CHAPTER 4

検出と接続データ構造の概要

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

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

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

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

eStreamer サーバーからのディスカバリ イベントまたは接続イベントの要求については、要求フラグ（2-15 ページ）を参照してください。

eStreamer イベント データ構造メッセージの一般的構造については、イベント データ メッセージの構成について（2-21 ページ）を参照してください。

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

- ディスカバリ イベントと接続イベントのデータ メッセージ（4-2 ページ）では、eStreamer がホスト ディスカバリ メッセージ、ユーザー メッセージ、接続メッセージに使用する構造の概要を紹介します。
- ディスカバリ イベントと接続イベントのレコード タイプ（4-2 ページ）では、ディスカバリ イベントと接続イベント レコード タイプについて説明します。
- ディスカバリ イベントのメタデータ（4-8 ページ）では、たとえば、イベント内のユーザー ID をユーザー名に変換するなど、数字データとコード化データをテキストに変換するためのコンテキスト情報を要求できるメタデータ レコードについて説明します。
- ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）では、すべてのディスカバリ メッセージと接続メッセージで使用する標準イベント ヘッダーの構造と、イベント タイプ フィールドとイベント サブタイプ フィールドで発生する値について説明します。さらに、イベント タイプ フィールドとサブタイプ フィールドは、メッセージで伝えるデータ レコードの構造を定義します。

- イベント タイプ別ホスト ディスカバリ構造（4-46 ページ）では、eStreamer が各種ホスト ディスカバリ イベント タイプに使用するデータ レコードの構造について説明します。
- イベント タイプ別のユーザー データ構造（4-63 ページ）では、eStreamer が各種ユーザー イベント タイプに使用するデータ レコードの構造について説明します。
- ディスカバリ（シリーズ1）ブロック（4-65 ページ）では、ディスカバリ イベント メッセージと接続イベント メッセージで複雑なレコードを伝えるために使用する一連のデータ ブロック構造について説明します。シリーズ 1 のデータ ブロックは、相関イベントでも使用します。
- ユーザー脆弱性データ ブロック 5.0+（4-169 ページ）では、複雑なユーザー イベント レコードを伝えるために使用するその他の シリーズ 1 ブロック構造について説明します。

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

ディスカバリ イベントと接続イベントのデータ メッセージ

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

- オプションの netmap ID
- レコード タイプを定義するレコード ヘッダー
- イベントを識別し、その特性を表すディスカバリ イベント ヘッダー。具体的にはイベント タイプとサブタイプを識別します。詳細については、ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照してください。
- ブロック ヘッダーとデータ ブロックからなるデータ レコード。ディスカバリ イベントと接続イベントのデータ メッセージは、シリーズ 1 のデータ ブロックを使用します。詳細については、ホスト ディスカバリ データ ブロックと接続データ ブロック（4-66 ページ）またはユーザー脆弱性データ ブロック 5.0+（4-169 ページ）を参照してください。

ディスカバリ イベントと接続イベントのレコード タイプ

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

表 4-1　ディスカバリ イベントと接続イベントのレコード タイプ

レコード タイプ	含まれるブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
10	139	1	新規ホストを検出	現在（Current）	新規ホスト メッセージと最後の確認日時ホスト メッセージ(4-47 ページ)
11	103	1	新規 TCP サーバー	現在（Current）	サーバー メッセージ(4-48 ページ)
12	103	1	新規 UDP サーバー	現在（Current）	サーバー メッセージ(4-48 ページ)
13	4	1	新規ネットワーク プロトコル	現在（Current）	新規ネットワーク プロトコル メッセージ(4-49 ページ)
14	4	1	新規トランスポート プロトコル	現在（Current）	新規トランスポート プロトコル メッセージ(4-49 ページ)
15	122	1	新規クライアント アプリケーション	現在（Current）	クライアント アプリケーション メッセージ(4-50 ページ)
16	103	1	TCP サーバー情報更新	現在（Current）	サーバー メッセージ(4-48 ページ)
17	103	1	UDP サーバー情報更新	現在（Current）	サーバー メッセージ(4-48 ページ)
18	53	1	OS 情報の更新	現在（Current）	オペレーティング システム更新メッセージ(4-51 ページ)
19	該当なし	該当なし	ホスト タイムアウト	現在（Current）	IP アドレスを再利用とホスト タイムアウト/削除メッセージ(4-52 ページ)
20	該当なし	該当なし	ホスト IP アドレスを再利用	現在（Current）	IP アドレスを再利用とホスト タイムアウト/削除メッセージ(4-52 ページ)
21	該当なし	該当なし	ホストを削除。ホスト上限に到達	現在（Current）	IP アドレスを再利用とホスト タイムアウト/削除メッセージ(4-52 ページ)
22	該当なし	該当なし	ホップ数の変更	現在（Current）	ホップ変更メッセージ(4-52 ページ)
23	該当なし	該当なし	TCP ポート クローズ	現在（Current）	TCP と UDP のポート クローズ メッセージ/タイムアウト メッセージ(4-52 ページ)
24	該当なし	該当なし	UDP ポート クローズ	現在（Current）	TCP と UDP のポート クローズ メッセージ/タイムアウト メッセージ(4-52 ページ)
25	該当なし	該当なし	TCP ポート タイムアウト	現在（Current）	TCP と UDP のポート クローズ メッセージ/タイムアウト メッセージ(4-52 ページ)
26	該当なし	該当なし	UDP ポート タイムアウト	現在（Current）	TCP と UDP のポート クローズ メッセージ/タイムアウト メッセージ(4-52 ページ)
27	該当なし	該当なし	MAC 情報の変更	現在（Current）	MAC アドレス メッセージ(4-53 ページ)

表 4-1　ディスカバリ イベントと接続イベントのレコード タイプ（続き）

レコード タイプ	含まれるブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
36	該当なし	該当なし	ホストの追加 MAC を検出	現在（Current）	MAC アドレス メッセージ(4-53 ページ)
29	該当なし	該当なし	ホスト IP アドレスを変更	現在（Current）	IP アドレス変更メッセージ(4-50 ページ)
31	該当なし	該当なし	ルータ/ブリッジとして識別したホスト	現在（Current）	ブリッジ/ルータとして識別したホスト メッセージ(4-53 ページ)
34	18	1	VLAN タグ情報更新	現在（Current）	VLAN タグ情報更新メッセージ(4-54 ページ)
35	122	1	クライアント アプリケーション タイムアウト	現在（Current）	クライアント アプリケーション メッセージ(4-50 ページ)
54	35	1	NetBIOS 名変更	現在（Current）	NetBIOS 名変更メッセージ(4-54 ページ)
44	該当なし	該当なし	ホストをドロップ。ホスト上限に到達	現在（Current）	IP アドレスを再利用とホスト タイムアウト/削除メッセージ(4-52 ページ)
45	37	1	更新バナー	現在（Current）	更新バナー メッセージ(4-55 ページ)
46	55	1	ホスト属性を追加	現在（Current）	属性メッセージ(4-59 ページ)
47	55	1	ホスト属性を更新	現在（Current）	属性メッセージ(4-59 ページ)
48	55	1	ホスト属性を削除	現在（Current）	属性メッセージ(4-59 ページ)
51	103	1	TCP サーバー信頼度更新	レガシー	サーバー メッセージ(4-48 ページ)
52	103	1	UDP サーバー信頼度更新	レガシー	サーバー メッセージ(4-48 ページ)
53	53	1	OS 信頼度更新	レガシー	オペレーティング システム更新メッセージ(4-51 ページ)
54	該当なし	該当なし	フィンガープリント メタデータ	現在（Current）	フィンガープリント レコード(4-9 ページ)
55	該当なし	該当なし	クライアント アプリケーション メタデータ	現在（Current）	クライアント アプリケーション レコード(4-10 ページ)
57	該当なし	該当なし	脆弱性メタデータ	現在（Current）	脆弱性レコード(4-11 ページ)
58	該当なし	該当なし	重要度メタデータ	現在（Current）	重要度レコード(4-13 ページ)
59	該当なし	該当なし	ネットワーク プロトコル メタデータ	現在（Current）	ネットワーク プロトコル レコード(4-14 ページ)
60	該当なし	該当なし	属性メタデータ	現在（Current）	属性レコード(4-15 ページ)

表 4-1　ディスカバリ イベントと接続イベントのレコード タイプ（続き）

レコード タイプ	含まれるブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
61	該当なし	該当なし	スキャン タイプ メタデータ	現在（Current）	スキャン タイプ レコード（4-16 ページ）
63	該当なし	該当なし	サーバー メタデータ	現在（Current）	サービス レコード（4-16 ページ）
71	144	1	接続統計情報	レガシー	接続統計データ ブロック 5.2.x（B-179 ページ）
71	152	1	接続統計情報	レガシー	接続統計データ ブロック 5.3（B-195 ページ）
71	154	1	接続統計情報	レガシー	接続統計データ ブロック 5.3.1（B-202 ページ）
71	155	1	接続統計情報	レガシー	接続統計データ ブロック 5.4（B-210 ページ）
71	157	1	接続統計情報	レガシー	接続統計データ ブロック 5.4.1（B-224 ページ）
71	160	1	接続統計情報	レガシー	接続統計データ ブロック 6.0.x（B-239 ページ）
71	163	1	接続統計情報	レガシー	接続統計データブロック 6.2 ～ 6.7.x（B-274 ページ）
71	173	1	接続統計情報	レガシー	接続統計データ ブロック 7.0（B-292 ページ）
71	174	1	接続統計情報	現在（Current）	接続統計データ ブロック 7.1+（4-125 ページ）
73	136	1	接続チャンク	現在（Current）	接続チャンク メッセージ（4-56 ページ）
74	該当なし	該当なし	ユーザー設定 OS	現在（Current）	ユーザー サーバー メッセージとオペレーティング システム メッセージ（4-60 ページ）
75	該当なし	該当なし	ユーザー設定サーバー	現在（Current）	ユーザー サーバー メッセージとオペレーティング システム メッセージ（4-60 ページ）
76	83	1	ユーザー削除プロトコル	現在（Current）	ユーザー プロトコル メッセージ（4-60 ページ）
77	60	1	ユーザー削除クライアント アプリケーション	現在（Current）	ユーザー クライアント アプリケーション メッセージ（4-61 ページ）
78	78	1	ユーザー削除アドレス	現在（Current）	ユーザー追加/削除ホスト メッセージ（4-57 ページ）
79	77	1	ユーザー削除サーバー	現在（Current）	ユーザー削除サーバー メッセージ（4-58 ページ）
80	80	1	ユーザー設定の有効な脆弱性	現在（Current）	バージョン4.6.1+ のユーザー設定脆弱性メッセージ（4-57 ページ）

表 4-1　ディスカバリ イベントと接続イベントのレコード タイプ（続き）

レコード タイプ	含まれるブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
81	80	1	ユーザー設定の無効な脆弱性	現在（Current）	バージョン4.6.1+ のユーザー設定脆弱性メッセージ(4-57 ページ)
82	81	1	ユーザー設定ホスト重要度	現在（Current）	ユーザー設定ホスト重要度メッセージ(4-58 ページ)
83	55	1	ユーザー設定属性値	現在（Current）	属性値メッセージ(4-59 ページ)
84	82	1	ユーザー削除属性値	現在（Current）	属性値メッセージ(4-59 ページ)
85	78	1	ユーザー追加ホスト	現在（Current）	ユーザー追加/削除ホスト メッセージ(4-57 ページ)
86	該当なし	該当なし	ユーザー追加サーバー	現在（Current）	ユーザー サーバー メッセージとオペレーティング システム メッセージ(4-60 ページ)
87	60	1	ユーザー追加クライアント アプリケーション	現在（Current）	ユーザー クライアント アプリケーション メッセージ(4-61 ページ)
88	83	1	ユーザー追加プロトコル	現在（Current）	ユーザー プロトコル メッセージ(4-60 ページ)
89	142	1	ユーザー追加スキャン結果	現在（Current）	スキャン結果を追加メッセージ(4-61 ページ)
90	該当なし	該当なし	ソース タイプ レコード	現在（Current）	ソース タイプ レコード(4-17 ページ)
91	該当なし	該当なし	ソース アプリケーション レコード	現在（Current）	ソース アプリケーション レコード(4-18 ページ)
92	120	1	ユーザー ドロップ変更イベント	現在（Current）	ユーザー変更メッセージ(4-64 ページ)
93	120	1	ユーザー削除変更イベント	現在（Current）	ユーザー変更メッセージ(4-64 ページ)
94	120	1	新規ユーザー識別イベント	現在（Current）	ユーザー変更メッセージ(4-64 ページ)
95	121	1	ユーザー ログイン変更イベント	現在（Current）	ユーザー情報更新メッセージ ブロック(4-64 ページ)
96	該当なし	該当なし	ソース ディテクタ レコード	現在（Current）	ソースディテクタ レコード(4-19 ページ)
98	57	2	ユーザー レコード	現在（Current）	ユーザー レコード(4-21 ページ)
101	該当なし	該当なし	新規 OS イベント	現在（Current）	新規オペレーティング システム メッセージ(4-62 ページ)
102	94	1	アイデンティティ競合イベント	現在（Current）	アイデンティティ競合とアイデンティティ タイムアウト システム メッセージ(4-62 ページ)

表 4-1　ディスカバリ イベントと接続イベントのレコード タイプ（続き）

レコード タイプ	含まれるブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
103	94	1	アイデンティティ タイムアウト イベント	現在（Current）	アイデンティティ競合とアイデンティティ タイムアウト システム メッセージ（4-62 ページ）
106	該当なし	該当なし	サードパーティ スキャナ脆弱性レコード	現在（Current）	サードパーティ スキャナの脆弱性レコード（4-20 ページ）
107	122	1	クライアント アプリケーション更新	現在（Current）	クライアント アプリケーション メッセージ（4-50 ページ）
109	該当なし	該当なし	Web アプリケーション レコード	現在（Current）	Web アプリケーション レコード（4-22 ページ）
114	121	1	失敗したユーザーのログイン イベント	現在（Current）	ユーザー情報更新メッセージ ブロック（4-64 ページ）
115	該当なし	該当なし	セキュリティ ゾーン名レコード	現在（Current）	セキュリティ ゾーン名レコード（3-31 ページ）
116	14	2	インターフェイス名レコード	現在（Current）	インターフェイス名レコード（3-32 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（3-33 ページ）
118	14	2	侵入ポリシー名レコード	現在（Current）	侵入ポリシー名レコード（4-23 ページ）
119	14	2	アクセス コントロール ルール ID レコード	現在（Current）	アクセス コントロール ルール ID レコードのメタデータ（3-35 ページ）
120	該当なし	該当なし	アクセス コントロール ルール アクション レコード	現在（Current）	アクセス コントロール ルール アクション レコード メタデータ（4-25 ページ）
121	該当なし	該当なし	URL カテゴリ統計	現在（Current）	URL カテゴリ レコード メタデータ（4-26 ページ）
122	該当なし	該当なし	URL レピュテーション メタデータ	現在（Current）	URL レピュテーション レコード メタデータ（4-27 ページ）
124	21	2	アクセス コントロール ルール理由メタデータ	現在（Current）	アクセス コントロール ルール理由メタデータ（4-28 ページ）
145	64	2	アクセス コントロール ポリシー メタデータ	現在（Current）	アクセス コントロール ポリシー メタデータ（4-29 ページ）
146	64	2	プレフィルタ ポリシー メタデータ	現在（Current）	プレフィルタ ポリシー メタデータ（4-31 ページ）
147	21	2	トンネルまたはプレフィルタ ルール メタデータ	現在（Current）	トンネルまたはプレフィルタのルールのメタデータ（4-33 ページ）
160	7	1	ホスト IOC セット メッセージ	現在（Current）	ホスト IOC セット メッセージ（4-63 ページ）
161	39	2	5.3+ の IOC 名データ ブロック	現在（Current）	5.3+ の IOC 名データ ブロック（4-38 ページ）

表 4-1　ディスカバリ イベントと接続イベントのレコード タイプ（続き）

レコード タイプ	含まれるブロック タイプ	シリーズ	説明	レコード ステータス	データ形式の参照先...
162	148	1	ユーザー ホスト IOC の削除	Current	ユーザー IOC の変更データ ブロック 5.3+（4-85 ページ）
163	148	1	ユーザー ホスト IOC の有効化	Current	ユーザー IOC の変更データ ブロック 5.3+（4-85 ページ）
164	148	1	ユーザー ホスト IOC の無効化	Current	ユーザー IOC の変更データ ブロック 5.3+（4-85 ページ）
170	95	1	VPN ユーザーのログイン イベント	Current	ユーザー情報更新メッセージ ブロック（4-64 ページ）
171	95	1	VPN ユーザーのログオフ イベント	現在（Current）	ユーザー情報更新メッセージ ブロック（4-64 ページ）
280	22	2	セキュリティ インテリジェンス カテゴリ メタデータ	現在（Current）	セキュリティ インテリジェンス カテゴリ メタデータ（4-34 ページ）
281	該当なし	該当なし	セキュリティ インテリジェンス送信元/宛先レコード	現在（Current）	セキュリティ インテリジェンス送信元/宛先レコード（4-35 ページ）

ディスカバリ イベントのメタデータ

メタデータ バージョン番号でメタデータを要求します。Cisco Secure Firewall システム のバージョンに対応するメタデータ バージョンについては、メタデータについて（2-47 ページ）を参照してください。eStreamer によるメタデータ レコードのストリーミング方法の重要な情報については、メタデータの伝送（2-47 ページ）を参照してください。

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

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

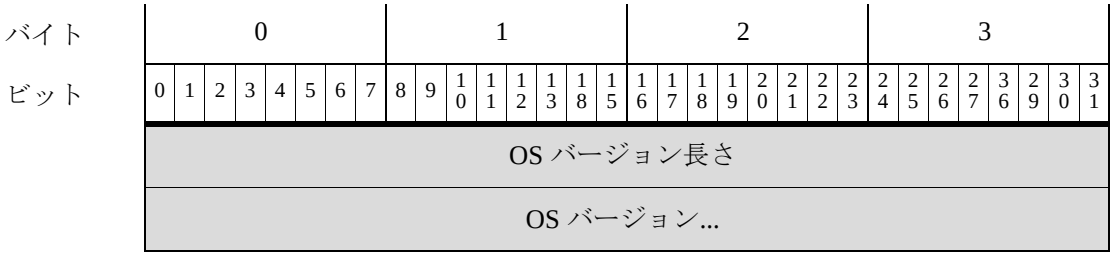
- Web アプリケーション レコード（4-22 ページ）
- 侵入ポリシー名レコード（4-23 ページ）
- アクセス コントロール ルール アクション レコード メタデータ（4-25 ページ）
- URL カテゴリ レコード メタデータ（4-26 ページ）
- URL レピュテーション レコード メタデータ（4-27 ページ）
- アクセス コントロール ルール理由メタデータ（4-28 ページ）
- セキュリティ インテリジェンス カテゴリ メタデータ（4-34 ページ）
- セキュリティ インテリジェンス送信元/宛先レコード（4-35 ページ）

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

フィンガープリント レコード

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ヘッダー バージョン（1）																メッセージ タイプ（4）															
	メッセージ長																															
	Netmap ID																レコード タイプ（54）															
	レコード長																															
フィンガープリント UUID	フィンガープリント UUID																															
	フィンガープリント UUID（続き）																															
	フィンガープリント UUID（続き）																															
	フィンガープリント UUID（続き）																															
	OS 名長さ																															
	OS 名...																															
	OS ベンダー長さ																															
	OS ベンダー...																															



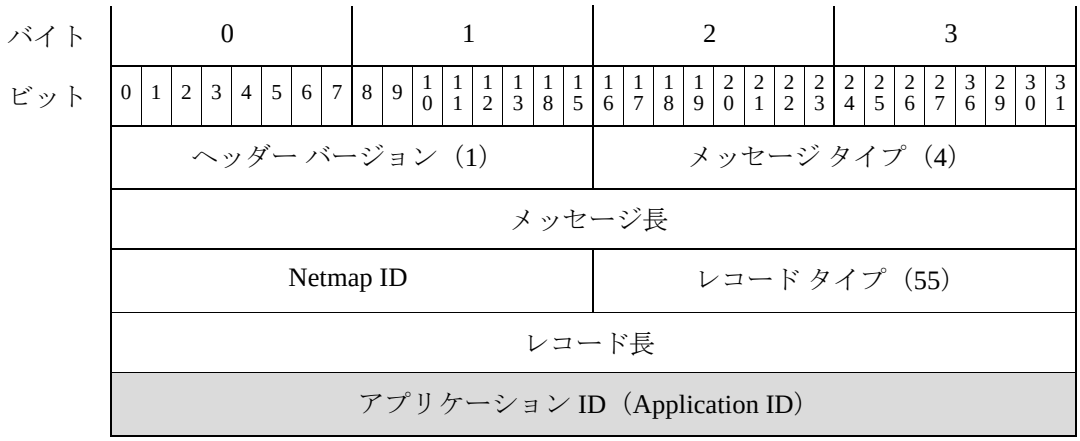
次の表では、フィンガープリント レコードのフィールドについて説明します。

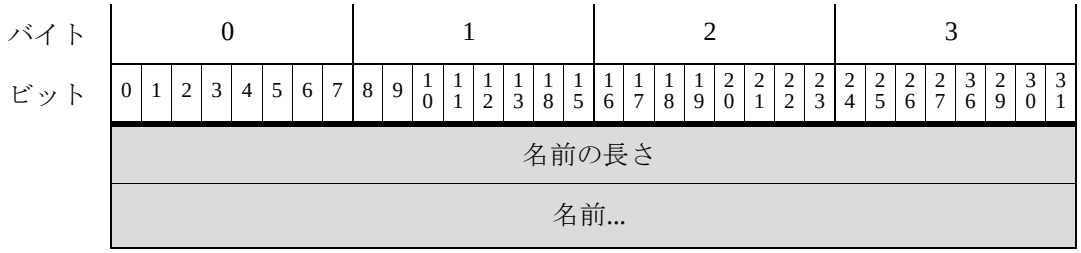
表 4-2　　フィンガープリント レコードのフィールド

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

クライアント アプリケーション レコード

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





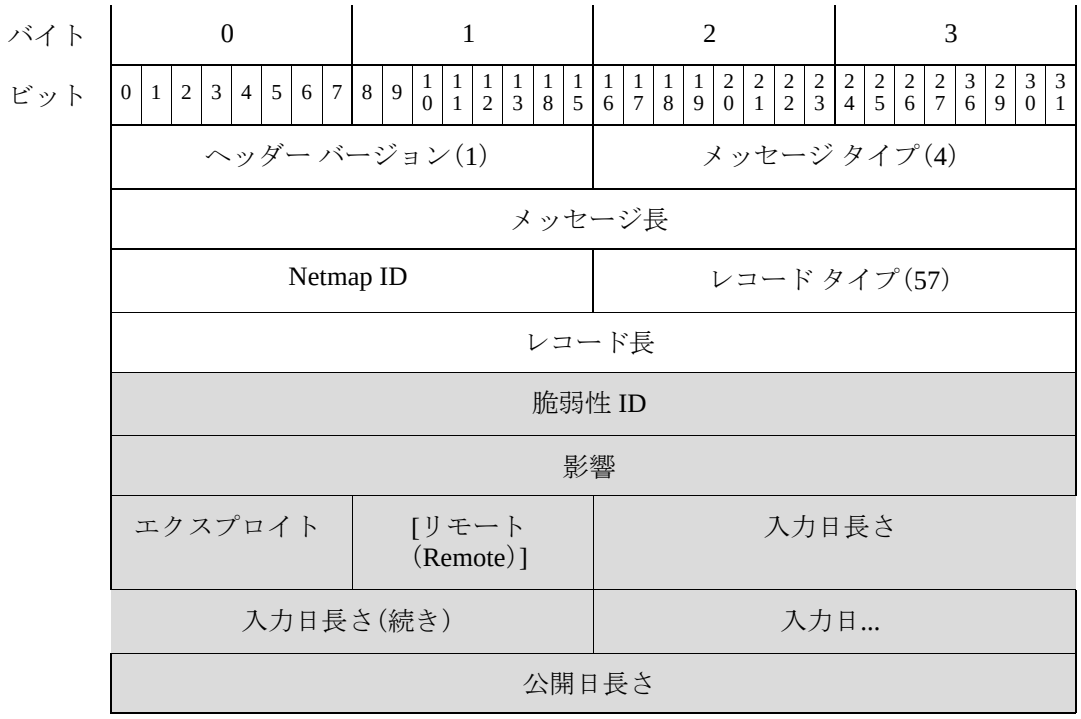
次の表では、クライアント アプリケーション レコードのフィールドについて説明します。

表 4-3　クライアント アプリケーション レコードのフィールド

フィールド	データタイプ	説明
アプリケーション ID（Application ID）	uint32	クライアント アプリケーションのアプリケーション ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	名前に含まれるバイト数。
[名前（Name）]	string	クライアント アプリケーション名。

脆弱性レコード

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



次の表では、脆弱性レコードのフィールドについて説明します。

表 4-4　　脆弱性レコードのフィールド

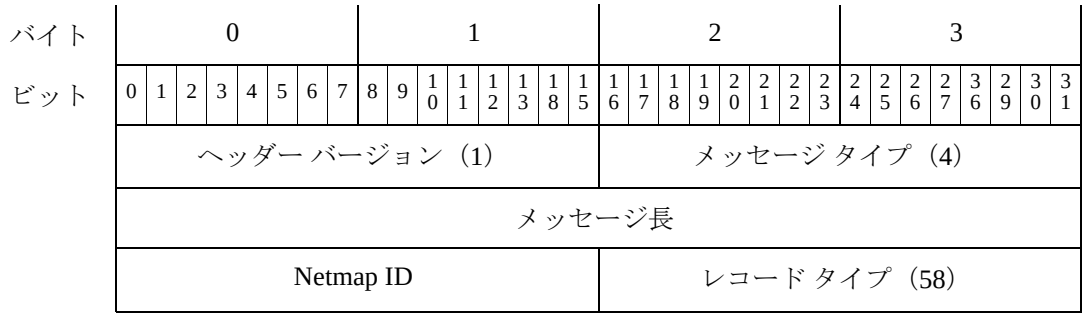
フィールド	データタイプ	説明
脆弱性 ID	uint32	脆弱性 ID 番号このフィールドは、このレコードの固有キーです。
影響	uint32	侵入データ、ホスト ディスカバリ イベント、脆弱性アセスメント間の相関に基づいて決定した影響レベルに対応した、脆弱性の影響。ここに設定可能な値の範囲は 1 ～ 10 です。最も深刻な場合で 10 です。脆弱性の影響度の値は、Bugtraq エントリの作成者が設定します。
エクスプロイト	uint8	脆弱性に既知のエクスプロイトがあるかどうかを示します。有効な値は次のとおりです。 • 0:はい • 1:いいえ

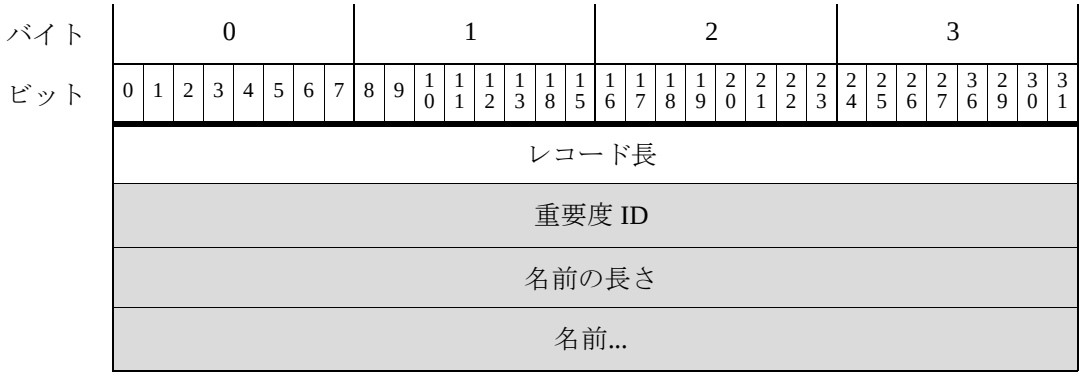
表 4-4　脆弱性レコードのフィールド（続き）

フィールド	データタイプ	説明
[リモート(Remote)]	uint8	ネットワーク上でつけ込まれる余地が脆弱性にあるかどうかを示します。有効な値は次のとおりです。 • 0:はい • 1:いいえ • 空白 — 不明なリモート エクスプロイトに対する脆弱性
入力日長さ	uint32	入力日付フィールド長さ。
入力日	string	脆弱性がデータベースに登録された日付。
公開日長さ	uint32	公開された日付フィールド長さ。
公開日	string	脆弱性が公開された日付。
変更日長さ	uint32	変更された日付フィールド長さ。
変更日	string	脆弱性の最終変更日(該当する場合)。
タイトル長さ	uint32	タイトル フィールド長さ。
役職(Title)	string	脆弱性のタイトル。
概略説明長さ	uint32	概略説明フィールド長さ。
概略説明(Short Description)	string	脆弱性の概略説明。
説明の長さ	uint32	説明フィールドの長さ。
説明	string	脆弱性に関する一般的な説明。
技術的説明の長さ	uint32	技術的説明フィールド長さ。
技術的説明	string	脆弱性に関する技術的説明。
ソリューション長さ	uint32	ソリューション フィールド長さ。
ソリューション	string	脆弱性に対するソリューション。

重要度レコード

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





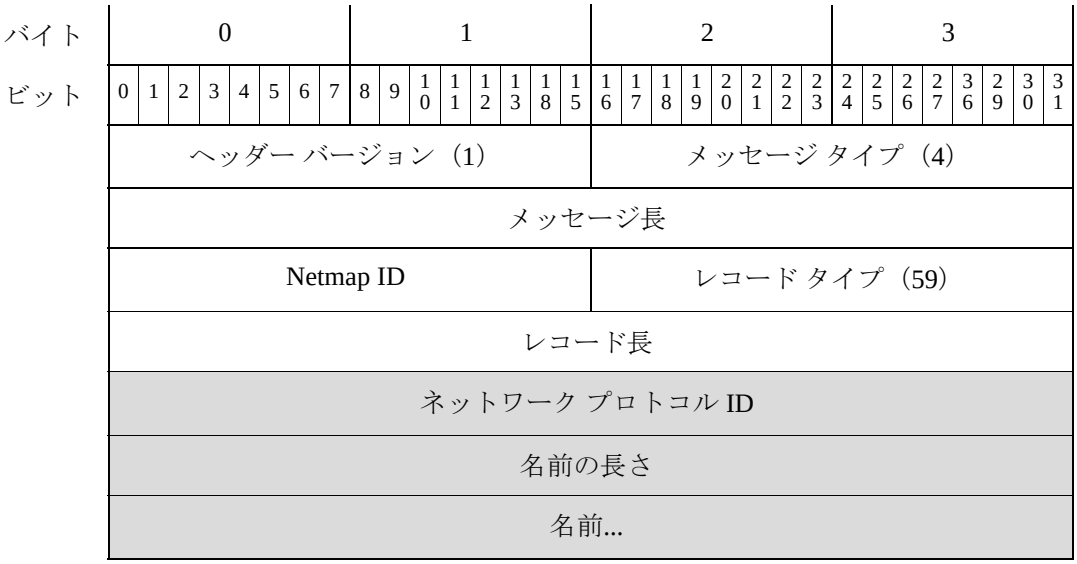
次の表では、重要度レコードのフィールドについて説明します。

表 4-5　　重要度レコードのフィールド

フィールド	データタイプ	説明
重要度 ID	uint32	重要度 ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	重要度レベルのバイト数。
[名前（Name）]	string	重要度レベル。

ネットワーク プロトコル レコード

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



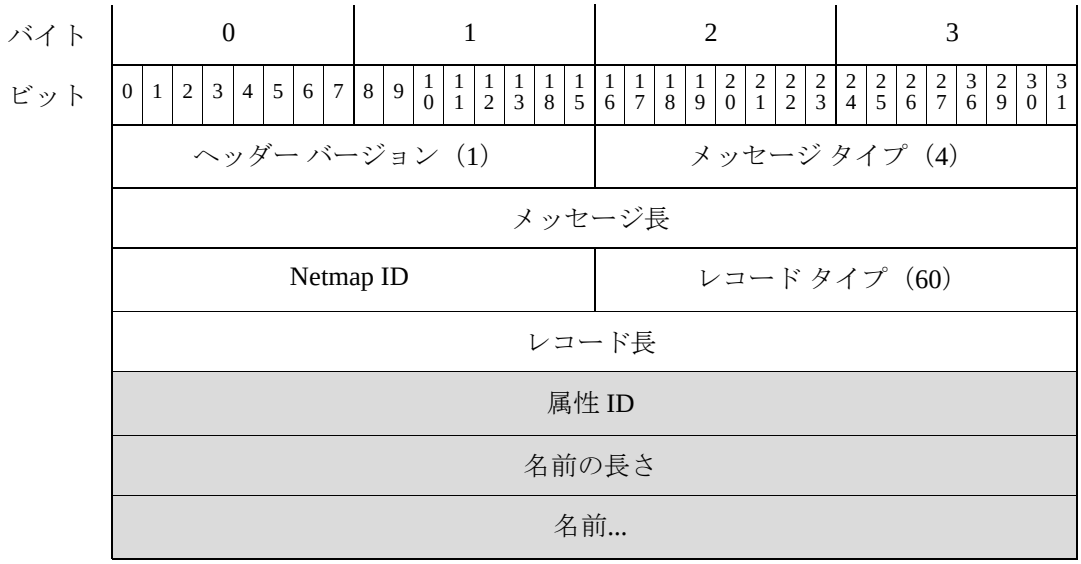
次の表では、ネットワーク プロトコル レコードのフィールドについて解説します。

表 4-6　ネットワーク プロトコル レコードのフィールド

フィールド	データタイプ	説明
ネットワーク プロトコル ID	uint32	ネットワーク プロトコル ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	ネットワーク プロトコル名のバイト数。
[名前(Name)]	string	ネットワーク プロトコル名。

属性レコード

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



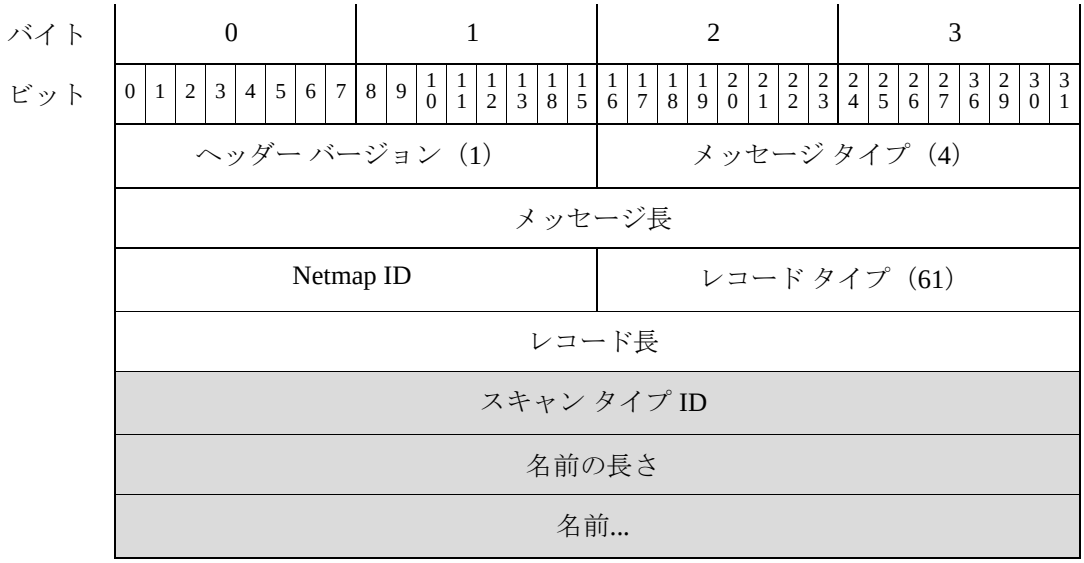
次の表では、属性レコードのフィールドについて説明します。

表 4-7　属性レコードのフィールド

フィールド	データタイプ	説明
Attribute ID	uint32	属性 ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	属性名のバイト数。
[名前(Name)]	string	属性の名前。

スキャン タイプ レコード

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



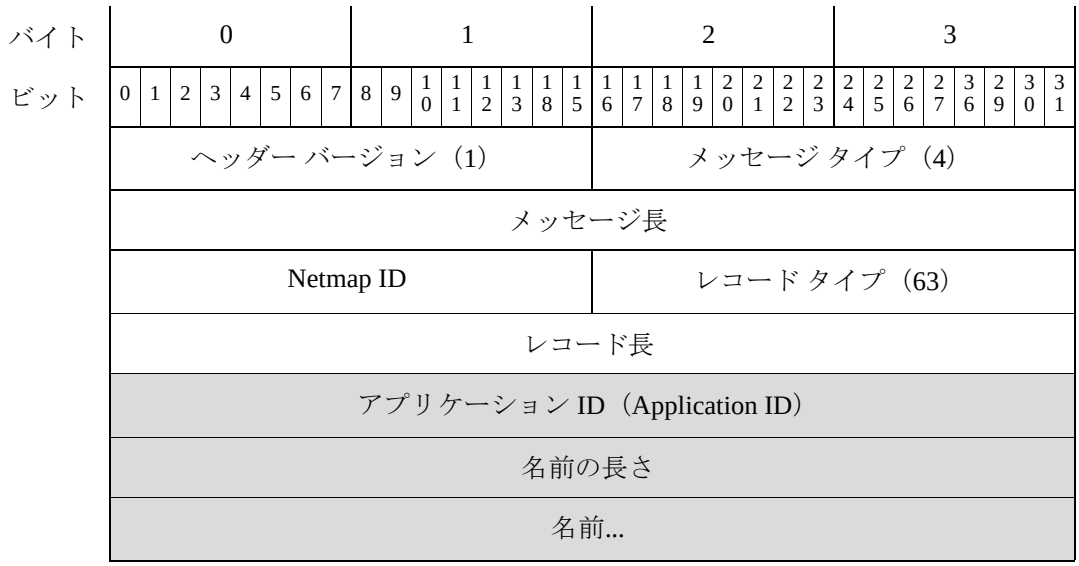
次の表では、スキャン タイプ レコードのフィールドについて説明します。

表 4-8　　スキャン タイプ レコードのフィールド

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

サービス レコード

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



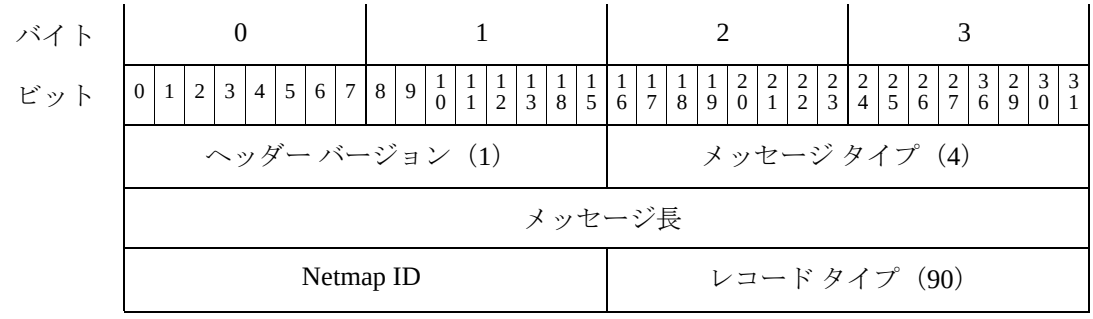
次の表では、サービス レコードのフィールドについて説明します。

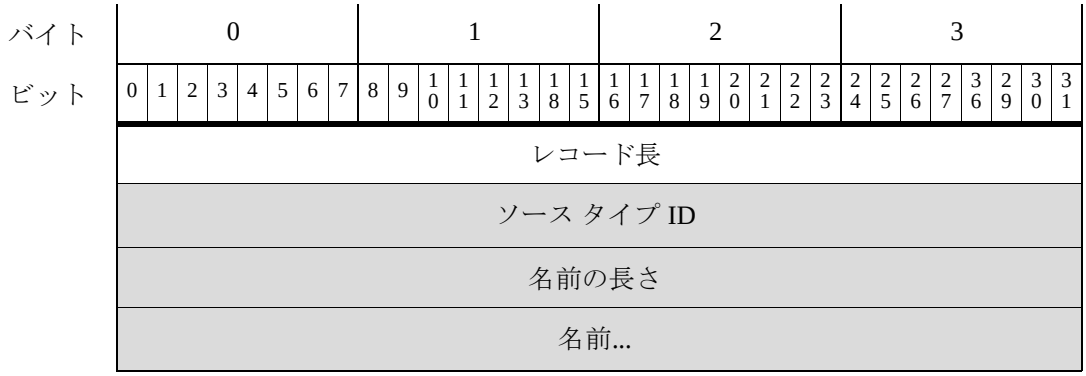
表 4-9　　サービス レコードのフィールド

フィールド	データタイプ	説明
アプリケーション ID（Application ID）	uint32	アプリケーション プロトコルのアプリケーション ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	サービス名に含まれるバイト数。
[名前（Name）]	string	アプリケーション プロトコル名アプリケーション ID 65535 の場合、名前は unknown です。

ソース タイプ レコード

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





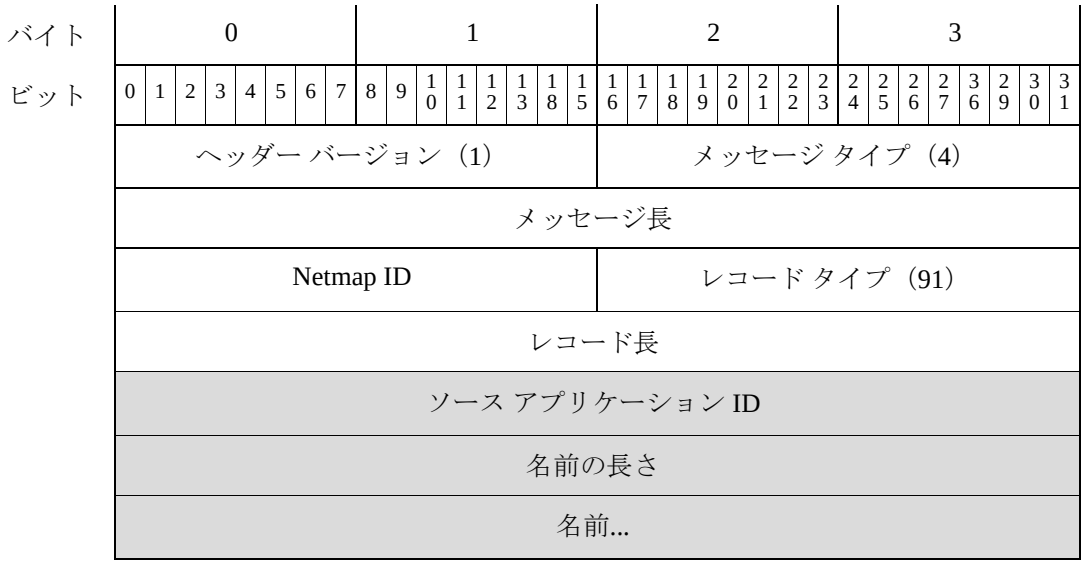
次の表では、ソース タイプ レコードのフィールドについて説明します。

表 4-10　　ソース タイプ レコードのフィールド

フィールド	データタイプ	説明
ソース タイプ ID	uint32	ソース タイプの ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	送信元タイプ名のバイト数。
[名前（Name）]	string	ソース タイプ名。

ソース アプリケーション レコード

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



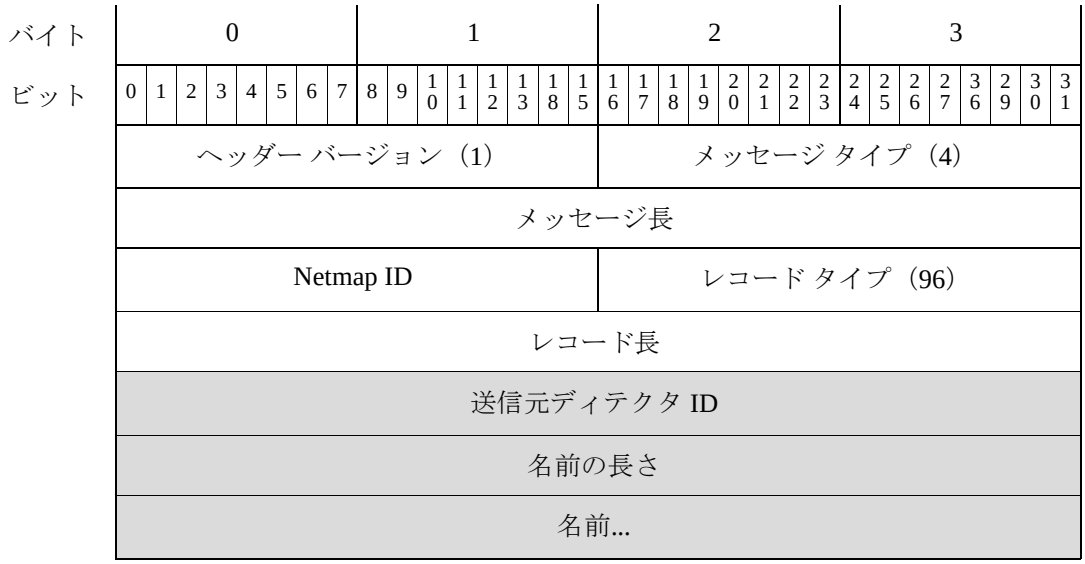
次の表では、ソース アプリケーション レコードのフィールドについて説明します。

表 4-11　送信元アプリケーション レコードのフィールド

フィールド	データタイプ	説明
ソース アプリケーション ID	uint32	送信元アプリケーションの ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	送信元アプリケーション名のバイト数。
[名前(Name)]	string	送信元アプリケーションの名前。

ソースディテクタ レコード

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



次の表では、送信元ディテクタ レコードのフィールドについて説明します。

表 4-12　送信元ディテクタ レコードのフィールド

フィールド	データタイプ	説明
送信元ディテクタ ID	uint32	送信元ディテクタの ID 文字列。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	送信元タイプ名のバイト数。
[名前(Name)]	string	送信元ディテクタの名前。

サードパーティ スキャナの脆弱性レコード

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

次の表では、脆弱性レコードのフィールドについて説明します。

表 4-13　サードパーティ スキャナ脆弱性レコードのフィールド

フィールド	データタイプ	説明
脆弱性 ID	uint32	サードパーティ脆弱性 ID 番号。このフィールドとスキャナ タイプを合わせると、このレコードの固有キーとなります。
スキャナ タイプ	uint32	サードパーティ スキャナ タイプ。このフィールドと脆弱性 ID を合わせると、このレコードの固有キーとなります。
タイトル長さ	uint32	タイトル フィールド長さ。

表 4-13　サードパーティ スキャナ脆弱性レコードのフィールド（続き）

フィールド	データタイプ	説明
役職（Title）	string	脆弱性のタイトル。
説明の長さ	uint32	説明フィールドの長さ。
説明	string	脆弱性に関する一般的な説明。
CVE ID 長さ	uint32	CVE ID フィールドの長さ。
CVE ID	string	脆弱性の Common Vulnerabilities and Exposures（CVE）ID 番号。
BugTraq ID の長さ	uint32	BugTraq ID フィールドの長さ。
BugTraq ID	string	脆弱性の BugTraq ID 番号

ユーザー レコード

eStreamer サービスは、次の形式のユーザー レコードで、システムが検出したユーザーに関する情報を格納したメタデータを送信します。（バージョン 4 メタデータとポリシー イベント要求フラグ（それぞれ要求メッセージの要求フラグ フィールドのビット 20 と 22）を設定すると、ユーザー情報が送信されます。要求フラグ（2-15 ページ） を参照してください）。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、ユーザー レコードを示す 98 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ヘッダー バージョン（1）																	メッセージ タイプ（4）															
メッセージ長																																
Netmap ID																	レコード タイプ（98）															
レコード長																																
ユーザー データ ブロック タイプ（57）																																
ユーザー データ ブロック長																																
ユーザー ID（User ID）																																
プロトコル																																
文字列ブロック タイプ（0）																																
文字列ブロック長																																
ユーザー名...																																

