



検出と接続データ構造の概要

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

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

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

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

eStreamer サーバからのディスカバリ イベントまたは接続イベントの要求については、[要求フラグ \(2-12 ページ\)](#) 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 \(2-19 ページ\)](#) を参照してください。

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

- [ディスカバリ イベントと接続イベントのデータ メッセージ \(4-2 ページ\)](#) では、eStreamer がホスト ディスカバリ メッセージ、ユーザ メッセージ、接続メッセージに使用する構造の概要を紹介しています。
- [ディスカバリ イベントと接続イベントのレコード タイプ \(4-2 ページ\)](#) では、ディスカバリ イベントと接続イベント レコード タイプについて説明します。
- [ディスカバリ イベントのメタデータ \(4-7 ページ\)](#) では、たとえば、イベント内のユーザ ID をユーザ名に変換するなど、数字データとコード化データをテキストに変換するためのコンテキスト情報を要求できるメタデータ レコードについて説明します。
- [ディスカバリ イベント ヘッダー 5.2+ \(4-41 ページ\)](#) 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(4-45 ページ)では、eStreamer が各種ホスト ディスカバリ イベントタイプに使用するデータ レコードの構造について説明します。
- イベントタイプ別のユーザデータ構造(4-62 ページ)では、eStreamer が各種ユーザ イベントタイプに使用するデータ レコードの構造について説明します。
- ディスカバリ (シリーズ 1) ブロック(4-63 ページ)では、ディスクバリ イベントメッセージと接続イベントメッセージで複雑なレコードを伝えるために使用する一連のデータ ブロック構造について説明します。シリーズ 1 のデータ ブロックは、関連イベントでも使用します。
- ユーザ脆弱性データ ブロック 5.0+(4-162 ページ)では、複雑なユーザ イベント レコードを伝えるために使用するその他のシリーズ 1 ブロック構造について説明します。



ヒント

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

ディスクバリ イベントと接続イベントのデータ メッセージ

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

- オプションの netmap ID
- レコードタイプを定義するレコード ヘッダー
- イベントを識別し、その特性を表すディスクバリ イベント ヘッダー。具体的にはイベントタイプとサブタイプを識別します。詳細については、ディスクバリ イベント ヘッダー 5.2+(4-41 ページ)を参照してください。
- ブロック ヘッダーとデータ ブロックからなるデータ レコード。ディスクバリ イベントと接続イベントのデータ メッセージは、シリーズ 1 のデータ ブロックを使用します。詳細については、ホスト ディスカバリ データ ブロックと接続データ ブロック(4-64 ページ)またはユーザ脆弱性データ ブロック 5.0+(4-162 ページ)を参照してください。

ディスクバリ イベントと接続イベントのレコードタイプ

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

表 4-1 ディスカバリ イベントと接続イベントのレコードタイプ

レコードタイプ	含まれるブロックタイプ	シリーズ	説明	レコードステータス	データ形式の参照先...
10	139	1	新規ホストを検出	現在 (Current)	新規ホスト メッセージと最後の確認日時ホスト メッセージ(4-46 ページ)
11	103	1	新規 TCP サーバ	現在 (Current)	サーバ メッセージ(4-47 ページ)
12	103	1	新規 UDP サーバ	現在 (Current)	サーバ メッセージ(4-47 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 (4-48 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 (4-48 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 (4-48 ページ)
16	103	1	TCP サーバ情報更新	現在 (Current)	サーバ メッセージ(4-47 ページ)
17	103	1	UDP サーバ情報更新	現在 (Current)	サーバ メッセージ(4-47 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 (4-50 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(4-50 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(4-50 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(4-50 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(4-51 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(4-51 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(4-51 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(4-51 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(4-51 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(4-52 ページ)
28	該当なし	該当なし	ホストの追加 MAC を検出	現在 (Current)	MAC アドレス メッセージ(4-52 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(4-49 ページ)

表 4-1 ディスカバリ イベントと接続イベントのレコードタイプ(続き)

レコードタイプ	含まれるブロックタイプ	シリーズ	説明	レコードステータス	データ形式の参照先...
31	該当なし	該当なし	ルータ/ブリッジとして識別したホスト	現在 (Current)	ブリッジ/ルータとして識別したホストメッセージ(4-52 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(4-53 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(4-48 ページ)
42	35	1	NetBIOS 名変更	現在 (Current)	NetBIOS 名変更メッセージ(4-53 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(4-50 ページ)
45	37	1	更新バナー	現在 (Current)	更新バナー メッセージ(4-54 ページ)
46	55	1	ホスト属性を追加	現在 (Current)	属性メッセージ(4-57 ページ)
47	55	1	ホスト属性を更新	現在 (Current)	属性メッセージ(4-57 ページ)
48	55	1	ホスト属性を削除	現在 (Current)	属性メッセージ(4-57 ページ)
51	103	1	TCP サーバ信頼度更新	レガシー	サーバメッセージ(4-47 ページ)
52	103	1	UDP サーバ信頼度更新	レガシー	サーバメッセージ(4-47 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(4-50 ページ)
54	該当なし	該当なし	フィンガープリントメタデータ	現在 (Current)	フィンガープリント レコード(4-8 ページ)
55	該当なし	該当なし	クライアントアプリケーションメタデータ	現在 (Current)	クライアントアプリケーション レコード(4-10 ページ)
57	該当なし	該当なし	脆弱性メタデータ	現在 (Current)	脆弱性レコード(4-10 ページ)
58	該当なし	該当なし	重要度メタデータ	現在 (Current)	重要度レコード(4-13 ページ)
59	該当なし	該当なし	ネットワーク プロトコルメタデータ	現在 (Current)	ネットワーク プロトコル レコード(4-13 ページ)
60	該当なし	該当なし	属性メタデータ	現在 (Current)	属性レコード(4-14 ページ)
61	該当なし	該当なし	スキャンタイプメタデータ	現在 (Current)	スキャンタイプ レコード(4-15 ページ)
63	該当なし	該当なし	サーバメタデータ	現在 (Current)	サービス レコード(4-16 ページ)

表 4-1 ディスカバリ イベントと接続イベントのレコードタイプ(続き)

レコードタイプ	含まれるブロックタイプ	シリーズ	説明	レコードステータス	データ形式の参照先...
71	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-144 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-160 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-167 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-175 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-189 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-203 ページ)
71	163	1	接続統計情報	現在 (Current)	接続統計データ ブロック 6.2+ (4-122 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 (4-55 ページ)
74	該当なし	該当なし	ユーザ設定 OS	現在 (Current)	ユーザ サーバ メッセージとオペレーティング システム メッセージ (4-59 ページ)
75	該当なし	該当なし	ユーザ設定サーバ	現在 (Current)	ユーザ サーバ メッセージとオペレーティング システム メッセージ (4-59 ページ)
76	83	1	ユーザ削除プロトコル	現在 (Current)	ユーザ プロトコル メッセージ (4-59 ページ)
77	60	1	ユーザ削除クライアント アプリケーション	現在 (Current)	ユーザ クライアント アプリケーション メッセージ (4-60 ページ)
78	78	1	ユーザ削除アドレス	現在 (Current)	ユーザ追加/削除ホスト メッセージ (4-56 ページ)
79	77	1	ユーザ削除サーバ	現在 (Current)	ユーザ削除サーバ メッセージ (4-57 ページ)
80	80	1	ユーザ設定の有効な脆弱性	現在 (Current)	バージョン 4.6.1+ のユーザ設定脆弱性メッセージ (4-56 ページ)
81	80	1	ユーザ設定の無効な脆弱性	現在 (Current)	バージョン 4.6.1+ のユーザ設定脆弱性メッセージ (4-56 ページ)
82	81	1	ユーザ設定ホスト重要度	現在 (Current)	ユーザ設定ホスト重要度メッセージ (4-57 ページ)
83	55	1	ユーザ設定属性値	現在 (Current)	属性値メッセージ (4-58 ページ)
84	82	1	ユーザ削除属性値	現在 (Current)	属性値メッセージ (4-58 ページ)
85	78	1	ユーザ追加ホスト	現在 (Current)	ユーザ追加/削除ホスト メッセージ (4-56 ページ)
86	該当なし	該当なし	ユーザ追加サーバ	現在 (Current)	ユーザ サーバ メッセージとオペレーティング システム メッセージ (4-59 ページ)
87	60	1	ユーザ追加クライアント アプリケーション	現在 (Current)	ユーザ クライアント アプリケーション メッセージ (4-60 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...
88	83	1	ユーザ追加プロトコル	現在 (Current)	ユーザ プロトコル メッセージ(4-59 ページ)
89	142	1	ユーザ追加スキャン結果	現在 (Current)	スキャン結果を追加メッセージ(4-60 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(4-17 ページ)
92	120	1	ユーザ ドロップ変更イベント	現在 (Current)	ユーザ変更メッセージ(4-62 ページ)
93	120	1	ユーザ削除変更イベント	現在 (Current)	ユーザ変更メッセージ(4-62 ページ)
94	120	1	新規ユーザ識別イベント	現在 (Current)	ユーザ変更メッセージ(4-62 ページ)
95	121	1	ユーザ ログイン変更イベント	現在 (Current)	ユーザ情報更新メッセージブロック(4-63 ページ)
96	該当なし	該当なし	ソース ディテクタ レコード	現在 (Current)	ソースディテクタ レコード(4-18 ページ)
98	57	2	ユーザ レコード	現在 (Current)	ユーザ レコード(4-20 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(4-61 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(4-61 ページ)
103	94	1	アイデンティティ タイムアウト イベント	現在 (Current)	アイデンティティ競合とアイデンティティ タイムアウトシステムメッセージ(4-61 ページ)
106	該当なし	該当なし	サードパーティ スキャナ脆弱性レコード	現在 (Current)	サードパーティ スキャナの脆弱性レコード(4-19 ページ)
107	122	1	クライアント アプリケーション更新	現在 (Current)	クライアント アプリケーション メッセージ(4-48 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)
115	該当なし	該当なし	セキュリティ ゾーン名レコード	現在 (Current)	セキュリティ ゾーン名レコード(3-31 ページ)
116	14	2	インターフェイス名レコード	現在 (Current)	インターフェイス名レコード(3-33 ページ)
117	14	2	アクセス コントロール ポリシー名メタデータ	現在 (Current)	アクセス コントロール ポリシー名のレコード(3-34 ページ)

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...
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(4-24 ページ)
121	該当なし	該当なし	URL カテゴリ統計	現在 (Current)	URL カテゴリ レコードメタデータ (4-25 ページ)
122	該当なし	該当なし	URL レピュテーションメタデータ	現在 (Current)	URL レピュテーションレコードメタデータ (4-26 ページ)
124	21	2	アクセスコントロールルール理由メタデータ	現在 (Current)	アクセスコントロールルール理由メタデータ(4-27 ページ)
145	64	2	アクセスコントロールポリシーメタデータ	現在 (Current)	アクセスコントロールポリシーメタデータ (4-29 ページ)
146	64	2	プレフィルタポリシーメタデータ	現在 (Current)	プレフィルタポリシーメタデータ (4-30 ページ)
147	21	2	トンネルまたはプレフィルタルールメタデータ	現在 (Current)	トンネルまたはプレフィルタのルールのメタデータ (4-32 ページ)
160	7	1	ホスト IOC セットメッセージ	現在 (Current)	ホスト IOC セットメッセージ(4-62 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)
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 (4-33 ページ)
281	該当なし	該当なし	セキュリティインテリジェンス送信元/宛先レコード	現在 (Current)	セキュリティインテリジェンス送信元/宛先レコード(4-35 ページ)

ディスカバリ イベントのメタデータ

メタデータバージョン番号でメタデータを要求します。Firepower システムのバージョンに対応するメタデータバージョンについては、[メタデータについて\(2-44 ページ\)](#)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\(2-45 ページ\)](#)を参照してください。

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

- [フィンガープリント レコード\(4-8 ページ\)](#)
- [クライアント アプリケーション レコード\(4-10 ページ\)](#)
- [脆弱性レコード\(4-10 ページ\)](#)
- [重要度レコード\(4-13 ページ\)](#)
- [ネットワーク プロトコル レコード\(4-13 ページ\)](#)
- [属性レコード\(4-14 ページ\)](#)
- [スキャンタイプ レコード\(4-15 ページ\)](#)
- [サービス レコード\(4-16 ページ\)](#)
- [ソース タイプ レコード\(4-17 ページ\)](#)
- [ソース アプリケーション レコード\(4-17 ページ\)](#)
- [ソースディテクタ レコード\(4-18 ページ\)](#)
- [サードパーティ スキャナの脆弱性レコード\(4-19 ページ\)](#)
- [ユーザ レコード\(4-20 ページ\)](#)
- [Web アプリケーション レコード\(4-22 ページ\)](#)
- [侵入ポリシー名レコード\(4-23 ページ\)](#)
- [アクセス コントロール ルール アクション レコード メタデータ\(4-24 ページ\)](#)
- [URL カテゴリ レコード メタデータ\(4-25 ページ\)](#)
- [URL レピュテーション レコード メタデータ\(4-26 ページ\)](#)
- [アクセス コントロール ルール理由メタデータ\(4-27 ページ\)](#)
- [セキュリティ インテリジェンス カテゴリ メタデータ\(4-33 ページ\)](#)
- [セキュリティ インテリジェンス送信元/宛先レコード\(4-35 ページ\)](#)

侵入イベントと関連イベントのメタデータ レコードについては、[侵入イベントとメタデータのレコードタイプ\(3-1 ページ\)](#)を参照してください。

フィンガープリント レコード

eStreamer サービスは、次の形式のフィンガープリント レコードで、イベントのフィンガープリント メタデータを送信します。(フィンガープリント メタデータは、以下のメタデータ フラグの1つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。[要求フラグ\(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、フィンガープリント レコードを示す 54 です。

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

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	Netmap ID																レコードタイプ(54)																							
	レコード長																																							
フィンガープリント UUID	フィンガープリント UUID フィンガープリント UUID(続き) フィンガープリント UUID(続き) フィンガープリント UUID(続き)																																							
	OS 名長さ																																							
	OS 名...																																							
	OS ベンダー長さ																																							
	OS ベンダー...																																							
	OS バージョン長さ																																							
	OS バージョン...																																							

次の表では、フィンガープリント レコードのフィールドについて説明します。

表 4-2 フィンガープリント レコードのフィールド

フィールド	データタイプ	説明
フィンガープリント UUID	uint8[16]	オペレーティング システムの一意の 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 \(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、クライアント アプリケーション レコードを示す 55 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン (1)																メッセージ タイプ (4)															
	メッセージ長																															
	Netmap ID																レコード タイプ (55)															
	レコード長																															
	アプリケーション ID (Application ID)																															
	名前の長さ																															
	名前...																															

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

表 4-3 クライアント アプリケーション レコードのフィールド

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

脆弱性レコード

eStreamer サービスは、次の形式の脆弱性レコードで、イベントの脆弱性情報を格納したメタデータを送信します。(脆弱性情報は、以下のメタデータ フラグの1つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。[要求フラグ \(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコード タイプ フィールドの値は、脆弱性レコードを示す 57 です。

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

次の表では、脆弱性レコードのフィールドについて説明します。

表 4-4 脆弱性レコードのフィールド

フィールド	データタイプ	説明
脆弱性 ID	uint32	脆弱性 ID 番号このフィールドは、このレコードの固有キーです。
影響	uint32	侵入データ、ホスト ディスカバリ イベント、脆弱性アセスメント間の相関に基づいて決定した影響レベルに対応した、脆弱性の影響。ここに設定可能な値の範囲は 1 ~ 10 です。最も深刻な場合で 10 です。脆弱性の影響度の値は、Bugtraq エントリの作成者が設定します。
エクスプロイト	uint8	脆弱性に既知のエクスプロイトがあるかどうかを示します。有効な値は次のとおりです。 <ul style="list-style-type: none"> 0: はい 1: いいえ
[リモート (Remote)]	uint8	ネットワーク上でつけ込まれる余地が脆弱性にあるかどうかを示します。有効な値は次のとおりです。 <ul style="list-style-type: none"> 0: はい 1: いいえ 空白 — 不明なリモート エクスプロイトに対する脆弱性
入力日長さ	uint32	入力日付フィールド長さ。
入力日	string	脆弱性がデータベースに登録された日付。
公開日長さ	uint32	公開された日付フィールド長さ。
公開日	string	脆弱性が公開された日付。
変更日長さ	uint32	変更された日付フィールド長さ。
変更日	string	脆弱性の最終変更日 (該当する場合)。
タイトル長さ	uint32	タイトルフィールド長さ。
役職 (Title)	string	脆弱性のタイトル。
概略説明長さ	uint32	概略説明フィールド長さ。
概略説明 (Short Description)	string	脆弱性の概略説明。
説明の長さ	uint32	説明フィールドの長さ。
説明	string	脆弱性に関する一般的な説明。
技術的説明の長さ	uint32	技術的説明フィールド長さ。
技術的説明	string	脆弱性に関する技術的説明。
ソリューション長さ	uint32	ソリューションフィールド長さ。
ソリューション	string	脆弱性に対するソリューション。

重要度レコード

eStreamer サービスは、次の形式の重要度レコードで、イベントのホスト重要度情報を格納したメタデータを送信します。(重要度情報は、以下のメタデータ フラグの1つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。[要求フラグ \(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、重要度レコードを示す 58 です。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ヘッダー バージョン(1)																メッセージタイプ(4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ(58)																							
	レコード長																																							
	重要度 ID																																							
	名前の長さ																																							
	名前...																																							

次の表では、重要度レコードのフィールドについて説明します。

表 4-5 重要度レコードのフィールド

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

ネットワーク プロトコル レコード

eStreamer サービスは、次の形式のネットワーク プロトコル レコードで、イベントのネットワーク プロトコル情報を格納したメタデータを送信します。(ネットワーク プロトコル情報は、以下のメタデータ フラグの1つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。[要求フラグ \(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、ネットワーク プロトコル レコードを示す値 59 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(59)															
	レコード長																															
	ネットワーク プロトコル ID																															
	名前の長さ																															
	名前...																															

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

表 4-6 ネットワーク プロトコル レコードのフィールド

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

属性レコード

eStreamer サービスは、次の形式の属性レコードで、イベントの属性情報を格納したメタデータを送信します。(属性情報は、以下のメタデータ フラグの1つ(要求メッセージの要求フラグフィールドのビット 1、14、15、または 20)が設定されると送信されます。[要求フラグ\(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、属性レコードを示す 60 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(60)															
	レコード長																															

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
属性 ID																																								
名前の長さ																																								
名前...																																								

次の表では、属性レコードのフィールドについて説明します。

表 4-7 属性レコードのフィールド

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

スキャンタイプレコード

eStreamer サービスは、次の形式のスキャンタイプレコードで、イベントのスキャンタイプ情報を格納したメタデータを送信します。(スキャンタイプ情報は、以下のメタデータフラグの1つ(要求メッセージの要求フラグフィールドのビット 1、14、15、または 20)が設定されると送信されます。[要求フラグ \(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、スキャンタイプレコードを示す 61 です。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
ヘッダーバージョン(1)																メッセージタイプ(4)																								
メッセージ長																																								
Netmap ID																レコードタイプ(61)																								
レコード長																																								
スキャンタイプ ID																																								
名前の長さ																																								
名前...																																								

次の表では、スキャンタイプレコードのフィールドについて説明します。

表 4-8 スキャンタイプレコードのフィールド

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

サービス レコード

eStreamer サービスは、次の形式のサービス レコードで、イベントのサービス情報を格納したメタデータを送信します。サービスのアプリケーション プロトコルのアプリケーション ID は、メタデータまでのクロスリファレンスを提供します。(サービス情報は、以下のメタデータ フラグの1つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。[要求フラグ \(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、サービス レコードを示す 63 です。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ヘッダー バージョン(1)																メッセージタイプ(4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ(63)																							
	レコード長																																							
	アプリケーション ID (Application ID)																																							
	名前の長さ																																							
	名前...																																							

次の表では、サービス レコードのフィールドについて説明します。

表 4-9 サービス レコードのフィールド

フィールド	データタイプ	説明
アプリケーション ID (Application ID)	uint32	アプリケーション プロトコルのアプリケーション ID 番号。このフィールドは、このレコードの固有キーです。
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\(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、送信元タイプレコードを示す 90 です。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ヘッダー バージョン(1)																メッセージ タイプ(4)																							
	メッセージ長																																							
	Netmap ID																レコード タイプ(90)																							
	レコード長																																							
	ソース タイプ ID																																							
	名前の長さ																																							
	名前...																																							

次の表では、ソース タイプ レコードのフィールドについて説明します。

表 4-10 ソース タイプ レコードのフィールド

フィールド	データタイプ	説明
ソース タイプ ID	uint32	ソース タイプの ID 番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	送信元タイプ名バイト数。
[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\(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、送信元アプリケーションレコードを示す 91 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン(1)																メッセージ タイプ(4)															
	メッセージ長																															
	Netmap ID																レコード タイプ(91)															
	レコード長																															
	ソース アプリケーション ID																															
	名前の長さ																															
	名前...																															

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

表 4-11 送信元アプリケーション レコードのフィールド

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

ソースディテクタ レコード

eStreamer サービスは、次の形式の送信元タイプ レコードで、ホスト ディスカバリ イベントの送信元アプリケーションに関する情報を格納したメタデータを送信します。(送信元タイプ情報は、以下のメタデータ フラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。[要求フラグ\(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプ フィールドの値は、送信元ディテクタ レコードを示す 96 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン(1)																メッセージ タイプ(4)															
	メッセージ長																															
	Netmap ID																レコード タイプ(96)															

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

次の表では、送信元ディテクタ レコードのフィールドについて説明します。

表 4-12 送信元ディテクタ レコードのフィールド

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

サードパーティ スキャナの脆弱性レコード

eStreamer サービスは、次の形式のサードパーティ スキャナ脆弱性レコードで、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\(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、サードパーティ スキャナ脆弱性レコードを示す 106 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダーバージョン(1)																メッセージタイプ(4)																
メッセージ長																																
Netmap ID																レコードタイプ(106)																
レコード長																																
脆弱性 ID																																
スキャナタイプ																																
タイトル長さ																																

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

次の表では、脆弱性レコードのフィールドについて説明します。

表 4-13 サードパーティ スキャナ脆弱性レコードのフィールド

フィールド	データタイプ	説明
脆弱性 ID	uint32	サードパーティ脆弱性 ID 番号。このフィールドとスキャナタイプを合わせると、このレコードの固有キーとなります。
スキャナタイプ	uint32	サードパーティ スキャナタイプ。このフィールドと脆弱性 ID を合わせると、このレコードの固有キーとなります。
タイトル長さ	uint32	タイトル フィールド長さ。
役職 (Title)	string	脆弱性のタイトル。
説明の長さ	uint32	説明フィールドの長さ。
説明	string	脆弱性に関する一般的な説明。
CVE ID 長さ	uint32	CVE ID フィールドの長さ。
CVE ID	string	脆弱性の Common Vulnerabilities and Exposures (CVE) ID 番号。
BugTraq ID の長さ	uint32	BugTraq ID フィールドの長さ。
BugTraq ID	string	脆弱性の BugTraq ID 番号

ユーザ レコード

eStreamer サービスは、次の形式のユーザ レコードで、システムが検出したユーザに関する情報を格納したメタデータを送信します。(バージョン 4 メタデータとポリシー イベント要求フラグ (それぞれ要求メッセージの要求フラグ フィールドのビット 20 と 22) を設定すると、ユーザ情報が送信されます。[要求フラグ \(2-12 ページ\)](#) を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプ フィールドの値は、ユーザ レコードを示す 98 です。

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

次の表は、ユーザレコードのフィールドについての説明です。

表 4-14 ユーザレコードのフィールド

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

表 4-14 ユーザレコードのフィールド(続き)

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

Web アプリケーション レコード

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

eStreamer サービスは、次の形式の Web アプリケーション レコードで、イベントの Web アプリケーション メタデータを送信します。(Web アプリケーション メタデータは、以下のメタデータフラグの 1 つ(要求メッセージの要求フラグ フィールドのビット 1、14、15、または 20)が設定されると送信されます。[要求フラグ\(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、Web アプリケーション レコードを示す 109 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(109)															
	レコード長																															

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
アプリケーション ID (Application ID)																																								
名前の長さ																																								
名前...																																								

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

表 4-15 Web アプリケーション レコードのフィールド

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

侵入ポリシー名レコード

eStreamer サービスは、次の形式の侵入ポリシー名レコードで、接続イベントの侵入ポリシー名情報を格納したメタデータを送信します。(侵入ポリシー名情報は、メタデータ フラグ (要求メッセージの要求フラグ フィールドのバージョン 4 メタデータ ビット 20) が設定されると送信されます。[要求フラグ \(2-12 ページ\)](#) を参照してください)。ちなみに、メッセージ長さフィールドの後のレコードタイプフィールドの値は、侵入ポリシー名レコードを示す 118 です。シリーズ 2 セットのデータ ブロックのブロック タイプ 14 の UUID 文字列データ ブロックが含まれています。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
ヘッダー バージョン (1)																メッセージ タイプ (4)																								
メッセージ長																																								
Netmap ID																レコード タイプ (118)																								
レコード長																																								
侵入ポリシー名データ ブロック (14)																																								
侵入ポリシー名データ ブロック長																																								
侵入ポリシー UUID																																								

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

次の表では、侵入ポリシー名データブロックのフィールドについて説明します。

表 4-16 侵入ポリシー名データブロックのフィールド

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

アクセスコントロールルールアクションレコードメタデータ

eStreamer サービスは、次の形式のアクセスコントロールルールアクションレコードで、トリガーのかかったアクセスコントロールルールに関連付けられたアクションを格納したメタデータを送信します。(アクセスコントロールルールアクション情報は、バージョン 4 メタデータフラグ(要求メッセージの要求フラグフィールドのビット 20)が設定されると送信されます。[要求フラグ\(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、アクセスコントロールルールアクションレコードを示す 120 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(120)															
	レコード長																															
	アクセスコントロールルールアクションID																															
	名前の長さ																															
	名前...																															

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

表 4-17 アクセスコントロールルールアクションレコードのフィールド

フィールド	データタイプ	説明
アクセスコントロールルールアクションID	uint32	アクセスコントロールルールアクションのID番号。このフィールドは、このレコードの固有キーです。
名前の長さ	uint32	名前に含まれるバイト数。
[名前(Name)]	string	ファイアウォールルールアクション名。

URL カテゴリ レコードメタデータ

eStreamer サービスは、次の形式の URL カテゴリ レコードで、接続ログの URL に関連付けられたカテゴリ名を格納したメタデータを送信します。(URL カテゴリ情報は、バージョン4メタデータフラグ(要求メッセージの要求フラグフィールドのビット20)が設定されると送信されます。[要求フラグ\(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、URL カテゴリ レコードを示す 121 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(121)															

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

次の表では、URL カテゴリ レコードのフィールドについて説明します。

表 4-18 URL カテゴリ レコードのフィールド

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

URL レピュテーション レコード メタデータ

eStreamer サービスは、次の形式の URL レピュテーション レコードで、URL に関連付けられたレピュテーション (リスク レベル) を格納したメタデータを送信します。(URL レピュテーション情報は、バージョン 4 メタデータ フラグ(要求メッセージの要求フラグ フィールドのビット 20)が設定されると送信されます。[要求フラグ\(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長さフィールドの後の URL レピュテーション メタデータ レコードフィールドの値は、URL レピュテーション メタデータ レコードを示す 122 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダー バージョン(1)																メッセージタイプ(4)																
メッセージ長																																
Netmap ID																レコードタイプ(122)																
レコード長																																
URL レピュテーション ID																																
名前の長さ																																
名前...																																

