.1 以上のルール メッセージのレコード (3-27 ページ)
67	該当なし	該当なし	分類のメタデータ (バージョン 4.6.1 以上)	現在 (Current)	4.6.1 以上の分類レコード (3-28 ページ)
69	該当なし	該当なし	関連ポリシーのメタデータ (バージョン 4.6.1 以上)	現在 (Current)	関連ポリシー レコード (3-30 ページ)
70	該当なし	該当なし	関連ルールのメタデータ (バージョン 4.6.1 以上)	現在 (Current)	関連ルール レコード (3-31 ページ)
104	該当なし	該当なし	侵入イベント (IPv4) レコード 4.9 ~ 4.10.x	レガシー (Legacy)	製品の旧バージョン
105	該当なし	該当なし	侵入イベント (IPv6) レコード 4.9 ~ 4.10.x	レガシー (Legacy)	製品の旧バージョン
110	4	2	侵入イベント追加データ (バージョン 4.10.0 以上)	レガシー (Legacy)	侵入イベント追加データレコード (B-69 ページ)
111	5	2	侵入イベント追加データのメタデータ (バージョン 4.10.0 以上)	レガシー (Legacy)	侵入イベント追加データのメタデータ (B-71 ページ)
112	128	1	5.1 ~ 5.3.x の関連イベント	レガシー (Legacy)	関連イベント 5.1 ~ 5.3.x (B-366 ページ)
112	156	1	5.4 以上の関連イベント	現在 (Current)	5.4 以上の関連イベント (3-46 ページ)
115	14	2	セキュリティ ゾーン名のメタデータ	現在 (Current)	セキュリティ ゾーン名レコード (3-33 ページ)
116	14	2	インターフェイス名のメタデータ	現在 (Current)	インターフェイス名レコード (3-34 ページ)
117	14	2	アクセス コントロール ポリシー名メタデータ	現在 (Current)	アクセス コントロール ポリシー名のレコード (3-35 ページ)
118	15	2	侵入ポリシー名のメタデータ	現在 (Current)	侵入ポリシー名レコード (4-23 ページ)
119	15	2	アクセス コントロール ルール ID のメタデータ	現在 (Current)	アクセス コントロール ルール ID レコードのメタデータ (3-37 ページ)
120	該当なし	該当なし	アクセス コントロール ルール アクションのメタデータ	現在 (Current)	アクセス コントロール ルール アクション レコード メタデータ (4-25 ページ)
121	該当なし	該当なし	URL カテゴリのメタデータ	現在 (Current)	URL カテゴリ レコード メタデータ (4-26 ページ)

表 3-1 侵入イベントと一般的なメタデータのレコードタイプ (続き)

レコードタイプ	ブロックタイプ	シリーズ	説明	レコードステータス	データ形式の参照先...
122	該当なし	該当なし	URL レピュテーション メタデータ	現在 (Current)	URL レピュテーション レコード メタデータ (4-27 ページ)
123	該当なし	該当なし	管理対象Deviceのメタデータ	現在 (Current)	管理対象Device レコードのメタデータ (3-38 ページ)
該当なし	64	2	アクセス コントロール ポリシー名のデータブロック	現在 (Current)	アクセス コントロール ポリシー名のデータ ブロック (3-87 ページ)
124	59	2	アクセス コントロール ポリシー ルール理由データ ブロック	現在 (Current)	6.0 以上のアクセス コントロール ポリシー ルール理由データ ブロック (3-85 ページ)
125	該当なし	2	マルウェア イベント レコード(バージョン 5.1.1 以上)	現在 (Current)	マルウェア イベント レコード 5.1.1 以上 (3-39 ページ)
125	24	2	マルウェア イベント(バージョン 5.1.1 以上)	レガシー (Legacy)	マルウェア イベント データ ブロック 5.1.1.x (B-77 ページ)
125	33	2	マルウェア イベント(バージョン 5.2.x)	レガシー (Legacy)	マルウェア イベント データ ブロック 5.2.x (B-83 ページ)
125	35	2	マルウェア イベント(バージョン 5.3)	レガシー (Legacy)	マルウェア イベントのデータ ブロック 5.3 (B-90 ページ)
125	44	2	マルウェア イベント(バージョン 5.3.1)	レガシー (Legacy)	マルウェア イベント データ ブロック 5.3.1 (B-97 ページ)
125	47	2	マルウェア イベント(バージョン 5.4.x)	レガシー (Legacy)	マルウェア イベント データ ブロック 5.4.x (B-105 ページ)
125	62	2	マルウェア イベント(バージョン 6.x)	レガシー (Legacy)	マルウェア イベント データ ブロック 6.x (B-116 ページ)
125	80	2	マルウェア イベント(バージョン 7.0 以上)	現在 (Current)	マルウェア イベントのデータ ブロック 7.0 以上 (3-100 ページ)
127	14	2	Cisco Advanced Malware Protection クラウドのメタデータ(バージョン 5.1 以上)	現在 (Current)	Cisco Advanced Malware Protection クラウド名のメタデータ (3-40 ページ)
128	該当なし	該当なし	マルウェア イベント タイプのメタデータ(バージョン 5.1 以上)	現在 (Current)	マルウェア イベント タイプのメタデータ (3-42 ページ)
129	該当なし	該当なし	マルウェア イベント サブタイプ のメタデータ(バージョン 5.1 以上)	現在 (Current)	マルウェア イベント サブタイプ のメタデータ (3-42 ページ)
130	該当なし	該当なし	エンドポイント向け AMP ディテクタ タイプのメタデータ(バージョン 5.1 以上)	現在 (Current)	エンドポイント向け AMP ディテクタ タイプのメタデータ (3-43 ページ)

表 3-1 侵入イベントと一般的なメタデータのレコードタイプ (続き)

レコードタイプ	ブロックタイプ	シリーズ	説明	レコードステータス	データ形式の参照先...
131	該当なし	該当なし	エンドポイント向け AMP ファイルタイプのメタデータ (バージョン 5.1 以上)	現在 (Current)	エンドポイント向け AMP ファイルタイプのメタデータ (3-44 ページ)
132	該当なし	該当なし	セキュリティ コンテキスト名	現在 (Current)	セキュリティ コンテキスト名 (3-45 ページ)
140	27	2	5.2 以上のルール ドキュメントのデータ ブロック	現在 (Current)	5.2 以上のルール ドキュメントのデータ ブロック (3-114 ページ)
207	該当なし	該当なし	侵入イベント (IPv4) レコード 5.0.x ~ 5.1	レガシー (Legacy)	侵入イベント (IPv4) レコード 5.0.x ~ 5.1 (B-2 ページ)
208	該当なし	該当なし	侵入イベント (IPv6) レコード 5.0.x ~ 5.1	レガシー (Legacy)	侵入イベント (IPv6) レコード 5.0.x ~ 5.1 (B-8 ページ)
260	19	2	ICMP タイプ データのデータ ブロック	現在 (Current)	ICMP タイプのデータ ブロック (3-73 ページ)
270	20	2	ICMP コードのデータ ブロック	現在 (Current)	ICMP コードのデータ ブロック (3-74 ページ)
282	該当なし	2	5.4.1 以上のセキュリティ インテリジェンス カテゴリのメタデータ	現在 (Current)	5.4.1 以上のセキュリティ インテリジェンス カテゴリのメタデータ (3-76 ページ)
300	該当なし	該当なし	6.0 以上のレルムのメタデータ	現在 (Current)	6.0 以上のレルムのメタデータ (3-77 ページ)
301	58	2	6.0 以上のエンドポイント プロファイル	現在 (Current)	6.0 以上のエンドポイント プロファイルのデータ ブロック (3-78 ページ)
302	該当なし	該当なし	6.0 以上のセキュリティ グループのメタデータ	現在 (Current)	6.0 以上のセキュリティ グループのメタデータ (3-79 ページ)
320	該当なし	該当なし	6.0 以上の DNS レコード タイプのメタデータ	現在 (Current)	6.0 以上の DNS レコード タイプのメタデータ (3-80 ページ)
321	該当なし	該当なし	6.0 以上の DNS レスポンス タイプのメタデータ	現在 (Current)	6.0 以上の DNS レスポンス タイプのメタデータ (3-81 ページ)
322	該当なし	該当なし	6.0 以上のシンクホールのメタデータ	現在 (Current)	6.0 以上のシンクホールのメタデータ (3-83 ページ)
350	該当なし	該当なし	6.0 以上の Netmap ドメインのメタデータ	現在 (Current)	6.0 以上の Netmap ドメインのメタデータ (3-84 ページ)
400	34	2	侵入イベント レコード 5.2.x	レガシー (Legacy)	侵入イベント レコード 5.2.x (B-14 ページ)
400	41	2	侵入イベント レコード 5.3	レガシー (Legacy)	侵入イベント レコード 5.3 (B-20 ページ)
400	54	2	侵入イベント レコード 5.3.1	レガシー (Legacy)	侵入イベント レコード 5.3.1 (B-32 ページ)
400	45	2	侵入イベント レコード 5.4.x	レガシー (Legacy)	侵入イベント レコード 5.4.x (B-38 ページ)

表 3-1 侵入イベントと一般的なメタデータのレコードタイプ (続き)

レコードタイプ	ブロックタイプ	シリーズ	説明	レコードステータス	データ形式の参照先...
400	60	2	侵入イベント レコード 6.x	レガシー (Legacy)	侵入イベント レコード 6.x (B-47 ページ)
400	81	2	侵入イベント レコード 7.0	レガシー (Legacy)	侵入イベント レコード 7.0 (B-56 ページ)
400	85	2	侵入イベント レコード 7.1 以上	現在 (Current)	侵入イベント レコード 7.1 以上 (3-9 ページ)
500	32	2	ファイル イベント (バージョン 5.2.x)	レガシー (Legacy)	ファイル イベント 5.2.x (B-317 ページ)
500	38	2	ファイル イベント (バージョン 5.3)	レガシー (Legacy)	ファイル イベント 5.3 (B-321 ページ)
500	43	2	ファイル イベント (バージョン 5.3.1)	レガシー (Legacy)	ファイル イベント 5.3.1 (B-328 ページ)
500	46	2	ファイル イベント (バージョン 5.4.x)	現在 (Current)	7.0 以降のファイル イベント (3-89 ページ)
502	32	2	ファイル イベント (バージョン 5.2.x)	レガシー (Legacy)	ファイル イベント 5.2.x (B-317 ページ)
502	38	2	ファイル イベント (バージョン 5.3)	レガシー (Legacy)	ファイル イベント 5.3 (B-321 ページ)
502	43	2	ファイル イベント (バージョン 5.3.1)	レガシー (Legacy)	ファイル イベント 5.3.1 (B-328 ページ)
502	46	2	ファイル イベント (バージョン 5.4.x)	レガシー (Legacy)	ファイル イベント 5.4.x (B-334 ページ)
502	72	2	ファイル イベント (バージョン 6.x)	レガシー (Legacy)	6.x のファイル イベント (B-345 ページ)
502	79	2	ファイル イベント (バージョン 7.0 以上)	現在 (Current)	7.0 以降のファイル イベント (3-89 ページ)
510	該当なし	該当なし	5.3 以上のファイルタイプ ID のメタデータ	現在 (Current)	5.3 以上のファイルタイプ ID のメタデータ (3-113 ページ)
511	26	2	5.11 ~ 5.2.x のファイル イベント SHA ハッシュ	レガシー (Legacy)	ファイル イベント SHA ハッシュ 5.1.1 ~ 5.2.x (B-356 ページ)
511	40	2	5.3 以上のファイル イベント SHA ハッシュ	現在 (Current)	5.3 以上のファイル イベント SHA ハッシュ (3-111 ページ)
515	該当なし	該当なし	6.0 以上の Filelog ストレージのメタデータ	現在 (Current)	6.0 以上の Filelog ストレージのメタデータ (3-118 ページ)
516	該当なし	該当なし	6.0 以上の Filelog サンドボックスのメタデータ	現在 (Current)	6.0 以上の Filelog サンドボックスのメタデータ (3-119 ページ)
517	該当なし	該当なし	6.0 以上の Filelog Spero のメタデータ	現在 (Current)	6.0 以上の Filelog Spero のメタデータ (3-120 ページ)
518	該当なし	該当なし	6.0 以上の Filelog アーカイブのメタデータ	現在 (Current)	6.0 以上の Filelog アーカイブのメタデータ (3-120 ページ)

表 3-1 侵入イベントと一般的なメタデータのレコードタイプ (続き)

レコードタイプ	ブロックタイプ	シリーズ	説明	レコードステータス	データ形式の参照先...
519	該当なし	該当なし	6.0以上のFilelogスタティック分析のメタデータ	現在 (Current)	6.0以上のFilelogスタティック分析のメタデータ(3-121ページ)
520	28	2	5.2以上の位置情報のデータブロック	現在 (Current)	5.2以上の位置情報のデータブロック(3-122ページ)
530	該当なし	該当なし	6.0以上のファイルポリシー名	現在 (Current)	6.0以上のファイルポリシー名(3-123ページ)
600	該当なし	該当なし	SSLポリシー名	現在 (Current)	SSLポリシー名(3-125ページ)
601	51	2	SSLルールID	現在 (Current)	SSLルールID(3-126ページ)
602	該当なし	該当なし	SSL暗号スイート	現在 (Current)	5.4以上のSSL証明書の詳細のデータブロック(3-133ページ)
604	該当なし	該当なし	SSLバージョン	現在 (Current)	SSLバージョン(3-128ページ)
605	該当なし	該当なし	SSLサーバ証明書ステータス	現在 (Current)	SSLサーバ証明書ステータス(3-129ページ)
606	該当なし	該当なし	実際のSSLアクション	現在 (Current)	実際のSSLアクション(3-130ページ)
607	該当なし	該当なし	予期されたSSLアクション	現在 (Current)	予期されたSSLアクション(3-131ページ)
608	該当なし	該当なし	SSLフローステータス	現在 (Current)	SSLフローステータス(3-132ページ)
613	該当なし	該当なし	SSLURLカテゴリ	現在 (Current)	SSLURLカテゴリ(3-132ページ)
614	50	2	5.4以上のSSL証明書の詳細のデータブロック	現在 (Current)	5.4以上のSSL証明書の詳細のデータブロック(3-133ページ)
700	該当なし	該当なし	ネットワーク分析ポリシーレコード	現在 (Current)	ネットワーク分析ポリシーレコード(3-137ページ)

パケットレコード 4.8.0.2 以上

eStreamer サービスは、パケットレコードのイベントに関連付けられたパケットデータを送信します。形式は次のとおりです。パケットフラグ(要求メッセージの[要求フラグ(Request Flags)]フィールドのビット0)が設定されていると、パケットデータが送信されます。[要求フラグ\(2-15ページ\)](#)を参照してください。ビット23を有効にすると、拡張イベントヘッダーがレコードに含まれます。メッセージ長フィールドの後に表示されるレコードタイプフィールドにパケットレコードを示す値2があることに注意してください。

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

次の表は、パケット レコードのフィールドについての説明です。

表 3-2 パケット レコード フィールド

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

表 3-2 パケットレコードフィールド (続き)

フィールド	データタイプ	説明
リンクタイプ	uint32	リンク層のタイプ。現在、値は常に 1 になります(イーサネット層を示します)。
パケット長	uint32	パケットデータに含まれるバイト数。
パケットデータ	変数 (variable)	キャプチャされた実際のパケットデータ(ヘッダーとペイロード)。

プライオリティレコード

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

バイト	0								1								2								3																		
ビット	0	1	2	3	4	5	6	7	8	9	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	2	2	2	2	2	2	2	2	3	2	3	3
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 (4)																											
レコード長																																											
プライオリティ ID																																											
名前の長さ																プライオリティ名...																											