次の表は、ユーザー レコードのフィールドについての説明です。

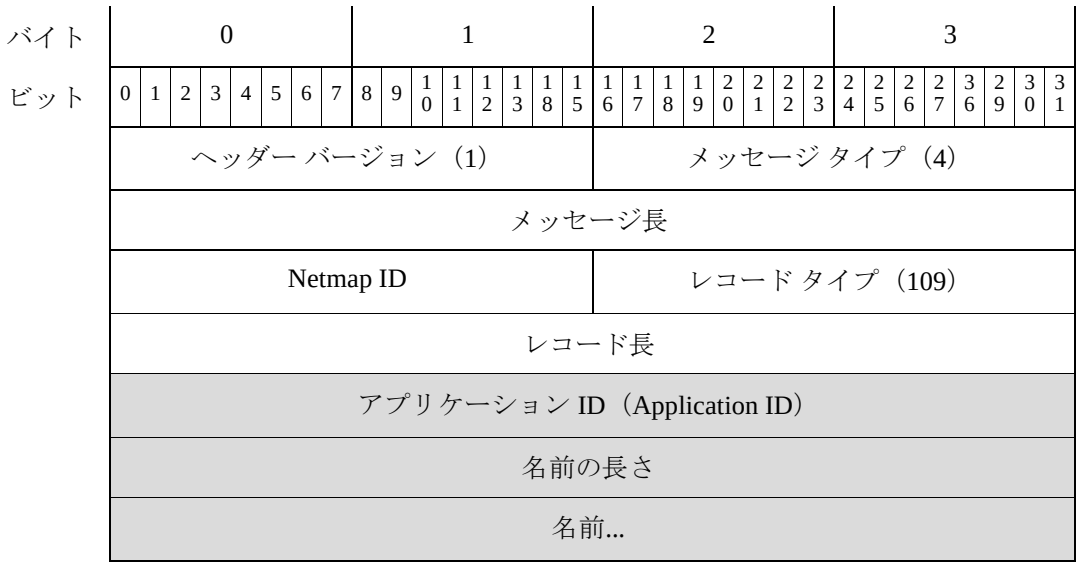
表 4-14　ユーザー レコードのフィールド

フィールド	データタイプ	説明
ユーザー データ ブロック タイプ	uint32	ユーザー データ ブロックを開始します。この値は常に 57 です。ブロック タイプは、シリーズ 2 ブロックです。
ユーザー データ ブロック長	uint32	データ ブロックの長さ。データのバイト数に 2 つのデータ ブロック ヘッダー フィールドの 8 バイトを加えたバイト数です。
ユーザー ID（User ID）	uint32	ユーザーの固有識別情報。このフィールドは、このレコードの固有キーです。
プロトコル	uint32	ユーザーの検出やレポートに使用するプロトコル。値は以下のとおりです。 • 165：FTP • 426：SIP • 547：AOL Instant Messenger • 683：IMAP • 710：LDAP • 767：NTP • 773：Oracle データベース • 788：POP3 • 1755：MDNS
文字列ブロック タイプ	uint32	ユーザー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトにユーザー名フィールドのバイト数を加えたユーザー名文字列データ ブロックのバイト数。
[ユーザー名（Username）]	string	ユーザーの名前

Web アプリケーション レコード

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

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



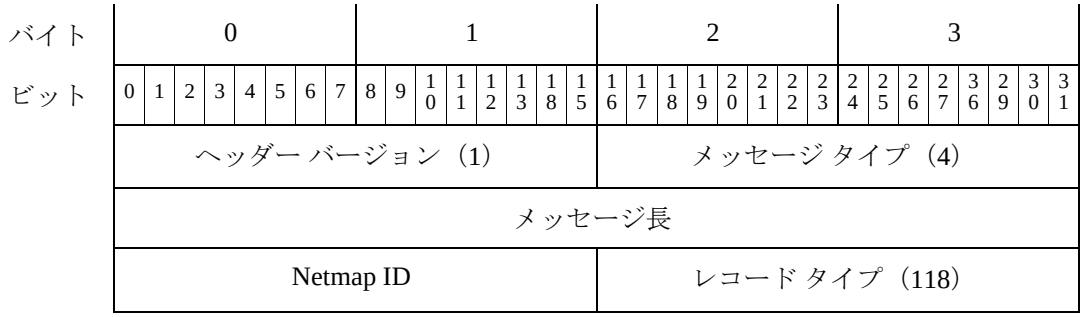
次の表では、Web アプリケーション レコードのフィールドについて説明します。

表 4-15　Web アプリケーション レコードのフィールド

フィールド	データタイプ	説明
アプリケーション ID	uint32	Web アプリケーションのアプリケーション ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	名前に含まれるバイト数。
名前	string	Web アプリケーションの内容の名前。

侵入ポリシー名レコード

eStreamer サービスは、次の形式の侵入ポリシー名レコードで、接続イベントの侵入ポリシー名情報を格納したメタデータを送信します。(侵入ポリシー名情報は、メタデータ フラグ(要求メッセージの要求フラグ フィールドのバージョン 4 メタデータ ビット 20)が設定されると送信されます。要求フラグ(2-15 ページ) を参照してください)。ちなみに、メッセージ長さフィールドの後のレコード タイプ フィールドの値は、侵入ポリシー名レコードを示す 118 です。シリーズ 2 セットのデータ ブロックのブロック タイプ 14 の UUID 文字列データ ブロックが含まれています。



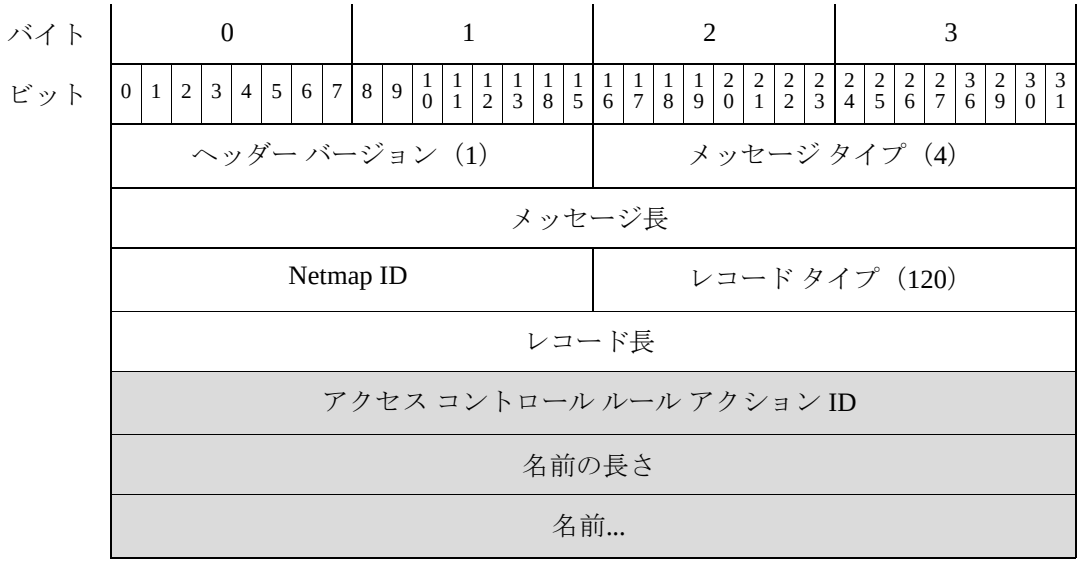
次の表では、侵入ポリシー名データ ブロックのフィールドについて説明します。

表 4-16　侵入ポリシー名データ ブロックのフィールド

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

アクセス コントロール ルール アクション レコード メタデータ

eStreamer サービスは、次の形式のアクセス コントロール ルール アクション レコードで、トリガーのかかったアクセス コントロール ルールに関連付けられたアクションを格納したメタデータを送信します。(アクセス コントロール ルール アクション情報は、バージョン 4 メタデータ フラグ(要求メッセージの要求フラグ フィールドのビット 20)が設定されると送信されます。要求フラグ (2-15 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、アクセス コントロール ルール アクション レコードを示す 120 です。



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

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

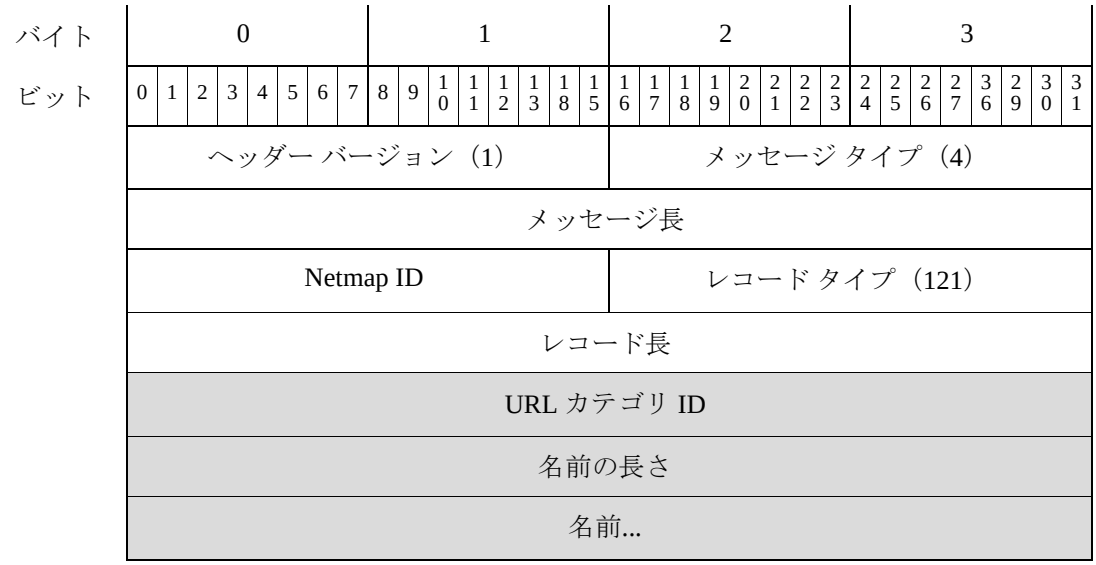
フィールド	データタイプ	説明
アクセス コントロール ルール アクション ID	uint32	アクセス コントロール ルール アクションの ID 番号。このフィールドは、このレコードの固有キーです。

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

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

URL カテゴリ レコード メタデータ

eStreamer サービスは、次の形式の URL カテゴリ レコードで、接続ログの URL に関連付けられたカテゴリ名を格納したメタデータを送信します。(URL カテゴリ情報は、バージョン 4 メタデータ フラグ(要求メッセージの要求フラグ フィールドのビット 20)が設定されると送信されます。要求フラグ (2-15 ページ) を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、URL カテゴリ レコードを示す 121 です。



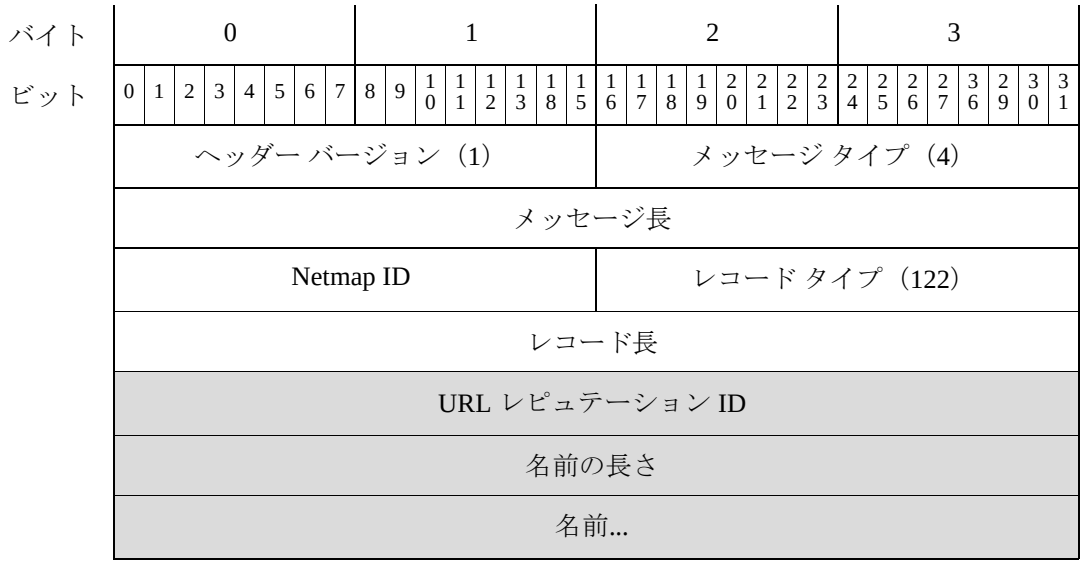
次の表では、URL カテゴリ レコードのフィールドについて説明します。

表 4-18　URL カテゴリ レコードのフィールド

フィールド	データタイプ	説明
URL カテゴリ ID	uint32	URL カテゴリの ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	名前に含まれるバイト数。
[名前（Name）]	string	URL カテゴリ名。

URL レピュテーション レコード メタデータ

eStreamer サービスは、次の形式の URL レピュテーション レコードで、URL に関連付けられたレピュテーション（リスク レベル）を格納したメタデータを送信します。（URL レピュテーション情報は、バージョン 4 メタデータ フラグ（要求メッセージの要求フラグ フィールドのビット 20）が設定されると送信されます。要求フラグ（2-15 ページ） を参照してください）。ちなみに、メッセージ長さフィールドの後の URL レピュテーション メタデータ レコード フィールドの値は、URL レピュテーション メタデータ レコードを示す 122 です。



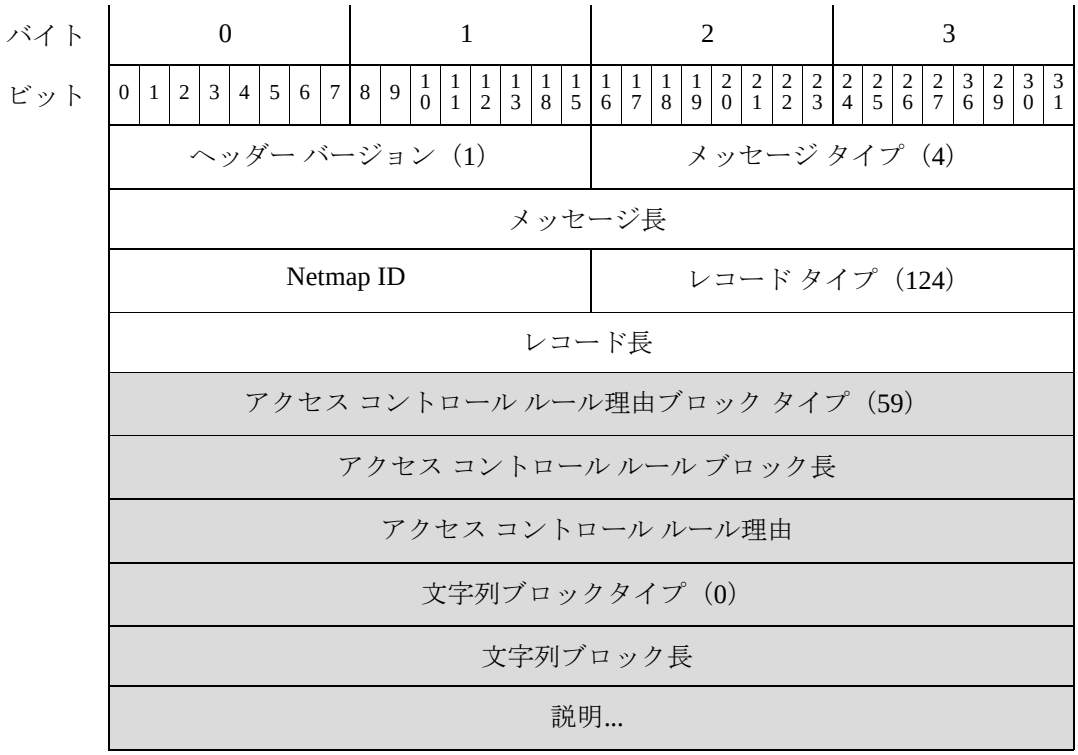
次の表では、URL レピュテーション レコードのフィールドについて説明します。

表 4-19　URL レピュテーション レコードのフィールド

フィールド	データタイプ	説明
URL レピュテーション ID	uint32	URL レピュテーションの ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	名前に含まれるバイト数。
[名前（Name）]	string	URL レピュテーション名。

アクセス コントロール ルール理由メタデータ

eStreamer サービスは、次の形式のアクセス コントロール ルール理由レコードで、アクセス コントロール ルールで侵入イベントまたは接続イベントにトリガーがかかった理由に関する情報を格納したメタデータを送信します。アクセス コントロール ルール理由メタデータは、バージョン 4 メタデータ フラグ（要求メッセージの要求フラグ フィールドのビット 20）が設定されると送信されます。要求フラグ（2-15 ページ）を参照してください。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、アクセス コントロール ルール理由レコードを示す 124 です。このメタデータには、アクセス コントロール ルール理由ブロックを格納します（アクセス コントロール ルール理由データ ブロック 6.0+（4-214 ページ）を参照）。アクセスコントロールルール理由データブロックのブロックタイプは、シリーズ 2 のブロックタイプ 59 です。



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

表 4-20　　アクセス コントロール ルール理由メタデータのフィールド

フィールド	データタイプ	説明
アクセス コントロール ルール理由ブロック タイプ	uint32	アクセス コントロール ルール理由ブロックを開始します。この値は常に 59 です。これはシリーズ 2 のデータ ブロックです。
アクセス コントロール ルール理由ブロック長	uint32	アクセス コントロール ルール理由ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ルール理由ブロックの合計バイト数。

表 4-20　アクセス コントロール ルール理由メタデータのフィールド（続き）

フィールド	データタイプ	説明
アクセス コントロール ルール理由	uint32	アクセス コントロール ルールによって接続がログに記録された理由。このフィールドは、このレコードの固有キーです。 イベントをトリガーしたルールの理由の番号。 ルールの理由は、複数のビットを設定できるバイナリ ビットマップです。ルールには、複数の理由がある場合があります。ビット値は次のとおりです。 • **1**：IP ブロック • **2**：IP モニター • **4**：ユーザー バイパス • **8**：ファイル モニター • **16**：ファイル ブロック • **32**：侵入モニター • **64**：侵入ブロック • **128**：ファイル再開ブロック • **256**：ファイル再開許可 • **512**：ファイルカスタム検出 • **1024**：SSL ブロック • **2048**：DNS ブロック • **4096**：DNS モニター • **8192**：URL ブロック • **16384**：URL モニター • **32768**：コンテンツ制約 • **65536**：インテリジェント アプリケーション バイパス • **131072**：WSA 脅威
文字列ブロック タイプ	uint32	アクセス コントロール ルール理由に関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	アクセス コントロール ルール理由の説明。

アクセス コントロール ポリシー メタデータ

eStreamer サービスは、次の形式のアクセス コントロール ポリシー メタデータ レコードで、侵入イベントまたは接続イベントにトリガーをかけたアクセス コントロール ポリシーに関する情報を格納したメタデータを送信します。アクセス コントロール ルール ポリシー メタデータは、バージョン 4 メタデータ フラグ（要求メッセージの要求フラグ フィールドのビット 20）が設定されると送信されます。要求フラグ（2-15 ページ）を参照してください。ちなみに、メッセージ長

フィールドの後のレコード タイプ フィールドの値は、アクセス コントロール ポリシー メタデータ レコードを示す 145 です。このメタデータには、アクセス コントロール ポリシー メタデータ ブロックを格納します(アクセス コントロール ポリシー メタデータ ブロック 6.0+ (4-218 ページ) を参照)。アクセス コントロール ポリシー メタデータ ブロックのブロック タイプは、シリーズ 2 のブロック タイプ 64 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ヘッダー バージョン（1）																メッセージ タイプ（4）															
	メッセージ長																															
	Netmap ID																レコード タイプ（145）															
	レコード長																															
	アクセス コントロール ポリシーのメタデータ ブロック タイプ（64）																															
	アクセス コントロール ポリシーのメタデータ ブロック長																															
AC ポリシー UUID	アクセス コントロール ポリシー UUID																															
	アクセス コントロール ポリシー UUID（続き）																															
	アクセス コントロール ポリシー UUID（続き）																															
	アクセス コントロール ポリシー UUID（続き）																															
	センサー ID（Sensor ID）																															
ポリシー名	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ポリシー名...																															

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

表 4-21　アクセス コントロール ポリシー メタデータのフィールド

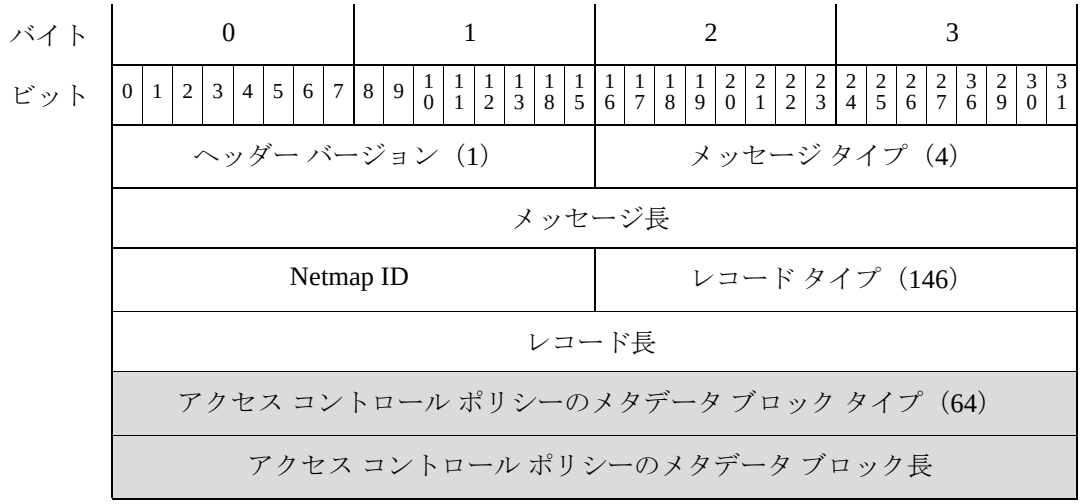
フィールド	データタイプ	説明
アクセス コントロール ポリシーのメタデータ ブロック タイプ	uint32	アクセス コントロール ポリシー メタデータ ブロックを開始します。この値は常に 64 です。これはシリーズ 2 のデータ ブロックです。
アクセス コントロール ポリシーのメタデータ ブロック長	uint32	アクセス コントロール ポリシーのメタデータ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ポリシー メタデータ ブロックの合計バイト数。

表 4-21　アクセス コントロール ポリシー メタデータのフィールド（続き）

フィールド	データタイプ	説明
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの UUID。このフィールドは、このレコードの固有キーです。
センサー ID（Sensor ID）	uint32	アクセス コントロール ポリシーに関連付けられたセンサー ID 番号。このフィールドは、このレコードの固有キーです。
文字列ブロック タイプ	uint32	アクセス コントロール ポリシーに関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
[名前（Name）]	string	アクセス コントロール ポリシーの名前。

プレフィルタ ポリシー メタデータ

eStreamer サービスは、次の形式のプレフィルタ ポリシーレコードで、侵入イベントまたは接続イベントにトリガーをかけたプレフィルタ ポリシーに関する情報を格納したメタデータを送信します。プレフィルタ ポリシー メタデータは、バージョン 4 メタデータ フラグ（要求メッセージの要求フラグ フィールドのビット 20）が設定されると送信されます。要求フラグ（2-15 ページ）を参照してください。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、プレフィルタポリシー メタデータ レコードであることを示す 146 です。このメタデータには、アクセス コントロール ポリシー メタデータ ブロックを格納します（アクセス コントロール ポリシー メタデータ ブロック 6.0+（4-218 ページ）を参照）。アクセス コントロール ポリシー メタデータ ブロックのブロック タイプは、シリーズ 2 のブロック タイプ 64 です。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
AC ポリシー UUID	アクセス コントロール ポリシー UUID																															
	アクセス コントロール ポリシー UUID（続き）																															
	アクセス コントロール ポリシー UUID（続き）																															
	アクセス コントロール ポリシー UUID（続き）																															
	センサー ID（Sensor ID）																															
ポリシー名	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ポリシー名...																															

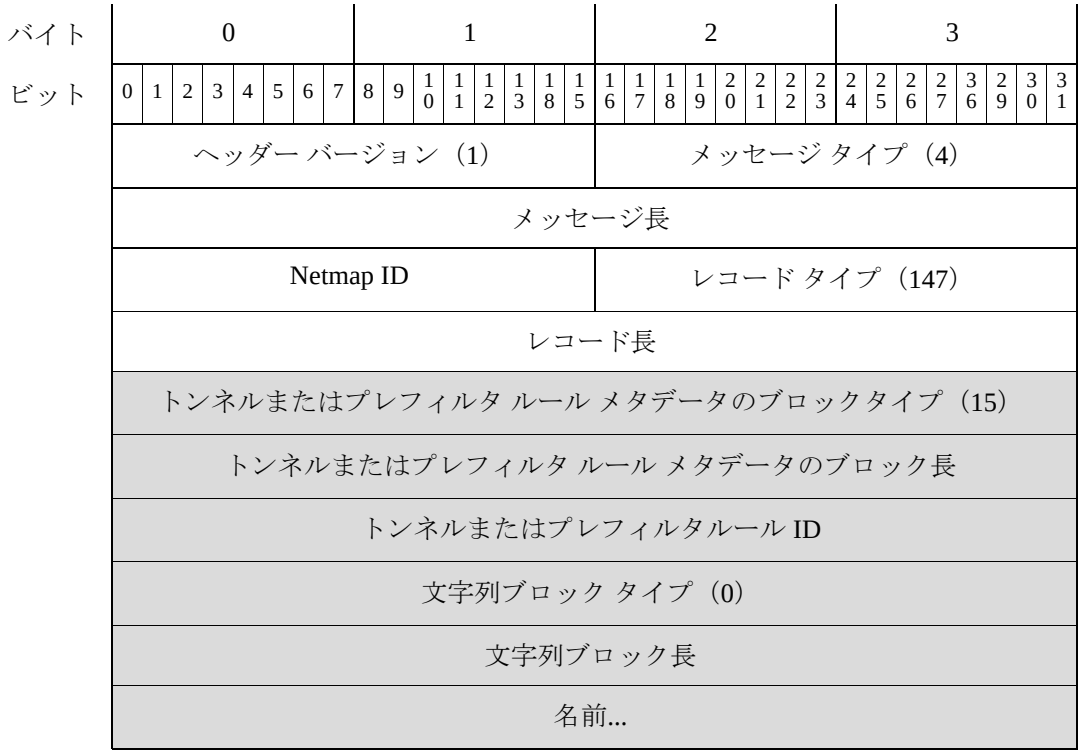
次の表では、プレフィルタ ポリシー メタデータ ブロックのフィールドについて説明します。

表 4-22　　プレフィルタ ポリシー メタデータ フィールド

フィールド	データタイプ	説明
プレフィルタ ポリシー ブロック タイプ	uint32	プレフィルタ ポリシー ブロックを開始します。この値は常に 64 です。これはシリーズ 2 のデータ ブロックです。
プレフィルタ ポリシー ブロック長	uint32	プレフィルタ ポリシー ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータのバイト数を加えたプレフィルタ ポリシー ブロックの合計バイト数。
アクセス コントロール ポリシー UUID	uint8[16]	アクセス コントロール ポリシーの UUID。このフィールドとセンサー ID を合わせると、このレコードの固有キーとなります。
センサー ID（Sensor ID）	uint32	アクセス コントロール ポリシーに関連付けられたセンサー ID 番号。このフィールドとアクセス コントロール ポリシー UUID を合わせると、このレコードの固有キーになります。
文字列ブロック タイプ	uint32	プレフィルタ ポリシーに関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
[名前（Name）]	string	プレフィルタ ポリシーの名前。

トンネルまたはプレフィルタのルールのメタデータ

eStreamer サービスは、次の形式のアクセス コントロール ルール理由レコードで、トンネル ルールまたはプレフィルタ ルールで侵入イベントまたは接続イベントにトリガーがかかった理由に関する情報を格納したメタデータを送信します。トンネル ルールまたはプレフィルタ ルールの理由メタデータは、バージョン 4 メタデータ フラグ（要求メッセージの要求フラグ フィールドのビット 20）が設定されると送信されます。要求フラグ（2-15 ページ）を参照してください。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、プレフィルタ ルール理由レコードであることを示す 147 です。
内容が同じなので、アクセス コントロール ルール理由ブロックを格納します（アクセス コントロール ルール データ ブロック（4-212 ページ）を参照）。アクセスコントロールルール理由データブロックのブロックタイプは、シリーズ 2 のブロックタイプ 59 です。



次の表は、トンネルまたはプレフィルタ ルール メタデータ ブロックのフィールドについての説明です。

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

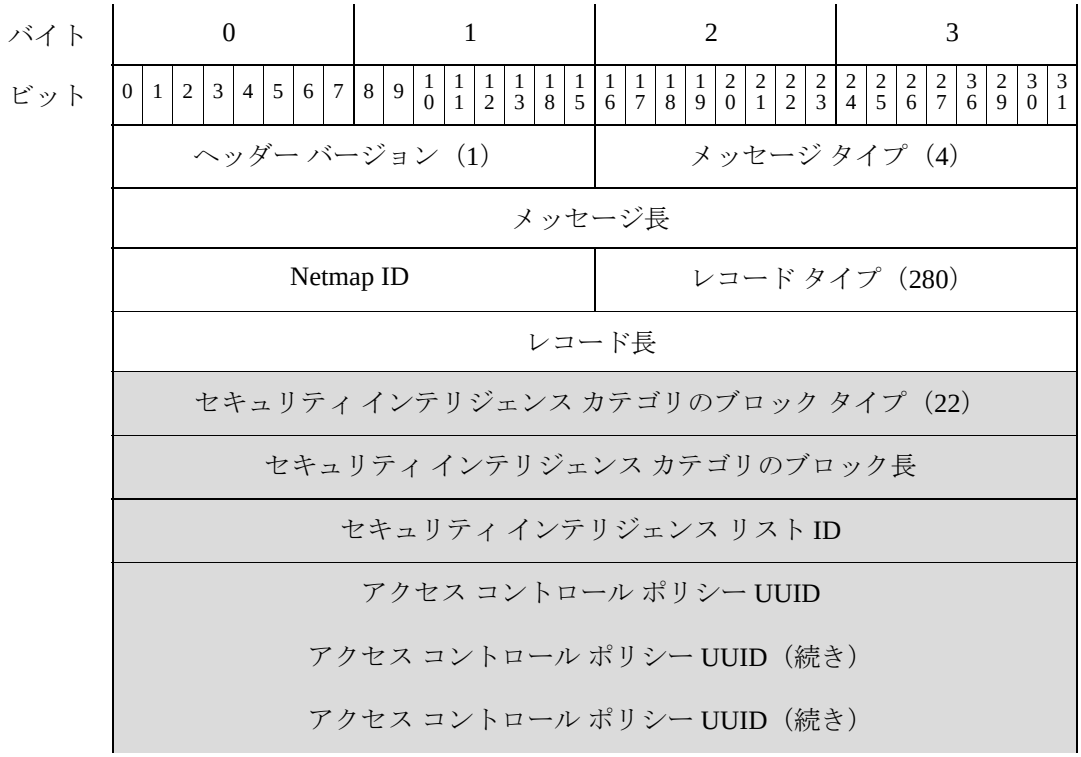
フィールド	データタイプ	説明
トンネルまたはプレフィルタルールのブロックタイプ	uint32	アクセス コントロール ルール ブロックを開始します。この値は常に 15 です。ちなみに、このブロックは、アクセス コントロール ルールだけでなく、トンネル ルールとプレフィルタ ルールにも使用します。
トンネルまたはプレフィルタルールのブロック長	uint32	トンネルまたはプレフィルタ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータのバイト数を加えたトンネルまたはプレフィルタルールブロックの合計バイト数。

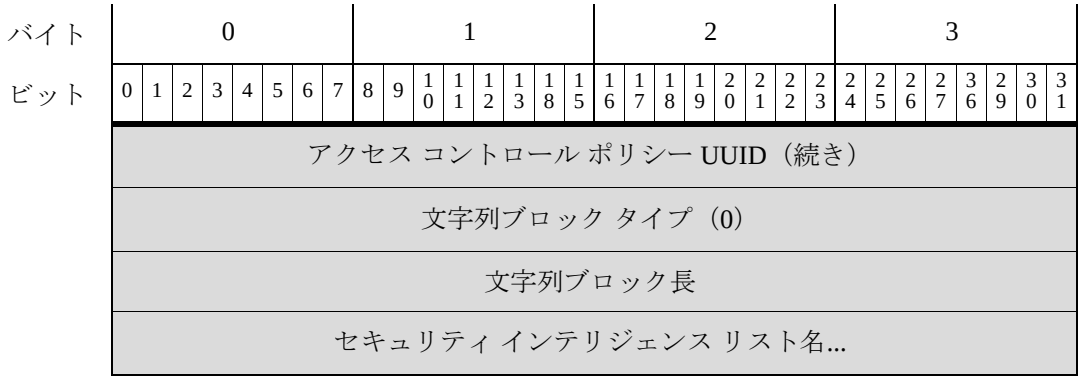
表 4-23　トンネルまたはプレフィルタ ルール理由メタデータ フィールド （続き）

フィールド	データタイプ	説明
トンネルまたはプレフィルタルール ID	uint32	トンネルまたはプレフィルタルールの内部 シスコ 識別子。
文字列ブロック タイプ	uint32	トンネルまたはプレフィルタルールの UUID とトンネルまたはプレフィルタルール ID に関連付けられた説明的な名前を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
[名前(Name)]	string	わかりやすい名前。

セキュリティ インテリジェンス カテゴリ メタデータ

eStreamer サービスは、次の形式のセキュリティ インテリジェンス カテゴリ レコードで、セキュリティ インテリジェンス カテゴリに関する情報を格納したメタデータを送信します。セキュリティ インテリジェンス カテゴリ メタデータは、バージョン 4 メタデータ フラグ(要求メッセージの要求フラグ フィールドのビット 20)が設定されると送信されます。要求フラグ(2-15 ページ)を参照してください。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、セキュリティ インテリジェンス カテゴリ レコードを示す 280 です。これには、セキュリティ インテリジェンス カテゴリ データ ブロックを格納します(セキュリティ インテリジェンス カテゴリ データ ブロック 5.1+(4-215 ページ) を参照)。セキュリティ インテリジェンス データ ブロックのブロック タイプは、シリーズ 2 のブロック タイプ 22 です。





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

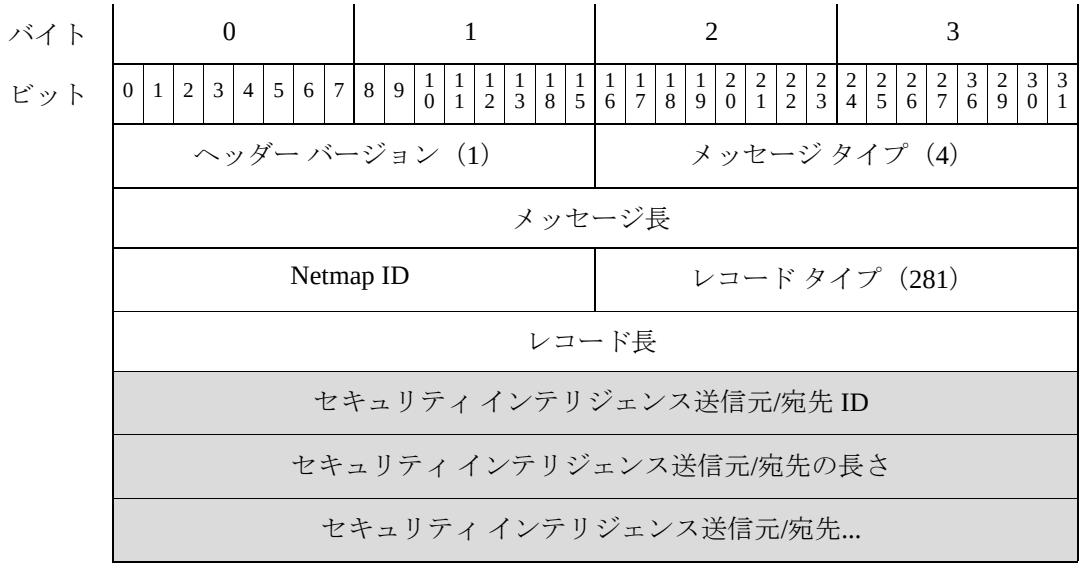
表 4-24　　セキュリティ インテリジェンス カテゴリ メタデータのフィールド

フィールド	データタイプ	説明
セキュリティ インテリジェンス カテゴリ ブロック タイプ	uint32	セキュリティ インテリジェンス カテゴリのデータ ブロックを開始します。この値は常に 22 です。これはシリーズ 2 のデータ ブロックです。
セキュリティ インテリジェンス カテゴリのブロック長	uint32	セキュリティ インテリジェンス カテゴリ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたセキュリティ インテリジェンス カテゴリ ブロックの合計バイト数。
セキュリティ インテリジェンス リスト ID	uint32	接続によってトリガーされた IP ブロックリストまたは許可リストの ID。このフィールドとアクセス コントロール ポリシー UUID を合わせると、このレコードの固有キーになります。
アクセス コントロール ポリシー UUID	uint8[16]	セキュリティ インテリジェンスに設定されたアクセス コントロール ポリシーの UUID。このフィールドとセキュリティ インテリジェンス リスト ID を合わせると、このレコードの固有キーとなります。
文字列ブロック タイプ	uint32	セキュリティ インテリジェンス リストに関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトにセキュリティ インテリジェンス リスト名フィールドのバイト数を加えた名前文字列データ ブロックのバイト数。
セキュリティ インテリジェンス リスト名	string	接続によってトリガーされた IP カテゴリブロックリストまたは許可リストの名前。

セキュリティ インテリジェンス送信元/宛先レコード

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

ると送信されます。要求フラグ（2-15 ページ）を参照してください）。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、セキュリティ インテリジェンス送信元/宛先レコードを示す 281 です。



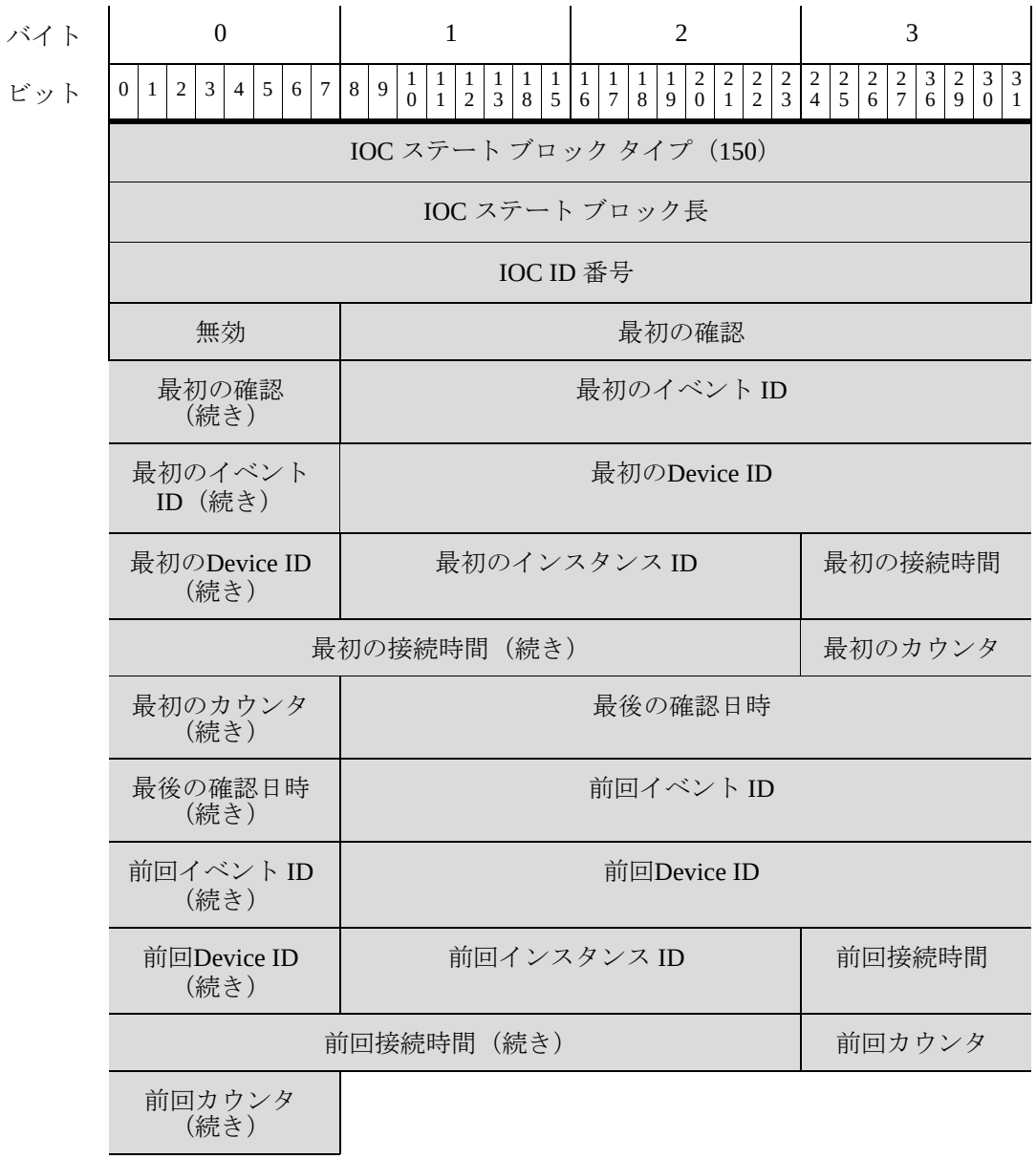
次の表では、セキュリティ インテリジェンス送信元/宛先レコードのフィールドについて説明します。

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

フィールド	データタイプ	説明
セキュリティ インテリジェンス送信元/宛先 ID	uint32	セキュリティ インテリジェンス送信元/宛先 ID 番号。このフィールドは、このレコードの固有キーです。
セキュリティ インテリジェンス送信元/宛先長さ	uint32	セキュリティ インテリジェンス送信元/宛先バイト数。
セキュリティ インテリジェンス送信元/宛先	string	検出した IP アドレスは、送信元または宛先の IP アドレスであるかどうか。

5.3+ の IOC ステート データ ブロック

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



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

表 4-26　　IOC ステート データ ブロックのフィールド

フィールド	データタイプ	説明
IOC ステート データ ブロック タイプ	uint32	IOC ステート データ ブロックを開始します。この値は常に 150 です。
IOC ステート データ ブロックの長さ	uint32	IOC ステート データ ブロック タイプ フィールドと長さ フィールドの 8 バイトに、後続のデータ バイト数を加えた IOC ステート データ ブロックの合計バイト数。

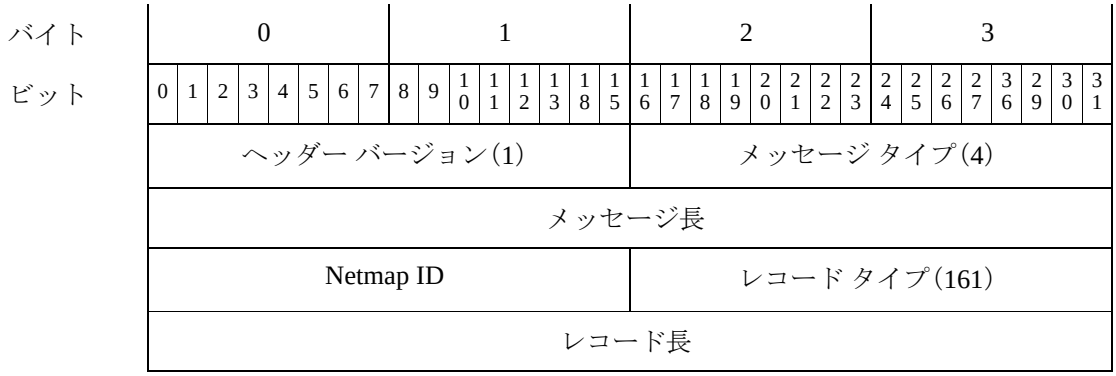
表 4-26　IOC ステート データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
IOC ID 番号	uint32	侵害の固有 ID 番号。
無効	uint8	侵害がホストで無効にされているかどうかを示します: • 0:侵害は無効ではありません。 • 1:侵害が無効です。
最初の確認	uint32	この侵害の最初の検出時を示す UNIX タイムスタンプ。
最初のイベント ID	uint32	この侵害が最初に確認されたイベントの ID 番号。
最初のDevice ID	uint32	最初に IOC を検出したセンサーの ID。
最初のインスタンス ID	uint16	最初に侵害を検出した管理対象デバイスの Snort インスタンスの数値 ID。
最初の接続時間	uint32	この侵害を最初に検出した接続の Unix タイムスタンプ。
最初のカウンタ	uint16	この侵害を最後の確認日時した接続のカウンタ。 これで、同時に発生する複数の接続を区別します。
最後の確認日時	uint32	この侵害の前回の検出時を示す UNIX タイムスタンプ。
前回イベント ID	uint32	この侵害を最後の確認日時したイベントの ID 番号。
前回 DeviceID	uint32	前回 IOC を検出したセンサーの ID。
前回インスタンス ID	uint16	前回侵害を検出した管理対象デバイスの Snort インスタンスの数値 ID。
前回接続時間	uint32	この侵害を最後の確認日時した接続の Unix タイムスタンプ。
前回カウンタ	uint16	この侵害を最後の確認日時した接続のカウンタ。 これで、同時に発生する複数の接続を区別します。

5.3+ の IOC 名データ ブロック

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

次の図は、IOC 名データ ブロックの構造です。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	IOC 名ブロック タイプ（39）																															
	IOC 名ブロック長																															
	IOC ID 番号																															
カテゴリ（Category）	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	カテゴリ...																															
イベント タイプ（Event Type）	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	イベント タイプ...																															

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

表 4-27　　IOC 名データ ブロックのフィールド

フィールド	データタイプ	説明
IOC 名データ ブロック タイプ	uint32	IOC 名データ ブロックを開始します。この値は常に 39 です。
IOC 名データ ブロック長	uint32	IOC 名データ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えた IOC 名データ ブロックの合計バイト数。
IOC ID 番号	uint32	侵害の固有 ID 番号。
文字列ブロック タイプ	uint32	侵害に関連付けられたカテゴリを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトとカテゴリ フィールドのバイト数が含まれます。

表 4-27　IOC 名データ ブロックのフィールド（続き）

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

表 4-27　IOC 名データ ブロックのフィールド（続き）

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

ディスカバリ イベント ヘッダー 5.2+

ディスカバリ イベントおよび接続イベントのメッセージには、ディスカバリ イベント ヘッダーが含まれます。これは、イベントのタイプおよびサブタイプ、イベントが発生した時刻、イベントが発生したデバイス、およびメッセージ内のイベント データの構造を伝えます。このヘッダーには、実際のホスト ディスカバリ、ユーザー、または接続イベントのデータが続きます。さまざまなイベントのタイプ/サブタイプ値に関連付けられる構造の詳細については、イベント タイプ別ホスト ディスカバリ構造（4-46 ページ）で説明します。このヘッダーは IPv6 をサポートしており、ディスカバリ イベント ヘッダー 5.0 ～ 5.1.1.x（B-127 ページ） はサポートを停止しました。

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ヘッダー バージョン（1）																メッセージ タイプ（4）															
	メッセージ長																															
	Netmap ID																レコード タイプ															
	レコード長																															
	eStreamer サーバー タイムスタンプ（イベント用、ビット 23 が設定されている場合のみ）																															
	将来の使用に備えて予約済み（イベントでビット 23 が設定されている場合のみ）																															
ディスカバリ イベント ヘッダー	Device ID																															
	レガシー IP アドレス																															
	MAC アドレス																															
	MAC アドレス（続き）																IPv6 あり								将来の使用に備えて予約済み							
	イベント秒																															
	イベント マイクロ秒																															
	イベント タイプ（Event Type）																															
	イベント サブタイプ																															
	ファイル番号（内部使用専用）																															
	ファイルの位置（内部使用専用）																															

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

次の表は、ディスカバリ イベント ヘッダーについての説明です。

表 4-28　　ディスカバリ イベント ヘッダーのフィールド

フィールド	データ型	説明
Device ID	uint32	ディスカバリ イベントを生成したデバイスの ID 番号。バージョン 3 および 4 のメタデータを要求すると、デバイスのメタデータを入手できます。詳細については、管理対象Device レコードのメタデータ（3-36 ページ）を参照してください。
レガシー IP アドレス	uint32	このフィールドは予約済みですが、設定されておりません。IPv4 アドレスは IPv6 アドレス フィールドに保存されます。詳細については、IP アドレス（1-4 ページ）を参照してください。
MAC アドレス	uint8[6]	イベントに関連するホストの MAC アドレス。
IPv6 あり	uint8	ホストに IPv6 アドレスがあることを示すフラグ。
将来の使用に備えて予約済み	uint8	将来の使用に備えて予約済み
イベント秒	uint32	システムがイベントを生成したときのUNIXタイムスタンプ（1970 年 1 月 1 日以降の秒数）。
イベント マイクロ秒	uint32	システムがイベントを生成したときのタイムスタンプの、マイクロ秒（100 万分の 1 秒）の増分。
イベント タイプ（Event Type）	uint32	イベント タイプ（新規イベントは 1000、変更イベントは、1001、ユーザー入力イベントは1002、フル ホスト プロファイルは1050）。使用可能なイベント タイプの一覧の詳細については、イベント タイプ別ホスト ディスカバリ構造（4-46 ページ）を参照してください。
イベント サブタイプ	uint32	イベント サブタイプ。使用可能なイベント サブタイプの一覧の詳細については、イベント タイプ別ホスト ディスカバリ構造（4-46 ページ）を参照してください。
ファイル番号	byte[4]	シリアル ファイル番号。このフィールドは、シスコ の内部使用のためのものであり、無視してかまいません。

表 4-28　ディスカバリ イベント ヘッダーのフィールド（続き）

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

ディスカバリ イベントと接続イベントのタイプとサブタイプ

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

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

表 4-29　タイプ/サブタイプ別のディスカバリ イベントと接続イベント

イベント名	イベント タイプ（Event Type）	イベント サブタイプ
新規ホスト	[1000]	1
新規 TCP サーバー	[1000]	2
新規ネットワーク プロトコル	[1000]	3
新規トランスポート プロトコル	[1000]	4
新規 IP 対 IP トラフィック	[1000]	5
新規 UDP サーバー	[1000]	6
新規クライアント アプリケーション	[1000]	7
新規 OS	[1000]	8
IPv6 トラフィックに新しい IPv6	[1000]	9
ホスト IP アドレスを変更	1001	1
OS 情報の更新	1001	2
ホスト IP アドレスを再利用	1001	3
脆弱性の変更	1001	4
ホップ数の変更	1001	5
TCP サーバー情報更新	1001	6
ホスト タイムアウト	1001	7
TCP ポート クローズ	1001	8
UDP ポート クローズ	1001	9
UDP サーバー情報更新	1001	10
TCP ポート タイムアウト	1001	11
UDP ポート タイムアウト	1001	12
MAC 情報の変更	1001	13
ホストの追加 MAC を検出	1001	14
最終検出時のホスト	1001	15

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

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

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

イベント名	イベント タイプ（Event Type）	イベント サブタイプ
ユーザー設定の有効な脆弱性（現在）	1002	22
ユーザー設定の無効な脆弱性（現在）	1002	23
ユーザー ホスト重要度	1002	24
ホスト属性設定値（現在）	1002	25
ホスト属性削除値（現在）	1002	26
ユーザー追加ホスト	1002	27
ユーザー追加サーバー	1002	28
ユーザー追加クライアント アプリケーション	1002	29
ユーザー追加プロトコル	1002	30
アプリを再読み込み	1002	31
アカウント削除	1002	32
接続統計情報	1003	1
接続チャンク	1003	2
新規ユーザー アイデンティティ	1004	1
ユーザー ログイン	1004	2
ユーザー アイデンティティを削除	1004	3
ユーザー アイデンティティをドロップ。ユーザー上限に到達	1004	4
失敗したユーザーのログイン	1004	5
VPN ユーザーのログイン	1004	8
VPN ユーザーのログオフ	1004	9
ホスト IOC 設定タイプ	1008	1
フル ホスト プロファイル	1050	該当なし

ヒント　各イベント タイプ/サブタイプに使用するデータ構造については、イベント タイプ別ホスト ディスカバリ構造（4-46 ページ）を参照してください。

イベント タイプ別ホスト ディスカバリ構造

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

- 新規ホスト メッセージと最後の確認日時ホスト メッセージ（4-47 ページ）
- サーバー メッセージ（4-48 ページ）
- 新規ネットワーク プロトコル メッセージ（4-49 ページ）
- 新規トランスポート プロトコル メッセージ（4-49 ページ）