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

表 4-19 URL レピュテーション レコードのフィールド

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

アクセス コントロール ルール理由メタデータ

eStreamer サービスは、次の形式のアクセス コントロール ルール理由レコードで、アクセス コントロール ルールで侵入イベントまたは接続イベントにトリガーがかかった理由に関する情報を格納したメタデータを送信します。アクセス コントロール ルール理由メタデータは、バージョン 4 メタデータ フラグ (要求メッセージの要求フラグ フィールドのビット 20) が設定されると送信されます。[要求フラグ \(2-12 ページ\)](#) を参照してください。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、アクセス コントロール ルール理由レコードを示す 124 です。このメタデータには、アクセス コントロール ルール理由ブロックを格納します ([アクセス コントロール ルール理由データ ブロック 5.1+\(4-207 ページ\)](#) を参照)。アクセス コントロール ルール理由データ ブロックのブロックタイプは、シリーズ 2 のブロックタイプ 21 です。

バイト	0								1					2				3														
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン (1)																メッセージ タイプ (4)															
	メッセージ長																															
	Netmap ID																レコード タイプ (124)															
	レコード長																															
	アクセス コントロール ルール理由ブロック タイプ (21)																															
	アクセス コントロール ルール理由ブロック長																															
	アクセス コントロール ルール理由																文字列ブロック タイプ (0)															
	文字列ブロック タイプ (0) (続き)																文字列ブロック長															
	文字列ブロック長 (続き)																説明...															

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

表 4-20 アクセス コントロール ルール理由メタデータのフィールド

フィールド	データ タイプ	説明
アクセス コントロール ルール理由ブロック タイプ	uint32	アクセス コントロール ルール理由ブロックを開始します。この値は常に 21 です。これはシリーズ 2 のデータ ブロックです。
アクセス コントロール ルール理由ブロック 長	uint32	アクセス コントロール ルール理由ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたアクセス コントロール ルール理由ブロックの合計バイト数。
アクセス コントロール ルール理由	uint16	<p>アクセス コントロール ルールによって接続がログに記録された理由。このフィールドは、このレコードの固有キーです。</p> <p>イベントをトリガーしたルールの理由の番号。</p> <p>ルールの理由は、複数のビットを設定できるバイナリ ビットマップです。ルールには、複数の理由がある場合があります。ビット値は次のとおりです。</p> <ul style="list-style-type: none"> • 1: IP ブロック • 2: IP モニタ • 4: ユーザ バイパス • 8: ファイル モニタ • 16: ファイル ブロック • 32: 侵入モニタ • 64: 侵入ブロック • 128: ファイル再開ブロック • 256: ファイル再開許可 • 512: ファイルカスタム検出 • 1024: SSL ブロック • 2048: DNS ブロック • 4096: DNS モニタ • 8192: URL ブロック • 16384: URL モニタ • 32768: コンテンツ制約 • 65536: インテリジェント アプリケーション バイパス • 131072: WSA 脅威
文字列ブロック タイプ	uint32	アクセス コントロール ルール理由に関連付けられたわかりやすい名前を含む文字列データ ブロックを開始します。この値は常に 0 です。
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\(2-12 ページ\)](#)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+\(4-211 ページ\)](#)を参照)。アクセスコントロールポリシーメタデータブロックのブロックタイプは、シリーズ2のブロックタイプ 64 です。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ヘッダーバージョン(1)																メッセージタイプ(4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ(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。
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\(2-12 ページ\)](#)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+\(4-211 ページ\)](#)を参照)。アクセスコントロールポリシーメタデータブロックのブロックタイプは、シリーズ 2 のブロックタイプ 64 です。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ヘッダーバージョン(1)																メッセージタイプ(4)																							
	メッセージ長																																							
	Netmap ID																		レコードタイプ(146)																					

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

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

表 4-22 プレフィルタ ポリシー メタデータ フィールド

フィールド	データタイプ	説明
プレフィルタ ポリシーブロックタイプ	uint32	プレフィルタ ポリシーブロックを開始します。この値は常に 64 です。これはシリーズ 2 のデータブロックです。
プレフィルタ ポリシーブロック長	uint32	プレフィルタ ポリシーブロックタイプフィールドと長さフィールドの 8 バイトに、後続のデータのバイト数を加えたプレフィルタ ポリシーブロックの合計バイト数。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの UUID。このフィールドとセンサー ID を合わせると、このレコードの固有キーとなります。
センサー ID(Sensor ID)	uint32	アクセスコントロールポリシーに関連付けられたセンサー ID 番号。このフィールドとアクセスコントロールポリシー UUID を合わせると、このレコードの固有キーになります。
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\(2-12 ページ\)](#)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\(4-205 ページ\)](#)を参照)。アクセス コントロール ルール理由データブロックのブロック タイプは、シリーズ 2 のブロック タイプ 15 です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(147)															
	レコード長																															
	アクセス コントロール ルール ブロック タイプ(15)																															
	アクセス コントロール ルール ブロック 長																															
AC ポリシー UUID	アクセス コントロール ポリシー UUID																															
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ルール ID																															
	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	名前...																															

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

表 4-23 トンネルまたはプレフィルタ ルール理由メタデータ フィールド

フィールド	データタイプ	説明
アクセスコントロールルールブロックタイプ	uint32	アクセスコントロールルールブロックを開始します。この値は常に 15 です。ちなみに、このブロックは、アクセスコントロールルールだけでなく、トンネルルールとプレフィルタルールにも使用します。
アクセスコントロールルールブロック長	uint32	アクセスコントロールルールブロックタイプフィールドと長さフィールドの 8 バイトに、後続のデータバイト数を加えたアクセスコントロールルールブロックの合計バイト数。
アクセスコントロールルール UUID	uint8[16]	アクセスコントロールルールの UUID。このフィールドは、このレコードの固有キーです。このフィールドとアクセスコントロールルール ID を合わせると、このレコードの固有キーになります。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの ID 番号。このフィールドとアクセスコントロールルール UUID を合わせると、このレコードの固有キーとなります。
文字列ブロックタイプ	uint32	アクセスコントロールルール UUID とアクセスコントロールルール ID に関連付けられているわかりやすい名前のある文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの 8 バイトと名前フィールドのバイト数が含まれます。
[名前(Name)]	string	わかりやすい名前。

セキュリティインテリジェンスカテゴリメタデータ

eStreamer サービスは、次の形式のセキュリティインテリジェンスカテゴリレコードで、セキュリティインテリジェンスカテゴリに関する情報を格納したメタデータを送信します。セキュリティインテリジェンスカテゴリメタデータは、バージョン 4 メタデータフラグ(要求メッセージの要求フラグフィールドのビット 20)が設定されると送信されます。[要求フラグ\(2-12 ページ\)](#)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+\(4-209 ページ\)](#)を参照)。セキュリティインテリジェンスデータブロックのブロックタイプは、シリーズ 2 のブロックタイプ 22 です。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ヘッダーバージョン(1)																メッセージタイプ(4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ(280)																							
	レコード長																																							
	セキュリティ インテリジェンス カテゴリのブロック タイプ(22)																																							
	セキュリティ インテリジェンス カテゴリのブロック長																																							
	セキュリティ インテリジェンス リスト ID																																							
	アクセス コントロール ポリシー UUID																																							
	アクセス コントロール ポリシー UUID(続き)																																							
	アクセス コントロール ポリシー UUID(続き)																																							
	アクセス コントロール ポリシー UUID(続き)																																							
	文字列ブロック タイプ(0)																																							
	文字列ブロック長																																							
	セキュリティ インテリジェンス リスト名...																																							

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

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

フィールド	データタイプ	説明
セキュリティ インテリジェンス カテゴリ ブロック タイプ	uint32	セキュリティ インテリジェンス カテゴリのデータ ブロックを開始します。この値は常に 22 です。これはシリーズ 2 のデータ ブロックです。
セキュリティ インテリジェンス カテゴリのブロック長	uint32	セキュリティ インテリジェンス カテゴリ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えたセキュリティ インテリジェンス カテゴリ ブロックの合計バイト数。
セキュリティ インテリジェンス リスト ID	uint32	接続でトリガーがかかる IP ブラックリストまたはホワイトリストの ID。このフィールドとアクセス コントロール ポリシー UUID を合わせると、このレコードの固有キーになります。

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(続き)

フィールド	データタイプ	説明
アクセスコントロールポリシー UUID	uint8[16]	セキュリティインテリジェンスに設定されたアクセスコントロールポリシーの UUID。このフィールドとセキュリティインテリジェンスリスト ID を合わせると、このレコードの固有キーとなります。
文字列ブロックタイプ	uint32	セキュリティインテリジェンスリストに関連付けられたわかりやすい名前を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドとヘッダーフィールドの 8 バイトにセキュリティインテリジェンスリスト名フィールドのバイト数を加えた名前文字列データブロックのバイト数。
セキュリティインテリジェンスリスト名	string	接続でトリガーがかかる IP カテゴリ ブラックリストまたはホワイトリストの名前。

セキュリティインテリジェンス送信元/宛先レコード

eStreamer サービスは、次の形式のセキュリティインテリジェンス送信元/宛先レコードで、セキュリティインテリジェンスで検出した IP アドレスが、送信元 IP アドレスと宛先 IP アドレスのいずれであるかを示すメタデータを送信します。(送信元/宛先 IP 情報は、以下のメタデータフラグの 1 つ(要求メッセージの要求フラグフィールドのビット 1、14、15、または 20)が設定されると送信されます。[要求フラグ\(2-12 ページ\)](#)を参照してください)。ちなみに、メッセージ長フィールドの後のレコードタイプフィールドの値は、セキュリティインテリジェンス送信元/宛先レコードを示す 281 です。

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

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

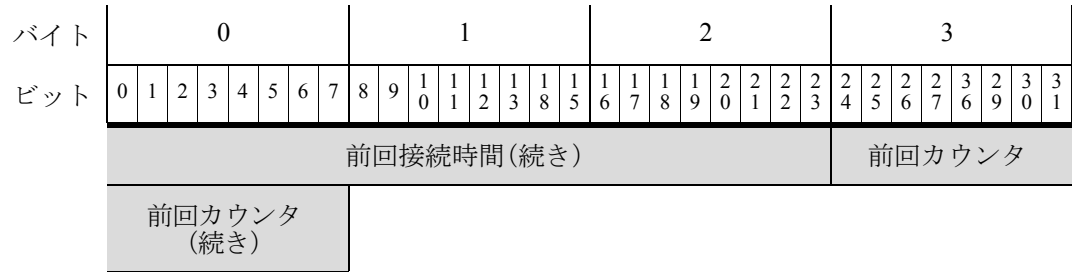
表 4-25 セキュリティ インテリジェンス送信元/宛先レコードのフィールド

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

5.3+ の IOC ステート データ ブロック

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

バイト	0								1								2								3											
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
IOC ステート ブロック タイプ (150)																																				
IOC ステート ブロック 長																																				
IOC ID 番号																																				
無効								最初の確認																												
最初の確認(続き)								最初のイベント ID																												
最初のイベント ID(続き)								最初の Device ID																												
最初の Device ID (続き)								最初のインスタンス ID																最初の接続時間												
最初の接続時間(続き)																最初のカウンタ																				
最初のカウンタ (続き)								最後の確認日時																												
最後の確認日時 (続き)								前回イベント ID																												
前回イベント ID (続き)								前回 Device ID																												
前回 Device ID(続き)								前回インスタンス ID																前回接続時間												



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

表 4-26 IOC ステート データ ブロックのフィールド

フィールド	データタイプ	説明
IOC ステート データ ブロック タイプ	uint32	IOC ステート データ ブロックを開始します。この値は常に 150 です。
IOC ステート データ ブロック の長さ	uint32	IOC ステート データ ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のデータ バイト数を加えた IOC ステート データ ブロックの合計バイト数。
IOC ID 番号	uint32	侵害の固有 ID 番号。
無効	uint8	侵害がホストで無効にされているかどうかを示します： <ul style="list-style-type: none"> 0: 侵害は無効ではありません。 1: 侵害が無効です。
最初の確認	uint32	この侵害の最初の検出時を示す UNIX タイムスタンプ。
最初のイベント ID	uint32	この侵害が最初に確認されたイベントの ID 番号。
最初の Device ID	uint32	最初に IOC を検出したセンサーの ID。
最初のインスタンス ID	uint16	最初に侵害を検出した管理対象デバイスの Snort インスタンスの数値 ID。
最初の接続時間	uint32	この侵害を最初に検出した接続の Unix タイムスタンプ。
最初のカウンタ	uint16	この侵害を最後の確認日時した接続のカウンタ。 これで、同時に発生する複数の接続を区別します。
最後の確認日時	uint32	この侵害の前の検出時を示す UNIX タイムスタンプ。
前回イベント ID	uint32	この侵害を最後の確認日時したイベントの ID 番号。
前回 DeviceID	uint32	前回 IOC を検出したセンサーの ID。
前回インスタンス ID	uint16	前回侵害を検出した管理対象デバイスの Snort インスタンスの数値 ID。
前回接続時間	uint32	この侵害を最後の確認日時した接続の Unix タイムスタンプ。
前回カウンタ	uint16	この侵害を最後の確認日時した接続のカウンタ。 これで、同時に発生する複数の接続を区別します。

5.3+ の IOC 名データ ブロック

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

次の図は、IOC 名データ ブロックの構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(161)															
	レコード長																															
	IOC 名ブロック タイプ(39)																															
	IOC 名ブロック長																															
	IOC ID 番号																															
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。

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
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。
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。 <ul style="list-style-type: none"> • CnC Connected • Exploit Kit • High Impact Attack • Low Impact Attack • Malware Detected • Malware Executed • Dropper Infection • Java Compromise • Word Compromise • Adobe Reader Compromise • Excel Compromise • PowerPoint Compromise • QuickTime Compromise
文字列ブロックタイプ	uint32	侵害に関連付けられたイベントタイプを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの 8 バイトとイベントタイプフィールドのバイト数が含まれます。

表 4-27 IOC 名データ ブロックのフィールド(続き)

フィールド	データタイプ	説明
イベントタイプ (Event Type)	string	<p>侵害のイベントタイプ。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • Adobe Reader launched shell • Dropper Infection Detected by 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、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\(4-45 ページ\)](#)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\(B-92 ページ\)](#)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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	ヘッダー バージョン(1)																メッセージ タイプ(4)																							
	メッセージ長																																							
	Netmap ID																レコード タイプ																							
	レコード長																																							
	eStreamer サーバ タイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																																							
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																																							
ディスカバリ イベント ヘッダー	Device ID																																							
	レガシー IP アドレス																																							
	MAC アドレス																																							
	MAC アドレス(続き)																IPv6 あり								将来の使用に備えて予約済み															
	イベント秒																																							
	イベント マイクロ秒																																							
	イベント タイプ(Event Type)																																							
	イベント サブタイプ																																							
	ファイル番号(内部使用専用)																																							
	ファイルの位置(内部使用専用)																																							

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IPv6 アドレス																															
	IPv6 アドレス(続き)																															
	IPv6 アドレス(続き)																															
	IPv6 アドレス(続き)																															

次の表は、ディスカバリ イベント ヘッダーについての説明です。

表 4-28 ディスカバリ イベント ヘッダーのフィールド

フィールド	データ型	説明
Device ID	uint32	ディスカバリ イベントを生成したデバイスの ID 番号。バージョン 3 および 4 のメタデータを要求すると、デバイスのメタデータを入手できます。詳細については、 管理対象 Device レコードのメタデータ (3-37 ページ) を参照してください。
レガシー IP アドレス	uint32	このフィールドは予約済みですが、設定されておりません。IPv4 アドレスは IPv6 アドレス フィールドに保存されます。詳細については、 IP アドレス (1-5 ページ) を参照してください。
MAC アドレス	uint86	イベントに関連するホストの MAC アドレス。
IPv6 あり	uint8	ホストに IPv6 アドレスがあることを示すフラグ。
将来の使用に備えて予約済み	uint8	将来の使用に備えて予約済み
イベント秒	uint32	システムがイベントを生成したときの UNIX タイムスタンプ(1970 年 1 月 1 日以降の秒数)。
イベント マイクロ秒	uint32	システムがイベントを生成したときのタイムスタンプの、マイクロ秒(100 万分の 1 秒)の増分。
イベント タイプ (Event Type)	uint32	イベント タイプ(新規イベントは 1000、変更イベントは、1001、ユーザ入力イベントは1002、フル ホスト プロファイルは1050)。使用可能なイベント タイプの一覧の詳細については、 イベント タイプ別ホスト ディスカバリ 構造 (4-45 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 (4-45 ページ) を参照してください。
ファイル番号	byte[4]	シリアル ファイル番号。このフィールドは、シスコ の内部使用のためのものであり、無視してかまいません。
ファイルの位置	byte[4]	シリアル ファイル内のイベントの位置。このフィールドは、シスコ の内部使用のためのものであり、無視してかまいません。
IPv6 アドレス	uint8[16]	IPv6 アドレス。このフィールドは、IPv6 フラグが設定されている場合に存在し、使用されます。

ディスカバリ イベントと接続イベントのタイプとサブタイプ

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

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

表 4-29 タイプ/サブタイプ別のディスカバリ イベントと接続イベント

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

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

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

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

イベント名	イベント タイプ (Event Type)	イベント サブタイプ
ユーザ追加ホスト	1002	27
ユーザ追加サーバ	1002	28
ユーザ追加クライアント アプリケーション	1002	29
ユーザ追加プロトコル	1002	30
アプリを再読み込み	1002	31
アカウント削除	1002	32
接続統計情報	1003	1
接続チャンク	1003	2
新規ユーザ アイデンティティ	1004	1
ユーザ ログイン	1004	2
ユーザ アイデンティティを削除	1004	3
ユーザ アイデンティティをドロップ。ユーザ上限に到達	1004	4
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\(4-45 ページ\)](#)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\(4-46 ページ\)](#)
- [サーバ メッセージ\(4-47 ページ\)](#)
- [新規ネットワーク プロトコル メッセージ\(4-48 ページ\)](#)
- [新規トランスポート プロトコル メッセージ\(4-48 ページ\)](#)
- [クライアント アプリケーション メッセージ\(4-48 ページ\)](#)
- [IP アドレス変更メッセージ\(4-49 ページ\)](#)
- [オペレーティング システム更新メッセージ\(4-50 ページ\)](#)
- [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\(4-50 ページ\)](#)
- [ホップ変更メッセージ\(4-51 ページ\)](#)
- [ホップ変更メッセージ\(4-51 ページ\)](#)

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

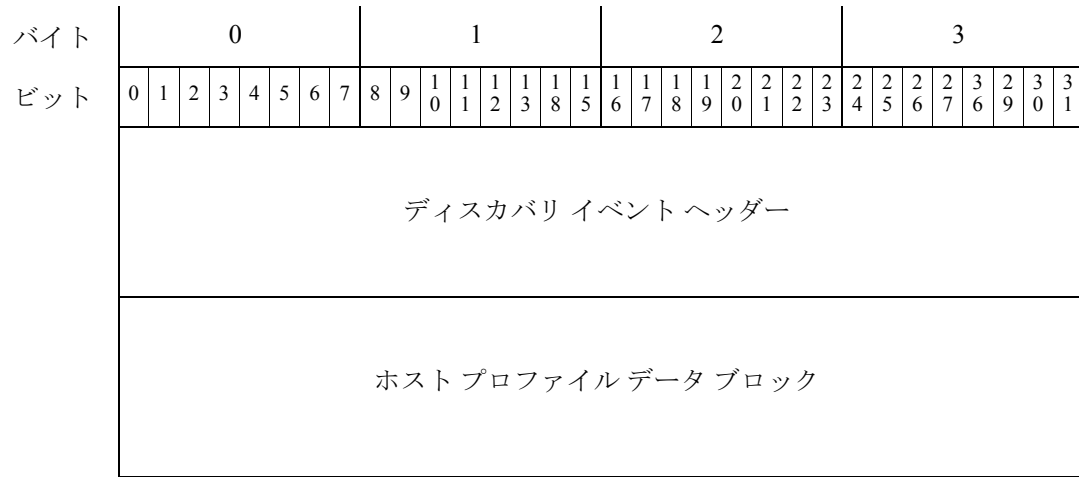
新規ホスト イベント メッセージと最後の確認日時ホスト イベント メッセージには、標準 ディスカバリ イベント ヘッダーとホスト プロファイル データ ブロックがあります([ホスト プロファイル データ ブロック 5.2+\(4-168 ページ\)](#)を参照)。ホスト プロファイル データ ブロックのブロック タイプは、シリーズ 1 のブロック タイプ 139 です。

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



(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\(B-285 ページ\)](#)を参照してください。



サーバメッセージ

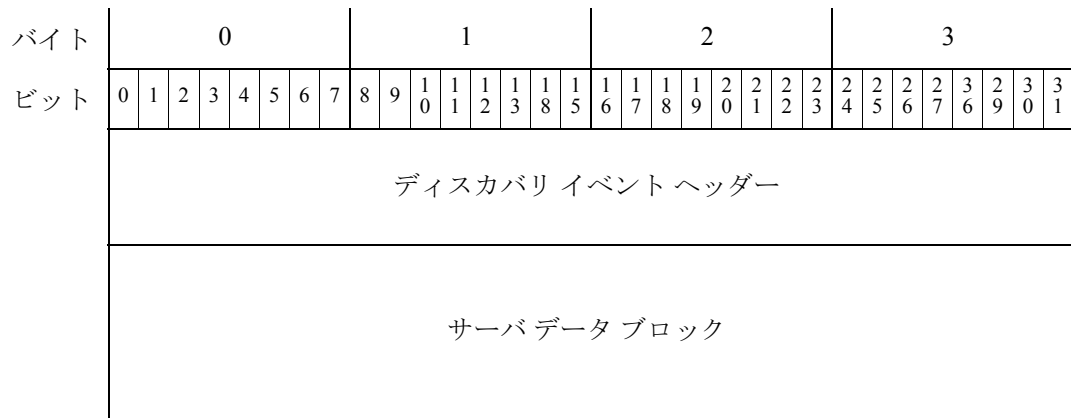
次の TCP サーバ イベント メッセージと UDP サーバ イベント メッセージには、標準ディスカバリ イベント ヘッダー (ディスカバリ イベント ヘッダー 5.2+(4-41 ページ) 参照) があり、サーバ データ ブロック (ホスト サーバ データ ブロック 4.10.0+(4-143 ページ) 参照、シリーズ 1 のブロック タイプ 103) がそれに続きます。

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



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

これらのイベントは、それぞれ次の形式を使用します:



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+(4-41 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。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
ディスカバリ イベント ヘッダー																																								
ネットワーク プロトコル																																								

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+(4-41 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。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
ディスカバリ イベント ヘッダー																																								
トランスポート プロトコル (Transport Protocol)																																								

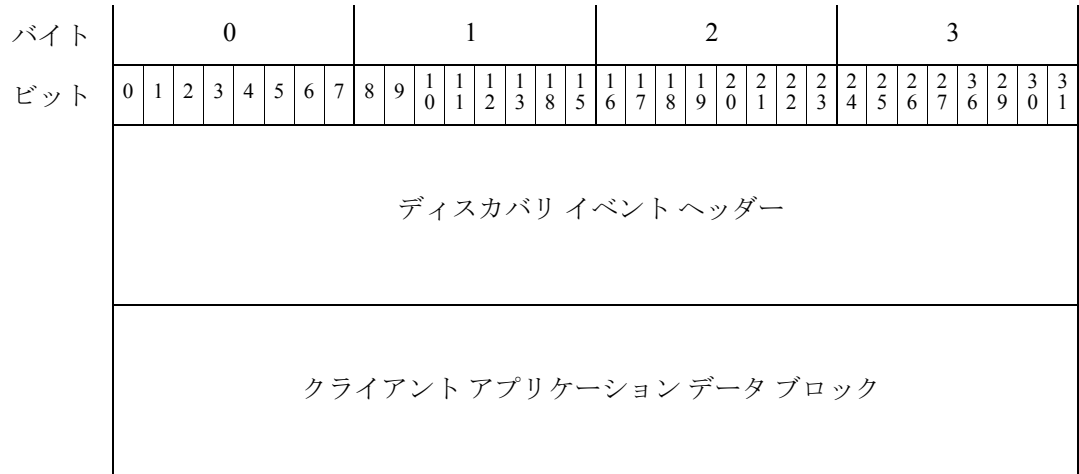
クライアント アプリケーション メッセージ

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+(4-41 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 (4-160 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。

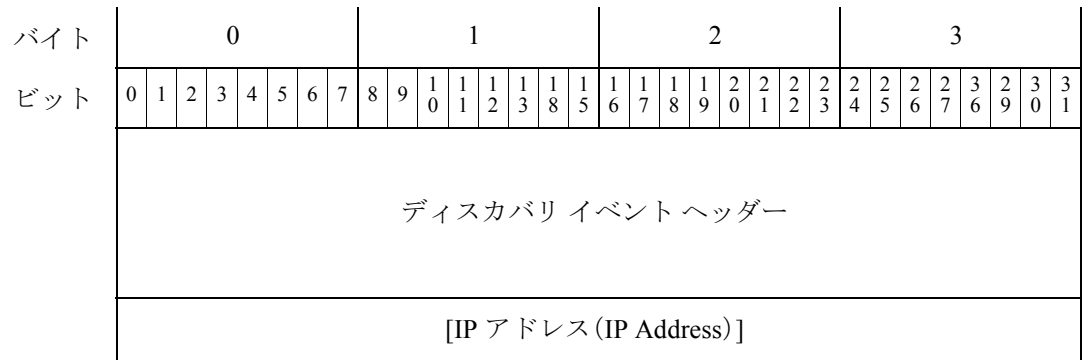


IP アドレス変更メッセージ

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+\(4-41 ページ\)](#))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

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
ディスクバリ イベント ヘッダー																																								
[IP アドレス (IP Address)]																																								
IP アドレス (続き)																																								
IP アドレス (続き)																																								
IP アドレス (続き)																																								

オペレーティング システム更新メッセージ

OS 情報更新イベントメッセージには、標準ディスクバリ イベント ヘッダー(ディスクバリ イベント ヘッダー 5.2+(4-41 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+(4-88 ページ))を参照。シリーズ 1 のブロック タイプ 53) がそれに続きます。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
ディスクバリ イベント ヘッダー																																								
オペレーティング システム データ ブロック																																								

IP アドレスを再利用とホスト タイムアウト/削除メッセージ

次のホスト イベント メッセージには、標準ディスクバリ イベント ヘッダー(ディスクバリ イベント ヘッダー 5.2+(4-41 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

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+(4-41 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 (4-52 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+(4-119 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。

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

ブリッジ/ルータとして識別したホスト メッセージ

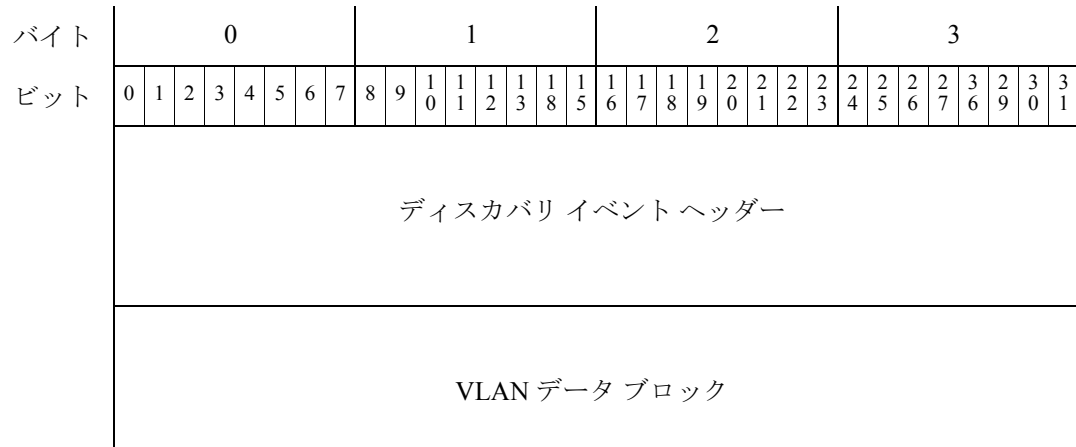
ブリッジ/ルータのイベントとして識別したホスト メッセージには、標準ディスカバリ イベント ヘッダー (ディスカバリ イベント ヘッダー 5.2+(4-41 ページ) を参照) があり、ホスト タイプと一致する値の 4 バイトフィールドが続きます。