次の表は、各プライオリティ固有のフィールドについての説明です。

表 3-3 プライオリティレコードフィールド

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

侵入イベント レコード7.1 以上

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

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

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ヘッダーバージョン(1)																メッセージタイプ(4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ(400)																							
	レコード長																																							
	eStreamer サーバー タイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																																							
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																																							
	ブロックタイプ(85)																																							
	ブロック長																																							
	デバイスID (Device ID)																																							
	イベント ID (Event ID)																																							
	イベント秒																																							
	イベントマイクロ秒																																							
	ルール ID (シグネチャ ID)																																							
	ジェネレータ ID																																							
	ルール リビジョン																																							
	分類 ID																																							
	プライオリティ ID																																							

■ 侵入イベントとメタデータのレコードタイプ

バイト	0								1								2								3										
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
送信元 IP アドレス																																			
送信元 IP アドレス(続き)																																			
送信元 IP アドレス(続き)																																			
送信元 IP アドレス(続き)																																			
宛先IPアドレス																																			
宛先 IP アドレス(続き)																																			
宛先 IP アドレス(続き)																																			
宛先 IP アドレス(続き)																																			
送信元ポートまたは ICMP タイプ																		送信先ポートまたは ICMP コード																	
IP プロトコル ID									影響フラグ									影響									[インライン結果 (Inline Result)]								
インライン結果理由									MPLSラベル(MPLS Label)																										
MPLS ラベル(続き)									VLAN ID (Admin. VLAN ID)																		パッド								
パッド(続き)									ポリシー UUID																										
ポリシー UUID(続き)																																			
ポリシー UUID(続き)																																			
ポリシー UUID(続き)																																			
ポリシー UUID(続き)																											ユーザー ID (User ID)								
ユーザー ID(続き)																											Web アプリケーション ID								
Web アプリケーション ID(続き)																											クライアントアプリケーション ID								
クライアントアプリケーション ID																											アプリケーションプロトコルID								
アプリケーションプロトコル ID(続き)																											アクセスコントロールルール ID								

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
アクセスコントロールルール ID (続き)																アクセス コントロール ポリシー UUID																
アクセス コントロール ポリシー UUID (続き)																																
アクセス コントロール ポリシー UUID (続き)																																
アクセス コントロール ポリシー UUID (続き)																																
アクセス コントロール ポリシー UUID (続き)																								インターフェイス入力 UUID								
インターフェイス入力 UUID (続き)																																
インターフェイス入力 UUID (続き)																																
インターフェイス入力 UUID (続き)																																
インターフェイス入力 UUID (続き)																								インターフェイス出力 UUID								
インターフェイス出力 UUID (続き)																																
インターフェイス出力 UUID (続き)																																
インターフェイス出力 UUID (続き)																																
インターフェイス出力 UUID (続き)																								秒ゾーン入力 UUID								
セキュリティ ゾーン入力 UUID (続き)																																
セキュリティ ゾーン入力 UUID (続き)																																
セキュリティ ゾーン入力 UUID (続き)																																
セキュリティ ゾーン入力 UUID (続き)																								秒ゾーン出力 UUID								
セキュリティ ゾーン出力 UUID (続き)																																
セキュリティ ゾーン出力 UUID (続き)																																
セキュリティ ゾーン出力 UUID (続き)																																
セキュリティ ゾーン出力 UUID (続き)																								接続タイムスタンプ								

■ 侵入イベントとメタデータのレコードタイプ

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	接続タイムスタンプ(続き)																								接続インスタンスID							
	接続インスタンスID								接続数カウンタ																送信元の国							
	送信元の国								宛先の国																IOC 番号							
	IOC 番号								セキュリティ コンテキスト																							
	秒コンテキスト(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(続き)								SSL 証明書フィンガープリント																							
									SSL 証明書フィンガープリント(続き)																							
									SSL 証明書フィンガープリント(続き)																							
									SSL 証明書フィンガープリント(続き)																							
	SSL 証明書フィンガープリント(続き)								実際の SSL アクション																SSL フローステータス							
									SSL フローステータス(続き)								ネットワーク分析ポリシー UUID															
	ネットワーク分析ポリシー UUID(続き)																															
	ネットワーク分析ポリシー UUID(続き)																															
	ネットワーク分析ポリシー UUID(続き)								[HTTPレスポンス(HTTP Response)]																							

バイト	0							1							2							3																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						
入力 VRF	HTTP レスポンス (続き)							文字列ブロック タイプ (0)																														
	文字列ブロック タイプ (0)							文字列ブロック長																														
	文字列ブロック長							入力 VRF 名																														
出力 VRF	文字列ブロック タイプ (0)																																					
	文字列ブロック長																																					
	出力 VRF 名																																					
ホストネーム HTTP (Hostname)	Snort バージョン							クライアントのオリジナル IP (Original Client IP)														文字列ブロック タイプ (0)																
	文字列ブロックタイプ(続き)														文字列ブロック長																							
	文字列ブロック長(続き)														HTTP ホスト名																							
HTTP URI	文字列ブロック タイプ (0)																																					
	文字列ブロック長																																					
	HTTP URI																																					
添付ファイル SMTP	文字列ブロック タイプ (0)																																					
	文字列ブロック長																																					
	SMTP 添付ファイル																																					
SMTP 送信元	文字列ブロック タイプ (0)																																					
	文字列ブロック長																																					
	SMTP 送信元																																					
SMTP ヘッダー	文字列ブロック タイプ (0)																																					
	文字列ブロック長																																					
	SMTP ヘッダー																																					

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

次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 3-4 侵入イベント レコード 7.1 以上のフィールド

フィールド	データタイプ	説明
ブロック タイプ	uint32	侵入イベント データ ブロックを開始します。この値は常に 85 です。
ブロック長	uint32	侵入イベント データ ブロックのバイトの合計数(侵入イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID (Device ID)	uint32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 管理対象 Device レコードのメタデータ (3-38 ページ) を参照してください。
イベント ID (Event ID)	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
イベント マイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒(100 万分の 1 秒)単位の増分。
ルール ID (シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Cisco Secure Firewall システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポートまたは ICMP タイプ	uint16	イベント プロトコル タイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。

表 3-4 侵入イベントレコード7.1以上のフィールド (続き)

フィールド	データタイプ	説明
送信先ポートまたはICMPコード	uint16	イベントプロトコルタイプがTCPまたはUDPの場合は宛先ポート番号、またはイベントがICMPトラフィックによって引き起こされた場合はICMPのコード。
IPプロトコルID	uint8	IANA指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none">• 0:IP• 1:ICMP• 6:TCP• 17:UDP

表 3-4 侵入イベント レコード 7.1 以上のフィールド (続き)

フィールド	データタイプ	説明
影響フラグ	bits[8]	<p>イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。</p> <ul style="list-style-type: none"> • 0x01 (ビット 0): 送信元または宛先ホストはシステムによってモニターされるネットワーク内にあります。 • 0x02 (ビット 1): 送信元または宛先ホストはネットワークマップ内に存在します。 • 0x04 (ビット 2): 送信元または宛先ホストはイベントのポート上のサーバーを実行しているか (TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08 (ビット 3): イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 • 0x10 (ビット 4): イベントで検出されたサーバーにマップされた脆弱性があります。 • 0x20 (ビット 5): イベントが原因で、管理対象デバイスがセッションをドロップしました (デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Cisco Secure Firewall システム Web インターフェイスのブロックされた状態に対応します。 • 0x40 (ビット 6): このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80 (ビット 7): イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) <p>次の影響レベル値は、Management Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。</p> <ul style="list-style-type: none"> • グレー (0、不明): 00x00000 • 赤 (1、脆弱): xxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx (バージョン 5.0+ のみ) • オレンジ (2、潜在的に脆弱): 00x0011x • 黄 (3、現在は脆弱でない): 00x0001x • 青 (4、不明なターゲット): 00x00001
影響	uint8	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> • 1: レッド (脆弱) • 2: オレンジ (脆弱の可能性あり) • 3: イエロー (現在は脆弱でない) • 4: ブルー (不明なターゲット) • 5: グレー (不明なインパクト)

表 3-4 侵入イベント レコード7.1 以上のフィールド (続き)

フィールド	データタイプ	説明
[インライン結果 (Inline Result)]	uint8	インライン結果を示す値。 <ul style="list-style-type: none"> • 0:合格 • 1:ドロップ • 2:ドロップされる可能性あり(設定では許可されていない) • 3:部分的にドロップ • 4:ブロック • 5:ブロック対象 • 6:部分的にブロック • 7:ドロップ • 8:ドロップ対象 • 9:拒否 • 10:拒否対象 • 11:応答 • 12:応答対象 • 13:書き換え • 14:書き換え対象
インライン結果理由	uint8	インライン結果の理由を示す値。 <ul style="list-style-type: none"> • 1:パッシブモードまたはタップモードのインターフェイス • 2:「検出」検査モードの侵入ポリシー • 3:「検出」検査モードのネットワーク分析ポリシー • 4:接続タイムアウト • 5:接続クローズ(内部使用) • 6:接続クローズ(内部使用) • 7:接続クローズ(内部使用)
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザー ID (User ID)	uint32	ユーザーの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。

表 3-4 侵入イベント レコード 7.1 以上のフィールド (続き)

フィールド	データタイプ	説明
アクセス コントロール ルール ID	uint32	アクセス コントロール ルールの固有識別子として機能するルール ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの固有識別子として機能するポリシー ID 番号。
インターフェイス入力 UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
インターフェイス出力 UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
セキュリティゾーン入力 UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
セキュリティゾーン出力 UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970年1月1日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数值 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティ コンテキスト	uint8[16]	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバー証明書の SHA1 ハッシュ。

表 3-4 侵入イベント レコード 7.1 以上のフィールド (続き)

フィールド	データタイプ	説明
実際の SSL アクション	uint16	<p>SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。</p> <ul style="list-style-type: none">• 0:「不明」• 1:「復号しない」• 2:「ブロックする」• 3:「リセットでブロック」• 4:「復号(既知のキー)」• 5:「復号(置換キー)」• 6:「復号(Resign)」

表 3-4 侵入イベント レコード 7.1 以上のフィールド (続き)

フィールド	データタイプ	説明
SSL フロー ステータス	uint16	<p>SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバー名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバーの証明書の処理」 • 16:「サーバー証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバー証明書の検証が使用できません」 • 27:「サーバー証明書の検証エラー」 • 28:「無効な操作」
ネットワーク分析ポリシー UUID	uint8[16]	侵入イベントを作成したネットワーク分析ポリシーの UUID。
HTTP レスポンス	uint32	HTTP 要求の応答コード。

表 3-4 侵入イベント レコード 7.1 以上のフィールド (続き)

フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	入力 VRF の名前を含む文字列データブロックを開始します。 この値は常に 0 です。
文字列ブロッ ク長	uint32	名前の文字列データブロックのバイト数。ブロックタイプと ヘッダーフィールドの 8 バイト、および入力 VRF 名フィール ドのバイト数が含まれています。
入力 VRF 名	string	トラフィックがネットワークに入るときに通過する仮想 ルータ。
文字列ブロック タイプ	uint32	出力 VRF の名前を含む文字列データブロックを開始します。 この値は常に 0 です。
文字列ブロッ ク長	uint32	名前の文字列データブロックのバイト数。ブロックタイプと ヘッダーフィールドの 8 バイト、および出力 VRF 名フィール ドのバイト数が含まれています。
出力 VRF 名	string	トラフィックがネットワークから出るときに通過する仮想 ルータの名前。
Snort バー ジョン	uint8	Snort のバージョン番号。
元のイニシエー タ IP	uint16	接続の元のイニシエータ IP アドレスが含まれています。
文字列ブロック タイプ	uint32	HTTP ホスト名の名前を含む文字列データブロックを開始し ます。この値は常に 0 です。
文字列ブロッ ク長	uint32	名前の文字列データブロックのバイト数。ブロックタイプと ヘッダーフィールドの 8 バイト、および HTTP ホスト名 フィールドのバイト数が含まれています。
HTTP ホスト名 (HTTP Hostname)	string	HTTP 接続で見つかったホスト名が含まれています。
文字列ブロック タイプ	uint32	HTTP URI を含む文字列データブロックを開始します。この 値は常に 0 です。
文字列ブロッ ク長	uint32	名前の文字列データブロックのバイト数。ブロックタイプと ヘッダーフィールドの 8 バイト、および HTTP URI フィール ドのバイト数が含まれています。
HTTP URI	string	HTTP 接続で見つかった Universal Resource Indicator が含ま れています。
文字列ブロック タイプ	uint32	SMTP 添付ファイルの名前を含む文字列データブロックを開 始します。この値は常に 0 です。
文字列ブロッ ク長	uint32	名前の文字列データブロックのバイト数。ブロックタイプと ヘッダーフィールドの 8 バイト、および SMTP 添付ファイル フィールドのバイト数が含まれています。

表 3-4 侵入イベント レコード 7.1 以上のフィールド (続き)

フィールド	データタイプ	説明
SMTP 添付ファイル	string	[MIME コンテンツ傾向 (MIME Content-Disposition)] ヘッダーから取得された MIME 添付ファイル名が含まれています。このフィールドに入力するには、SMTP プリプロセッサの [MIME 添付ファイル名のログ (Log MIME Attachment Names)] オプションを有効にする必要があります。複数の添付ファイル名がサポートされます。
文字列ブロックタイプ	uint32	SMTP 送信元アドレス含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの 8 バイト、および SMTP 送信元フィールドのバイト数が含まれています。
SMTP 送信元	string	SMTP MAIL FROM コマンドから取得された電子メール送信者のアドレスが含まれています。このフィールドに入力するには、SMTP プリプロセッサの [送信元アドレスのログ (Log From Address)] オプションを有効にする必要があります。複数の送信者アドレスがサポートされます。
文字列ブロックタイプ	uint32	SMTP ヘッダーを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの 8 バイト、および SMTP ヘッダーフィールドのバイト数が含まれています。
SMTP ヘッダー	string	電子メールのヘッダーから取得したデータが含まれています。電子メールのヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーのログ (Log Headers)] オプションを有効にする必要があります。
文字列ブロックタイプ	uint32	SMTP 宛先アドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの 8 バイト、および SMTP 宛先フィールドのバイト数が含まれています。
SMTP 宛先	string	SMTP RCPT TO コマンドから取得された電子メール受信者のアドレスが含まれています。このフィールドに入力するには、SMTP プリプロセッサの [宛先アドレスのログ (Log To Address)] オプションを有効にする必要があります。複数の受信者アドレスがサポートされます。

侵入の影響アラート データ 5.3 以上

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

要求メッセージのフラグ フィールドにビット 5 を設定することで、eStreamer が侵入の影響イベントを送信するように要求できます。要求メッセージの詳細については、[イベントストリーム要求メッセージの形式\(2-13 ページ\)](#)を参照してください。これらのアラートのバージョン 1 は、IPv4 のみを処理します。5.3 で導入されたバージョン 2 は、IPv4 に加えて IPv6 イベントを処理します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (9)															
	eStreamer サーバー タイムスタンプ (イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み (イベントでビット 23 が設定されている場合のみ)																															
	侵入影響アラートブロックタイプ (153)																															
	侵入影響アラートブロック長																															
	イベント ID (Event ID)																															
	Device ID																															
	イベント秒																															
	影響																															
	送信元 IP アドレス																															
	送信元 IP アドレス (続き)																															
	送信元 IP アドレス (続き)																															
	送信元 IP アドレス (続き)																															
	宛先IPアドレス																															
	宛先 IP アドレス (続き)																															
	宛先 IP アドレス (続き)																															
	宛先 IP アドレス (続き)																															

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

次の表は、影響イベントの各データ フィールドについての説明です。

表 3-5 影響イベント データ フィールド

フィールド	データタイプ	説明
侵入影響アラート ブロック タイプ	uint32	侵入影響アラート データ ブロックが続くことを示します。このフィールドの値は、常に 153 です。 侵入イベントとメタデータのレコードタイプ(3-1 ページ) を参照してください。
侵入影響アラート ブロック長	uint32	侵入の影響アラートのブロック タイプの長さを示します。後続のすべてのデータ、および侵入の影響アラートのブロック タイプと長さの 8 バイトを含みます。
イベント ID (Event ID)	uint32	イベント ID 番号を表示します。
Device ID	uint32	管理対象デバイス ID 番号を表示します。
イベント秒	uint32	イベントが検出された秒(1970年1月1日からの経過秒数)を示します。

表 3-5 影響イベント データ フィールド (続き)

フィールド	データタイプ	説明
影響	bits[8]	<p>イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。</p> <ul style="list-style-type: none"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニターされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワーク マップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバーを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバーにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Cisco Secure Firewall システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) <p>次の影響レベル値は、Management Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。</p> <ul style="list-style-type: none"> グレー(0、不明):00x00000 赤(1、脆弱):xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx (バージョン 5.0+ のみ) オレンジ(2、潜在的に脆弱):00x0011x 黄(3、現在は脆弱でない):00x0001x 青(4、不明なターゲット):00x00001
送信元 IP アドレス	uint8[16]	影響イベントに関連付けられているホストの IP アドレス。これは、IPv4 または IPv6 アドレスにできます。詳細については、 IP アドレス(1-4 ページ) を参照してください。
宛先 IP アドレス	uint8[16]	影響イベントに関連付けられた宛先 IP アドレスの IP アドレス(該当する場合)。これは、IPv4 または IPv6 アドレスにできます。詳細については、 IP アドレス(1-4 ページ) を参照してください。宛先 IP アドレスがない場合、この値は 0 です。

表 3-5 影響イベント データ フィールド (続き)

フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	影響名を含む文字列データのブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、 文字列データ ブロック (4-75 ページ) を参照してください。
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数。これには文字列ブロックタイプ用の 4 バイト、文字列ブロック長用の 4 バイト、および説明のバイト数が含まれます。
説明	string	影響イベントについての説明。