- クライアント アプリケーション メッセージ(4-50 ページ)
- IP アドレス変更メッセージ(4-50 ページ)
- オペレーティング システム更新メッセージ(4-51 ページ)
- IP アドレスを再利用とホスト タイムアウト/削除メッセージ(4-52 ページ)
- ホップ変更メッセージ(4-52 ページ)
- ホップ変更メッセージ(4-52 ページ)
- TCP と UDP のポート クローズ メッセージ/タイムアウト メッセージ(4-52 ページ)
- MAC アドレス メッセージ(4-53 ページ)
- ブリッジ/ルータとして識別したホスト メッセージ(4-53 ページ)
- VLAN タグ情報更新メッセージ(4-54 ページ)
- NetBIOS 名変更メッセージ(4-54 ページ)
- 更新バナー メッセージ(4-55 ページ)
- ポリシー制御の概要(4-55 ページ)
- 接続統計データ メッセージ(4-56 ページ)
- 接続チャンク メッセージ(4-56 ページ)
- バージョン4.6.1+ のユーザー設定脆弱性メッセージ(4-57 ページ)
- ユーザー追加/削除ホスト メッセージ(4-57 ページ)
- ユーザー削除サーバー メッセージ(4-58 ページ)
- ユーザー設定ホスト重要度メッセージ(4-58 ページ)
- 属性メッセージ(4-59 ページ)
- 属性値メッセージ(4-59 ページ)
- ユーザー サーバー メッセージとオペレーティング システム メッセージ(4-60 ページ)
- ユーザー プロトコル メッセージ(4-60 ページ)
- ユーザー クライアント アプリケーション メッセージ(4-61 ページ)
- スキャン結果を追加メッセージ(4-61 ページ)
- 新規オペレーティング システム メッセージ(4-62 ページ)
- アイデンティティ競合とアイデンティティ タイムアウト システム メッセージ(4-62 ページ)
- ホスト IOC セット メッセージ(4-63 ページ)

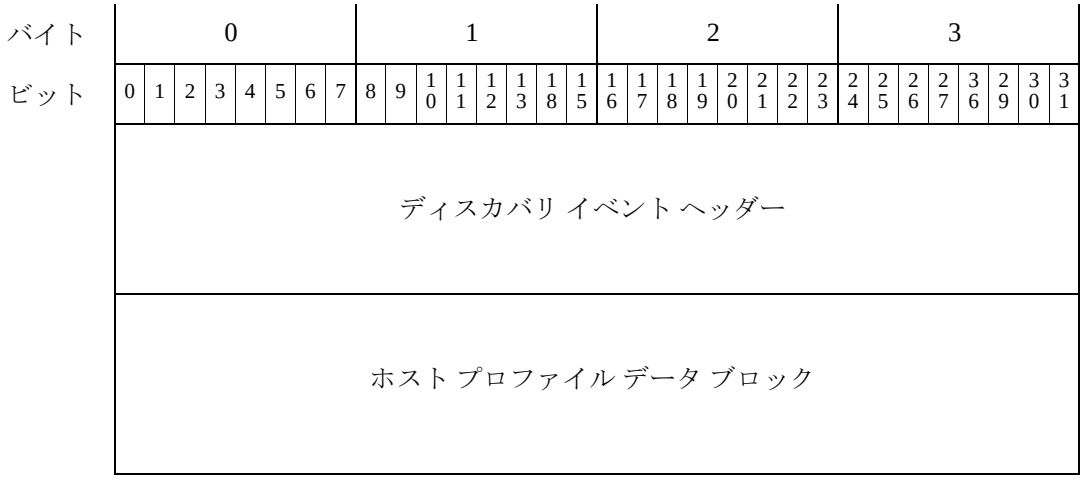
以下の項のデータ ブロック図は、ホスト ディスカバリ イベント メッセージで返る各種レコード データ ブロックです。

新規ホスト メッセージと最後の確認日時ホスト メッセージ

新規ホスト イベント メッセージと最後の確認日時ホスト イベント メッセージには、標準ディスカバリ イベント ヘッダーとホスト プロファイル データ ブロックがあります(ホスト プロファイル データブロック 5.2+(4-175 ページ) を参照)。ホスト プロファイル データ ブロックのブロック タイプは、シリーズ 1 のブロック タイプ 139 です。

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

(注)　ホスト プロファイル データ ブロックは、どのシステム バージョンでメッセージを作成したかによって異なります。ホスト プロファイル データ ブロックのレガシー バージョンについては、レガシー ホスト データ構造(B-373 ページ) を参照してください。



サーバー メッセージ

次の TCP サーバー イベント メッセージと UDP サーバー イベント メッセージには、標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-42 ページ) 参照)があり、サーバー データ ブロック(ホスト サーバー データ ブロック 4.10.0+(4-149 ページ) 参照、シリーズ 1 のブロック タイプ 103)がそれに続きます。

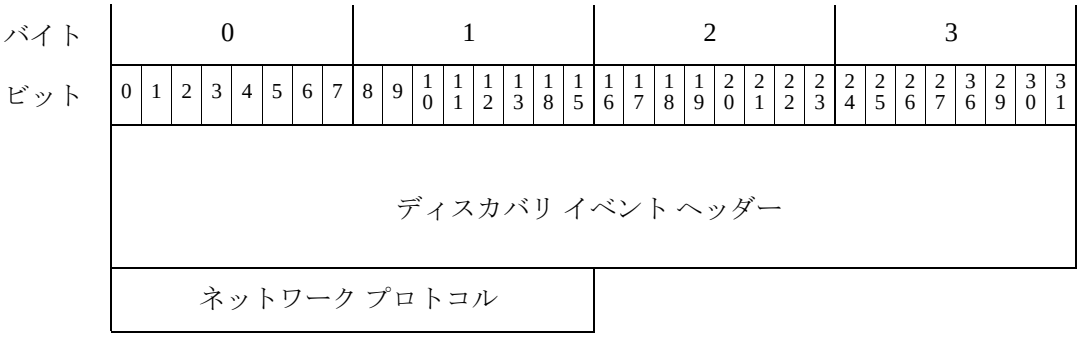
- 新規 TCP サーバー
- 新規 UDP サーバー
- TCP サーバー情報更新
- UDP サーバー情報更新
- TCP サーバー信頼度更新
- UDP サーバー信頼度更新

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

これらのイベントは、それぞれ次の形式を使用します:

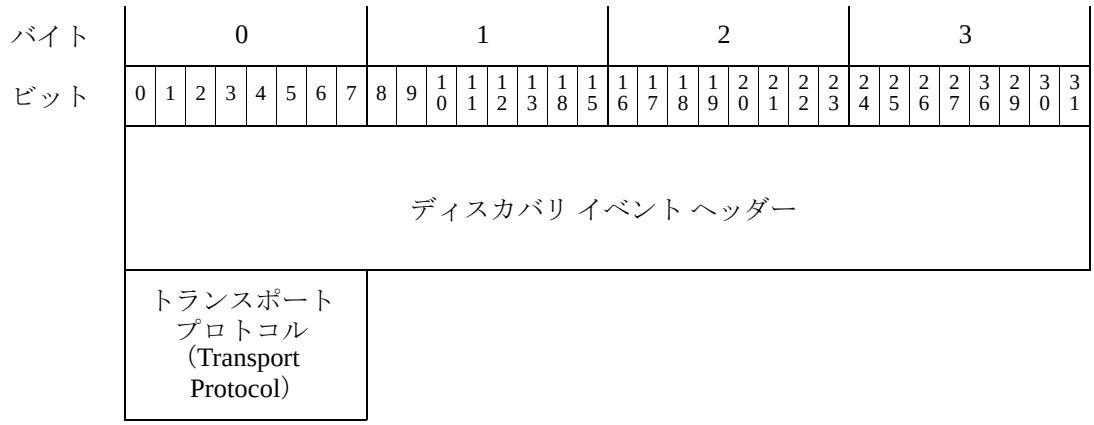
新規ネットワーク プロトコル メッセージ

新しいネットワーキング プロトコル イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照）があり、ネットワーク プロトコルの 2 バイトフィールド（次の表のプロトコル値を使用）が続きます。



新規トランスポート プロトコル メッセージ

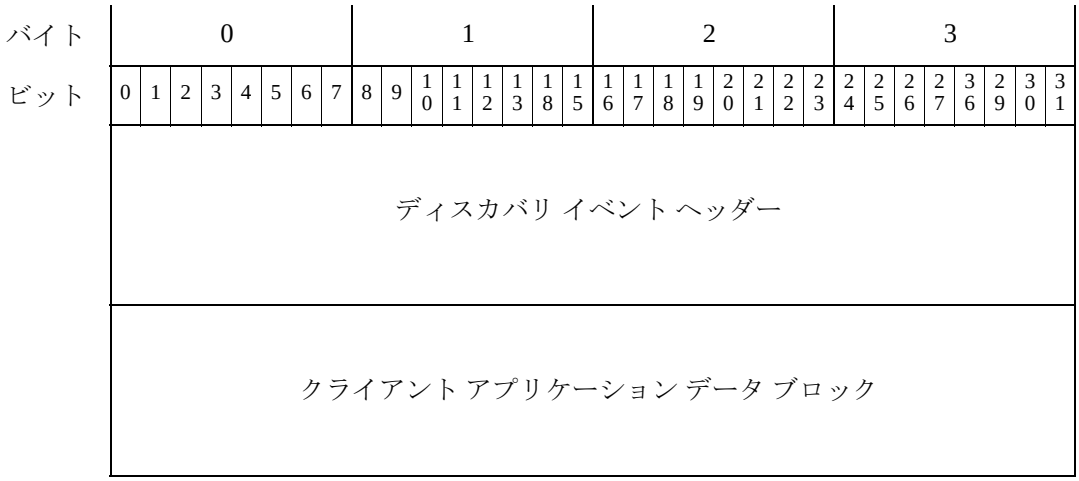
新規トランスポート プロトコルのイベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照。シリーズ 1 のブロック タイプ 4）と、トランスポート プロトコル番号の 1 バイト フィールド（次の表の値を使用）があります。



クライアント アプリケーション メッセージ

新規クライアント アプリケーション、クライアント アプリケーション アップデート、クライアント アプリケーション タイムアウト イベントは同じ形式であり、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）と、続けてクライアント アプリケーション データ ブロック（5.0+ のホスト クライアント アプリケーション データ ブロック（4-167 ページ）を参照。シリーズ 1 のブロック タイプ 122）があります。ディスカバリ イベント ヘッダーにあるレコード タイプ、イベント タイプ、イベント サブタイプは、送信されるイベントによって異なります。

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

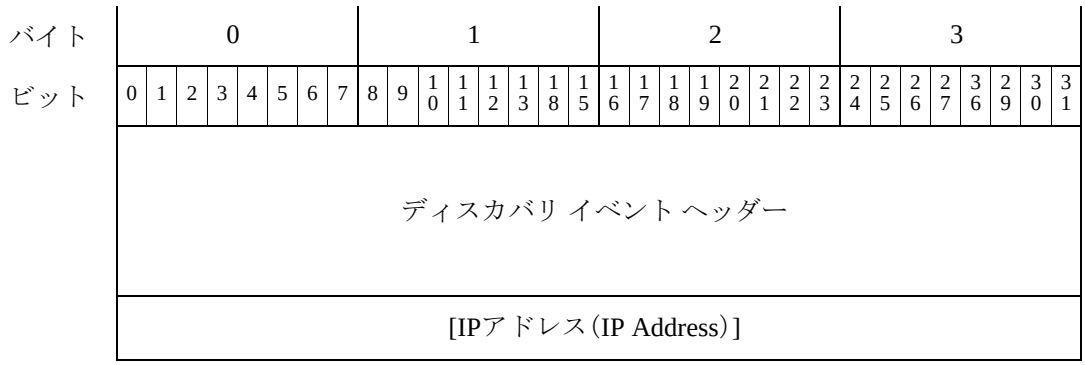


IP アドレス変更メッセージ

次のホスト ディスカバリ メッセージには、標準イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）と、2 種類の形式/構造（IP アドレスの 4 バイトと IP アドレスの 16バイト）があります。

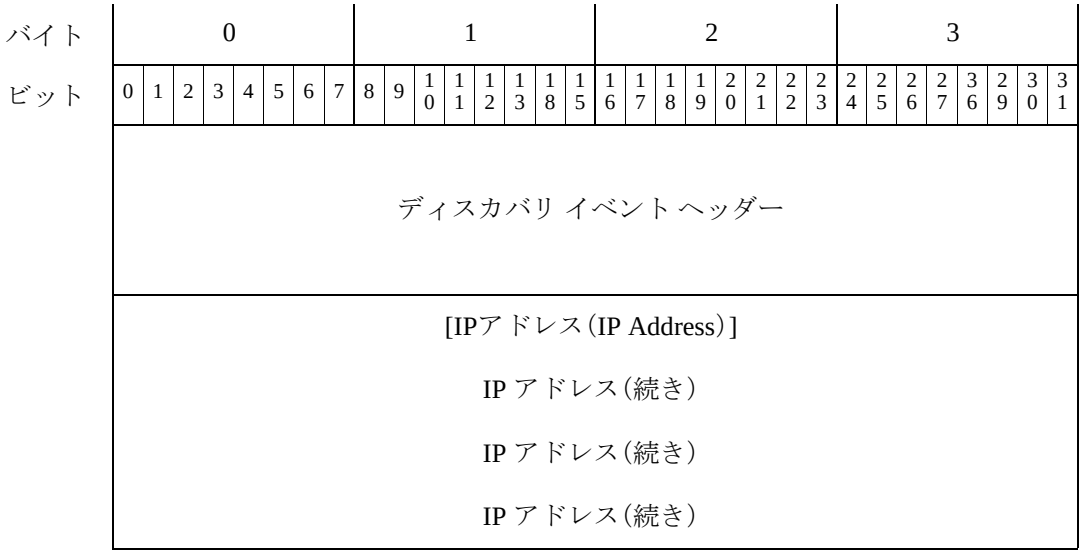
次の場合は、IP アドレスに（IP アドレス オクテット）4 バイトを使用します。

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



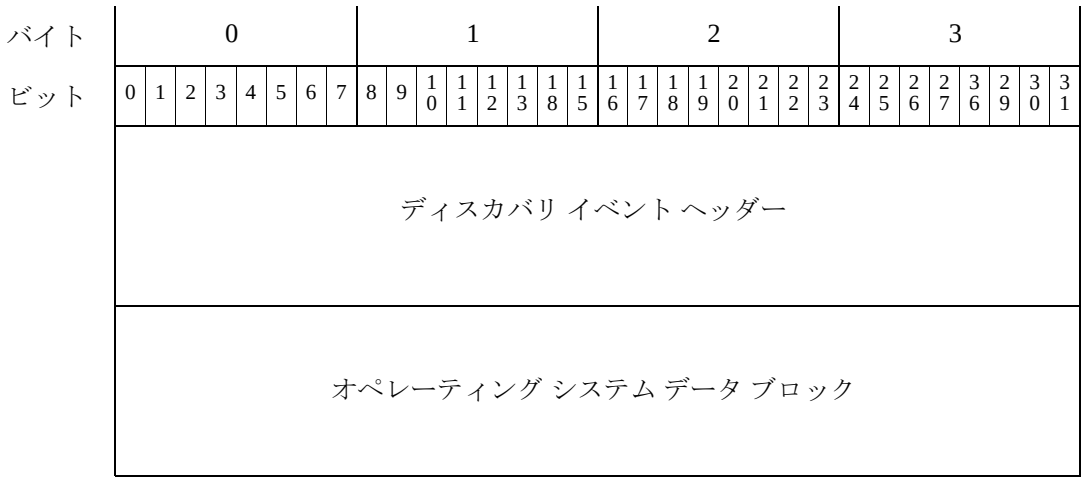
次の場合は、IP アドレスに（IP アドレス オクテット）16 バイトを使用します。

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



オペレーティング システム更新メッセージ

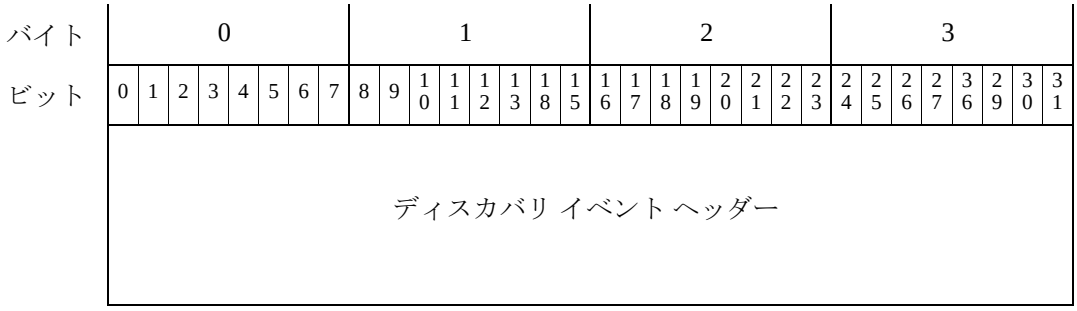
OS 情報更新イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照）があり、オペレーティング システム データ ブロック（オペレーティング システム データ ブロック 3.5+（4-91 ページ） を参照。シリーズ 1 のブロック タイプ 53）がそれに続きます。



IP アドレスを再利用とホスト タイムアウト/削除メッセージ

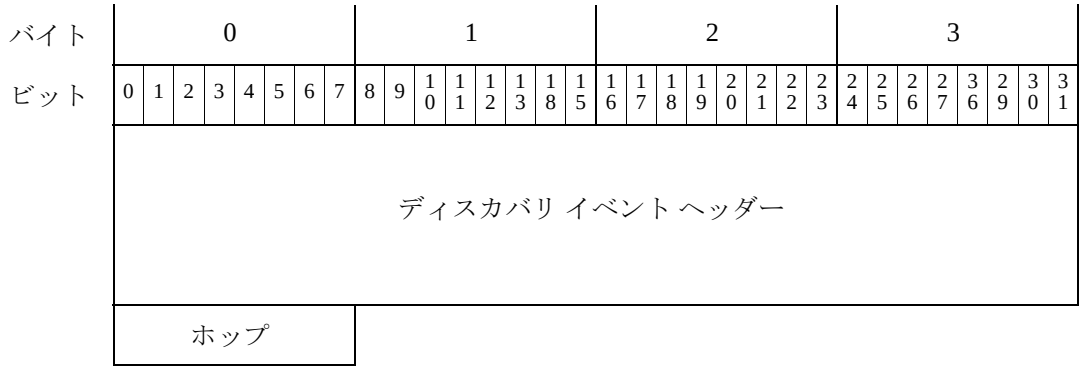
次のホスト イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照）があります。他にデータはありません。

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



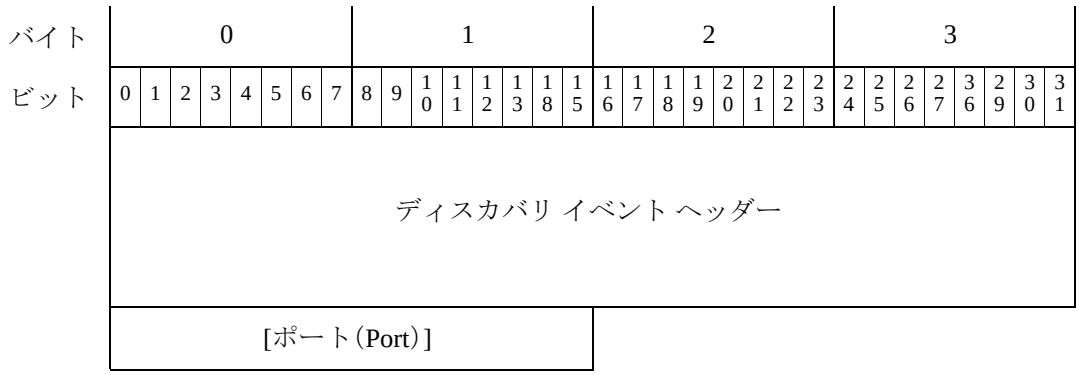
ホップ変更メッセージ

ホップ変更イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照）があります。ホップ カウントの 1 バイト フィールドがそれに続きます。



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

TCP ポートと UDP のポート クローズ メッセージ/タイムアウト メッセージは、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照）があり、ポート番号の 2 バイトがそれに続きます。

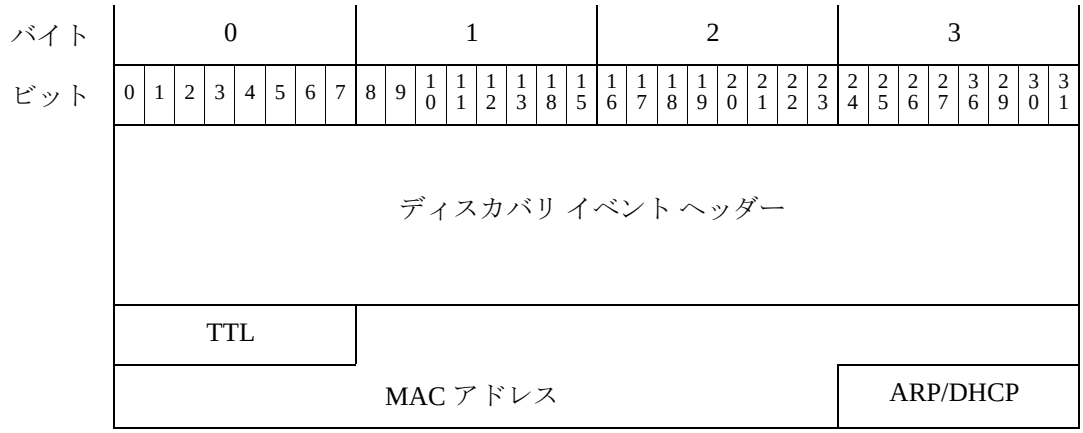


MAC アドレス メッセージ

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

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

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

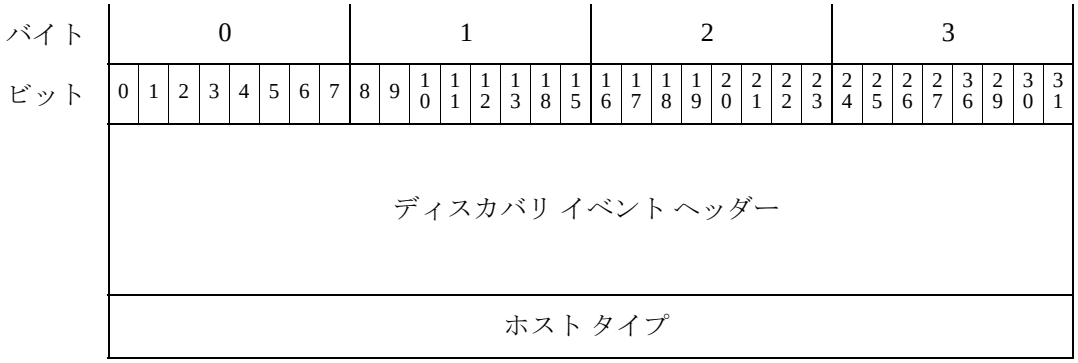


ブリッジ/ルータとして識別したホスト メッセージ

ブリッジ/ルータのイベントとして識別したホスト メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+(4-42 ページ) を参照）があり、ホスト タイプと一致する値の 4 バイト フィールドが続きます。

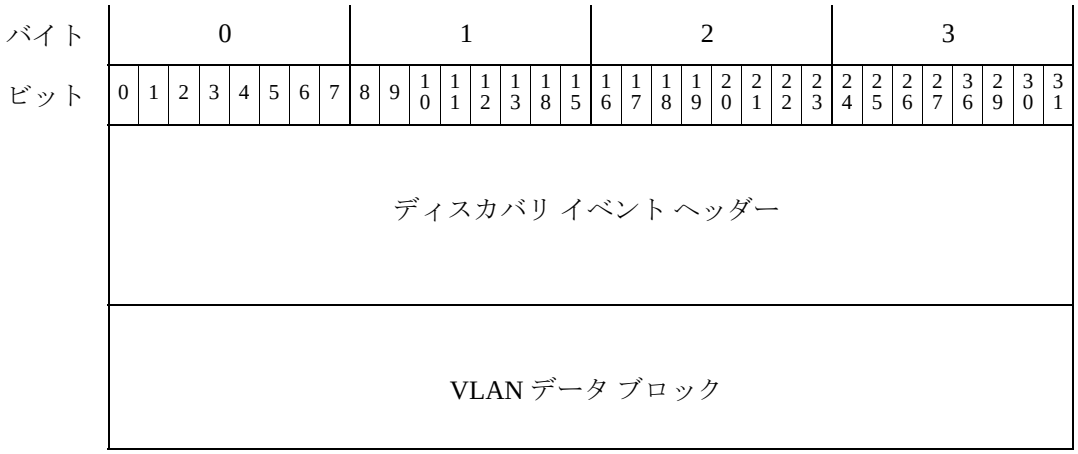
- 0：ホスト

- 1 — ルータ
- 2:ブリッジ



VLAN タグ情報更新メッセージ

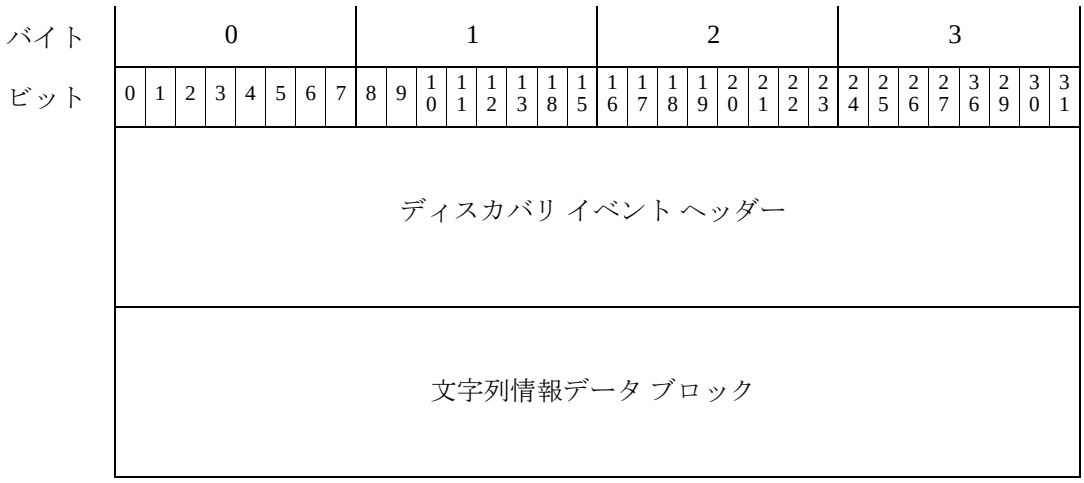
VLAN タグ情報更新イベントには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）があり、VLAN データ ブロックが続きます（VLAN データ ブロック（4-82 ページ）を参照）。VLAN データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 14 です。



NetBIOS 名変更メッセージ

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

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



更新バナー メッセージ

更新バナー イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）があり、サーバー バナーのデータ ブロックがそれに続きます（サーバー バナー データ ブロック（4-82 ページ）を参照）。サーバー バナーのデータ ブロックのブロック タイプは、シリーズ 1 のブロック タイプ 37 です。

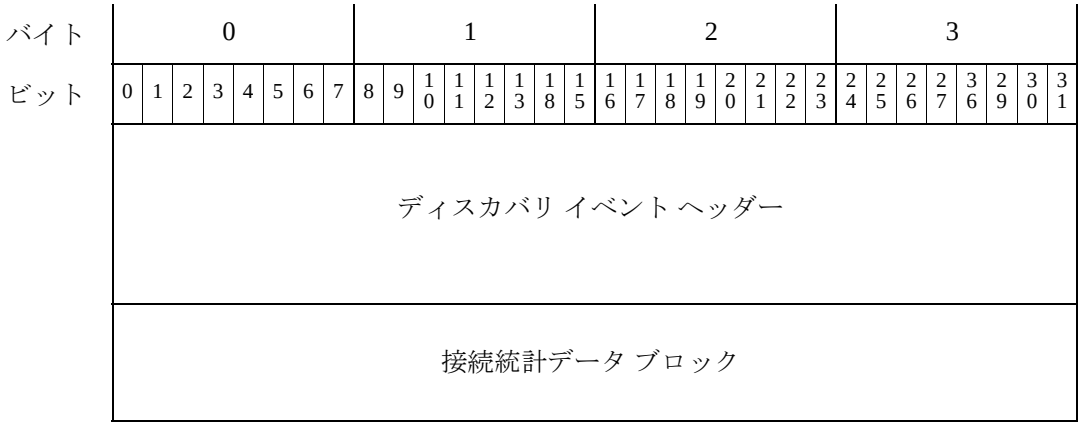
ポリシー制御の概要

ポリシー制御ポリシー イベントには、標準ディスカバリ イベント ヘッダーがあり（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）、ポリシー制御メッセージ データ ブロックがそれに続きます。ポリシー制御メッセージ データ ブロックの形式はシステム バージョンによって異なります。現行バージョンのポリシー制御メッセージ データ ブロック形式については、ポリシー エンジン制御メッセージ データ ブロック（4-92 ページ）を参照してください。

接続統計データ メッセージ

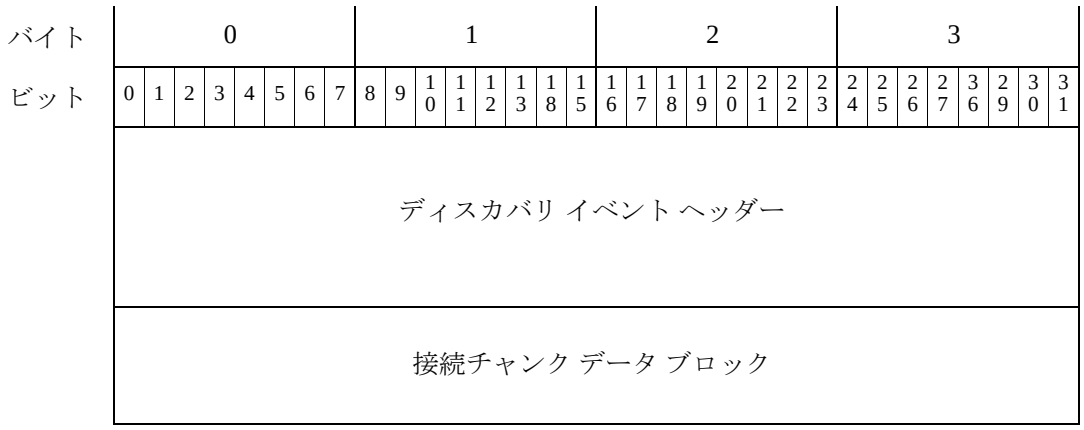
接続統計イベントには、標準ディスカバリ イベント ヘッダーがあり（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照）、接続統計データ ブロックがそれに続きます。接続統計データ ブロックの各バージョンのドキュメントには、それを使用するシステム バージョンを格納します。バージョンの 6.1+ の接続統計データ ブロックの形式については、接続統計データ ブロック 7.1+（4-125 ページ）を参照してください。

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



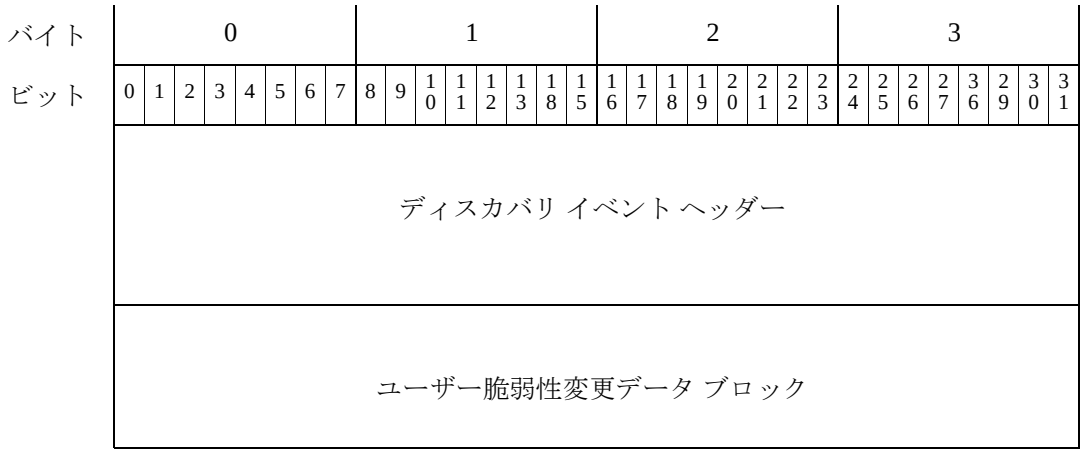
接続チャンク メッセージ

接続チャンク イベントには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照）があり、接続チャンク データ ブロックがそれに続きます。形式は、システム バージョンによって異なります。現行バージョンの接続チャンク データ ブロックの形式については、6.1+ の接続チャンク データ ブロック（4-106 ページ） を参照してください。接続チャンク データ ブロックのブロック タイプは、シリーズ 1 のブロック タイプ 136 です。



バージョン4.6.1+ のユーザー設定脆弱性メッセージ

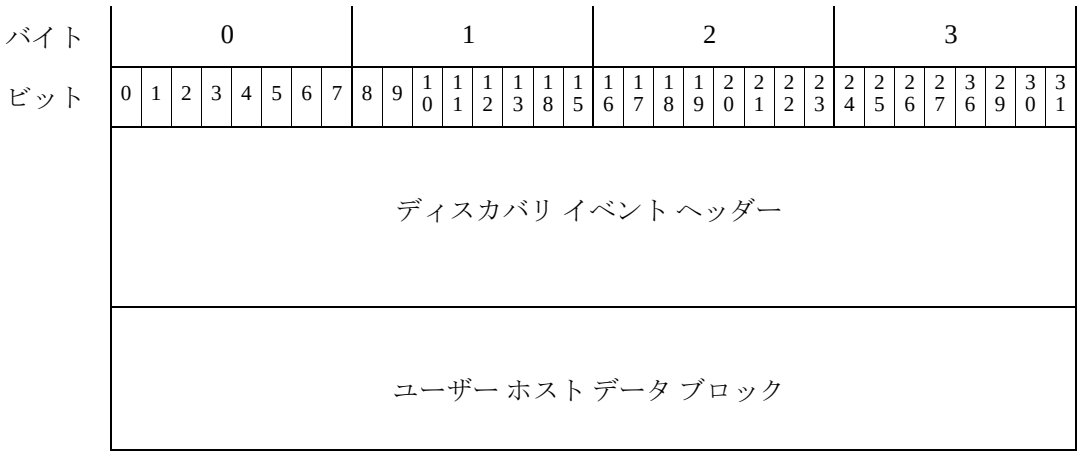
ユーザー設定の有効な脆弱性、ユーザー設定の無効な脆弱性、ユーザー脆弱性資格メッセージは、同じデータ形式を使用します。すなわち、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）にユーザー脆弱性変更データ ブロックが続きます（ユーザー脆弱性変更データ ブロック 4.7+（4-113 ページ）を参照。シリーズ 1 のブロック タイプ 80）。これらはレコード タイプ、イベント タイプ、イベント サブタイプで区別します。



ユーザー追加/削除ホスト メッセージ

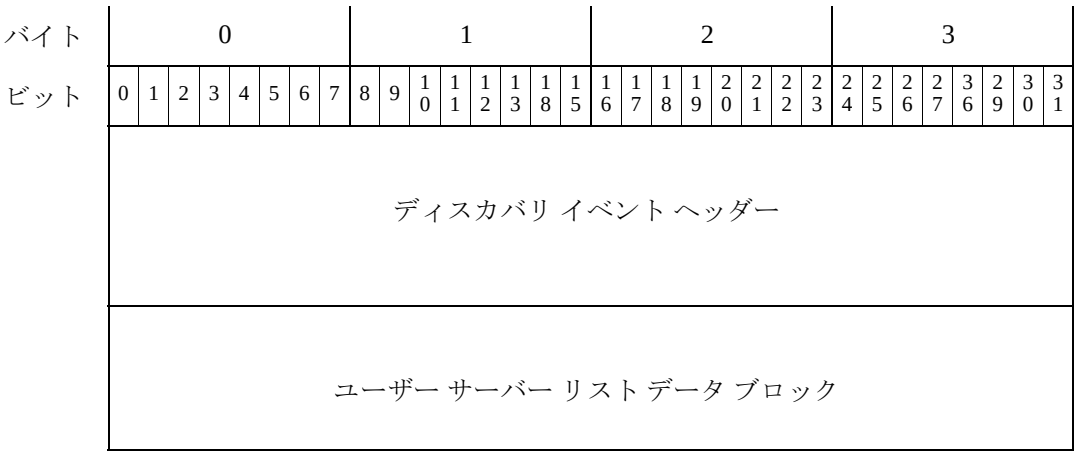
次のホスト入力イベント メッセージには、標準ディスカバリ イベント ヘッダーがあり（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）、ユーザー ホスト データ ブロックがそれに続きます（ユーザー ホスト データ ブロック 4.7+（4-111 ページ）を参照。シリーズ 1 のブロック タイプ 78）。

- ユーザー削除アドレス
- ユーザー追加ホスト



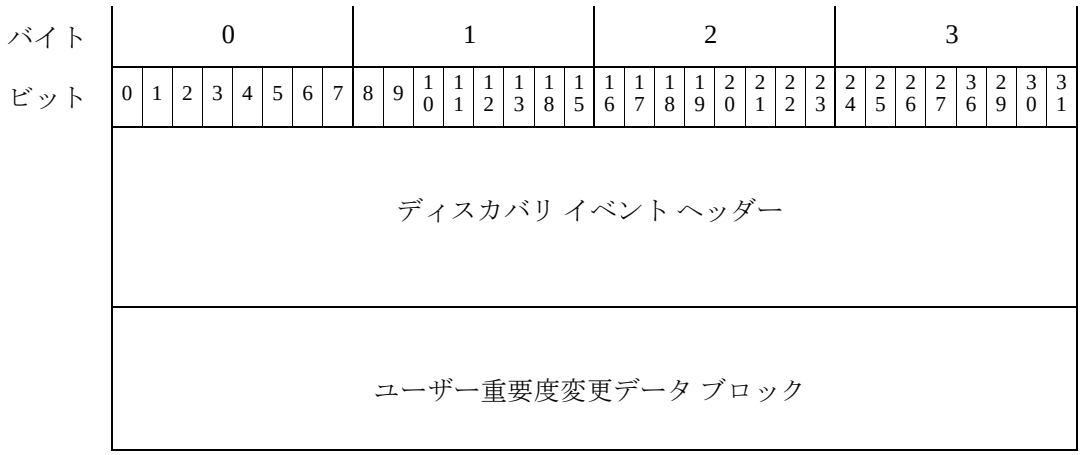
ユーザー削除サーバー メッセージ

ユーザー削除サーバー メッセージには、標準ディスカバリ イベント ヘッダーがあり（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）、ユーザー サーバー リスト データ ブロックがそれに続きます（ユーザー サーバー リスト データ ブロック（4-110 ページ）を参照）。ユーザー サーバー リスト データ ブロックはシリーズ 1 のブロック タイプ 77 です。



ユーザー設定ホスト重要度メッセージ

ユーザー設定ホスト重要度メッセージには、標準ディスカバリ イベント ヘッダーがあり（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）、ユーザー重要度変更データ ブロックがそれに続きます（ユーザー重要度変更データ ブロック 4.7+（4-114 ページ）を参照）。ユーザー重要度変更データ ブロックのブロック タイプは、シリーズ 1 ブロック タイプ 81 です。



属性メッセージ

次のイベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）があり、属性定義データ ブロック（4.7+ の定義属性データ ブロック（4-93 ページ）を参照。シリーズ 1 ブロック タイプ 55）がそれに続きます。

- ホスト属性を追加
- ホスト属性を更新
- ホスト属性を削除

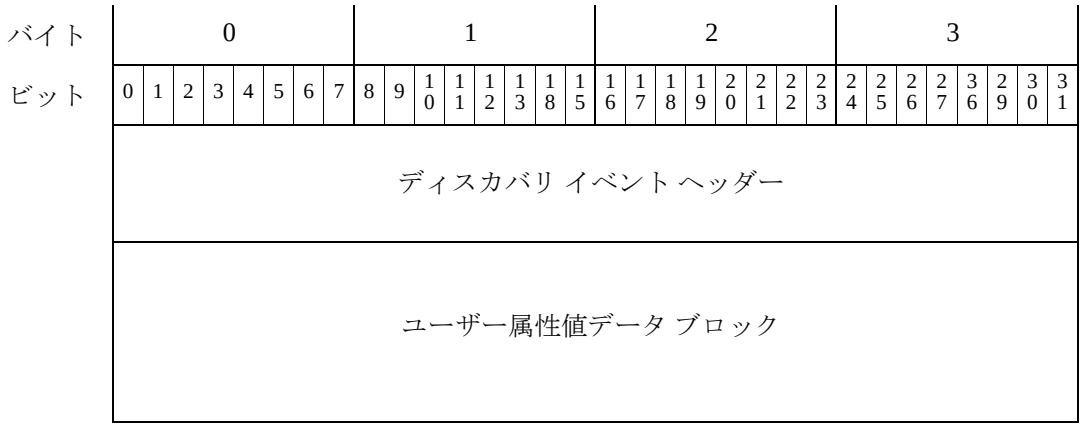
これらのイベントは、それぞれ次の形式を使用します:

属性値メッセージ

次のイベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）があり、ユーザー属性値データ ブロック（ユーザー属性値データ ブロック 4.7+（4-116 ページ）を参照。シリーズ 1 ブロック タイプ 82）がそれに続きます。

- ホスト属性値を設定
- ホスト属性地を削除

これらのイベントは、それぞれ次の形式を使用します:

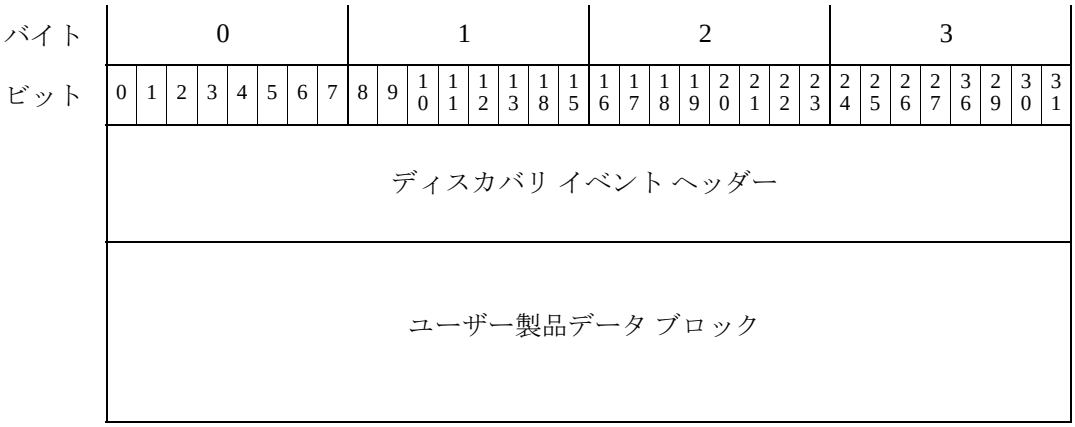


ユーザー サーバー メッセージとオペレーティング システム メッセージ

次のイベント メッセージには、標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-42 ページ) を参照)があり、ユーザー製品データ ブロック(ユーザー製品データ ブロック 5.1+(4-183 ページ) を参照。シリーズ 1 ブロック タイプ 60)がそれに続きます。

- オペレーティング システム定義を設定
- サーバー定義を設定
- サーバーの追加(Add Server)

これらのイベントは、それぞれ次の形式を使用します:

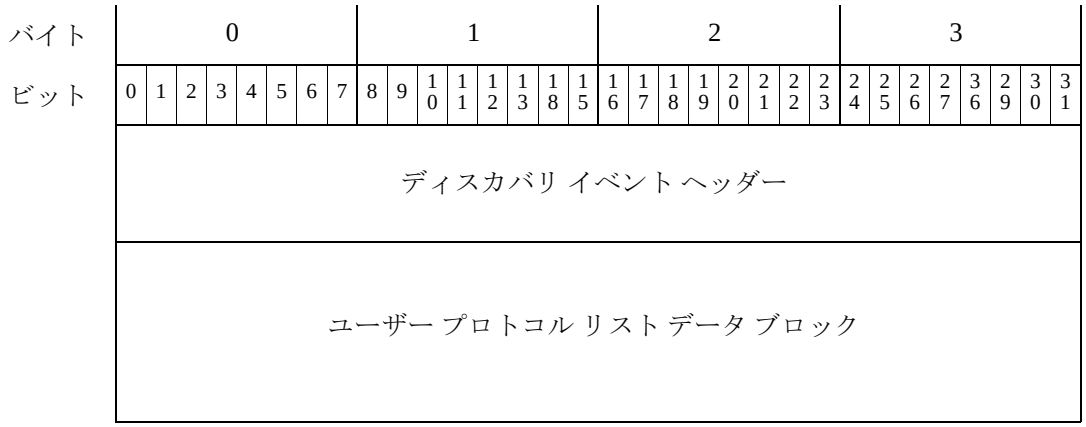


ユーザー プロトコル メッセージ

次のイベント メッセージには、標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-42 ページ) を参照)があり、ユーザー プロトコル リスト データ ブロック(ユーザー プロトコル リスト データ ブロック 4.7+(4-118 ページ) を参照。シリーズ 1 ブロック タイプ 83)がそれに続きます。

- プロトコルを削除
- プロトコルを追加

これらのイベントは、それぞれ次の形式を使用します:

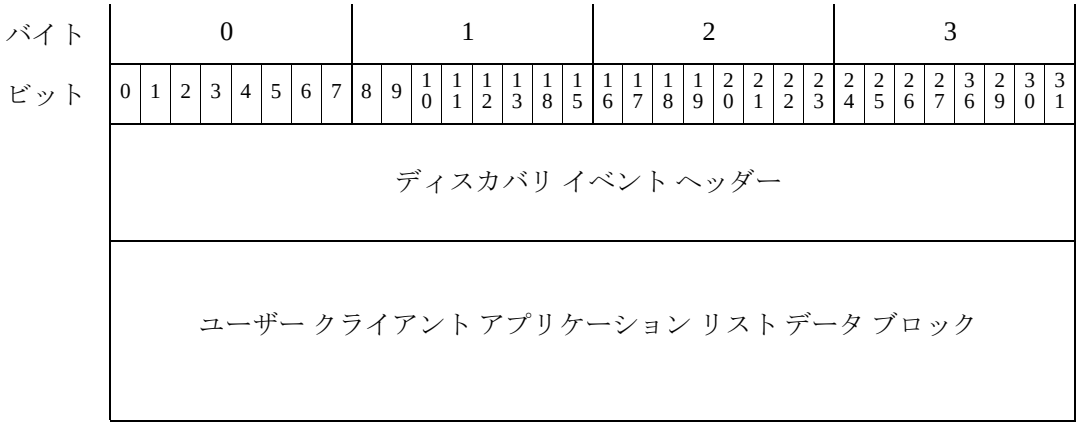


ユーザー クライアント アプリケーション メッセージ

次のイベント メッセージには、標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-42 ページ) を参照)があり、ユーザー クライアント アプリケーション リスト データ ブロック(ユーザー クライアント アプリケーション リスト データ ブロック(4-99 ページ) を参照。シリーズ 1 ブロック タイプ 60)がそれに続きます。

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

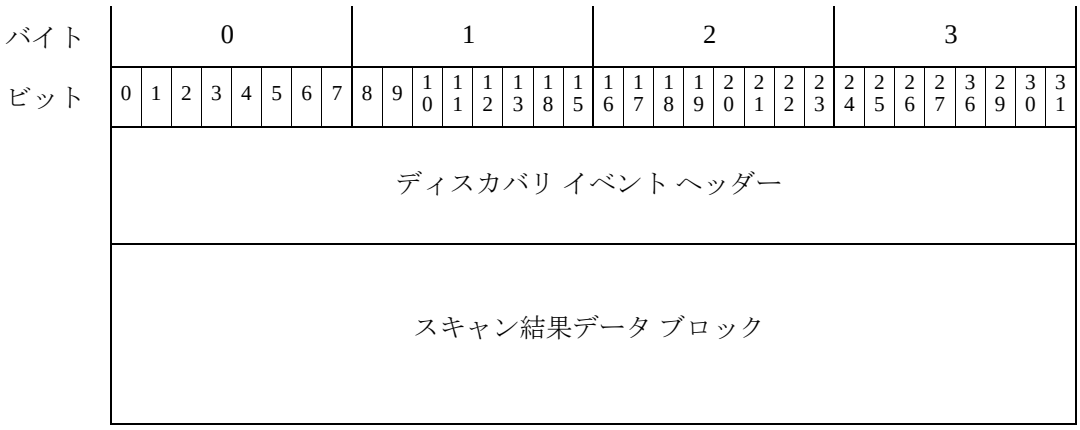
これらのイベントは、それぞれ次の形式を使用します:



スキャン結果を追加メッセージ

スキャン結果を追加イベント メッセージには、標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-42 ページ) を参照)があり、スキャン結果データ ブロックがそれに続きます(スキャン結果データ ブロック 5.2+(4-146 ページ) を参照)。スキャン結果データ ブロックのブロック タイプは、シリーズ 1 ブロック タイプ 142 です。

このイベントでは、次の形式を使用します。



新規オペレーティング システム メッセージ

新規 OS イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照）があり、オペレーティング システム フィンガープリント データ ブロックがそれに続きます（オペレーティング システム フィンガープリント データ ブロック 5.1+（4-172 ページ） を参照）。

このイベントでは、次の形式を使用します。

アイデンティティ競合とアイデンティティ タイムアウト システム メッセージ

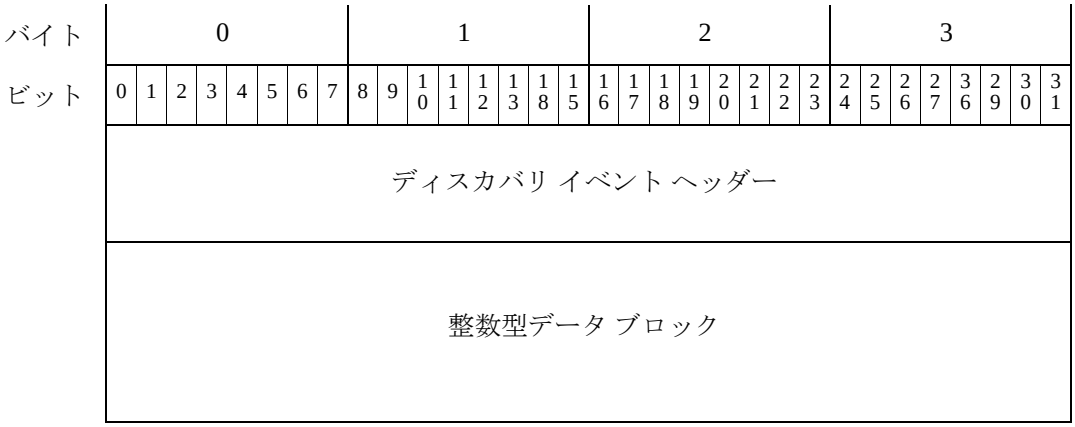
アイデンティティ競合イベント メッセージとアイデンティティ タイムアウト イベント メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ） を参照）があり、アイデンティティ データ ブロックがそれに続きます（アイデンティティ データ ブロック（4-120 ページ） を参照）。アイデンティティ データ ブロックのブロック タイプは、シリーズ 1 ブロック タイプ 94 です。これらのメッセージは、フィンガープリント送信元アイデンティティで競合またはタイムアウトが発生すると生成されます。

このイベントでは、次の形式を使用します。

ホスト IOC セット メッセージ

ホスト IOC セット メッセージには、標準ディスカバリ イベント ヘッダー（ディスカバリ イベント ヘッダー 5.2+（4-42 ページ）を参照）があり、整数型データ ブロックがそれに続きます（整数型（INT32）データ ブロック（4-81 ページ）を参照）。この整数型データ ブロックには、ホストの IOC セットの ID 番号を格納します。