- 0:ホスト
- 1:ルータ
- 2:ブリッジ

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

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+(4-41 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 (4-80 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。

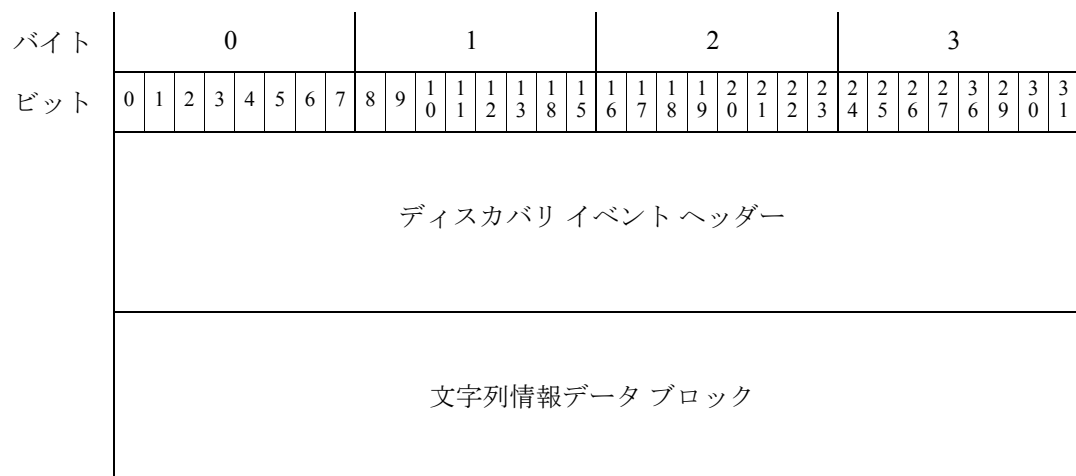


NetBIOS 名変更メッセージ

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+(4-41 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 (4-81 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、Firepower 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+\(4-41 ページ\)](#))を参照)があり、サーババナーのデータブロックがそれに続きます([サーババナー データブロック \(4-80 ページ\)](#)を参照)。サーババナーのデータブロックのブロックタイプは、シリーズ1のブロックタイプ37です。

バイト	0								1								2								3													
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
ディスカバリ イベント ヘッダー																																						
サーババナー データ ブロック																																						

ポリシー制御の概要

ポリシー制御ポリシー イベントには、標準ディスカバリ 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+\(4-41 ページ\)](#)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 \(4-89 ページ\)](#)を参照してください。

バイト	0								1								2								3													
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
ディスカバリ イベント ヘッダー																																						
ポリシー制御メッセージデータ ブロック																																						

接続統計データ メッセージ

接続統計イベントには、標準ディスカバリ 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+(4-41 ページ)を参照)、接続統計データ ブロックがそれに続きます。接続統計データ ブロックの各バージョンのドキュメントには、それを使用するシステム バージョンを格納します。バージョンの 6.1+ の接続統計データ ブロックの形式については、[接続統計データ ブロック 6.2+\(4-122 ページ\)](#)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\(B-1 ページ\)](#)。

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

接続チャンク メッセージ

接続チャンク イベントには、標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-41 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 \(4-103 ページ\)](#)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。

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

バージョン 4.6.1+ のユーザ設定脆弱性メッセージ

ユーザ設定の有効な脆弱性、ユーザ設定の無効な脆弱性、ユーザ脆弱性資格メッセージは、同じデータ形式を使用します。すなわち、標準ディスクバリ イベント ヘッダー(ディスクバリ イベント ヘッダー 5.2+(4-41 ページ)を参照)にユーザ脆弱性変更データ ブロックが続きます(ユーザ脆弱性変更データ ブロック 4.7+(4-110 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。

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

ユーザ追加/削除ホストメッセージ

次のホスト入力イベント メッセージには、標準ディスクバリ イベント ヘッダーがあり(ディスクバリ イベント ヘッダー 5.2+(4-41 ページ)を参照)、ユーザホスト データ ブロックがそれに続きます(ユーザホスト データ ブロック 4.7+(4-108 ページ)を参照。シリーズ 1 のブロック タイプ 78)。

- ユーザ削除アドレス
- ユーザ追加ホスト

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

ユーザ削除サーバメッセージ

ユーザ削除サーバメッセージには、標準ディスカバリ 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+(4-41 ページ)を参照)、ユーザサーバリストデータブロックがそれに続きます(ユーザサーバリストデータブロック(4-107 ページ)を参照)。ユーザサーバリストデータブロックはシリーズ1のブロックタイプ77です。

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

ユーザ設定ホスト重要度メッセージ

ユーザ設定ホスト重要度メッセージには、標準ディスカバリ イベント ヘッダーがあり(ディスカバリ イベント ヘッダー 5.2+(4-41 ページ)を参照)、ユーザ重要度変更データブロックがそれに続きます(ユーザ重要度変更データブロック 4.7+(4-111 ページ)を参照)。ユーザ重要度変更データブロックのブロックタイプは、シリーズ1ブロックタイプ81です。

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

属性メッセージ

次のイベントメッセージには、標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-41 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(4-90 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。

■ ディスカバリ イベントのメタデータ

- ホスト属性を追加
- ホスト属性を更新
- ホスト属性を削除

これらのイベントは、それぞれ次の形式を使用します:

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

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+(4-41 ページ)を参照)があり、ユーザ属性値データ ブロック(ユーザ属性値データ ブロック 4.7+(4-113 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:

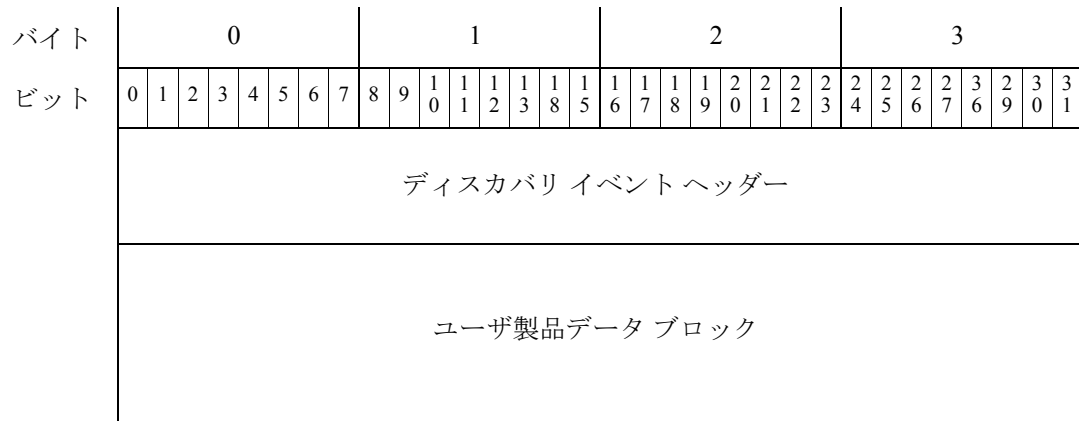
バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ディスカバリ イベント ヘッダー																																
ユーザ属性値データ ブロック																																

ユーザサーバメッセージとオペレーティングシステムメッセージ

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+(4-41 ページ)を参照)があり、ユーザ製品データブロック(ユーザ製品データブロック 5.1+(4-176 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
- サーバ定義を設定
- サーバの追加(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:

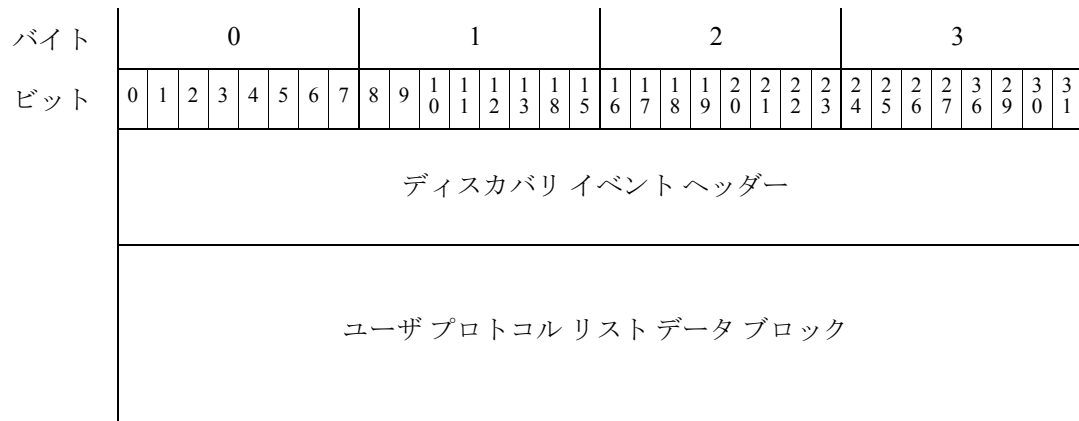


ユーザプロトコルメッセージ

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+(4-41 ページ)を参照)があり、ユーザプロトコルリストデータブロック(ユーザプロトコルリストデータブロック 4.7+(4-114 ページ)を参照。シリーズ1ブロックタイプ 83)がそれに続きます。

- プロトコルを削除
- プロトコルを追加

これらのイベントは、それぞれ次の形式を使用します:



ユーザクライアントアプリケーションメッセージ

次のイベントメッセージには、標準ディスカバリ イベントヘッダー(ディスカバリ イベントヘッダー 5.2+(4-41 ページ)を参照)があり、ユーザクライアントアプリケーションリストデータブロック(ユーザクライアントアプリケーションリストデータブロック (4-96 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:

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
ディスカバリ イベントヘッダー																																								
ユーザクライアントアプリケーションリストデータブロック																																								

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+(4-41 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+(4-140 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。

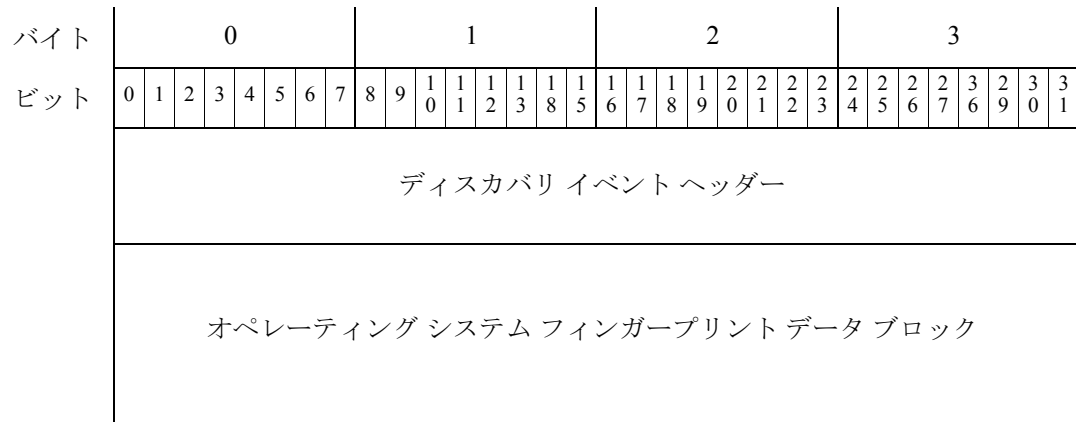
このイベントでは、次の形式を使用します。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
ディスカバリ イベントヘッダー																																								
スキャン結果データブロック																																								

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+(4-41 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+(4-165 ページ)を参照)。

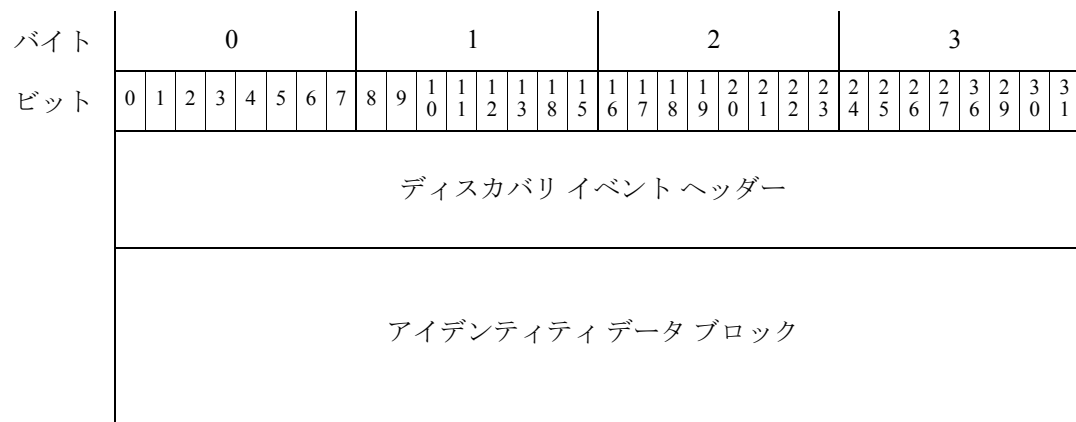
このイベントでは、次の形式を使用します。



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+(4-41 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 (4-117 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。

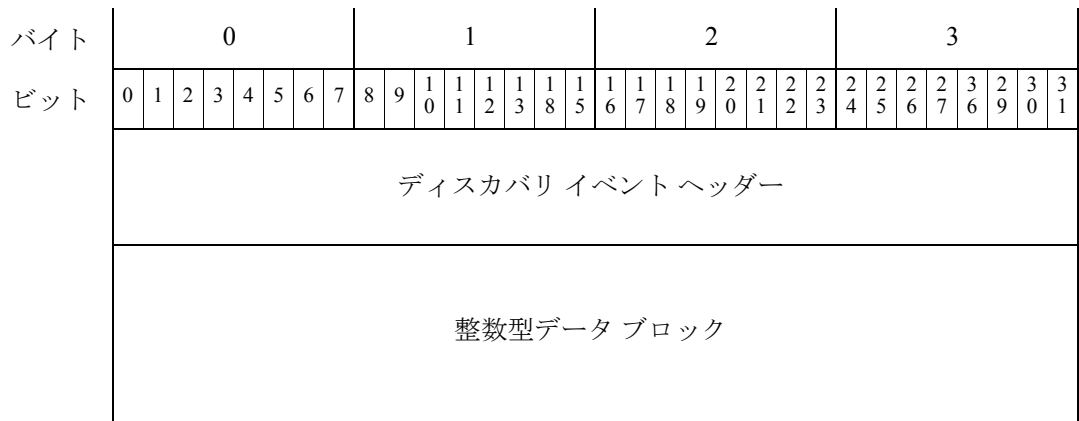
このイベントでは、次の形式を使用します。



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、標準ディスクバリ イベント ヘッダー(ディスクバリ イベント ヘッダー 5.2+(4-41 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 (4-79 ページ)を参照)。この整数型データ ブロックには、ホストの IOC セットの ID 番号を格納します。

このイベントでは、次の形式を使用します。



イベント タイプ別のユーザ データ 構造

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

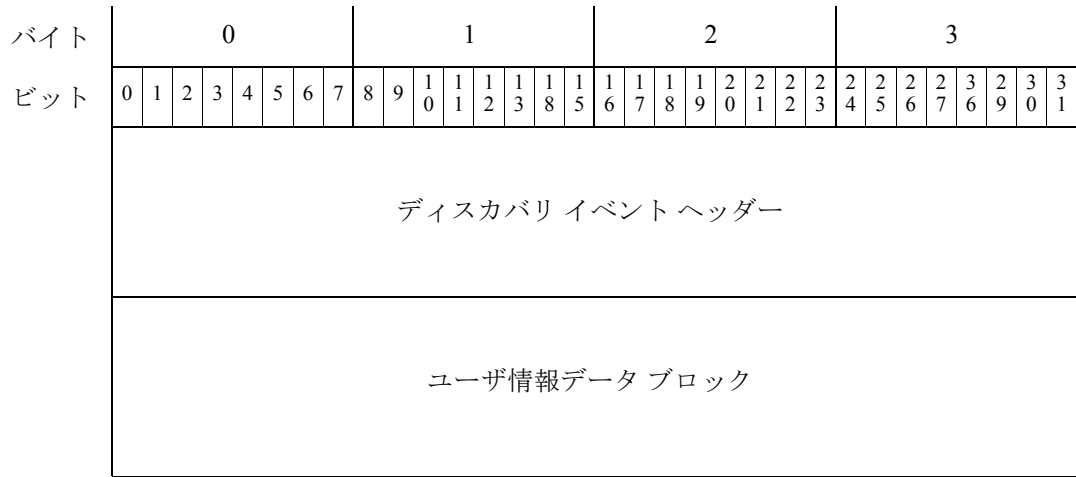
- ユーザ変更メッセージ(4-62 ページ)
- ユーザ情報更新メッセージブロック(4-63 ページ)

ユーザ変更メッセージ

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

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

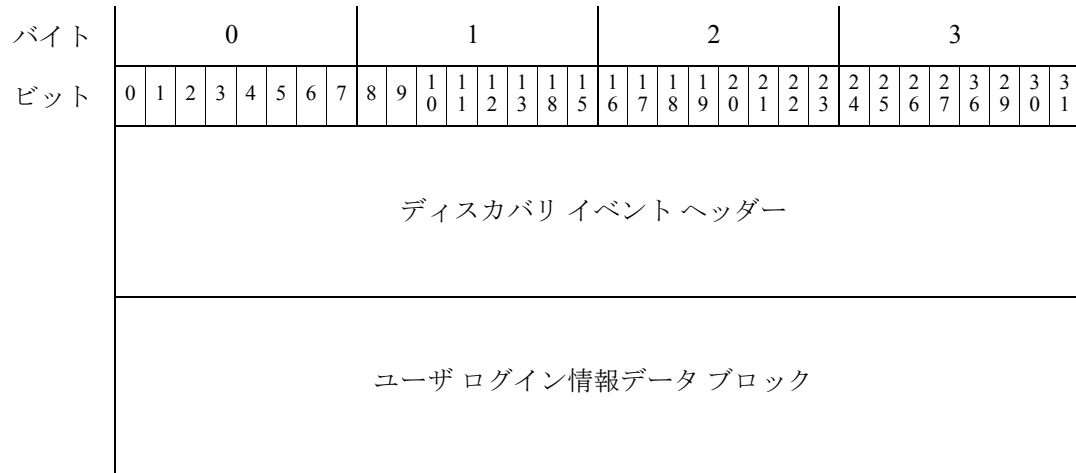
ユーザ変更イベント メッセージには、標準ディスクバリ イベント ヘッダー(ディスクバリ イベント ヘッダー 5.2+(4-41 ページ)を参照)があり、ユーザ情報データ ブロックがそれに続きます(6.0+ の情報データ ユーザ ブロック (4-194 ページ)を参照)。ユーザ情報データ ブロックはシリーズ 1 ブロック タイプ 120 です。



ユーザ情報更新メッセージブロック

システムがユーザのログインの変更(ユーザログインイベント — イベントタイプ 1004、サブタイプ 2)を検出すると、ユーザ情報更新メッセージが送信されます。

ユーザ情報更新イベントメッセージには標準ディスカバリ イベント ヘッダー(ディスカバリ イベント ヘッダー 5.2+(4-41 ページ)を参照)とユーザ ログイン情報データ ブロックがあります(ユーザ ログイン情報データ ブロック 6.2+(4-200 ページ)を参照)。ユーザ ログイン情報データ ブロックのブロック タイプは、シリーズ1 ブロック タイプ 121 です。



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 (2-27 ページ)を参照してください。

シリーズ1データブロックヘッダーシリーズ

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

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



(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 \(4-73 ページ\)](#)
- [BLOB データブロック \(4-74 ページ\)](#)
- [リストデータブロック \(4-75 ページ\)](#)
- [汎用リストブロック \(4-76 ページ\)](#)

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 \(4-65 ページ\)](#)を参照してください。ユーザイベントブロックタイプについては、[表 4-85 \(4-184 ページ\)](#)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 (4-73 ページ) を参照してください。
1	サブサーバ	現在 (Current)	サーバで検出したサブサーバに関する情報を格納します。詳細については、 サブサーバデータブロック (4-76 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 (4-78 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 (4-79 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 (4-74 ページ) を参照してください。
11	リスト	現在 (Current)	その他のデータブロックリストを含みます。詳細については、 リストデータブロック (4-75 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 (4-80 ページ) を参照してください。
20	侵入の影響アラート	現在 (Current)	侵入影響アラート情報を格納します。侵入影響イベントアラートのヘッダーは、他のデータブロックは若干異なります。詳細については、 侵入の影響アラートデータ 5.3 以上 (3-18 ページ) を参照してください。
31	汎用リスト	現在 (Current)	たとえば、クライアントアプリケーションブロックなど、カプセル化する汎用リスト情報をブロックリストをホストプロファイルブロックに格納します。詳細については、 汎用リストブロック (4-76 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せん。 文字列情報データブロック (4-81 ページ) を参照してください。
37	サーババナー	現在 (Current)	サーババナーデータを格納します。詳細については、 サーババナーデータブロック (4-80 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。

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
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 (4-83 ページ) を参照してください。
42	ホストクライアントアプリケーション	レガシー	新規クライアントアプリケーションイベントのクライアントアプリケーション情報を格納します(本製品の旧バージョンを参照のこと)。
47	フルホストプロファイル	レガシー	ホストプロファイル情報一式を格納します(本製品の旧バージョンを参照のこと)。
48	属性値 (Attribute Value)	現在 (Current)	ホスト属性の ID 番号と値を格納します。詳細については、 属性値データブロック (4-84 ページ) を参照してください。
51	フルサブサーバ	現在 (Current)	サーバで検出したサブサーバに関する情報を格納します。フルサーバ情報ブロックとフルホストプロファイルで参照します。各サブサーバの脆弱性情報を格納します。詳細については、 フルサブサーバデータブロック (4-86 ページ) を参照してください。
53	オペレーティングシステム (Operating System)	現在 (Current)	バージョン 3.5+ のオペレーティングシステム情報を格納します。詳細については、 オペレーティングシステムデータブロック 3.5+ (4-88 ページ) を参照してください。
54	ポリシーエンジン制御メッセージ	現在 (Current)	ユーザポリシー制御の変更に関する情報を格納します。詳細については、 ポリシーエンジン制御メッセージデータブロック (4-89 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 (4-90 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	ユーザプロトコル	現在 (Current)	ユーザ入力のプロトコル情報を格納します。詳細については、 ユーザプロトコルデータブロック (4-93 ページ) を参照してください。
59	ユーザクライアントアプリケーション	レガシー	ユーザ入力 of クライアントアプリケーションデータを格納します。詳細については、 ユーザクライアントアプリケーションデータブロック 5.0 ~ 5.1 (B-95 ページ) を参照してください。ブロック 138 に置き換わります。
60	ユーザクライアントアプリケーションリスト	現在 (Current)	ユーザクライアントアプリケーションデータブロックのリストを格納します。詳細については、 ユーザクライアントアプリケーションリストデータブロック (4-96 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
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-327 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 (4-99 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 (4-101 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 (4-102 ページ) を参照してください。
65	ユーザ製品	レガシー	サードパーティ アプリケーション文字列マッピングなど、サードパーティ アプリケーションからインポートしたホスト入力データを格納します。詳細については、 ユーザ製品データブロック 5.0.x (B-99 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-151 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 (4-105 ページ) を参照してください。
71	汎用スキャン結果	レガシー	Nmap スキャンの結果を格納します(本製品の旧バージョンを参照のこと)。
72	スキャン結果	レガシー	サードパーティ スキャンの結果を格納します(本製品の旧バージョンを参照のこと)。
76	ユーザ サーバ	現在 (Current)	ユーザ入力イベントのサーバ情報を格納します。詳細については、 ユーザ サーバデータブロック (4-106 ページ) を参照してください。
77	ユーザ サーバリスト	現在 (Current)	ユーザ サーバブロックのリストを格納します。詳細については、 ユーザ サーバリストデータブロック (4-107 ページ) を参照してください。
78	ユーザ ホスト	現在 (Current)	ユーザ ホスト入力イベントからのホスト範囲に関する情報を格納します。詳細については、 ユーザ ホストデータブロック 4.7+(4-108 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
79	ユーザ脆弱性	レガシー	ホスト脆弱性に関する情報を格納します(本製品の旧バージョンを参照のこと)。バージョン 5.0 で導入したサクセサブロックのブロックタイプは 124 です。
80	ユーザ ホスト脆弱性の変更	現在(Current)	非アクティブ化した脆弱性のリスト、またはアクティブ化した脆弱性のリストを格納します。詳細については、 ユーザ脆弱性変更データブロック 4.7+(4-110 ページ) を参照してください。
81	ユーザ重要度	現在(Current)	ホストまたはホストの重要度の変更に関する情報を格納します。詳細については、 ユーザ重要度変更データブロック 4.7+(4-111 ページ) を参照してください。
82	ユーザ属性値	現在(Current)	ホストの属性値の変更を格納します。詳細については、 ユーザ属性値データブロック 4.7+(4-113 ページ) を参照してください。
83	ユーザプロトコルリスト	現在(Current)	ホストのプロトコルリストを示します。詳細については、 ユーザプロトコルリストデータブロック 4.7+(4-114 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+(4-116 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-131 ページ) を参照してください。バージョン 5.1 で導入したサクセサブロックのブロックタイプは 130 です。
88	サーバ情報	レガシー	サーバフィンガープリントで使用するサーバ情報を格納します(本製品の旧バージョンを参照のこと)。
89	ホスト/サーバ	レガシー	ホストサーバ情報を格納します(本製品の旧バージョンを参照のこと)。
90	フルホストサーバ	レガシー	ホストサーバ情報を格納します(本製品の旧バージョンを参照のこと)。
91	ホストプロファイル	レガシー	ホストのプロファイル情報を格納します。詳細については、 ホストプロファイルデータブロック 5.2+(4-168 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 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。

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
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 (4-117 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+ (4-119 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 (4-120 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。
97	Web アプリケーション (Web Application)	レガシー	Web アプリケーションデータのリストを格納します(本製品の旧バージョンを参照のこと)。バージョン 5.0 で導入したサクセサブロックのブロックタイプは 123 です。
98	ホスト/サーバ	レガシー	ホストサーバ情報を格納します(本製品の旧バージョンを参照のこと)。
99	フルホストサーバ	レガシー	ホストサーバ情報を格納します(本製品の旧バージョンを参照のこと)。
100	ホストクライアントアプリケーション	レガシー	新規クライアントアプリケーションイベントのクライアントアプリケーション情報を格納します(本製品の旧バージョンを参照のこと)。バージョン 5.0 で導入したサクセサブロックタイプ 122 には、ブロックタイプ 100 と同じ構造があります。
101	接続統計情報	レガシー	4.9.1+ の接続統計イベントの情報を格納します(本製品の旧バージョンを参照のこと)。
102	スキャン結果	レガシー	脆弱性に関する情報を格納しており、スキャン結果を追加イベントで使用します。 スキャン結果データブロック 5.0 ~ 5.1.1.x (B-97 ページ) を参照してください。
103	ホスト/サーバ	現在 (Current)	ホストサーバ情報を格納します。詳細については、 ホストサーバデータブロック 4.10.0+ (4-143 ページ) を参照してください。
104	フルホストサーバ	現在 (Current)	ホストサーバ情報を格納します。詳細については、 フルホストサーバデータブロック 4.10.0+ (4-145 ページ) を参照してください。
105	サーバ情報	レガシー	サーバフィンガープリントで使用するサーバ情報を格納します。詳細については、 4.10.x、5.0 ~ 5.0.2 のサーバ情報データブロック (4-149 ページ) を参照してください。5.0 で導入したサクセサブロックタイプ 117 には、ブロックタイプ 105 と同じ構成があります。
106	フルサーバ情報	現在 (Current)	ホストで検出したサーバに関する情報を格納します。詳細については、 フルサーバ情報データブロック (4-151 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
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 (4-153 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 (4-155 ページ) を参照してください。
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-286 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+(4-158 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-133 ページ) を参照してください。バージョン 5.1 で導入したサクセサブロックのブロックタイプは 126 です。
117	サーバ情報	現在 (Current)	サーバフィンガープリントで使用するサーバ情報を格納します。詳細については、 4.10.x、5.0 ~ 5.0.2 のサーバ情報データブロック (4-149 ページ) を参照してください。
118	ユーザ製品	レガシー	サードパーティ アプリケーション文字列マッピングなど、サードパーティ アプリケーションからインポートしたホスト入力データを格納します。詳細については、 ユーザ製品データブロック 5.0.x (B-99 ページ) を参照してください。先行ブロックタイプ 65 は 5.0 で更新され、このブロックタイプと同じ構造があります。バージョン 5.1 で導入したサクセサブロックのブロックタイプは 132 です。
119	接続チャック	レガシー	バージョン 4.10.1 ~ 5.1 の接続チャック情報を格納します。詳細については、 接続チャックデータブロック 5.0 ~ 5.1 (B-151 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 (4-160 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。