ユーザー レコード

メタデータを要求すると、Cisco Secure Firewall システムのコンポーネントによって生成されたイベントで参照されるユーザーに関する情報を取得できます。eStreamer サービスは、ユーザーレコード内のイベントのユーザー情報を含むメタデータを送信します。形式は次のとおりです。ユーザーレコードには、ユーザー ID と対応する名前が含まれています。ユーザーのメタデータレコードを使用すると、メタデータとユーザー ID 値を関連付けることによってイベントと関連付けられたユーザー名を特定できます(メタデータフラグのいずれか(要求メッセージの [要求フラグ (Request Flags)] フィールドのビット 1、14、15、または 20) が設定されていると、ユーザー情報が送信されます。[要求フラグ \(2-15 ページ\)](#) を参照してください)。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	ヘッダーバージョン (1)																メッセージタイプ (4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ (62)																							
	レコード長																																							
	ユーザー ID (User ID)																																							
	名前の長さ																																							
	名前...																																							

次の表は、ユーザーレコードのフィールドについての説明です。

表 3-6 ユーザーレコードのフィールド

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

表 3-6 ユーザー レコードのフィールド (続き)

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

4.6.1 以上のルール メッセージのレコード

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

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

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ヘッダー バージョン (1)																メッセージ タイプ (4)																							
	メッセージ長																																							
	Netmap ID																		レコード タイプ (66)																					
	レコード長																																							
シグネチャ キー (Key)	ジェネレータ ID																																							
	ルール ID																																							
	リビジョン番号																																							
	表示されるシグネチャ ID																																							
	メッセージ長																		ルール UUID																					

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

次の表は、各ルール固有のフィールドについての説明です。

表 3-7 ルールメッセージのレコードのフィールド

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

4.6.1 以上の分類レコード

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

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

次の表は、分類レコードのフィールドについての説明です。

表 3-8 分類レコードフィールド

フィールド	データタイプ	説明
分類 ID	uint32	分類 ID 番号。
名前の長さ	uint16	名前に含まれるバイト数。
[名前(Name)]	string	分類の名前。
説明の長さ	uint16	説明に含まれるバイト数。
説明	string	分類の説明。

表 3-8 分類レコードフィールド (続き)

フィールド	データタイプ	説明
UUID	uint8[16]	分類の固有識別子として機能する分類 ID 番号。
リビジョン UUID	uint8[16]	分類リビジョンの固有識別子として機能する分類リビジョン ID 番号。

関連ポリシーレコード

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (69)															
	レコード長																															
	関連ポリシー ID																															
	名前の長さ																名前...															
	説明の長さ																説明...															
関連ポリシー UUID	関連ポリシー UUID 関連ポリシー UUID (続き) 関連ポリシー UUID (続き) 関連ポリシー UUID (続き)																															
関連ポリシーリビジョン UUID	関連ポリシーリビジョン UUID 関連ポリシーリビジョン UUID (続き) 関連ポリシーリビジョン UUID (続き) 関連ポリシーリビジョン UUID (続き)																															

次の表は、関連ポリシー レコードのフィールドについての説明です。

表 3-9 関連ポリシー レコードフィールド

フィールド	データタイプ	説明
関連ポリシー ID	uint32	関連ポリシー ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint16	関連ポリシー名に含まれるバイト数。
[名前(Name)]	string	イベントをトリガーした関連ポリシーの名前。
説明の長さ	uint16	関連ポリシーの説明に含まれるバイト数。
説明	string	イベントをトリガーした関連ポリシーの説明。
UUID	uint8[16]	関連ポリシーの固有識別子として機能する関連ポリシー ID 番号。
リビジョン UUID	uint8[16]	関連ポリシーの固有識別子として機能する関連ポリシー リビジョン ID 番号。

関連ルール レコード

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (70)															
	レコード長																															
	関連ルール ID																															
	名前の長さ																名前...															
	名前...																説明の長さ															
	説明...																															
	イベントタイプの長さ																イベントタイプ...															
	イベントタイプ...																関連ルール UUID															

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

次の表は、関連ルール レコードのフィールドについての説明です。

表 3-10 関連ルール レコード フィールド

フィールド	データタイプ	説明
関連ルール ID	uint32	関連ルール ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint16	関連ルール名に含まれるバイト数。
[名前(Name)]	string	イベントをトリガーした関連ルールの名前。
説明の長さ	uint16	関連ルールの説明に含まれるバイト数。
説明	string	イベントをトリガーした関連ルールの説明。
イベントタイプの長さ	uint16	イベントタイプの説明に含まれるバイト数。
イベントタイプ (Event Type)	string	関連ルールをトリガーしたイベントの説明。
UUID	uint8[16]	関連ルールの固有識別子として機能する関連ルール ID 番号。

表 3-10 関連ルールレコードフィールド (続き)

フィールド	データタイプ	説明
リビジョン UUID	uint8[16]	関連ルール リビジョンの固有識別子として機能する関連ルール リビジョン ID 番号。
許可リスト UUID	uint8[16]	許可リスト違反の結果として送信されるイベントの固有識別子として機能する関連 ID 番号。

セキュリティゾーン名レコード

eStreamer サービスは、セキュリティゾーン名レコード内の侵入イベントまたは接続イベントに関連付けられたセキュリティゾーンの名前の情報を含むメタデータを送信します。形式は次のとおりです。(バージョン4のメタデータフラグ(要求メッセージの[要求フラグ(Request Flags)]フィールドのビット20)が設定されていると、セキュリティゾーン情報が送信されます。[要求フラグ\(2-15 ページ\)](#)を参照してください)。メッセージ長フィールドの後に表示されるレコードタイプフィールドにセキュリティゾーン名レコードを示す値 115 があることに注意してください。シリーズ2セットのデータブロックのブロックタイプ14のUUID文字列データブロックが含まれています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (115)															
	レコード長																															
	セキュリティゾーン名のデータブロック (14)																															
	セキュリティゾーン名のデータブロック長																															
	セキュリティゾーン UUID																															
	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	セキュリティゾーン名...																															

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

表 3-11 セキュリティゾーンの名のデータブロック フィールド

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

インターフェイス名レコード

eStreamer サービスは、インターフェイス名レコード内の侵入イベントまたは接続イベントに関連付けられたインターフェイスの名前の情報を含むメタデータを送信します。形式は次のとおりです。(バージョン4のメタデータフラグ(要求メッセージの[要求フラグ(Request Flags)]フィールドのビット20)が設定されていると、インターフェイス名の情報が送信されます。[要求フラグ\(2-15ページ\)](#)を参照してください)。メッセージ長フィールドの後に表示されるレコードタイプフィールドにインターフェイス名レコードを示す値 116 があることに注意してください。シリーズ2セットのデータブロックのブロックタイプ14のUUID文字列データブロックが含まれています。

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

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

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

表 3-12 インターフェイス名のデータブロック フィールド

フィールド	データタイプ	説明
インターフェイス名のデータブロックタイプ	uint32	インターフェイス名のデータブロックを開始します。この値は常に 14 です。ブロックタイプは、シリーズ 2 ブロックです。
インターフェイス名のデータブロック長	uint32	データブロックの長さ。データのバイト数に 2 つのデータブロックヘッダーフィールドの 8 バイトを加えたバイト数です。
インターフェース UUID	uint8[16]	接続イベントに関連付けられたインターフェイスの固有識別子として機能するインターフェイス ID 番号。このフィールドは、このレコードの固有キーです。
文字列ブロックタイプ	uint32	インターフェイスの名前を含む文字列データのブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	インターフェイス名の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの 8 バイトとインターフェイス名のバイト数が含まれます。
インターフェイス名	string	インターフェイス名。

アクセスコントロールポリシー名のレコード

eStreamer サービスは、アクセスコントロールポリシー名レコード内の侵入イベントまたは接続イベントをトリガーしたアクセスコントロールポリシーの名前に関するメタデータを送信します。形式は次のとおりです。(バージョン 4 のメタデータフラグ(要求メッセージの [要求フラグ (Request Flags)] フィールドのビット 20) が設定されていると、アクセスコントロールポリシー名の情報が送信されます。要求フラグ(2-15 ページ) を参照してください)。メッセージ長フィールドの後に表示されるレコードタイプフィールドにアクセスコントロールポリシー名レコードを示す値 117 があることに注意してください。シリーズ 2 セットのデータブロックのブロックタイプ 14 の UUID 文字列データブロックが含まれています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (117)															
	レコード長																															
	アクセスコントロール ポリシー名のデータ ブロック (14)																															
	アクセスコントロール ポリシー名のデータ ブロック長																															
	アクセスコントロール ポリシー UUID																															
	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	アクセスコントロール ポリシー名...																															

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

表 3-13 アクセスコントロールポリシー名のデータブロック フィールド

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

アクセスコントロールルールIDレコードのメタデータ

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (119)															
	レコード長																															
	アクセスコントロールルールIDのデータブロック (15)																															
	アクセスコントロールルールIDのデータブロック長																															
ACルール UUID	アクセスルールポリシー UUID																															
	アクセスコントロールルール UUID (続き)																															
	アクセスコントロールルール UUID (続き)																															
	アクセスコントロールルール UUID (続き)																															
	アクセスコントロールルールID																															
	文字列ブロックタイプ (0)																															
	文字列ブロック長																															
	アクセスコントロールルール名...																															

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

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

フィールド	データタイプ	説明
アクセスコントロールルール ID のデータブロックタイプ	uint32	アクセスコントロールルール ID のデータブロックを開始します。この値は常に 15 です。ブロックタイプは、シリーズ 2 ブロックです。
アクセスコントロールルール ID のデータブロック長	uint32	データブロックの長さ。データのバイト数に 2 つのデータブロックヘッダーフィールドの 8 バイトを加えたバイト数です。
アクセスコントロールルール UUID	uint8[16]	アクセスコントロールルールの UUID。このフィールドとアクセスコントロールルール ID を合わせると、このレコードの固有キーになります。
アクセスコントロールルール ID	uint32	接続イベントに関連付けられたアクセスコントロールポリシーのルールの内部 ID。このフィールドとアクセスコントロールルール UUID を合わせると、このレコードの固有キーになります。
文字列ブロックタイプ	uint32	アクセスコントロールルールの名前を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの 8 バイトとルール名のバイト数が含まれます。
アクセスコントロールルール名	string	アクセスコントロールルールの名前。

管理対象 Device レコードのメタデータ

eStreamer サービスは、管理対象 Device レコード内の侵入イベントに関連付けられた管理対象デバイスの情報を含むメタデータを送信します。形式は次のとおりです。(バージョン 4 のメタデータフラグ(要求メッセージの [要求フラグ (Request Flags)] フィールドのビット 20) が設定されていると、管理対象デバイスのメタデータが送信されます。[要求フラグ \(2-15 ページ\)](#) を参照してください)。メッセージ長フィールドの後に表示されるレコードタイプフィールドに管理対象 Device レコードを示す値 123 があることに注意してください。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ヘッダーバージョン (1)																メッセージタイプ (4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ (123)																							
	レコード長																																							

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

次の表は、管理対象 Device レコードのフィールドについての説明です。

表 3-15 管理対象 Device レコードフィールド

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

マルウェア イベント レコード 5.1.1 以上

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

イベントバージョンが 2 でイベントコードが 101 の要求メッセージでマルウェア イベントフラグ ([要求フラグ (Request Flags)] フィールドのビット 30) を設定することで、マルウェア イベントレコードを要求します。[要求フラグ \(2-15 ページ\)](#) を参照してください。ビット 23 を有効にすると、拡張イベントヘッダーがレコードに含まれます。シリーズ 2 セットのデータブロックのブロックタイプ 24、33、35、44、47 のいずれかのマルウェア イベントのデータブロックが含まれています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダーバージョン (1)																メッセージタイプ (4)																
メッセージ長																																
Netmap ID																レコードタイプ (125)																
レコード長																																
eStreamer サーバー タイムスタンプ (イベント用、ビット 23 が設定されている場合のみ)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																																
マルウェア イベントのデータ ブロック																																

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

表 3-16 マルウェア イベント レコード フィールド

フィールド	データタイプ	説明
マルウェア イベントのデータ ブロック	変数 (variable)	マルウェア イベントのデータ ブロックを示します。詳細については、 マルウェア イベントのデータ ブロック 7.0 以上 (3-100 ページ) を参照してください。

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

eStreamer サービスは、Cisco Advanced Malware Protection クラウドの名前レコード内の侵入イベントまたは接続イベントに関連付けられた (AMP クラウドまたは単にクラウドと呼ばれる) Cisco Advanced Malware Protection クラウドの名前に関する情報を含むメタデータを送信します。この形式を以下に示します。(バージョン 4 のメタデータ フラグ (要求メッセージの [要求フラグ (Request Flags)] フィールドのビット 20) が設定されていると、AMP クラウド名の情報が送信されます。[要求フラグ \(2-15 ページ\)](#) を参照してください)。メッセージ長フィールドの後に表示されるレコードタイプフィールドに Cisco Advanced Malware Protection クラウド名のレコードを示す値 127 があることに注意してください。シリーズ 2 セットのデータ ブロックのブロックタイプ 14 の UUID 文字列データ ブロックが含まれています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダーバージョン (1)																メッセージタイプ (4)																
メッセージ長																																
Netmap ID																レコードタイプ (127)																
レコード長																																
Cisco Advanced Malware Protection クラウド名のデータ ブロック (14)																																
Cisco Advanced Malware Protection クラウド名のデータ ブロック長																																
Cisco Advanced Malware Protection クラウド UUID																																
Cisco Advanced Malware Protection クラウド UUID (続き)																																

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

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

表 3-17 Cisco Advanced Malware Protection クラウド名のデータブロック フィールド

フィールド	データタイプ	説明
Cisco Advanced Malware Protection クラウド名のデータブロックタイプ	uint32	Cisco Advanced Malware Protection クラウド名のデータブロックを開始します。この値は常に 14 です。ブロックタイプは、シリーズ 2 ブロックです。
Cisco Advanced Malware Protection クラウド名のデータブロック長	uint32	データブロックの長さ。データのバイト数に 2 つのデータブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
Cisco Advanced Malware Protection クラウド UUID	uint8[16]	接続イベントに関連付けられた Cisco Advanced Malware Protection クラウドの固有識別子として機能する Cisco Advanced Malware Protection クラウド ID 番号。このフィールドは、このレコードの固有キーです。
文字列ブロックタイプ	uint32	Cisco Advanced Malware Protection クラウドの名前を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	Cisco Advanced Malware Protection クラウド名のデータブロックのバイト数です。ブロックタイプとヘッダーフィールドの 8 バイトと Cisco Advanced Malware Protection クラウド名のバイト数が含まれます。
Cisco Advanced Malware Protection クラウド名	string	Cisco Advanced Malware Protection クラウド名。

マルウェア イベント タイプのメタデータ

eStreamer サービスは、マルウェア イベント タイプ レコード内のイベントのマルウェア イベント タイプ情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグ(要求メッセージの [要求フラグ (Request Flags)] フィールドのビット 20)が設定されると、マルウェア イベント タイプ情報が送信されます。[要求フラグ\(2-15 ページ\)](#) を参照してください)。メッセージ長フィールドの後に表示されるレコードタイプフィールドにマルウェア イベント タイプレコードを示す値 128 があることに注意してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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 (128)															
	レコード長																															
	マルウェア イベント タイプ ID																															
	マルウェア イベント タイプの長さ																															
	マルウェア イベント タイプ...																															

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

表 3-18 マルウェア イベント タイプ レコード フィールド

フィールド	データタイプ	説明
マルウェア イベント タイプ ID	uint32	マルウェア イベント タイプ ID 番号。このフィールドは、このレコードの固有キーです。
マルウェア イベント タイプの長さ	uint32	マルウェア イベント タイプに含まれるバイト数。
マルウェア イベント タイプ	string	マルウェア イベントのタイプ。

マルウェア イベント サブタイプのメタデータ

eStreamer サービスは、マルウェア イベント サブタイプ レコード内のイベントのマルウェア イベント サブタイプ情報を含むメタデータを送信します。形式は次のとおりです。(メタデータ フラグ(要求メッセージの [要求フラグ (Request Flags)] フィールドのビット 20)が設定されると、マルウェア イベント タイプ情報が送信されます。[要求フラグ\(2-15 ページ\)](#) を参照してください)。メッセージ長フィールドの後に表示されるレコードタイプフィールドにマルウェア イベント サブタイプレコードを示す値 129 があることに注意してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (129)															
	レコード長																															
	マルウェア イベント サブタイプ ID																															
	マルウェア イベント サブタイプの長さ																															
	マルウェア イベント サブタイプ...																															