このイベントでは、次の形式を使用します。



イベント タイプ別のユーザー データ構造

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

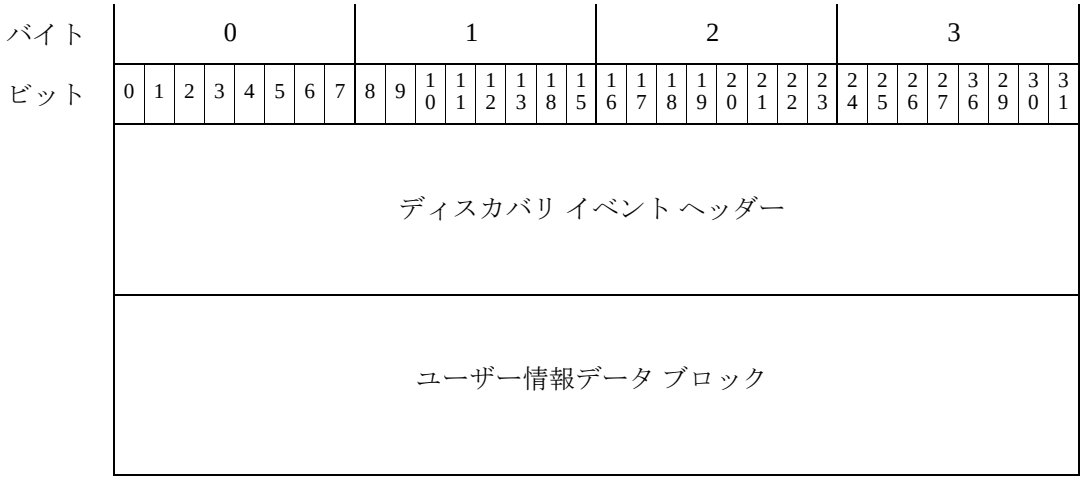
- ユーザー変更メッセージ（4-64 ページ）
- ユーザー情報更新メッセージ ブロック（4-64 ページ）

ユーザー変更メッセージ

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

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

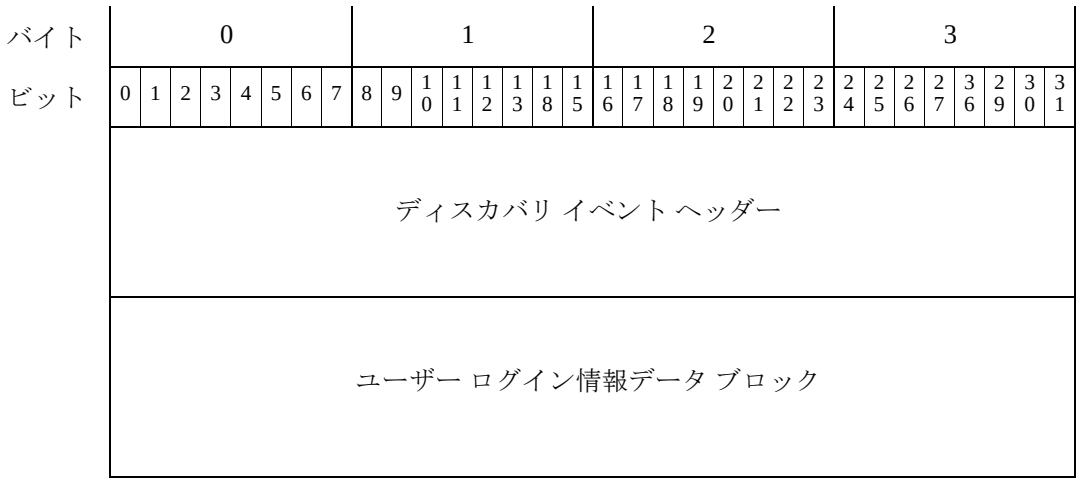
ユーザー変更イベント メッセージには、標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-42 ページ) を参照)があり、ユーザー情報データ ブロックがそれに続きます(6.0+ の情報データ ユーザー ブロック(4-201 ページ) を参照)。ユーザー情報データ ブロックはシリーズ 1 ブロック タイプ 120 です。



ユーザー情報更新メッセージ ブロック

システムがユーザーのログインの変更(ユーザー ログイン イベント — イベント タイプ 1004、サブタイプ2)を検出すると、ユーザー情報更新メッセージが送信されます。このブロックは、ユーザーがログインに失敗したとき(失敗したユーザーのログイン イベント:イベント タイプ 1004、サブタイプ 5)、VPN ユーザーがログインするとき(VPN ユーザーのログイン イベント:イベント タイプ 1004、サブタイプ 8)、または VPN ユーザーがログオフするとき(VPN ユーザーのログオフ イベント:イベント タイプ 1004、サブタイプ 9)にも使用されます。

ユーザー情報更新イベント メッセージには標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-42 ページ) を参照)とユーザー ログイン情報データ ブロックがあります(ユーザー ログイン情報データ ブロック 6.2+(4-207 ページ) を参照)。ユーザー ログイン情報データ ブロックのブロック タイプは、シリーズ 1 ブロック タイプ 121 です。

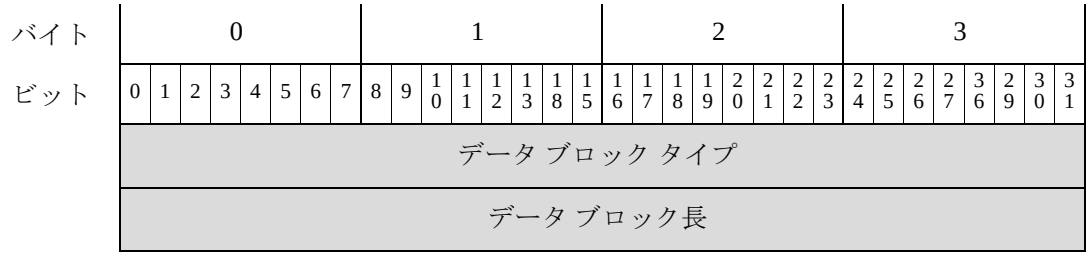


ディスカバリ（シリーズ1）ブロック

ほとんどのディスカバリ イベントと接続イベントには、シリーズ 1 グループ データ構造の 1 つ以上のデータ ブロックがあります。シリーズ 1 データ ブロック タイプは、それぞれ特定の情報タイプを伝えます。ブロック タイプ番号は、ブロックのデータにするデータに先行するデータ ブロック ヘッダーにあります。ブロック ヘッダー形式については、データ ブロック ヘッダー（2-29 ページ）を参照してください。

シリーズ 1 データ ブロック ヘッダー シリーズ

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



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

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

シリーズ 1 プリミティブ データ ブロック

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

- 文字列データ ブロック (4-75 ページ)
- BLOB データ ブロック (4-76 ページ)
- リスト データ ブロック (4-77 ページ)
- 汎用リスト ブロック (4-78 ページ)

ホスト ディスカバリ データ ブロックと接続データ ブロック

ホスト ディスカバリ イベントと接続イベント ブロック タイプのリストについては、表 4-30 (4-66 ページ) を参照してください。ユーザー イベント ブロック タイプについては、表 4-86 (4-191 ページ) を参照してください。これらはすべてシリーズ 1 データ ブロックです。

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

表 4-30　　ホスト ディスカバリと接続データ ブロック タイプ

タイプ (Type)	目次	データ ブロック ステータス	説明
[0]	文字列	現在 (Current)	文字列データを格納します。詳細については、文字列データ ブロック (4-75 ページ) を参照してください。
1	サブサーバー	現在 (Current)	サーバーで検出したサブサーバーに関する情報を格納します。詳細については、サブサーバー データ ブロック (4-78 ページ) を参照してください。
4	プロトコル	現在 (Current)	プロトコル データを格納します。詳細については、「プロトコル データ ブロック (4-80 ページ)」を参照してください。
7	整数型データ	現在 (Current)	整数型 (数値) データを格納します。詳細については、整数型 (INT32) データ ブロック (4-81 ページ) を参照してください。
10	BLOB	現在 (Current)	バイナリ データの生ブロックを格納し、主にバナーに使用します。詳細については、BLOB データ ブロック (4-76 ページ) を参照してください。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ（続き）

タイプ（Type）	目次	データ ブロック ステータス	説明
11	リスト	現在（Current）	その他のデータ ブロック リストを含みます。詳細については、リスト データ ブロック（4-77 ページ）を参照してください。
14	VLAN	現在（Current）	VLAN 情報を格納します。詳細については、VLAN データ ブロック（4-82 ページ）を参照してください。
20	侵入の影響アラート	現在（Current）	侵入影響アラート情報を格納します。侵入影響イベントアラートのヘッダーは、他のデータ ブロックは若干異なります。詳細については、侵入の影響アラート データ 5.3 以上（3-20 ページ）を参照してください。
31	汎用リスト	現在（Current）	たとえば、クライアント アプリケーション ブロックなど、カプセル化する汎用リスト情報をブロック リストをホスト プロファイル ブロックに格納します。詳細については、汎用リスト ブロック（4-78 ページ）を参照してください。
35	文字列情報	現在（Current）	文字列情報を格納します。たとえば、スキャン脆弱性データ ブロックで使用すると、文字列情報データ ブロックには CVE ID 番号データが格納されます。文字列情報データ ブロック（4-83 ページ）を参照してください。
37	サーバー バナー	現在（Current）	サーバー バナー データを格納します。詳細については、サーバー バナー データ ブロック（4-82 ページ）を参照してください。
38	属性アドレス	レガシー	ホスト属性アドレスを格納します（本製品の旧バージョンを参照のこと）。サクセサ ブロックは 146 です。
39	属性リスト項目	現在（Current）	ホスト属性リスト項目値を格納します。詳細については、属性リスト項目データ ブロック（4-87 ページ）を参照してください。
54	ホスト クライアント アプリケーション	レガシー	新規クライアント アプリケーション イベントのクライアント アプリケーション情報を格納します（本製品の旧バージョンを参照のこと）。
47	フル ホスト プロファイル	レガシー	ホスト プロファイル情報一式を格納します（本製品の旧バージョンを参照のこと）。
48	属性値（Attribute Value）	現在（Current）	ホスト属性の ID 番号と値を格納します。詳細については、属性値データ ブロック（4-87 ページ）を参照してください。
51	フル サブサーバー	現在（Current）	サーバーで検出したサブサーバーに関する情報を格納します。フル サーバー情報ブロックとフル ホスト プロファイルで参照します。各サブサーバーの脆弱性情報を格納します。詳細については、フル サブサーバー データ ブロック（4-89 ページ）を参照してください。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ（続き）

タイプ（Type）	目次	データ ブロック ステータス	説明
53	オペレーティング システム（Operating System）	現在（Current）	バージョン 3.5+ のオペレーティング システム情報を格納します。詳細については、オペレーティング システム データ ブロック 3.5+（4-91 ページ）を参照してください。
54	ポリシー エンジン制御メッセージ	現在（Current）	ユーザー ポリシー制御の変更に関する情報を格納します。詳細については、ポリシー エンジン制御メッセージ データ ブロック（4-92 ページ）を参照してください。
55	属性定義	現在（Current）	属性定義の情報を格納します。詳細については、4.7+ の定義属性データ ブロック（4-93 ページ）を参照してください。
72	接続統計情報	レガシー	4.7 ～ 4.9.0 の接続統計イベントの情報を格納します（本製品の旧バージョンを参照のこと）。
57	ユーザー プロトコル	現在（Current）	ユーザー入力のプロトコル情報を格納します。詳細については、ユーザー プロトコル データ ブロック（4-96 ページ）を参照してください。
59	ユーザー クライアント アプリケーション	レガシー	ユーザー入力のクライアント アプリケーション データを格納します。詳細については、ユーザー クライアント アプリケーション データ ブロック 5.0 ～ 5.1（B-130 ページ）を参照してください。ブロック 138 に置き換わります。
60	ユーザー クライアント アプリケーション リスト	現在（Current）	ユーザー クライアント アプリケーション データ ブロックのリストを格納します。詳細については、ユーザー クライアント アプリケーション リスト データ ブロック（4-99 ページ）を参照してください。
61	IP 範囲指定	レガシー	IP アドレス範囲指定を格納します。詳細については、IP 範囲仕様データ ブロック 5.0 ～ 5.1.1.x（B-415 ページ）を参照してください。ブロック 141 に置き換わります。
62	属性指定	現在（Current）	属性名と値を格納します。詳細については、属性指定データ ブロック（4-102 ページ）を参照してください。
63	MAC アドレス指定	現在（Current）	MAC アドレス範囲指定を格納します。詳細については、MAC アドレス指定データ ブロック（4-104 ページ）を参照してください。
64	IP アドレス指定	現在（Current）	IP と MAC アドレス指定ブロック リストを格納します。詳細については、アドレス指定データ ブロック（4-105 ページ）を参照してください。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ（続き）

タイプ（Type）	目次	データ ブロック ステータス	説明
65	ユーザー製品	レガシー	サードパーティ アプリケーション文字列マッピングなど、サードパーティ アプリケーションからインポートしたホスト入力データを格納します。詳細については、ユーザー製品データ ブロック 5.0.x（B-134 ページ）を参照してください。5.0 で導入したサクセサ ブロック タイプ 118 には、ブロック タイプ 65 と同じ構成があります。
66	接続チャンク	レガシー	接続チャンク情報を格納します。詳細については、接続チャンク データ ブロック 5.0 ～ 5.1（B-186 ページ）を参照してください。5.0 で導入したサクセサ ブロック タイプ 119 には、ブロック タイプ 66 と同じ構成があります。
67	フィックス リスト	現在（Current）	ホストに適用するフィックスを格納します。詳細については、フィックス リスト データ ブロック（4-108 ページ）を参照してください。
71	汎用スキャン結果	レガシー	Nmap スキャンの結果を格納します（本製品の旧バージョンを参照のこと）。
72	スキャン結果	レガシー	サードパーティ スキャンの結果を格納します（本製品の旧バージョンを参照のこと）。
76	ユーザー サーバー	現在（Current）	ユーザー入力イベントのサーバー情報を格納します。詳細については、ユーザー サーバー データ ブロック（4-109 ページ）を参照してください。
77	ユーザー サーバー リスト	現在（Current）	ユーザー サーバー ブロックのリストを格納します。詳細については、ユーザー サーバー リスト データ ブロック（4-110 ページ）を参照してください。
78	ユーザー ホスト	現在（Current）	ユーザー ホスト入力イベントからのホスト範囲に関する情報を格納します。詳細については、ユーザー ホスト データ ブロック 4.7+（4-111 ページ）を参照してください。
79	ユーザー脆弱性	レガシー	ホスト脆弱性に関する情報を格納します（本製品の旧バージョンを参照のこと）。バージョン 5.0 で導入したサクセサ ブロックのブロック タイプは 124 です。
80	ユーザー ホスト脆弱性の変更	現在（Current）	非アクティブ化した脆弱性のリスト、またはアクティブ化した脆弱性のリストを格納します。詳細については、ユーザー脆弱性変更データ ブロック 4.7+（4-113 ページ）を参照してください。
81	ユーザー重要度	現在（Current）	ホストまたはホストの重要度の変更に関する情報を格納します。詳細については、ユーザー重要度変更データ ブロック 4.7+（4-114 ページ）を参照してください。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ（続き）

タイプ（Type）	目次	データ ブロック ステータス	説明
82	ユーザー属性値	現在（Current）	ホストの属性値の変更を格納します。詳細については、ユーザー属性値データ ブロック 4.7+（4-116 ページ）を参照してください。
83	ユーザー プロトコル リスト	現在（Current）	ホストのプロトコル リストを示します。詳細については、ユーザー プロトコル リスト データ ブロック 4.7+（4-118 ページ）を参照してください。
85	脆弱性リスト	現在（Current）	ホストに適用する脆弱性を格納します。詳細については、ホスト脆弱性データ ブロック 4.9.0+（4-119 ページ）を参照してください。
86	スキャン脆弱性	レガシー	スキャンで検出した脆弱性に関する情報を格納します（本製品の旧バージョンを参照のこと）。
87	オペレーティング システム フィンガープリント	レガシー	オペレーティング システム フィンガープリントのリストを格納します。詳細については、オペレーティング システム フィンガープリント データ ブロック 5.0 ～ 5.0.2（B-166 ページ）を参照してください。バージョン 5.1 で導入したサクセサ ブロックのブロック タイプは 130 です。
88	サーバー情報	レガシー	サーバー フィンガープリントで使用するサーバー情報を格納します（本製品の旧バージョンを参照のこと）。
89	ホスト/サーバー	レガシー	ホスト サーバー情報を格納します（本製品の旧バージョンを参照のこと）。
90	フル ホスト サーバー	レガシー	ホスト サーバー情報を格納します（本製品の旧バージョンを参照のこと）。
91	ホスト プロファイル	レガシー	ホストのプロファイル情報を格納します。詳細については、ホスト プロファイル データブロック 5.2+（4-175 ページ）を参照してください。バージョン 5.1 で導入したサクセサ ブロックのブロック タイプは 132 です。
92	フル ホスト プロファイル	レガシー	ホスト プロファイル情報一式を格納します（本製品の旧バージョンを参照のこと）。データ ブロック 47 に置き換わります。
94	アイデンティティ データ	現在（Current）	ホストのアイデンティティ データを格納します。詳細については、アイデンティティ データ ブロック（4-120 ページ）を参照してください。
95	ホスト MAC アドレス	現在（Current）	ホストの MAC アドレス情報を格納します。詳細については、ホスト MAC アドレス 4.9+（4-122 ページ）を参照してください。
96	セカンダリ ホスト更新	現在（Current）	セカンダリ セカンダリ ホストの更新（4-123 ページ）で報告された MAC アドレス情報のリストを格納します。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ（続き）

タイプ（Type）	目次	データ ブロック ステータス	説明
97	Web アプリケーション（Web Application）	レガシー	Web アプリケーション データのリストを格納します（本製品の旧バージョンを参照のこと）。バージョン 5.0 で導入したサクセサ ブロックのブロック タイプは 123 です。
98	ホスト/サーバー	レガシー	ホスト サーバー情報を格納します（本製品の旧バージョンを参照のこと）。
99	フル ホスト サーバー	レガシー	ホスト サーバー情報を格納します（本製品の旧バージョンを参照のこと）。
100	ホスト クライアント アプリケーション	レガシー	新規クライアント アプリケーション イベントのクライアント アプリケーション情報を格納します（本製品の旧バージョンを参照のこと）。バージョン 5.0 で導入したサクセサ ブロック タイプ 122 には、ブロック タイプ 100 と同じ構造があります。
101	接続統計情報	レガシー	4.9.1+ の接続統計イベントの情報を格納します（本製品の旧バージョンを参照のこと）。
102	スキャン結果	レガシー	脆弱性に関する情報を格納しており、スキャン結果を追加イベントで使用します。スキャン結果データ ブロック 5.0 ～ 5.1.1.x（B-132 ページ）を参照してください。
103	ホスト/サーバー	現在（Current）	ホスト サーバー情報を格納します。詳細については、ホスト サーバー データ ブロック 4.10.0+（4-149 ページ）を参照してください。
104	フル ホスト サーバー	現在（Current）	ホスト サーバー情報を格納します。詳細については、フル ホスト サーバー データ ブロック 4.10.0+（4-151 ページ）を参照してください。
105	サーバー情報	レガシー	サーバー フィンガープリントで使用するサーバー情報を格納します。詳細については、4.10.x、5.0 ～ 5.0.2 のサーバー情報データ ブロック（4-155 ページ）を参照してください。5.0 で導入したサクセサ ブロック タイプ 117 には、ブロック タイプ 105 と同じ構成があります。
106	フル サーバー情報	現在（Current）	ホストで検出したサーバーに関する情報を格納します。詳細については、フル サーバー情報データ ブロック（4-158 ページ）を参照してください。
108	汎用スキャン結果	現在（Current）	Nmap スキャンで得た結果を格納します。詳細については、4.10.0+ の汎用スキャン結果データ ブロック（4-160 ページ）を参照してください。
109	スキャン脆弱性	現在（Current）	サードパーティ スキャンで検出した脆弱性に関する情報を格納します。4.10.0+のスキャン脆弱性データ ブロック（4-162 ページ）を参照してください。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ（続き）

タイプ（Type）	目次	データ ブロック ステータス	説明
111	フル ホスト プロファイル	レガシー	ホスト プロファイル情報一式を格納します。詳細については、フル ホスト プロファイル データ ブロック 5.0 ～ 5.0.2（B-374 ページ）を参照してください。データ ブロック 92 に置き換わります。
112	フル ホスト クライアント アプリケーション	現在（Current）	脆弱性リストとともに新規クライアント アプリケーション イベントのクライアント アプリケーション情報を格納します。詳細については、フル クライアント アプリケーション データ ブロック 5.0+（4-165 ページ）を参照してください。
115	接続統計情報	レガシー	5.0 ～ 5.0.2 の接続統計イベントの情報を格納します。詳細については、接続統計データ ブロック 5.0 ～ 5.0.2（B-168 ページ）を参照してください。バージョン 5.1 で導入したサクセサ ブロックのブロック タイプは 126 です。
117	サーバー情報	現在（Current）	サーバー フィンガープリントで使用するサーバー情報を格納します。詳細については、4.10.x、5.0 ～ 5.0.2 のサーバー情報データ ブロック（4-155 ページ）を参照してください。
118	ユーザー製品	レガシー	サードパーティ アプリケーション文字列マッピングなど、サードパーティ アプリケーションからインポートしたホスト入力データを格納します。詳細については、ユーザー製品データ ブロック 5.0.x（B-134 ページ）を参照してください。先行ブロック タイプ 65 は 5.0 で更新され、このブロック タイプと同じ構造があります。バージョン 5.1 で導入したサクセサ ブロックのブロック タイプは 132 です。
119	接続チャンク	レガシー	バージョン 4.10.1 ～ 5.1 の接続チャンク情報を格納します。詳細については、接続チャンク データ ブロック 5.0 ～ 5.1（B-186 ページ）を参照してください。サクセサ ブロックは 136 です。
122	ホスト クライアント アプリケーション	現在（Current）	バージョン 5.0 + の新規クライアント アプリケーション イベントのクライアント アプリケーション情報を格納します。詳細については、5.0+ のホスト クライアント アプリケーション データ ブロック（4-167 ページ）を参照してください。これはブロック タイプ 100 に置き換わります。
123	Web アプリケーション（Web Application）	現在（Current）	バージョン 5.0 +の Web アプリケーション データを格納します。詳細については、5.0+の Web アプリケーション データ ブロック（4-124 ページ）を参照してください。これはブロック タイプ 97 に置き換わります。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ（続き）

タイプ（Type）	目次	データ ブロック ステータス	説明
124	ユーザー脆弱性	現在（Current）	ホスト脆弱性に関する情報を格納します。ユーザー脆弱性データ ブロック 5.0+（4-169 ページ）を参照してください。これはブロック タイプ 79 に置き換わります。
125	接続統計情報	レガシー	4.10.2 の接続統計イベントの情報を格納します（本製品の旧バージョンを参照のこと）。バージョン 5.1 で導入したサクセサ ブロックのブロック タイプは 115 です。
126	接続統計情報	レガシー	5.1 の接続統計イベントの情報を格納します。詳細については、接続統計データ ブロック 5.1（B-173 ページ）を参照してください。これはブロック タイプ 115 に置き換わります。このブロック タイプはブロック タイプ 137 に置き換わります。
130	オペレーティング システム フィンガープリント	現在（Current）	オペレーティング システム フィンガープリントのリストを格納します。詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-172 ページ）を参照してください。これはブロック タイプ 87 に置き換わります。
131	モバイルDevice情報	現在（Current）	検出したモバイル デバイスのハードウェアに関する情報を格納します。詳細については、5.1+ のモバイルDevice 情報データ ブロック（4-173 ページ）を参照してください。
132	ホスト プロファイル	レガシー	ホストのプロファイル情報を格納します。詳細については、フル ホスト プロファイル データ ブロック 5.2.x（B-395 ページ）を参照してください。これはブロック タイプ 91 に置き換わります。ブロック 139 に置き換わります。
134	ユーザー製品	現在（Current）	サードパーティ アプリケーション文字列マッピングなど、サードパーティ アプリケーションからインポートしたホスト入力データを格納します。詳細については、ユーザー製品データ ブロック 5.1+（4-183 ページ）を参照してください。これは先行ブロック タイプ 118 に置き換わります。
135	フル ホスト プロファイル	レガシー	ホスト プロファイル情報一式を格納します。詳細については、フル ホスト プロファイル データ ブロック 5.1.1（B-384 ページ）を参照してください。データ ブロック 111 に置き換わります。
136	接続チャンク	現在（Current）	接続チャンク情報を格納します。詳細については、6.1+ の接続チャンク データ ブロック（4-106 ページ）を参照してください。ブロック 119 に置き換わります。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ（続き）

タイプ（Type）	目次	データ ブロック ステータス	説明
137	接続統計情報	レガシー	5.1.1 の接続イベントの情報を格納します。詳細については、接続チャンク データ ブロック 5.0 ～ 5.1（B-186 ページ）を参照してください。これはブロック タイプ 126 に置き換わります。これはブロック タイプ 144 に置き換わります。
138	ユーザー クライアント アプリケーション	現在（Current）	ユーザー入力のクライアント アプリケーション データを格納します。詳細については、5.1.1+ のユーザー クライアント アプリケーション データ ブロック（4-98 ページ）を参照してください。これはブロック タイプに置き換わります。
139	ホスト プロファイル	現在（Current）	ホストのプロファイル情報を格納します。詳細については、ホスト プロファイル データブロック 5.2+（4-175 ページ）を参照してください。これはブロック タイプ 132 に置き換わります。
140	フル ホスト プロファイル	レガシー	ホスト プロファイル情報一式を格納します。詳細については、全ホスト プロファイル データ ブロック 5.3+（5-1 ページ）を参照してください。データ ブロック 135 に置き換わります。
141	IP 範囲指定	現在（Current）	IP アドレス範囲指定を格納します。詳細については、5.2+の IP アドレス範囲データ ブロック（4-101 ページ）を参照してください。これはブロック 61 に置き換わります。
142	スキャン結果	現在（Current）	脆弱性に関する情報を格納しており、スキャン結果を追加イベントで使用します。スキャン結果データ ブロック 5.2+（4-146 ページ）を参照してください。これはブロック 102 に置き換わります。
143	ホスト名/アドレス（Host IP）	現在（Current）	ホストの IP アドレスと最後の確認日時情報を格納します。詳細については、ホスト IP アドレス データ ブロック（4-103 ページ）を参照してください。
144	接続統計情報	レガシー	5.2.x. の接続イベントの情報を格納します。詳細については、接続統計データ ブロック 5.2.x（B-179 ページ）を参照してください。これはブロック タイプ 137 に置き換わります。
146	属性アドレス	現在（Current）	5.2+ のホスト属性アドレスを格納します。詳細については、属性アドレス データ ブロック 5.2+（4-84 ページ）を参照してください。これはブロック タイプ 38 に取って代わります。
148	ユーザー IOC の変更	Current	ユーザーの IOC への変更に関する情報が含まれています。詳細については、ユーザー IOC の変更データ ブロック 5.3+（4-85 ページ）を参照してください。

表 4-30　ホスト ディスカバリと接続データ ブロック タイプ（続き）

タイプ（Type）	目次	データ ブロック ステータス	説明
149	フル ホスト プロファイル	現在（Current）	ホスト プロファイル情報一式を格納します。詳細については、全ホスト プロファイル データ ブロック 5.3+（5-1 ページ）を参照してください。データ ブロック 135 に置き換わります。
152	接続統計情報	レガシー	5.3+ の接続イベントの情報を格納します。詳細については、接続統計データ ブロック 5.3（B-195 ページ）を参照してください。これはブロック タイプ 144 に置き換わります。
154	接続統計情報	レガシー	5.3 の接続イベントの情報を格納します。詳細については、接続統計データ ブロック 5.3.1（B-202 ページ）を参照してください。これはブロック タイプ 152 に置き換わります。
155	接続統計情報	レガシー	5.4 の接続イベントの情報を格納します。詳細については、接続統計データ ブロック 5.4（B-210 ページ）を参照してください。これはブロック タイプ 154 に置き換わります。
157	接続統計情報	レガシー	5.4.1 の接続イベントの情報を格納します。詳細については、接続統計データ ブロック 5.4.1（B-224 ページ）を参照してください。これはブロック タイプ 155 に置き換わります。
160	接続統計情報	レガシー	5.4.1 の接続イベントの情報を格納します。詳細については、接続統計データ ブロック 6.0.x（B-239 ページ）を参照してください。これはブロック タイプ 157 に置き換わります。
163	接続統計情報	現在（Current）	6.0+ の接続イベントの情報を格納します。詳細については、接続統計データ ブロック 7.1+（4-125 ページ）を参照してください。これはブロック タイプ 160 に置き換わります。

文字列データ ブロック

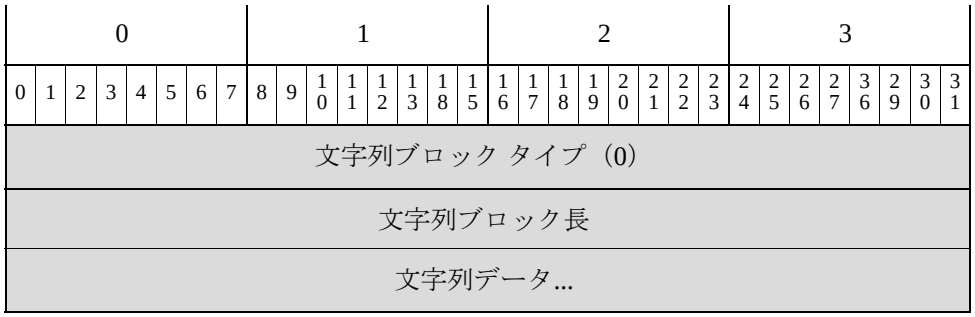
文字列データ ブロックは、シリーズ 1 ブロックの文字列データ送信に使用します。他のシリーズ 1 データ ブロックで、主に、たとえば、オペレーティング システムやサーバー名の記述に使用します。

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

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

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

次の図に、文字列データ ブロックの形式を示します。



次の表に、文字列データ ブロックのフィールドの説明を示します。

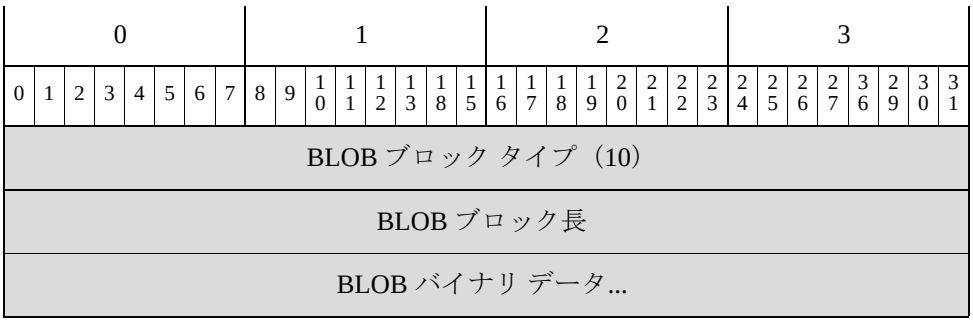
表 4-31　　文字列データ ブロックのフィールド

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

BLOB データ ブロック

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

次の図に、BLOB データ ブロックの形式を示します。



次の表に、BLOB データ ブロックのフィールドの説明を示します。

表 4-32　BLOB データ ブロック フィールド

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

リスト データ ブロック

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

次の図に、リスト データ ブロックの基本的な形式を示します。

次の表では、リスト データ ブロックのフィールドについて説明します。

表 4-33　リスト データ ブロックのフィールド

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

汎用リスト ブロック

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

次の図に、汎用リストのデータ ブロックの基本的な構造を示します。

次の表では、汎用リスト データ ブロックのフィールドについて説明します。

表 4-34　　汎用リスト データ ブロックのフィールド

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

サブサーバー データ ブロック

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

次の図は、サブサーバー データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	サブサーバー ブロック タイプ(1)																															
	サブサーバー ブロック長																															
サブサーバー [名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	サブサーバー名...																															
ベンダー [名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ベンダー名...																															
バージョン バージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	バージョン...																															

次の表では、サブサーバー データ ブロックのフィールドについて説明します。

表 4-35　　サブサーバー データ ブロックのフィールド

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

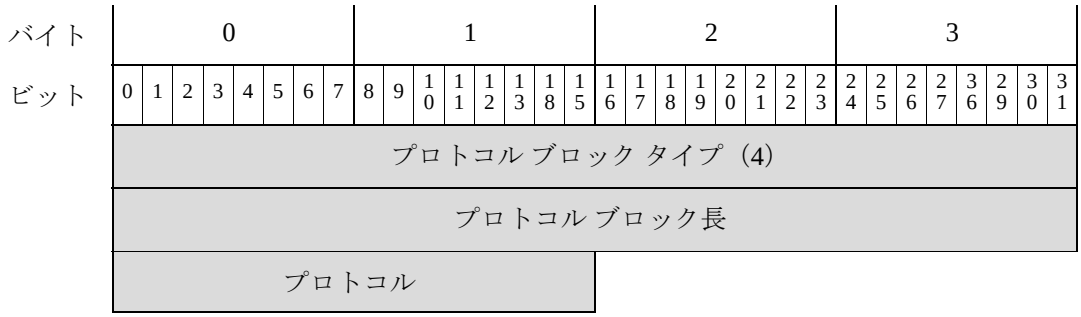
表 4-35　サブサーバー データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
ベンダー名（Vendor Name）	string	サブサーバー ベンダー名。
文字列ブロック タイプ	uint32	サブサーバー バージョンを格納した文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプ フィールドと長さフィールドにバージョンのバイト数を加えたサブサーバー バージョン文字列データ ブロックのバイト数。
バージョン	string	サブサーバー長

プロトコル データ ブロック

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

次の図は、プロトコル データ ブロックの形式です。



次の表では、プロトコル データ ブロックのフィールドについて説明します。

表 4-36　プロトコル データ ブロックのフィールド

フィールド	データタイプ	説明
プロトコル ブロック タイプ	uint32	プロトコル データ ブロックを開始します。この値は常に 4 です。
プロトコル ブロック長	uint32	プロトコル データ ブロックのバイト数。この値は常に 10 です。

表 4-36　プロトコル データ ブロックのフィールド（続き）

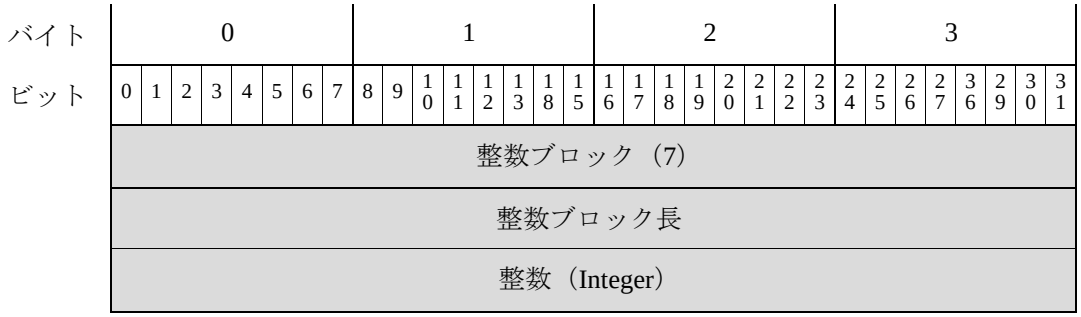
フィールド	データタイプ	説明
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6：TCP • 17：UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048：IP

整数型（INT32）データ ブロック

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

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

次の図は、整数型データ ブロックの形式です。



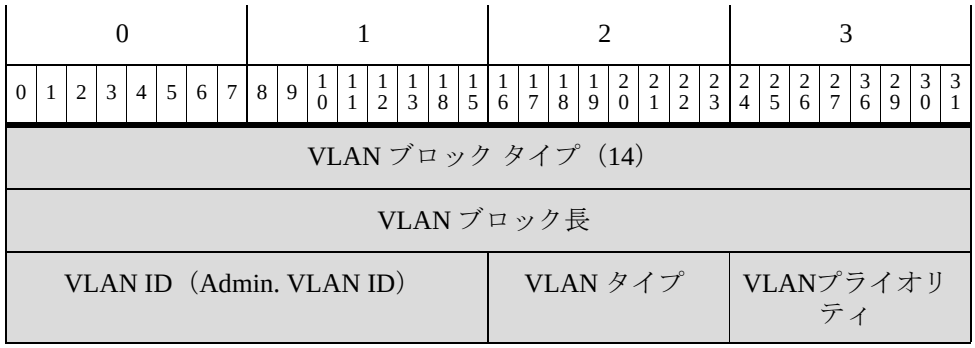
次の表では、整数型データ ブロックのフィールドについて説明します。

表 4-37　整数型データ ブロックのフィールド

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

VLAN データ ブロック

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



次の表では、VLAN データ ブロックのフィールドについて説明します。

表 4-38　VLAN データ ブロックのフィールド

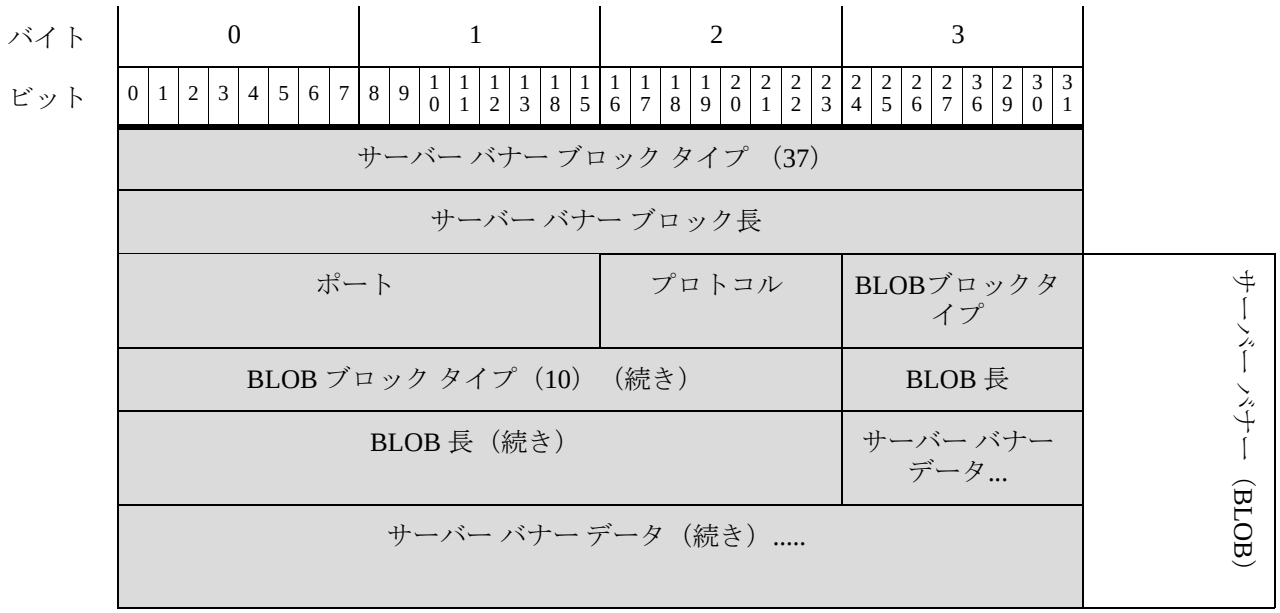
フィールド	データタイプ	説明
VLAN ブロック タイプ	uint32	VLAN データ ブロックを開始します。この値は常に 14 です。
VLAN ブロック長	uint32	VLAN データ ブロックのバイト数。この値は常に 12 です。
VLAN ID（Admin. VLAN ID）	uint16	ホストがメンバーとして所属している VLAN を示す VLAN ID 番号を格納します。
VLAN タイプ	uint8	VLAN タグ内でカプセル化されるパケットのタイプ。 • 0:イーサネット • 1:トークン リング
VLAN プライオリティ	uint8	VLAN タグに含まれる優先順位値。

サーバー バナー データ ブロック

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

次の図は、サーバー バナー データ ブロックの形式です。

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



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

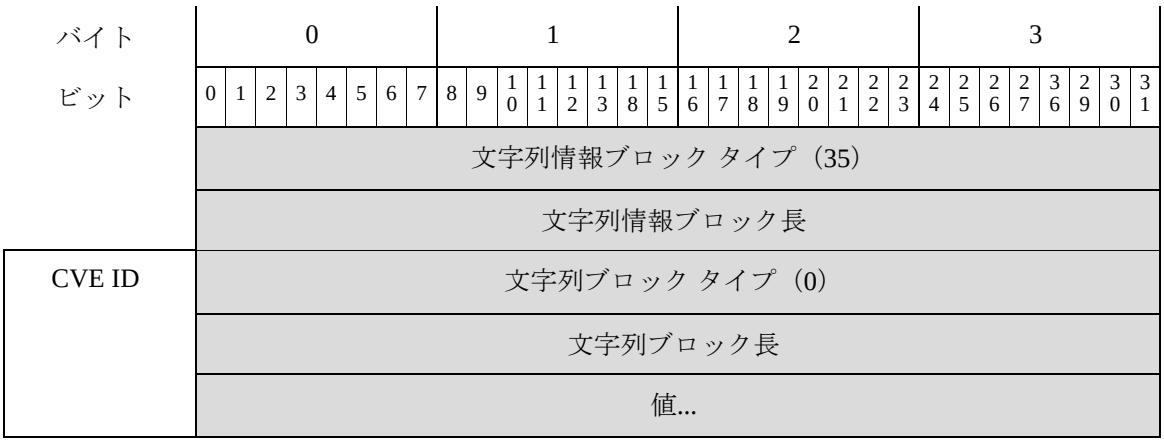
表 4-39　サーバー バナー データ ブロックのフィールド

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

文字列情報データ ブロック

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

次の図は、文字列情報データ ブロックの形式です。



次の表では、文字列情報データ ブロックのフィールドについて説明します。

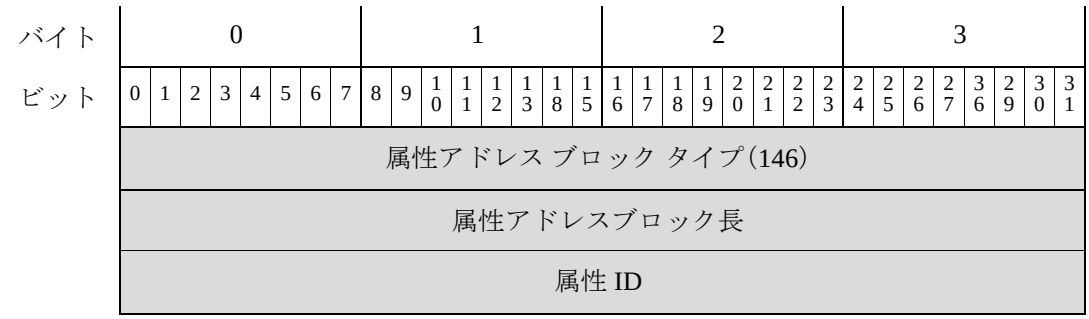
表 4-40　　文字列情報データ ブロックのフィールド

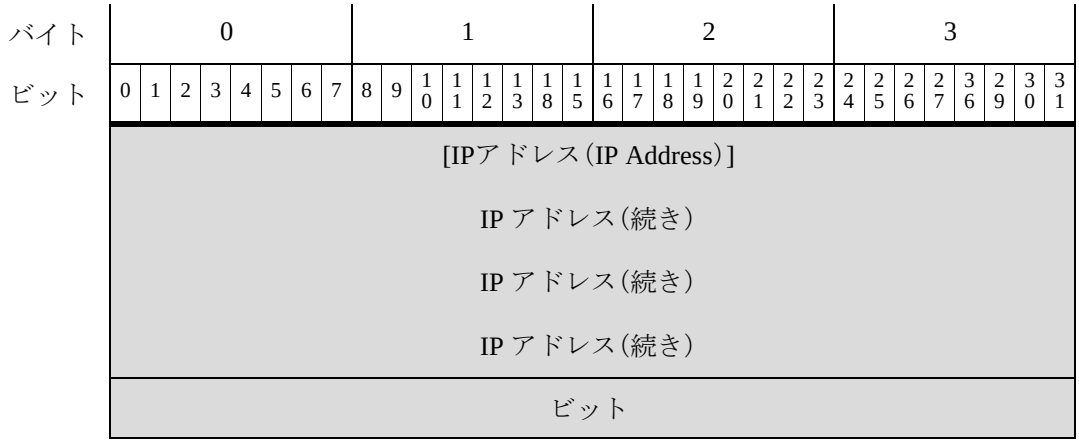
フィールド	データタイプ	説明
文字列情報ブロック タイプ	uint32	文字列情報データ ブロックを開始します。この値は常に 35 です。
文字列情報ブロック長	uint32	文字列情報データ ブロック ヘッダーと文字列情報データを組み合わせた長さ。
文字列ブロック タイプ	uint32	値を含む文字列データ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、値のバイト数を加えた値の文字列データ ブロックのバイト数。
値	string	文字列情報データ ブロックを使用した脆弱性のデータ ブロックの Common Vulnerabilities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

属性アドレス データ ブロック 5.2+

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

次の図は、属性アドレス ブロックの基本構造を示しています。





次の表は、属性アドレス データ ブロックのフィールドについての説明です。

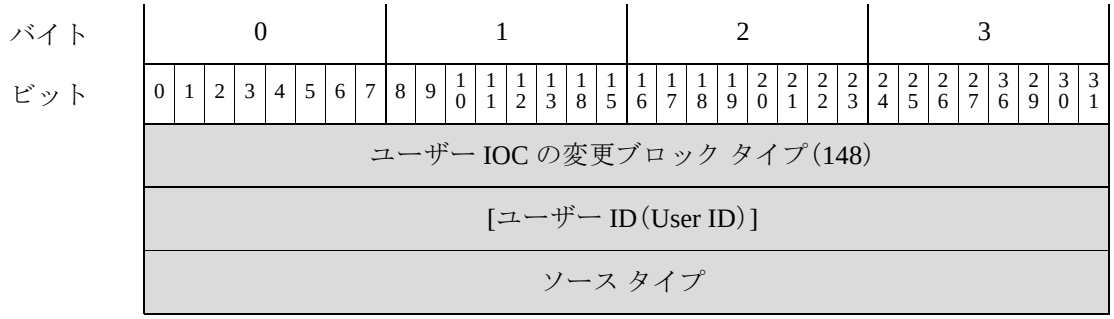
表 4-41　属性アドレス データ ブロック 5.2+ のフィールド

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

ユーザー IOC の変更データ ブロック 5.3+

ユーザー IOC の変更データ ブロックには、ユーザーが行った IOC の変更に関する情報が含まれています。これは、ユーザー ホスト IOC の削除、ユーザー ホスト IOC の有効化、およびユーザー ホスト IOC の無効化レコード内で使用されます。このブロック タイプは シリーズ 1 ブロック グループのブロック タイプ 148 です。

次の図で、ユーザー IOC 変更データ ブロックの基本構造を示します。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
[IPアドレス（IP Address）]範囲	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
	IP 範囲仕様データ ブロック*																															
	IOC ID																															
	ターゲット UID																															

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

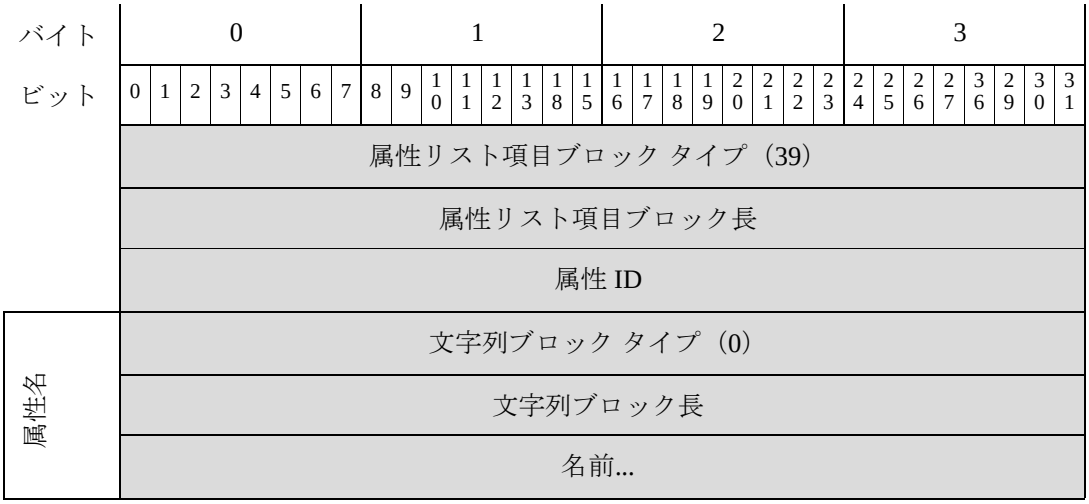
表 4-42　　ユーザー IOC の変更データ ブロック 5.3+ フィールド

フィールド	データタイプ	説明
ユーザー IOC の変更ブロック タイプ	uint32	ユーザー IOC の変更データ ブロックを開始します。この値は、常に `148` です。
ユーザー ID（User ID）	uint32	IOC に変更を加えたユーザーの ID 番号。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA）がクライアント データを検出した場合、`0` • ユーザーがクライアント データを提供した場合、`1` • サードパーティ スキャナがクライアント データを検出した場合、`2` • `nmimport.pl` やホスト入力 API クライアントなどのコマンド ライン ツールでクライアント データを提供した場合、`3`
汎用リスト ブロック タイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で構成された汎用リスト データ ブロックを開始します。この値は常に `31` です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リスト データ ブロックのバイト数。
IP 範囲仕様データ ブロック*	変数（variable）	ユーザー入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データ ブロック。このデータ ブロックの説明の詳細については、5.2+の IP アドレス範囲データ ブロック（4-101 ページ）を参照してください。
IOC ID	uint32	変更された IOC の ID 番号。
ターゲット UID	unit32	eStreamer 出力でサポートされているイベントでは使用されません。