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
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 (4-121 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。
124	ユーザ脆弱性	現在 (Current)	ホスト脆弱性に関する情報を格納します。 ユーザ脆弱性データブロック 5.0+(4-162 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-138 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+(4-165 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+ Device のモバイル情報データブロック (4-166 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-307 ページ) を参照してください。これはブロック タイプ 91 に置き換わります。ブロック 139 に置き換わります。
134	ユーザ製品	現在 (Current)	サードパーティアプリケーション文字列マッピングなど、サードパーティアプリケーションからインポートしたホスト入力データを格納します。詳細については、 ユーザ製品データブロック 5.1+(4-176 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-296 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。

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
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 (4-103 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。
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-151 ページ) を参照してください。これはブロック タイプ 126 に置き換わります。これはブロック タイプ 144 に置き換わります。
138	ユーザ クライアント アプリケーション	現在 (Current)	ユーザ入力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 クライアント アプリケーション データ ブロック (4-95 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+ (4-168 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 (4-98 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+ (4-140 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 (4-100 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-144 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+ (4-82 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。

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
140	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-160 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-167 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-175 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-189 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-203 ページ) を参照してください。これはブロックタイプ 157 に置き換わります。
163	接続統計情報	現在 (Current)	6.0+ の接続イベントの情報を格納します。詳細については、 接続統計データブロック 6.2+ (4-122 ページ) を参照してください。これはブロックタイプ 160 に置き換わります。

文字列データブロック

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

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

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



(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。

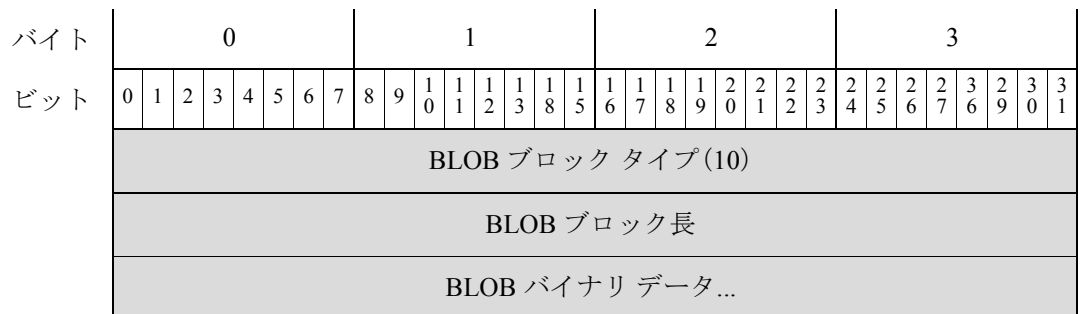
表 4-31 文字列データ ブロックのフィールド

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バナーを BLOB データ ブロックで保存できます。BLOB データ ブロックのブロックタイプは、シリーズ 1 ブロック グループのブロックタイプ 10 です。

次の図に、BLOB データ ブロックの形式を示します。



次の表に、BLOB データ ブロックのフィールドの説明を示します。

表 4-32 BLOB データ ブロック フィールド

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

リスト データ ブロック

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

次の図に、リスト データ ブロックの基本的な形式を示します。



次の表では、リスト データ ブロックのフィールドについて説明します。

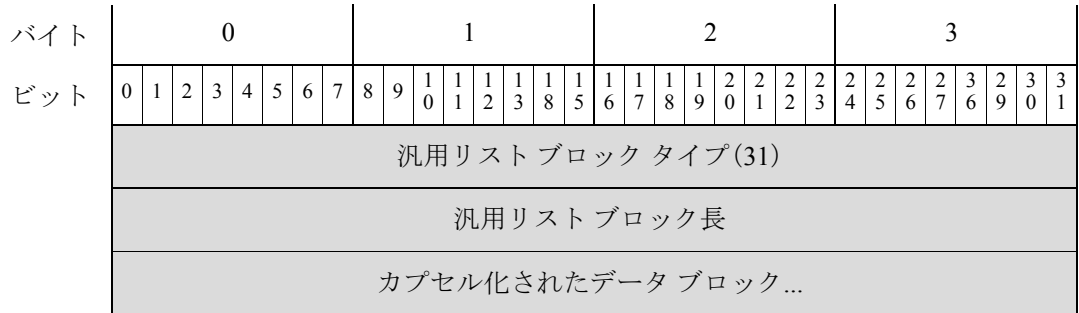
表 4-33 リスト データ ブロックのフィールド

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

汎用リストブロック

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

次の図に、汎用リストのデータブロックの基本的な構造を示します。



次の表では、汎用リストデータブロックのフィールドについて説明します。

表 4-34 汎用リストデータブロックのフィールド

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

サブサーバデータブロック

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

次の図は、サブサーバデータブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	サブサーバブロック タイプ(1)																															
	サブサーバブロック長																															
サブサーバ [名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	サブサーバ名...																															
ベンダー [名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ベンダー名...																															
バージョン バージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	バージョン...																															

次の表では、サブサーバデータブロックのフィールドについて説明します。

表 4-35 サブサーバデータブロックのフィールド

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

表 4-35 サブサーバデータブロックのフィールド(続き)

フィールド	データタイプ	説明
ベンダー名 (Vendor Name)	string	サブサーバベンダー名。
文字列ブロックタイプ	uint32	サブサーババージョンを格納した文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	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)

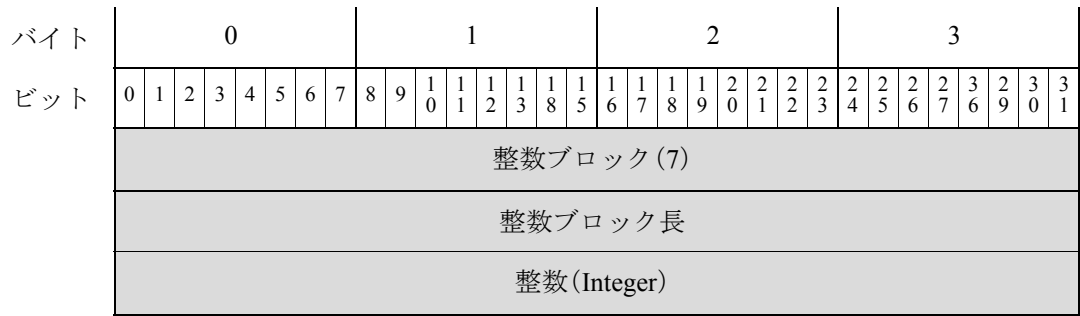
フィールド	データタイプ	説明
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 <ul style="list-style-type: none"> • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 <ul style="list-style-type: none"> • 2048:IP

整数型 (INT32) データ ブロック

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

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

次の図は、整数型データブロックの形式です。



次の表では、整数型データブロックのフィールドについて説明します。

表 4-37 整数型データブロックのフィールド

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

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。

バイト	0								1								2								3													
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
VLAN ブロック タイプ (14)																																						
VLAN ブロック 長																																						
VLAN ID (Admin. VLAN ID)																		VLAN タイプ									VLAN 優先順位											

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 タグにカプセル化されたパケットのタイプ。 <ul style="list-style-type: none"> 0: イーサネット 1: トークンリング
VLAN 優先順位	uint8	VLAN タグに含まれる優先順位値。

サーババナー データ ブロック

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

バイト	0								1								2								3														
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	
	サーババナー ブロック タイプ (37)																																						
	サーババナー ブロック長																																						
	[ポート (Port)]																		プロトコル									BLOB ブロック タイプ									サーババナー (BLOB)		
	BLOB ブロック タイプ (10) (続き)																		BLOB 長																				
	BLOB 長 (続き)																		サーババナー データ...																				
	サーババナー データ (続き).....																																						

次の表では、サーババナー データ ブロックのフィールドについて説明します。

表 4-39 サーババナー データ ブロックのフィールド

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

文字列情報データ ブロック

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

次の図は、文字列情報データ ブロックの形式です。

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

次の表では、文字列情報データ ブロックのフィールドについて説明します。

表 4-40 文字列情報データ ブロックのフィールド

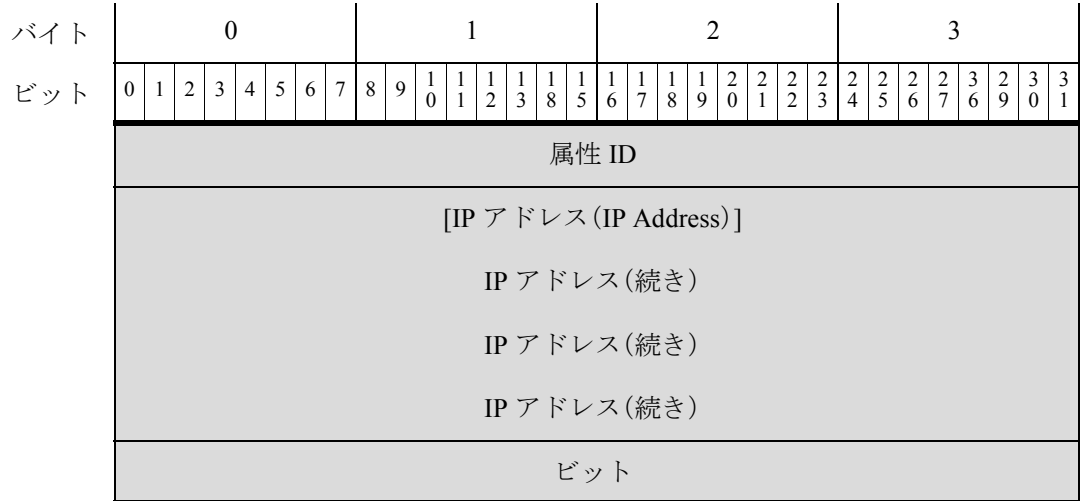
フィールド	データタイプ	説明
文字列情報ブロックタイプ	uint32	文字列情報データ ブロックを開始します。この値は常に 35 です。
文字列情報ブロック長	uint32	文字列情報データ ブロック ヘッダーと文字列情報データを組み合わせた長さ。
文字列ブロックタイプ	uint32	値を含む文字列データ ブロックを開始します。
文字列ブロック長	uint32	文字列ブロック タイプと長さの 8 バイトに、値のバイト数を加えた値の文字列データ ブロックのバイト数。
値	string	文字列情報データ ブロックを使用した脆弱性のデータ ブロックの Common Vulnerabilities and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

属性アドレス データ ブロック 5.2+

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

次の図は、属性アドレス ブロックの基本構造を示しています。

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



次の表は、属性アドレス データ ブロックのフィールドについての説明です。

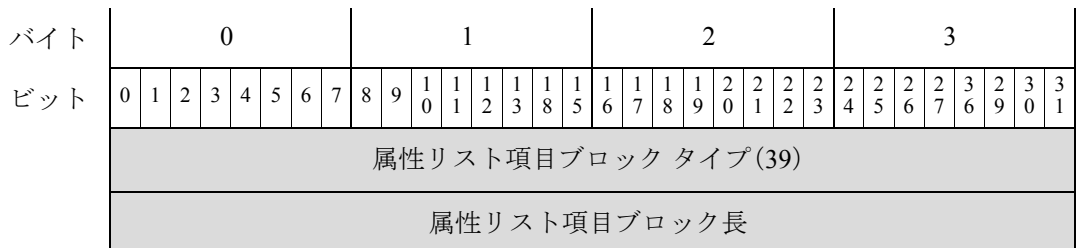
表 4-41 属性アドレス データ ブロック 5.2+ のフィールド

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

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。



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

次の表では、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 4-42 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	属性値ブロックタイプ(48)																															
	属性値ブロック長																															

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

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 4-43 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。 <ul style="list-style-type: none"> 0: 値としてのテキストによる属性。文字列データを使用します 1: 範囲の値による属性。整数型データを使用します 2: 使用可能値のリストによる属性。整数型データを使用します 3: 値としての URL による属性。文字列データを使用します 4: 値としてのバイナリ BLOB による属性。文字列データを使用します
属性整数値	uint32	属性に整数値 (該当する場合)。
文字列ブロックタイプ	uint32	属性名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロック タイプ フィールドと長さフィールドに属性名のバイト数を加えた文字列データ ブロックのバイト数。
属性値 (Attribute Value)	string	属性値。

フルサブサーバデータブロック

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



(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を示します。

次の図は、フルサブサーバデータブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	フルサブサーバブロックタイプ(51)																															
	フルサブサーバブロック長																															
	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	サブサーバ名文字列...																															
	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	サブサーバベンダー名文字列...																															
	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	サブサーババージョン文字列...																															
	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	(VDB)ホスト脆弱性データブロック																															
	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	(サードパーティ スキャン)ホスト脆弱性データブロック*																															

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

表 4-44 フルサブサーバデータブロックのフィールド

フィールド	データタイプ	説明
フルサブサーバブロックタイプ	uint32	フルサブサーバブロックを開始します。この値は常に 51 です。
フルサブサーバブロック長	uint32	フルサブサーバブロックタイプフィールドと長さフィールドの 8 バイトに、後続のフルサブサーバブロックのバイト数を加えたフルサブサーバデータブロックの合計バイト数。
文字列ブロックタイプ	uint32	サブサーバ名を格納した文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにサブサーバ名のバイト数を加えたサブサーバ名文字列データブロックのバイト数。
サブサーバ名	string	サブサーバ名。
文字列ブロックタイプ	uint32	サブサーバベンダー名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにサブサーバ名のバイト数を加えたベンダー名文字列データブロックのバイト数。
サブサーバベンダー名	string	サブサーバベンダーの名前。
文字列ブロックタイプ	uint32	サブサーババージョンを格納した文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにサブサーババージョンのバイト数を加えたサブサーババージョン文字列データブロックのバイト数。
サブサーババージョン	string	サブサーバ長
汎用リストブロックタイプ	uint32	VDB 脆弱性データを伝えるホスト脆弱性データブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべてのホスト脆弱性データブロックを含む汎用リストデータブロックのバイト数。
VDB ホスト脆弱性ブロック*	変数 (variable)	シスコで確認されたホスト脆弱性に関する情報を格納したホスト脆弱性データブロック。このデータブロックの説明の詳細については、 ホスト脆弱性データブロック 4.9.0+(4-116 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。

表 4-44 フルサブサーバデータブロックのフィールド(続き)

フィールド	データタイプ	説明
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+(4-116 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	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 4-45 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。

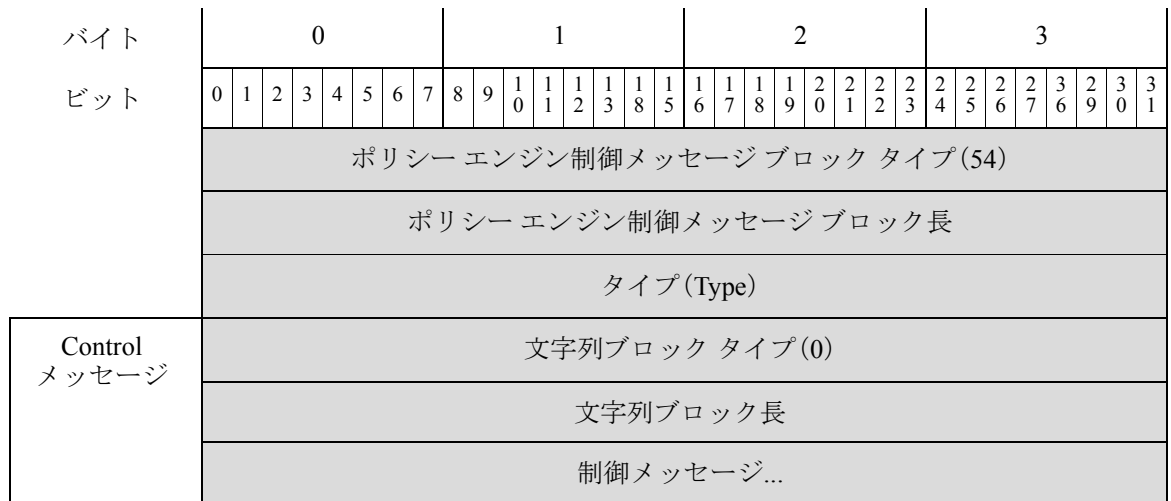
表 4-45 オペレーティングシステムのデータブロック 3.5+ のフィールド(続き)

フィールド	データタイプ	説明
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 4-46 ポリシーエンジン制御メッセージデータブロックのフィールド

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

表 4-46 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(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	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\(4-57 ページ\)](#)を参照してください。

次の図は、属性定義データブロックの基本構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	属性定義ブロックタイプ(55)																															
	属性定義ブロック長																															
	ソース																															
	UUID																															
	UUID(続き)																															
	UUID(続き)																															
	UUID(続き)																															
	ID																															
[名前(Name)]	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	名前...																															
	属性タイプ																															

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
	属性カテゴリ																																
	整数型範囲の開始値																																
	整数型範囲の終了値																																
	自動割り当て IP アドレス フラグ																																
	属性リスト項目ブロック タイプ (39)																																属性一覧 項目をリスト
	属性リスト項目ブロック長																																
項目をリスト	リストブロック タイプ (11)																																
	リストブロック長																																
	属性リスト項目...																																
	属性アドレスブロック タイプ (38)																																属性一覧 アドレス
	属性アドレスブロック長																																
アドレス一覧	リストブロック タイプ (11)																																
	リストブロック長																																
	属性アドレス リスト...																																

次の表では、属性定義データ ブロックのフィールドについて説明します。

表 4-47 属性定義データ ブロックのフィールド

フィールド	データタイプ	説明
属性定義ブロックタイプ	uint32	属性定義データ ブロックを開始します。この値は常に 55 です。
属性定義ブロック長	uint32	属性定義データ ブロック タイプと長さの 8 バイトに、後続の属性定義データのバイト数を加えた属性定義データ ブロックのバイト数。
ソース	uint32	属性データの送信元にマッピングする ID 番号。送信元タイプによって、これは無応答 (RNA)、ユーザ、スキャナ、またはサードパーティ 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。

表 4-47 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
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。 <ul style="list-style-type: none"> 0: 値としてのテキストによる属性。文字列データを使用します 1: 範囲の値による属性。整数型データを使用します 2: 使用可能値のリストによる属性。整数型データを使用します 3: 値としてのURLによる属性。文字列データを使用します 4: 値としてのバイナリ BLOB による属性。文字列データを使用します
属性カテゴリ	uint32	属性カテゴリ
範囲の開始値	uint32	定義した属性の整数範囲内の最初の整数。
範囲の終了値	uint32	定義した属性の整数範囲の最後の整数。
自動割り当て IP アドレス フラグ	uint32	属性に基づいて IP アドレスが自動的に割り当てられるかどうかを示すフラグ。
リストブロックタイプ	uint32	属性リスト項目を伝える属性リスト項目データブロックリストで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの8バイトに、カプセル化されたすべての属性リスト項目データブロックを加えた値です。 このフィールドの後にはゼロか、さらに属性リスト項目のデータブロックが続きます。
属性リスト項目ブロックタイプ	uint32	最初の属性リスト項目データブロックを開始します。このデータブロックには、他の属性リスト項目データブロックを、リストブロック長フィールドで定義した上限まで続けることができます。
属性リスト項目ブロック長	uint32	ブロックタイプフィールドとヘッダーフィールドの8バイトに属性リスト項目のバイト数を加えた属性リスト項目文字列データブロックのバイト数。
属性リスト項目	変数 (variable)	属性リスト項目データブロック (4-83 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。

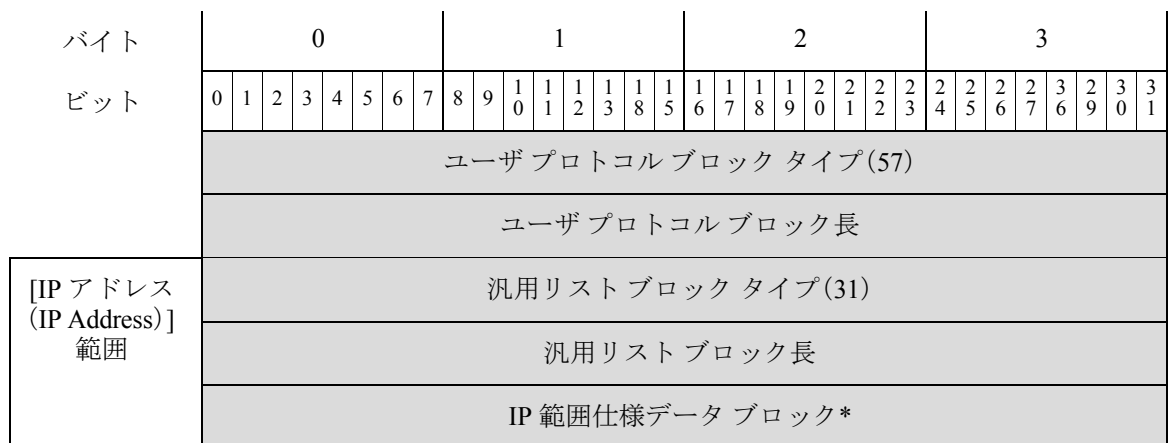
表 4-47 属性定義データブロックのフィールド(続き)

フィールド	データタイプ	説明
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+(4-82 ページ)に記載されている属性アドレスデータ。

ユーザプロトコルデータブロック

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

次の図は、ユーザプロトコルデータブロックの基本構造です。



バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MAC アドレス 範囲	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	MAC 範囲指定データ ブロック...																															
	プロトコルタイプ (Protocol Type)								プロトコル																							

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

表 4-48 ユーザプロトコルデータブロックのフィールド

フィールド	バイト数	説明
ユーザプロトコルブロックタイプ	uint32	ユーザプロトコルデータブロックを開始します。この値は常に 57 です。
ユーザプロトコルブロック長	uint32	ユーザプロトコルブロックタイプフィールドと長さフィールドの 8 バイトに、後続のユーザプロトコルデータのバイト数を加えたユーザプロトコルデータブロックの合計バイト数。
汎用リストブロックタイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データブロック* で構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべての IP 範囲仕様データブロック* を含む汎用リストデータブロックのバイト数。
IP 範囲仕様データブロック*	変数 (variable)	ユーザ入力の 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 (4-98 ページ) を参照してください。
汎用リストブロックタイプ	uint32	MAC アドレス範囲データを伝える MAC 範囲指定データブロックで構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべての MAC 範囲指定データブロックを含む汎用リストデータブロックのバイト数。
MAC 範囲指定データブロック*	変数 (variable)	ユーザ入力の MAC アドレス範囲に関する情報を含む MAC 範囲指定データブロック。このデータブロックの説明の詳細については、 MAC アドレス指定データブロック (4-101 ページ) を参照してください。
プロトコルタイプ (Protocol Type)	uint8	プロトコルのタイプを示します。プロトコルには、IP などネットワーク層プロトコルの 0、または TCP や UDP などトランスポート層プロトコルの 1 があります。
プロトコル	uint16	データブロックに格納されるデータのプロトコルを示します。

5.1.1+ のユーザクライアントアプリケーションデータブロック

ユーザクライアントアプリケーションデータブロックには、クライアントアプリケーションデータの送信元に関する情報、データを追加したユーザの ID 番号、および IP アドレス範囲データブロックのリストが含まれます。バージョン 6.2.3 に追加されたペイロード ID は、レコードに関連付けられたアプリケーションインスタンスを指定します。ユーザクライアントアプリケーションデータブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ 138 です。ブロックタイプ 59 を置換します。

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザクライアントアプリケーションブロックタイプ(138)																															
	ユーザクライアントアプリケーションブロック長																															
IP Range 仕様	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	IP 範囲仕様データブロック*																															
	アプリケーションプロトコル ID																															
	クライアントアプリケーション ID																															
バージョン	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	バージョン...																															
	ペイロードタイプ(Payload Type)																															
	Web アプリケーション ID																															

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

表 4-49 ユーザクライアントアプリケーションデータブロックのフィールド

フィールド	バイト数	説明
ユーザクライアントアプリケーションブロックタイプ	uint32	ユーザクライアントアプリケーションデータブロックを開始します。この値は常に 138 です。
ユーザクライアントアプリケーションブロック長	uint32	ユーザクライアントアプリケーションデータブロックのバイトの合計数(ユーザクライアントアプリケーションブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザクライアントアプリケーションデータのバイト数を含む)。
汎用リストブロックタイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データブロック* で構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべての IP 範囲仕様データブロック* を含む汎用リストデータブロックのバイト数。
IP 範囲仕様データブロック*	変数 (variable)	ユーザ入力 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 (4-98 ページ) を参照してください。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
文字列ブロックタイプ	uint32	クライアントアプリケーションバージョンを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーションバージョン文字列データブロックのバイト数(文字列ブロックタイプと長さのフィールド、およびバージョンのバイト数を含む)。
バージョン	string	クライアントアプリケーションバージョン。
ペイロードタイプ (Payload Type)	uint32	このフィールドは下位互換性のために用意したものです。常に 0 です。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。

ユーザクライアントアプリケーションリストデータブロック

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザクライアントアプリケーションブロック タイプ(60)																															
	ユーザ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 4-50 ユーザクライアントアプリケーションリストデータブロックのフィールド

フィールド	バイト数	説明
ユーザクライアントアプリケーションリストブロックタイプ	uint32	ユーザクライアントアプリケーションリストデータブロックを開始します。この値は常に 60 です。
ユーザクライアントアプリケーションリストブロック長	uint32	ユーザクライアントアプリケーションリストブロックタイプフィールドと長さフィールドの 8 バイトに、後続のユーザクライアントリストアプリケーションデータのバイト数を加えたユーザクライアントアプリケーションリストデータブロックの合計バイト数。
ソースタイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> 無応答 (RNA) がクライアントデータを検出した場合、0 ユーザがクライアントデータを提供した場合、1 サードパーティ スキャナがクライアントデータを検出した場合、2 nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでクライアントデータを提供した場合、3
ソース	uint32	影響を受けるクライアントアプリケーションを追加した送信元にマッピングする ID 番号。送信元タイプによって、これは無応答 (RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
汎用リストブロックタイプ	uint32	汎用リストデータブロックを開始します。この値は常に 31 です。

表 4-50 ユーザクライアント アプリケーション リスト データ ブロックのフィールド(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。
ユーザクライアントアプリケーションブロック	変数(variable)	リストブロック長の最大バイト数を上限としてカプセル化したユーザクライアントアプリケーションデータブロック。ユーザクライアントアプリケーションデータブロックの詳細については、 5.1.1+のユーザクライアントアプリケーションデータブロック(4-95ページ) を参照してください。