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

表 3-19 マルウェア イベント サブタイプ レコード フィールド

フィールド	データタイプ	説明
マルウェア イベント サブタイプ ID	uint32	マルウェア イベント サブタイプ ID 番号。このフィールドは、このレコードの固有キーです。
マルウェア イベント サブタイプの長さ	uint32	マルウェア イベント サブタイプに含まれるバイト数。
マルウェア イベント サブタイプ	string	マルウェア イベントのサブタイプ。

エンドポイント向け AMPディテクタ タイプのメタデータ

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Netmap ID																レコードタイプ (130)															
	レコード長																															
	エンドポイント向け AMP ディテクタ タイプ ID																															
	エンドポイント向け AMP ディテクタ タイプの長さ																															
	エンドポイント向け AMP ディテクタ タイプ...																															

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

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

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

エンドポイント向け AMP ファイルタイプのメタデータ

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

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

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

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

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

フィールド	データタイプ	説明
エンドポイント向け AMP ファイル タイプ ID	uint32	エンドポイント向け AMP ファイル タイプ ID 番号。このフィールドは、このレコードの固有キーです。
エンドポイント向け AMP ファイル タイプの長さ	uint32	エンドポイント向け AMP ファイル タイプに含まれるバイト数。
エンドポイント向け AMP ファイル タイプ	string	検出されたファイルのタイプ。

セキュリティ コンテキスト名

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダーバージョン (1)																メッセージタイプ (4)																
メッセージ長																																
Netmap ID																レコードタイプ (132)																
レコード長																																
セキュリティ コンテキスト UUID																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	セキュリティ コンテキスト UUID (続き)																															
	セキュリティ コンテキスト UUID (続き)																															
	セキュリティ コンテキスト UUID (続き)																															
	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	セキュリティ コンテキスト名...																															

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

表 3-22 セキュリティ コンテキスト名のレコードフィールド

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

5.4 以上の関連イベント

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

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

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

トストリーム要求メッセージのフラグ フィールドでビット 23 を有効にして、拡張イベントヘッダーを含めることができます。また、フラグ フィールドでビット 20 を有効にして、ユーザーメタデータを含めることもできます。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (112)															
	レコード長																															
	eStreamer サーバー タイムスタンプ (イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み (イベントでビット 23 が設定されている場合のみ)																															
	関連ブロックのタイプ (156)																															
	関連ブロック長																															
	デバイスID (Device ID)																															
	(関連) イベント秒																															
	イベント ID (Event ID)																															
	ポリシー ID																															
	ルール ID																															
	[プライオリティ (Priority)]																															
	文字列ブロック タイプ (0)																イベント 説明															
	文字列ブロック長																															
	説明...																イベントタイプ (Event Type)															
	イベントデバイス ID																															
	シグネチャ ID																															
	シグネチャ ジェネレータ ID																															
	(トリガー) イベント秒																															

■ 侵入イベントとメタデータのレコードタイプ

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
	(トリガー) イベント マイクロ秒																																
	イベント ID (Event ID)																																
	イベントで定義されたマスク																																
	イベント影響フラグ								IPプロトコル								ネットワーク プロトコル																
	ソース IP																																
	送信元ホストタイプ								送信元 VLAN ID																送信元 OS フィンガープリント UUID								送信元 OS フィンガープリント UUID
	送信元 OS フィンガープリント UUID (続き)																																
	送信元 OS フィンガープリント UUID (続き)																																
	送信元 OS フィンガープリント UUID (続き)																																
	送信元 OS フィンガープリント UUID (続き)																送信元重要度																
	送信元重要度 (続き)								送信元ユーザー ID																								
	送信元ユーザー ID (続き)								送信元ポート																送信元サーバー ID								
	送信元サーバー ID (続き)																宛先 IP (Destination IP)																
	宛先 IP (続き)																着信ホストタイプ																
	着信VLAN ID (Admin. VLAN ID)																宛先 OS フィンガープリント UUID																宛先 OS フィンガープリント UUID
	宛先 OS フィンガープリント UUID (続き)																																
	宛先 OS フィンガープリント UUID (続き)																																
	宛先 OS フィンガープリント UUID (続き)																																
	宛先OSフィンガープリントUUID (続き)																宛先重要度																
	着信ユーザー ID (User ID)																																
	接続先ポート																宛先サーバー ID																

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
ビット																																	
	宛先サーバー ID (続き)																影響								ブロック								
	侵入ポリシー (Intrusion Policy) 侵入ポリシー (続き) 侵入ポリシー (続き) 侵入ポリシー (続き)																																
	ルールアクション																																
	文字列ブロック タイプ (0)																																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レビジョン アクセス制御ポリシーのレビジョン (続き) アクセス制御ポリシーのレビジョン (続き) アクセス制御ポリシーのレビジョン (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)																																

■ 侵入イベントとメタデータのレコードタイプ

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
セキュリティ インテリジェンス UUID (続き)																																
セキュリティ インテリジェンス UUID (続き)																																
セキュリティ インテリジェンス UUID (続き)																																
セキュリティ コンテキスト																																
セキュリティ コンテキスト (続き)																																
セキュリティ コンテキスト (続き)																																
セキュリティ コンテキスト (続き)																																
SSL ポリシー ID																																
SSL ポリシー ID (続き)																																
SSL ポリシー ID (続き)																																
SSL ポリシー ID (続き)																																
SSL ルール ID (続き)																																
実際の SSL アクション																																
SSL フロー ステータス																																
SSL 証明書フィンガープリント																																
SSL 証明書フィンガープリント (続き)																																
SSL 証明書フィンガープリント (続き)																																
SSL 証明書フィンガープリント (続き)																																
SSL 証明書フィンガープリント (続き)																																

レコード構造には、シリーズ 1 のブロックである、文字列ブロック タイプが含まれることに注目してください。シリーズ 1 ブロックの詳細については、[ディスカバリ \(シリーズ1\) ブロック \(4-65 ページ\)](#)を参照してください。

表 3-23 関連イベント 5.4 以上のデータ フィールド

フィールド	データタイプ	説明
関連ブロックタイプ	uint32	関連イベント データブロックが続くことを示します。このフィールドの値は常に 156 です。 ディスカバリ (シリーズ1) ブロック (4-65 ページ) を参照してください。
関連ブロック長	uint32	関連データ ブロック長(関連ブロック タイプと長さの 8 バイト、およびそれに続く関連データを含む)。
デバイスID (Device ID)	uint32	関連イベントを生成した管理対象デバイスまたは Management Center の内部 ID 番号。ゼロ値は Management Center を示します。バージョン 3 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 管理対象Device レコードのメタデータ (3-38 ページ) を参照してください。
(関連) イベント秒	uint32	関連イベントが生成された時刻を示す UNIX タイムスタンプ (1970 年 1 月 1 日からの秒数)。
イベント ID (Event ID)	uint32	関連イベント ID 番号。
ポリシー ID	uint32	違反された関連ポリシーの ID 番号。データベースからのポリシー ID 番号を入手する方法の詳細については、 サービス レコード (4-16 ページ) を参照してください。
ルール ID	uint32	トリガーしてポリシー違反となった関連ルールの ID 番号。データベースからポリシー ID 番号を取得する方法の詳細については、 サービス レコード (4-16 ページ) を参照してください。
[プライオリティ (Priority)]	uint32	イベントに割り当てられた優先順位。これは、0 ~ 5 の整数値です。
文字列ブロックタイプ	uint32	関連違反イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、 文字列データ ブロック (4-75 ページ) を参照してください。
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数(文字列のブロックタイプのための 4 バイト、文字列ブロック長のための 4 バイト、説明のバイト数を含む)。
説明	string	関連イベントについての説明。
イベントタイプ (Event Type)	uint8	<p>関連イベントが、侵入、ホスト検出、またはユーザー イベントによってトリガーされたかどうかを示します。</p> <ul style="list-style-type: none"> • 1: 侵入 • 2: ホストの検出 • 3: ユーザー
イベントデバイス ID	uint32	関連イベントをトリガーしたイベントを生成したデバイスの ID 番号。バージョン 3 メタデータを要求するとデバイス名を入手できます。詳細については、 管理対象Device レコードのメタデータ (3-38 ページ) を参照してください。
シグネチャ ID	uint32	イベントが侵入イベントであった場合、イベントに対応するルール ID 番号を示します。そうでない場合、この値は 0 になります。

表 3-23 関連イベント 5.4 以上のデータ フィールド (続き)

フィールド	データタイプ	説明
シグネチャ ジェネレータ ID	uint32	イベントが侵入イベントであった場合、イベントを生成した Cisco Secure Firewall システムプリプロセッサまたはルールエンジンの ID 番号を示します。
(トリガー)イ ベント秒	uint32	関連ポリシー ルールをトリガーしたイベントの時刻を示す UNIX タイムスタンプ(1970年1月1日からの秒数)。
(トリガー)イ ベントマイク ロ秒	uint32	イベントが検出されたタイムスタンプの、マイクロ秒(100万分の1秒)の増分。
イベント ID (Event ID)	uint32	Cisco デバイスによって生成されたイベントの ID 番号。
イベントで 定義された マスク	bits[32]	このフィールドに設定されたビットは、メッセージ内の続くどのフィールドが有効であるかを示します。各ビット値のリストの詳細については、表 3-21 (3-45 ページ) を参照してください。

表 3-23 関連イベント 5.4 以上のデータ フィールド (続き)

フィールド	データタイプ	説明
イベント影響フラグ	bits[8]	<p>イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。</p> <ul style="list-style-type: none"> • 0x01(ビット 0):送信元または宛先ホストはシステムによってモニターされるネットワーク内にあります。 • 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 • 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバーを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 • 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティング システムにマップされた脆弱性があります。 • 0x10(ビット 4):イベントで検出されたサーバーにマップされた脆弱性があります。 • 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Cisco Secure Firewall システム Web インターフェイスのブロックされた状態に対応します。 • 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 • 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) <p>次の影響レベル値は、Management Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。</p> <ul style="list-style-type: none"> • グレー(0、不明):00x00000 • 赤(1、脆弱):xxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx(バージョン 5.0+ のみ) • オレンジ(2、潜在的に脆弱):00x0011x • 黄(3、現在は脆弱でない):00x0001x • 青(4、不明なターゲット):00x00001
IPプロトコル	uint8	イベントに関連付けられている IP プロトコルの ID(該当する場合)。
ネットワークプロトコル	uint16	イベントに関連付けられているネットワーク プロトコル(該当する場合)。
送信元 IP アドレス	uint8[4]	このフィールドは予約済みですが、設定されておりません。送信元 IPv4 アドレスは、送信元 IPv6 アドレス フィールドに保存されます。詳細については、 IP アドレス(1-4 ページ) を参照してください。

表 3-23 関連イベント 5.4 以上のデータ フィールド (続き)

フィールド	データタイプ	説明
送信元ホストタイプ	uint8	送信元ホストのタイプ: <ul style="list-style-type: none"> • 0: ホスト • 1: ルータ • 2: ブリッジ
送信元 VLAN ID	uint16	送信元ホストの VLAN ID 番号(該当する場合)。
送信元 OS フィンガープリント UUID	uint8[16]	送信元ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID。 フィンガープリント ID にマップする値の取得の詳細については、 サービス レコード(4-16 ページ) を参照してください。
送信元重要度	uint16	送信元ホストの、ユーザー定義の重要度値: <ul style="list-style-type: none"> • 0: なし • 1: 低 • 2: 中 • 3: 高
送信元ユーザー ID	uint32	システムにより識別される、送信元ホストにログインしたユーザーの ID 番号。
送信元ポート	uint16	イベントの送信元ポート。
送信元サーバー ID	uint32	送信元ホスト上で実行するサーバーの ID 番号。
宛先 IP アドレス	uint8[4]	このフィールドは予約済みですが、設定されておりません。宛先 IPv4 アドレスは、宛先 IPv6 アドレス フィールドに保存されます。詳細については、 IP アドレス(1-4 ページ) を参照してください。
宛先ホストタイプ	uint8	宛先ホストのタイプ: <ul style="list-style-type: none"> • 0: ホスト • 1: ルータ • 2: ブリッジ
宛先 VLAN ID	uint16	宛先ホストの VLAN ID 番号(該当する場合)。
宛先 OS フィンガープリント UUID	uint8[16]	宛先ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID 番号。 フィンガープリント ID にマップする値の取得の詳細については、 サービス レコード(4-16 ページ) を参照してください。
宛先重要度	uint16	宛先ホストの、ユーザー定義の重要度値: <ul style="list-style-type: none"> • 0: なし • 1: 低 • 2: 中 • 3: 高

表 3-23 関連イベント 5.4 以上のデータ フィールド (続き)

フィールド	データタイプ	説明
宛先ユーザー ID	uint32	システムにより識別される、宛先ホストにログインしたユーザーの ID 番号。
接続先ポート	uint16	イベントの宛先ポート。
宛先サービス ID	uint32	送信元ホスト上で実行するサーバーの ID 番号。
影響	uint8	イベントの影響フラグ値。値は次のとおりです。 <ul style="list-style-type: none"> • 1: レッド(脆弱) • 2: オレンジ(脆弱の可能性あり) • 3: イエロー(現在は脆弱でない) • 4: ブルー(不明なターゲット) • 5: グレー(不明なインパクト)
ブロック	uint8	侵入イベントをトリガーしたパケットの処理を示す値。 <ul style="list-style-type: none"> • 0: 侵入イベントがドロップされていない • 1: 侵入イベントがドロップされている(展開がインライン型、スイッチ型、またはルーティング型である場合はドロップ) • 2: 侵入ポリシーが、インライン型、スイッチ型、またはルーティング型展開のデバイスに適用されている場合は、イベントをトリガーしたパケットがドロップされている可能性がある。
侵入ポリシー (Intrusion Policy)	uint8[16]	イベントに関連付けられた侵入ポリシーの UUID。
ルールアクション	uint32	イベントをトリガーしたルールのユーザー インターフェイスで選択したアクション(許可、ブロックなど)。
文字列ブロックタイプ	uint32	NetBIOS ドメインを含む文字列データ ブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、 文字列データ ブロック (4-75 ページ) を参照してください。
文字列ブロック長	uint32	イベント説明の文字列ブロックのバイト数。これには、文字列ブロックタイプ用の 4 バイト、文字列ブロック長用の 4 バイト、および NetBIOS ドメイン内のバイト数が含まれます。
NetBIOS ドメイン (NetBIOS Domain)	string	NetBIOS ドメインの名前。
URL カテゴリ	uint32	URL カテゴリを指定する番号。詳細については、 URL カテゴリレコードメタデータ (4-26 ページ) を参照してください。
URLレピュテーション	uint32	URL レピュテーションの ID 番号。 URL レピュテーションレコードメタデータ (4-27 ページ) を参照してください
文字列ブロックタイプ	uint32	URL ドメインを含む文字列データ ブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、 文字列データ ブロック (4-75 ページ) を参照してください。

表 3-23 関連イベント 5.4 以上のデータ フィールド (続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	イベント説明の文字列ブロックのバイト数。これには、文字列ブロックタイプ用の4バイト、文字列ブロック長用の4バイト、およびURLのバイト数が含まれます。
URL	string	関連イベントをトリガーしたURLです。
Client ID	uint32	イベントを検出したクライアントのID番号。
文字列ブロックタイプ	uint32	クライアントバージョンを含む文字列データブロックを開始します。この値は常に0に設定されます。文字列ブロックの詳細については、 文字列データブロック (4-75 ページ) を参照してください。
文字列ブロック長	uint32	イベント説明の文字列ブロックのバイト数。これには、文字列ブロックタイプ用の4バイト、文字列ブロック長用の4バイト、およびクライアントバージョン内のバイト数が含まれます。
クライアントバージョン (Client Version)	string	イベントを検出したクライアントのバージョン。
アクセス制御ポリシーのリビジョン	uint8[16]	トリガーされた関連イベントに関連付けられたルールのリビジョン番号。
アクセスコントロールルールID	uint32	イベントをトリガーしたルールの内部ID。
入力インターフェイスUUID	uint8[16]	関連イベントに関連付けられている入力インターフェイスの固有識別子として機能するインターフェイスID。
出力インターフェイスUUID	uint8[16]	関連イベントに関連付けられている出力インターフェイスの固有識別子として機能するインターフェイスID。
入力ゾーンUUID	uint8[16]	関連イベントに関連付けられている入力セキュリティゾーンの固有識別子として機能するゾーンID。
出力ゾーンUUID	uint8[16]	関連イベントに関連付けられている出力セキュリティゾーンの固有識別子として機能するゾーンID。
送信元IPv6アドレス	uint8[16]	IPv6アドレスオクテットの、イベントの送信元ホストのIPアドレス。
宛先IPv6アドレス	uint8[16]	IPv6アドレスオクテットの、イベントの宛先ホストのIPアドレス。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
セキュリティインテリジェンスUUID	uint8[16]	セキュリティインテリジェンスに設定されたアクセスコントロールポリシーのUUID。
セキュリティコンテキスト	uint8[16]	トラフィックが通過したセキュリティコンテキスト(仮想ファイアウォール)のID番号。マルチコンテキストモードのASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