属性リスト項目データ ブロック

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

次の図は、属性リスト項目データ ブロックの基本構造です。



次の表では、属性リスト項目データ ブロックのフィールドについて説明します。

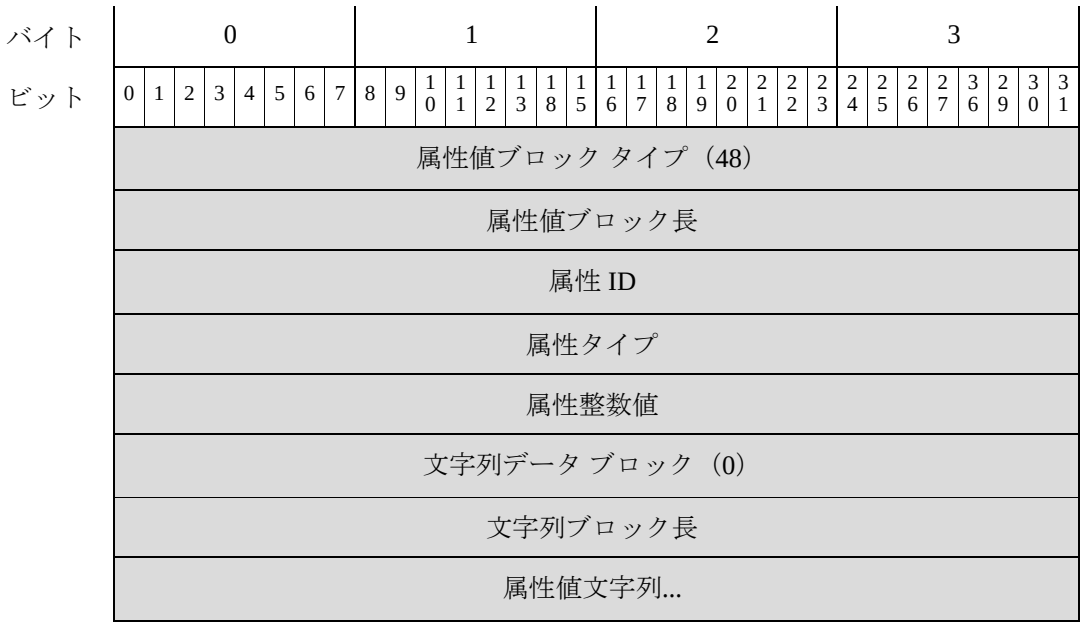
表 4-43　　属性リスト項目データ ブロックのフィールド

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

属性値データ ブロック

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

次の図は、属性値データ ブロックの形式です。



次の表では、属性値データ ブロックのコンポーネントについて説明します。

表 4-44　　属性値データ ブロックのフィールド

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

表 4-44　　属性値データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
文字列ブロック長	uint32	文字列ブロック タイプ フィールドと長さフィールドに属性名のバイト数を加えた文字列データ ブロックのバイト数。
属性値（Attribute Value）	string	属性値。

フル サブサーバー データ ブロック

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

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

次の図は、フル サブサーバー データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
フル サブサーバー ブロック タイプ（51）																																
フル サブサーバー ブロック長																																
文字列ブロック タイプ（0）																																
文字列ブロック長																																
サブサーバー名文字列...																																
文字列ブロック タイプ（0）																																
文字列ブロック長																																
サブサーバー ベンダー名文字列...																																
文字列ブロック タイプ（0）																																
文字列ブロック長																																
サブサーバー バージョン文字列...																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
汎用リスト ブロック タイプ（31）																																
汎用リスト ブロック長																																
（VDB）ホスト脆弱性データ ブロック																																
汎用リスト ブロック タイプ（31）																																
汎用リスト ブロック長																																
（サードパーティ スキャン）ホスト脆弱性データ ブロック*																																

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

表 4-45　　フル サブサーバー データ ブロックのフィールド

フィールド	データタイプ	説明
フル サブサーバー ブロック タイプ	uint32	フル サブサーバー ブロックを開始します。この値は常に 51 です。
フル サブサーバー ブロック長	uint32	フルサブサーバー ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のフル サブサーバー ブロックのバイト数を加えたフル サブサーバー データ ブロックの合計バイト数。
文字列ブロック タイプ	uint32	サブサーバー名を格納した文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにサブサーバー名のバイト数を加えたサブサーバー名文字列データ ブロックのバイト数。
サブサーバー名	string	サブサーバー名。
文字列ブロック タイプ	uint32	サブサーバー ベンダー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにサブサーバー名のバイト数を加えたベンダー名文字列データ ブロックのバイト数。
サブサーバー ベンダー名	string	サブサーバー ベンダーの名前。
文字列ブロック タイプ	uint32	サブサーバー バージョンを格納した文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにサブサーバー バージョンのバイト数を加えたサブサーバー バージョン文字列データ ブロックのバイト数。
サブサーバー バージョン	string	サブサーバー長

表 4-45　フル サブサーバー データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
汎用リスト ブロック タイプ	uint32	VDB 脆弱性データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのホスト脆弱性データ ブロックを含む汎用リスト データ ブロックのバイト数。
VDB ホスト脆弱性ブロック*	変数（variable）	シスコ で確認されたホスト脆弱性に関する情報を格納したホスト脆弱性データブロック。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+（4-119 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	サード パーティ スキャン脆弱性データを伝えるホスト脆弱性データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのホスト脆弱性データ ブロックを含む汎用リスト データ ブロックのバイト数。
サードパーティ スキャン ホスト脆弱性データ ブロック*	変数（variable）	サードパーティの脆弱性のスキャナで確認されたホスト脆弱性に関する情報を格納したホスト脆弱性データブロック。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+（4-119 ページ）を参照してください。

オペレーティング システム データ ブロック 3.5+

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	オペレーティング システム ブロック タイプ（53）																															
	オペレーティング システム ブロック長																															
	信頼度																															
OS フィンガープリント UUID	フィンガープリント UUID																															
	フィンガープリント UUID（続き）																															
	フィンガープリント UUID（続き）																															
	フィンガープリント UUID（続き）																															

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

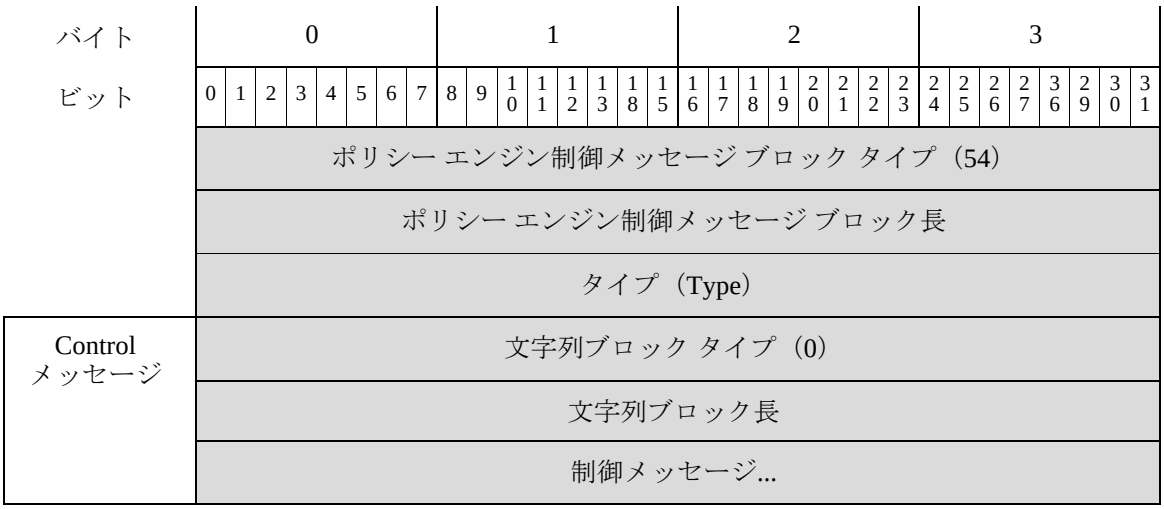
表 4-46　　オペレーティング システムのデータ ブロック 3.5+ のフィールド

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

ポリシー エンジン制御メッセージ データ ブロック

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

次の図は、ポリシー エンジン制御メッセージ データ ブロックの形式です。



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

表 4-47　ポリシー エンジン制御メッセージ データ ブロックのフィールド

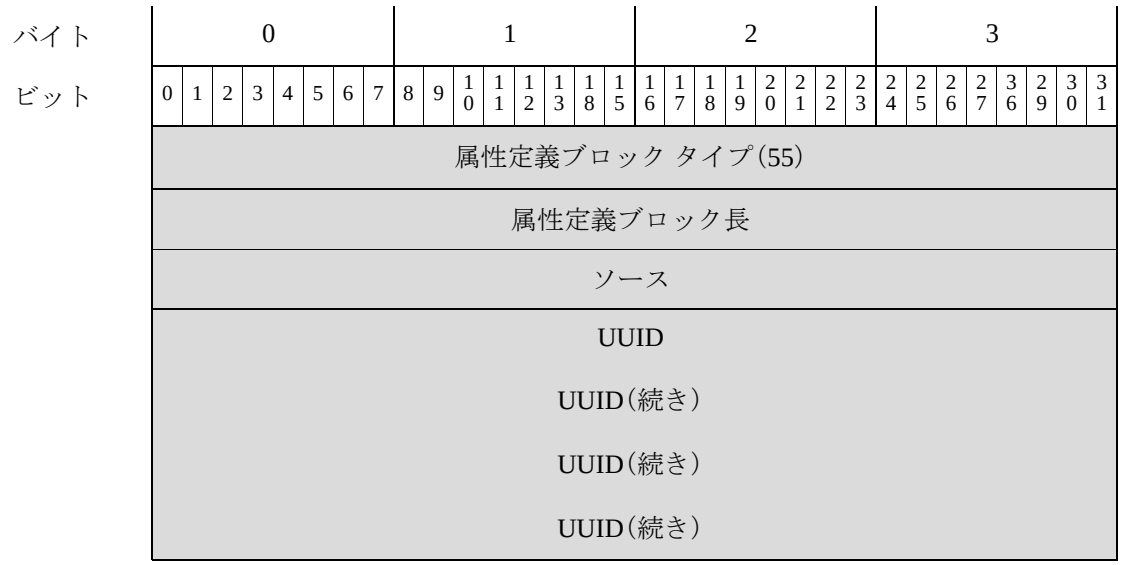
フィールド	データタイプ	説明
ポリシー エンジン制御メッセージ ブロック タイプ	uint32	ポリシー エンジン制御メッセージ データ ブロックを開始します。この値は常に 54 です。
ポリシー エンジン制御メッセージ長さ	uint32	ポリシー エンジン制御ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のポリシー エンジン制御データのバイト数を加えたポリシー エンジン制御メッセージ データ ブロックの合計バイト数。
タイプ	uint32	イベントのポリシーのタイプを示します。
文字列ブロック タイプ	uint32	制御メッセージを含む文字列データ ブロックを開始します。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

4.7+ の定義属性データ ブロック

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

これらのイベントの詳細については、属性メッセージ（4-59 ページ） を参照してください。

次の図は、属性定義データ ブロックの基本構造です。



次の表では、属性定義データ ブロックのフィールドについて説明します。

表 4-48　　属性定義データ ブロックのフィールド

フィールド	データタイプ	説明
属性定義ブロック タイプ	uint32	属性定義データ ブロックを開始します。この値は常に 55 です。
属性定義ブロック長	uint32	属性定義データ ブロック タイプと長さの 8 バイトに、後続の属性定義データのバイト数を加えた属性定義データ ブロックのバイト数。

表 4-48　属性定義データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
ソース	uint32	属性データの送信元にマッピングするID 番号。送信元タイプによって、これは無応答（RNA）、ユーザー、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
UUID	uint8[16]	影響を受ける属性の固有識別子として機能する ID 番号。
属性 ID	uint32	影響を受ける属性の ID 番号（該当する場合）。
文字列ブロック タイプ	uint32	属性定義名の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、属性定義名のバイト数を加えた、属性定義名の文字列データ ブロックの合計バイト数。
[名前（Name）]	string	属性定義名。
属性タイプ	uint32	属性のタイプ。値は以下のとおりです。 • 0：値としてのテキストによる属性。文字列データを使用します • 1：範囲の値による属性。整数型データを使用します • 2：使用可能値のリストによる属性。整数型データを使用します • 3：値としての URL による属性。文字列データを使用します • 4：値としてのバイナリ BLOB による属性。文字列データを使用します
属性カテゴリ	uint32	属性カテゴリ
範囲の開始値	uint32	定義した属性の整数範囲内の最初の整数。
範囲の終了値	uint32	定義した属性の整数範囲の最後の整数。
自動割り当て IP アドレス フラグ	uint32	属性に基づいて IP アドレスが自動的に割り当てられるかどうかを示すフラグ。
リスト ブロック タイプ	uint32	属性リスト項目を伝える属性リスト項目データ ブロック リストで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべての属性リスト項目データ ブロックを加えた値です。 このフィールドの後にはゼロか、さらに属性リスト項目のデータ ブロックが続きます。
属性リスト項目ブロック タイプ	uint32	最初の属性リスト項目データ ブロックを開始します。このデータ ブロックには、他の属性リスト項目データ ブロックを、リスト ブロック長フィールドで定義した上限まで続けることができます。

表 4-48　属性定義データ ブロックのフィールド（続き）

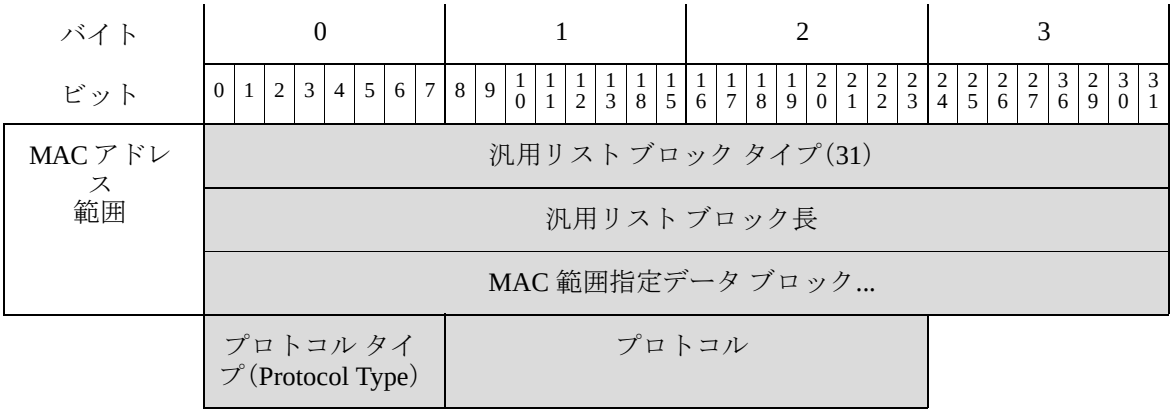
フィールド	データタイプ	説明
属性リスト項目ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトに属性リスト項目のバイト数を加えた属性リスト項目文字列データ ブロックのバイト数。
属性リスト項目	変数（variable）	属性リスト項目データ ブロック（4-87 ページ）に記載の属性リスト項目データ。
リスト ブロック タイプ	uint32	ホストの IP アドレスを属性とともに伝える属性アドレス データ ブロックで構成されるリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべての属性アドレス データ ブロックを加えた値です。 このフィールドの後にはゼロか、さらに属性アドレス データ ブロックが続きます。
属性アドレス ブロック タイプ	uint32	最初の属性アドレス データ ブロックを開始します。このデータ ブロックには、他の属性アドレス データ ブロックを、リスト ブロック長フィールドで定義した上限まで続けることができます。
属性アドレスブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトに属性アドレスのバイト数を加えた属性アドレス データ ブロックのバイト数。
属性アドレス	変数（variable）	属性アドレス データ ブロック 5.2+（4-84 ページ）に記載されている属性アドレス データ。

ユーザー プロトコル データ ブロック

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

次の図は、ユーザー プロトコル データ ブロックの基本構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ユーザー プロトコル ブロック タイプ（57）																															
	ユーザー プロトコル ブロック長																															
[IPアドレス（IP Address）]範囲	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
	IP 範囲仕様データ ブロック*																															



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

表 4-49　ユーザー プロトコル データ ブロックのフィールド

フィールド	バイト数	説明
ユーザー プロトコル ブロック タイプ	uint32	ユーザー プロトコル データ ブロックを開始します。この値は常に 57 です。
ユーザー プロトコル ブロック長	uint32	ユーザー プロトコル ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザー プロトコル データのバイト数を加えたユーザー プロトコル データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リスト データ ブロックのバイト数。
IP 範囲仕様データ ブロック*	変数（variable）	ユーザー入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データ ブロック。このデータ ブロックの説明の詳細については、5.2+の IP アドレス範囲データ ブロック（4-101 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	MAC アドレス範囲データを伝える MAC 範囲指定データ ブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての MAC 範囲指定データ ブロックを含む汎用リスト データ ブロックのバイト数。
MAC 範囲指定データ ブロック*	変数（variable）	ユーザー入力の MAC アドレス範囲に関する情報を含む MAC 範囲指定データ ブロック。このデータ ブロックの説明の詳細については、MAC アドレス指定データ ブロック（4-104 ページ）を参照してください。
プロトコル タイプ（Protocol Type）	uint8	プロトコルのタイプを示します。プロトコルには、IP などネットワーク層プロトコルの 0、または TCP や UDP などトランスポート層プロトコルの 1 があります。
プロトコル	uint16	データ ブロックに格納されるデータのプロトコルを示します。

5.1.1+ のユーザー クライアント アプリケーション データ ブロック

ユーザー クライアント アプリケーション データ ブロックには、クライアント アプリケーション データの送信元に関する情報、データを追加したユーザーの ID 番号、および IP アドレス範囲データ ブロックのリストが含まれます。バージョン 7.2 に追加されたペイロード IDは、レコードに関連付けられたアプリケーション インスタンスを指定します。ユーザー クライアント アプリケーション データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 138 です。ブロック タイプ 59 を置換します。

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

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ユーザー クライアント アプリケーション ブロック タイプ（138）																																
	ユーザー クライアント アプリケーション ブロック長																																
IP Range 仕様	汎用リスト ブロック タイプ（31）																																
	汎用リスト ブロック長																																
	IP 範囲仕様データ ブロック*																																
	アプリケーション プロトコル ID																																
	クライアント アプリケーション ID																																
バージョン	文字列ブロック タイプ（0）																																
	文字列ブロック長																																
	バージョン...																																
	ペイロード タイプ（Payload Type）																																
	Web アプリケーション ID																																

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

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

フィールド	バイト数	説明
ユーザー クライアント アプリケーション ブロック タイプ	uint32	ユーザー クライアント アプリケーション データ ブロックを開始します。この値は常に 138 です。
ユーザー クライアント アプリケーション ブロック長	uint32	ユーザー クライアント アプリケーション データ ブロックのバイトの合計数（ユーザー クライアント アプリケーション ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザー クライアント アプリケーション データのバイト数を含む）。
汎用リスト ブロック タイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リスト データ ブロックのバイト数。
IP 範囲仕様データ ブロック*	変数（variable）	ユーザー入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データ ブロック。このデータ ブロックの説明の詳細については、5.2+の IP アドレス範囲データ ブロック（4-101 ページ）を参照してください。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルの内部 ID 番号（該当する場合）。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号（該当する場合）。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション バージョン文字列データ ブロックのバイト数（文字列ブロック タイプと長さのフィールド、およびバージョンのバイト数を含む）。
バージョン	string	クライアント アプリケーション バージョン。
ペイロード タイプ（Payload Type）	uint32	このフィールドは下位互換性のために用意したものです。常に 0 です。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号（該当する場合）。

ユーザー クライアント アプリケーション リスト データ ブロック

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

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

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

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

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

フィールド	バイト数	説明
ユーザー クライアント アプリケーション リスト ブロック タイプ	uint32	ユーザー クライアント アプリケーション リスト データ ブロックを開始します。この値は常に 60 です。
ユーザー クライアント アプリケーション リスト ブロック長	uint32	ユーザー クライアント アプリケーション リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザー クライアント リスト アプリケーション データのバイト数を加えたユーザー クライアント アプリケーション リスト データ ブロックの合計バイト数。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答(RNA) がクライアント データを検出した場合、0 • ユーザーがクライアント データを提供した場合、1 • サードパーティ スキャナがクライアント データを検出した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでクライアント データを提供した場合、3
ソース	uint32	影響を受けるクライアント アプリケーションを追加した送信元にマッピングするID 番号。送信元タイプによって、これは無応答(RNA)、ユーザー、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。

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

フィールド	バイト数	説明
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
ユーザー クライアント アプリケーション ブロック	変数（variable）	リスト ブロック長の最大バイト数を上限としてカプセル化したユーザー クライアント アプリケーション データ ブロック。ユーザー クライアント アプリケーション データ ブロックの詳細については、5.1.1+ のユーザー クライアント アプリケーション データ ブロック（4-98 ページ） を参照してください。

5.2+の IP アドレス範囲データ ブロック

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

次の図は、IP アドレス範囲データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
IP アドレス範囲ブロック タイプ（141）																																
IP アドレス範囲ブロック長																																
IP アドレス範囲の開始 IP アドレス範囲の開始（続き） IP アドレス範囲の開始（続き） IP アドレス範囲の開始（続き）																																
IP アドレス範囲の最後 IP アドレス範囲の最後（続き） IP アドレス範囲の最後（続き） IP アドレス範囲の最後（続き）																																

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

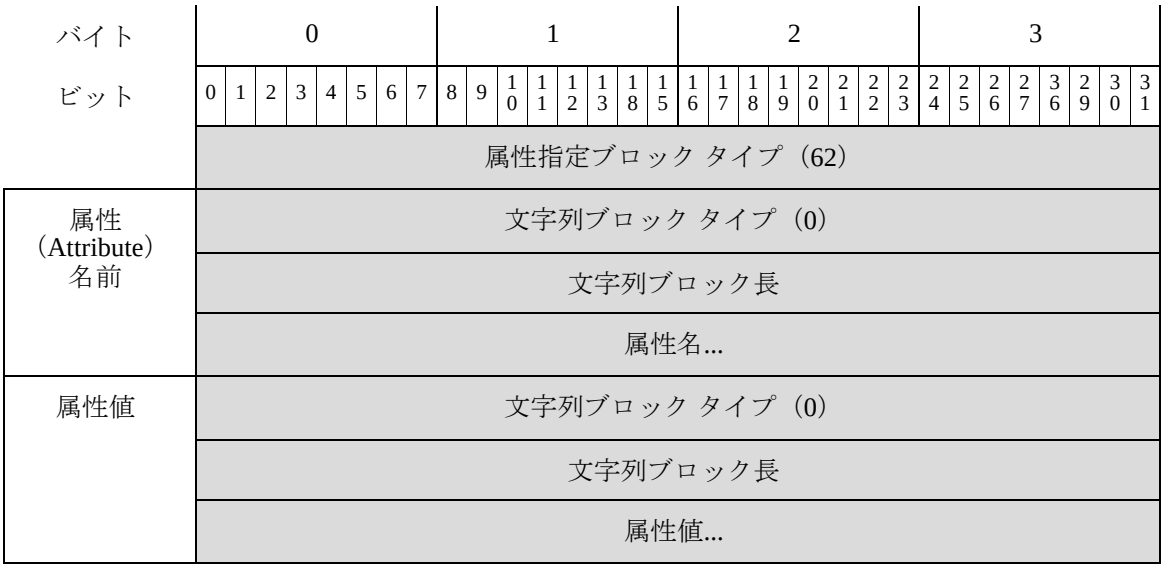
表 4-52　IP アドレス範囲データ ブロックのフィールド

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

属性指定データ ブロック

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

次の図は、属性指定データ ブロックの形式です。



次の表では、属性指定データ ブロックのコンポーネントについて説明します。

表 4-53　属性指定データ ブロックのフィールド

フィールド	データタイプ	説明
属性指定ブロック タイプ	uint32	属性指定データ ブロックを開始します。この値は常に 62 です。
文字列ブロック タイプ	uint32	属性名を含む文字列データ ブロックを開始します。この値は常に 0 です。

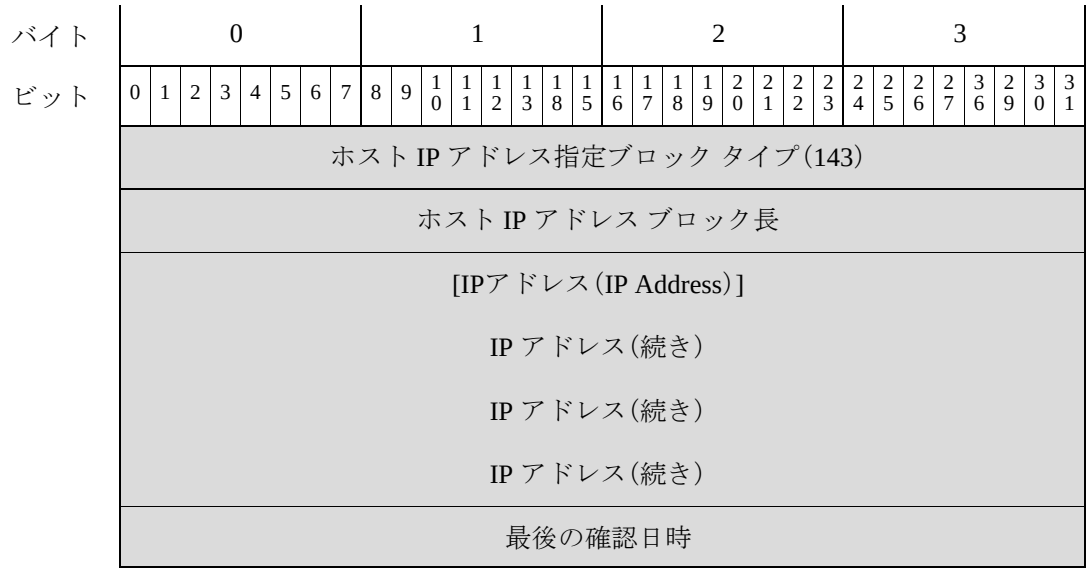
表 4-53　　属性指定データ ブロックのフィールド（続き）

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

ホスト IP アドレス データ ブロック

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

次の図は、ホスト IP アドレス データ ブロックの形式です。



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

表 4-54　　ホスト IP アドレス データ ブロックのフィールド

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

MAC アドレス指定データ ブロック

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

次の図は、MAC アドレス指定データ ブロックの形式です。

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

表 4-55　　MAC アドレス指定データ ブロックのフィールド

フィールド	データタイプ	説明
MAC アドレス指定ブロック タイプ	uint32	MAC アドレス指定データ ブロックを開始します。この値は常に 63 です。

表 4-55　MAC アドレス指定データ ブロックのフィールド（続き）

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

アドレス指定データ ブロック

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

次の図は、アドレス指定データ ブロックの基本構造です。

次の表では、アドレス指定データ ブロックのフィールドについて説明します。

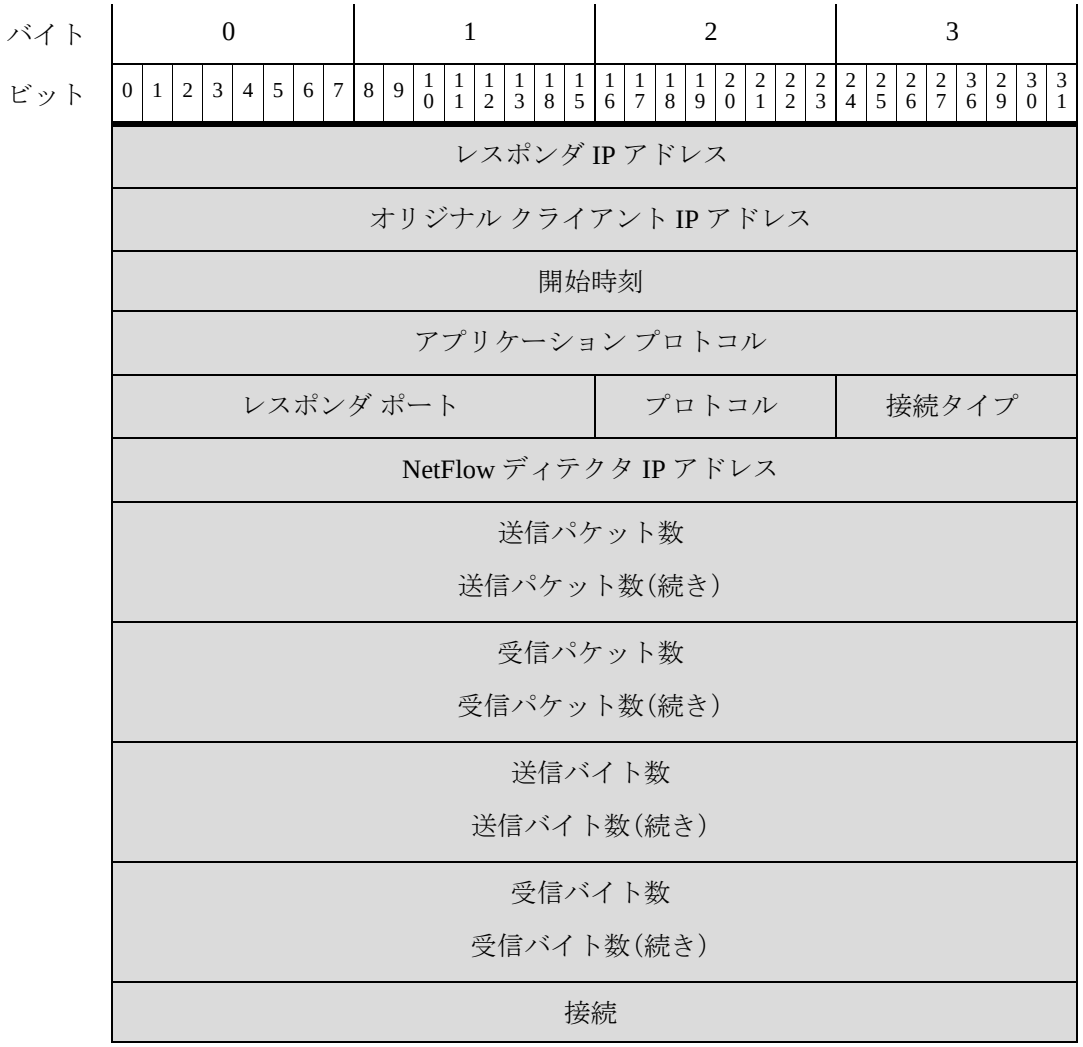
表 4-56　アドレス指定データ ブロックのフィールド

フィールド	バイト数	説明
アドレス指定データ ブロック タイプ	uint32	アドレス指定データ ブロックを開始します。この値は常に 64 です。
アドレス指定ブロック長	uint32	アドレス指定ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のアドレス指定データのバイト数を加えたアドレス指定データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
IP アドレス範囲指定データ ブロック	変数（variable）	リスト ブロック長の最大バイト数を上限としてカプセル化した IP アドレス範囲指定データ ブロック。詳細については、5.2+の IP アドレス範囲データ ブロック（4-101 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
MAC アドレス指定データ ブロック	変数（variable）	リスト ブロック長の最大バイト数を上限としてカプセル化した MAC アドレス指定データ ブロック。詳細については、MAC アドレス指定データ ブロック（4-104 ページ）を参照してください。

6.1+ の接続チャンク データ ブロック

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

次の図は、接続チャンク データ ブロックの形式を示しています。



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

表 4-57　　接続チャンク データ ブロックのフィールド

フィールド	データタイプ	説明
接続チャンク ブロック タイプ	uint32	接続チャンク データ ブロックを開始します。この値は常に 164 です。
接続チャンク ブロック長	uint32	接続チャンク データ ブロックのバイト数(接続チャンク ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続チャンク データのバイト数を含む)。
イニシエータ IP アドレス	uint8(4)	この接続タイプのイニシエータの IP アドレス。このアドレスは、オリジナル クライアントとレスポンダの IP アドレスに使用して、同一の接続を識別します。
レスポンダ IP アドレス	uint8(4)	この接続タイプのレスポンダの IP アドレス。このアドレスは、イニシエータとオリジナル クライアントの IP アドレスに使用して、同一の接続を識別します。

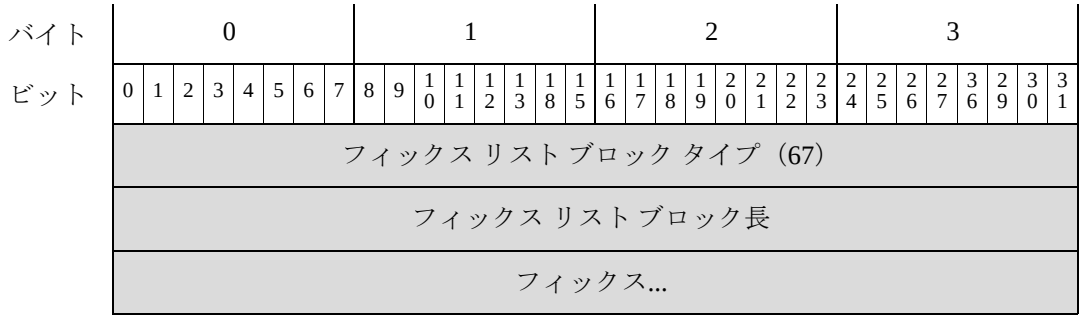
表 4-57　接続チャンク データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
オリジナル クライアント IP アドレス	uint8(4)	要求の送信元であるプロキシの背後にあるホストの IP アドレス。これは、イニシエータとレスポンダの IP アドレスで使用して同一の接続を確認します。
開始時刻	uint32	接続チャンクの開始時刻。
アプリケーション プロトコル	uint32	接続で使用されたプロトコルの ID 番号。
レスポンダ ポート	uint16	接続チャンクでレスポンダが使用したポート。
プロトコル	uint8	ユーザー情報を含むパケットのプロトコル。
接続タイプ	uint8	接続の種類。
NetFlow ディテクタ IP アドレス	uint8[4]	IP アドレス オクテットの、接続を検出した NetFlow デバイスの IP アドレス。
送信パケット数	uint64	接続チャンクで送信されたパケット数。
受信パケット数	uint64	接続チャンクで受信されたパケット数。
送信バイト数	uint64	接続チャンクで送信されたバイト数。
受信バイト数	uint64	接続チャンクで受信されたバイト数。
接続	uint32	5 分間の接続数。

フィックス リスト データ ブロック

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

次の図は、フィックス リスト データ ブロックの形式です。



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

表 4-58　フィックス リスト データ ブロックのフィールド

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

ユーザー サーバー データ ブロック

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

次の図は、ユーザー サーバー データ ブロックの基本構造です。

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

表 4-59　ユーザー サーバー データ ブロックのフィールド

フィールド	バイト数	説明
ユーザー サーバー データ ブロック タイプ	uint32	ユーザー サーバー データ ブロックを開始します。この値は常に 76 です。
ユーザー サーバー ブロック長	uint32	ユーザー サーバー ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザー サーバー データのバイト数を加えたユーザー サーバー データ ブロックの合計バイト数。

表 4-59　ユーザー サーバー データ ブロックのフィールド（続き）

フィールド	バイト数	説明
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
IP アドレス範囲指定データ ブロック	変数（variable）	リスト ブロック長の最大バイト数を上限としてカプセル化した IP アドレス範囲指定データ ブロック。
[ポート（Port）]	uint16	サーバーで使用するポート。
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6：TCP • 17：UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048：IP

ユーザー サーバー リスト データ ブロック

ユーザー サーバー リスト データ ブロックには、ユーザー入力のサーバー リスト データ ブロックを格納します。ユーザー サーバー リスト データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 77 です。次の図は、ユーザー サーバー リスト データ ブロックの基本構造です。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ユーザー サーバー リスト データ ブロック タイプ（77）																																
	ユーザー サーバー リスト ブロック長																																
	ソース タイプ																																
	ソース																																
ユーザー（User）サーバー ブロック	汎用リスト ブロック タイプ（31）																																
	汎用リスト ブロック長																																
	ユーザー サーバー データ ブロック*																																

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

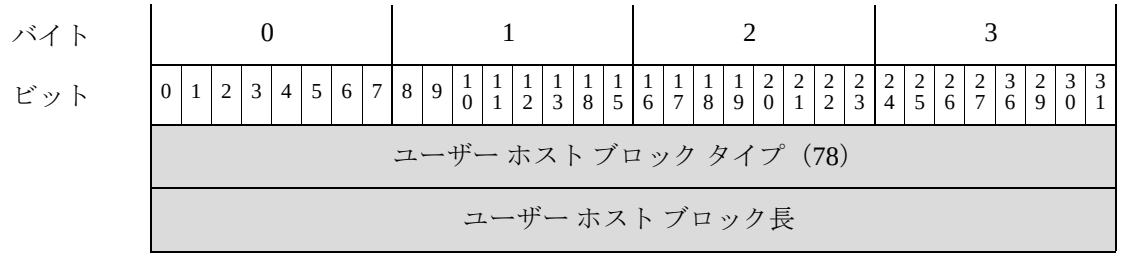
表 4-60　ユーザー サーバー リスト データ ブロックのフィールド

フィールド	バイト数	説明
ユーザー サーバー リスト データ ブロック タイプ	uint32	ユーザー サーバー リスト データ ブロックを開始します。この値は常に 77 です。
ユーザー サーバー リスト ブロック長	uint32	ユーザー サーバー リスト ブロック タイプ フィールドと長さ フィールドの 8 バイトに、後続のユーザー サーバー リスト データのバイト数を加えたユーザー サーバー リスト データ ブロックの合計バイト数。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA）がサーバー データを検出した場合、0 • ユーザーがサーバー データを提供した場合、1 • サードパーティ スキャナがサーバー データを検出した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでサーバー データを提供した場合、3
ソース	uint32	サーバー データの送信元にマッピングするID 番号。送信元タイプによって、これは無応答（RNA）、ユーザー、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
ユーザー サーバー データ ブロック	変数（variable）	リスト ブロック長の最大バイト数を上限としてカプセル化したユーザー サーバー データ ブロック。

ユーザー ホスト データ ブロック 4.7+

ユーザー ホスト データ ブロックは、ユーザー追加/削除ホスト メッセージ（4-57 ページ）で使用し、ホスト範囲、ユーザー ホスト入力イベントから得られるユーザー アイデンティティとソース アイデンティティに関する情報を格納します。ユーザー ホスト データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 78 です。

次の図は、ユーザー ホスト データ ブロックの基本構造です。



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

表 4-61　ユーザー ホスト データ ブロックのフィールド

フィールド	バイト数	説明
ユーザー ホスト ブロック タイプ	uint32	ユーザー ホスト データ ブロックを開始します。この値は常に 78 です。
ユーザー ホスト ブロック長	uint32	ユーザー ホスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザー ホスト データのバイト数を加えたユーザー ホスト データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リスト データ ブロックのバイト数。
IP 範囲仕様データ ブロック*	変数（variable）	ユーザー入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データブロック。このデータブロックの説明の詳細については、5.2+の IP アドレス範囲データ ブロック（4-101 ページ） を参照してください。
汎用リスト ブロック タイプ	uint32	MACアドレス範囲データを伝えるMAC範囲指定データブロックで構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての MAC 範囲指定データ ブロックを含む汎用リスト データ ブロックのバイト数。
MAC範囲指定データ ブロック*	変数（variable）	ユーザー入力のMACアドレス範囲に関する情報を含むMAC範囲指定データ ブロック。このデータ ブロックの説明の詳細については、MACアドレス指定データ ブロック（4-104ページ） を参照してください。

表 4-61　ユーザー ホスト データ ブロックのフィールド（続き）

フィールド	バイト数	説明
ソース	uint32	ホストデータを追加または更新した送信元にマッピングするID番号。送信元タイプによって、これは無応答（RNA）、ユーザー、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA） がホスト データを検出した場合、0 • ユーザーがホスト データを提供した場合、1 • サードパーティ スキャナがホスト データを検出した場合、2 • nmimport.plやホスト入力APIクライアントなどのコマンドライン ツールでホスト データを提供した場合、3

ユーザー脆弱性変更データ ブロック 4.7+

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

次の図は、脆弱性変更データ ブロックの基本構造です。

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ユーザー脆弱性変更データ ブロック タイプ（80）																																
	ユーザー脆弱性変更ブロック長																																
	ソース																																
	ソース タイプ																																
Vuln Ack ブロック	汎用リスト ブロック タイプ（31）																																
	汎用リスト ブロック長																																
	ユーザー脆弱性データ ブロック...*																																

次の表では、汎用リスト データ ブロックのフィールドについて説明します。

表 4-62　ユーザー脆弱性変更データ ブロックのフィールド

フィールド	バイト数	説明
ユーザー脆弱性変更データ ブロック タイプ	uint32	ユーザー脆弱性変更データ ブロックを開始します。この値は常に 80 です。
ユーザー脆弱性変更ブロック長	uint32	ホスト脆弱性ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のホスト脆弱性データのバイト数を加えたユーザー脆弱性変更データ ブロックの合計バイト数。
ソース	uint32	ホスト脆弱性変更値を更新または追加した送信元にマッピングされるID 番号。送信元タイプによって、これは無応答（RNA）、ユーザー、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA）がホスト脆弱性データを検出した場合、0 • ユーザーがホスト脆弱性データを提供した場合、1 • サードパーティ スキャナがホスト脆弱性データを検出した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでホスト脆弱性データを提供した場合、3
タイプ（Type）	uint32	脆弱性のタイプ。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
ユーザー脆弱性データ ブロック	変数（variable）	リスト ブロック長の最大バイト数を上限としてカプセル化したユーザー脆弱性データ ブロック。詳細については、ユーザー脆弱性データ ブロック 5.0+（4-169 ページ）を参照してください。

ユーザー重要度変更データ ブロック 4.7+

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

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

次の図は、ユーザー重要度データ ブロックの基本構造です。

次の表では、ユーザー重要度データ ブロックのフィールドについて説明します。

表 4-63　　ユーザー重要度データ ブロックのフィールド

フィールド	バイト数	説明
ユーザー重要度データ ブロック タイプ	uint32	ユーザー重要度データ ブロックを開始します。この値は常に 81 です。
ユーザー重要度ブロック長	uint32	ユーザー重要度ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザー重要度データのバイト数を加えたユーザー重要度データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
IP アドレス範囲指定データ ブロック	変数（variable）	リスト ブロック長の最大バイト数を上限としてカプセル化した IP アドレス範囲指定データ ブロック。
ソース	uint32	ユーザー重要度値を更新または追加した送信元にマッピングされるID 番号。送信元タイプによって、これは無応答（RNA）、ユーザー、スキャナ、またはサードパーティ アプリケーションにマッピングされます。

表 4-63　ユーザー重要度データ ブロックのフィールド（続き）

フィールド	バイト数	説明
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA）がユーザー重要度値を提供した場合、0 • ユーザーがユーザー重要度値を提供した場合、1 • サードパーティ スキャナがユーザー重要度値を提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでユーザー重要度値を提供した場合、3
重要度値	uint32	ユーザーの重要度値。

ユーザー属性値データ ブロック 4.7+

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

次の図は、ユーザー属性値データ ブロックの構造です。

次の表では、ユーザー属性値データ ブロックのフィールドについて説明します。

表 4-64　ユーザー属性値データ ブロックのフィールド

フィールド	バイト数	説明
ユーザー属性値データ ブロック タイプ	uint32	ユーザー属性値データ ブロックを開始します。この値は常に 82 です。
ユーザー属性値ブロック長	uint32	ユーザー属性値ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザー属性ブロック データのバイト数を加えた属性値データ ブロックの合計バイト数。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
IP アドレス範囲指定データ ブロック	変数（variable）	リスト ブロック長の最大バイト数を上限とした IP アドレス範囲指定データ ブロック（それぞれ開始 IP アドレスと終了 IP アドレスを含む）。
ソース	uint32	属性データを追加または更新した送信元にマッピングする ID 番号。送信元タイプによって、これは無応答（RNA）、ユーザー、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA）がユーザー属性を提供した場合、0 • ユーザーが属性値を提供した場合、1 • サードパーティ スキャナがユーザー属性値を提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでユーザー属性値を提供した場合、3
属性 ID	uint32	更新した属性の ID 番号（該当する場合）。
BLOB ブロック タイプ	uint32	BLOB データ ブロックを開始します。この値は常に 10 です。
BLOB ブロック長	uint32	BLOB データ ブロックのバイト数です。BLOB ブロック タイプとブロック長フィールドの 8 バイトと後続のバイナリ データの長さが含まれます。
値	変数（variable）	バイナリ形式でユーザー属性値を格納します。

ユーザー プロトコル リスト データ ブロック 4.7+

ユーザー プロトコル リスト データ ブロックには、プロトコル データの送信元に関する情報、データを追加したユーザーの ID 番号、プロトコル データ ブロックのリストを格納します。ユーザー プロトコル リスト データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 83 です。ユーザー プロトコル データ ブロックの詳細については、ユーザー プロトコル データ ブロック（4-96 ページ）を参照してください。

ユーザー プロトコル メッセージ（4-60 ページ）にあるように、ユーザー プロトコル メッセージでは、ユーザー プロトコル リスト データ ブロックを使用します。

次の図は、ユーザー プロトコル リスト データ ブロックの基本構造です。

次の表では、汎用リスト データ ブロックのフィールドについて説明します。

表 4-65　ユーザー プロトコル リスト データ ブロックのフィールド

フィールド	バイト数	説明
ユーザープロトコル リスト ブロック タイプ	uint32	ユーザー プロトコル リスト データ ブロックを開始します。この値は常に 83 です。
ユーザープロトコル リスト ブロック長	uint32	ユーザー プロトコル リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザー プロトコル リスト データのバイト数を加えたユーザー プロトコル リスト データ ブロックの合計バイト数。

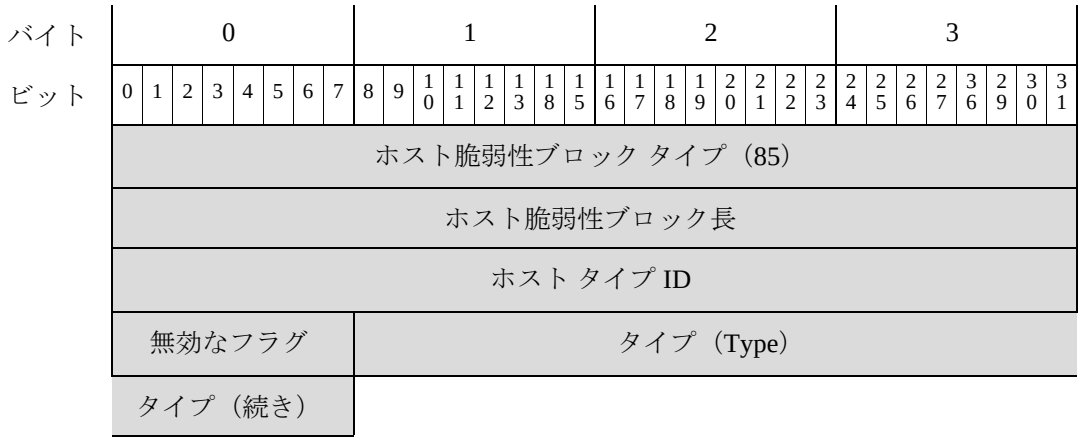
表 4-65　ユーザー プロトコル リスト データ ブロックのフィールド（続き）

フィールド	バイト数	説明
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA）がプロトコル データを提供した場合、0 • ユーザーがプロトコル データを提供した場合、1 • サードパーティ スキャナがプロトコル データを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでプロトコル データを提供した場合、3
ソース	uint32	影響を受けるプロトコルの送信元にマッピングするID 番号。送信元タイプによって、これは無応答（RNA）、ユーザー、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
ユーザー プロトコル データ ブロック	変数（variable）	リスト ブロック長の最大バイト数を上限としてカプセル化されたユーザー プロトコル データ ブロック。

ホスト脆弱性データ ブロック 4.9.0+

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

次の図は、ホスト脆弱性データ ブロックの形式です。



次の表では、ホスト脆弱性データ ブロックのコンポーネントについて説明します。

表 4-66　　ホスト脆弱性データ ブロックのフィールド

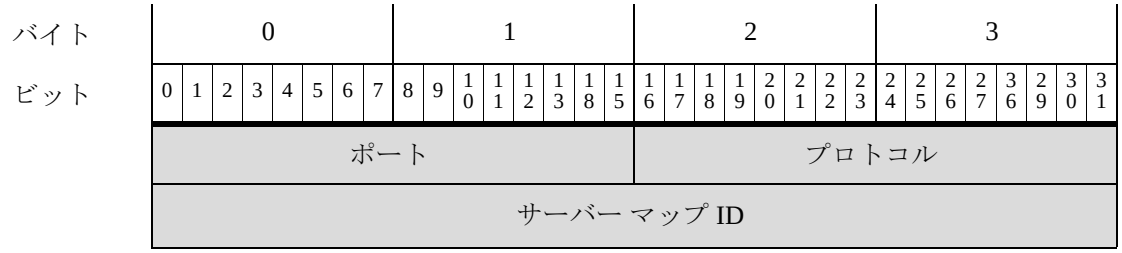
フィールド	データタイプ	説明
ホスト脆弱性ブロック タイプ	uint32	ホスト脆弱性データ ブロックを開始します。この値は常に 85 です。
ホスト脆弱性ブロック長	uint32	ホスト脆弱性ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のホスト脆弱性データのバイト数を加えたホスト脆弱性データ ブロックの合計バイト数。
ホスト タイプ ID	uint32	脆弱性の ID 番号。
無効なフラグ	uint8	脆弱性がそのホストで有効であるかどうかを示す値。
タイプ（Type）	uint32	脆弱性のタイプ。

アイデンティティ データ ブロック

アイデンティティ データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 94 です。アイデンティティ データ ブロックは、オペレーティング システムやサーバー フィンガープリント送信元のアイデンティティがいつ競合するか、あるいはいつタイムアウトになるかを示すアイデンティティの競合メッセージとアイデンティティ タイムアウト メッセージで使用します。このデータ ブロックは、アクティブ送信元アイデンティティ（ユーザー、スキャナ、またはアプリケーション）と競合中であると報告されたアイデンティティを記述します。詳細については、アイデンティティ競合とアイデンティティ タイムアウト システム メッセージ（4-62 ページ）を参照してください。

次の図は、4.9+ のアイデンティティ データ ブロックの形式です。

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



次の表では、シスコ アイデンティティ データ ブロックのフィールドについて説明します。

表 4-67　アイデンティティ データ ブロックのフィールド

フィールド	データタイプ	説明
アイデンティティ データ ブロック タイプ	uint32	アイデンティティ データ ブロックを開始します。この値は常に 94 です。
アイデンティティ データ ブロック長	uint32	アイデンティティ データ ブロックのバイト数。この値は常に 40 です。内訳は、データ ブロック タイプ フィールドと長さ フィールド、および送信元タイプ フィールドと ID フィールドの 16 バイト、フィンガープリント UUID 値の 16バイト、ポートの 2 バイト、プロトコルの 2 バイト、そして SM ID の 4 バイトです。
アイデンティティ データ送信元タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA）がフィンガープリント データを提供した場合、0 • ユーザーがフィンガープリント データを提供した場合、1 • サードパーティ スキャナがフィンガープリント データを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでフィンガープリント データを提供した場合、3
アイデンティティ データ送信元 ID	uint32	フィンガープリント データの送信元にマッピングするID 番号。送信元タイプによって、これは無応答（RNA）、ユーザー、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
UUID	uint8[16]	アイデンティティがオペレーティング システム アイデンティティの場合、フィンガープリントの固有識別子として機能するオクテット形式の ID 番号。
[ポート（Port）]	uint16	アイデンティティがサーバー アイデンティティの場合、サーバー データを含むパケットで使用するポートを示します。