5.2+ の IP アドレス範囲データ ブロック

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

次の図は、IP アドレス範囲データ ブロックの形式です。



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。

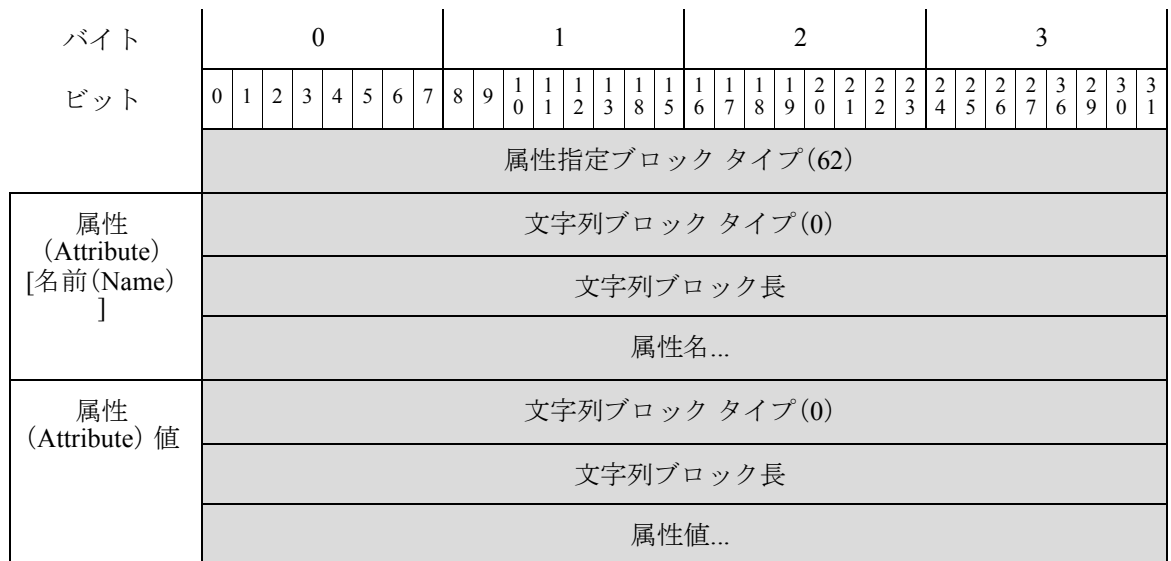
表 4-51 IP アドレス範囲データ ブロックのフィールド

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 4-52 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。

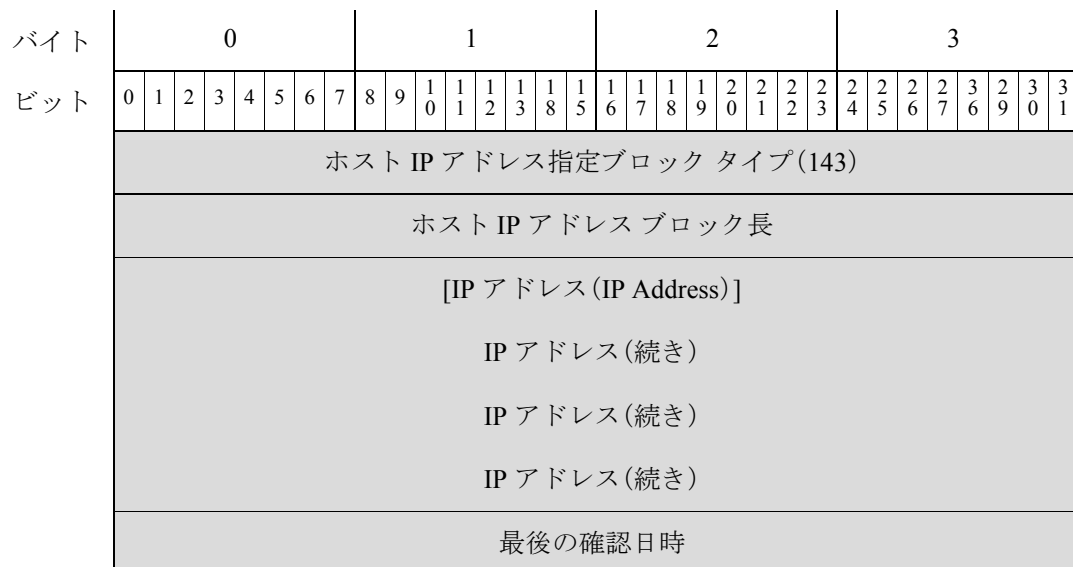
表 4-52 属性指定データブロックのフィールド(続き)

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

次の図は、ホスト IP アドレス データ ブロックの形式です。



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 4-53 ホスト IP アドレス データ ブロックのフィールド

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

MAC アドレス指定データブロック

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

次の図は、MAC アドレス指定データブロックの形式です。



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 4-54 MAC アドレス指定データブロックのフィールド

フィールド	データタイプ	説明
MAC アドレス指定ブロックタイプ	uint32	MAC アドレス指定データブロックを開始します。この値は常に 63 です。
MAC アドレス指定ブロック長	uint32	MAC アドレス指定ブロックタイプフィールドと長さフィールドの 8 バイトに、後続の MAC アドレス指定データのバイト数を加えた MAC アドレス指定データブロックの合計バイト数。
MAC アドレス ブロック サイズ 1 ~ 6	uint8	順に並んだ MAC アドレス ブロック。

アドレス指定データブロック

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

次の図は、アドレス指定データブロックの基本構造です。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	アドレス指定データブロックタイプ(64)																																							
	アドレス指定ブロック長																																							
[IP アドレス (IP Address)] 範囲 ブロック	汎用リストブロックタイプ(31)																																							
	汎用リストブロック長																																							
	IP アドレス範囲指定ブロック...																																							
MAC アドレス (Address) ブロック	汎用リストブロックタイプ(31)																																							
	汎用リストブロック長																																							
	MAC アドレス指定データブロック...																																							

次の表では、アドレス指定データブロックのフィールドについて説明します。

表 4-55 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。

表 4-55 アドレス指定データブロックのフィールド(続き)

フィールド	バイト数	説明
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 (4-98 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 (4-101 ページ) を参照してください。

6.1+ の接続チャンク データブロック

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

次の図は、接続チャンク データブロックの形式を示しています。



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

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

表 4-56 接続チャンク データ ブロックのフィールド

フィールド	データタイプ	説明
接続チャンク ブロックタイプ	uint32	接続チャンク データ ブロックを開始します。この値は常に 164 です。
接続チャンク ブロック長	uint32	接続チャンク データ ブロックのバイト数(接続チャンク ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く接続チャンク データのバイト数を含む)。
イニシエータ IP アドレス	uint8(4)	この接続タイプのイニシエータの IP アドレス。このアドレスは、オリジナルクライアントとレスポンドの IP アドレスに使用して、同一の接続を識別します。
レスポンド IP アドレス	uint8(4)	この接続タイプのレスポンドの IP アドレス。このアドレスは、イニシエータとオリジナルクライアントの IP アドレスに使用して、同一の接続を識別します。
オリジナルクライアント IP アドレス	uint8(4)	要求の送信元であるプロキシの背後にあるホストの IP アドレス。これは、イニシエータとレスポンドの IP アドレスで使用して同一の接続を確認します。
開始時刻	uint32	接続チャンクの開始時刻。
アプリケーションプロトコル	uint32	接続で使用されたプロトコルの ID 番号。
レスポンドポート	uint16	接続チャンクでレスポンドが使用したポート。
プロトコル	uint8	ユーザ情報を含むパケットのプロトコル。
接続タイプ	uint8	接続の種類。
NetFlow ディテクタ IP アドレス	uint8[4]	IP アドレス オクテットの、接続を検出した NetFlow デバイスの IP アドレス。
送信パケット数	uint64	接続チャンクで送信されたパケット数。

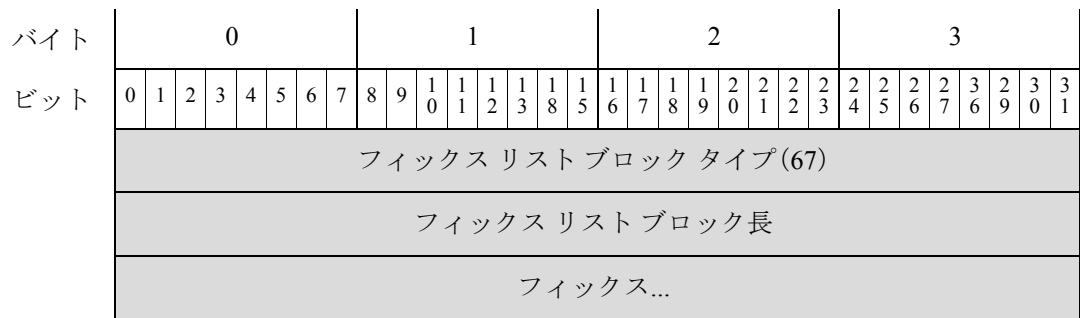
表 4-56 接続チャンク データブロックのフィールド(続き)

フィールド	データタイプ	説明
受信パケット数	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 4-57 フィックス リスト データ ブロックのフィールド

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

ユーザサーバデータブロック

ユーザサーバデータブロックには、ユーザ入力サーバの詳細を格納します。ユーザサーバデータブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ76です。次の図は、ユーザサーバデータブロックの基本構造です。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	ユーザサーバデータブロックタイプ(76)																																							
	ユーザサーバブロック長																																							
IP Range 仕様	汎用リストブロックタイプ(31)																																							
	汎用リストブロック長																																							
	IPアドレス範囲の固有ブロック*																																							
	[ポート (Port)]																プロトコル																							

次の表では、ユーザサーバデータブロックのフィールドについて説明します。

表 4-58 ユーザサーバデータブロックのフィールド

フィールド	バイト数	説明
ユーザサーバデータブロックタイプ	uint32	ユーザサーバデータブロックを開始します。この値は常に 76 です。
ユーザサーバブロック長	uint32	ユーザサーバブロックタイプフィールドと長さフィールドの 8 バイトに、後続のユーザサーバデータのバイト数を加えたユーザサーバデータブロックの合計バイト数。
汎用リストブロックタイプ	uint32	汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストブロックとカプセル化されたデータブロックのバイト数。この値は、汎用リストブロックヘッダーフィールドの 8 バイトに、カプセル化されたすべてのデータブロックのバイト数を加えた値です。
IPアドレス範囲指定データブロック	変数 (variable)	リストブロック長の最大バイト数を上限としてカプセル化した IP アドレス範囲指定データブロック。
[ポート (Port)]	uint16	サーバで使用するポート。

表 4-58 ユーザサーバ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
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 <ul style="list-style-type: none"> • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 <ul style="list-style-type: none"> • 2048:IP

ユーザサーバリストデータブロック

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



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

表 4-59 ユーザサーバリストデータブロックのフィールド

フィールド	バイト数	説明
ユーザサーバリストデータブロックタイプ	uint32	ユーザサーバリストデータブロックを開始します。この値は常に 77 です。
ユーザサーバリストブロック長	uint32	ユーザサーバリストブロックタイプフィールドと長さフィールドの 8 バイトに、後続のユーザサーバリストデータのバイト数を加えたユーザサーバリストデータブロックの合計バイト数。

表 4-59 ユーザサーバリスト データブロックのフィールド(続き)

フィールド	バイト数	説明
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> • 無応答(RNA)がサーバ データを検出した場合、0 • ユーザがサーバ データを提供した場合、1 • サードパーティ スキャナがサーバ データを検出した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでサーバ データを提供した場合、3
ソース	uint32	サーバ データの送信元にマッピングするID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
汎用リストブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リストブロック 長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リストブロック ヘッダーフィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
ユーザ サーバ データ ブロック	変数 (variable)	リスト ブロック長の最大バイト数を上限としてカプセル化したユーザ サーバ データ ブロック。

ユーザ ホスト データ ブロック 4.7+

ユーザ ホスト データ ブロックは、[ユーザ追加/削除ホスト メッセージ\(4-56 ページ\)](#)で使用し、ホスト範囲、ユーザ ホスト入力イベントから得られるユーザ アイデンティティとソース アイデンティティに関する情報を格納します。ユーザ ホスト データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 78 です。

次の図は、ユーザ ホスト データ ブロックの基本構造です。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	ユーザ ホストブロック タイプ (78)																																							
	ユーザ ホストブロック 長																																							
IP 範囲	汎用リストブロック タイプ (31)																																							
	汎用リストブロック 長																																							
	IP 範囲仕様データ ブロック*																																							

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

次の表では、ユーザ 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 4-60 ユーザ ホスト データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ ホスト ブロック タイプ	uint32	ユーザ ホスト データ ブロックを開始します。この値は常に 78 です。
ユーザ ホスト ブロック長	uint32	ユーザ ホスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のユーザ ホスト データのバイト数を加えたユー ザ ホスト データ ブロックの合計バイト数。
汎用リストブ ロック タイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で 構成された汎用リスト データ ブロックを開始します。この値は常 に 31 です。
汎用リストブ ロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リスト データ ブロックのバイト数。
IP 範囲仕様 データ ブ ロック*	変数 (variable)	ユーザ入力の IP アドレス範囲に関する情報を含む IP 範囲仕様 データ ブロック。このデータ ブロックの説明の詳細については、 5.2+ の IP アドレス範囲データ ブロック (4-98 ページ) を参照して ください。
汎用リストブ ロック タイプ	uint32	MAC アドレス範囲データを伝える MAC 範囲指定データ ブロッ クで構成された汎用リスト データ ブロックを開始します。この値 は常に 31 です。
汎用リストブ ロック長	uint32	リスト ヘッダーとカプセル化されたすべての MAC 範囲指定デー タ ブロックを含む汎用リスト データ ブロックのバイト数。
MAC 範囲指 定データ ブ ロック*	変数 (variable)	ユーザ入力の MAC アドレス範囲に関する情報を含む MAC 範囲 指定データ ブロック。このデータ ブロックの説明の詳細について は、 MAC アドレス指定データ ブロック (4-101 ページ) を参照して ください。

表 4-60 ユーザ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、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> 無応答 (RNA) がホスト データを検出した場合、0 ユーザがホスト データを提供した場合、1 サードパーティ スキャナがホスト データを検出した場合、2 nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでホスト データを提供した場合、3

ユーザ脆弱性変更データ ブロック 4.7+

ユーザ脆弱性変更データ ブロックには、非アクティブ化したホスト脆弱性、脆弱性を非アクティブ化したユーザ、脆弱性変更を提供した送信元に関する情報、重要度値を格納します。ユーザ脆弱性変更データ ブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ 80 です。前のユーザ脆弱性変更データ ブロックからの変更では、新規ソース タイプフィールドが加えられ、リスト データ ブロックの代わりに、汎用リスト データ ブロックで脆弱性非アクティブ化を保存するようになりました。このデータ ブロックは、ユーザ脆弱性変更メッセージで使用します(バージョン 4.6.1+ のユーザ設定脆弱性メッセージ(4-56 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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ脆弱性変更データ ブロック タイプ (80)																															
	ユーザ脆弱性変更ブロック長																															
	ソース																															
	ソース タイプ																															
Vuln Ack ブロック	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	ユーザ脆弱性データ ブロック...*																															

次の表では、汎用リスト データ ブロックのフィールドについて説明します。

表 4-61 ユーザ脆弱性変更データ ブロックのフィールド

フィールド	バイト数	説明
ユーザ脆弱性変更データ ブロック タイプ	uint32	ユーザ脆弱性変更データ ブロックを開始します。この値は常に 80 です。
ユーザ脆弱性変更データ ブロック長	uint32	ホスト脆弱性ブロック タイプ フィールドと長さフィールドの 8 バイトに、後続のホスト脆弱性データのバイト数を加えたユーザ脆弱性変更データ ブロックの合計バイト数。
ソース	uint32	ホスト脆弱性変更値を更新または追加した送信元にマッピングされる ID 番号。送信元タイプによって、これは無応答 (RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
ソース タイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> 無応答 (RNA) がホスト脆弱性データを検出した場合、0 ユーザがホスト脆弱性データを提供した場合、1 サードパーティ スキャナがホスト脆弱性データを検出した場合、2 nmimport.pl やホスト入力 API クライアントなどのコマンド ライン ツールでホスト脆弱性データを提供した場合、3
タイプ (Type)	uint32	脆弱性のタイプ。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リストブロック ヘッダーフィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
ユーザ脆弱性データ ブロック	変数 (variable)	リストブロック長の最大バイト数を上限としてカプセル化したユーザ脆弱性データ ブロック。詳細については、 ユーザ脆弱性データ ブロック 5.0+(4-162 ページ) を参照してください。

ユーザ重要度変更データ ブロック 4.7+

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

[ユーザ設定ホスト重要度メッセージ\(4-57 ページ\)](#)にあるように、ユーザ設定ホスト重要度メッセージでは、ユーザ重要度データ ブロックを使用します。

次の図は、ユーザ重要度データ ブロックの基本構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ重要度データブロック タイプ (81)																															
	ユーザ重要度ブロック長																															
[IP アドレス (IP Address)] 範囲ブロック	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	IP アドレス範囲指定ブロック...																															
	ソース																															
	ソース タイプ																															
	重要度値...																															

次の表では、ユーザ重要度データブロックのフィールドについて説明します。

表 4-62 ユーザ重要度データブロックのフィールド

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

表 4-62 ユーザ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: <ul style="list-style-type: none"> • 無応答(RNA)がユーザ重要度値を提供した場合、0 • ユーザがユーザ重要度値を提供した場合、1 • サードパーティ スキャナがユーザ重要度値を提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでユーザ重要度値を提供した場合、3
重要度値	uint32	ユーザの重要度値。

ユーザ属性値データ ブロック 4.7+

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

次の図は、ユーザ属性値データ ブロックの構造です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ属性値データ ブロック タイプ (82)																															
	ユーザ属性値ブロック長																															
[IP アドレス (IP Address) 範囲ブロック]	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	IP アドレス範囲指定ブロック...																															
	ソース																															
	ソース タイプ																															
	属性 ID																															
値	BLOB ブロック タイプ (10)																															
	BLOB ブロック長																															
	値...																															

次の表では、ユーザ属性値データブロックのフィールドについて説明します。

表 4-63 ユーザ属性値データブロックのフィールド

フィールド	バイト数	説明
ユーザ属性値データブロックタイプ	uint32	ユーザ属性値データブロックを開始します。この値は常に 82 です。
ユーザ属性値ブロック長	uint32	ユーザ属性値ブロックタイプフィールドと長さフィールドの 8 バイトに、後続のユーザ属性ブロックデータのバイト数を加えた属性値データブロックの合計バイト数。
汎用リストブロックタイプ	uint32	汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストブロックとカプセル化されたデータブロックのバイト数。この値は、汎用リストブロックヘッダーフィールドの 8 バイトに、カプセル化されたすべてのデータブロックのバイト数を加えた値です。
IP アドレス範囲指定データブロック	変数 (variable)	リストブロック長の最大バイト数を上限とした IP アドレス範囲指定データブロック(それぞれ開始 IP アドレスと終了 IP アドレスを含む)。
ソース	uint32	属性データを追加または更新した送信元にマッピングする ID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティアプリケーションにマッピングされます。
ソースタイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> • 無応答(RNA)がユーザ属性を提供した場合、0 • ユーザが属性値を提供した場合、1 • サードパーティスキャナがユーザ属性値を提供した場合、2 • nmimport.pl やホスト入力 API クライアントなどのコマンドラインツールでユーザ属性値を提供した場合、3
属性 ID	uint32	更新した属性の ID 番号(該当する場合)。
BLOB ブロックタイプ	uint32	BLOB データブロックを開始します。この値は常に 10 です。
BLOB ブロック長	uint32	BLOB データブロックのバイト数です。BLOB ブロックタイプとブロック長フィールドの 8 バイトと後続のバイナリデータの長さが含まれます。
値	変数 (variable)	バイナリ形式でユーザ属性値を格納します。

ユーザプロトコルリストデータブロック 4.7+

ユーザプロトコルリストデータブロックには、プロトコルデータの送信元に関する情報、データを追加したユーザの ID 番号、プロトコルデータブロックのリストを格納します。ユーザプロトコルリストデータブロックのブロックタイプは、シリーズ 1 ブロックグループのブロックタイプ 83 です。ユーザプロトコルデータブロックの詳細については、[ユーザプロトコルデータブロック \(4-93 ページ\)](#)を参照してください。

ユーザプロトコルメッセージ(4-59 ページ)にあるように、ユーザプロトコルメッセージでは、ユーザプロトコルリストデータブロックを使用します。

次の図は、ユーザプロトコルリストデータブロックの基本構造です。

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

次の表では、汎用リストデータブロックのフィールドについて説明します。

表 4-64 ユーザプロトコルリストデータブロックのフィールド

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

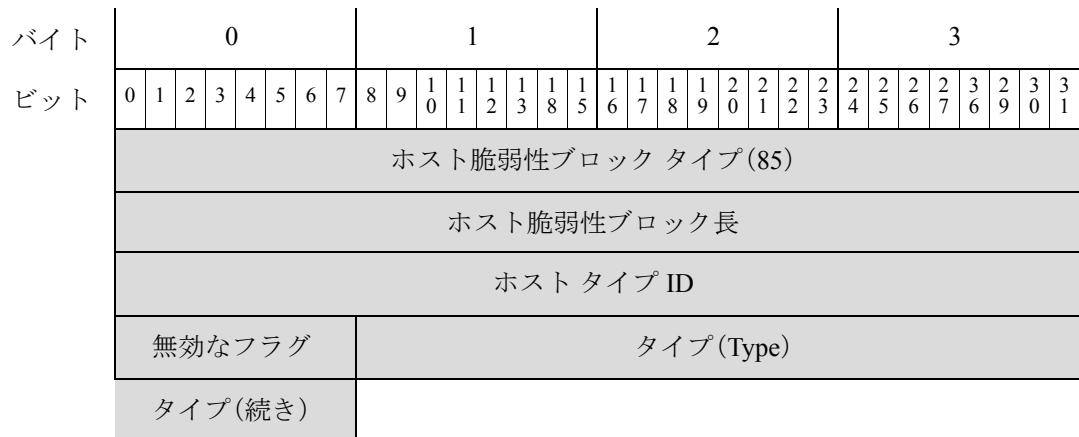
表 4-64 ユーザプロトコル リスト データ ブロックのフィールド(続き)

フィールド	バイト数	説明
汎用リスト ブロック 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 プロトコル データ ブロック	変数 (variable)	リスト ブロック長の最大バイト数を上限としてカプセル化されたユーザ プロトコル データ ブロック。

ホスト脆弱性データ ブロック 4.9.0+

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

次の図は、ホスト脆弱性データ ブロックの形式です。



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

表 4-65 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。

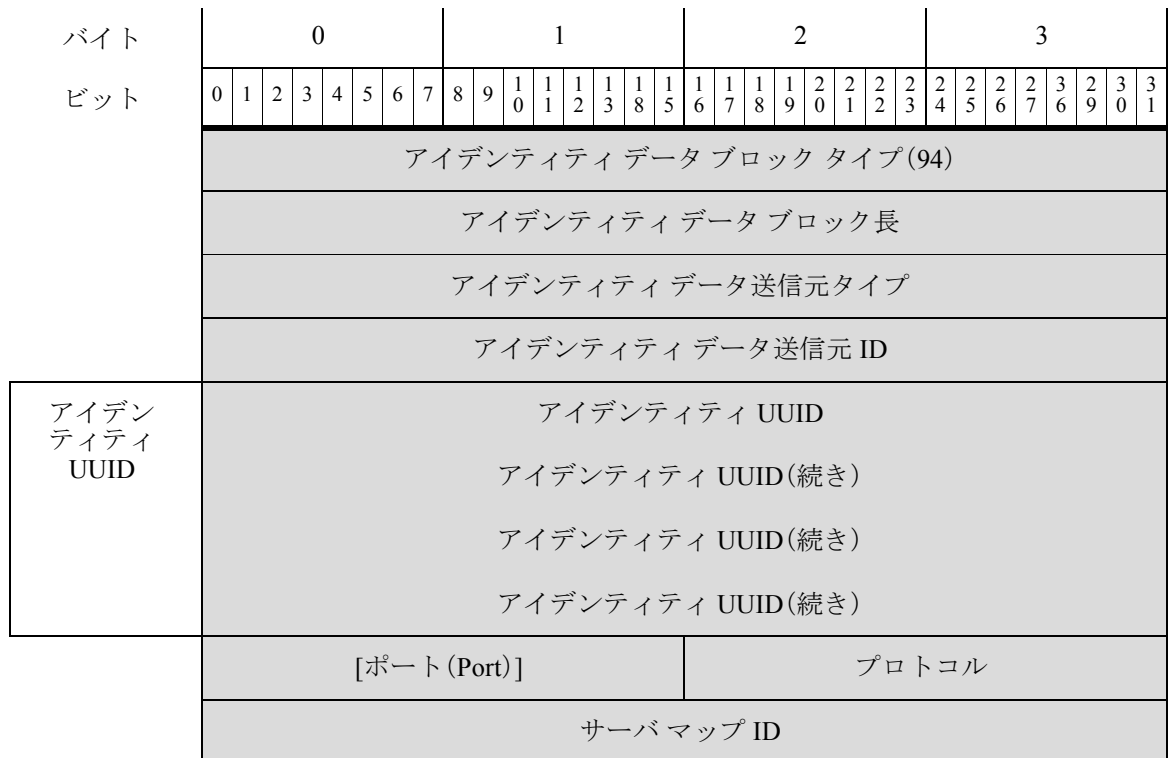
表 4-65 ホスト脆弱性データブロックのフィールド(続き)

フィールド	データタイプ	説明
無効なフラグ	uint8	脆弱性があるかどうかを示す値。
タイプ(Type)	uint32	脆弱性のタイプ。

アイデンティティ データ ブロック

アイデンティティ データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 94 です。アイデンティティ データ ブロックは、オペレーティング システムやサーバフィンガープリント送信元のアイデンティティがいつ競合するか、あるいはいつタイムアウトになるかを示すアイデンティティの競合メッセージとアイデンティティ タイムアウトメッセージで使用します。このデータ ブロックは、アクティブ送信元アイデンティティ(ユーザ、スキャナ、またはアプリケーション)と競合中であると報告されたアイデンティティを記述します。詳細については、[アイデンティティ競合とアイデンティティ タイムアウト システム メッセージ\(4-61 ページ\)](#)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。



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。

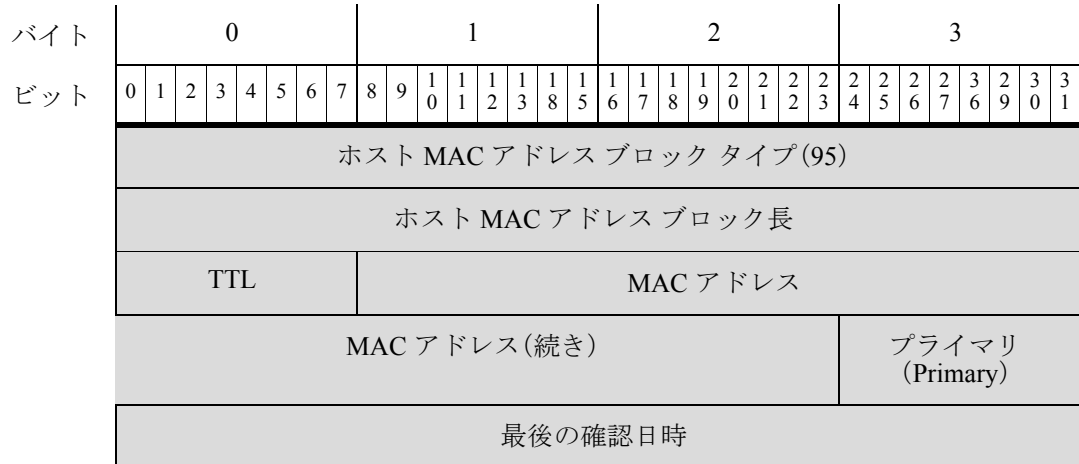
表 4-66 アイデンティティ データ ブロックのフィールド

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: <ul style="list-style-type: none"> 無応答 (RNA) がフィンガープリント データを提供した場合、0 ユーザがフィンガープリント データを提供した場合、1 サードパーティ スキャナがフィンガープリント データを提供した場合、2 nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでフィンガープリント データを提供した場合、3
アイデンティティ データ 送信元 ID	uint32	フィンガープリント データの送信元にマッピングする ID 番号。送信元タイプによって、これは無応答 (RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
UUID	uint8[16]	アイデンティティがオペレーティング システム アイデンティティの場合、フィンガープリントの固有識別子として機能するオクテット形式の ID 番号。
[ポート (Port)]	uint16	アイデンティティがサーバ アイデンティティの場合、サーバ データを含むパケットで使用するポートを示します。
プロトコル	uint16	アイデンティティがサーバ アイデンティティの場合、ネットワーク プロトコルの IANA 番号またはサーバ データを含むパケットが使用する Ethertype を示します。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 <ul style="list-style-type: none"> 6:TCP 7:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 <ul style="list-style-type: none"> 2048:IP
サーバ マップ ID	uint32	アイデンティティがサーバ アイデンティティの場合、サーバの ID、ベンダー、バージョンの組み合わせを表すサーバ マッピング ID を示します。

ホスト MAC アドレス 4.9+

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

次の図は、4.9+ の MAC アドレス データ ブロックの形式です。



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 4-67 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。

バイト	0								1								2								3												
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	
	セカンダリホスト更新ブロックタイプ(96)																																				
	セカンダリホスト更新ブロック長																																				
	[IPアドレス(IP Address)]																																				
	リストブロックタイプ(11)																																				ホストMAC アドレスリ スト
	リストブロック長																																				
ホストMAC アドレス一覧	ホストMACアドレスブロックタイプ(95)																																				
	ホストMACアドレスブロック長																																				
	ホストMACアドレスデータブロック...																																				