表 3-23 関連イベント 5.4 以上のデータ フィールド (続き)

フィールド	データタイプ	説明
SSL 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	<p>SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 3-23 関連イベント 5.4 以上のデータ フィールド (続き)

フィールド	データタイプ	説明
SSL フロー ステータス	uint32	<p>SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバー名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバーの証明書の処理」 • 16:「サーバー証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバー証明書の検証が使用できません」 • 27:「サーバー証明書の検証エラー」 • 28:「無効な操作」
SSL 証明書フィンガープリント	uint8[20]	SSL サーバー証明書の SHA1 ハッシュ。

シリーズ2のデータブロックの概要

バージョン 4.10.0 から、eStreamer サービスは、2 番目のシリーズのデータブロックを使用して、侵入イベント追加データなどの特定のレコードをパッケージしています。このシリーズのすべてのブロックタイプのリストの詳細については、表 3-24(3-60 ページ)を参照してください。シリーズ2のブロックは、シリーズ1のブロックと同様に、可変長フィールドとネストされたブロックの階層をサポートします。シリーズ2のブロックタイプには、シリーズ1のシリーズのプリミティブのブロックタイプと同様に、ネストされた内部のブロックをカプセル化する機能を備えたプリミティブブロックが含まれています。ただし、シリーズ2のブロックとシリーズ1のブロックは別個の番号システムを備えています。

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

バイト	0								1								2								3									
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
	リストデータブロックタイプ (2)																																	
	データブロック長																																	
サーバー フィンガー プリント	オペレーティングシステムフィンガープリントブロックタイプ (87)																																	
	オペレーティングシステムフィンガープリントブロック長																																	
	オペレーティングシステムサーバーフィンガープリントデータ																																	

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

表 3-24 シリーズ2のブロックタイプ

タイプ (Type)	目次	データブロック ステータス	説明
[0]	文字列	現在 (Current)	さまざまな文字列データをカプセル化します。詳細については、 文字列データブロック (3-66 ページ) を参照してください。
1	BLOB	現在 (Current)	バイナリ データをカプセル化し、バナー専用として使用します。詳細については、 BLOB データブロック (3-67 ページ) を参照してください。
2	リスト	現在 (Current)	他のデータブロックのリストをカプセル化します。詳細については、 リストデータブロック (3-68 ページ) を参照してください。

表 3-24 シリーズ2のブロックタイプ (続き)

タイプ (Type)	目次	データブロックステータス	説明
3	汎用リスト	現在 (Current)	他のデータブロックのリストをカプセル化します。逆シリアル化では、リストのデータブロックに相当します。詳細については、 汎用リストのデータブロック (3-69 ページ) を参照してください。
4	イベント追加データ	レガシー	侵入イベント追加データが含まれています。詳細については、 侵入イベント追加データレコード (B-69 ページ) を参照してください。
5	追加データタイプ	現在 (Current)	追加データのメタデータが含まれています。詳細については、 侵入イベント追加データのメタデータ (B-71 ページ) を参照してください。
14	UUID 文字列マッピング	現在 (Current)	記述文字列に UUID 値をマッピングするためにさまざまなメタデータメッセージで使用されるブロック。 UUID 文字列マッピングのデータブロック (3-69 ページ) を参照してください。
15	アクセスコントロールポリシールールIDのメタデータ	現在 (Current)	アクセスコントロールルールのメタデータが含まれています。 アクセスコントロールポリシールールIDのメタデータブロック (3-72 ページ) を参照してください。
16	マルウェアイベント	レガシー	Cisco Advanced Malware Protection クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザーといったマルウェアイベントに関する情報が含まれています。 マルウェアイベントのデータブロック 5.1 (B-73 ページ) を参照してください。ブロック 24 により廃止される予定です。 マルウェアイベントデータブロック 5.3.1 (B-97 ページ) 。
19	ICMP タイプのデータブロック	現在 (Current)	ICMP タイプを示すメタデータが含まれています。 ICMP タイプのデータブロック (3-73 ページ) を参照してください。
20	ICMP コードのデータブロック	現在 (Current)	ICMP コードを示すメタデータが含まれています。 ICMP コードのデータブロック (3-74 ページ) を参照してください。
21	アクセスコントロールポリシールール理由データブロック	現在 (Current)	アクセスコントロールポリシールールの理由を説明する情報が含まれています。 6.0 以上のアクセスコントロールポリシールール理由データブロック (3-85 ページ) を参照してください。
22	IP レピュテーションカテゴリのデータブロック	現在 (Current)	IP アドレスがブロックされた理由を説明する IP レピュテーションカテゴリに関する情報が含まれています。 アクセスコントロールポリシー名のデータブロック (3-87 ページ) を参照してください。

表 3-24 シリーズ2のブロックタイプ (続き)

タイプ (Type)	目次	データブロックステータス	説明
23	ファイル イベント	レガシー	送信元、SHA ハッシュ、およびファイルの特性などのファイル イベントに関する情報が含まれています。ファイル イベント 5.1.1.x (B-313 ページ) を参照してください。これはブロック 32 に取って代わられますアクセス コントロール ポリシー ルール ID のメタデータ ブロック (3-72 ページ)。
24	マルウェア イベント	レガシー	Cisco Advanced Malware Protection クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザーといったマルウェア イベントに関する情報が含まれています。マルウェア イベント データ ブロック 5.1.1.x (B-77 ページ) を参照してください。ブロック 16 は廃止予定ですマルウェア イベントのデータ ブロック 5.1 (B-73 ページ)。ブロック 33 により廃止される予定ですマルウェア イベント データ ブロック 5.3.1 (B-97 ページ)。
25	侵入イベント	レガシー	接続およびマルウェア イベントと侵入イベントを照合するための情報をはじめとして、侵入イベントに関する情報が含まれています。侵入イベント レコード 5.1.1.x (B-26 ページ) を参照してください。ブロック 34 により廃止される予定です侵入イベント レコード 5.2.x (B-14 ページ)。
26	ファイル イベント SHA ハッシュ	レガシー	マルウェアが含まれていると認識されたファイルの SHA ハッシュと名前が含まれています。ファイル イベント SHA ハッシュ 5.1.1 ~ 5.2.x (B-356 ページ) を参照してください。ブロック 40 により廃止される予定です5.3 以上のファイル イベント SHA ハッシュ (3-111 ページ)。
27	ルール ドキュメントのデータ ブロック	現在 (Current)	イベントの生成に使用されるルールに関する情報が含まれています。詳細については、5.2 以上のルール ドキュメントのデータ ブロック (3-114 ページ) を参照してください。
28	位置情報のデータ ブロック	現在 (Current)	国コードおよび関連付けられた国名が含まれています。5.2 以上の位置情報のデータ ブロック (3-122 ページ) を参照してください。
32	ファイル イベント	レガシー	送信元、SHA ハッシュ、およびファイルの特性などのファイル イベントに関する情報が含まれています。ファイル イベント 5.2.x (B-317 ページ) を参照してください。廃止予定ですファイル イベント 5.1.1.x (B-313 ページ)。ブロック 38 により廃止される予定ですファイル イベント 5.3 (B-321 ページ)。

表 3-24 シリーズ2のブロックタイプ (続き)

タイプ (Type)	目次	データブロックステータス	説明
33	マルウェア イベント	現在 (Current)	Cisco Advanced Malware Protection クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザーといったマルウェア イベントに関する情報が含まれています。マルウェア イベント データ ブロック 5.2.x (B-83 ページ) を参照してください。ブロック 24 は廃止予定です。マルウェア イベント データ ブロック 5.1.1.x (B-77 ページ)。ブロック 35 により廃止される予定です。マルウェア イベントのデータ ブロック 5.3 (B-90 ページ)。
34	侵入イベント	レガシー	接続およびマルウェア イベントと侵入イベントを照合するための情報をはじめとして、侵入イベントに関する情報が含まれています。侵入イベント レコード 5.2.x (B-14 ページ) を参照してください。ブロック 25 は廃止予定です。ブロック 41 により廃止される予定です。侵入イベント レコード 5.3 (B-20 ページ)。
35	マルウェア イベント	レガシー	IOC 情報をはじめとするマルウェア イベントに関する情報が含まれています。マルウェア イベントのデータ ブロック 5.3 (B-90 ページ) を参照してください。ブロック 33 は廃止予定です。マルウェア イベント データ ブロック 5.2.x (B-83 ページ)。ブロック 44 により廃止される予定です。マルウェア イベントのデータ ブロック 5.3 (B-90 ページ)。
38	ファイル イベント	レガシー	送信元、SHA ハッシュ、およびファイルの特性などのファイル イベントに関する情報が含まれています。ファイル イベント 5.3 (B-321 ページ) を参照してください。ブロック 32 は廃止予定です。ブロック 43 により廃止される予定です。マルウェア イベントのデータ ブロック 7.0 以上 (3-100 ページ)。
39	IOC 名のデータ ブロック	現在 (Current)	IOC に関する情報が含まれています。5.3+ の IOC 名 データ ブロック (4-38 ページ) を参照してください。
40	ファイル イベント SHA ハッシュ	現在 (Current)	マルウェアが含まれていると認識されたファイルの SHA ハッシュと名前が含まれています。5.3 以上のファイル イベント SHA ハッシュ (3-111 ページ) を参照してください。ブロック 26 は廃止予定です。ファイル イベント SHA ハッシュ 5.1.1 ~ 5.2.x (B-356 ページ)。
41	侵入イベント	レガシー	IOC と侵入イベントを照合するための情報をはじめとして、侵入イベントに関する情報が含まれています。侵入イベント レコード 5.3 (B-20 ページ) を参照してください。ブロック 34 は廃止予定です。ブロック 42 により廃止される予定です。侵入イベント レコード 5.3.1 (B-32 ページ)。

表 3-24 シリーズ2のブロックタイプ (続き)

タイプ (Type)	目次	データブロックステータス	説明
54	侵入イベント	レガシー	IOC と侵入イベントを照合するための情報をはじめとして、侵入イベントに関する情報が含まれています。 侵入イベント レコード 5.3.1 (B-32 ページ) を参照してください。ブロック 41 は廃止予定です。 侵入イベント レコード 5.3 (B-20 ページ) 。ブロック 45 により廃止される予定です。 侵入イベント レコード 5.4.x (B-38 ページ) 。
43	ファイル イベント	レガシー	送信元、SHA ハッシュ、およびファイルの特性などのファイル イベントに関する情報が含まれています。 ファイル イベント 5.3.1 (B-328 ページ) を参照してください。ブロック 38 は廃止予定です。 ファイル イベント 5.3 (B-321 ページ) 。ブロック 46 により廃止される予定です。 7.0 以降のファイル イベント (3-89 ページ) 。
44	マルウェア イベント	レガシー	IOC 情報をはじめとするマルウェア イベントに関する情報が含まれています。 マルウェア イベントのデータブロック 7.0 以上 (3-100 ページ) を参照してください。ブロック 35 は廃止予定です。 マルウェア イベントのデータブロック 5.3 (B-90 ページ) 。ブロック 47 により廃止される予定です。 マルウェア イベントのデータブロック 7.0 以上 (3-100 ページ) 。
45	侵入イベント	レガシー	侵入イベントに関する情報が含まれています。「 侵入イベント レコード 5.4.x (B-38 ページ) 」を参照してください。ブロック 42 は廃止予定です。 侵入イベント レコード 5.3.1 (B-32 ページ) 。ブロック 60 により廃止される予定です。 侵入イベント レコード 6.x (B-47 ページ) 。
46	ファイル イベント	レガシー	送信元、SHA ハッシュ、およびファイルの特性などのファイル イベントに関する情報が含まれています。 マルウェア イベントのデータブロック 7.0 以上 (3-100 ページ) を参照してください。ブロック 43 は廃止予定です。 ファイル イベント 5.3.1 (B-328 ページ) 。
47	マルウェア イベント	現在 (Current)	IOC 情報をはじめとするマルウェア イベントに関する情報が含まれています。 マルウェア イベントのデータブロック 7.0 以上 (3-100 ページ) を参照してください。ブロック 44 は廃止予定です。 マルウェア イベント データブロック 5.3.1 (B-97 ページ) 。
50	SSL 証明書の詳細	現在 (Current)	SSL 証明書に関する情報が含まれています。 5.4 以上の SSL 証明書の詳細のデータブロック (3-133 ページ) を参照してください。
51	SSL ルール ID	現在 (Current)	SSL ルールに関する情報が含まれています。 SSL ルール ID (3-126 ページ) を参照してください。

表 3-24 シリーズ2のブロックタイプ (続き)

タイプ (Type)	目次	データブロックステータス	説明
72	ファイル イベント	レガシー	ファイルイベントに関する情報が含まれています。「 6.xのファイルイベント (B-345 ページ) 」を参照してください。ブロック 46 は廃止予定です。 ファイル イベント 5.4.x (B-334 ページ) 。ブロックタイプ 79 で廃止されます。マルウェア イベントのデータ ブロック 7.0 以上 (3-100 ページ)
57	ユーザー レコード	現在 (Current)	ユーザーに関する情報が含まれています。 ユーザー レコード (3-26 ページ) を参照してください
58	エンドポイント プロファイル (Endpoint Profile)	現在 (Current)	ネットワークエンドポイントに関する情報が含まれています。 6.0以上のエンドポイント プロファイルのデータ ブロック (3-78 ページ) を参照してください
59	アクセス コントロール ポリシー ルールの理由	現在 (Current)	アクセス コントロール ポリシー ルールに関する情報が含まれています。 6.0以上のアクセス コントロール ポリシー ルール理由データ ブロック (3-85 ページ) を参照してください
60	侵入イベント	レガシー	侵入イベントに関する情報が含まれています。「 侵入 イベント レコード 6.x (B-47 ページ) 」を参照してください。ブロック 45 は廃止予定です。 侵入 イベント レコード 5.3.1 (B-32 ページ) 。ブロック 81 により廃止される予定です。 侵入 イベント レコード 7.1 以上 (3-9 ページ) 。
61	名前説明マッピング	現在 (Current)	多くの状況で、名前を説明にマッピングするために使用されます。 名前説明マッピングのデータ ブロック (3-71 ページ) を参照してください
62	マルウェア イベント	レガシー	マルウェア イベントに関する情報が含まれています。 マルウェア イベント データ ブロック 6.x (B-116 ページ) を参照してください。ブロック 44 は廃止予定です。 マルウェア イベント データ ブロック 5.3.1 (B-97 ページ) 。ブロックタイプ 80 で廃止されます。マルウェア イベントのデータ ブロック 7.0 以上 (3-100 ページ)
64	アクセス コントロール ポリシー名	現在 (Current)	アクセス コントロール ポリシー名に関する情報が含まれています。 アクセス コントロール ポリシー名のデータ ブロック (3-87 ページ) を参照してください
79	ファイル イベント	現在 (Current)	ファイルイベントに関する情報が含まれています。「 7.0以降のファイルイベント (3-89 ページ) 」を参照してください。ブロック 56 は廃止予定です。 6.xのファイルイベント (B-345 ページ) 。

表 3-24 シリーズ2のブロックタイプ (続き)

タイプ (Type)	目次	データブロックステータス	説明
80	マルウェア イベント	現在 (Current)	マルウェア イベントに関する情報が含まれています。「 マルウェア イベントのデータブロック 7.0 以上 (3-100 ページ) 」を参照してください。ブロック 62 は廃止予定です。 マルウェア イベント データ ブロック 6.x (B-116 ページ) 。
81	侵入 イベント	現在 (Current)	侵入 イベントに関する情報が含まれています。「 侵入 イベント レコード 7.1 以上 (3-9 ページ) 」を参照してください。ブロック 60 は廃止予定です。 侵入 イベント レコード 6.x (B-47 ページ) 。

シリーズ2のプリミティブデータブロック

シリーズ2とシリーズ1のブロックには、メッセージ内の可変長の文字列と BLOB に加えて、可変長ブロックのリストのカプセル化に使用される一連のプリミティブがあります。こうしたプリミティブブロックには、[データブロック ヘッダー \(2-29 ページ\)](#) で説明した標準的な eStreamer ブロック ヘッダーがありますが、表示されるのは他のデータブロック内のみです。所定のブロックタイプに任意の数値を含めることができます。これらのブロックの構造の詳細については、次の項を参照してください。

- [文字列データブロック \(3-66 ページ\)](#)
- [BLOB データブロック \(3-67 ページ\)](#)
- [リスト データブロック \(3-68 ページ\)](#)
- [汎用リストのデータブロック \(3-69 ページ\)](#)
- [UUID 文字列マッピングのデータブロック \(3-69 ページ\)](#)
- [名前説明マッピングのデータブロック \(3-71 ページ\)](#)