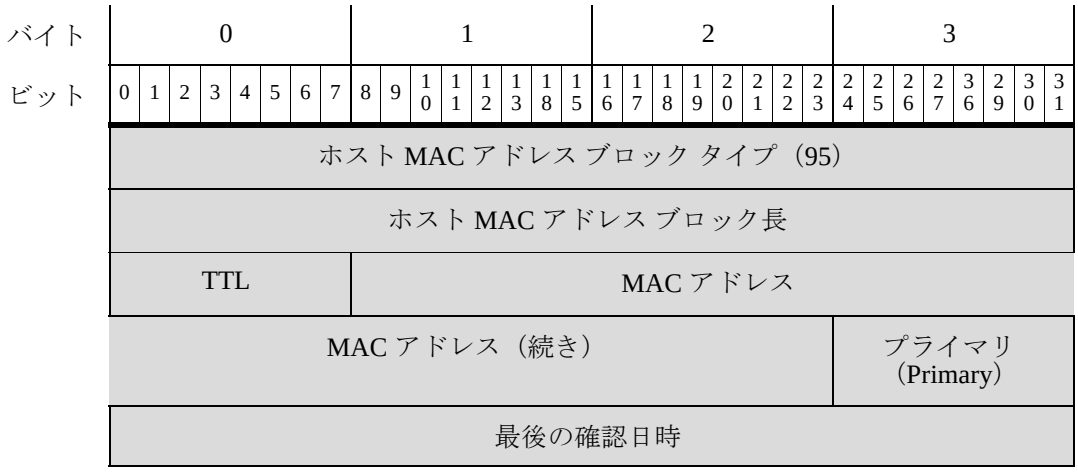
表 4-67　アイデンティティ データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
プロトコル	uint16	アイデンティティがサーバー アイデンティティの場合、ネットワーク プロトコルの IANA 番号またはサーバー データを含むパケットが使用する Ethertype を示します。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6：TCP • 7：UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048：IP
サーバーマップ ID	uint32	アイデンティティがサーバー アイデンティティの場合、サーバーの ID、ベンダー、バージョンの組み合わせを表すサーバー マッピング ID を示します。

ホスト MAC アドレス 4.9+

ホスト MAC アドレス データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 95 です。このブロックには、ホスト データのパケット存続時間の他、MAC アドレス、ホストのプライマリ サブネット、ホストの最後の確認日時値を格納します。

次の図は、4.9+ の MAC アドレス データ ブロックの形式です。



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

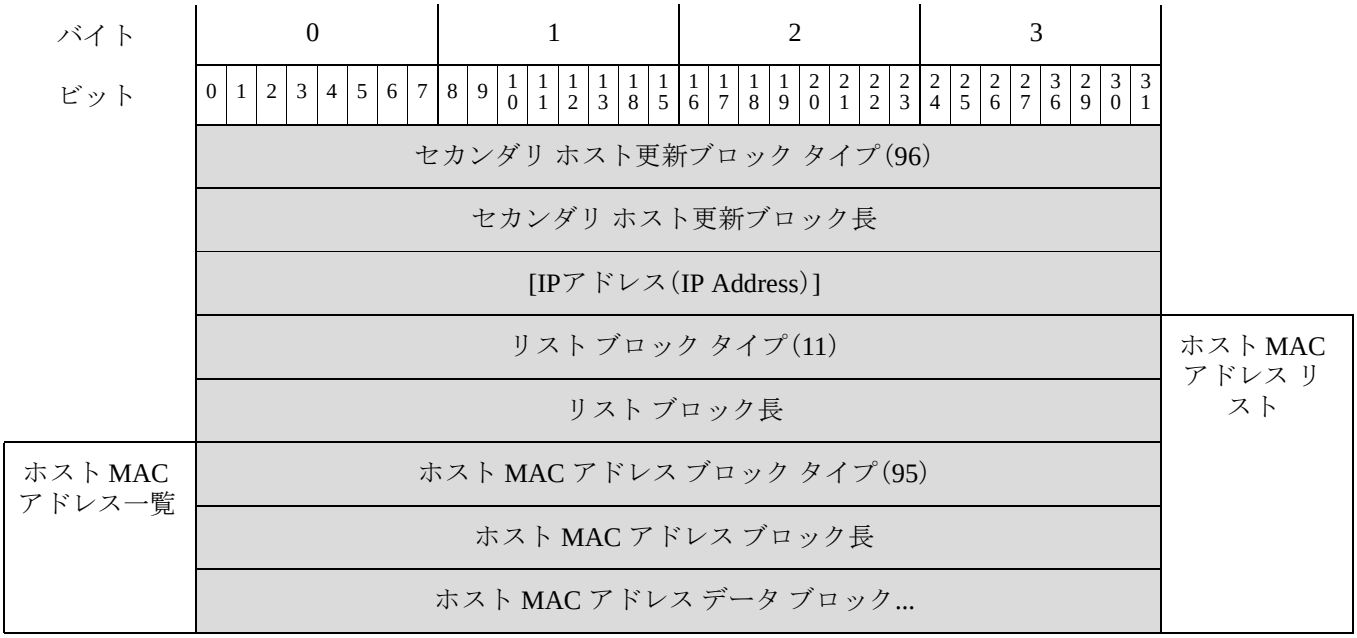
表 4-68　　ホスト MAC アドレス データ ブロックのフィールド

フィールド	データタイプ	説明
ホスト MAC アドレス データ ブロック タイプ	uint32	ホスト MAC アドレス データ ブロックを開始します。この値は常に 95 です。
ホスト MAC アドレス データ ブロック長	uint32	ホスト MAC アドレス データ ブロックのバイト数。この値は常に 20 です。内訳は、データ ブロック タイプ フィールドと長さフィールドの 8 バイト、TTL の 1 バイト、MAC アドレスの 6 バイト、プライマリ サブネットの 1 バイト、最後の確認日時値の 4 バイトです。
TTL	uint8	ホストのフィンガープリントを実行するために使用するパケットの TTL 値の違いを示します。
MAC アドレス	uint8 [6]	ホストの MAC アドレスを示します。
プライマリ（Primary）	uint8	ホストのプライマリ サブネットを示しています。
最後の確認日時	uint32	トラフィックで前回ホストを確認した時刻を示します。

セカンダリ ホストの更新

セカンダリ ホスト更新データ ブロックには、ホストが存在する場所以外のサブネットをモニタリングするデバイスからセカンダリ ホスト更新として送信されるホストの情報を格納します。これは変更セカンダリ更新イベントで使用します（イベント タイプ 100 1、サブタイプ 31）。セカンダリ ホスト更新データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 96 です。

次の図は、セカンダリ ホスト更新データ ブロックの形式です。



次の表では、ホスト更新データ ブロックのフィールドについて説明します。

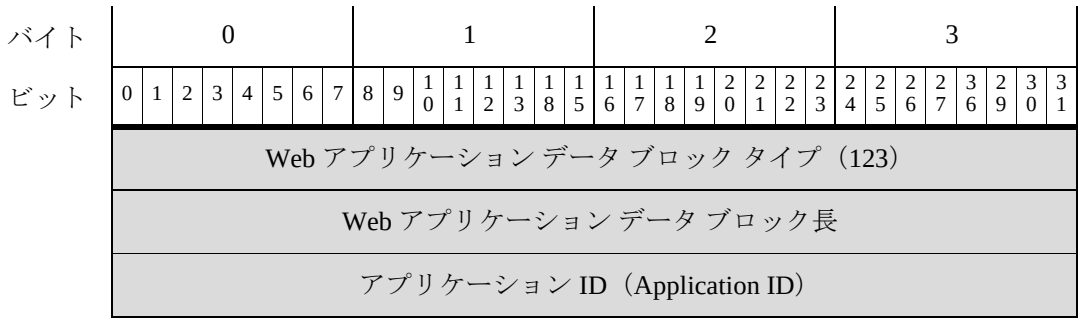
表 4-69　セカンダリ ホスト更新データ ブロックのフィールド

フィールド	データタイプ	説明
セカンダリ ホスト更新 ブロック タイプ	uint32	セカンダリ ホスト更新データ ブロックを開始します。この値は常に 96 です。
セカンダリ ホスト更新ブロック長	uint32	セカンダリ ホスト更新ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のホスト脆弱性データのバイト数を加えたセカンダリ ホスト更新データ ブロックの合計バイト数。
[IPアドレス(IP Address)]	uint8[4]	IP アドレスのオクテットの更新に、記載されているホストの IP アドレス。
リスト ブロック タイプ	uint32	ホスト MAC アドレス データを伝えるホスト MAC アドレス ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのホスト MAC アドレス データ ブロックを加えた値です。 このフィールドの後にはゼロか、さらにホスト MAC アドレス データ ブロックが続きます。
ホスト MAC アドレス ブロック タイプ	uint32	セカンダリ ホストを記述するホスト MAC アドレス データ ブロックを開始します。この値は常に 95 です。
ホスト MAC アドレス データ ブロック長	uint32	ホスト MAC アドレス データ ブロックのバイト数。この値は常に 20 です。内訳は、データ ブロック タイプ フィールドと長さフィールドの 8 バイト、TTL の 1 バイト、MAC アドレスの 6 バイト、プライマリ サブネットの 1 バイト、最後の確認日時値の 4 バイトです。
ホスト MAC アドレス データ ブロック	string	更新情報内のホスト MAC アドレス関連情報。

5.0+の Web アプリケーション データ ブロック

5.0+ の Web アプリケーション データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 123 です。このデータ ブロックは、検出した HTTP クライアント要求から得られた Web アプリケーションを記述します。

次の図は、5.0+ の Web アプリケーション データ ブロックの形式です。



次の表では、Web アプリケーション データ ブロックのフィールドについて説明します。

表 4-70　Web アプリケーション データ ブロックのフィールド

フィールド	データタイプ	説明
Web アプリケーション データ ブロック タイプ	uint32	Web アプリケーション データ ブロックを開始します。この値は常に 123 です。
Web アプリケーション データ ブロック長	uint32	Web アプリケーション データ ブロック タイプと長さの 8 バイトに、後続の ID フィールドのバイト数を加えた Web アプリケーション データ ブロックのバイト数。
アプリケーション ID（Application ID）	uint32	Web アプリケーションのアプリケーション ID。

接続統計データ ブロック 7.1+

接続統計データ ブロックは、接続データ メッセージで使用されます。TLS Confidence フィールド、クライアント アプリケーション ディテクタ フィールド、および NAT フィールドが追加されました。バージョン 7.0 以降の接続統計データブロックのブロックタイプは、シリーズ 1 ブロック グループのブロックタイプ 174 です。これはブロック タイプ173 接続統計データ ブロック 7.0（B-292 ページ） に置き換わります。

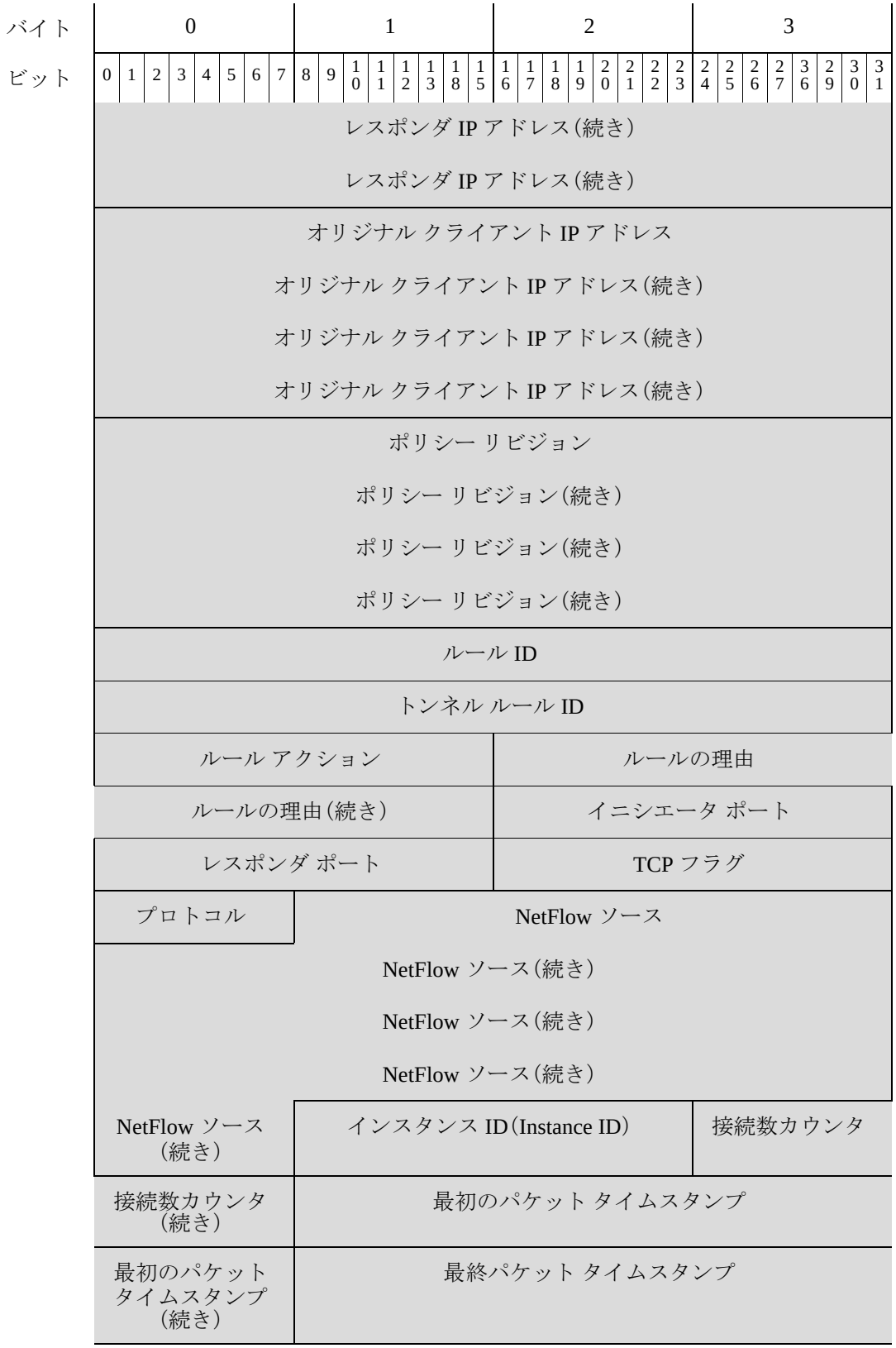
接続イベントレコードを要求するには、イベントバージョン 16 およびイベントコード 71 の要求メッセージ内に、拡張イベントフラグ（要求フラグフィールドのビット 30）を設定します。要求フラグ（2-15 ページ）を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

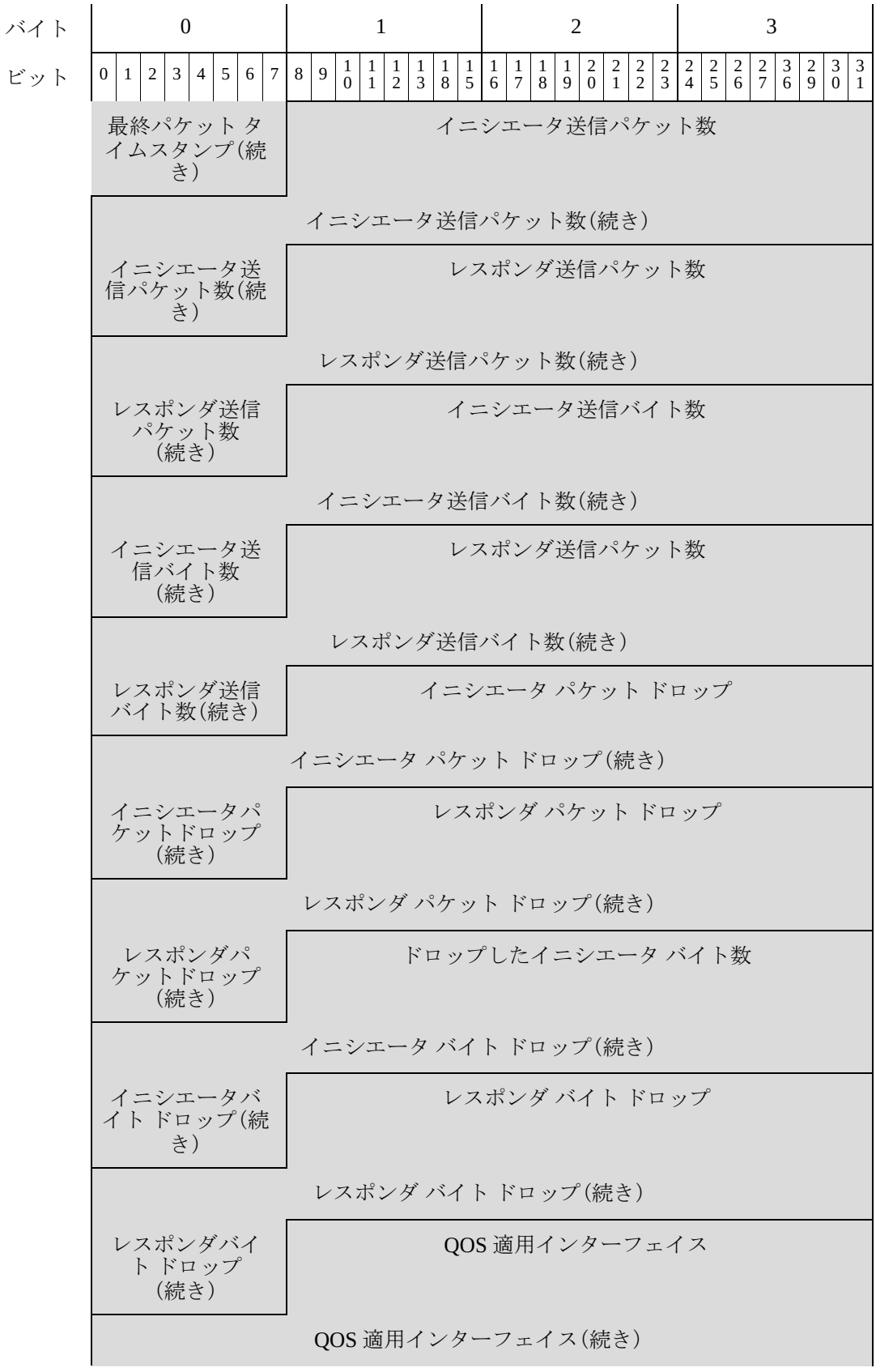
接続統計データ メッセージの詳細については、接続統計データ メッセージ（4-56 ページ）を参照してください。

次の図は、7.1+ の接続統計データ ブロックの形式です。

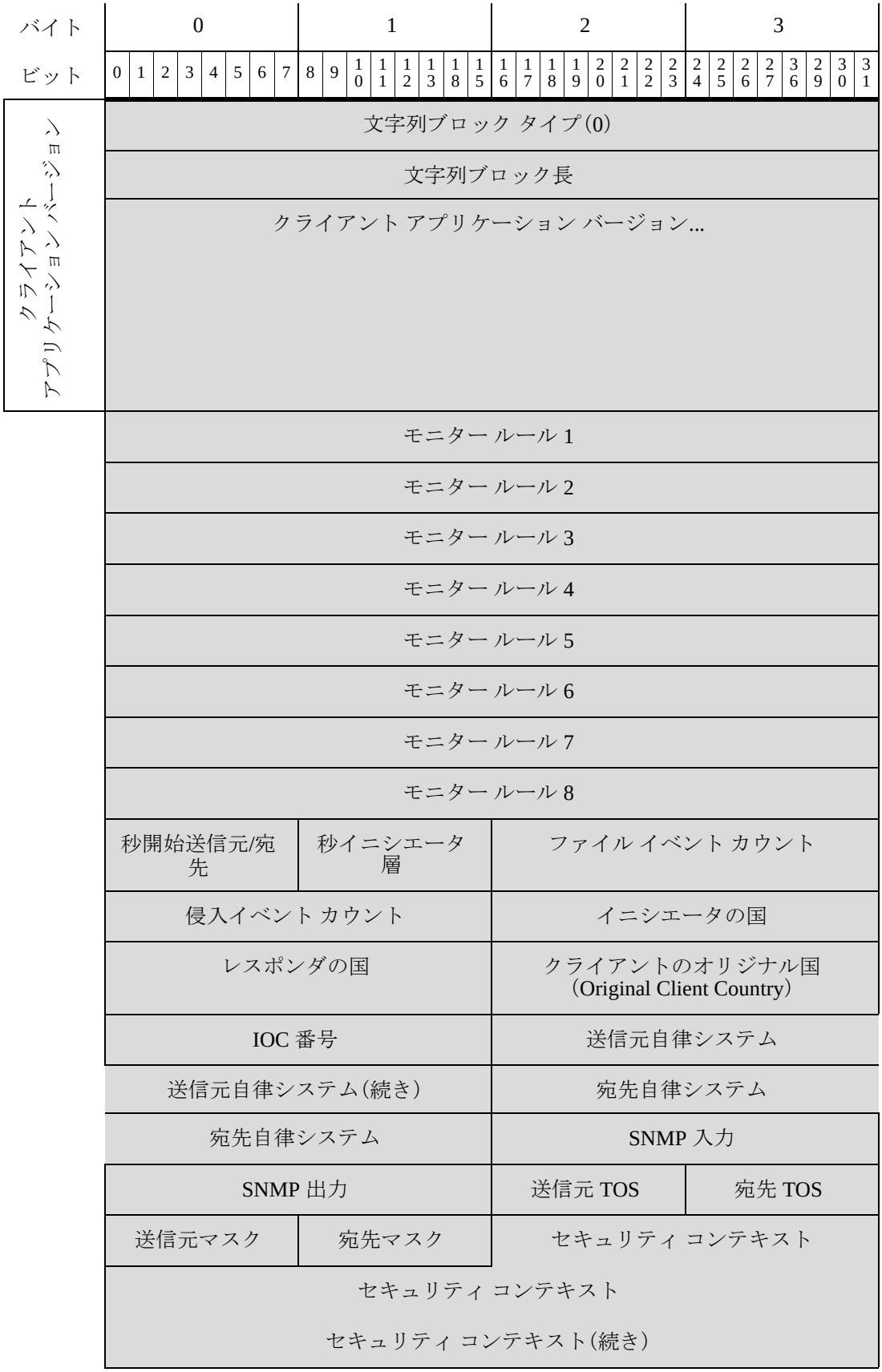
7

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
接続統計データ ブロック タイプ（174）																																
接続統計データ ブロック長																																
デバイスID（Device ID）																																
入力ゾーン																																
入力ゾーン（続き）																																
入力ゾーン（続き）																																
入力ゾーン（続き）																																
出力ゾーン																																
出力ゾーン（続き）																																
出力ゾーン（続き）																																
出力ゾーン（続き）																																
入力インターフェイス																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
入力インターフェイス（続き）																																
出力インターフェイス																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
出力インターフェイス（続き）																																
イニシエータ IP アドレス																																
イニシエータ IP アドレス（続き）																																
イニシエータ IP アドレス（続き）																																
イニシエータ IP アドレス（続き）																																
レスポンダ IP アドレス																																
レスポンダ IP アドレス（続き）																																

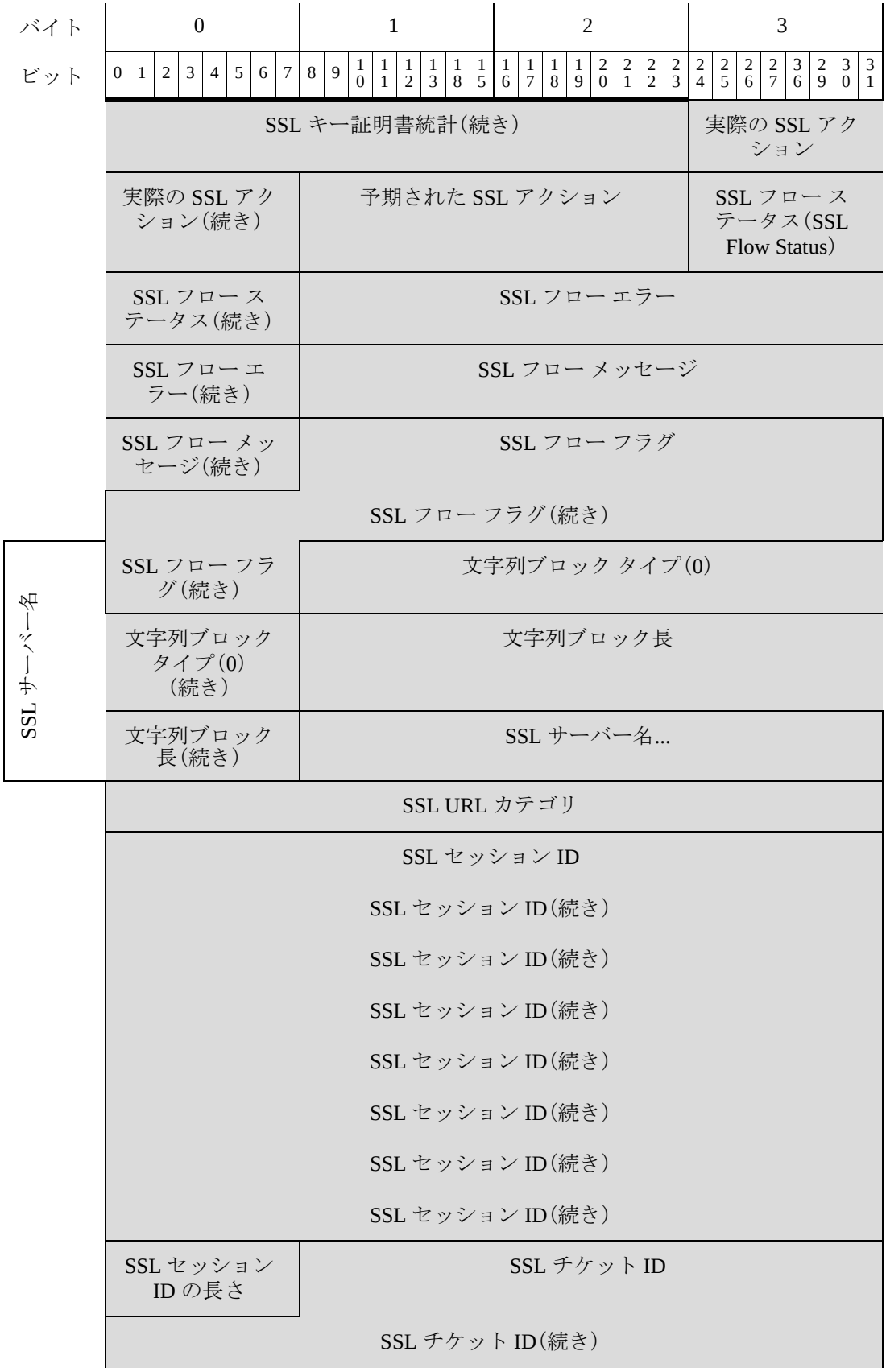

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
レスポンダ IP アドレス（続き）
レスポンダ IP アドレス（続き）
オリジナル クライアント IP アドレス
オリジナル クライアント IP アドレス（続き）
オリジナル クライアント IP アドレス（続き）
オリジナル クライアント IP アドレス（続き）
ポリシー リビジョン
ポリシー リビジョン（続き）
ポリシー リビジョン（続き）
ポリシー リビジョン（続き）
ルール ID
トンネ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

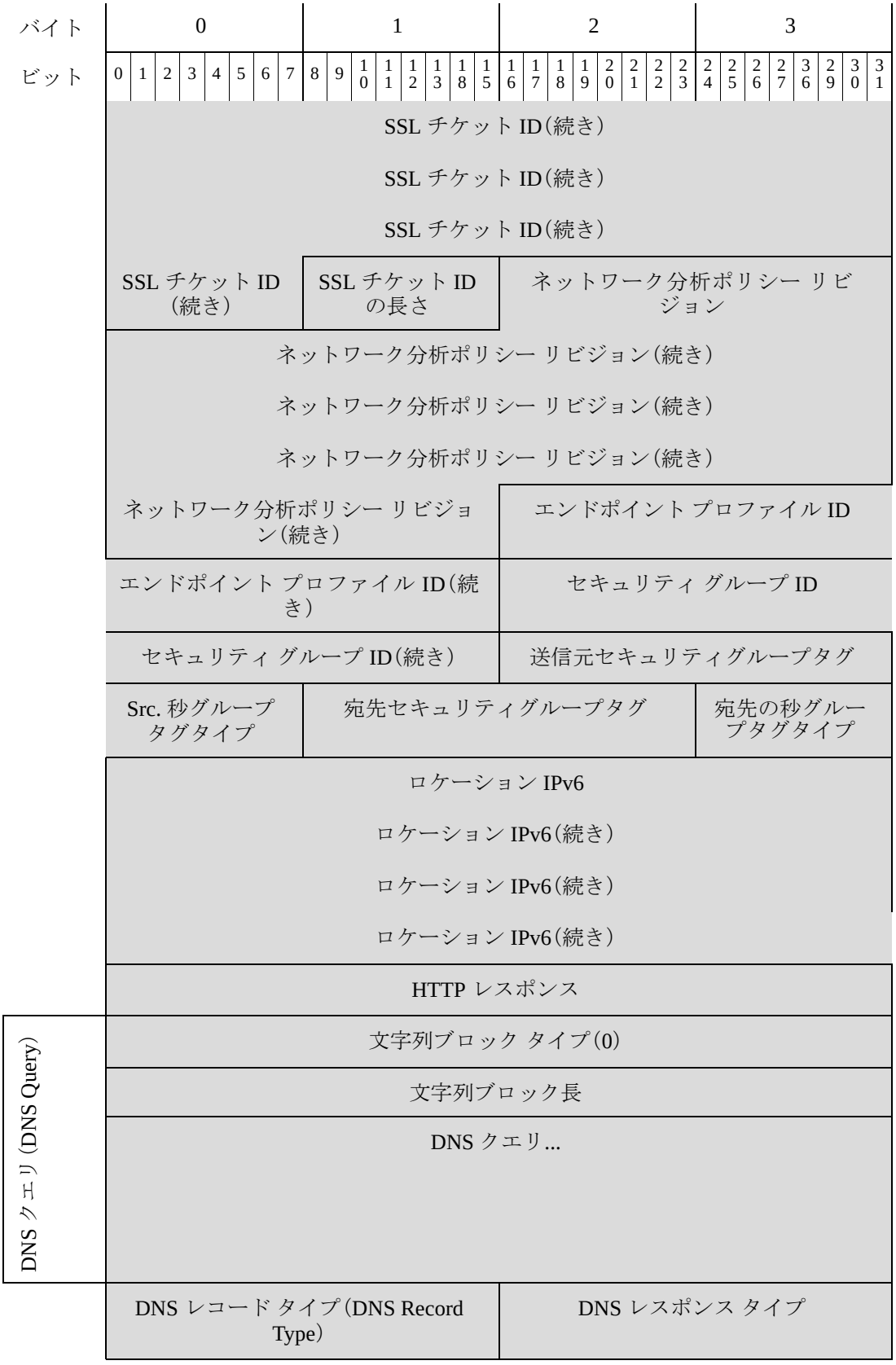

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
最終パケット タイムスタンプ(続き)
イニシエータ送信パケット数
イニシエータ送信パケット数(続き)
イニシエータ送信パケット数(続き)
レスポンダ送信パケット数
レスポンダ送信パケット数(続き)
レスポンダ送信パケット数(続き)
イニシエータ送信バイト数
イニシエータ送信バイト数(続き)
イニシエータ送信バイト数(続き)
レスポンダ送信パケット数
レスポンダ送信バイト数(続き)
レスポンダ送信バイト数(続き)
イニシエータ パケット ドロップ
イニシエータ パケット ドロップ(続き)
イニシエータパケットドロップ(続き)
レスポンダ パケット ドロップ
レスポンダ パケット ドロップ(続き)
レスポンダパケットドロップ(続き)
ドロップしたイニシエータ バイト数
イニシエータ バイト ドロップ(続き)
イニシエータバイト ドロップ(続き)
レスポンダ バイト ドロップ
レスポンダ バイト ドロップ(続き)
レスポンダバイト ドロップ(続き)
QOS 適用インターフェイス
QOS 適用インターフェイス(続き)

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	QOS 適用インターフェイス（続き）																															
	QOS 適用インターフェイス（続き）																															
	QOS インターフェイス（続き）								QOS ルール ID																							
	QOS ルール ID（続き）								ユーザー ID（User ID）																							
	ユーザー ID（続き）								アプリケーション プロトコル ID																							
	アプリケーション プロトコルID（続き）								URL カテゴリ																							
	URL カテゴリ（続き）								URLレピュテーション																							
	URL レピュテーション（続き）								クライアント アプリケーション ID																							
	クライアント アプリケーション ID（続き）								Web アプリケーション ID																							
クライアント URL	Web アプリケーションID（続き）								文字列ブロック タイプ（0）																							
	文字列ブロック タイプ（続き）								文字列ブロック長																							
	文字列ブロック長（続き）								クライアント アプリケーションURL...																							
NetBIOS [名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	NetBIOS 名...																															

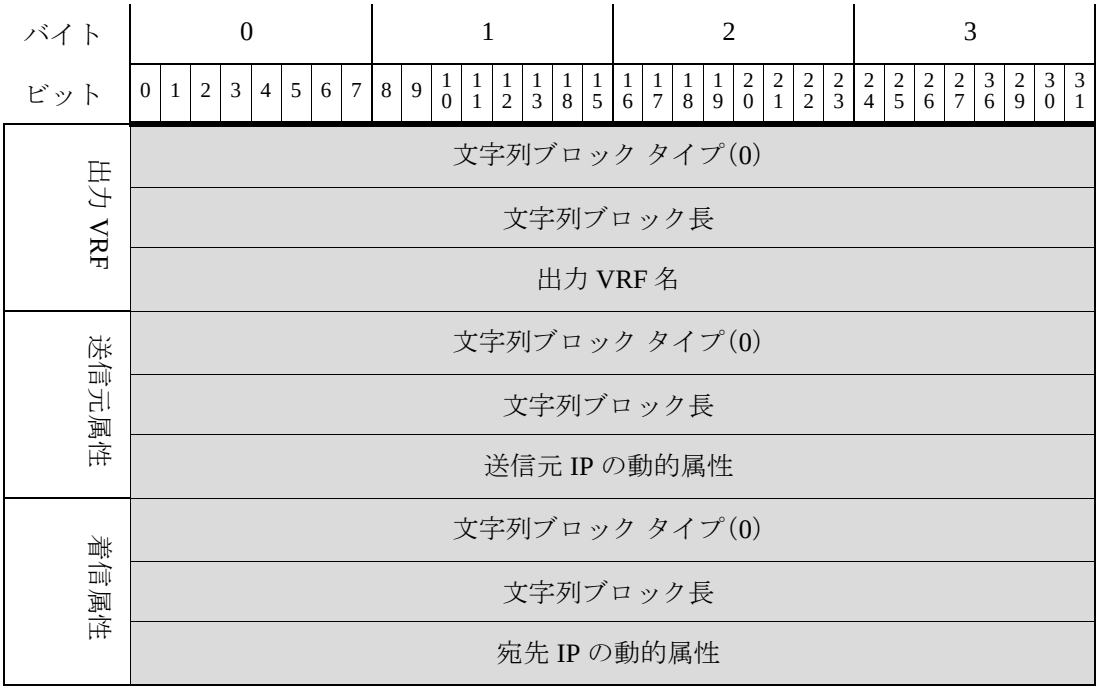

バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
クライアント アプリケーション バージョン
文字列ブロック タイプ(0)
文字列ブロック長
クライアント アプリケーション バージョン...
モニター ルール 1
モニター ルール 2
モニター ルール 3
モニター ルール 4
モニター ルール 5
モニター ルール 6
モニター ルール 7
モニター ルール 8
秒開始送信元/宛先
秒イニシエータ層
ファイル イベント カウント
侵入イベント カウント
イニシエータの国
レスポンダの国
クライアントのオリジナル国(Original Client Country)
IOC 番号
送信元自律システム
送信元自律システム(続き)
宛先自律システム
宛先自律システム
SNMP 入力
SNMP 出力
送信元 TOS
宛先 TOS
送信元マスク
宛先マスク
セキュリティ コンテキスト
セキュリティ コンテキスト
セキュリティ コンテキスト(続き)


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
セキュリティ コンテキスト(続き)
セキュリティ コンテキスト(続き)
VLAN ID(Admin. VLAN ID)
参照ホスト
文字列ブロック タイプ(0)
文字列ブロック長
参照ホスト...
ユーザー エージェント
文字列ブロック タイプ(0)
文字列ブロック長
ユーザー エージェント...
HTTP リファラ
文字列ブロック タイプ(0)
文字列ブロック長
HTTP リファラ...
SSL 証明書フィンガープリント
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL 証明書フィンガープリント(続き)
SSL ポリシー ID
SSL ポリシー ID(続き)
SSL ポリシー ID(続き)
SSL ポリシー ID(続き)
SSL ルール ID
SSL 暗号スイート
SSL バージョン
SSL キー証明書統計


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
SSL キー証明書統計(続き)
実際の SSL アクション
実際の SSL アクション(続き)
予期された SSL アクション
SSL フロー ステータス(SSL Flow Status)
SSL フロー ステータス(続き)
SSL フロー エラー
SSL フロー エラー(続き)
SSL フロー メッセージ
SSL フロー メッセージ(続き)
SSL フロー フラグ
SSL フロー フラグ(続き)
SSL フロー フラグ(続き)
文字列ブロック タイプ(0)
文字列ブロック タイプ(0)(続き)
文字列ブロック長
文字列ブロック長(続き)
SSL サーバー名...
SSL サーバー名
SSL URL カテゴリ
SSL セッション ID
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID(続き)
SSL セッション ID の長さ
SSL チケット ID
SSL チケット ID(続き)


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
SSL チケット ID（続き）
SSL チケット ID（続き）
SSL チケット ID（続き）
SSL チケット ID（続き）
SSL チケット ID の長さ
ネットワーク分析ポリシー リビジョン
ネットワーク分析ポリシー リビジョン（続き）
ネットワーク分析ポリシー リビジョン（続き）
ネットワーク分析ポリシー リビジョン（続き）
ネットワーク分析ポリシー リビジョン（続き）
エンドポイント プロファイル ID
エンドポイント プロファイル ID（続き）
セキュリティ グループ ID
セキュリティ グループ ID（続き）
送信元セキュリティグループタグ
Src. 秒グループ タグタイプ
宛先セキュリティグループタグ
宛先の秒グループタグタイプ
ロケーション IPv6
ロケーション IPv6（続き）
ロケーション IPv6（続き）
ロケーション IPv6（続き）
HTTP レスポンス
DNS クエリ（DNS Query）
文字列ブロック タイプ（0）
文字列ブロック長
DNS クエリ...
DNS レコード タイプ（DNS Record Type）
DNS レスポンス タイプ


バイト
0
1
2
3
ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 18 15 16 17 18 19 20 21 22 23 24 25 26 27 36 29 30 31
DNS TTL
シンクホール UUID
シンクホール UUID（続き）
シンクホール UUID（続き）
シンクホール UUID（続き）
セキュリティ インテリジェンス リスト 1
セキュリティ インテリジェンス リスト 2
脅威インテリジェンスカテゴリ
TLS FP プロセス
文字列ブロック タイプ（0）
文字列ブロック長
TLS FP プロセス
プロセス信頼度
マルウェア信頼度
マルウェアインデックス
クライアントディテクタ
NAT イニシエータポート
NAT レスポンダポート
NAT イニシエータ IP アドレス
NAT イニシエータ IP アドレス（続き）
NAT イニシエータ IP アドレス（続き）
NAT イニシエータ IP アドレス（続き）
NAT レスポンダ IP アドレス
NAT レスポンダ IP アドレス（続き）
NAT レスポンダ IP アドレス（続き）
NAT レスポンダ IP アドレス（続き）
入力 VRF
文字列ブロック タイプ（0）
文字列ブロック長
入力 VRF 名



次の表では、7.1+ の接続統計データ ブロックのフィールドについて説明します。

表 4-71　接続統計データ ブロック 7.1+ のフィールド

フィールド	データタイプ	説明
接続統計データ ブロック タイプ	uint32	7.1+ の接続統計データ ブロックを開始します。値は常に 174 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイスID（Device ID）	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティ ゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティ ゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポンダ IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。

表 4-71　接続統計データ ブロック 7.1+ のフィールド （続き）

フィールド	データタイプ	説明
オリジナル クライアント IP アドレス	uint8[16]	要求の送信元であるプロキシの背後にあるホストの IP アドレス(オクテットの IP アドレス)。
ポリシー リビジョン	uint8[16]	トリガーされた相関イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
トンネル ルール ID	uint32	イベントにトリガーをかけたトンネル ルールの内部 ID(該当する場合)。
ルール アクション	uint16	そのルールに対してユーザー インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint32	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポンダ ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID（Instance ID）	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケット タイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケット タイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポンダ送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポンダ送信バイト数	uint64	応答ホストから送信バイト数。
イニシエータ パケット ドロップ	uint64	レート制限により、セッション イニシエータからドロップしたパケット数。
レスポンダ パケット ドロップ	uint64	レート制限により、セッション レスポンダからドロップしたパケット数。
ドロップしたイニシエータ バイト数	uint64	レート制限により、セッション イニシエータからドロップしたバイト数。

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

フィールド	データタイプ	説明
レスポンダ バイト ドロップ	uint64	レート制限により、セッション レスポンダからドロップしたバイト数。
QOS 適用インターフェイス	uint8[16]	レート制限された接続で、レート制限が適用されるインターフェイスの名前。
QOS ルール ID	uint32	接続に適用される QoS ルールの内部 ID 番号（該当する場合）。
ユーザー ID（User ID）	uint32	トラフィックを生成したホストの最終ログイン ユーザーの内部 ID 番号。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URL レピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号（該当する場合）。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号（該当する場合）。
文字列ブロック タイプ	uint32	クライアント アプリケーション URL の文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション URL の文字列データ ブロックのバイト数（文字列ブロック タイプと長さのフィールド用の 8 バイト、およびクライアント アプリケーション URL 文字列のバイト数を含む）。
クライアント アプリケーション URL	string	クライアント アプリケーションがアクセスする URL（該当する場合）（`/files/index.html` など）。
文字列ブロック タイプ	uint32	ホストの NetBIOS 名の文字列データ ブロックを表示します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプ フィールドおよび文字列ブロック長フィールドの 8 バイトを含む文字列データ ブロック内のバイト数と NetBIOS 名文字列のバイト数。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアント アプリケーション バージョンの文字列データ ブロックのバイト数（文字列ブロック タイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む）。
クライアント アプリケーション バージョン	string	クライアント アプリケーション バージョン。
モニター ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニター ルールの ID。

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

フィールド	データタイプ	説明
モニター ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニター ルールの ID。
モニター ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニター ルールの ID。
モニター ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニター ルールの ID。
モニター ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニター ルールの ID。
モニター ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニター ルールの ID。
モニター ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニター ルールの ID。
モニター ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニター ルールの ID。
セキュリティ インテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスが IP ブロックリストに一致しているかどうか。
セキュリティ インテリジェンス層	uint8	IP ブロックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入イベント カウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポンダの国	uint 16	応答ホストの国のコード。
クライアントのオリジナル国（Original Client Country）	uint 16	要求を開始したプロキシの背後にあるホストの国コード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。
SNMP 出力	uint16	出力インターフェイスの SNMP インデックス
送信元 TOS	uint8	着信インターフェイス用のタイプ オブ サービス バイト設定。
宛先 TOS	uint8	発信インターフェイス用のタイプ オブ サービス バイト設定。
送信元マスク	uint8	送信元アドレス プレフィックス マスク。

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

フィールド	データタイプ	説明
宛先マスク	uint8	宛先アドレス プレフィックス マスク。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
VLAN ID（Admin. VLAN ID）	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
文字列ブロック タイプ	uint32	参照ホストを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	参照ホスト文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および参照ホスト フィールドのバイト数を含む)。
参照ホスト	string	HTTP または DNS で提供されるホスト名情報。
文字列ブロック タイプ	uint32	ユーザー エージェントを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザー エージェント文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザー エージェント フィールドのバイト数を含む)。
ユーザー エージェント	string	セッションのユーザー エージェント ヘッダー フィールドからの情報。
文字列ブロック タイプ	uint32	HTTP リファラを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	HTTP リファラ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および HTTP リファラ フィールドのバイト数を含む)。
HTTP リファラ	string	ページの発生元のサイト。これは HTTP トラフィック内の参照ヘッダー情報にあります。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバー証明書の SHA1 ハッシュ。
SSL ポリシー ID	uint8[16]	接続を処理した SSL ポリシーの ID 番号。
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルト アクションの ID 番号。
SSL 暗号スイート	uint16	SSL 接続で使用される暗号スイート。値は 10 進形式で保存されます。値により指定されている暗号スイートの詳細については、www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
SSL バージョン	uint8	接続の暗号化に使用された SSL または TLS プロトコル バージョン。

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

フィールド	データタイプ	説明
SSL サーバー証明書ステータス	uint32	SSL 証明書のステータス。有効な値は次のとおりです。 • 0(チェックなし):サーバー証明書のステータスは評価されませんでした。 • 1(不明):サーバー証明書のステータスは判別できませんでした。 • 2(有効):サーバー証明書は有効です。 • 4(自己署名済み):サーバー証明書は自己署名です。 • 16(無効な発行者):サーバー証明書に無効な発行者があります。 • 32(無効な署名):サーバー証明書に無効な署名があります。 • 64(期限切れ):サーバー証明書は期限切れです。 • 128(まだ有効でない):サーバー証明書はまだ有効ではありません。 • 256(取り消し):サーバー証明書は取り消されました。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」
予期された SSL アクション	uint16	SSL ルールに基づいて接続に対して実行する必要があるアクション。有効な値は次のとおりです。 • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

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

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

フィールド	データタイプ	説明
SSL フロー メッセージ	uint32	SSL ハンドシェイク時にクライアントとサーバーとの間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。 • 0x00000001：NSE_MT__HELLO_REQUEST • 0x00000002：NSE_MT__CLIENT_ALERT • 0x00000004：NSE_MT__SERVER_ALERT • 0x00000008：NSE_MT__CLIENT_HELLO • 0x00000010：NSE_MT__SERVER_HELLO • 0x00000020：NSE_MT__SERVER_CERTIFICATE • 0x00000040：NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080：NSE_MT__CERTIFICATE_REQUEST • 0x00000100：NSE_MT__SERVER_HELLO_DONE • 0x00000200：NSE_MT__CLIENT_CERTIFICATE • 0x00000400：NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800：NSE_MT__CERTIFICATE_VERIFY • 0x00001000：NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000：NSE_MT__CLIENT_FINISHED • 0x00004000：NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000：NSE_MT__SERVER_FINISHED • 0x00010000：NSE_MT__NEW_SESSION_TICKET • 0x00020000：NSE_MT__HANDSHAKE_OTHER • 0x00040000：NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000：NSE_MT__APP_DATA_FROM_SERVER
SSL フロー フラグ	uint64	暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。 • 0x00000001（NSE_FLOW__VALID）：他のフィールドを有効にするために設定する必要があります • 0x00000002（NSE_FLOW__INITIALIZED）：内部構造が処理可能です • 0x00000004（NSE_FLOW__INTERCEPT）：SSL セッションが代行受信されました
文字列ブロック タイプ	uint32	SSL サーバー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	SSL サーバー名文字列データ ブロックに含まれるバイト数（ブロック タイプとヘッダー フィールド用の 8 バイト、および SSL サーバー名フィールドのバイト数を含む）。

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

フィールド	データタイプ	説明
SSL サーバー名	string	SSL Client Hello でサーバー名に指定された名前。
SSL URL カテゴリ	uint32	サーバー名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバーがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできます。
SSL チケット ID	uint8[20]	クライアントとサーバーがセッション チケットの使用に同意する場合に使用されるセッション チケットのハッシュ。
SSL チケット ID の長さ	uint8	SSL チケット ID の長さ。チケット ID は 20 バイトより長くすることはできませんが、20 バイト未満であってもかまいません。
ネットワーク分析ポリシー リビジョン	uint8[16]	接続イベントに関連付けられているネットワーク分析ポリシーのリビジョン。
エンドポイント プロファイル ID	uint32	ISE により識別される、接続エンドポイントで使用されるデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
セキュリティ グループ ID	uint32	ポリシーに基づいて ISE によりユーザーに割り当てられた ID 番号。
送信元セキュリティグループタグ	uint16	接続の送信元のセキュリティグループタグ。
送信元セキュリティ グループ タグ タイプ	uint8	送信元セキュリティグループタグの割り当て方法: • 0:不明 • 1:インライン • 2:セッションディレクトリ • 3:Security Group Tag Exchange Protocol（SXP）
宛先セキュリティグループタグ	uint16	接続の宛先のセキュリティグループタグ。
宛先セキュリティ グループ タグ タイプ	uint8	宛先セキュリティグループタグの割り当て方法: • 0:不明 • 1:インライン • 2:セッションディレクトリ • 3:Security Group Tag Exchange Protocol（SXP）
ロケーション IPv6	uint8[16]	ISE と通信するインターフェイスの IP アドレス。IPv4 または IPv6 のアドレスを使用できます。

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

フィールド	データタイプ	説明
HTTP レスポンス	uint32	HTTP 要求の応答コード。
文字列ブロック タイプ	uint32	DNS クエリを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データ ブロックのバイト数（文字列ブロック タイプと長さのフィールド用の 8 バイト、および DNS クエリ文字列のバイト数を含む）。
DNS クエリ（DNS Query）	string	DNS サーバーに送信されたクエリの内容。
DNS レコード タイプ（DNS Record Type）	uint16	DNS レコード タイプの数値。
DNS レスポンス タイプ	uint16	DNS 応答タイプの数値。
DNS TTL	uint32	DNS レスポンスの存続期間（秒単位）。
シンクホール UUID	uin8[16]	このシンクホール オブジェクトに関連付けられているリビジョン UUID。
セキュリティ インテリジェンス リスト 1	uint32	イベントに関連付けられているセキュリティ インテリジェンス リスト。これは、関連メタデータのセキュリティ インテリジェンス リストにマップされます。接続に関連付けられた 3 つのセキュリティ インテリジェンス リストが存在する場合があります。
セキュリティ インテリジェンス リスト 2	uint32	イベントに関連付けられているセキュリティ インテリジェンス リスト。これは、関連メタデータのセキュリティ インテリジェンス リストにマップされます。接続に関連付けられた 3 つのセキュリティ インテリジェンス リストが存在する場合があります。
脅威インテリジェンスカテゴリ	uint32	イベントに関連付けられた脅威インテリジェンスカテゴリ。これは、関連メタデータの脅威インテリジェンスリストにマップされます。
文字列ブロック タイプ	uint32	TLS フィンガープリントプロセスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの 8 バイトとTLS フィンガープリント プロセス フィールドのバイト数が含まれます。
TLS フィンガープリント プロセス	文字列	暗号化された可視性エンジンからの識別されたフィンガープリントのプロセス名ファミリ。
TLSFP プロセス信頼度	uint8	暗号化された可視性エンジン（EVE）が適切なプロセスを検出しているかを示す 0 ? 100% の範囲内の信頼値。たとえば、プロセス名が Firefox で、信頼スコアが 80% の場合、エンジンが検出したプロセスが Firefox であると 80% 信頼していることを示します。