次の表では、ホスト更新データブロックのフィールドについて説明します。

表 4-68 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。

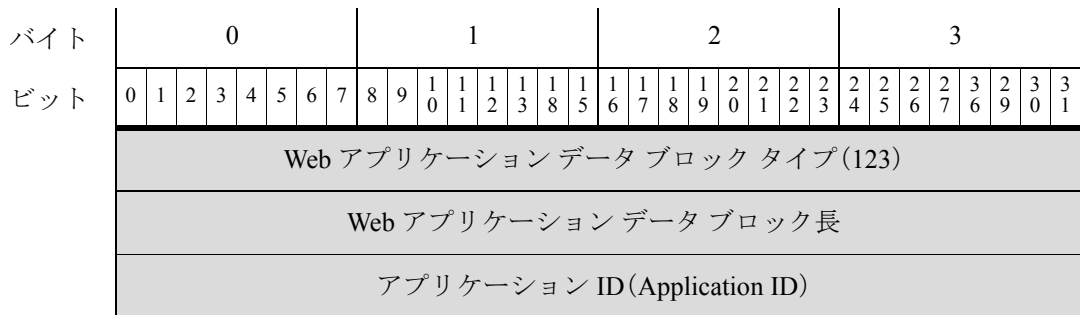
表 4-68 セカンダリ ホスト更新データ ブロックのフィールド(続き)

フィールド	データタイプ	説明
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 4-69 Web アプリケーションデータブロックのフィールド

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

接続統計データブロック 6.2+

接続統計データブロックは、接続データメッセージで使用されます。3 番目の [セキュリティインテリジェンス (Security Intelligence)] フィールドが 6.2+ の接続統計データブロックに追加されました。バージョン 6.2+ の接続統計データブロックには、シリーズ 1 グループのブロックのブロックタイプ 168 が含まれています。これはブロックタイプ 163 [接続統計データブロック 6.1.x \(B-220 ページ\)](#) に置き換わります。

接続イベントレコードは、要求メッセージにイベントバージョン 13 とイベントコード 71 とともに拡張イベントフラグを設定して要求します。[要求フラグ \(2-12 ページ\)](#) を参照してください。ビット 23 を有効にすると、拡張イベントヘッダーがレコードに含まれます。

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 \(4-55 ページ\)](#) を参照してください。

次の図は、6.2+ の接続統計データブロックの形式です。

バイト	0								1								2								3										
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
接続統計データブロックタイプ (168)																																			
接続統計データブロック長																																			
デバイス ID (Device ID)																																			
入力ゾーン																																			
入力ゾーン (続き)																																			
入力ゾーン (続き)																																			
入力ゾーン (続き)																																			
出力ゾーン																																			

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	出力ゾーン(続き)																															
	出力ゾーン(続き)																															
	出力ゾーン(続き)																															
	入力インターフェイス																															
	入力インターフェイス(続き)																															
	入力インターフェイス(続き)																															
	入力インターフェイス(続き)																															
	出力インターフェイス																															
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	イニシエータ IP アドレス																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	レスポнда IP アドレス																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	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)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ポリシー リビジョン(続き)																																
ポリシー リビジョン(続き)																																
ルール ID																																
トンネル ルール ID																																
ルール アクション																ルールの理由																
ルールの理由(続き)																イニシエータ ポート																
レスポнда ポート																TCP フラグ																
プロトコル								NetFlow ソース																								
NetFlow ソース(続き)																																
NetFlow ソース(続き)																																
NetFlow ソース(続き)																																
NetFlow ソース(続き)								インスタンス ID (Instance ID)																接続数カウンタ								
接続数カウンタ(続き)								最初のパケット タイムスタンプ																								
最初のパケット タイムスタンプ(続き)								最終パケット タイムスタンプ																								
最終パケット タイムスタンプ(続き)								イニシエータ送信パケット数																								
イニシエータ送信パケット数(続き)																																
イニシエータ送信パケット数(続き)								レスポнда送信パケット数																								
レスポнда送信パケット数(続き)																																
レスポнда送信パケット数(続き)								イニシエータ送信バイト数																								
イニシエータ送信バイト数(続き)																																
イニシエータ送信バイト数(続き)								レスポнда送信パケット数																								
レスポнда送信バイト数(続き)																																

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IOC 番号																送信元自律システム															
	送信元自律システム(続き)																宛先自律システム															
	宛先自律システム																SNMP 入力															
	SNMP 出力																送信元 TOS								宛先 TOS							
	送信元マスク								宛先マスク								セキュリティ コンテキスト															
	セキュリティ コンテキスト																															
	セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト(続き)																VLAN ID (Admin. VLAN ID)															
参照ホスト	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	参照ホスト...																															
ユーザエージェント	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ エージェント...																															
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																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	SSL ポリシー ID(続き)																															
	SSL ポリシー ID(続き)																															
	SSL ポリシー ID(続き)																															
	SSL ルール ID																															
	SSL 暗号スイート																SSL バージョン								SSL キー証明書統計							
	SSL キー証明書統計(続き)																								実際の SSL アクション							
	実際の SSL アクション(続き)								予期された SSL アクション																SSL フローステータス (SSL Flow Status)							
	SSL フローステータス(続き)								SSL フロー エラー																							
	SSL フローエラー(続き)								SSL フローメッセージ																							
	SSL フローメッセージ(続き)								SSL フロー フラグ																							
	SSL フロー フラグ(続き)																															
SSL サーバ名	SSL フロー フラグ(続き)								文字列ブロック タイプ(0)																							
	文字列ブロック タイプ(0)(続き)								文字列ブロック長																							
	文字列ブロック長(続き)								SSL サーバ名...																							
	SSL URL カテゴリ																															
	SSL セッション ID																															
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															
	SSL セッション ID の長さ								SSL チケット ID																							
	SSL チケット ID(続き)																															
	SSL チケット ID(続き)																															
	SSL チケット ID(続き)																															
	SSL チケット ID(続き)																															
	SSL チケット ID (続き)								SSL チケット ID の長さ								ネットワーク分析ポリシー リビジョン															
	ネットワーク分析ポリシー リビジョン(続き)																															
	ネットワーク分析ポリシー リビジョン(続き)																															
	ネットワーク分析ポリシー リビジョン(続き)																															
	ネットワーク分析ポリシー リビジョン(続き)																エンドポイントプロファイル ID															
	エンドポイントプロファイル ID(続き)																セキュリティグループ ID															
	セキュリティグループ ID(続き)																ロケーション IPv6															
	ロケーション IPv6(続き)																															
	ロケーション IPv6(続き)																															
	ロケーション IPv6(続き)																															
	ロケーション IPv6(続き)																HTTP レスポンス															
DNS クエリ (DNS Query)	HTTP レスポンス(続き)																文字列ブロック タイプ(0)															
	文字列ブロック タイプ(0)(続き)																文字列ブロック長															
	文字列ブロック長(続き)																DNS クエリ...															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	DNS レコードタイプ (DNS Record Type)																DNS レスポンスタイプ															
	DNS TTL																															
	シンクホール UUID																															
	シンクホール UUID(続き)																															
	シンクホール UUID(続き)																															
	シンクホール UUID(続き)																															
	セキュリティ インテリジェンス リスト 1																															
	セキュリティ インテリジェンス リスト 2																															
	セキュリティ インテリジェンス リスト 3																															

次の表では、6.2+ の接続統計データ ブロックのフィールドについて説明します。

表 4-70 接続統計データブロック 6.2+ のフィールド

フィールド	データタイプ	説明
接続統計データブロックタイプ	uint32	6.2+ の接続統計データ ブロックを開始します。値は常に 168 です。
接続統計データブロック長	uint32	接続統計データブロックのバイト数(接続統計ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID (Device ID)	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。

表 4-70 接続統計データブロック 6.2+ のフィールド(続き)

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

表 4-70 接続統計データブロック 6.2+ のフィールド(続き)

フィールド	データタイプ	説明
ドロップしたイニシエータバイト数	uint64	レート制限により、セッションイニシエータからドロップしたバイト数。
レスポндаバイトドロップ	uint64	レート制限により、セッションレスポндаからドロップしたバイト数。
QoS 適用インターフェイス	uint8[16]	レート制限された接続で、レート制限が適用されるインターフェイスの名前。
QoS ルール ID	uint32	接続に適用される QoS ルールの内部 ID 番号(該当する場合)。
ユーザ ID (User ID)	uint32	トラフィックを生成したホストの最終ログインユーザの内部 ID 番号。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URL レピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロックタイプ	uint32	クライアントアプリケーション URL の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーション URL の文字列データブロックのバイト数(文字列ブロックタイプと長さのフィールド用の 8 バイト、およびクライアントアプリケーション URL 文字列のバイト数を含む)。
クライアントアプリケーション URL	string	クライアントアプリケーションがアクセスする URL (該当する場合) (/files/index.html など)。
文字列ブロックタイプ	uint32	ホスト NetBIOS 名の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列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 NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロックタイプ	uint32	クライアントアプリケーションバージョンの文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーションバージョンの文字列データブロックのバイト数(文字列ブロックタイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。

表 4-70 接続統計データブロック 6.2+ のフィールド(続き)

フィールド	データタイプ	説明
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 番目のモニターールの ID。
モニターール 2	uint32	接続イベントに関連付けられている 2 番目のモニターールの ID。
モニターール 3	uint32	接続イベントに関連付けられている 3 番目のモニターールの ID。
モニターール 4	uint32	接続イベントに関連付けられている 4 番目のモニターールの ID。
モニターール 5	uint32	接続イベントに関連付けられている 5 番目のモニターールの ID。
モニターール 6	uint32	接続イベントに関連付けられている 6 番目のモニターールの ID。
モニターール 7	uint32	接続イベントに関連付けられている 7 番目のモニターールの ID。
モニターール 8	uint32	接続イベントに関連付けられている 8 番目のモニターールの ID。
セキュリティインテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティインテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイルイベントカウント	uint16	同じ秒で発生するファイルイベントを区別するために使用される値。
侵入イベントカウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポンドの国	uint16	応答ホストの国のコード。
クライアントのオリジナル国 (Original Client Country)	uint16	要求を開始したプロキシの背後にあるホストの国コード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
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。

表 4-70 接続統計データブロック 6.2+ のフィールド(続き)

フィールド	データタイプ	説明
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。
SNMP 出力	uint16	出力インターフェイスの SNMP インデックス
送信元 TOS	uint8	着信インターフェイス用のタイプ オブ サービス バイト設定。
宛先 TOS	uint8	発信インターフェイス用のタイプ オブ サービス バイト設定。
送信元マスク	uint8	送信元アドレス プレフィックス マスク。
宛先マスク	uint8	宛先アドレス プレフィックス マスク。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキストモードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
VLAN ID (Admin. VLAN ID)	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
文字列ブロックタイプ	uint32	参照ホストを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	参照ホスト文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および参照ホストフィールドのバイト数を含む)。
参照ホスト	string	HTTP または DNS で提供されるホスト名情報。
文字列ブロックタイプ	uint32	ユーザエージェントを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザエージェント文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびユーザエージェントフィールドのバイト数を含む)。
ユーザエージェント	string	セッションのユーザエージェントヘッダーフィールドからの情報。
文字列ブロックタイプ	uint32	HTTP リファラを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	HTTP リファラ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および HTTP リファラフィールドのバイト数を含む)。
HTTP リファラ	string	ページの発生元のサイト。これは HTTP トラフィック内の参照ヘッダー情報にあります。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
SSL ポリシー ID	uint8[16]	接続を処理した SSL ポリシーの ID 番号。
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルトアクションの ID 番号。

表 4-70 接続統計データブロック 6.2+ のフィールド(続き)

フィールド	データタイプ	説明
SSL 暗号スイート	uint16	SSL 接続で使用される暗号スイート。値は 10 進形式で保存されます。値により指定されている暗号スイートの詳細については、 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
SSL バージョン	uint8	接続の暗号化に使用された SSL または TLS プロトコルバージョン。
SSL サーバ証明書ステータス	uint32	SSL 証明書のステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 1(不明):サーバ証明書のステータスは判別できませんでした。 2(有効):サーバ証明書は有効です。 4(自己署名済み):サーバ証明書は自己署名です。 16(無効な発行者):サーバ証明書に無効な発行者があります。 32(無効な署名):サーバ証明書に無効な署名があります。 64(期限切れ):サーバ証明書は期限切れです。 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 256(取り消し):サーバ証明書は取り消されました。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 <ul style="list-style-type: none"> 0:「不明」 1:「復号しない」 2:「ブロックする」 3:「リセットでブロック」 4:「復号(既知のキー)」 5:「復号(置換キー)」 6:「復号(Resign)」

表 4-70 接続統計データブロック 6.2+ のフィールド(続き)

フィールド	データタイプ	説明
予期された SSL アクション	uint16	SSL ルールに基づいて接続に対して実行する必要があるアクション。有効な値は次のとおりです。 <ul style="list-style-type: none">• 0:「不明」• 1:「復号しない」• 2:「ブロックする」• 3:「リセットでブロック」• 4:「復号(既知のキー)」• 5:「復号(置換キー)」• 6:「復号(Resign)」

表 4-70 接続統計データブロック 6.2+ のフィールド(続き)

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

表 4-70 接続統計データブロック 6.2+ のフィールド(続き)

フィールド	データタイプ	説明
SSL フローメッセージ	uint32	<p>SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。</p> <ul style="list-style-type: none"> 0x00000001:NSE_MT__HELLO_REQUEST 0x00000002:NSE_MT__CLIENT_ALERT 0x00000004:NSE_MT__SERVER_ALERT 0x00000008:NSE_MT__CLIENT_HELLO 0x00000010:NSE_MT__SERVER_HELLO 0x00000020:NSE_MT__SERVER_CERTIFICATE 0x00000040:NSE_MT__SERVER_KEY_EXCHANGE 0x00000080:NSE_MT__CERTIFICATE_REQUEST 0x00000100:NSE_MT__SERVER_HELLO_DONE 0x00000200:NSE_MT__CLIENT_CERTIFICATE 0x00000400:NSE_MT__CLIENT_KEY_EXCHANGE 0x00000800:NSE_MT__CERTIFICATE_VERIFY 0x00001000: NSE_MT__CLIENT_CHANGE_CIPHER_SPEC 0x00002000:NSE_MT__CLIENT_FINISHED 0x00004000: NSE_MT__SERVER_CHANGE_CIPHER_SPEC 0x00008000:NSE_MT__SERVER_FINISHED 0x00010000:NSE_MT__NEW_SESSION_TICKET 0x00020000:NSE_MT__HANDSHAKE_OTHER 0x00040000:NSE_MT__APP_DATA_FROM_CLIENT 0x00080000:NSE_MT__APP_DATA_FROM_SERVER
SSL フローフラグ	uint64	<p>暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> 0x00000001 (NSE_FLOW__VALID):他のフィールドを有効にするために設定する必要があります 0x00000002 (NSE_FLOW__INITIALIZED):内部構造が処理可能です 0x00000004 (NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました
文字列ブロックタイプ	uint32	SSL サーバ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	SSL サーバ名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および SSL サーバ名フィールドのバイト数を含む)。

表 4-70 接続統計データブロック 6.2+ のフィールド(続き)

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

表 4-70 接続統計データブロック 6.2+ のフィールド(続き)

フィールド	データタイプ	説明
セキュリティインテリジェンスリスト 1	uint32	イベントに関連付けられているセキュリティインテリジェンスリスト。これは、関連メタデータのセキュリティインテリジェンスリストにマップされます。接続に関連付けられた3つのセキュリティインテリジェンスリストが存在する場合があります。
セキュリティインテリジェンスリスト 2	uint32	イベントに関連付けられているセキュリティインテリジェンスリスト。これは、関連メタデータのセキュリティインテリジェンスリストにマップされます。接続に関連付けられた3つのセキュリティインテリジェンスリストが存在する場合があります。
セキュリティインテリジェンスリスト 3	uint32	イベントに関連付けられているセキュリティインテリジェンスリスト。これは、関連メタデータのセキュリティインテリジェンスリストにマップされます。接続に関連付けられた3つのセキュリティインテリジェンスリストが存在する場合があります。

スキャン結果データブロック 5.2+

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

次の図は、スキャン結果データブロックの形式を示しています。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
スキャン結果ブロック タイプ(142)																																								
スキャン結果ブロック長																																								
ユーザ ID(User ID)																																								
スキャンタイプ																																								
[IP アドレス (IP Address)]																																								
IP アドレス(続き)																																								
IP アドレス(続き)																																								
IP アドレス(続き)																																								
[ポート (Port)]																				プロトコル																				

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
	フラグ (Flag)																リストブロック タイプ (11)																脆弱性スキャン リスト
	リストブロック タイプ (11)																リストブロック長																
脆弱性 リスト	リストブロック長																スキャン脆弱性ブロック タイプ (109)																
	スキャン脆弱性ブロック タイプ (109)																スキャン脆弱性ブロック長																
	スキャン脆弱性ブロック長																脆弱性データ...																
	リストブロック タイプ (11)																																汎用スキャン 結果リスト
	リストブロック長																																
スキャン結果 リスト	汎用スキャン結果ブロック タイプ (108)																																
	汎用スキャン結果ブロック長																																
	汎用スキャン結果...																																
ユーザ (User) 製品リスト	汎用リストブロック タイプ (31)																																
	汎用リストブロック長																																
	ユーザ製品データブロック*																																

次の表は、スキャン結果データ ブロックのフィールドについての説明です。

表 4-71 スキャン結果データ ブロックのフィールド

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

表 4-71 スキャン結果データブロックのフィールド(続き)

フィールド	データタイプ	説明
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 <ul style="list-style-type: none"> • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 <ul style="list-style-type: none"> • 2048:IP
フラグ (Flag)	uint16	予約済
リストブロックタイプ	uint32	トランスポート スキャン脆弱性データを伝えるスキャン脆弱性データブロックで構成されるリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数には、リストブロックタイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのスキャン脆弱性データブロックが含まれています。 このフィールドには、ゼロ以上のスキャン脆弱性データブロックが続きます。
スキャン脆弱性ブロックタイプ	uint32	スキャン中に検出された脆弱性を記述するスキャン脆弱性データブロックを開始します。この値は常に 109 です。
スキャン脆弱性ブロック長	uint32	スキャン脆弱性データブロックのバイト数(接続統計ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン脆弱性データのバイト数を含む)。
脆弱性データ	string	各脆弱性に関する情報。
リストブロックタイプ	uint32	トランスポート スキャン脆弱性データを伝えるスキャン脆弱性データブロックで構成されるリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数には、リストブロックタイプと長さのフィールド用の 8 バイトと、カプセル化されたすべてのスキャン脆弱性データブロックが含まれています。 このフィールドには、ゼロ以上のスキャン脆弱性データブロックが続きます。
汎用スキャン結果ブロックタイプ	uint32	スキャン中に検出されたサーバおよびオペレーティング システムを記述する汎用スキャン結果データブロックを開始します。この値は常に 108 です。
汎用スキャン結果ブロック長	uint32	汎用スキャン結果データブロックのバイト数(汎用スキャン結果ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン結果データのバイト数を含む)。
汎用スキャン結果データ	string	各スキャン結果に関する情報。

表 4-71 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のホスト入力データを伝えるユーザ製品データブロックから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	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのユーザ製品データブロックを含む)。
ユーザ製品データブロック*	変数 (variable)	ホスト入力データを含むユーザ製品データブロック。このデータブロックの説明の詳細については、 ユーザ製品データブロック 5.1+(4-176 ページ) を参照してください。

ホストサーバデータブロック 4.10.0+

ホストサーバデータブロックは、ホストで検出したサーバに関する情報を伝えます。ここには、検出したサーバごとにブロックとともに、サーバが実行している Web アプリケーションの Web アプリケーションデータブロックのリストも格納します。ホストサーバデータブロックは、新規と変更された TCP サーバと UDP サーバのメッセージに含まれます。詳細については、[サーバメッセージ\(4-47 ページ\)](#)を参照してください。ホストサーバデータブロックのブロックタイプは、シリーズ 1 ブロックグループのブロックタイプ 103 です。



(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、ホストサーバデータブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
サーバブロックタイプ(103)																																
サーバブロック長																																
[ポート(Port)]																ヒット																
ヒット(続き)																前回の使用 (Last Used)																
サブサーバ情報	前回の使用(続き)																汎用リストブロックタイプ(31)															
	汎用リストブロックタイプ(続き)																汎用リストブロック長															
	汎用リストブロック長(続き)																サーバ情報ブロックタイプ(117)*															
信頼度																																
汎用リストブロックタイプ(31)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用リストブロック長																															
Web Application	Web アプリケーションブロック タイプ(123)*																															
	Web アプリケーションブロック長																															
	Web アプリケーションデータ...																															

次の表では、ホストサーバデータブロックのフィールドについて説明します。

表 4-72 ホストサーバデータブロックのフィールド

フィールド	データタイプ	説明
ホストサーバブロックタイプ	uint32	ホストサーバデータブロックを開始します。この値は常に 103 です。
ホストサーバブロック長	uint32	ホストサーバブロックタイプフィールドと長さフィールドの 8 バイトに、後続のデータバイト数を加えたホストサーバデータブロックの合計バイト数。
[ポート (Port)]	uint16	サーバが実行しているポート番号。
ヒット	uint32	サーバが受信したヒット数。
前回の使用 (Last Used)	uint32	システムが使用中のサーバを検出した前回時刻を表す UNIX タイムスタンプ。
汎用リストブロックタイプ	uint32	汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストブロックとカプセル化されたサブサーバ情報データブロックのバイト数。この値は、汎用リストブロックヘッダーフィールドの 8 バイトに、カプセル化されたすべてのデータブロックのバイト数を加えた値です。
サーバ情報データブロック*	変数 (variable)	リストブロック長の最大バイト数を上限としたサーバ情報データブロック。詳細は、 4.10.x 、 5.0 ~ 5.0.2 のサーバ情報データブロック (4-149 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 (4-121 ページ) を参照してください。

フルホストサーバデータブロック 4.10.0+

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



(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、フルサーバデータブロックの形式です。

バイト	0								1								2								3												
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
ビット	フルサーバブロックタイプ(104)																																				
	フルサーバブロック長																																				
	[ポート(Port)]																ヒット																				
サブサーバ-シスコ	ヒット(続き)																汎用リストブロックタイプ(31)																				
	汎用リストブロックタイプ(続き)																汎用リストブロック長																				
	汎用リストブロック長(続き)																フルサーバ情報データブロック(106)*																				
サブサーバ-ユーザ(User)	汎用リストブロックタイプ(31)																																				
	汎用リストブロック長																																				
	フルサーバ情報データブロックタイプ(106)*																																				
サブサーバ-スキャナ	汎用リストブロックタイプ(31)																																				
	汎用リストブロック長																																				
	フルサーバ情報データブロック(106)*																																				
サブサーバ-Application	汎用リストブロックタイプ(31)																																				
	汎用リストブロック長																																				
	フルサーバ情報データブロック(106)*																																				
	信頼度																																				

バイト	0								1							2							3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
サーババナー	BLOB ブロック タイプ (10)																														
	BLOB ブロック長																														
	サーババナーデータ...																														
VDB脆弱性	汎用リストブロック タイプ (31)																														
	汎用リストブロック長																														
	(VDB)ホスト脆弱性データブロック (85)*																														
サードパーティ/VDB脆弱性	汎用リストブロック タイプ (31)																														
	汎用リストブロック長																														
	(サードパーティ/VDB)ホスト脆弱性データブロック (85)*																														
サードパーティホスト脆弱性	汎用リストブロック タイプ (31)																														
	汎用リストブロック長																														
	(サードパーティ)ホスト脆弱性データブロック (85)*																														
Web Application	汎用リストブロック タイプ (31)																														
	汎用リストブロック長																														
	Web アプリケーションデータ (123)*																														

次の表では、フルサーバデータブロックのコンポーネントについて説明します。

表 4-73 フルホストサーバデータブロック 4.10.0+ のフィールド

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

表 4-73 フルホストサーバデータブロック 4.10.0+ のフィールド(続き)

フィールド	データタイプ	説明
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべてのサブサーバ情報データブロックを含む汎用リストデータブロックのバイト数。
サブサーバ情報 - シスコデータブロック*	変数 (variable)	シスコが検出したホストサーバのサブサーバに関する情報を含むフルサーバ情報データブロック。このデータブロックの説明の詳細については、 フルサーバ情報データブロック (4-151 ページ) を参照してください。
汎用リストブロックタイプ	uint32	ユーザが追加したサブサーバデータを伝えるサブサーバ情報データブロックで構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべてのサーバ情報データブロックを含む汎用リストデータブロックのバイト数。
サブサーバ情報 - ユーザが追加したデータブロック*	変数 (variable)	ユーザが検出したホストサーバのサブサーバに関する情報を含むフルサーバ情報データブロック。このデータブロックの説明の詳細については、 フルサーバ情報データブロック (4-151 ページ) を参照してください。
汎用リストブロックタイプ	uint32	スキャナが追加したサブサーバデータを伝えるサブサーバ情報データブロックで構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべてのサブサーバ情報データブロックを含む汎用リストデータブロックのバイト数。
サブサーバ情報 - スキャナが追加したデータブロック*	変数 (variable)	スキャナが検出したホストサーバのサブサーバに関する情報を含むフルサーバ情報データブロック。このデータブロックの説明の詳細については、 フルサーバ情報データブロック (4-151 ページ) を参照してください。
汎用リストブロックタイプ	uint32	アプリケーションが追加したサブサーバデータを伝えるサブサーバ情報データブロックで構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべてのサブサーバ情報データブロックを含む汎用リストデータブロックのバイト数。
サブサーバ情報 - アプリケーションが追加したデータブロック*	変数 (variable)	アプリケーションが検出したホストサーバのサブサーバに関する情報を含むフルサーバ情報データブロック。このデータブロックの説明の詳細については、 フルサーバ情報データブロック (4-151 ページ) を参照してください。
信頼度	uint32	フルサーバデータの正しい識別におけるシスコの信頼度のパーセンテージ。
BLOB ブロックタイプ	uint32	バナーデータを含む BLOB データブロックを開始します。この値は常に 10 です。
BLOB ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに、バナーのバイト数を加えた BLOB データブロックのバイト数。

表 4-73 フルホストサーバデータブロック 4.10.0+ のフィールド(続き)

フィールド	データタイプ	説明
サーババナー データ	byte[n]	パケットの最初の n バイトがサーバ イベントに関わるバイトであり、n は 256 以下です。
汎用リストブロックタイプ	uint32	シスコ 脆弱性データを搬送するホスト脆弱性データブロックで構成された汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべてのホスト脆弱性データブロックを含む汎用リストデータブロックのバイト数。
(VDB)ホスト脆弱性データブロック*	変数 (variable)	脆弱性データベース (VDB) でホスト脆弱性に関する情報を格納したホスト脆弱性データブロック。このデータブロックの説明の詳細については、 ホスト脆弱性データブロック 4.9.0+(4-116 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 スキャナから得られた サードパーティ ホスト脆弱性データを搬送し、VDB に登録済みの脆弱性情報を含む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+(4-116 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えるホスト脆弱性データブロックで構成される汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべてのホスト脆弱性データブロックを含む汎用リストデータブロックのバイト数。
サードパーティ スキャン ホスト脆弱性データブロック*	変数 (variable)	サードパーティ スキャナで識別済みでも VDB には登録されていない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+(4-116 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 のサーバ情報データ ブロック

サーバ情報データ ブロックは、サーバ ID、サーバ ベンダーとバージョン、送信元情報など、サーバに関する情報を伝えます。サーバ情報データ ブロックのブロック タイプは、4.10.x のシリーズ 1 ブロック グループのブロック タイプ 105 と、5.0 ~ 5.0.2 のシリーズ 1 ブロック グループのブロック タイプ 117 です。サーバ情報データ ブロックは、ホスト サーバ ブロックとフル ホスト サーバ データ ブロックのリストで搬送されます。詳細については、[ホスト サーバ データ ブロック 4.10.0+\(4-143 ページ\)](#)と[フル ホスト サーバ データ ブロック 4.10.0+\(4-145 ページ\)](#)を参照してください。

次の図は、サーバ情報データ ブロックの形式です。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	サーバ情報ブロック タイプ (105 117)																															
	サーバ情報ブロック長																															
	アプリケーション ID (Application ID)																															
	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	サーバベンダー名文字列...																															
	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	サーババージョン文字列...																															
	前回の使用 (Last Used)																															
	ソース タイプ																															
	ソース																															
	リストブロック タイプ (11)																															
	リストブロック長																															
サブサーバ	サブサーバブロック タイプ (1)*																															
	サブサーバブロック長																															
	サブサーバデータ...																															