文字列データブロック

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

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

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



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

次の図に、文字列データブロックの形式を示します。



次の表に、文字列データブロックのフィールドの説明を示します。

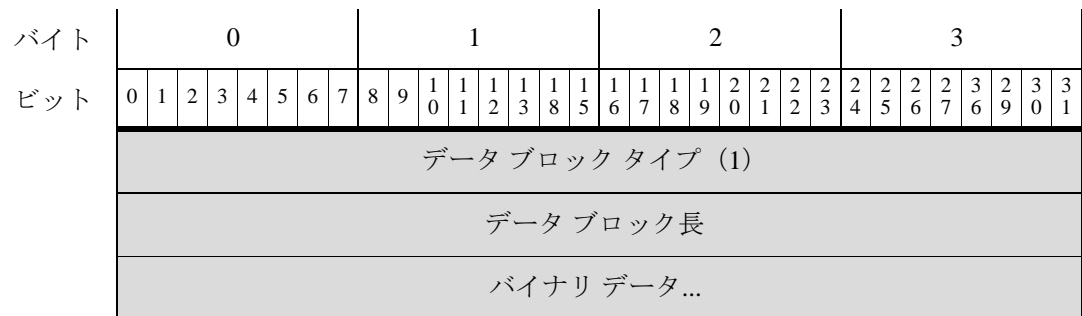
表 3-25 文字列ブロック フィールド

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

BLOB データ ブロック

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

次の図に、BLOB データブロックの形式を示します。



次の表に、BLOB データ ブロックのフィールドの説明を示します。

表 3-26 BLOB データブロック フィールド

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

リスト データ ブロック

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

次の図に、リスト データ ブロックの基本的な形式を示します。



次の表では、リスト データ ブロックのフィールドについて説明します。

表 3-27 リスト データ フィールド

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

汎用リストのデータブロック

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

次の図に、汎用リストのデータ ブロックの基本的な構造を示します。



次の表では、汎用リスト データ ブロックのフィールドについて説明します。

表 3-28 汎用リスト データ ブロックのフィールド

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

UUID 文字列マッピングのデータ ブロック

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

次の図に、UUID 文字列マッピングのデータ ブロックの構造を示します。

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

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

表 3-29 UUID 文字列マッピングのデータ ブロック フィールド

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

名前説明マッピングのデータブロック

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

次の図に、名前説明マッピングのデータ ブロックの構造を示します。



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

表 3-30 名前説明マッピングのデータ ブロック フィールド

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

表 3-30 名前説明マッピングのデータブロックフィールド (続き)

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

アクセスコントロールポリシールールIDのメタデータブロック

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

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

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

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

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

表 3-32 ICMP タイプのデータ ブロック フィールド

フィールド	データタイプ	説明
ICMP タイプのデータ ブロック タイプ	uint32	ICMP タイプのデータ ブロックを開始します。この値は常に 19 です。
ICMP タイプのデータのブロック長	uint32	ICMP タイプのデータ ブロックの合計バイト数です。ICMP タイプのデータ ブロック タイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
タイプ (Type)	uint16	イベントの ICMP タイプ。
プロトコル	uint16	IANA 指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none"> • 0:IP • 1:ICMP • 6:TCP • 17:UDP
文字列ブロック タイプ	uint32	ICMP タイプの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	イベントの ICMP タイプの説明。

ICMP コードのデータ ブロック

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (270)															
	ICMP コードのデータブロックタイプ (20)																															
	ICMP コードのデータブロック長																															
	コード (Code)																タイプ															
説明	プロトコル																文字列ブロックタイプ (0)															
	文字列ブロックタイプ (0) (続き)																文字列ブロック長															
	文字列ブロック長 (続き)																説明...															

次の表は、ICMP コードのデータブロックのフィールドについての説明です。

表 3-33 ICMP コードのデータブロック フィールド

フィールド	データタイプ	説明
ICMP コードのデータブロックタイプ	uint32	ICMP コードのデータブロックを開始します。この値は常に 20 です。
ICMP コードのデータブロック長	uint32	ICMP コードのデータブロックの合計バイト数です。ICMP コードのデータブロックタイプとブロック長フィールドの 8 バイトと後続のデータのバイト数が含まれます。
コード(Code)	uint16	イベントの ICMP コード。
タイプ(Type)	uint16	イベントの ICMP タイプ。
プロトコル	uint16	IANA 指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none"> • 0:IP • 1:ICMP • 6:TCP • 17:UDP
文字列ブロックタイプ	uint32	ICMP コードの説明を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	イベントの ICMP コードの説明。

5.4.1 以上のセキュリティ インテリジェンス カテゴリのメタデータ

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (282)															
	レコード長																															
	セキュリティ インテリジェンス UUID																															
	セキュリティ インテリジェンス UUID (続き)																															
	セキュリティ インテリジェンス UUID (続き)																															
	セキュリティ インテリジェンス UUID (続き)																															
	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	セキュリティ インテリジェンスのカテゴリ...																															

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

表 3-34 セキュリティ コンテキスト名のレコードフィールド

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

表 3-34 セキュリティ コンテキスト名のレコードフィールド (続き)

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

6.0 以上のレルムのメタデータ

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン (1)																メッセージ タイプ (4)															
	メッセージ長																															
	Netmap ID																レコード タイプ (300)															
	レコード長																															
	レルム ID																															
	レルム名の長さ																															
	レルム名...																															

次の表は、レルムのメタデータのレコードのフィールドについての説明です。

表 3-35 レルムのメタデータのレコードフィールド

フィールド	データタイプ	説明
レルム ID	uint32	レルム ID 番号。このフィールドは、このレコードの固有キーです。
レルム名の長さ	uint32	レルム名に含まれるバイト数。
レルム名	string	レルム名

6.0 以上のエンドポイント プロファイルのデータ ブロック

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

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

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	ヘッダーバージョン(1)																メッセージタイプ(4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ(301)																							
	エンドポイント プロファイルのブロックタイプ(58)																																							
	エンドポイント プロファイルのデータのブロック長																																							
	ID																																							
プロファイル名 (Profile Name)	文字列ブロックタイプ(0)																																							
	文字列ブロック長																																							
	プロファイル名...																																							
正式名称	文字列ブロックタイプ(0)																																							
	文字列ブロック長																																							
	正式名称...																																							

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

表 3-36 エンドポイント プロファイルのデータ ブロック フィールド

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

表 3-36 エンドポイントプロファイルのデータブロックフィールド (続き)

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

6.0 以上のセキュリティグループのメタデータ

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

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	ヘッダーバージョン (1)																メッセージタイプ (4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ (302)																							
	レコード長																																							
	セキュリティグループ ID																																							
	セキュリティグループ名の長さ																																							
	セキュリティグループ名...																																							

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

表 3-37 セキュリティ グループのメタデータのレコードフィールド

フィールド	データタイプ	説明
セキュリティ グループ ID	uint32	セキュリティ グループ ID 番号。このフィールドは、このレコードの固有キーです。
セキュリティ グループ名の長さ	uint32	セキュリティ グループ名に含まれるバイト数。
セキュリティ グループ名	string	セキュリティ グループ名。

6.0 以上の DNS レコードタイプのメタデータ

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

バイト	0								1								2								3										
ビット	0	1	2	3	4	5	6	7	8	9	0	1	1	2	3	4	5	6	7	8	9	0	1	2	2	2	2	2	2	2	2	3	2	3	3
	ヘッダーバージョン (1)																メッセージタイプ (4)																		
	メッセージ長																																		
	Netmap ID																レコードタイプ (320)																		
	レコード長																																		
	名前説明のブロック タイプ (61)																																		
	名前説明のデータ ブロック長																																		
	DNS レコード ID																																		
DNS レコードタイプ名	文字列ブロック タイプ (0)																																		
	文字列ブロック長																																		
	DNS レコードタイプ名...																																		
DNS レコードタイプの説明	文字列ブロック タイプ (0)																																		
	文字列ブロック長																																		
	DNS レコードタイプの説明...																																		

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

表 3-38 DNS レコードタイプメタデータ フィールド

フィールド	データタイプ	説明
名前説明のデータ ブロック タイプ	uint32	名前説明のデータ ブロックを開始します。この値は常に 61 です。
名前説明のデータ ブロック 長	uint32	名前説明のデータ ブロック内の総バイト数。これには、名前説明のデータ ブロックのタイプ フィールドおよび長さフィールド用の 8 バイトと、その後のデータのバイト数が含まれます。
DNS レコード ID	uint32	DNS レコード ID 番号。このフィールドは、このレコードの固有キーです。
文字列ブロック タイプ	uint32	DNS レコード タイプの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック 長	uint32	DNS レコード タイプ名文字列のデータ ブロック内に含まれるバイト数。これには、ブロック タイプ フィールドおよびヘッダー フィールド用の 8 バイトと、DNS レコード タイプ名フィールド内のバイト数が含まれます。
DNS レコード タイプ名	string	DNS レコード タイプの名前。
文字列ブロック タイプ	uint32	DNS レコード タイプの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック 長	uint32	DNS レコード タイプ説明文字列のデータ ブロック内に含まれるバイト数。これには、ブロック タイプ フィールドおよびヘッダー フィールド用の 8 バイトと、DNS レコード タイプ説明フィールド内のバイト数が含まれます。
DNS レコード タイプの 説明	string	DNS レコード タイプの説明。

6.0 以上の DNS レスponse タイプのメタデータ

eStreamer サービスは、DNS レスponse 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ponse 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																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	名前説明のブロック タイプ (61)																															
	名前説明のデータ ブロック長																															
	DNS 応答 ID																															
DNSレスポ ンスタイ プ名	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	DNS レスポンス タイプ名...																															
DNSレスポ ンスタイ プの説明	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	DNS レスポンス タイプの説明...																															

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

表 3-39 DNS レスポンス タイプのメタデータ フィールド

フィールド	データタイプ	説明
名前説明のデータ ブロ ック タイプ	uint32	名前説明のデータブロックを開始します。この値は常に 61 です。
名前説明のデータ ブロ ック長	uint32	名前説明のデータブロック内の総バイト数。これには、名前説明のデータブロックのタイプフィールドおよび長さフィールド用の 8 バイトと、その後のデータのバイト数が含まれます。
DNS 応答 ID	uint32	DNS レスポンス ID 番号。このフィールドは、このレコードの固有キーです。
文字列ブロック タイプ	uint32	DNS レスポンス タイプの名前を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	DNS レスポンス タイプ名文字列のデータブロック内に含まれるバイト数。これには、ブロックタイプフィールドおよびヘッダーフィールド用の 8 バイトと、DNS レスポンス タイプ名フィールド内のバイト数が含まれます。
DNS レスポンス タイプ名	string	DNS レスポンス タイプの名前。
文字列ブロック タイプ	uint32	DNS レスポンス タイプの説明を含む文字列データブロックを開始します。この値は常に 0 です。

表 3-39 DNS レスポンス タイプのメタデータ フィールド (続き)

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

6.0 以上のシンクホールのメタデータ

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (322)															
	レコード長																															
	UUID 文字列データ ブロック タイプ (14)																															
	UUID 文字列データ ブロック長																															
	シンクホール UUID																															
	シンクホール UUID (続き)																															
	シンクホール UUID (続き)																															
	シンクホール UUID (続き)																															
シンク ホール名	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	シンクホール名...																															

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

表 3-40 シンクホールのメタデータのレコードフィールド

フィールド	データタイプ	説明
UUID 文字列データ ブロックタイプ	uint32	UUID 文字列データ ブロックを開始します。この値は常に 14 です。
UUID 文字列データ ブロック長	uint32	UUID 文字列データ ブロック内の総バイト数。これには、UUID 文字列データ ブロックのタイプフィールドおよび長さフィールド用の 8 バイトと、その後のデータのバイト数が含まれます。
シンクホール UUID	uint8[16]	シンクホールの UUID 番号。このフィールドは、このレコードの固有キーです。
文字列ブロック タイプ	uint32	シンクホールの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	シンクホール名文字列のデータ ブロック内に含まれるバイト数。これには、ブロックタイプフィールドおよびヘッダーフィールド用の 8 バイトと、シンクホール名フィールド内のバイト数が含まれます。
シンクホール名	string	シンクホールの名前。

6.0 以上の Netmap ドメインのメタデータ

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

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

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

表 3-41 シンクホールのメタデータのレコードフィールド

フィールド	データタイプ	説明
Netmap ドメイン ID	uint32	Netmap ドメイン ID 番号。このフィールドは、このレコードの固有キーです。
Netmap ドメイン名の長さ	uint32	Netmap ドメイン名に含まれるバイト数。
Netmap ドメイン名	string	Netmap ドメイン名

6.0 以上のアクセスコントロールポリシールール理由データブロック

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (124)															
	アクセスコントロールポリシールール理由データブロックタイプ (59)																															
	アクセスコントロールポリシールールの理由のデータブロックの長さ																															
	理由																															
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 3-42 アクセスコントロールポリシールール理由データブロックのフィールド

フィールド	データタイプ	説明
アクセスコントロールポリシールール理由データブロックタイプ	uint32	アクセスコントロールポリシールール理由データブロックを開始します。この値は常に 59 です。
アクセスコントロールポリシールールの理由のデータブロックの長さ	uint32	アクセスコントロールポリシールール理由データブロックのバイトの合計数(アクセスコントロールポリシールール理由データブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
理由 (Reason)	uint32	<p>イベントをトリガーしたルールの理由の番号。</p> <p>ルールの理由は、複数のビットを設定できるバイナリビットマップです。ルールには、複数の理由がある場合があります。ビット値は次のとおりです。</p> <ul style="list-style-type: none"> • 1: IP ブロック • 2: IP モニター • 4: ユーザー バイパス • 8: ファイル モニター • 16: ファイル ブロック • 32: 侵入モニター • 64: 侵入ブロック • 128: ファイル再開ブロック • 256: ファイル再開許可 • 512: ファイルカスタム検出 • 1024: SSL ブロック • 2048: DNS ブロック • 4096: DNS モニター • 8192: URL ブロック • 16384: URL モニター • 32768: コンテンツ制約 • 65536: インテリジェント アプリケーション バイパス • 131072: WSA 脅威
文字列ブロックタイプ	uint32	アクセスコントロールポリシールール理由の説明を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	ルールの理由の説明。

アクセスコントロールポリシー名のデータブロック

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

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



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

表 3-43 アクセスコントロールポリシーのポリシー名のデータブロックフィールド

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

表 3-43 アクセスコントロールポリシーのポリシー名のデータブロック フィールド (続き)

フィールド	データタイプ	説明
センサー ID (Sensor ID)	uint32	アクセスコントロールポリシーに関連付けられたセンサー ID 番号
文字列ブロックタイプ	uint32	アクセスコントロールポリシーの名前を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの 8 バイトと名前フィールドのバイト数が含まれます。
[名前(Name)]	string	アクセスコントロールポリシーの名前。

IP レピュテーションカテゴリのデータブロック

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

次の図に、IP レピュテーションカテゴリのデータブロックの構造を示します。

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

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

表 3-44 IP レピュテーション カテゴリのデータ ブロック フィールド

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

7.0 以降のファイルイベント

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

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

次の図は、ファイル イベント データ ブロックの構造を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイルイベントのブロックタイプ (79)																																
ファイルイベントブロック長																																
デバイスID (Device ID)																																
接続インスタンス																接続数カウンタ																

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

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

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

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

表 3-45 7.0 以上のファイル イベントのデータブロック フィールド

フィールド	データタイプ	説明
ファイル イベント ブロック タイプ	uint32	ファイル イベント データ ブロックを開始します。この値は常に 79 です。
ファイル イベント ブロック 長	uint32	ファイル イベント ブロックのバイトの合計数(ファイル イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID (Device ID)	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または侵入 イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続タイムスタンプ	uint32	関連する接続イベントの UNIX タイムスタンプ(1970年1月1日からの秒数)。
ファイル イベント タイムスタンプ (File Event Timestamp)	uint32	ファイル タイプが識別されてファイル イベントが生成されたときの UNIX タイムスタンプ(1970年1月1日からの秒数)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> • 1 (CLEAN) : ファイルはクリーンであり、マルウェアは含まれていません。 • 2 (UNKNOWN) : ファイルにマルウェアが含まれているかどうかは不明です。 • 3 (MALWARE) : ファイルにはマルウェアが含まれています。 • 4 : UNAVAILABLE。ソフトウェアから AMP クラウドに対して、特性を確認する要求を送信できなかったか、または AMP クラウド サービスが要求に応答しなかった。 • 5 (CUSTOM SIGNATURE) : ファイルがユーザー定義のハッシュと一致するため、ユーザーが指定した方法で処理されました。
SPERO 解析 結果	uint8	SPERO 署名がファイル分析で使用されたかどうかを示します。値が 1、2、または 3 であれば、SPERO 分析は使用されました。それ以外の値であれば、SPERO 分析は使用されませんでした。