表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

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

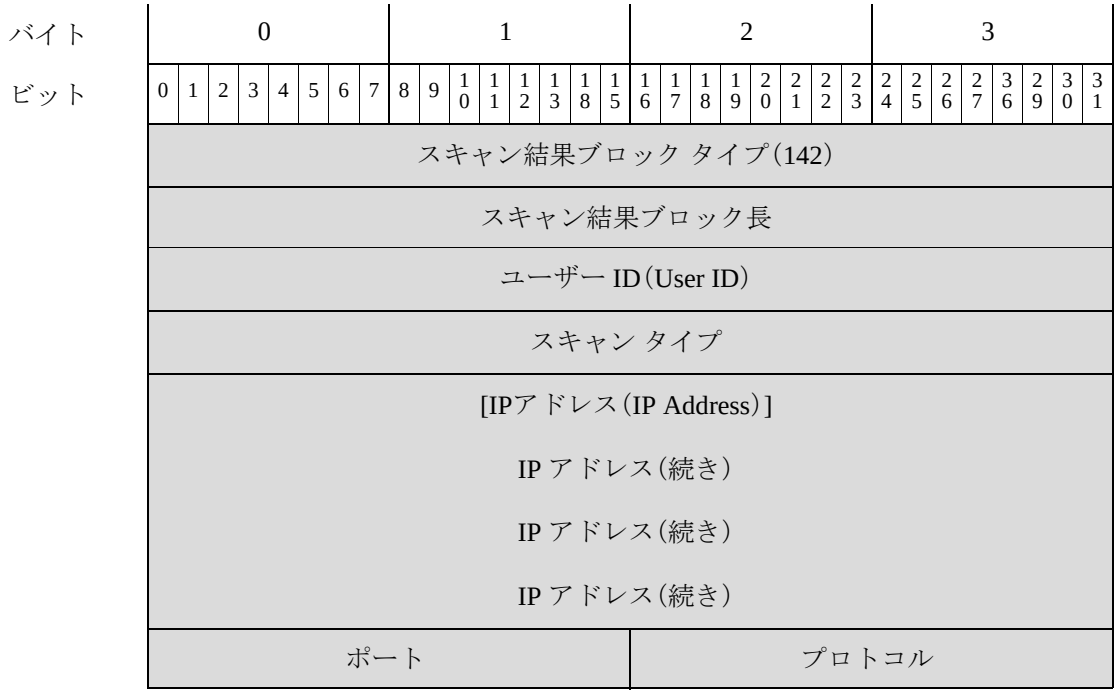
表 4-71　接続統計データ ブロック 7.1+ のフィールド（続き）

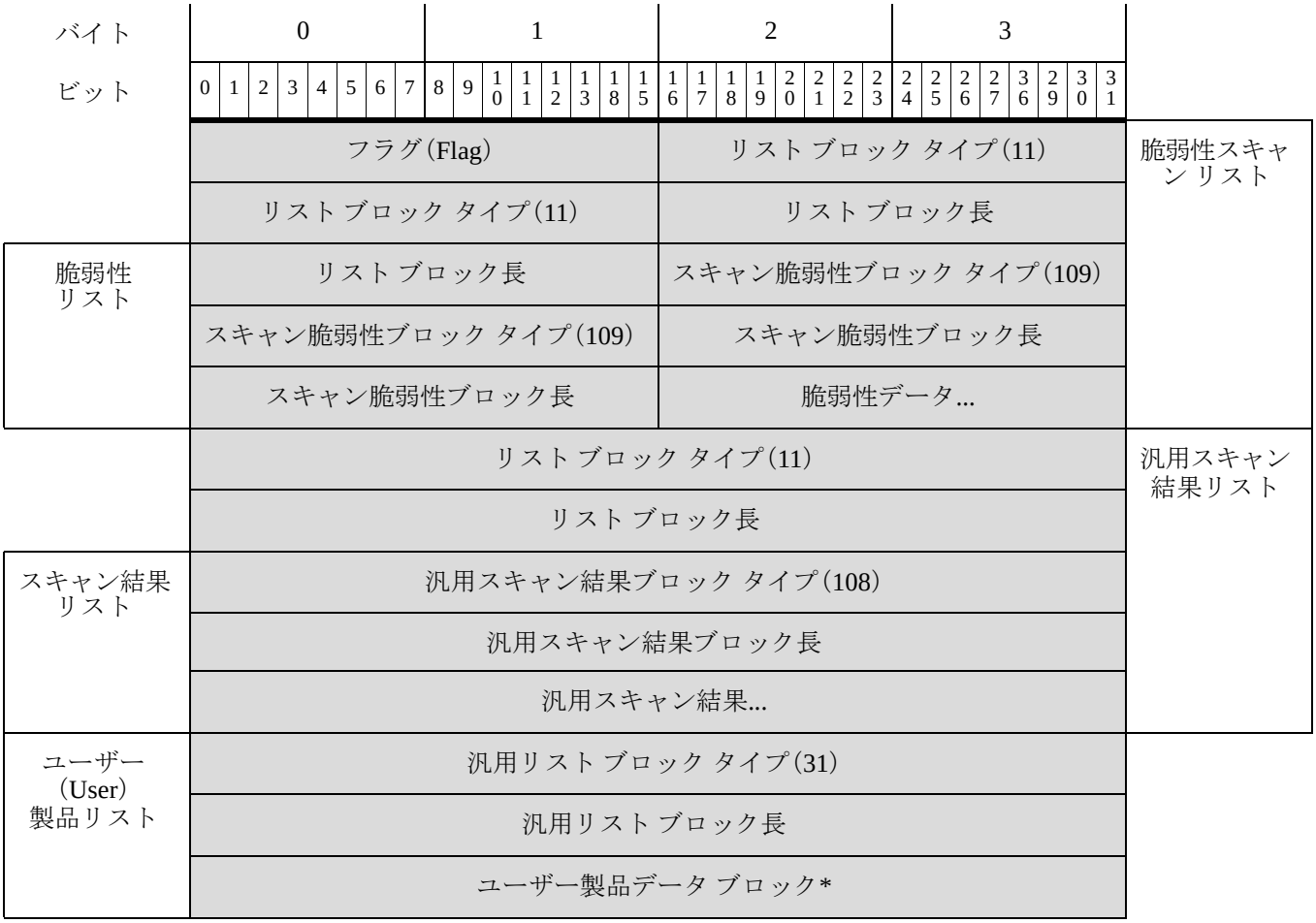
フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	宛先 IP の動的属性の名前を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数。ブロックタイプとヘッダーフィールドの 8 バイト、および宛先 IP の動的属性フィールドのバイト数が含まれています。
宛先 IP の動的属性	文字列	宛先 IP アドレスに関連付けられた動的属性。

スキャン結果データ ブロック 5.2+

スキャン結果データ ブロックは、脆弱性を説明し、スキャン結果追加イベント内で使用されます（イベント タイプ 1002、サブタイプ 11）。スキャン結果データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 142 です。これはブロック タイプ 102 に置き換わります。IP アドレス フィールドはバージョン 5.2 で 16 バイトに増えました。

次の図は、スキャン結果データ ブロックの形式を示しています。





次の表は、スキャン結果データ ブロックのフィールドについての説明です。

表 4-72　スキャン結果データ ブロックのフィールド

フィールド	データタイプ	説明
スキャン結果ブロック タイプ	uint32	スキャン結果データ ブロックを開始します。この値は常に 142 です。
スキャン結果ブロック長	uint32	スキャン脆弱性データブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン脆弱性データのバイト数を含む)。
ユーザー ID (User ID)	uint32	スキャン結果をインポートしたユーザー、またはスキャン結果を生成したスキャンを実行したユーザーのユーザー ID 番号が含まれます。
スキャン タイプ	uint32	結果がシステムに追加された方法を示します。
[IPアドレス(IP Address)]	uint8[16]	IP アドレス オクテットの、結果の脆弱性によって影響を受けるホストの IP アドレス。
[ポート(Port)]	uint16	結果の脆弱性の影響を受ける、サブサーバーで使用されるポート。

表 4-72　スキャン結果データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6：TCP • 17：UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048：IP
フラグ（Flag）	uint16	予約済
リスト ブロック タイプ	uint32	トランスポート スキャン脆弱性データを伝えるスキャン脆弱性データ ブロックで構成されるリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのスキャン脆弱性データ ブロックが含まれています。 このフィールドには、ゼロ以上のスキャン脆弱性データ ブロックが続きます。
スキャン脆弱性ブロック タイプ	uint32	スキャン中に検出された脆弱性を記述するスキャン脆弱性データ ブロックを開始します。この値は常に 109 です。
スキャン脆弱性ブロック長	uint32	スキャン脆弱性データブロックのバイト数（接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン脆弱性データのバイト数を含む）。
脆弱性データ	string	各脆弱性に関する情報。
リスト ブロック タイプ	uint32	トランスポート スキャン脆弱性データを伝えるスキャン脆弱性データ ブロックで構成されるリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数には、リスト ブロック タイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのスキャン脆弱性データ ブロックが含まれています。 このフィールドには、ゼロ以上のスキャン脆弱性データ ブロックが続きます。
汎用スキャン結果ブロック タイプ	uint32	スキャン中に検出されたサーバーおよびオペレーティング システムを記述する汎用スキャン結果データ ブロックを開始します。この値は常に 108 です。
汎用スキャン結果ブロック長	uint32	汎用スキャン結果データ ブロックのバイト数（汎用スキャン結果ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン結果データのバイト数を含む）。
汎用スキャン結果データ	string	各スキャン結果に関する情報。

表 4-72　スキャン結果データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
汎用リスト ブロック タイプ	uint32	サードパーティ アプリケーションからのホスト入力データを伝送するユーザー製品データブロックを構成する、汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのユーザー製品データ ブロックを含む）。
ユーザー製品データ ブロック*	変数（variable）	ホスト入力データを含むユーザー製品データ ブロック。このデータブロックの説明の詳細については、ユーザー製品データ ブロック 5.1+（4-183 ページ）を参照してください。

ホスト サーバー データ ブロック 4.10.0+

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

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

次の図は、ホスト サーバー データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	汎用リスト ブロック長																															
Web Application	Web アプリケーション ブロック タイプ(123)*																															
	Web アプリケーション ブロック長																															
	Web アプリケーション データ...																															

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

表 4-73　　ホスト サーバー データ ブロックのフィールド

フィールド	データタイプ	説明
ホスト サーバー ブロック タイプ	uint32	ホスト サーバー データ ブロックを開始します。この値は常に 103 です。
ホスト サーバー ブロック長	uint32	ホスト サーバー ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたホスト サーバー データ ブロックの合計バイト数。
[ポート(Port)]	uint16	サーバーが実行しているポート番号。
ヒット	uint32	サーバーが受信したヒット数。
前回の使用(Last Used)	uint32	システムが使用中のサーバーを検出した前回時刻を表す UNIX タイムスタンプ。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたサブサーバー情報データ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
サーバー情報データ ブロック*	変数(variable)	リスト ブロック長の最大バイト数を上限としたサーバー情報データ ブロック。詳細は、4.10.x、5.0 ～ 5.0.2 のサーバー情報データ ブロック (4-155 ページ) を参照してください。
信頼度	uint32	信頼度のパーセンテージ。
汎用リスト ブロック タイプ	uint32	包括的データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	包括的ブロックとカプセル化された Web アプリケーション データ ブロックのバイト数。この数値は、カプセル化された Web アプリケーション データ ブロックすべてにバイト数と汎用リスト ブロックの 8 バイトのヘッダー フィールドを示します。
Web アプリケーション データ ブロック*	変数(variable)	リスト ブロック長の最大バイト数を上限としてカプセル化した Web アプリケーション データ ブロック。詳細は、5.0+の Web アプリケーション データ ブロック (4-124 ページ) を参照してください。

フル ホスト サーバー データ ブロック 4.10.0+

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

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

次の図は、フル サーバー データ ブロックの形式です。

::

	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	フル サーバー ブロック タイプ(104)																																
	フル サーバー ブロック長																																
	[ポート(Port)]																	ヒット															
サブサーバー - シスコ	ヒット(続き)																	汎用リスト ブロック タイプ(31)															
	汎用リスト ブロック タイプ(続き)																	汎用リスト ブロック長															
	汎用リスト ブロック長(続き)																	フル サーバー情報データ ブロック (106)*															
サブサーバー - ユーザー (User)	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
	フル サーバー情報データ ブロック タイプ(106)*																																
サブサーバー - スキャナ	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
	フル サーバー情報データ ブロック(106)*																																
サブサーバー - Application	汎用リスト ブロック タイプ(31)																																
	汎用リスト ブロック長																																
	フル サーバー情報データ ブロック(106)*																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	信頼度																															
サーバー バナー	BLOB ブロック タイプ（10）																															
	BLOB ブロック長																															
	サーバー バナー データ...																															
VDB 脆弱性	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
	（VDB）ホスト脆弱性データ ブロック（85）*																															
サードパーティ/VDB 脆弱性	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
	（サードパーティ/VDB）ホスト脆弱性データ ブロック（85）*																															
サードパーティ ホスト 脆弱性	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
	（サードパーティ）ホスト脆弱性データ ブロック（85）*																															
Web Application	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
	Web アプリケーション データ（123）*																															

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

表 4-74　　フル ホスト サーバー データ ブロック 4.10.0+ のフィールド

フィールド	データタイプ	説明
フル サーバー ブロック タイプ	uint32	フル サーバー データ ブロックを開始します。この値は常に 104 です。
フル サーバー ブロック長	uint32	フル サーバー ブロック タイプ フィールドと長さ フィールドの 8 バイトに、後続のフル サーバー データのバイト数を加えたフル サーバー データ ブロックの合計バイト数。
[ポート（Port）]	uint16	サーバー ポート番号。
ヒット	uint32	サーバーが受信したヒット数。

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

フィールド	データタイプ	説明
汎用リスト ブロック タイプ	uint32	検出したサブサーバー データでデータ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのサブサーバー情報データ ブロックを含む汎用リスト データ ブロックのバイト数。
サブサーバー情報 - シスコ データ ブロック *	変数（variable）	シスコ が検出したホスト サーバーのサブサーバーに関する情報を含むフル サーバー情報データ ブロック。このデータ ブロックの説明の詳細については、フル サーバー情報データ ブロック（4-158 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	ユーザーが追加したサブサーバー データを伝えるサブサーバー情報データ ブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのサーバー情報データ ブロックを含む汎用リスト データ ブロックのバイト数。
サブサーバー情報 - ユーザーが追加したデータ ブロック *	変数（variable）	ユーザーが検出したホスト サーバーのサブサーバーに関する情報を含むフル サーバー情報データ ブロック。このデータ ブロックの説明の詳細については、フル サーバー情報データ ブロック（4-158 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	スキャナが追加したサブサーバー データを伝えるサブサーバー情報データ ブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのサブサーバー情報データ ブロックを含む汎用リスト データ ブロックのバイト数。
サブサーバー情報 - スキャンで追加したデータ ブロック *	変数（variable）	スキャナが検出したホスト サーバーのサブサーバーに関する情報を含むフル サーバー情報データ ブロック。このデータ ブロックの説明の詳細については、フル サーバー情報データ ブロック（4-158 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	アプリケーションが追加したサブサーバー データを伝えるサブサーバー情報データ ブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのサブサーバー情報データ ブロックを含む汎用リスト データ ブロックのバイト数。
サブサーバー情報 - アプリケーションが追加したデータ ブロック *	変数（variable）	アプリケーションが検出したホスト サーバーのサブサーバーに関する情報を含むフル サーバー情報データ ブロック。このデータ ブロックの説明の詳細については、フル サーバー情報データ ブロック（4-158 ページ）を参照してください。

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

フィールド	データタイプ	説明
信頼度	uint32	フル サーバー データの正しい識別における シスコ の信頼度のパーセンテージ。
BLOB ブロック タイプ	uint32	バナー データを含む BLOB データ ブロックを開始します。この値は常に 10 です。
BLOB ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに、バナーのバイト数を加えた BLOB データ ブロックのバイト数。
サーバー バナー データ	byte[*n*]	パケットの最初の *n* バイトがサーバー イベントに関わるバイトであり、*n* は 256 以下です。
汎用リスト ブロック タイプ	uint32	シスコ 脆弱性データを搬送するホスト脆弱性データ ブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのホスト脆弱性データ ブロックを含む汎用リスト データ ブロックのバイト数。
（VDB）ホスト脆弱性データ ブロック*	変数（variable）	脆弱性データベース（VDB）でホスト脆弱性に関する情報を格納したホスト脆弱性データ ブロック。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+（4-119 ページ） を参照してください。
汎用リスト ブロック タイプ	uint32	サードパーティ スキャナで得られ、すでに VDB に登録されている脆弱性に関する情報を格納したサードパーティ ホスト脆弱性データを伝送するホスト脆弱性データ ブロックで構成された、汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのホスト脆弱性データ ブロックを含む汎用リスト データ ブロックのバイト数。
（サード パーティ /VDB）ホスト脆弱性データ ブロック*	変数（variable）	サードパーティ スキャナで得られ、脆弱性データベース（VDB）に登録されているホスト脆弱性に関する情報を格納したホスト脆弱性データ ブロック。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+（4-119 ページ） を参照してください。
汎用リスト ブロック タイプ	uint32	サードパーティ スキャナで生成したサードパーティ ホスト脆弱性データを伝送する、ホスト脆弱性データ ブロックで構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべてのホスト脆弱性データ ブロックを含む汎用リスト データ ブロックのバイト数。

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

フィールド	データタイプ	説明
サードパーティ スキャン ホスト脆弱性データ ブロック*	変数（variable）	サードパーティ スキャナで識別されたが VDB には登録されていない脆弱性に関する、サードパーティ脆弱性データを含むホスト脆弱性データ ブロック。このデータ ブロックの説明の詳細については、ホスト脆弱性データ ブロック 4.9.0+（4-119 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化された Web アプリケーション データ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
Web アプリケーション データ ブロック*	変数（variable）	リスト ブロック長の最大バイト数を上限としてカプセル化した Web アプリケーション データ ブロック。

4.10.x、5.0 ～ 5.0.2 のサーバー情報データ ブロック

サーバー情報データ ブロックは、サーバー ID、サーバー ベンダーとバージョン、送信元情報など、サーバーに関する情報を伝えます。サーバー情報データ ブロックのブロック タイプは、4.10.x のシリーズ 1 ブロック グループのブロック タイプ 105 と、5.0 ～ 5.0.2 のシリーズ 1 ブロック グループのブロック タイプ 117 です。サーバー情報データ ブロックは、ホスト サーバー ブロックとフル ホスト サーバー データ ブロックのリストで搬送されます。詳細については、ホスト サーバー データ ブロック 4.10.0+（4-149 ページ）と フル ホスト サーバー データ ブロック 4.10.0+（4-151 ページ）を参照してください。

次の図は、サーバー情報データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
サーバー情報ブロック タイプ（105	117）																															
サーバー情報ブロック長																																
アプリケーション ID（Application ID）																																
文字列ブロック タイプ（0）																																
文字列ブロック長																																
サーバー ベンダー名 文字列...																																

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

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

表 4-75　　サーバー情報データ ブロックのフィールド

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

表 4-75　サーバー情報データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	サーバー バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにサーバー バージョンのバイト数を加えたサーバー バージョン文字列データ ブロックのバイト数。
サーバー バージョン	string	サーバー バージョン
前回使用時刻	uint32	トラフィックで前回サーバー情報を使用した時刻を示します。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA）がサーバー データを提供した場合、0 • ユーザーがサーバー データを提供した場合、1 • サードパーティ スキャナがサーバー データを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでサーバー データを提供した場合、3
ソース	uint32	サーバー データの送信元にマッピングするID 番号。送信元タイプによって、これは無応答（RNA）、ユーザー、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
リスト ブロック タイプ	uint32	サブサーバー データ ブロック リストを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のカプセル化されたサブサーバー データブロックのバイト数を加えたリスト データ ブロックの合計バイト数。
サブサーバー ブロック タイプ	uint32	最初のサブサーバー データ ブロックを開始します。このデータ ブロックには、他のサブサーバー データ ブロックを、リスト ブロック長フィールドで定義した上限まで続けることができます。
サブサーバー ブロック長	uint32	サブサーバー ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えた各サブサーバー データ ブロックの合計バイト数。
サブサーバー データ	変数（variable）	サブサーバー データ ブロック（4-78 ページ） に記載のサブサーバー データ。

フル サーバー情報データ ブロック

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

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

次の図は、フル サーバー情報データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	フル サーバー ブロック タイプ（106）																															
	フル サーバー ブロック長																															
	アプリケーション プロトコル ID																															
ベンダー	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ベンダー名文字列...																															
バージョン	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	バージョン文字列...																															
	前回の使用（Last Used）																															
	ソース タイプ																															
	ソース																															
	リスト ブロック タイプ（11）																															
	リスト ブロック長																															
サブサーバー	フル サブサーバー ブロック タイプ（51）*																															
	フル サブサーバー ブロック長																															
	フル サブサーバー データ...																															

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

表 4-76　フル サーバー情報データ ブロックのフィールド

フィールド	データタイプ	説明
フル サーバー情報ブロック タイプ	uint32	フル サーバー情報データ ブロックを開始します。この値は常に 106 です。
フル サーバー情報ブロック長	uint32	フル サーバー ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のフル サーバー データのバイト数を加えたフル サーバー情報データ ブロックの合計バイト数。
アプリケーション プロトコル ID	uint32	サーバーで実行しているアプリケーション プロトコルのアプリケーション ID。
文字列ブロック タイプ	uint32	アプリケーション プロトコル ベンダー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにベンダー名のバイト数を加えたベンダー名文字列データ ブロックのバイト数。
ベンダー名（Vendor Name）	string	サーバー ベンダーの名前。
文字列ブロック タイプ	uint32	アプリケーション プロトコル バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにバージョンのバイト数を加えた文字列データ ブロックのバイト数。
バージョン	string	サーバーのバージョン。
前回の使用（Last Used）	uint32	システムが使用中のサーバーを検出した前回時刻を表す UNIX タイムスタンプ。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答（RNA）がサーバー データを提供した場合、0 • ユーザーがサーバー データを提供した場合、1 • サードパーティ スキャナがクライアント データを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでサーバー データを提供した場合、3
ソース	uint32	サーバー データの送信元にマッピングするID 番号。送信元タイプによって、これは無応答（RNA）、ユーザー、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
リスト ブロック タイプ	uint32	サブサーバー データを伝えるフル サーバー情報データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。

表 4-76　フル サーバー情報データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのフル サブサーバー データ ブロックを加えた値です。 このフィールドの後にはゼロか、さらにフル サブサーバー データ ブロックが続きます。
フル サブサーバー ブロック タイプ	uint32	最初のフル サブサーバー データ ブロックを開始します。このデータ ブロックには、他のフル サブサーバー データ ブロックを、リスト ブロック長フィールドで定義した上限まで続けることができます。
フル サブサーバー ブロック長	uint32	フル サブサーバー ブロック タイプ フィールドと長さ フィールドの 8 バイトに、後続のデータ バイト数を加えた各フル サブサーバー データ ブロックの合計バイト数。
フル サブサーバー データ ブロック*	uint32	このサーバーのサブサーバーを含むフル サブサーバー データ ブロック。このデータ ブロックの説明の詳細については、フル サブサーバー データ ブロック（4-89 ページ）を参照してください。

4.10.0+ の汎用スキャン結果データ ブロック

汎用スキャン結果データ ブロックにはスキャン結果が格納され、スキャン結果データ ブロック 5.2+（4-146 ページ）で使用します。汎用スキャン結果データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 108 です。

次の図は、汎用スキャン結果データ ブロックの基本構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
スキャン結果サブサーバー	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	スキャン結果サブサーバー(不定様式)文字列...																															
スキャン結果値	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	スキャン結果値...																															

次の表では、汎用スキャン結果データ ブロックのフィールドについて説明します。

表 4-77　　汎用スキャン結果データ ブロックのフィールド

フィールド	バイト数	説明
汎用スキャン結果データ ブロック タイプ	uint32	汎用スキャン結果データ ブロックを開始します。この値は常に 108 です。
汎用スキャン結果ブロック長	uint32	汎用スキャン結果ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のスキャン結果データのバイト数を加えた汎用スキャン結果データ ブロックの合計バイト数。
[ポート(Port)]	uint16	結果の脆弱性による影響を受けたサーバーが使用するポート。
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048:IP
文字列ブロック タイプ	uint32	サブサーバーを格納した文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにサブサーバーのバイト数を加えたサブサーバー文字列データ ブロックのバイト数。
スキャン結果サブサーバー	string	サブサーバー。
文字列ブロック タイプ	uint32	値を含む文字列データ ブロックを開始します。この値は常に 0 です。

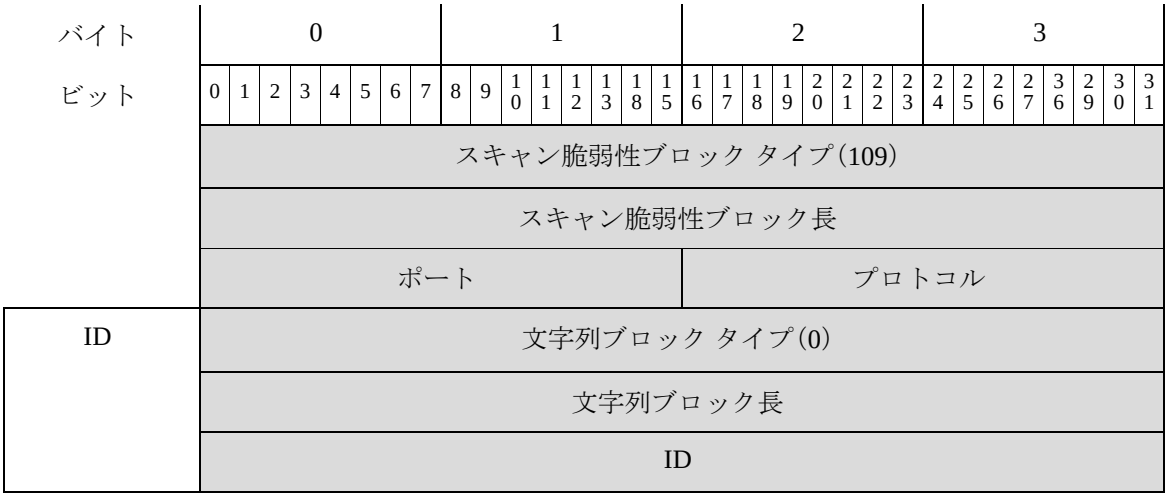
表 4-77　汎用スキャン結果データ ブロックのフィールド（続き）

フィールド	バイト数	説明
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに値のバイト数を加えた値文字列データ ブロックのバイト数。
スキャン結果値	string	スキャン結果値。
文字列ブロック タイプ	uint32	サブサーバーを格納した文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにサブサーバーのバイト数を加えたサブサーバー文字列データ ブロックのバイト数。
スキャン結果サブサーバー	string	サブサーバー（不定様式）。
文字列ブロック タイプ	uint32	値を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに値のバイト数を加えた値文字列データ ブロックのバイト数。
スキャン結果値	string	スキャン結果値（不定様式）。

4.10.0+のスキャン脆弱性データ ブロック

スキャン脆弱性データ ブロックは、脆弱性を記述し、スキャン結果データ ブロックで使用します。そのスキャン結果データ ブロックは、追加スキャン結果イベント（イベント タイプ 100 2、サブタイプ 11）で使用します。詳細については、スキャン結果データ ブロック 5.2+（4-146 ページ）およびスキャン結果を追加メッセージ（4-61 ページ）を参照してください。スキャン脆弱性データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 109 です。

次の図は、スキャン脆弱性データ ブロックの形式です。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
[名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	脆弱性名...																															
説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	説明...																															
名前クリーン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	脆弱性名クリーン...																															
説明クリーン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	記述クリーン...																															
Bugtraq ID	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	整数型データ ブロック(Bugtraq ID)...																															
CVE ID	リスト ブロック タイプ(11)																															
	リスト ブロック長																															
	CVE ID...																															

次の表では、スキャン脆弱性データ ブロックのフィールドについて説明します。

表 4-78　　スキャン脆弱性データ ブロックのフィールド

フィールド	データタイプ	説明
スキャン脆弱性ブロック タイプ	uint32	スキャン脆弱性データ ブロックを開始します。この値は常に 109 です。
スキャン脆弱性ブロック長	uint32	スキャン脆弱性データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン脆弱性データのバイト数を含む)。
[ポート(Port)]	uint16	脆弱性の影響を受けるサブサーバーで使用するポート。

表 4-78　スキャン脆弱性データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6：TCP • 17：UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048：IP
文字列ブロック タイプ	uint32	ID を含む文字列データ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、ID のバイト数を加えた ID の文字列データ ブロックのバイト数。
ID	string	脆弱性を検出したスキャン ユーティリティの指定に従って報告されたその脆弱性の ID。Qualys スキャンで検出した脆弱性の場合、たとえばこのフィールドには Qualys ID が設定されます。
文字列ブロック タイプ	uint32	脆弱性名を含むデータ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、脆弱性名のバイト数を加えた、脆弱性名の文字列データ ブロックの合計バイト数。
[名前（Name）]	string	脆弱性の名前。
文字列ブロック タイプ	uint32	脆弱性記述文字列データ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、脆弱性の記述のバイト数を加えた、脆弱性の記述の文字列データ ブロックの合計バイト数。
説明	string	脆弱性の記述。
文字列ブロック タイプ	uint32	脆弱性名を含むデータ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、脆弱性名のバイト数を加えた、脆弱性名の文字列データ ブロックの合計バイト数。
名前クリーン	string	脆弱性の名前（不定様式）。
文字列ブロック タイプ	uint32	脆弱性記述文字列データ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、脆弱性の記述のバイト数を加えた、脆弱性の記述の文字列データ ブロックの合計バイト数。
記述クリーン	string	脆弱性の記述（不定様式）。

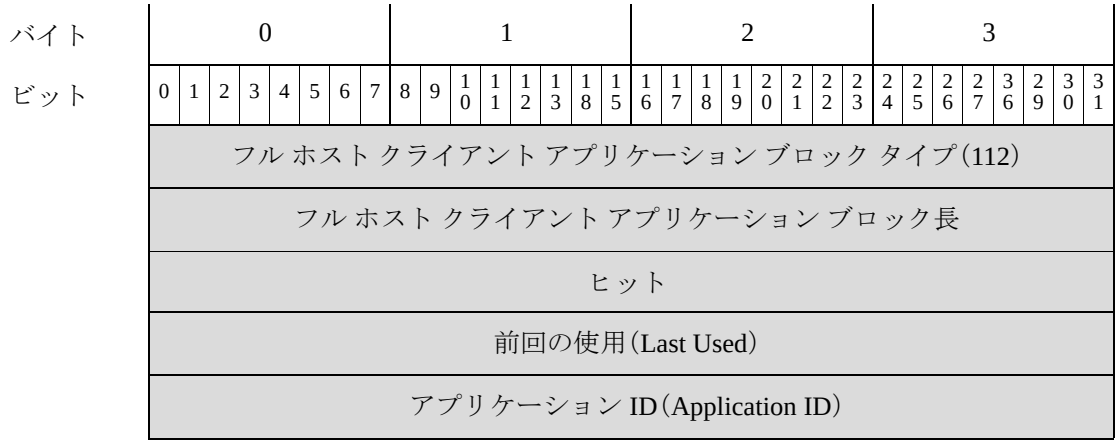
表 4-78　スキャン脆弱性データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
リスト ブロック タイプ	uint32	Bugtraq ID 番号のリストのリスト データ ブロックを開始します。
リスト ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、Bugtraq ID を格納した整数型データのバイト数を加えた、Bugtraq ID 番号のリスト データ ブロックの合計バイト数。
Bugtraq ID	string	Bugtraq ID 番号のリストを形成するゼロ以上の Bugtraq（INT32）データ ブロック。これらのデータ ブロックの詳細については、整数型（INT32）データ ブロック（4-81 ページ）を参照してください。
リスト ブロック タイプ	uint32	Common Vulnerability Exposure（CVE）のリストのリスト データ ブロックを開始します。
リスト ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、CVE ID 番号のバイト数を加えた CVE ID 番号のリスト データ ブロックのバイト数。
CVE ID	string	CVE ID 番号のリストを形成するゼロ以上の文字列情報データ ブロック。これらのデータ ブロックの詳細については、文字列情報データ ブロック（4-83 ページ）を参照してください。

フル クライアント アプリケーション データ ブロック 5.0+

バージョン 5.0 + のフル ホスト クライアント アプリケーション データ ブロックは、クライアント アプリケーションと、合わせて、関連 Web アプリケーションと脆弱性の添付リストを記述します。フル ホスト クライアント アプリケーション データ ブロックは、フル ホスト プロファイル データ ブロック（111）内で使用します。このブロック タイプは シリーズ 1 ブロック グループのブロック タイプ 112 です。

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



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
バージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	バージョン...																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
Web Application	Web アプリケーション ブロック タイプ(123)*																															
	Web アプリケーション ブロック長																															
	Web アプリケーション データ...																															
	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
脆弱性	脆弱性ブロック タイプ(85)*																															
	脆弱性ブロック長																															
	脆弱性データ...																															

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

表 4-79　フル ホスト クライアント アプリケーション データ ブロック 5.0+ のフィールド

フィールド	データタイプ	説明
フル ホスト クライアント アプリケーション ブロック タイプ	uint32	フル ホスト クライアント アプリケーション データ ブロックを開始します。この値は常に 112 です。
フル ホスト クライアント アプリケーション ブロック長	uint32	クライアント アプリケーション ブロック タイプと長さの 8 バイトに、後続のクライアント アプリケーション データのバイト数を加えたフル ホスト クライアント アプリケーション データ ブロックの合計バイト数。
ヒット	uint32	システムが使用中のクライアント アプリケーションを検出した回数。
前回の使用(Last Used)	uint32	システムが使用中のクライアントを検出した前回時刻を表す UNIX タイムスタンプ。
アプリケーション ID(Application ID)	uint32	検出したクライアント アプリケーションのアプリケーション ID(該当する場合)。

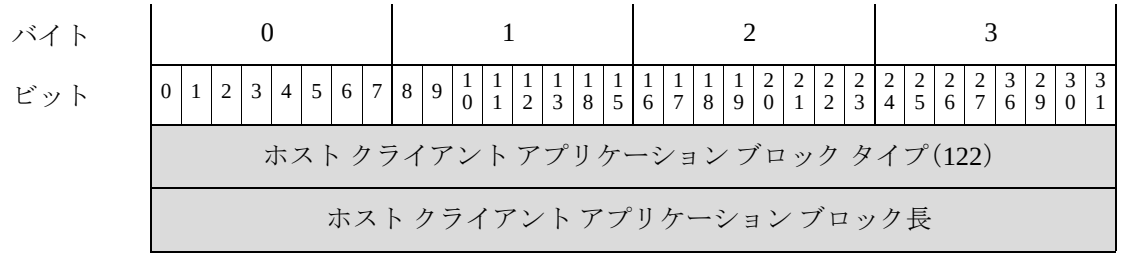
表 4-79　フル ホスト クライアント アプリケーション データ ブロック 5.0+ のフィールド（続き）

フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、クライアント アプリケーション バージョンのバイト数を加えたクライアント アプリケーション名の文字列データ ブロックのバイト数。
バージョン	string	クライアント アプリケーション バージョン。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化された Web アプリケーション データ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
Web アプリケーション データ ブロック	変数（variable）	汎用リスト ブロック長の最大バイト数を上限としてカプセル化した Web アプリケーション データ ブロック。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化された脆弱性データ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべての脆弱性データ ブロックのバイト数を加えた値です。
脆弱性データ ブロック	変数（variable）	汎用リスト ブロック長の最大バイト数を上限としてカプセル化した脆弱性データ ブロック。

5.0+ のホスト クライアント アプリケーション データ ブロック

5.0+ のホスト クライアント アプリケーション データ ブロックは、クライアント アプリケーションを記述し、新規クライアント アプリケーション イベント（イベント タイプ 1000、サブタイプ 7）、クライアント アプリケーション タイムアウト イベント（イベント タイプ 1001、サブタイプ 20）、クライアント アプリケーション更新イベント（イベント タイプ 1001、サブタイプ 32）で使用します。4.10.2+ のホスト クライアント アプリケーション データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 122 です。

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



	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
		ヒット																															
		前回の使用（Last Used）																															
		ID																															
		アプリケーション プロトコル ID																															
バージョン		文字列ブロック タイプ（0）																															
		文字列ブロック長																															
		バージョン...																															
		汎用リスト ブロック タイプ（31）																															
		汎用リスト ブロック長																															
Web Application		Web アプリケーション ブロック タイプ（123）*																															
		Web アプリケーション ブロック長																															
		Web アプリケーション データ...																															

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

表 4-80　　ホスト クライアント アプリケーション データ ブロックのフィールド

フィールド	データタイプ	説明
クライアント アプリケーション ブロック タイプ	uint32	ホスト クライアント アプリケーション データ ブロックを開始します。この値は常に 122 です。
クライアント アプリケーション ブロック長	uint32	クライアント アプリケーション ブロック タイプと長さの 8 バイトに、後続のクライアント アプリケーション データのバイト数を加えたクライアント アプリケーション データ ブロックの合計バイト数。
ヒット	uint32	システムが使用中のクライアント アプリケーションを検出した回数。
前回の使用（Last Used）	uint32	システムが使用中のクライアントを検出した前回時刻を表す UNIX タイムスタンプ。
ID	uint32	検出したクライアント アプリケーションの ID 番号（該当する場合）。
アプリケーション プロトコル ID	uint32	アプリケーション プロトコルの内部 ID 番号（該当する場合）。

表 4-80　ホスト クライアント アプリケーション データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	クライアント アプリケーション バージョンの文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、クライアント アプリケーション バージョンのバイト数を加えたクライアント アプリケーション バージョンの文字列データ ブロックのバイト数。
バージョン	string	クライアント アプリケーション バージョン。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化された Web アプリケーション データ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
Web アプリケーション データ ブロック	変数（variable）	リスト ブロック長の最大バイト数を上限としてカプセル化した Web アプリケーション データ ブロック。カプセル化されたデータ ブロック（ブロック タイプ 123）については、5.0+の Web アプリケーション データ ブロック（4-124 ページ）を参照してください。

ユーザー脆弱性データ ブロック 5.0+

ユーザー脆弱性データ ブロックは、脆弱性について記述し、ユーザー脆弱性変更ブロック内で使用します。さらに、ユーザー脆弱性変更ブロックはユーザー設定有効脆弱性イベントとユーザー設定無効脆弱性イベントで使用します。5.0+ のユーザー脆弱性データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 124 です。これはブロック タイプ 79 に置き換わります。ユーザー脆弱性変更データ ブロックの詳細については、ユーザー脆弱性変更データ ブロック 4.7+（4-113 ページ）を参照してください。

次の図は、ユーザー脆弱性変更データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	脆弱性 ID																															
サードパーティ脆弱性 UUID	サードパーティ脆弱性 UUID UUID（続き） UUID（続き） UUID（続き）																															
	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	脆弱性文字列...																															
	クライアント アプリケーション ID																															
	アプリケーション プロトコル ID																															
	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	バージョン文字列...																															

次の表では、ユーザー脆弱性データ ブロックのフィールドについて説明します。

表 4-81　　ユーザー脆弱性データ ブロックのフィールド

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

表 4-81　ユーザー脆弱性データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
[ポート(Port)]	uint16	脆弱性の影響を受けるサーバーで使用するポート。クライアント アプリケーション脆弱性の場合、値は 0 です。
プロトコル	uint16	このブロックには、フィンガープリント Universally Unique Identifier(UUID)の他、フィンガープリント タイプ、フィンガープリント送信元タイプ、フィンガープリント送信元 ID を格納します。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048:IP クライアント アプリケーション脆弱性の場合、値は 0 です。
脆弱性 ID	uint32	シスコ 脆弱性 ID。
サードパーティ脆弱性 UUID	uint8 [16]	指定する場合は、サードパーティ脆弱性の固有 ID 番号。そうでない場合、この値は0 です。
文字列ブロック タイプ	uint32	脆弱性名を含むデータ ブロックを開始します。値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、脆弱性名のバイト数を加えた、脆弱性名の文字列データ ブロックの合計バイト数。
脆弱性名	string	脆弱性名
クライアント アプリケーション ID	uint32	クライアント アプリケーションのアプリケーション ID。シングルモードの場合、この値は 0 になります。
アプリケーション プロトコル ID	uint32	クライアント アプリケーションで使用しているアプリケーション プロトコルのアプリケーション ID。シングルモードの場合、この値は 0 になります。
文字列ブロック タイプ	uint32	バージョン文字列を含む文字列データ ブロックを開始します。値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、クライアント アプリケーション バージョン文字列のバイト数を加えた文字列データ ブロックのバイト数。
バージョン	string	クライアント アプリケーション バージョン。シングルモードの場合、この値は 0 になります。

オペレーティング システム フィンガープリント データ ブロック 5.1+

オペレーティング システム フィンガープリント データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 130 です。このブロックには、フィンガープリント Universally Unique Identifier（UUID）の他、フィンガープリント タイプ、フィンガープリント送信元タイプ、フィンガープリント送信元 ID を格納します。

次の図は、5.1+ のオペレーティング システム フィンガープリント データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	オペレーティング システム フィンガープリント ブロック タイプ（130）																															
	オペレーティング システム フィンガープリント ブロック長																															
OS フィンガープリント UUID	フィンガープリント UUID フィンガープリント UUID（続き） フィンガープリント UUID（続き） フィンガープリント UUID（続き）																															
	フィンガープリント タイプ																															
	フィンガープリント ソース タイプ																															
	フィンガープリント ソース ID																															
	最後の確認日時																															
モバイル Device 情報	TTL 差異								汎用リスト ブロック タイプ（31）																							
	汎用リスト ブロック タイプ（続き）								汎用リスト ブロック長																							
	汎用リスト ブロック長（続き）								モバイルDevice情報データ ブロック*																							

次の表では、オペレーティング システムフィンガープリント データ ブロックのフィールドについて説明します。

表 4-82　オペレーティング システム フィンガープリント データ ブロックのフィールド

フィールド	データタイプ	説明
オペレーティング システム フィンガープリント データ ブロック タイプ	uint32	オペレーティング システム データ ブロックを開始します。この値は常に 130 です。
オペレーティング システム データ ブロック長	uint32	オペレーティング システム フィンガープリント データ ブロック タイプと長さの 8 バイトに、後続のオペレーティング システム フィンガープリント データのバイト数を加えたオペレーティング システム フィンガープリント データ ブロックのバイト数。
フィンガープリント UUID	uint8[16]	オペレーティング システムの固有識別子として機能するフィンガープリントID 番号（オクテット）。フィンガープリント UUID は、脆弱性データベース（VDB）内のオペレーティング システム名、ベンダー、バージョンにマップされます。
フィンガープリント タイプ	uint32	フィンガープリントのタイプを示します。
フィンガープリント ソース タイプ	uint32	オペレーティング システム フィンガープリントを提供するソースのタイプ（ユーザーやスキャナ）を示します。
フィンガープリント ソース ID	uint32	ID 番号。オペレーティング システム フィンガープリントを提供したユーザーのログイン名にマップします。
最後の確認日時	uint32	トラフィックで前回フィンガープリントを確認した時刻を示します。
TTL 差異	uint8	フィンガープリントの TTL 値とホストにフィンガープリントを実行するときに使用するパケット上の TTL 値との差を示します。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
モバイルDevice情報データ ブロック	変数（variable）	リスト ブロック長の最大バイト数を上限としてカプセル化したモバイル Device 情報データ ブロック。このデータ ブロックの説明の詳細については、5.1+ のモバイルDevice 情報データ ブロック（4-173 ページ） を参照してください。

5.1+ のモバイルDevice 情報データ ブロック

次の図は、モバイル Device 情報データ ブロックの形式です。このデータ ブロックには、ホストを前回検出した時刻、モバイル デバイス情報、そのモバイル デバイスが改造されていないかどうかに関する情報を格納します。モバイル Device 情報データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 131 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	モバイル Device 情報ブロック タイプ(131)																															
	モバイル Device 情報ブロック長																															
モバイル Device データ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	モバイル Device 文字列データ...																															
	モバイル Device 最後の確認日時																															
	Mobile																															
	改造																															

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

表 4-83　　モバイルDevice情報データ ブロック 5.1+ のフィールド

フィールド	データタイプ	説明
モバイル Device 情報ブロック タイプ(131)	uint32	オペレーティング システム データ ブロックを開始します。この値は常に 131 です。
モバイル Device 情報ブロック長	uint32	モバイル Device 情報データ ブロック タイプと長さの 8 バイトに、後続のモバイル Device 情報データのバイト数を加えたモバイル Device 情報データ ブロックのバイト数。
文字列ブロック タイプ	uint32	モバイル デバイス文字列を含む文字列データ ブロックを開始します。この値は文字列データを表す 0 に設定されます。
文字列ブロック長	uint32	文字列ブロック タイプ フィールドと長さフィールドの 8 バイトに、モバイル デバイス文字列データのバイト数を加えたモバイル デバイス文字列データ ブロックのバイト数を示します。
モバイル Device 文字列データ	変数	検出したホストのモバイル デバイスのハードウェア情報を格納します。
モバイル Device 最後の確認日時	uint32	モバイル デバイスを最後の確認日時した時刻のタイムスタンプを格納します。
Mobile	uint32	検出したホストがモバイル デバイスであるかどうかを示す true/false フラグ。
改造	uint32	ホストが改造したモバイル デバイスであるかどうかを示す true/false フラグ。

ホスト プロファイル データブロック 5.2+

次の図は、ホスト プロファイル データ ブロックの形式を示しています。さらに、このデータ ブロックには、ホスト重要度値が含まれていませんが、VLAN プレゼンス インジケータは含まれています。さらに、このデータ ブロックは、ホストの NetBIOS 名を伝えることができます。ホスト プロファイル データ ブロックのブロック タイプは、ブロックのシリーズ 1 グループのブロック タイプ 139 です。データ ブロックは、IPv6 アドレスをサポートするようになり、クライアント アプリケーション データ ブロックを追加しました。

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ホスト プロファイル ブロック タイプ(139)																															
	ホスト プロファイル ブロック長																															
	[IPアドレス(IP Address)] IP アドレス(続き) IP アドレス(続き) IP アドレス(続き)																															
サーバー フィンガープリント	ホップ								プライマリ/セカンダリ								汎用リスト ブロック タイプ(31)															
	汎用リスト ブロック タイプ(続き)																汎用リスト ブロック長															
	汎用リスト ブロック長(続き)																サーバー フィンガープリント データ ブロック*															
クライアント フィンガープリント	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	クライアント フィンガープリント データ ブロック*																															
SMB フィンガープリント	汎用リスト ブロック タイプ(31)																															
	汎用リスト ブロック長																															
	SMB フィンガープリント データ ブロック*																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
DHCP フィンガープリント	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
	DHCP フィンガープリント データ ブロック*																															
モバイル Device フィンガープリント	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
	モバイルDevice フィンガープリント データ ブロック*																															
IPv6 サーバー フィンガープリント	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
	Ipv6 サーバー フィンガープリント データ ブロック*																															
IPv6 クライアント フィンガープリント	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
	IPv6 クライアント フィンガープリント データ ブロック*																															
IPv6 DHCP フィンガープリント	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
	IPv6 DHCP フィンガープリント データ ブロック*																															
ユーザー エージェント フィンガープリント	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
	ユーザー エージェント フィンガープリント データ ブロック*																															
TCP サーバー ブロック*	リスト ブロック タイプ（11）																															TCP のリスト サーバー
	リスト ブロック長																															
	TCP サーバー データ ブロック																															
UDP サーバー ブロック*	リスト ブロック タイプ（11）																															UDP のリスト サーバー
	リスト ブロック長																															
	UDP サーバー データ ブロック																															

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31	
ネットワーク プロトコル ブロック*	リスト ブロック タイプ(11)																																ネットワーク のリスト プロトコル
	リスト ブロック長																																
	ネットワーク プロトコル データ ブロック																																
トランスポート(Transport) プロトコル ブロック*	リスト ブロック タイプ(11)																																トランスポート リスト プロトコル
	リスト ブロック長																																
	トランスポート プロトコル データ ブロック																																
MAC アドレス ブロック*	リスト ブロック タイプ(11)																																MAC のリスト アドレス
	リスト ブロック長																																
	ホスト MAC アドレス データ ブロック																																
	最終検出時のホスト																																
	ホスト タイプ																																
	Mobile								改造								VLAN の有無								VLAN ID(Admin. VLAN ID)								
クライアント アプリケーション データ	VLAN ID(続き)								VLAN タイプ								VLAN プライオリティ								汎用リスト ブロック タイプ(31)								クライアント のリスト アプリケーション
	汎用リスト ブロック タイプ(31)(続き)																								汎用リスト ブロック長								
	汎用リスト ブロック長(続き)																								クライアント アプリケーション データ ブロック								
NetBIOS [名前(Name)]	文字列ブロック タイプ(0)																																
	文字列ブロック長																																
	NetBIOS 文字列データ...																																