次の表では、サーバ情報データ ブロックのコンポーネントについて説明します。

表 4-74 サーバ情報データブロックのフィールド

フィールド	データタイプ	説明
サーバ情報ブロックタイプ	uint32	サーバ情報データブロックを開始します。ブロックタイプは 4.10.x の場合、105、5.0+ の場合、117 です。
サーバ情報ブロック長	uint32	サーバ情報データブロックの合計バイト数。サーバ情報ブロックタイプフィールドと長さフィールドの 8 バイト、サーバ ID の 4 バイト、ベンダー名ブロックタイプと長さの 8 バイト、ベンダー名にさらに 4 バイト、バージョン文字列ブロックタイプと長さに 8 バイト、バージョン文字列にさらに 4 バイト、最後に使用する送信元タイプと送信元 ID フィールドごとに 4 バイトで構成します。
アプリケーション ID (Application ID)	uint32	検出したサーバで実行しているアプリケーションプロトコルのアプリケーション ID。
文字列ブロックタイプ	uint32	サーバベンダー名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにサーバベンダー名のバイト数を加えたベンダー名文字列データブロックのバイト数。
サーバベンダー名	string	サーバベンダーの名前。
文字列ブロックタイプ	uint32	サーババージョンを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにサーババージョンのバイト数を加えたサーババージョン文字列データブロックのバイト数。
サーババージョン	string	サーババージョン
前回使用時刻	uint32	トラフィックで前回サーバ情報を使用した時刻を示します。
ソースタイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> 無応答 (RNA) がサーバデータを提供した場合、0 ユーザがサーバデータを提供した場合、1 サードパーティ スキャナがサーバデータを提供した場合、2 nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでサーバデータを提供した場合、3
ソース	uint32	サーバデータの送信元にマッピングする ID 番号。送信元タイプによって、これは無応答 (RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
リストブロックタイプ	uint32	サブサーバデータブロック リストを開始します。この値は常に 11 です。
リストブロック長	uint32	リストブロックタイプフィールドと長さフィールドの 8 バイトに、後続のカプセル化されたサブサーバデータブロックのバイト数を加えたリストデータブロックの合計バイト数。

表 4-74 サーバ情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
サブサーバブロックタイプ	uint32	最初のサブサーバデータブロックを開始します。このデータブロックには、他のサブサーバデータブロックを、リストブロック長フィールドで定義した上限まで続けることができます。
サブサーバブロック長	uint32	サブサーバブロックタイプフィールドと長さフィールドの8バイトに、後続のデータバイト数を加えた各サブサーバデータブロックの合計バイト数。
サブサーバデータ	変数(variable)	サブサーバデータブロック(4-76 ページ)に記載のサブサーバデータ。

フルサーバ情報データブロック

フルサーバ情報データブロックは、サブサーバのアプリケーションプロトコル、ベンダー、バージョン、関連サブサーバなど、ホストで検出したサーバに関する情報を伝えます。サブサーバごとに、情報は、フルサブサーバデータブロックに格納します(フルサブサーバデータブロック(4-86 ページ)を参照)。フルサーバ情報データブロックのブロックタイプは、シリーズ1ブロックグループのブロックタイプ106です。



(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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
	フルサーバブロックタイプ(106)																																					
	フルサーバブロック長																																					
	アプリケーションプロトコルID																																					
ベンダー	文字列ブロックタイプ(0)																																					
	文字列ブロック長																																					
	ベンダー名文字列...																																					
バージョン	文字列ブロックタイプ(0)																																					
	文字列ブロック長																																					
	バージョン文字列...																																					

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	前回の使用 (Last Used)																															
	ソース タイプ																															
	ソース																															
	リストブロック タイプ (11)																															
	リストブロック長																															
サブサーバ	フルサブサーバブロック タイプ (51)*																															
	フルサブサーバブロック長																															
	フルサブサーバデータ...																															

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

表 4-75 フルサーバ情報データブロックのフィールド

フィールド	データタイプ	説明
フルサーバ情報ブロックタイプ	uint32	フルサーバ情報データブロックを開始します。この値は常に 106 です。
フルサーバ情報ブロック長	uint32	フルサーバブロックタイプフィールドと長さフィールドの 8 バイトに、後続のフルサーバデータのバイト数を加えたフルサーバ情報データブロックの合計バイト数。
アプリケーションプロトコル ID	uint32	サーバで実行しているアプリケーションプロトコルのアプリケーション ID。
文字列ブロックタイプ	uint32	アプリケーションプロトコルベンダー名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにベンダー名のバイト数を加えたベンダー名文字列データブロックのバイト数。
ベンダー名 (Vendor Name)	string	サーバベンダーの名前。
文字列ブロックタイプ	uint32	アプリケーションプロトコルバージョンを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにバージョンのバイト数を加えた文字列データブロックのバイト数。
バージョン	string	サーバのバージョン。
前回の使用 (Last Used)	uint32	システムが使用中のサーバを検出した前回時刻を表す UNIX タイムスタンプ。

表 4-75 フルサーバ情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
ソースタイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> 無応答(RNA)がサーバデータを提供した場合、0 ユーザがサーバデータを提供した場合、1 サードパーティ スキャナがクライアント データを提供した場合、2 nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでサーバデータを提供した場合、3
ソース	uint32	サーバデータの送信元にマッピングする ID 番号。送信元タイプによって、これは無応答(RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
リストブロックタイプ	uint32	サブサーバデータを伝えるフルサーバ情報データブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのフルサブサーバデータブロックを加えた値です。このフィールドの後にはゼロか、さらにフルサブサーバデータブロックが続きます。
フルサブサーバブロックタイプ	uint32	最初のフルサブサーバデータブロックを開始します。このデータブロックには、他のフルサブサーバデータブロックを、リストブロック長フィールドで定義した上限まで続けることができます。
フルサブサーバブロック長	uint32	フルサブサーバブロックタイプフィールドと長さフィールドの 8 バイトに、後続のデータバイト数を加えた各フルサブサーバデータブロックの合計バイト数。
フルサブサーバデータブロック*	uint32	このサーバのサブサーバを含むフルサブサーバデータブロック。このデータブロックの説明の詳細については、 フルサブサーバデータブロック (4-86 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+\(4-140 ページ\)](#)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	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	汎用スキャン結果データ ブロック タイプ (108)																															
	汎用スキャン結果ブロック長																															
	[ポート (Port)]																プロトコル															
スキャン結果サブサーバ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	スキャン結果サブサーバ文字列...																															
スキャン結果値	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	スキャン結果値...																															
スキャン結果サブサーバ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	スキャン結果サブサーバ (不定様式) 文字列...																															
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 4-76 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が使用するポート。

表 4-76 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
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 <ul style="list-style-type: none"> • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 <ul style="list-style-type: none"> • 2048:IP
文字列ブロックタイプ	uint32	サブサーバを格納した文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにサブサーバのバイト数を加えたサブサーバ文字列データブロックのバイト数。
スキャン結果サブサーバ	string	サブサーバ。
文字列ブロックタイプ	uint32	値を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに値のバイト数を加えた値文字列データブロックのバイト数。
スキャン結果値	string	スキャン結果値。
文字列ブロックタイプ	uint32	サブサーバを格納した文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにサブサーバのバイト数を加えたサブサーバ文字列データブロックのバイト数。
スキャン結果サブサーバ	string	サブサーバ(不定様式)。
文字列ブロックタイプ	uint32	値を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに値のバイト数を加えた値文字列データブロックのバイト数。
スキャン結果値	string	スキャン結果値(不定様式)。

4.10.0+ のスキャン脆弱性データブロック

スキャン脆弱性データブロックは、脆弱性を記述し、スキャン結果データブロックで使用します。そのスキャン結果データブロックは、追加スキャン結果イベント(イベントタイプ 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+\(4-140 ページ\)](#) および [スキャン結果を追加メッセージ\(4-60 ページ\)](#) を参照してください。スキャン脆弱性データブロックのブロックタイプは、シリーズ 1 ブロックグループのブロックタイプ 109 です。

次の図は、スキャン脆弱性データ ブロックの形式です。

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	スキャン脆弱性ブロック タイプ(109)																															
	スキャン脆弱性ブロック長																															
	[ポート (Port)]																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																															
	ID																															
[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 4-77 スキャン脆弱性データブロックのフィールド

フィールド	データタイプ	説明
スキャン脆弱性ブロックタイプ	uint32	スキャン脆弱性データブロックを開始します。この値は常に109です。
スキャン脆弱性ブロック長	uint32	スキャン脆弱性データブロックのバイト数(接続統計ブロックタイプと長さのフィールド用の8バイト、およびそれに続くスキャン脆弱性データのバイト数を含む)。
[ポート(Port)]	uint16	脆弱性の影響を受けるサブサーバで使用するポート。
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 <ul style="list-style-type: none"> • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 <ul style="list-style-type: none"> • 2048:IP
文字列ブロックタイプ	uint32	ID を含む文字列データブロックを開始します。
文字列ブロック長	uint32	文字列ブロックタイプと長さの8バイトに、IDのバイト数を加えたIDの文字列データブロックのバイト数。
ID	string	脆弱性を検出したスキャンユーティリティの指定に従って報告されたその脆弱性のID。Qualys スキャンで検出した脆弱性の場合、たとえばこのフィールドには Qualys ID が設定されます。
文字列ブロックタイプ	uint32	脆弱性名を含むデータブロックを開始します。
文字列ブロック長	uint32	文字列ブロックタイプと長さの8バイトに、脆弱性名のバイト数を加えた、脆弱性名の文字列データブロックの合計バイト数。
[名前(Name)]	string	脆弱性の名前。
文字列ブロックタイプ	uint32	脆弱性記述文字列データブロックを開始します。
文字列ブロック長	uint32	文字列ブロックタイプと長さの8バイトに、脆弱性の記述のバイト数を加えた、脆弱性の記述の文字列データブロックの合計バイト数。
説明	string	脆弱性の記述。
文字列ブロックタイプ	uint32	脆弱性名を含むデータブロックを開始します。
文字列ブロック長	uint32	文字列ブロックタイプと長さの8バイトに、脆弱性名のバイト数を加えた、脆弱性名の文字列データブロックの合計バイト数。
名前クリーン	string	脆弱性の名前(不定様式)。

表 4-77 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
文字列ブロックタイプ	uint32	脆弱性記述文字列データブロックを開始します。
文字列ブロック長	uint32	文字列ブロックタイプと長さの8バイトに、脆弱性の記述のバイト数を加えた、脆弱性の記述の文字列データブロックの合計バイト数。
記述クリーン	string	脆弱性の記述(不定様式)。
リストブロックタイプ	uint32	Bugtraq ID 番号のリストのリストデータブロックを開始します。
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 (4-79 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 (4-81 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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
フルホストクライアントアプリケーションブロックタイプ(112)																																								
フルホストクライアントアプリケーションブロック長																																								
ヒット																																								

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	前回の使用 (Last Used)																															
	アプリケーション ID (Application ID)																															
バージョン	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	バージョン...																															
	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 4-78 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。

表 4-78 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
前回の使用 (Last Used)	uint32	システムが使用中のクライアントを検出した前回時刻を表す UNIX タイムスタンプ。
アプリケーション ID (Application ID)	uint32	検出したクライアントアプリケーションのアプリケーション ID(該当する場合)。
文字列ブロック タイプ	uint32	クライアントアプリケーションバージョンの文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロックタイプと長さの 8 バイトに、クライアントアプリケーションバージョンのバイト数を加えたクライアントアプリケーション名の文字列データブロックのバイト数。
バージョン	string	クライアントアプリケーションバージョン。
汎用リストブロックタイプ	uint32	汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストブロックとカプセル化された Web アプリケーションデータブロックのバイト数。この値は、汎用リストブロックヘッダーフィールドの 8 バイトに、カプセル化されたすべてのデータブロックのバイト数を加えた値です。
Web アプリケーションデータブロック	変数 (variable)	汎用リストブロック長の最大バイト数を上限としてカプセル化した Web アプリケーションデータブロック。
汎用リストブロックタイプ	uint32	汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストブロックとカプセル化された脆弱性データブロックのバイト数。この値は、汎用リストブロックヘッダーフィールドの 8 バイトに、カプセル化されたすべての脆弱性データブロックのバイト数を加えた値です。
脆弱性データブロック	変数 (variable)	汎用リストブロック長の最大バイト数を上限としてカプセル化した脆弱性データブロック。

5.0+ のホストクライアントアプリケーションデータブロック

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ホストクライアントアプリケーションブロック タイプ(122)																															
	ホストクライアントアプリケーションブロック長																															
	ヒット																															
	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 4-79 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。

表 4-79 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
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)。
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 (4-121 ページ) を参照してください。

ユーザ脆弱性データブロック 5.0+

ユーザ脆弱性データブロックは、脆弱性について記述し、ユーザ脆弱性変更ブロック内で使用します。さらに、ユーザ脆弱性変更ブロックはユーザ設定有効脆弱性イベントとユーザ設定無効脆弱性イベントで使用します。5.0+ のユーザ脆弱性データブロックのブロックタイプは、シリーズ 1 ブロックグループのブロックタイプ 124 です。これはブロックタイプ 79 に置き換わりません。ユーザ脆弱性変更データブロックの詳細については、[ユーザ脆弱性変更データブロック 4.7+\(4-110 ページ\)](#) を参照してください。

次の図は、ユーザ脆弱性変更データブロックの形式です。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
ユーザ脆弱性ブロックタイプ (124)																																								
ユーザ脆弱性ブロック長																																								

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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 Range 指定ブロック	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	IP 範囲仕様データ ブロック..*																															
	[ポート (Port)]																プロトコル															
	脆弱性 ID																															
サードパー ティ脆弱性 UUID	サードパーティ脆弱性 UUID																															
	UUID(続き)																															
	UUID(続き)																															
	UUID(続き)																															
	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	脆弱性文字列...																															
	クライアントアプリケーション ID																															
	アプリケーションプロトコル ID																															
	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	バージョン文字列...																															

次の表では、ユーザ脆弱性データ ブロックのフィールドについて説明します。

表 4-80 ユーザ脆弱性データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザ脆弱性ブロック タイプ	uint32	ユーザ脆弱性データ ブロックを開始します。この値は常に124です。
ユーザ脆弱性ブロック長	uint32	ユーザ脆弱性ブロック タイプ フィールドと長さフィールドの8バイトに、後続のユーザ脆弱性データのバイト数を加えたユーザ脆弱性データ ブロックの合計バイト数。

表 4-80 ユーザ脆弱性データブロックのフィールド(続き)

フィールド	データタイプ	説明
汎用リストブロックタイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データブロック* で構成された汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーとカプセル化されたすべての IP 範囲仕様データブロック* を含む汎用リスト データ ブロックのバイト数。
IP 範囲仕様データブロック*	変数 (variable)	ユーザ入力からの IP アドレス範囲。このデータ ブロックの説明の詳細については、5.2+ の IP アドレス範囲データブロック (4-98 ページ) を参照してください。
[ポート (Port)]	uint16	脆弱性の影響を受けるサーバで使用するポート。クライアント アプリケーション脆弱性の場合、値は 0 です。
プロトコル	uint16	このブロックには、フィンガープリント Universally Unique Identifier (UUID) の他、フィンガープリントタイプ、フィンガープリント送信元タイプ、フィンガープリント送信元 ID を格納します。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。 トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 <ul style="list-style-type: none"> • 6: TCP • 17: UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 <ul style="list-style-type: none"> • 2048: IP クライアント アプリケーション脆弱性の場合、値は 0 です。
脆弱性 ID	uint32	シスコ 脆弱性 ID。
サードパーティ脆弱性 UUID	uint8 [16]	指定する場合は、サードパーティ脆弱性の固有 ID 番号。そうでない場合、この値は 0 です。
文字列ブロックタイプ	uint32	脆弱性名を含むデータ ブロックを開始します。値は常に 0 です。
文字列ブロック長	uint32	文字列ブロックタイプと長さの 8 バイトに、脆弱性名のバイト数を加えた、脆弱性名の文字列データ ブロックの合計バイト数。
脆弱性名	string	脆弱性名
クライアントアプリケーション ID	uint32	クライアント アプリケーションのアプリケーション ID。シングルモードの場合、この値は 0 になります。
アプリケーションプロトコル ID	uint32	クライアント アプリケーションで使用す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。

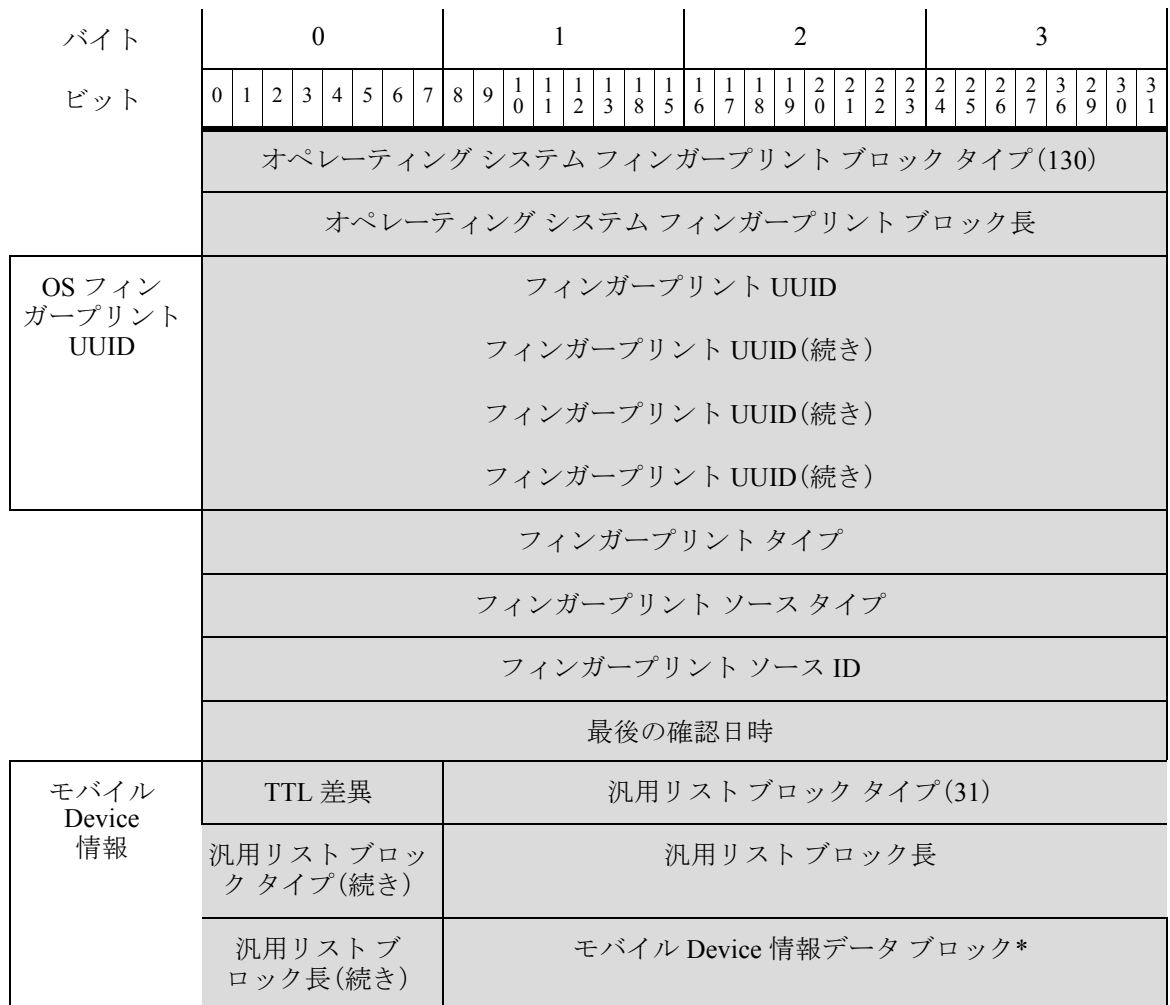
表 4-80 ユーザ脆弱性データブロックのフィールド(続き)

フィールド	データタイプ	説明
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。



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 4-81 オペレーティング システム フィンガープリント データ ブロックのフィールド

フィールド	データタイプ	説明
オペレーティング システム フィンガープリント データ ブロック タイプ	uint32	オペレーティング システム データ ブロックを開始します。この値は常に 130 です。
オペレーティング システム データ ブロック長	uint32	オペレーティング システム フィンガープリント データ ブロック タイプと長さの 8 バイトに、後続のオペレーティング システム フィンガープリント データのバイト数を加えたオペレーティング システム フィンガープリント データ ブロックのバイト数。
フィンガープリント UUID	uint8[16]	オペレーティング システムの固有識別子として機能するフィンガープリント ID 番号(オクテット)。フィンガープリント UUID は、脆弱性データベース (VDB) 内のオペレーティング システム名、ベンダー、バージョンにマップされます。
フィンガープリント タイプ	uint32	フィンガープリントのタイプを示します。
フィンガープリント ソース タイプ	uint32	オペレーティング システム フィンガープリントを提供するソースのタイプ(ユーザやスキャナ)を示します。
フィンガープリント ソース ID	uint32	ID 番号。オペレーティング システム フィンガープリントを提供したユーザのログイン名にマップします。
最後の確認日時	uint32	トラフィックで前回フィンガープリントを確認した時刻を示します。
TTL 差異	uint8	フィンガープリントの TTL 値とホストにフィンガープリントを実行するとき使用するパケット上の TTL 値との差を示します。
汎用リスト ブロック タイプ	uint32	汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト ブロックとカプセル化されたデータ ブロックのバイト数。この値は、汎用リスト ブロック ヘッダー フィールドの 8 バイトに、カプセル化されたすべてのデータ ブロックのバイト数を加えた値です。
モバイル Device 情報データ ブロック	変数 (variable)	リストブロック長の最大バイト数を上限としてカプセル化したモバイル Device 情報データ ブロック。このデータ ブロックの説明の詳細については、 5.1+ Device のモバイル情報データ ブロック (4-166 ページ) を参照してください。

5.1+ Device のモバイル情報データ ブロック

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	モバイル Device 情報ブロック タイプ (131)																															
	モバイル Device 情報ブロック長																															
モバイル Device データ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	モバイル Device 文字列データ...																															
	モバイル Device 最後の確認日時																															
	Mobile																															
	改造																															

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

表 4-82 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。

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

■ ホストディスカバリ データブロックと接続データブロック

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
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 優先順位								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 4-83 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データブロックタイプ	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データブロック長	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データブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く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かのネットワークにあるかを示します。 <ul style="list-style-type: none"> 0: ホストはプライマリ ネットワークにあります。 1: ホストはセカンダリ ネットワークにあります。
汎用リストデータブロックタイプ	uint32	サーバフィンガープリントを使用して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。
汎用リストデータブロック長	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(サーバフィンガープリント)データブロック*	変数 (variable)	サーバフィンガープリントを使用して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+ (4-165 ページ) を参照してください。
汎用リストデータブロックタイプ	uint32	クライアントフィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストデータブロック長	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+ (4-165 ページ) を参照してください。

表 4-83 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+ (4-165 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+ (4-165 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+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	IPv6 サーバ フィンガープリントを使用して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。

表 4-83 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) データ ブロック*	変数 (variable)	IPv6 サーバ フィンガープリントを使用して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+(4-165 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 (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+(4-165 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+(4-165 ページ) を参照してください。
汎用リストブロック タイプ	uint32	ユーザ エージェント フィンガープリントで識別するフィンガープリント データを搬送するオペレーティング システム フィンガープリント データ ブロックで構成される汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。

表 4-83 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(ユーザエージェントフィンガープリント)データブロック*	変数(variable)	ユーザエージェントフィンガープリントで識別したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
リストブロックタイプ	uint32	TCP サーバデータを伝えるサーバデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバデータブロックを加えた値です。 このフィールドには、ゼロ以上のサーバデータブロックが続きます。
TCP サーバデータブロック	変数(variable)	TCP サーバを記述するホストサーバデータブロック。このデータブロックの説明の詳細については、 ホストサーバデータブロック 4.10.0+(4-143 ページ) を参照してください。
リストブロックタイプ	uint32	UDP サーバデータを伝えるサーバデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバデータブロックを加えた値です。 このフィールドには、ゼロ以上のサーバデータブロックが続きます。
UDP サーバデータブロック	uint32	UDP サーバを記述するホストサーバデータブロック。このデータブロックの説明の詳細については、 ホストサーバデータブロック 4.10.0+(4-143 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 (4-78 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 4-83 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 (4-78 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+(4-119 ページ) を参照してください。
最終検出時のホスト	uint32	システムがホストアクティビティを検出した前回時刻を表すUNIXタイムスタンプ。
ホストタイプ	uint32	ホストタイプを示します。表示される可能性がある値は次のとおりです。 <ul style="list-style-type: none"> 0:ホスト 1:ルータ 2:ブリッジ 3:NAT デバイス 4:LB(ロードバランサ)
Mobile	uint8	検出したホストがモバイルデバイスであるかどうかを示す true/false フラグ。
改造	uint8	ホストが(ジェイルブレイクされていない)モバイルデバイスであるかどうかを示す true/false フラグ。
VLANの有無	uint8	VLANが存在するかどうかを示します。 <ul style="list-style-type: none"> 0:はい 1:いいえ
VLAN ID (Admin. VLAN ID)	uint16	ホストがメンバーであるVLANを示すVLAN ID番号。
VLANタイプ	uint8	VLANタグにカプセル化されたパケットのタイプ。
VLAN優先順位	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 4-83 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のブロックのリスト。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+(4-158 ページ) を参照してください。
文字列ブロックタイプ	uint32	ホスト NetBIOS 名の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列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 NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。