表 3-45 7.0 以上のファイルイベントのデータブロックフィールド (続き)

フィールド	データタイプ	説明
ファイルストレージステータス	uint8	<p>ファイルの保存ステータス。値は以下のとおりです。</p> <ul style="list-style-type: none"> • 1:ファイルが保存されました • 2:ファイルが保存されました • 3:ファイルを保存できません • 4:ファイルを保存できません • 5:ファイルを保存できません • 6:ファイルを保存できません • 7:ファイルを保存できません • 8:ファイルサイズが大きすぎます • 9:ファイルサイズが小さすぎます • 10:ファイルを保存できません • 11:ファイルは保存されておらず、解析結果を入手できません

表 3-45 7.0 以上のファイルイベントのデータブロック フィールド (続き)

フィールド	データタイプ	説明
ファイル分析ステータス	uint8	<p>ファイルが動的分析のために送信されているかどうかを示します。値は以下のとおりです。</p> <ul style="list-style-type: none"> • 0: ファイルが分析のために送信されていません • 1: 分析のために送信されました • 2: 分析のために送信されました • 4: 分析のために送信されました • 5: 送信に失敗しました • 6: 送信に失敗しました • 7: 送信に失敗しました • 8: 送信に失敗しました • 9: ファイルサイズが小さすぎます • 10: ファイルサイズが大きすぎます • 11: 分析のために送信されました • 12: 分析が完了しました • 13: 失敗(ネットワークの問題) • 14: 失敗(レート制限) • 15: 失敗(ファイルが大きすぎます) • 16: 失敗(ファイルの読み取りエラー) • 17: 失敗(内部ライブラリ エラー) • 19: ファイルは送信されておらず、解析結果を入手できません • 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ため、ファイル キャパシティが処理されました(センサーに保存) • 25(ファイル送信サーバー制限超過によるキャパシティの処理): サーバーの速度制限が原因でファイル キャパシティが処理されました • 26(通信障害): クラウド接続失敗が原因でファイル キャパシティが処理されました • 27(未送信): 設定が原因でファイルは送信されていません。 • 28(事前分類の一致なし): 事前分類でファイル内に埋め込みオブジェクトまたは疑わしいオブジェクトが検出されなかったため、ファイルはダイナミック分析用に送信されませんでした • 29(Transmit Sent Sandbox Private Cloud): ダイナミック分析のためにファイルがプライベートクラウドに送信されました。 • 30(送信ボックスはプライベートクラウドに未送信): ファイルは分析のためにプライベートクラウドに送信されませんでした。

表 3-45 7.0 以上のファイルイベントのデータブロック フィールド (続き)

フィールド	データタイプ	説明
ローカルのマルウェア分析ステータス	uint8	ファイルのマルウェア分析ステータス。値は以下のとおりです。 <ul style="list-style-type: none"> 0: ファイルが分析されません 1: 分析が実行されました 2: 分析が失敗しました 3: 手動による分析の要求
アーカイブファイルステータス	uint8	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。 <ul style="list-style-type: none"> 0 (N/A): ファイルがアーカイブとして検査されていません。 1: 保留中。アーカイブは調査中です 2: 取得済み。調査が問題なく正常に実行されました 3: 失敗。システムのリソース不足のため調査に失敗しました。 4: 深度の超過。調査は正常に実行されましたが、アーカイブがネストされた調査の深度を超過しました 5: 暗号化。部分的に正常に実行されましたが、アーカイブが暗号化されているか、暗号化されたアーカイブが含まれています 6: 調査できませんでした。部分的に正常に実行されましたが、ファイル形式が不正であるか破損しています
脅威スコア	uint8	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。 <ul style="list-style-type: none"> 1: 検出 2: ブロック 3: マルウェアクラウドルックアップ 4: マルウェアブロック 5: マルウェア許可リスト 6: クラウドルックアップのタイムアウト 7: カスタム検出 8: カスタム検出ブロック 9: アーカイブブロック (深度超過) 10: アーカイブブロック (暗号化されている) 11: アーカイブブロック (調査エラー)
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
ファイルタイプ ID	uint32	ファイルタイプにマップされている ID 番号。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、 エンドポイント向け AMP ファイルタイプのメタデータ (3-44 ページ) を参照してください。
ファイル名	string	ファイルの名前。

表 3-45 7.0 以上のファイルイベントのデータブロック フィールド (続き)

フィールド	データタイプ	説明
ファイル サイズ (File size)	uint64	ファイルのサイズ(バイト単位)。
方向 (Direction)	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示す値。次のいずれかの値になります。 <ul style="list-style-type: none"> • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザー ID (User ID)	uint32	システムにより識別される、宛先ホストにログインしたユーザーの ID 番号。
URI	string	接続の Uniform Resource Identifier (URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザーが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキストモードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバー証明書の SHA1 ハッシュ。

表 3-45 7.0 以上のファイルイベントのデータブロックフィールド (続き)

フィールド	データタイプ	説明
実際の SSL アクション	uint16	<p>SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 3-45 7.0 以上のファイルイベントのデータブロック フィールド (続き)

フィールド	データタイプ	説明
SSL フロー ステータス	uint16	<p>SSL フローのステータス。アクションが実行された理由、またはエラーメッセージが出された理由を示す値です。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバー名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバーの証明書の処理」 • 16:「サーバー証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバー証明書の検証が使用できません」 • 27:「サーバー証明書の検証エラー」 • 28:「無効な操作」
文字列ブロックタイプ	uint32	<p>アーカイブ SHA を含む文字列データ ブロックを開始します。この値は常に 0 です。</p>

表 3-45 7.0 以上のファイルイベントのデータブロックフィールド (続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	アーカイブ SHA 文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、および侵入ポリシー名のバイト数を含む)。
アーカイブ SHA	string	ファイルが含まれる親アーカイブの SHA1 ハッシュ。
文字列ブロックタイプ	uint32	アーカイブ名を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	アーカイブ名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびアーカイブ名のバイト数を含む)。
アーカイブ名	string	親アーカイブの名前。
アーカイブ深度	uint8	ファイルがネストされている層の数。たとえば、テキストファイルが zip アーカイブ内にある場合、この値は1になります。
HTTP 応答コード (HTTP Response Code)	uint32	HTTP 応答コード。
文字列ブロックタイプ	uint32	入力 VRF の名前を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの8バイト、および入力 VRF 名フィールドのバイト数が含まれています。
入力 VRF 名	文字列	トラフィックがネットワークに入るときに通過する仮想ルータ。
文字列ブロックタイプ	uint32	出力 VRF の名前を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの8バイト、および出力 VRF 名フィールドのバイト数が含まれています。
出力 VRF 名	文字列	トラフィックがネットワークから出るときに通過する仮想ルータの名前。

マルウェア イベントのデータブロック 7.0 以上

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

マルウェアイベントレコードの一部としてイベントを要求するには、イベントバージョン8およびイベントコード101の要求メッセージ内に、マルウェアイベントフラグ(要求フラグフィールドのビット30)を設定します。

次の図に、マルウェア イベントのデータブロックの構造を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	マルウェア イベントのブロック タイプ (80)																															
	マルウェア イベントのブロック長																															
	エージェント UUID エージェント UUID(続き) エージェント UUID(続き) エージェント UUID(続き)																															
	クラウド UUID クラウド UUID(続き) クラウド UUID(続き) クラウド UUID(続き)																															
	マルウェア イベント タイムスタンプ																															
	イベント タイプ ID																															
	イベント サブタイプ ID																															
検出名	ディテクタ ID								文字列ブロック タイプ (0)																							
	文字列ブロック タイプ (0) (続き)								文字列ブロック長																							
	文字列ブロック長 (続き)								検出名...																							
ユーザー (User)	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザー...																															
ファイル名	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイル名...																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイルパス	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイルパス...																															
ファイル SHA ハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイル サイズ (File size)																															
	ファイル タイプ																															
	ファイルのタイムスタンプ																															
親ファイル [名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル名...																															
親ファイル SHA ハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル SHA ハッシュ...																															
イベント 説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	イベントの説明...																															
デバイスID (Device ID)																																
接続インスタンス																接続数カウンタ																
接続イベント タイムスタンプ																																
方向 (Direction)								送信元 IP アドレス																								
送信元 IP アドレス(続き)																																
送信元 IP アドレス(続き)																																
送信元 IP アドレス(続き)																																

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
	送信元 IP (続き)								宛先 IP アドレス																															
	宛先 IP アドレス (続き)																																							
	宛先 IP アドレス (続き)																																							
	宛先 IP アドレス (続き)																																							
	宛先 IP (続き)								アプリケーション ID (Application ID)																															
	アプリケーション ID (続き)								ユーザー ID (User ID)																															
	ユーザー ID (続き)								アクセス コントロール ポリシー UUID																															
	アクセス コントロール ポリシー UUID (続き)																																							
	アクセス コントロール ポリシー UUID (続き)																																							
	アクセス コントロール ポリシー UUID (続き)																																							
URI	アクセス コントロール ポリシー UUID (続き)								傾向								レトロスペクティブ傾向								文字列ブロックタイプ(0)															
	文字列ブロックタイプ(0) (続き)																文字列ブロック長																							
	文字列ブロック長 (続き)																URI...																							
	送信元ポート (Source Port)																接続先ポート																							
	送信元の国																宛先の国																							
	Web アプリケーション ID																																							
	クライアントアプリケーション ID																																							
	操作								プロトコル								脅威スコア								IOC 番号															
	IOC 番号 (続き)								セキュリティ コンテキスト																															
	セキュリティ コンテキスト (続き)																																							
	セキュリティ コンテキスト (続き)																																							
	セキュリティ コンテキスト (続き)																																							

バイト	0								1								2								3															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
ビット	セキュリティ コンテキスト (続き)								SSL 証明書フィンガープリント																															
									SSL 証明書フィンガープリント(続き)																															
									SSL 証明書フィンガープリント(続き)																															
									SSL 証明書フィンガープリント(続き)																															
	SSL 証明書 フィンガー プリント(続き)								実際の SSL アクション																SSL フロース テータス															
アーカイブ SHA	SSL フロース テータス(続き)								文字列ブロック タイプ(0)																															
	文字列ブロック タイプ(続き)								文字列ブロック タイプ(0)																															
	文字列長さ (続き)								アーカイブ SHA...																															
アーカイブ名	文字列ブロック タイプ(0)																																							
	文字列ブロック長																																							
	アーカイブ名...																																							
	アーカイブ深度								HTTP レスポンス (HTTP Response)																															
入力 VRF	HTTP レスポンス (続き)								文字列ブロック タイプ(0)																															
	文字列ブロック タイプ(続き)								文字列ブロック長																															
	文字列ブロック 長(続き)								入力 VRF 名																															
出力 VRF	文字列ブロック タイプ(0)																																							
	文字列ブロック長																																							
	出力 VRF 名																																							

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

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

フィールド	データタイプ	説明
マルウェア イベントブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 80 です。
マルウェア イベントのブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベントブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする エンドポイント向け AMP エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェア イベントの発生元 AMP クラウドの、内部の固有 ID。
マルウェア イベント タイムスタンプ	uint32	マルウェア イベント生成時のタイムスタンプ。
イベント タイプ ID	uint32	マルウェア イベント タイプの内部 ID。
イベント サブタイプ ID	uint32	マルウェア 検出につながったアクションの内部 ID。
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。
文字列ブロック タイプ	uint32	検出名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	検出名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロック タイプ	uint32	ユーザー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザー文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザー フィールドのバイト数を含む)。
ユーザー (User)	string	Cisco Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザー。これらのユーザーはユーザー ディスカバリには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイルパスを含む文字列データ ブロックを開始します。この値は常に 0 です。

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

フィールド	データタイプ	説明
文字列ブロック長	uint32	ファイルパス文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびファイルパスフィールドのバイト数を含む)。
ファイルパス	string	検出または検疫されたファイルのファイルパス。ファイル名は含まれません。
文字列ブロックタイプ	uint32	ファイル SHA ハッシュを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびファイル SHA ハッシュフィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値のレンダリングされた文字列。
ファイルサイズ (File size)	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイルタイプ	uint32	検出または検疫されたファイルのファイルタイプ。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、 エンドポイント向け AMP ファイルタイプのメタデータ (3-44 ページ) を参照してください。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ(1970年1月1日からの経過秒数)。
文字列ブロックタイプ	uint32	親ファイル名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロックタイプ	uint32	親ファイル SHA ハッシュを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、および親ファイル SHA ハッシュフィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロックタイプ	uint32	イベントの説明を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベントタイプに関連付けられている追加イベント情報。

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

フィールド	データタイプ	説明
デバイスID (Device ID)	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または IDS イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続イベント タイムスタンプ	uint32	接続イベントのタイムスタンプ。
方向 (Direction)	uint8	<p>ファイルのアップロードとダウンロードのどちらが行われたかを示します。次のいずれかの値になります。</p> <ul style="list-style-type: none"> • 1: ダウンロード • 2: アップロード <p>現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。</p>
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザー ID (User ID)	uint32	システムにより識別される、宛先ホストにログインしたユーザーの ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する ID 番号。
傾向	uint8	<p>ファイルのマルウェア ステータス。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • 1(CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE): ファイルにはマルウェアが含まれています。 • 4: UNAVAILABLE。ソフトウェアから AMP クラウドに対して、特性を確認する要求を送信できなかったか、または AMP クラウド サービスが要求に応答しなかった。 • 5(CUSTOM SIGNATURE): ファイルがユーザー定義のハッシュと一致するため、ユーザーが指定した方法で処理されました。

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

フィールド	データタイプ	説明
レトロスペクティブ 特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロック タ イプ	uint32	URI を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データ ブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
Web アプリケーショ ン ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプ リケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
操作	uint8	ファイルタイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 <ul style="list-style-type: none"> • 1:検出 • 2:ブロック • 3:マルウェア クラウドルックアップ • 4:マルウェア ブロック • 5:マルウェア許可リスト • 6:クラウドルックアップのタイムアウト • 7:カスタム検出 • 8:カスタム検出ブロック • 9:アーカイブ ブロック (深度超過) • 10:アーカイブ ブロック (暗号化されている) • 11:アーカイブ ブロック (調査エラー)
プロトコル	uint8	ユーザーが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。

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

フィールド	データタイプ	説明
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ~ 100)。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト (仮想ファイアウォール) の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバー証明書の SHA1 ハッシュ。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 <ul style="list-style-type: none"> • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

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

フィールド	データタイプ	説明
SSL フロー ステータス	uint16	<p>SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバー名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバーの証明書の処理」 • 16:「サーバー証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバー証明書の検証が使用できません」 • 27:「サーバー証明書の検証エラー」 • 28:「無効な操作」
文字列ブロック タイプ	uint32	<p>アーカイブ SHA を含む文字列データ ブロックを開始します。この値は常に 0 です。</p>

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

フィールド	データタイプ	説明
文字列ブロック長	uint32	アーカイブ SHA 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および侵入ポリシー名のバイト数を含む)。
アーカイブ SHA	string	ファイルが含まれる親アーカイブの SHA1 ハッシュ。
文字列ブロック タイプ	uint32	アーカイブ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	アーカイブ名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびアーカイブ名のバイト数を含む)。
アーカイブ名	string	親アーカイブの名前。
アーカイブ深度	uint8	ファイルがネストされている層の数。たとえば、テキスト ファイルが zip アーカイブ内にある場合、この値は 1 になります。
HTTP レスポンス	uint32	HTTP 要求の応答コード。
文字列ブロック タイプ	uint32	入力 VRF の名前を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの 8 バイト、および入力 VRF 名フィールドのバイト数が含まれています。
入力 VRF 名	文字列	トラフィックがネットワークに入るときに通過する仮想ルータ。
文字列ブロック タイプ	uint32	出力 VRF の名前を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの 8 バイト、および出力 VRF 名フィールドのバイト数が含まれています。
出力 VRF 名	文字列	トラフィックがネットワークから出るときに通過する仮想ルータの名前。

5.3 以上のファイルイベント SHA ハッシュ

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ファイルイベント SHA ハッシュのブロック タイプ (40)																															
	ファイルイベント SHA ハッシュ ブロック長																															
	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)																															
ファイル名	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイル名...																															
	傾向																ユーザー定義															

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

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

フィールド	データタイプ	説明
ファイル イベント SHA ハッシュ ブロック タイプ	uint32	ファイル イベント SHA ハッシュ ブロックを開始します。この値は常に 40 です。
ファイル イベント SHA ハッシュ ブロック長	uint32	ファイル イベント SHA ハッシュ ブロックのバイトの合計数(ファイル イベント SHA ハッシュ ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
文字列ブロック タイプ	uint32	ファイルに関連付けられている記述名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロックタイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。