次の表では、5.2+ で返るホスト プロファイル データ ブロックのフィールドについて説明します。

表 4-84　ホスト プロファイル データブロック 5.2+ のフィールド

フィールド	データタイプ	説明
ホスト プロファイル ブロック タイプ	uint32	5.2+ のホスト プロファイル データ ブロックを開始します。この値は常に 139 です。
ホスト プロファイル ブロック長	uint32	ホスト プロファイル データ ブロックのバイト数(ホスト プロファイル ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くホスト プロファイル データに含まれるバイト数を含む)。
[IPアドレス(IP Address)]	uint8(16)	ホストの IP アドレスこれには、IPv4 または IPv6 のいずれも使用できます。
ホップ	uint8	ホストからのデバイスまでのホップ数。
プライマリ/セカンダリ	uint8	ホストがそれを検出したデバイスのプライマリまたはセカンダリのどちらのネットワークにあるかを示します。 • 0:ホストはプライマリ ネットワークにあります。 • 1:ホストはセカンダリ ネットワークにあります。
汎用リスト ブロック タイプ	uint32	サーバー フィンガープリントを使用して特定されたフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(サーバー フィンガープリント)データ ブロック*	変数(variable)	サーバー フィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-172 ページ)を参照してください。
汎用リスト ブロック タイプ	uint32	クライアント フィンガープリントを使用して特定したフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(クライアント フィンガープリント)データ ブロック*	変数(variable)	クライアント フィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-172 ページ) を参照してください。

表 4-84　ホスト プロファイル データブロック 5.2+ のフィールド（続き）

フィールド	データタイプ	説明
汎用リスト ブロック タイプ	uint32	SMB フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。
オペレーティング システム フィンガープリント（SMB フィンガープリント）データ ブロック*	変数（variable）	SMB フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-172 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	DHCP フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。
オペレーティング システム フィンガープリント（DHCP フィンガープリント）データ ブロック*	変数（variable）	DHCP フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-172 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	モバイル デバイス フィンガープリントで識別するフィンガープリント データを搬送するオペレーティング システム フィンガープリント データ ブロックで構成される汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む）。
オペレーティング システム フィンガープリント モバイル データ ブロック*	変数（variable）	モバイル デバイス フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-172 ページ）を参照してください。
汎用リスト ブロック タイプ	uint32	IPv6 サーバー フィンガープリントを使用して特定されたフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。

表 4-84　ホスト プロファイル データブロック 5.2+ のフィールド（続き）

フィールド	データタイプ	説明
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(IPv6 サーバー)データ ブロック*	変数(variable)	IPv6 サーバー フィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-172 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	IPv6 クライアント フィンガープリントを使用して特定されたフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(IPv6 クライアント)データ ブロック*	変数(variable)	IPv6 クライアント フィンガープリントで識別したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-172 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	IPv6 DHCP フィンガープリントで識別するフィンガープリント データを搬送するオペレーティング システム フィンガープリント データ ブロックで構成される汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント(IPv6 DHCP フィンガープリント)データ ブロック*	変数(variable)	IPv6 DHCP フィンガープリントで識別したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+(4-172 ページ) を参照してください。
汎用リスト ブロック タイプ	uint32	ユーザー エージェント フィンガープリントで識別するフィンガープリント データを搬送するオペレーティング システム フィンガープリント データ ブロックで構成される汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。

表 4-84　ホスト プロファイル データブロック 5.2+ のフィールド（続き）

フィールド	データタイプ	説明
オペレーティング システム フィンガープリント(ユーザー エージェント フィンガープリント)データ ブロック*	変数（variable）	ユーザー エージェント フィンガープリントで識別したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、オペレーティング システム フィンガープリント データ ブロック 5.1+（4-172 ページ）を参照してください。
リストブロック タイプ	uint32	TCP サーバー データを伝えるサーバー データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバー データ ブロックを加えた値です。 このフィールドには、ゼロ以上のサーバー データ ブロックが続きます。
TCP サーバー データ ブロック	変数（variable）	TCP サーバーを記述するホスト サーバー データ ブロック。このデータ ブロックの説明の詳細については、ホスト サーバー データ ブロック 4.10.0+(4-149 ページ) を参照してください。
リストブロック タイプ	uint32	UDP サーバー データを伝えるサーバー データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバー データ ブロックを加えた値です。 このフィールドには、ゼロ以上のサーバー データ ブロックが続きます。
UDP サーバー データ ブロック	uint32	UDP サーバーを記述するホスト サーバー データ ブロック。このデータ ブロックの説明の詳細については、ホスト サーバー データ ブロック 4.10.0+(4-149 ページ) を参照してください。
リストブロック タイプ	uint32	ネットワーク プロトコル データを伝えるプロトコル データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのプロトコル データ ブロックを加えた値です。 このフィールドには、ゼロ以上のプロトコル データ ブロックが続きます。
ネットワーク プロトコルデータ ブロック	uint32	ネットワーク プロトコルを記述するプロトコル データ ブロック。このデータ ブロックの説明の詳細については、プロトコル データ ブロック (4-80 ページ) を参照してください。
リストブロック タイプ	uint32	トランスポート プロトコル データを伝えるプロトコル データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。

表 4-84　ホスト プロファイル データブロック 5.2+ のフィールド（続き）

フィールド	データタイプ	説明
リスト ブロック長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのプロトコル データ ブロックを加えた値です。 このフィールドには、ゼロ以上のトランスポート プロトコル データ ブロックが続きます。
トランスポート プロトコル データ ブロック	uint32	トランスポート プロトコルを記述するプロトコル データ ブロック。このデータ ブロックの説明の詳細については、プロトコル データ ブロック（4-80 ページ）を参照してください。
リストブロック タイプ	uint32	MAC アドレス データ ブロックを構成するリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リストのバイト数（リスト ヘッダーと、カプセル化されたすべての MAC アドレス データ ブロックを含む）。
ホスト MAC アドレス データ ブロック	uint32	ホスト MAC アドレスを記述するホスト MAC アドレス データ ブロック。このデータ ブロックの説明の詳細については、ホスト MAC アドレス 4.9+（4-122 ページ）を参照してください。
最終検出時のホスト	uint32	システムがホスト アクティビティを検出した前回時刻を表す UNIX タイムスタンプ。
ホスト タイプ	uint32	ホスト タイプを示します。表示される可能性がある値は次のとおりです。 • 0：ホスト • 1 — ルータ • 2：ブリッジ • 3：NAT デバイス • 4：LB（ロード バランサ）
Mobile	uint8	検出したホストがモバイル デバイスであるかどうかを示す true/false フラグ。
改造	uint8	ホストが（ジェイルブレイクされていない）モバイル デバイスであるかどうかを示す true/false フラグ。
VLAN の有無	uint8	VLAN が存在するかどうかを示します。 • 0：はい • 1：いいえ
VLAN ID（Admin. VLAN ID）	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグ内でカプセル化されるパケットのタイプ。
VLAN プライオリティ	uint8	VLAN タグに含まれる優先順位値。
文字列ブロック タイプ	uint32	ホスト クライアント アプリケーション データを含む文字列データ ブロックを開始します。この値は常に 112 です。

表 4-84　ホスト プロファイル データブロック 5.2+ のフィールド（続き）

フィールド	データタイプ	説明
文字列ブロック長	uint32	文字列ブロック タイプ フィールドと長さフィールドの 8 バイトに、ホスト クライアント アプリケーション データのバイト数を加えた文字列データ ブロックのバイト数。
ホスト クライアント アプリケーション データ ブロック	変数（variable）	クライアント アプリケーション データ ブロックのリスト。このデータ ブロックの説明の詳細については、フル クライアント アプリケーション データ ブロック 5.0+（4-165 ページ）を参照してください。
文字列ブロック タイプ	uint32	ホストの NetBIOS 名の文字列データ ブロックを表示します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプ フィールドおよび文字列ブロック長フィールドの 8 バイトを含む文字列データ ブロック内のバイト数と NetBIOS 名文字列のバイト数。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。

ユーザー製品データ ブロック 5.1+

ユーザー製品データ ブロックは、サードパーティ アプリケーション文字列マッピングを含む、サードパーティ アプリケーションからインポートされたホスト入力データを伝送します。このデータ ブロックは スキャン結果データ ブロック 5.2+（4-146 ページ）と ユーザー サーバー メッセージとオペレーティング システム メッセージ（4-60 ページ）で使用します。ユーザー製品データ ブロックのブロック タイプのブロック タイプは、4.7 ～ 4.10.1 のシリーズ 1 ブロック グループのブロック タイプ 65 と、4.10.2 ～ 5.0.x のブロック タイプ 118、そして 5.1+ のシリーズ 1 ブロック グループのブロック タイプ 134 です。ブロック タイプ 65 と 118 の構造は同じです。

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

次の図は、ユーザー製品データ ブロックの形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
[IPアドレス（IP Address）]範囲	汎用リスト ブロック タイプ（31）																															
	汎用リスト ブロック長																															
	IP 範囲仕様データ ブロック*																															
	ポート																プロトコル															
	ドロップ ユーザー製品																															
カスタム（Custom）ベンダー文字列	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	カスタム ベンダー文字列...																															
カスタム（Custom）製品文字列	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	カスタム製品文字列...																															
カスタム（Custom）バージョン文字列	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	カスタム バージョン文字列...																															
	ソフトウェア ID																															
	サーバー ID																															
	ベンダー ID																															
	製品 ID																															
メジャー バージョン文字列	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	メジャー バージョン文字列...																															
マイナー バージョン文字列	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	マイナー用バージョン文字列...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
リビジョン文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	リビジョン文字列...																															
メジャー用文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	メジャー用バージョン文字列...																															
マイナー用文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	マイナー用バージョン文字列...																															
リビジョン用文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	リビジョン用文字列...																															
ビルド文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ビルド文字列...																															
パッチ文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	パッチ文字列...																															
内線番号文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	拡張文字列...																															
OS UUID	オペレーティング システム UUID																															
	オペレーティング システム UUID(続き)																															
	オペレーティング システム UUID(続き)																															
	オペレーティング システム UUID(続き)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Device 文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	Device 文字列...																															
修正のリスト	Mobile								改造								汎用リスト ブロック タイプ(31)															
	汎用リスト ブロック タイプ(31)（続き）																汎用リスト ブロック長															
	汎用リスト ブロック長(続き)																修正リスト データ ブロック*															
	修正リスト データ ブロック*(続き)																															

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

表 4-85　　ユーザー製品データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザー製品データブロック タイプ	uint32	ユーザー製品データ ブロックを開始します。5.1+ の場合、この値は 134 です。
ユーザー製品ブロック長	uint32	ユーザー製品データ ブロックのバイトの合計数(ユーザー製品ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザー製品データのバイト数を含む)。
ソース	uint32	データをインポートした送信元にマッピングするID 番号。送信元タイプによって、これは無応答(RNA)、ユーザー、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: • 無応答(RNA) がデータを提供した場合、0 • ユーザーがデータを提供した場合、1 • サードパーティ スキャナがデータを提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでデータを提供した場合、3
汎用リスト ブロック タイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リスト データ ブロックのバイト数。

表 4-85　ユーザー製品データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
IP 範囲仕様データ ブロック*	変数（variable）	ユーザー入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データ ブロック。このデータ ブロックの説明の詳細については、5.2+の IP アドレス範囲データ ブロック（4-101 ページ）を参照してください。
[ポート（Port）]	uint16	ユーザーが指定するポート。
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 • 6：TCP • 17：UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 • 2048：IP
ドロップ ユーザー製品	uint32	ユーザー OS 定義がホストから削除されたかどうかを示します： • 0：いいえ • 1：はい
文字列ブロック タイプ	uint32	ユーザー入力に指定されたカスタム ベンダー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタム ベンダー文字列データ ブロックのバイト数（ブロック タイプと長さのフィールド用の 8 バイト、およびベンダー名のバイト数を含む）。
カスタム ベンダー名	string	ユーザー入力で指定されたカスタム ベンダー名。
文字列ブロック タイプ	uint32	ユーザー入力に指定されたカスタム製品名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタム製品文字列データ ブロックのバイト数（ブロック タイプと長さのフィールド用の 8 バイト、および製品名のバイト数を含む）。
カスタム製品名	string	ユーザー入力に指定されたカスタム製品名。
文字列ブロック タイプ	uint32	ユーザー入力に指定されたカスタム バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタム バージョン文字列データ ブロックのバイト数（ブロック タイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む）。
カスタム バージョン	string	ユーザー入力に指定されたカスタム バージョン。
ソフトウェア ID	uint32	データベースのサーバーまたはオペレーティング システムの特定のリビジョンの識別子。

表 4-85　ユーザー製品データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
サーバー ID	uint32	ユーザー入力に指定したホスト サーバーのアプリケーション プロトコルの Cisco Secure Firewall システム アプリケーション識別子。
ベンダー ID	uint32	サードパーティ オペレーティング システムを Cisco Secure Firewall システム OS 定義にマップしたときに指定したサードパーティ オペレーティング システムのベンダーの識別子。
製品 ID	uint32	サードパーティ オペレーティング システム文字列を Cisco Secure Firewall システム OS 定義にマップしたときに指定したサードパーティ オペレーティング システム文字列の製品識別文字列。
文字列ブロック タイプ	uint32	ユーザー入力のサードパーティ オペレーティング システム文字列をマップする Cisco Secure Firewall システム オペレーティング システム定義のメジャー バージョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	メジャー文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
メジャー バージョン	string	サードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システム定義のメジャー バージョン。
文字列ブロック タイプ	uint32	サードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システム定義のマイナー バージョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	マイナー文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
マイナー バージョン	string	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システム定義のマイナー バージョン番号。
文字列ブロック タイプ	uint32	ユーザー入力のサードパーティ オペレーティング システム文字列をマップする Cisco Secure Firewall システム オペレーティングシステム定義のリビジョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	メジャー用文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
リビジョン	string	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システム定義のリビジョン番号。
文字列ブロック タイプ	uint32	サードパーティ オペレーティング システム文字列をマップする Cisco Secure Firewall システム オペレーティング システム定義の最新のメジャー バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。

表 4-85　ユーザー製品データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにバージョンのバイト数を加えた移行先メジャー文字列データ ブロックのバイト数。
移行先メジャー	string	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システム定義のメジャー バージョン番号の範囲における最新のバージョン番号。
文字列ブロックタイプ	uint32	サードパーティ オペレーティング システム文字列をマップする Cisco Secure Firewall システム オペレーティング システム定義の最新のマイナー バージョンを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにバージョンのバイト数を加えたマイナー用文字列データ ブロックのバイト数。
マイナー用	string	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システム定義のマイナー バージョン番号の範囲における最新のバージョン番号。
文字列ブロックタイプ	uint32	サードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システム定義の最新のリビジョン番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにリビジョン番号のバイト数を加えたリビジョン用文字列データ ブロックのバイト数。
リビジョン用	string	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システム定義のリビジョン番号の範囲における最新のリビジョン番号。
文字列ブロックタイプ	uint32	サードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システムのビルド番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ビルド文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびビルド番号のバイト数を含む)。
ビルド	string	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システムのビルド番号。
文字列ブロックタイプ	uint32	サードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システムのパッチ番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	パッチ文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびパッチ番号のバイト数を含む)。
パッチ	string	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システムのパッチ番号。

表 4-85　ユーザー製品データ ブロックのフィールド （続き）

フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	サードパーティ オペレーティング システム文字列をマップする Cisco Secure Firewall システム OS の拡張番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	拡張文字列データ ブロックのバイト数（ブロック タイプと長さのフィールド用の 8 バイト、および拡張番号のバイト数を含む）。
内線番号	string	ユーザー入力のサードパーティ OS 文字列をマップする Cisco Secure Firewall システム オペレーティング システムの拡張番号。
UUID	uint8 [x16]	オペレーティング システム用の固有 ID 番号が含まれます。
文字列ブロック タイプ	uint32	ユーザー入力に指定されたデバイス ハードウェア情報を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ビルド文字列データ ブロックのバイト数（ブロック タイプと長さのフィールド用の 8 バイト、およびビルド番号のバイト数を含む）。
Device 文字列	string	モバイル デバイス ハードウェア情報。
Mobile	uint8	オペレーティング システムがモバイル デバイスで動作しているかどうかを示す true/false フラグ。
Jailbroken	uint8	モバイル デバイスのオペレーティング システムがジェイルブレイクされているかどうかを示す true/false フラグ。
汎用リスト ブロック タイプ	uint32	どの修正が特定の IP アドレス範囲内のホストに適用されているかに関するユーザー入力データを伝える修正リスト データ ブロックで構成される、汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数（リスト ヘッダーと、カプセル化されたすべての修正リスト データ ブロックを含む）。
修正リスト データ ブロック*	変数（variable）	ホストに適用された修正に関する情報を含む修正リスト データ ブロック。このデータ ブロックの説明の詳細については、フィックス リスト データ ブロック（4-108 ページ）を参照してください。

ユーザー データ ブロック

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

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

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

表 4-86　ユーザー データ ブロック タイプ

タイプ（Type）	目次	データ ブロック カテゴリ	説明
73	ユーザー ログイン情報	レガシー	システムが検出したユーザーのログイン情報の変更を格納します。詳細については、ユーザー ログイン情報データ ブロック 5.0 ～ 5.0.2（B-141 ページ）を参照してください。バージョン 5.0 で導入したサクセサ ブロック タイプは、ブロック タイプ 73 と同じ構造ですが、そのフィールド内のデータは異なります。
74	ユーザー アカウント更新メッセージ	現在（Current）	ユーザー アカウント情報の変更を格納します。詳細については、ユーザー アカウント更新メッセージ データ ブロック（4-192 ページ）を参照してください。
75	4.7 ～ 4.10.x のユーザー情報	レガシー	システムが検出したユーザーの情報の変更を格納します。詳細については、ユーザー情報データ ブロック 5.x（B-156 ページ）を参照してください。バージョン 6.0 で導入したサクセサ ブロックのブロック タイプは 158 です。
120	5.x のユーザー情報	現在（Current）	システムが検出したユーザーの情報の変更を格納します。詳細については、ユーザー情報データ ブロック 5.x（B-156 ページ）を参照してください。ブロック タイプ 75 に置き換わります。これはブロック タイプ 158 に更新しました。
121	ユーザー ログイン情報	レガシー	システムが検出したユーザーのログイン情報の変更を格納します。詳細については、ユーザー ログイン情報データ ブロック 5.0 ～ 5.0.2（B-141 ページ）を参照してください。プロトコル フィールドの内容であるブロック 73 とは異なります。ここには、イベントで検出したアプリケーション プロトコル ID のバージョン 5.0 +アプリケーション ID を保存します。バージョン 5.1 で導入したサクセサ ブロックのブロック タイプは 127 です。
127	ユーザー ログイン情報	レガシー	システムが検出したユーザーのログイン情報の変更を格納します。詳細については、ユーザー ログイン情報データ ブロック 5.1 ～ 5.4.x（B-143 ページ）を参照してください。これはブロック タイプ 121 に置き換わります。6.0 で導入したサクセサ ブロックのブロック タイプは 159 です。
150	IOC 状態	現在（Current）	侵害に関する情報を格納します。詳細については、5.3+ の IOC ステート データ ブロック（4-36 ページ）を参照してください。
158	6.0+ のユーザー情報	現在（Current）	システムが検出したユーザーの情報の変更を格納します。詳細については、6.0+ の情報データ ユーザー ブロック（4-201 ページ）を参照してください。ブロック タイプ 120 に置き換わります。
159	ユーザー ログイン情報	レガシー	システムが検出したユーザーのログイン情報の変更を格納します。詳細については、ユーザー ログイン情報データ ブロック 6.0.x（B-145 ページ）を参照してください。これはブロック タイプ 127 に置き換わります。

表 4-86　ユーザー データ ブロック タイプ（続き）

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

ユーザー アカウント更新メッセージ データ ブロック

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

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

次の図は、ユーザー アカウント更新メッセージ データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ユーザー アカウント更新メッセージ ブロック タイプ（74）																															
	ユーザー アカウント更新メッセージ ブロック長																															
ユーザー（User）[名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー名...																															
ファースト [名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	名...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ミドルネーム イニシャル（Initials）	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ミドルネーム イニシャル...																															
姓 [名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	姓...																															
正式名称	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	正式名称...																															
役職（Title）	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	タイトル...																															
スタッフ ID	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	スタッフ アイデンティティ...																															
アドレス（Address）	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	住所...																															
市区町村郡（City）	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	市区町村郡...																															
県	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	県...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
国/地域	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	国/地域																															
郵便番号コード(Code)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	郵便番号...																															
建物	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	建物...																															
参照先	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	場所...																															
会議室(Room)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	会議室...																															
会社	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	会社...																															
部門(Division)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	部門...																															
部署名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	部署名...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
オフィス（Office）	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	オフィス...																															
郵便配達先	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	郵便配達先...																															
E メール	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	電子メール...																															
電話	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	電話...																															
IP Phone	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	IP 電話...																															
ユーザー 1	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー 1...																															
ユーザー 2	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー 2...																															
ユーザー 3	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー 3...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ユーザー 4	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザー 4...																															
電子メール エイリアス 1	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール エイリアス 1...																															
電子メール エイリアス 2	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール エイリアス 2...																															
電子メール エイリアス 3	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール エイリアス 3...																															

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

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

フィールド	データタイプ	説明
ユーザー アカウント更新メッセージブロック タイプ	uint32	ユーザー アカウント更新メッセージのデータ ブロックを開始します。この値は常に 74 です。
ユーザー アカウント更新メッセージ ブロック長	uint32	ユーザー アカウント更新メッセージ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザー アカウント更新メッセージ データのバイト数を加えたユーザー アカウント更新メッセージ データ ブロックの合計バイト数。
文字列ブロック タイプ	uint32	ユーザーのユーザー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザー名文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびユーザー名のバイト数を含む)。
[ユーザー名(Username)]	string	ユーザーのユーザー名。

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

フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	ユーザーの名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに名のバイト数を加えた名文字列データ ブロックのバイト数。
名	string	ユーザーの名前。
文字列ブロック タイプ	uint32	ユーザーのミドル ネーム イニシャルを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにミドル ネーム イニシャルのバイト数を加えたミドル ネーム イニシャル文字列データ ブロックのバイト数。
ミドル ネーム イニシャル	string	ユーザーのミドル ネーム イニシャル。
文字列ブロック タイプ	uint32	ユーザーの姓を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに姓のバイト数を加えた姓文字列データ ブロックのバイト数。
姓	string	ユーザーの姓。
文字列ブロック タイプ	uint32	ユーザーの姓名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに姓名のバイト数を加えた姓名文字列データ ブロックのバイト数。
正式名称	string	ユーザーの姓名。
文字列ブロック タイプ	uint32	ユーザーの役職を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに役職のバイト数を加えた役職文字列データ ブロックのバイト数。
役職（Title）	string	ユーザーの役職。
文字列ブロック タイプ	uint32	ユーザーのスタッフの識別子を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにスタッフ アイデンティティのバイト数を加えたスタッフ アイデンティティ文字列データ ブロックのバイト数。
スタッフ アイデンティティ	string	ユーザーのスタッフ アイデンティティ。
文字列ブロック タイプ	uint32	ユーザーのアドレスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにアドレスのバイト数を加えたアドレス文字列データ ブロックのバイト数。

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

フィールド	データタイプ	説明
アドレス（Address）	string	ユーザーの住所。
文字列ブロック タイプ	uint32	ユーザーの住所から得た市町村郡を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに市町村郡のバイト数を加えた市町村郡文字列データ ブロックのバイト数。
市区町村郡（City）	string	ユーザーの住所から得た市町村郡。
文字列ブロック タイプ	uint32	ユーザーの住所から得た県を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに県のバイト数を加えた県文字列データ ブロックのバイト数。
県	string	ユーザーの県。
文字列ブロック タイプ	uint32	ユーザーの住所から得た国または地域を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに国または地域のバイト数を加えた国または地域文字列データ ブロックのバイト数。
国/地域	string	ユーザーの住所から得た国または地域。
文字列ブロック タイプ	uint32	ユーザーの住所から得た郵便番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに郵便番号のバイト数を加えた郵便番号文字列データ ブロックのバイト数。
郵便番号	string	ユーザーの住所から得た郵便番号。
文字列ブロック タイプ	uint32	ユーザーの住所から得た建物を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに建物名のバイト数を加えた建物文字列データ ブロックのバイト数。
建物	string	ユーザーの住所から得た建物。
文字列ブロック タイプ	uint32	ユーザーの住所から得た場所を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに場所名のバイト数を加えた場所文字列データ ブロックのバイト数。
参照先	string	ユーザーの住所から得た場所。
文字列ブロック タイプ	uint32	ユーザーの住所から得たルームを含む文字列データ ブロックを開始します。この値は常に 0 です。

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

フィールド	データタイプ	説明
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにルームのバイト数を加えたルーム文字列データ ブロックのバイト数。
会議室（Room）	string	ユーザーの住所から得たルーム。
文字列ブロックタイプ	uint32	ユーザーの住所から得た会社を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに会社名のバイト数を加えた会社文字列データ ブロックのバイト数。
会社	string	ユーザーの住所から得た会社。
文字列ブロックタイプ	uint32	ユーザーの住所から得た部門を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに部門名のバイト数を加えた部門文字列データ ブロックのバイト数。
部門（Division）	string	ユーザーの住所から得た部門。
文字列ブロックタイプ	uint32	ユーザーの住所から得た部署を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	部署文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、および部署のバイト数を含む)。
部署名（Department）	string	ユーザーの住所から得た部署。
文字列ブロックタイプ	uint32	ユーザーの住所から得たオフィスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにオフィスのバイト数を加えたオフィス文字列データ ブロックのバイト数。
オフィス（Office）	string	ユーザーの住所から得たオフィス。
文字列ブロックタイプ	uint32	ユーザーの住所から得た郵便配達先を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに郵便配達先のバイト数を加えた郵便配達先文字列データ ブロックのバイト数。
郵便配達先	string	ユーザーの住所から得た郵便配達先。
文字列ブロックタイプ	uint32	ユーザーの電子メールアドレスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メール アドレスのバイト数を加えた電子メール アドレス文字列データ ブロックのバイト数。
E メール	string	ユーザーの電子メール アドレス。

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

フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	ユーザーの電話番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電話番号のバイト数を加えた電話番号文字列データ ブロックのバイト数。
電話	string	ユーザーの電話番号。
文字列ブロック タイプ	uint32	ユーザーのインターネット電話番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにインターネット電話番号のバイト数を加えたインターネット電話番号文字列データ ブロックのバイト数。
インターネット電話	string	ユーザーのインターネット電話番号。
文字列ブロック タイプ	uint32	ユーザーの代替ユーザー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにユーザー名のバイト数を加えたユーザー文字列データ ブロックのバイト数。
ユーザー 1	string	ユーザーの代替ユーザー名。
文字列ブロック タイプ	uint32	ユーザーの代替ユーザー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにユーザー名のバイト数を加えたユーザー文字列データ ブロックのバイト数。
ユーザー 2	string	ユーザーの代替ユーザー名。
文字列ブロック タイプ	uint32	ユーザーの代替ユーザー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにユーザー名のバイト数を加えたユーザー文字列データ ブロックのバイト数。
ユーザー 3	string	ユーザーの代替ユーザー名。
文字列ブロック タイプ	uint32	ユーザーの代替ユーザー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにユーザー名のバイト数を加えたユーザー文字列データ ブロックのバイト数。
ユーザー 4	string	ユーザーの代替ユーザー名。
文字列ブロック タイプ	uint32	ユーザーの電子メール エイリアスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メール エイリアスのバイト数を加えた電子メール エイリアス文字列データ ブロックのバイト数。

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

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

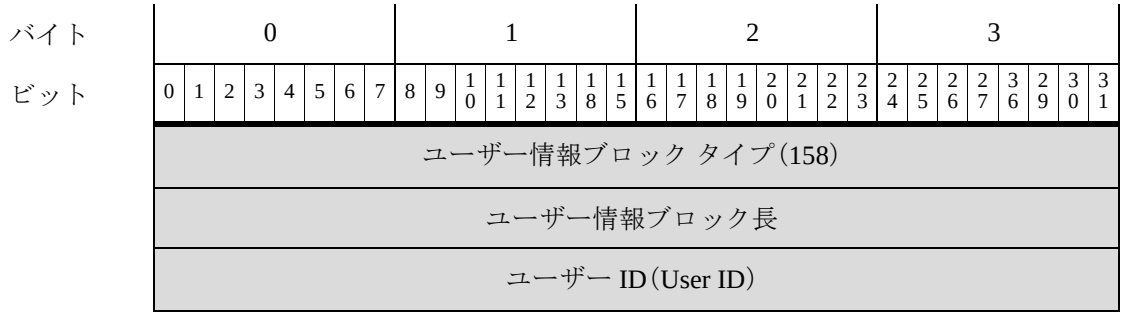
6.0+ の情報データ ユーザー ブロック

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

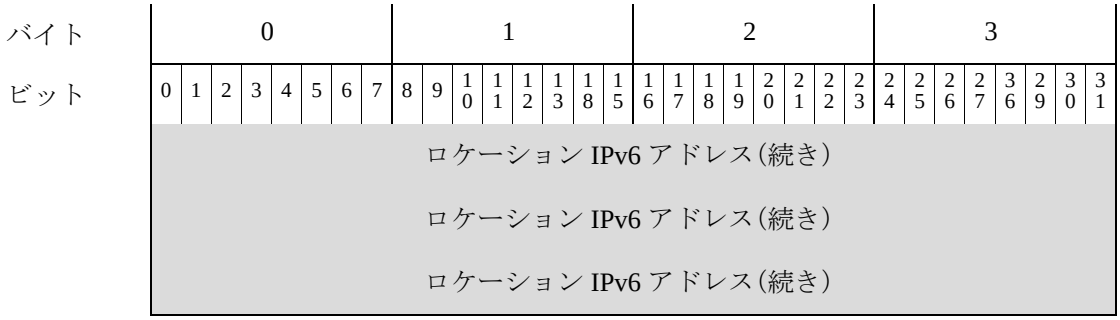
ユーザー情報データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 158 です。ユーザー重要度データ ブロックには、新しいエンドポイント プロファイル フィールド、セキュリティ インテリジェンスフィールド、IPv6 フィールドがあります。

ユーザー情報データ ブロックのブロック タイプは、4.7 ～ 4.10.x のシリーズ 1 ブロック グループのブロック タイプ 75 と、5.x のシリーズ 1 ブロック グループのブロック タイプ 120 です。詳細については、ユーザー情報データ ブロック 5.x（B-156 ページ）を参照してください。

次の図は、ユーザー情報データ ブロックの形式です。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
ユーザー（User）[名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ユーザー名...																															
	レルム ID																															
	プロトコル																															
ファースト [名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	名...																															
姓 [名前（Name）]	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	姓...																															
E メール	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	電子メール...																															
部署名（Department）	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	部署名...																															
電話	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	電話...																															
	エンドポイント プロファイル ID																															
	セキュリティ グループ ID																															
	ロケーション IPv6 アドレス																															



次の表は、ユーザー情報データ ブロックのコンポーネントについての説明です。

表 4-88　　ユーザー情報データ ブロックのフィールド

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

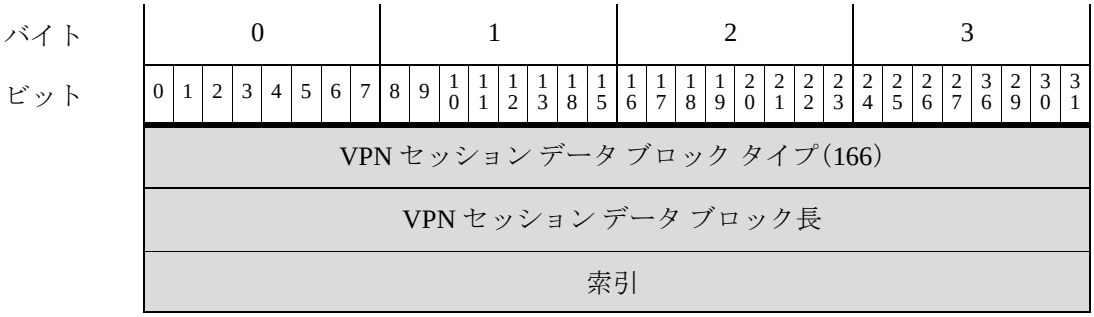
表 4-88　ユーザー情報データ ブロックのフィールド （続き）

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

6.2+ の VPN セッション データ ブロック

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

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



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
[グループ ポリシー（Group Policy）]	タイプ（Type）								文字列ブロック タイプ（0）																							
	文字列ブロック タイプ								文字列ブロック長																							
	文字列ブロック長								グループ ポリシー...																							
接続プロファイル	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	接続プロファイル...																															
	クライアント IP アドレス クライアント IP アドレス（続き） クライアント IP アドレス（続き） クライアント IP アドレス（続き）																															
クライアント オペレーティング システム	クライアントの国（Client Country）																文字列ブロック タイプ（0）															
	文字列ブロック タイプ（0）（続き）																文字列ブロック長															
	文字列ブロック長（続き）																クライアント オペレーティング システム...															
クライアント アプリケーション	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	クライアント アプリケーション...																															
	接続期間（Connection Duration）																															
	送信バイト数 送信バイト数（続き）																															
	受信バイト数（Bytes Received） 受信バイト数（続き）																															

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

表 4-89　VPN セッション データ ブロック フィールド

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

表 4-89　VPN セッション データ ブロック フィールド（続き）

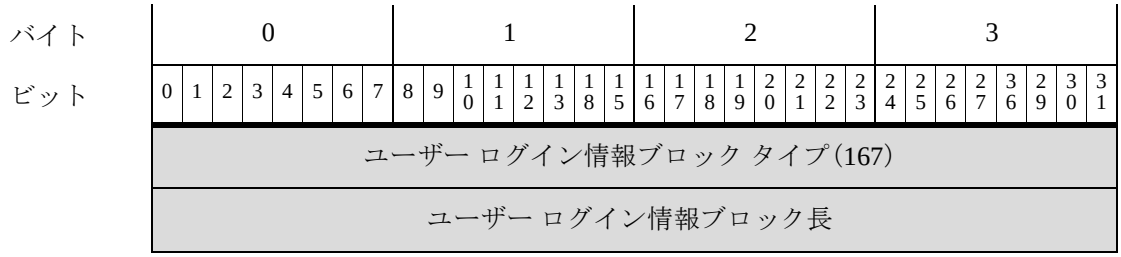
フィールド	データタイプ	説明
文字列ブロック長	uint32	ユーザー名文字列のデータ ブロック内のバイト数。これには、ブロック タイプ フィールドおよび長さフィールド用の 8 バイトと、オペレーティング システム名内のバイト数が含まれます。
クライアント オペレーティング システム	string	クライアント デバイスのオペレーティング システム。
文字列ブロック タイプ	uint32	クライアント デバイスで使用される VPN アプリケーションを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザー名文字列のデータ ブロック内のバイト数。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

ユーザー ログイン情報データ ブロック 6.2+

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

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

次の図は、ユーザー ログイン情報データ ブロックの形式を示しています。



	バイト	0								1								2								3							
	ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Timestamp																																
	IPv4 アドレス（IPv4 Address）																																
ユーザー（User）[名前（Name）]	文字列ブロック タイプ（0）																																
	文字列ブロック長																																
	ユーザー名...																																
ドメイン	文字列ブロック タイプ（0）																																
	文字列ブロック長																																
	ドメイン...																																
	ユーザー ID（User ID）																																
	レルム ID																																
	エンドポイント プロファイル ID																																
	セキュリティ グループ ID																																
	プロトコル																																
	ポート																	範囲の開始															
	開始ポート																	終了ポート															
E メール	文字列ブロック タイプ（0）																																
	文字列ブロック長																																
	電子メール...																																
	IPv6 アドレス IPv6 アドレス（続き） IPv6 アドレス（続き） IPv6 アドレス（続き）																																
	ロケーション IPv6 アドレス ロケーション IPv6 アドレス（続き） ロケーション IPv6 アドレス（続き）																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	ロケーション IPv6 アドレス（続き）																															
レポート基準	ログイン タイプ								承認タイプタイプ（Type）								文字列ブロック タイプ（0）															
	文字列ブロック タイプ（0）（続き）																文字列ブロック長															
	文字列ブロック長（続き）																レポート基準...															
説明	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	説明...																															
VPN セッション	VPN セッション データ ブロック タイプ（166）																															
	VPN セッション データ ブロック長																															
	VPN セッション...																															

次の表は、ユーザー ログイン情報データ ブロックのコンポーネントについての説明です。

表 4-90　　ユーザー ログイン情報データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザー ログイン情報ブロック タイプ	uint32	ユーザー ログイン情報データ ブロックを開始します。バージョン 6.2+ の場合、この値は 167 です。
ユーザー ログイン情報ブロック長	uint32	ユーザー ログイン情報データ ブロックのバイトの合計数（ユーザー ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザー ログイン情報データのバイト数を含む）。
Timestamp	uint32	イベントのタイムスタンプ。
IPv4 アドレス（IPv4 Address）	uint32	このフィールドは予約済みですが、設定されておりません。IPv4 アドレスは IPv6 アドレス フィールドに保存されます。詳細については、IP アドレス（1-4 ページ）を参照してください。
文字列ブロック タイプ	uint32	ユーザーのユーザー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザー名文字列データ ブロックのバイト数（ブロック タイプと長さのフィールド用の 8 バイト、およびユーザー名のバイト数を含む）。
[ユーザー名（Username）]	string	ユーザーのユーザー名。

表 4-90　ユーザー ログイン情報データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	ドメインを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにドメインのバイト数を加えたユーザー名文字列データ ブロックのバイト数。
ドメイン	string	ユーザーがログインしているドメイン。
ユーザー ID（User ID）	uint32	ユーザーの ID 番号。
レルム ID	uint32	アイデンティティ レルムに対応する整数 ID。
エンドポイント プロファイル ID	uint32	接続エンドポイントが使用するデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
セキュリティ グループ ID	uint32	ネットワーク トラフィック グループの ID 番号。
プロトコル	uint32	ユーザーの検出やレポートに使用するプロトコル。値は以下のとおりです。 • 165：FTP • 426：SIP • 547：AOL Instant Messenger • 683：IMAP • 710：LDAP • 767：NTP • 773：Oracle データベース • 788：POP3 • 1755：MDNS
[ポート（Port）]	uint16	ユーザーを検出したポート番号。
範囲の開始	uint16	TS エージェントが使用するポート範囲の開始ポート
開始ポート	uint16	TS エージェントが個々のユーザーに割り当てられている範囲の開始ポート。
終了ポート	uint16	TS エージェントが個々のユーザーに割り当てられている範囲の最終ポート。
文字列ブロック タイプ	uint32	ユーザーの電子メールアドレスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メール アドレスのバイト数を加えた電子メール アドレス文字列データ ブロックのバイト数。
E メール	string	ユーザーの電子メール アドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザーのログインが検出されたホストからの IPv6 アドレス。
ロケーション IPv6 アドレス	uint8[16]	ユーザーがログインした最新の IP アドレス。IPv4 または IPv6 のどちらかのアドレスになります。

表 4-90　ユーザー ログイン情報データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
ログイン タイプ	uint8	検出されたユーザー ログインのタイプ。
認証タイプ（Authentication Type）	uint8	ユーザーが使用する認証のタイプ。値は次のとおりです。 • 0：認証は不要 • 1：パッシブ認証、AD エージェント、または ISE セッション • 2：キャプティブ ポータルの正常な認証 • 3：キャプティブ ポータルのゲスト認証 • 4：キャプティブ ポータルの失敗認証
文字列ブロック タイプ	uint32	レポート基準値を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	レポート基準文字列データ ブロックのバイト数（ブロック タイプと長さのフィールド用の 8 バイト、およびレポート基準フィールドのバイト数を含む）。
レポート基準	string	Active Directory サーバーの名前など、このアクティビティのレポーター。
文字列ブロック タイプ	uint32	説明の値を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	説明文字列のデータ ブロック内のバイト数。これには、ブロック タイプ フィールドおよび長さフィールド用の 8 バイトと、説明フィールド内のバイト数が含まれます。
説明	string	ログインまたはログオフ アクティビティの説明。
VPN セッション ブロック タイプ	uint32	VPN セッション データを含む VPN セッション データ ブロックを開始します。この値は常に 166 です。
VPN セッション データ ブロック長	uint32	VPN セッション のデータ ブロック内のバイト数。これには、ブロック タイプ フィールドおよび長さフィールド用の 8 バイトと、VPN セッション データ ブロック内のバイト数が含まれます。
VPN セッション データ	VPN セッション データ	ログインを VPN セッションに関連付けた場合は、検出された VPN セッションに関する情報。VPN セッションが存在するときのみ使用されます。

ディスカバリ/接続イベント シリーズ 2 データ ブロック

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

表 4-91　ディスカバリ /接続イベント シリーズ 2 ブロック タイプ

タイプ（Type）	目次	データ ブロック ステータス	説明
15	アクセス コントロール ルール（Access Control Rule）	現在（Current）	アクセス コントロール ルールのメタデータ メッセージが、ポリシー UUID 値とルール ID 値を記述文字列にマップするときに使用します。アクセス コントロール ルール データ ブロック（4-212 ページ）を参照してください。
21	アクセス コントロール ルール理由	レガシー	アクセス コントロール ルールのメタデータ メッセージが、アクセス コントロール ルール理由を記述文字列にマップするときに使用します。アクセス コントロール ポリシー ルール理由データ ブロック（B-416 ページ）を参照してください。
22	セキュリティ インテリジェンスのカテゴリ（Security Intelligence Category）	現在（Current）	セキュリティ インテリジェンス情報の保存に使用します。セキュリティ インテリジェンス カテゴリ データ ブロック 5.1+（4-215 ページ）を参照してください。
57	ユーザー データ（User Data）	現在（Current）	ユーザー レコード メタデータ メッセージが、ユーザーを検出したユーザー ID 番号、プロトコル、そしてユーザー名を提供するために使用します。ユーザー データ ブロック（4-217 ページ）を参照してください。
59	アクセス コントロール ルール理由	現在（Current）	アクセス コントロール ルールのメタデータ メッセージが、アクセス コントロール ルール理由を記述文字列にマップするときに使用します。アクセス コントロール ルール理由データ ブロック 6.0+（4-214 ページ）を参照してください。

アクセス コントロール ルール データ ブロック

eStreamer サービスは、アクセス コントロール ルールのメタデータ メッセージでアクセス コントロール ルール データ ブロックを使用し、ポリシー UUID とルール ID を組み合わせて、記述文字列にマップします。アクセス コントロール ルール データ ブロックのブロック タイプは、シリーズ 2 ブロック グループのブロック タイプ 15 です。

次の図は、アクセス コントロール ルール データ ブロックの構造です。

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

表 4-92　　アクセス コントロール ルール データ ブロックのフィールド

フィールド	データタイプ	説明
アクセス コントロール ルール ブロック タイプ	uint32	アクセス コントロール ルール ブロックを開始します。この値は常に 15 です。
アクセス コントロール ルール ブロック長	uint32	アクセス コントロール ルール ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ルール ブロックの合計バイト数。
アクセス コントロール ルール UUID	uint8[16]	アクセス コントロール ルールの固有識別子。このフィールドとアクセス コントロール ルール ID を合わせると、このレコードの固有キーになります。
アクセス コントロール ルール ID	uint32	アクセス コントロール ルールの内部 シスコ 識別子。このフィールドとアクセス コントロール ルール UUID を合わせると、このレコードの固有キーになります。

表 4-92　アクセス コントロール ルール データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	アクセス コントロール ルール UUID とアクセス コントロール ルール ID に関連付けられているわかりやすい名前のある文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
[名前（Name）]	string	わかりやすい名前。

アクセス コントロール ルール理由データ ブロック 6.0+

eStreamer サービスでは、アクセス コントロール ルール理由データ ブロックをアクセス コントロール ルール理由メタデータ メッセージで使用して、アクセス制御原因を記述文字列にマッピングします。アクセスコントロールルール理由データブロックのブロックタイプは、シリーズ 2 ブロック グループのブロックタイプ 59 です。これはブロック タイプ 21 に取って代わります。

次の図は、アクセス コントロール ルール理由データ ブロックの構造です。

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

表 4-93　アクセス コントロール ルール理由データ ブロックのフィールド

フィールド	データタイプ	説明
アクセス コントロール ルール理由ブロック タイプ	uint32	アクセス コントロール ルール理由ブロックを開始します。この値は常に 59 です。
アクセス コントロール ルール理由ブロック長	uint32	アクセス コントロール ルール理由ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ルール理由ブロックの合計バイト数。

表 4-93　アクセス コントロール ルール理由データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
アクセス コントロール ルール理由	uint32	アクセス コントロール ルールによって接続がログに記録された理由。このフィールドは、このレコードの固有キーです。 イベントをトリガーしたルールの理由の番号。 ルールの理由は、複数のビットを設定できるバイナリ ビットマップです。ルールには、複数の理由がある場合があります。ビット値は次のとおりです。 • **1**：IP ブロック • **2**：IP モニター • **4**：ユーザー バイパス • **8**：ファイル モニター • **16**：ファイル ブロック • **32**：侵入モニター • **64**：侵入ブロック • **128**：ファイル再開ブロック • **256**：ファイル再開許可 • **512**：ファイルカスタム検出 • **1024**：SSL ブロック • **2048**：DNS ブロック • **4096**：DNS モニター • **8192**：URL ブロック • **16384**：URL モニター • **32768**：コンテンツ制約 • **65536**：インテリジェント アプリケーション バイパス • **131072**：WSA 脅威
文字列ブロック タイプ	uint32	アクセス コントロール ルール理由に関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	アクセス コントロール ルール理由の説明。

セキュリティ インテリジェンス カテゴリ データ ブロック 5.1+

eStreamer サービスは、アクセス コントロール ルール メタデータ メッセージのセキュリティ インテリジェンス カテゴリ データ ブロックで、セキュリティ インテリジェンス情報をストリーミングします。セキュリティ インテリジェンス カテゴリ データ ブロックのブロック タイプは、シリーズ 2 ブロック グループのブロック タイプ 22 です。

次の図は、セキュリティ インテリジェンス カテゴリ データ ブロックの構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
	セキュリティ インテリジェンス カテゴリのブロック タイプ（22）																															
	セキュリティ インテリジェンス カテゴリのブロック長																															
	セキュリティ インテリジェンス リスト ID																															
AC ポリシー UUID	アクセス コントロール ポリシー UUID																															
	アクセス コントロール ポリシー UUID（続き）																															
	アクセス コントロール ポリシー UUID（続き）																															
	アクセス コントロール ポリシー UUID（続き）																															
ルール名（Rule Name）	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	セキュリティ インテリジェンス リスト名...																															

次の表では、セキュリティ インテリジェンス カテゴリ データ ブロックのフィールドについて説明します。

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

フィールド	データタイプ	説明
セキュリティ インテリジェンス カテゴリ ブロック タイプ	uint32	セキュリティ インテリジェンス カテゴリのデータ ブロックを開始します。この値は常に 22 です。
セキュリティ インテリジェンス カテゴリのブロック長	uint32	セキュリティ インテリジェンス カテゴリ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたセキュリティ インテリジェンス カテゴリ ブロックの合計バイト数。
セキュリティ インテリジェンス リスト ID	uint32	接続によってトリガーされた IP ブロックリストまたは許可リストの ID。このフィールドとアクセス コントロール ポリシー UUID を合わせると、このレコードの固有キーになります。
アクセス コントロール ポリシー UUID	uint8[16]	セキュリティ インテリジェンスに設定されたアクセス コントロール ポリシーの UUID。このフィールドとセキュリティ インテリジェンス リスト ID を合わせると、このレコードの固有キーとなります。

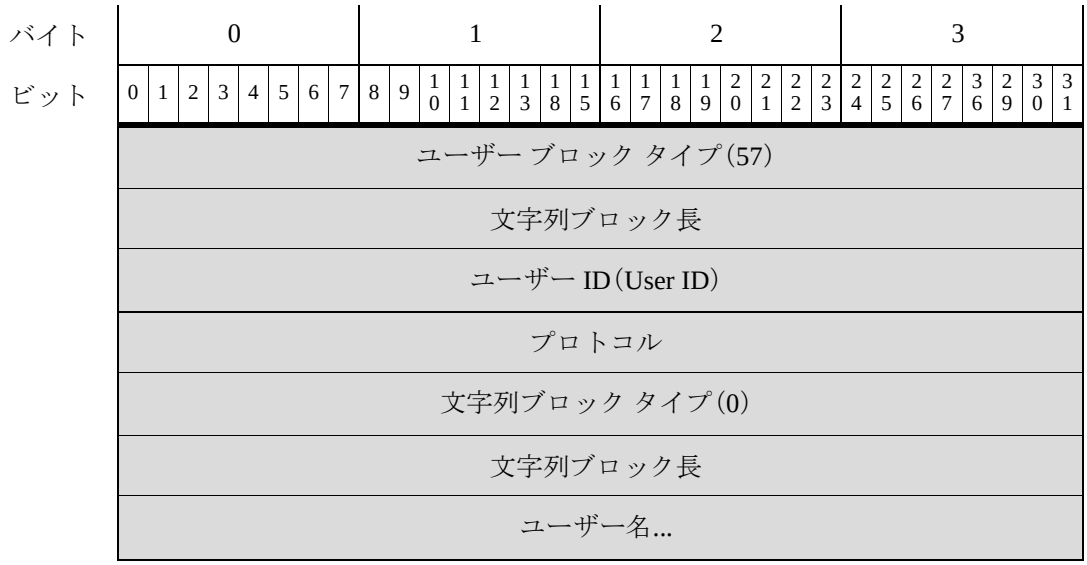
表 4-94　セキュリティ インテリジェンス カテゴリ データ ブロックのフィールド（続き）

フィールド	データタイプ	説明
文字列ブロック タイプ	uint32	セキュリティ インテリジェンス リストに関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトにセキュリティ インテリジェンス リスト名フィールドのバイト数を加えた名前文字列データ ブロックのバイト数。
セキュリティ インテリジェンス リスト名	string	接続でトリガーされたセキュリティ インテリジェンス カテゴリ IP ブロックリストまたは許可リストの名前。

ユーザー データ ブロック

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

次の図は、ユーザー データ ブロックの構造です。



次の表では、ユーザー データ ブロックのフィールドについて説明します。

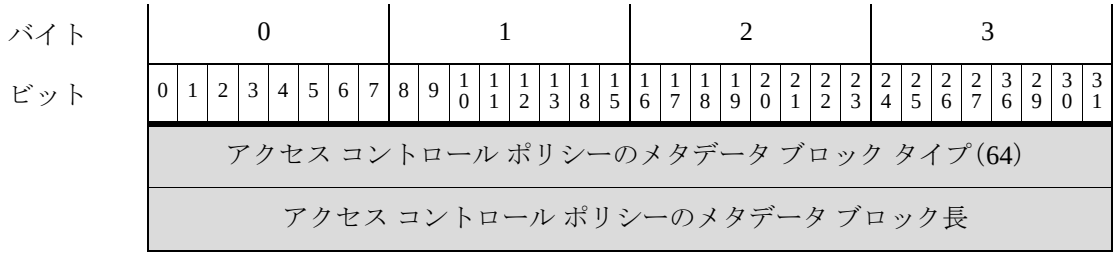
表 4-95　ユーザー データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザー ブロック タイプ	uint32	ユーザー ブロックを開始します。この値は常に 57 です。
文字列ブロック長	uint32	ユーザー ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータのバイト数を加えたユーザー ブロックの合計バイト数。
ユーザー ID（User ID）	uint32	ユーザーの固有識別情報。このフィールドは、このレコードの固有キーです。
プロトコル	uint32	ユーザーの検出やレポートに使用するプロトコル。値は以下のとおりです。 • 165：FTP • 426：SIP • 547：AOL Instant Messenger • 683：IMAP • 710：LDAP • 767：NTP • 773：Oracle データベース • 788：POP3 • 1755：MDNS
文字列ブロック タイプ	uint32	ユーザー名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドとヘッダー フィールドの 8 バイトにユーザー名フィールドのバイト数を加えたユーザー名文字列データ ブロックのバイト数。
[ユーザー名（Username）]	string	ユーザーの名前

アクセス コントロール ポリシー メタデータ ブロック 6.0+

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

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



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	18	15	16	17	18	19	20	21	22	23	24	25	26	27	36	29	30	31
AC ポリシー UUID	アクセス コントロール ポリシー UUID																															
	アクセス コントロール ポリシー UUID（続き）																															
	アクセス コントロール ポリシー UUID（続き）																															
	アクセス コントロール ポリシー UUID（続き）																															
	センサー ID（Sensor ID）																															
ポリシー名	文字列ブロック タイプ（0）																															
	文字列ブロック長																															
	ポリシー名...																															

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

表 4-96　　アクセス コントロール ポリシーのメタデータブロックのフィールド

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

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。