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

フィールド	データタイプ	説明
ファイル名または解析結果	string	ファイルの記述名または解析結果。ファイルがクリーンである場合、この値は Clean です。ファイルの解析結果が不明の場合、この値は Neutral です。ファイルにマルウェアが含まれている場合、ファイル名が示されます。
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> • 1(CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE): ファイルにはマルウェアが含まれています。 • 4: UNAVAILABLE。ソフトウェアから AMP クラウドに対して、特性を確認する要求を送信できなかったか、または AMP クラウド サービスが要求に回答しなかった。 • 5(CUSTOM SIGNATURE): ファイルがユーザー定義のハッシュと一致するため、ユーザーが指定した方法で処理されました。
ユーザー定義	uint8	ファイル名の表示方法を示します。 <ul style="list-style-type: none"> • 0: AMP 定義 • 1: ユーザー定義

5.3 以上のファイルタイプ ID のメタデータ

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイルタイプ 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 3-48 ファイルタイプ ID のレコードフィールド

フィールド	データタイプ	説明
ファイルタイプ ID	uint32	ファイルタイプ ID 番号。このフィールドは、このレコードの固有キーです。
ファイルタイプの長さ	uint32	ファイルタイプ名に含まれるバイト数。
ファイルタイプ名	string	ファイルタイプ名の記述名。

5.2 以上のルール ドキュメントのデータ ブロック

eStreamer サービスは、ルール ドキュメントのデータ ブロックを使用して、アラートの生成に使用するルールに関する情報を表示します。ブロック タイプは、シリーズ2セットのデータ ブロックの27です。タイプ 10 のホスト要求メッセージで要求することができます。詳細については、[ホスト要求メッセージの形式\(2-30 ページ\)](#)を参照してください。

次の図に、ルール ドキュメントのデータ ブロックの構造を示します。

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

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

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

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

表 3-49 ルール ドキュメントのデータ ブロック フィールド

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

表 3-49 ルールドキュメントのデータブロックフィールド (続き)

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

表 3-49 ルールドキュメントのデータブロックフィールド (続き)

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

6.0 以上の Filelog ストレージのメタデータ

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

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ヘッダーバージョン (1)																メッセージタイプ (4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ (515)																							
	レコード長																																							
	Filelog ストレージのステータス																																							
	Filelog ストレージのステータスの説明の長さ																																							
	Filelog ストレージのステータスの説明...																																							

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

表 3-50 Filelog ストレージのメタデータのレコードフィールド

フィールド	データタイプ	説明
Filelog ストレージのステータス	uint32	filelog ストレージのステータスを示す番号。このフィールドは、このレコードの固有キーです。
Filelog ストレージのステータスの説明の長さ	uint32	Filelog ストレージのステータスの説明に含まれるバイト数。
Filelog ストレージのステータスの説明	string	filelog ストレージのステータスの記述名。

6.0 以上の Filelog サンドボックスのメタデータ

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

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ヘッダーバージョン (1)																メッセージタイプ (4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ (516)																							
	レコード長																																							
	Filelog サンドボックスのステータス																																							
	Filelog サンドボックスのステータスの説明の長さ																																							
	Filelog サンドボックスのステータスの説明...																																							

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

表 3-51 Filelog サンドボックスのメタデータのレコードフィールド

フィールド	データタイプ	説明
Filelog サンドボックスのステータス	uint32	filelog サンドボックスのステータスを示す番号。このフィールドは、このレコードの固有キーです。
Filelog サンドボックスのステータスの説明の長さ	uint32	Filelog サンドボックスのステータスの説明に含まれるバイト数。
Filelog サンドボックスのステータスの説明	string	filelog サンドボックスのステータスの記述名。

6.0 以上の Filelog Spero のメタデータ

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (517)															
	レコード長																															
	Filelog Spero のステータス																															
	Filelog Spero のステータスの説明の長さ																															
	Filelog Spero のステータスの説明...																															

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

表 3-52 Filelog Spero のメタデータのレコードフィールド

フィールド	データタイプ	説明
Filelog Spero のステータス	uint32	filelog spero のステータスを示す番号。このフィールドは、このレコードの固有キーです。
Filelog Spero のステータスの説明の長さ	uint32	Filelog Spero のステータスの説明に含まれるバイト数。
Filelog Spero のステータスの説明	string	filelog spero のステータスの記述名。

6.0 以上の Filelog アーカイブのメタデータ

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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 (518)															
	レコード長																															
	Filelog アーカイブのステータス																															
	Filelog アーカイブのステータスの説明の長さ																															
	Filelog アーカイブのステータスの説明...																															

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

表 3-53 Filelog アーカイブのメタデータのレコードフィールド

フィールド	データタイプ	説明
Filelog アーカイブのステータス	uint32	filelog アーカイブのステータスを示す番号。このフィールドは、このレコードの固有キーです。
Filelog アーカイブのステータスの説明の長さ	uint32	Filelog アーカイブのステータスの説明に含まれるバイト数。
Filelog アーカイブのステータスの説明	string	filelog アーカイブ ステータスの記述名。

6.0 以上の Filelog スタティック分析のメタデータ

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (519)															
	レコード長																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Filelog スタティック分析のステータス																																
Filelog スタティック分析のステータスの説明の長さ																																
Filelog スタティック分析のステータスの説明...																																

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

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

フィールド	データタイプ	説明
Filelog スタティック分析のステータス	uint32	filelog スタティック分析のステータスを示す番号。このフィールドは、このレコードの固有キーです。
Filelog スタティック分析のステータスの説明の長さ	uint32	Filelog スタティック分析のステータスの説明に含まれるバイト数。
Filelog スタティック分析のステータスの説明	string	filelog スタティック分析のステータスの記述名。

5.2 以上の位置情報のデータ ブロック

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

次の図に、位置情報のデータ ブロックの構造を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	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(520)																
位置情報のブロックタイプ(28)																																
位置情報のブロック長																																
国コード(Country Code)																文字列ブロックタイプ(0)																

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

次の表は、位置情報のデータブロックのフィールドについての説明です。

表 3-55 位置情報のデータブロック フィールド

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

6.0 以上のファイルポリシー名

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン (1)																メッセージタイプ (4)																
メッセージ長																																
Netmap ID																レコードタイプ (530)																
レコード長																																

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

次の表は、ファイル ポリシー名のレコードのフィールドについての説明です。

表 3-56 ファイルポリシー名フィールド

フィールド	データタイプ	説明
UUID 文字列データ ブロック タイプ	uint32	UUID 文字列データ ブロックを開始します。この値は常に 14 です。
UUID 文字列データ ブロック長	uint32	UUID 文字列データ ブロック内の総バイト数。これには、UUID 文字列データ ブロックのタイプ フィールドおよび長さフィールド用の 8 バイトと、その後のデータのバイト数が含まれます。
ファイル ポリシー UUID	uint8[16]	ファイル ポリシーの UUID。このフィールドは、このレコードの固有キーです。
文字列ブロック タイプ	uint32	ファイル ポリシー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	SSL ポリシー名の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとファイル ポリシー名のバイト数が含まれます。
ファイル ポリシー名	string	ファイル ポリシーの名前。

SSL ポリシー名

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (600)															
	レコード長																															
	UUID 文字列ブロック タイプ (14)																															
	UUID 文字列ブロック長																															
	SSL ポリシー UUID																															
	SSL ポリシー UUID (続き)																															
	SSL ポリシー UUID (続き)																															
	SSL ポリシー UUID (続き)																															
SSL ポリシー名	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	SSL ポリシー名...																															

次の表は、SSL ポリシー名のレコードのフィールドについての説明です。

表 3-57 SSL ポリシー名レコードフィールド

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

表 3-57 SSL ポリシー名レコードフィールド (続き)

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

SSL ルール ID

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (601)															
	レコード長																															
	SSL ルール ID ブロックタイプ (51)																															
	SSL ルール ID ブロック長																															
	リビジョン																															
	リビジョン (続き)																															
	リビジョン (続き)																															
	リビジョン (続き)																															
	ルール ID																															

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

次の表は、SSL ルール ID レコードのフィールドについての説明です。

表 3-58 SSL ポリシー名レコード フィールド

フィールド	データタイプ	説明
SSL ルール ID ブロックタイプ	uint32	SSL ルール ID データブロックのブロックタイプ。この値は常に 51 です。
SSL ルール ID ブロック長	uint32	SSL ルール ID データブロックのバイト数。ブロックタイプとヘッダーフィールドの 8 バイトと SSL ルール ID ブロックのバイト数が含まれます。
リビジョン	uint8[16]	SSL ルール リビジョンの UUID。このフィールドとルール ID を組み合わせると、このレコードの固有キーとなります。
ルール ID	uint32	SSL ルール ID 番号。このフィールドとリビジョンを組み合わせると、このレコードの固有キーとなります。
文字列ブロック タイプ	uint32	SSL ルールの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	SSL ルール名の文字列データ ブロックのバイト数です。ブロックタイプとヘッダー フィールドの 8 バイトと SSL ルール名のバイト数が含まれます。
SSL ルール名	string	SSL ルールの名前。

SSL 暗号スイート

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (602)															
	レコード長																															
	SSL 暗号 ID																															
	SSL 暗号スイート名の長さ																															
	SSL 暗号スイート名...																															

次の表は、SSL 暗号スイートレコードのフィールドについての説明です。

表 3-59 SSL 暗号スイート フィールド

フィールド	データタイプ	説明
SSL 暗号 ID	uint32	SSL 暗号 ID 番号。このフィールドは、このレコードの固有キーです。
SSL 暗号スイート名の長さ	uint32	SSL 暗号スイート名に含まれるバイト数。
SSL 暗号スイート名	string	SSL 暗号スイートの記述名。

SSL バージョン

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (604)															
	レコード長																															

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

次の表は、SSL バージョン レコードのフィールドについての説明です。

表 3-60 SSL バージョンフィールド

フィールド	データタイプ	説明
SSL バージョン ID	uint32	SSL バージョン ID 番号。このフィールドは、このレコードの固有キーです。
SSL バージョン名	uint32	SSL バージョン名に含まれるバイト数。
SSL 暗号スイート名	string	SSL バージョンの記述名。

SSL サーバー証明書ステータス

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン (1)																メッセージタイプ (4)																
メッセージ長																																
Netmap ID																レコードタイプ (605)																
レコード長																																
SSL サーバー証明書ステータス																																
SSL サーバー証明書ステータスの説明の長さ																																
SSL サーバー証明書ステータスの説明...																																

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

表 3-61 SSL サーバー証明書ステータス レコードフィールド

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

実際の SSL アクション

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (606)															
	レコード長																															
	実際の SSL アクションの番号																															
	実際の SSL アクションの説明の長さ																															
	実際の SSL アクションの説明...																															

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

表 3-62 実際の SSL アクションフィールド

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

表 3-62 実際の SSL アクションフィールド (続き)

フィールド	データタイプ	説明
実際の SSL アクションの説明の長さ	uint32	実際の SSL アクションの説明に含まれるバイト数。
実際の SSL アクションの説明	string	実際の SSL アクションの説明。

予期された SSL アクション

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

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

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

表 3-63 実際の SSL アクションフィールド

フィールド	データタイプ	説明
予期していた SSL アクションの番号	uint32	予期していた SSL アクションを指定する番号。このフィールドは、このレコードの固有キーです。
予期していた SSL アクションの説明の長さ	uint32	予期していた SSL アクションの説明に含まれるバイト数。
予期していた SSL アクションの説明	string	予期していた SSL アクションの説明。

SSL フロー ステータス

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

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

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

表 3-64 SSL フロー ステータス フィールド

フィールド	データタイプ	説明
SSL フロー ステータス番号	uint32	SSL フロー ステータスを指定する番号。このフィールドは、このレコードの固有キーです。
SSL フロー ステータスの説明の長さ	uint32	SSL フロー ステータスの説明に含まれるバイト数。
SSL フロー ステータスの説明	string	SSL フロー ステータスの説明。

SSL URL カテゴリ

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (613)															
	レコード長																															
	SSL URL カテゴリ番号																															
	SSL URL カテゴリの説明の長さ																															
	SSL URL カテゴリの説明...																															

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

表 3-65 SSL URL カテゴリ フィールド

フィールド	データタイプ	説明
SSL URL カテゴリ番号	uint32	SSLURLカテゴリを指定する番号。このフィールドは、このレコードの固有キーです。
SSL URL カテゴリの説明の長さ	uint32	SSLサーバーURLカテゴリの説明に含まれるバイト数。
SSL URL カテゴリの説明	string	SSL URL カテゴリの説明。

5.4 以上の SSL 証明書の詳細のデータブロック

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

次の図に、SSL 証明書の詳細のデータブロックの構造を示します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (614)															
	レコード長																															

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
ビット																																	
	SSL 証明書の詳細のデータブロック タイプ (50)																																
	SSL 証明書の詳細のブロック長																																
	フィンガープリント SHA ハッシュ																																
	フィンガープリント SHA ハッシュ (続き)																																
	フィンガープリント SHA ハッシュ (続き)																																
	フィンガープリント SHA ハッシュ (続き)																																
	フィンガープリント SHA ハッシュ (続き)																																
	公開キーの SHA ハッシュ																																
	公開キーの SHA ハッシュ (続き)																																
	公開キーの SHA ハッシュ (続き)																																
	公開キーの SHA ハッシュ (続き)																																
	公開キーの SHA ハッシュ (続き)																																
	シリアル番号 (Serial Number)																																
	シリアル番号 (続き)																																
	シリアル番号 (続き)																																
	シリアル番号 (続き)																																
	シリアル番号 (続き)																																
	シリアル番号の長さ																																
サブジェク トの共通名	文字列ブロック タイプ (0)																																
	文字列ブロック長																																
	サブジェクトの共通名...																																
サブジェク ト組織	文字列ブロック タイプ (0)																																
	文字列ブロック長																																
	サブジェクト組織...																																

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
サブジェクトの組織単位	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	サブジェクトの組織単位....																															
サブジェクトの国	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	サブジェクトの国...																															
発行元の共通名	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	発行元の共通名...																															
発行者組織	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	発行者組織...																															
発行者の組織単位	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	発行者の組織単位...																															
発行者の国	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	発行者の国...																															
	有効な開始日																															
	有効な終了日																															

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

表 3-66 SSL 証明書の詳細のデータ ブロック フィールド

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

表 3-66 SSL 証明書の詳細のデータブロック フィールド (続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	名前の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの8バイトとイベントタイプフィールドのバイト数が含まれます。
サブジェクトの国	string	証明書のサブジェクトの国。
文字列ブロックタイプ	uint32	侵害に関連付けられたカテゴリを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの8バイトとカテゴリフィールドのバイト数が含まれます。
発行元の共通名	string	SSL 証明書の発行者の共通名。これは通常、証明書の発行者のホストとドメイン名ですが、他の情報が含まれていることもあります。
文字列ブロックタイプ	uint32	侵害に関連付けられたイベントタイプを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの8バイトとイベントタイプフィールドのバイト数が含まれます。
発行者組織	string	証明書の発行者の組織。
文字列ブロックタイプ	uint32	侵害に関連付けられたイベントタイプを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの8バイトとイベントタイプフィールドのバイト数が含まれます。
発行者の組織単位	string	証明書の発行者の組織単位。
文字列ブロックタイプ	uint32	侵害に関連付けられたイベントタイプを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの8バイトとイベントタイプフィールドのバイト数が含まれます。
発行者の国	string	証明書の発行者の国。
有効な開始日	uint32	証明書が発行された時刻の Unix タイムスタンプ。
有効な終了日	uint32	証明書が有効でなくなる時刻の Unix タイムスタンプ。

ネットワーク分析ポリシーレコード

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

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ヘッダーバージョン (1)																メッセージタイプ (4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ (700)																							
	レコード長																																							
	UUID 文字列ブロック タイプ (14)																																							
	UUID 文字列ブロック長																																							
	ネットワーク分析ポリシー UUID																																							
	ネットワーク分析 UUID (続き)																																							
	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 3-67 ネットワーク分析ポリシー名レコードフィールド

フィールド	データタイプ	説明
UUID 文字列データ ブロック タイプ	uint32	UUID 文字列データ ブロックを開始します。この値は常に 14 です。
UUID 文字列データ ブロック長	uint32	UUID 文字列データ ブロック内の総バイト数。これには、UUID 文字列データ ブロックのタイプ フィールドおよび長さフィールド用の 8 バイトと、その後のデータのバイト数が含まれます。
ネットワーク分析ポリシー UUID	uint8[16]	ネットワーク分析ポリシーの UUID。このフィールドは、このレコードの固有キーです。
文字列ブロック タイプ	uint32	ネットワーク分析ポリシーの名前を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 3-67 ネットワーク分析ポリシー名レコードフィールド (続き)

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

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。