ユーザ製品データブロック 5.1+

ユーザ製品データブロックは、サードパーティアプリケーション文字列マッピングなど、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伝えます。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+\(4-140 ページ\)](#)と[ユーザサーバメッセージとオペレーティングシステムメッセージ\(4-59 ページ\)](#)で使用します。ユーザ製品データブロックのブロックタイプは、バージョン 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 以降のシリーズ 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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
ユーザ製品データブロックタイプ (134)																																								
ユーザ製品ブロック長																																								
ソース																																								
ソースタイプ																																								

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
[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 (Port)]																プロトコル															
	ドロップ ユーザ製品																															
カスタム (Custom) ベンダー文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	カスタム ベンダー文字列...																															
カスタム (Custom) 製品文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	カスタム製品文字列...																															
カスタム (Custom) バージョン文字列	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	カスタム バージョン文字列...																															
	ソフトウェア ID																															
	サーバ ID																															
	ベンダー ID																															
	製品 ID																															
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							
	0	1	2	3	4	5	6	7	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															
	0	1	2	3	4	5	6	7	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 4-84 ユーザ製品データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザ製品データブロックタイプ	uint32	ユーザ製品データ ブロックを開始します。5.1+ の場合、この値は 134 です。
ユーザ製品ブロック長	uint32	ユーザ製品データ ブロックのバイトの合計数(ユーザ製品ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ製品データのバイト数を含む)。
ソース	uint32	データをインポートした送信元にマッピングする ID 番号。送信元タイプによって、これは無応答 (RNA)、ユーザ、スキャナ、またはサードパーティ アプリケーションにマッピングされます。
ソースタイプ	uint32	データ送信元のタイプにマッピングする番号: <ul style="list-style-type: none"> 無応答 (RNA) がデータを提供した場合、0 ユーザがデータを提供した場合、1 サードパーティ スキャナがデータを提供した場合、2 nmimport.pl やホスト入力 API クライアントなどのコマンドライン ツールでデータを提供した場合、3
汎用リストブロックタイプ	uint32	IP アドレス範囲データを伝える IP 範囲仕様データ ブロック* で構成された汎用リストデータ ブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リスト ヘッダーとカプセル化されたすべての IP 範囲仕様データ ブロック* を含む汎用リストデータ ブロックのバイト数。

表 4-84 ユーザ製品データブロックのフィールド(続き)

フィールド	データタイプ	説明
IP 範囲仕様データブロック*	変数 (variable)	ユーザ入力の IP アドレス範囲に関する情報を含む IP 範囲仕様データブロック。このデータブロックの説明の詳細については、5.2+ の IP アドレス範囲データブロック (4-98 ページ) を参照してください。
[ポート (Port)]	uint16	ユーザが指定するポート。
プロトコル	uint16	IANA プロトコル番号、または Ethertype。扱いは、トランスポート層プロトコルとネットワーク層プロトコルでは異なります。トランスポート層プロトコルは、IANA プロトコル番号で識別します。次に例を示します。 <ul style="list-style-type: none"> • 6:TCP • 17:UDP ネットワーク層プロトコルは IEEE 登録 Ethertype の 10 進数形式で識別します。次に例を示します。 <ul style="list-style-type: none"> • 2048:IP
ドロップ ユーザ製品	uint32	ユーザ OS 定義がホストから削除されたかどうかを示します: <ul style="list-style-type: none"> • 0:いいえ • 1:はい
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタムベンダー名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタムベンダー文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびベンダー名のバイト数を含む)。
カスタムベンダー名	string	ユーザ入力に指定されたカスタムベンダー名。
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタム製品名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタム製品文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および製品名のバイト数を含む)。
カスタム製品名	string	ユーザ入力に指定されたカスタム製品名。
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタムバージョンを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタムバージョン文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
カスタムバージョン	string	ユーザ入力に指定されたカスタムバージョン。
ソフトウェア ID	uint32	データベースのサーバまたはオペレーティングシステムの特定のリビジョンの識別子。

表 4-84 ユーザ製品データブロックのフィールド(続き)

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

表 4-84 ユーザ製品データ ブロックのフィールド(続き)

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

表 4-84 ユーザ製品データブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	拡張文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の8バイト、および拡張番号のバイト数を含む)。
内線番号	string	ユーザ入力のサードパーティ OS 文字列をマップする Firepower システム オペレーティング システムの拡張番号。
UUID	uint8 [x16]	オペレーティング システム用の固有 ID 番号が含まれます。
文字列ブロックタイプ	uint32	ユーザ入力に指定されたデバイス ハードウェア情報を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ビルド文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の8バイト、およびビルド番号のバイト数を含む)。
Device 文字列	string	モバイル デバイス ハードウェア情報。
Mobile	uint8	オペレーティング システムがモバイル デバイスで動作しているかどうかを示す true/false フラグ。
改造	uint8	モバイル デバイスのオペレーティング システムがジェイルブレイクされているかどうかを示す true/false フラグ。
汎用リストブロックタイプ	uint32	どの修正が特定の IP アドレス範囲内のホストに適用されているかに関するユーザ入力データを伝える修正リストデータブロックで構成される、汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべての修正リストデータブロックを含む)。
修正リストデータブロック*	変数 (variable)	ホストに適用された修正に関する情報を含む修正リストデータブロック。このデータブロックの説明の詳細については、 フィックス リスト データ ブロック (4-105 ページ) を参照してください。

ユーザデータブロック

ユーザデータブロックはユーザイベントメッセージに表示されます。これらはシリーズ1データブロックのサブセットです。シリーズ1データブロックの一般的な形式については、[ディスカバリ \(シリーズ1\) ブロック \(4-63 ページ\)](#)を参照してください。



(注)

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

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

表 4-85 ユーザデータブロックタイプ

タイプ (Type)	目次	データブロックカテゴリ	説明
73	ユーザログイン情報	レガシー	システムが検出したユーザのログイン情報の変更を格納します。詳細については、 ユーザログイン情報データブロック 5.0 ~ 5.0.2 (B-106 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ブロックタイプは、ブロックタイプ 73 と同じ構造ですが、そのフィールド内のデータは異なります。
74	ユーザアカウント更新メッセージ	現在 (Current)	ユーザアカウント情報の変更を格納します。詳細については、 ユーザアカウント更新メッセージデータブロック (4-185 ページ) を参照してください。
75	4.7 ~ 4.10.x のユーザ情報	レガシー	システムが検出したユーザの情報の変更を格納しません。詳細については、 ユーザ情報データブロック 5.x (B-121 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ブロックのブロックタイプは 158 です。
120	5.x のユーザ情報	現在 (Current)	システムが検出したユーザの情報の変更を格納しません。詳細については、 ユーザ情報データブロック 5.x (B-121 ページ) を参照してください。ブロックタイプ 75 に置き換わります。これはブロックタイプ 158 に更新しました。
121	ユーザログイン情報	レガシー	システムが検出したユーザのログイン情報の変更を格納します。詳細については、 ユーザログイン情報データブロック 5.0 ~ 5.0.2 (B-106 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ブロックのブロックタイプは 127 です。
127	ユーザログイン情報	レガシー	システムが検出したユーザのログイン情報の変更を格納します。詳細については、 ユーザログイン情報データブロック 5.1 ~ 5.4.x (B-108 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ブロックのブロックタイプは 159 です。
150	IOC 状態	現在 (Current)	侵害に関する情報を格納します。詳細については、 5.3+ の IOC ステートデータブロック (4-36 ページ) を参照してください。
158	6.0+ のユーザ情報	現在 (Current)	システムが検出したユーザの情報の変更を格納しません。詳細については、 6.0+ の情報データユーザブロック (4-194 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。

表 4-85 ユーザデータブロックタイプ(続き)

タイプ (Type)	目次	データブロック カテゴリ	説明
159	ユーザ ログイン情報	レガシー	システムが検出したユーザのログイン情報の変更を格納します。詳細については、 ユーザ ログイン情報 データブロック 6.0.x (B-110 ページ) を参照してください。これはブロック タイプ 127 に置き換わります。
165	ユーザ ログイン情報	レガシー	システムが検出したユーザのログイン情報の変更を格納します。詳細については、 ユーザ ログイン情報 データブロック 6.1.x (B-117 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 (4-197 ページ) を参照してください。
167	ユーザ ログイン情報	現在 (Current)	システムが検出したユーザのログイン情報の変更を格納します。詳細については、 ユーザ ログイン情報 データブロック 6.2+ (4-200 ページ) を参照してください。これはブロック タイプ 165 に置き換わります。

ユーザ アカウント更新メッセージデータブロック

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

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

次の図は、ユーザ アカウント更新メッセージデータ ブロックの形式です。

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

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファースト [名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	名...																															
ミドルネーム イニシャル (Initials)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ミドルネーム イニシャル...																															
名 [名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	姓...																															
正式名称	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	正式名称...																															
役職 (Title)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	タイトル...																															
スタッフ ID	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	スタッフ アイデンティティ...																															
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...																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
県	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	県...																															
国/地域	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	国/地域																															
郵便番号 コード (Code)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	郵便番号...																															
建物	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	建物...																															
参照先	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	場所...																															
会議室 (Room)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	会議室...																															
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...																															

バイト ビット	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
部署名	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	部署名...																															
オフィス (Office)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	オフィス...																															
郵便配達先	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	郵便配達先...																															
E メール	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール...																															
電話	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電話...																															
IP Phone	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	IP 電話...																															
ユーザ 1	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ 1...																															
ユーザ 2	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ 2...																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ユーザ 3	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ 3...																															
ユーザ 4	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ユーザ 4...																															
電子メール エイリアス 1	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール エイリアス 1...																															
電子メール エイリアス 2	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール エイリアス 2...																															
電子メール エイリアス 3	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール エイリアス 3...																															

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

表 4-86 ユーザ アカウント更新メッセージのデータ ブロックのフィールド

フィールド	データタイプ	説明
ユーザ アカウント更新メッセージブロックタイプ	uint32	ユーザ アカウント更新メッセージのデータ ブロックを開始します。この値は常に 74 です。
ユーザ アカウント更新メッセージブロック長	uint32	ユーザ アカウント更新メッセージブロックタイプフィールドと長さフィールドの 8 バイトに、後続のユーザ アカウント更新メッセージデータのバイト数を加えたユーザ アカウント更新メッセージデータ ブロックの合計バイト数。
文字列ブロックタイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 4-86 ユーザアカウント更新メッセージのデータブロックのフィールド(続き)

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

表 4-86 ユーザアカウント更新メッセージのデータブロックのフィールド (続き)

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

表 4-86 ユーザアカウント更新メッセージのデータブロックのフィールド(続き)

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

表 4-86 ユーザアカウント更新メッセージのデータブロックのフィールド (続き)

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

表 4-86 ユーザアカウント更新メッセージのデータブロックのフィールド (続き)

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

6.0+ の情報データ ユーザブロック

ユーザ情報データブロックはユーザ変更メッセージで使用され、検出、削除、またはドロップされたユーザの情報を伝えます。詳細については、[ユーザ変更メッセージ \(4-62 ページ\)](#) を参照してください。

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

ユーザ情報データブロックのブロックタイプは、4.7 ~ 4.10.x のシリーズ 1 ブロックグループのブロックタイプ 75 と、5.x のシリーズ 1 ブロックグループのブロックタイプ 120 です。詳細については、[ユーザ情報データブロック 5.x \(B-121 ページ\)](#) を参照してください。

次の図は、ユーザ情報データブロックの形式です。

バイト	0								1								2								3																			
ビット	0	1	2	3	4	5	6	7	8	9	0	1	1	2	3	8	5	1	6	7	8	9	0	2	2	2	2	2	2	2	2	3	4	5	6	7	3	6	2	9	3	0	3	1
ユーザ情報ブロックタイプ (158)																																												
ユーザ情報ブロック長																																												
ユーザ ID (User ID)																																												

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ユーザ (User) [名前 (Name)]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザ名...																															
	レルム ID																															
	プロトコル																															
ファースト [名前 (Name)]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	名...																															
姓 [名前 (Name)]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	姓...																															
E メール	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	電子メール...																															
部署名 (Department)	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	部署名...																															
電話	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	電話...																															
	エンドポイント プロファイル ID																															
	セキュリティ グループ ID																															
	ロケーション IPv6 アドレス																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ロケーション IPv6 アドレス(続き)																															
	ロケーション IPv6 アドレス(続き)																															
	ロケーション IPv6 アドレス(続き)																															

次の表は、ユーザ情報データブロックのコンポーネントについての説明です。

表 4-87 ユーザ情報データブロックのフィールド

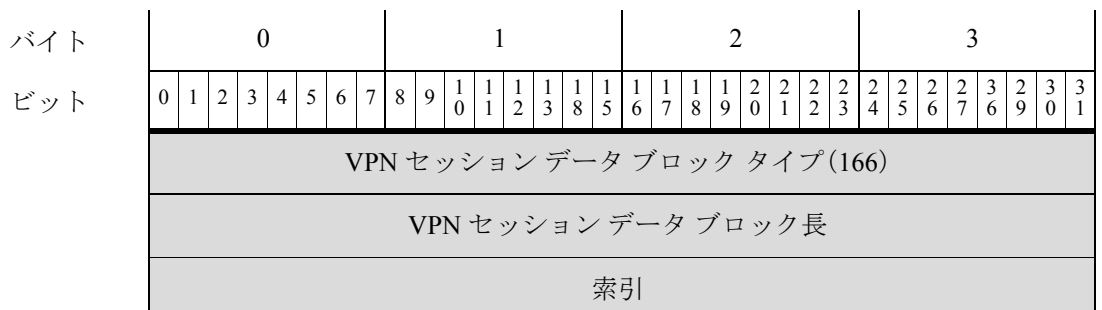
フィールド	データタイプ	説明
ユーザ情報ブロックタイプ	uint32	ユーザ情報データブロックを開始します。この値は 158 です。
ユーザ情報ブロック長	uint32	ユーザ情報データブロックのバイトの合計数(ユーザログイン情報ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ情報データのバイト数を含む)。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。
文字列ブロックタイプ	uint32	ユーザのユーザ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データブロックのバイト数(ブ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

表 4-87 ユーザ情報データブロックのフィールド(続き)

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

6.2+ のVPNセッションデータブロック

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



バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
[グループポリシー (Group Policy)]	タイプ (Type)								文字列ブロック タイプ (0)																							
	文字列ブロック タイプ								文字列ブロック長																							
	文字列ブロック長								グループ ポリシー...																							
接続プロファイル	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	接続プロファイル...																															
クライアントオペレーティングシステム	クライアントの国 (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 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 4-88 VPN セッションデータブロック フィールド

フィールド	データタイプ	説明
VPNセッションデータブロックタイプ	uint32	VPN セッションデータブロックを開始します。この値は常に166です。
VPNセッションブロック長	uint32	VPN セッションデータブロック内の総バイト数。これには、VPN セッションデータブロックのタイプフィールドおよび長さフィールド用の8バイトと、その後のVPN データフィールド内のバイト数が含まれます。
索引	uint32	セッションを識別するためにVPN デバイスによって生成された番号。
タイプ (Type)	uint8	VPN セッションのタイプ。有効な値は次のとおりです。 <ul style="list-style-type: none"> • 0: 不明 • 1: Cisco IKEv1 クライアント • 2: AnyConnect IKEv1 クライアント • 3: AnyConnect SSL • 4: WebVPN クライアントレス • 5: サイト間 IKEv2 • 6: サイト間 IKEv2 • 7: 汎用 IKEv2 RA クライアント
文字列ブロックタイプ	uint32	VPN セッションのグループポリシーを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ユーザ名文字列のデータブロック内のバイト数。これには、ブロックタイプフィールドおよび長さフィールド用の8バイトと、グループポリシー内のバイト数が含まれます。
[グループポリシー (Group Policy)]	string	VPN セッションが確立されたときにクライアントに割り当てられたグループポリシーの名前。
文字列ブロックタイプ	uint32	VPN セッションの接続プロファイルを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ユーザ名文字列のデータブロック内のバイト数。これには、ブロックタイプフィールドおよび長さフィールド用の8バイトと、接続プロファイル内のバイト数が含まれます。
接続プロファイル	string	VPN セッションで使用する接続プロファイル(トンネルグループ)の名前。
クライアント IP アドレス	uint8[16]	VPN クライアントデバイスの IP アドレス。
クライアントの国 (Client Country)	uint16	VPN クライアントの国のコード。
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 4-88 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	ユーザ名文字列のデータブロック内のバイト数。これには、ブロックタイプフィールドおよび長さフィールド用の8バイトと、オペレーティングシステム名内のバイト数が含まれます。
クライアントオペレーティングシステム	string	クライアントデバイスのオペレーティングシステム。
文字列ブロックタイプ	uint32	クライアントデバイスで使用されるVPNアプリケーションを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ユーザ名文字列のデータブロック内のバイト数。これには、ブロックタイプフィールドおよび長さフィールド用の8バイトと、VPNアプリケーション内のバイト数が含まれます。
クライアントアプリケーション	string	クライアントデバイスのVPNアプリケーション。
接続期間 (Connection Duration)	uint32	VPNセッションの期間(秒単位)VPNログアウトアクションにだけ指定されます。それ以外は0です。
送信バイト数	uint64	VPNセッション中にVPNクライアントに送信されるバイト数。VPNログアウトアクションにだけ指定されます。それ以外は0です。
受信バイト数	uint64	VPNセッション中にVPNクライアントから受信したバイト数。VPNログアウトアクションにだけ指定されます。それ以外は0です。

ユーザログイン情報データブロック 6.2+

ユーザログイン情報データブロックは、ユーザ情報更新メッセージで使用され、検出されたユーザのログイン情報の変更を伝えます。詳細については、[ユーザ情報更新メッセージブロック \(4-63 ページ\)](#)を参照してください。

バージョン 6.2+ では、ユーザログイン情報データブロックには、シリーズ 1 グループのブロック内にブロックタイプ 167 が含まれています。VPN サポート用の新しいフィールドがあります。これはブロックタイプ 165 に置き換わります。詳細については、[ユーザログイン情報データブロック 6.1.x \(B-114 ページ\)](#)を参照してください。

次の図は、ユーザログイン情報データブロックの形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ユーザログイン情報ブロックタイプ(167)																																
ユーザログイン情報ブロック長																																
Timestamp																																

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

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
レポート基準	ログインタイプ								承認タイプ (Type)								文字列ブロック タイプ(0)															
	文字列ブロック タイプ(0) (続き)																文字列ブロック長															
	文字列ブロック長 (続き)																レポート基準...															
説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	説明...																															
VPNセッション	VPNセッションデータブロック タイプ(166)																															
	VPNセッションデータブロック長																															
	VPNセッション...																															

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

表 4-89 ユーザ ログイン情報データ ブロックのフィールド

フィールド	データタイプ	説明
ユーザ ログイン情報ブロック タイプ	uint32	ユーザ ログイン情報データ ブロックを開始します。バージョン 6.2+ の場合、この値は 167 です。
ユーザ ログイン情報ブロック長	uint32	ユーザ ログイン情報データ ブロックのバイトの合計数 (ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ ログイン情報データのバイト数を含む)。
Timestamp	uint32	イベントのタイムスタンプ。
IPv4 アドレス (IPv4 Address)	uint32	このフィールドは予約済みですが、設定されておりません。IPv4 アドレスは IPv6 アドレス フィールドに保存されます。詳細については、 IP アドレス (1-5 ページ) を参照してください。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
文字列ブロック タイプ	uint32	ドメインを含む文字列データ ブロックを開始します。この値は常に 0 です。

表 4-89 ユーザログイン情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトにドメインのバイト数を加えたユーザ名文字列データブロックのバイト数。
ドメイン	string	ユーザがログインしているドメイン。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。
レルム ID	uint32	アイデンティティレルムに対応する整数 ID。
エンドポイントプロファイル ID	uint32	接続エンドポイントが使用するデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
セキュリティグループ ID	uint32	ネットワークトラフィックグループの ID 番号。
プロトコル	uint32	ユーザの検出やレポートに使用するプロトコル。値は以下のとおりです。 <ul style="list-style-type: none"> • 165:FTP • 426:SIP • 547:AOL Instant Messenger • 683:IMAP • 710:LDAP • 767:NTP • 773:Oracle データベース • 788:POP3 • 1755:MDNS
[ポート (Port)]	uint16	ユーザを検出したポート番号。
範囲の開始	uint16	TS エージェントが使用するポート範囲の開始ポート
開始ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の開始ポート。
終了ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の最終ポート。
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの8バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IPv6 アドレス。
ロケーション IPv6 アドレス	uint8[16]	ユーザがログインした最新の IP アドレス。IPv4 または IPv6 のどちらかのアドレスになります。
ログインタイプ	uint8	検出されたユーザログインのタイプ。

表 4-89 ユーザログイン情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
認証タイプ (Authentication Type)	uint8	ユーザが使用する認証のタイプ。値は次のとおりです。 <ul style="list-style-type: none"> 0: 認証は不要 1: パッシブ認証、AD エージェント、または ISE セッション 2: キャプティブ ポータルの正常な認証 3: キャプティブ ポータルのゲスト認証 4: キャプティブ ポータルの失敗認証
文字列ブロックタイプ	uint32	レポート基準値を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	レポート基準文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびレポート基準フィールドのバイト数を含む)。
レポート基準	string	Active Directory サーバの名前など、このアクティビティのレポーター。
文字列ブロックタイプ	uint32	説明の値を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	説明文字列のデータブロック内のバイト数。これには、ブロックタイプフィールドおよび長さフィールド用の 8 バイトと、説明フィールド内のバイト数が含まれます。
説明	string	ログインまたはログオフ アクティビティの説明。
VPN セッションブロックタイプ	uint32	VPN セッションデータを含む VPN セッションデータブロックを開始します。この値は常に 166 です。
VPN セッションデータブロック長	uint32	VPN セッションのデータブロック内のバイト数。これには、ブロックタイプフィールドおよび長さフィールド用の 8 バイトと、VPN セッションデータブロック内のバイト数が含まれます。
VPN セッションデータ	VPN セッションデータ	ログインを VPN セッションに関連付けた場合は、検出された VPN セッションに関する情報。VPN セッションが存在するときのみ使用されます。

ディスカバリ/接続イベントシリーズ2データブロック

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

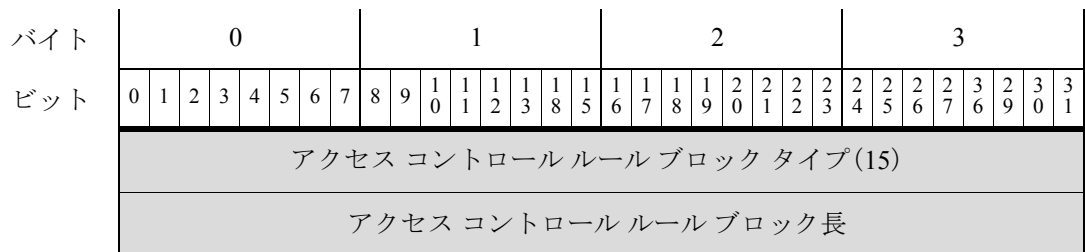
表 4-90 ディスカバリ/接続イベントシリーズ2 ブロックタイプ

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 (4-205 ページ) を参照してください。
21	アクセスコントロールルール理由	現在 (Current)	アクセスコントロールルールのメタデータメッセージが、アクセスコントロールルール理由を記述文字列にマップするときに使用します。 アクセスコントロールルール理由データブロック 5.1+ (4-207 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+(4-209 ページ) を参照してください。
57	ユーザデータ (User Data)	現在 (Current)	ユーザレコードメタデータメッセージが、ユーザを検出したユーザ ID 番号、プロトコル、そしてユーザ名を提供するために使用します。 ユーザデータブロック (4-210 ページ) を参照してください。

アクセスコントロールルールデータブロック

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

次の図は、アクセスコントロールルールデータブロックの構造です。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ACルール UUID	アクセスルールポリシー UUID																															
	アクセスコントロールルール UUID(続き)																															
	アクセスコントロールルール UUID(続き)																															
	アクセスコントロールルール UUID(続き)																															
	アクセスコントロールルール ID																															
	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	名前...																															

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

表 4-91 アクセスコントロールルールデータブロックのフィールド

フィールド	データタイプ	説明
アクセスコントロールルールブロックタイプ	uint32	アクセスコントロールルールブロックを開始します。この値は常に 15 です。
アクセスコントロールルールブロック長	uint32	アクセスコントロールルールブロックタイプフィールドと長さフィールドの 8 バイトに、後続のデータバイト数を加えたアクセスコントロールルールブロックの合計バイト数。
アクセスコントロールルール UUID	uint8[16]	アクセスコントロールルールの固有識別子。このフィールドとアクセスコントロールルール ID を合わせると、このレコードの固有キーになります。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの内部 シスコ 識別子。このフィールドとアクセスコントロールルール UUID を合わせると、このレコードの固有キーになります。
文字列ブロックタイプ	uint32	アクセスコントロールルール UUID とアクセスコントロールルール ID に関連付けられているわかりやすい名前のある文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの 8 バイトと名前フィールドのバイト数が含まれます。
[名前(Name)]	string	わかりやすい名前。

アクセスコントロールルール理由データブロック 5.1+

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

次の図は、アクセスコントロールルール理由データブロックの構造です。



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 4-92 アクセスコントロールルール理由データブロックのフィールド

フィールド	データタイプ	説明
アクセスコントロールルール理由ブロックタイプ	uint32	アクセスコントロールルール理由ブロックを開始します。この値は常に 21 です。
アクセスコントロールルール理由ブロック長	uint32	アクセスコントロールルール理由ブロックタイプフィールドと長さフィールドの 8 バイトに、後続のデータバイト数を加えたアクセスコントロールルール理由ブロックの合計バイト数。

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

フィールド	データタイプ	説明
アクセスコントロールルール理由	uint16	<p>アクセスコントロールルールによって接続がログに記録された理由。このフィールドは、このレコードの固有キーです。</p> <p>イベントをトリガーしたルールの理由の番号。</p> <p>ルールの理由は、複数のビットを設定できるバイナリビットマップです。ルールには、複数の理由があります。ビット値は次のとおりです。</p> <ul style="list-style-type: none"> • 1: IP ブロック • 2: IP モニタ • 4: ユーザ バイパス • 8: ファイル モニタ • 16: ファイル ブロック • 32: 侵入モニタ • 64: 侵入ブロック • 128: ファイル再開ブロック • 256: ファイル再開許可 • 512: ファイルカスタム検出 • 1024: SSL ブロック • 2048: DNS ブロック • 4096: DNS モニタ • 8192: URL ブロック • 16384: URL モニタ • 32768: コンテンツ制約 • 65536: インテリジェント アプリケーション バイパス • 131072: WSA 脅威
文字列ブロックタイプ	uint32	アクセスコントロールルール理由に関連付けられたわかりやすい名前を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データブロックのバイト数です。ブロックタイプとヘッダーフィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	アクセスコントロールルール理由の説明。

セキュリティインテリジェンス カテゴリ データ ブロック 5.1+

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

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

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
	セキュリティ インテリジェンス カテゴリのブロック タイプ (22)																																							
	セキュリティ インテリジェンス カテゴリのブロック長																																							
	セキュリティ インテリジェンス リスト ID																																							
AC ポリシー UUID	アクセス コントロール ポリシー UUID アクセス コントロール ポリシー UUID (続き) アクセス コントロール ポリシー UUID (続き) アクセス コントロール ポリシー UUID (続き)																																							
ルール名 (Rule Name)	文字列ブロック タイプ (0) 文字列ブロック長 セキュリティ インテリジェンス リスト名...																																							

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

表 4-93 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。

表 4-93 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
セキュリティインテリジェンスリストID	uint32	接続でトリガーがかかるIPブラックリストまたはホワイトリストのID。このフィールドとアクセスコントロールポリシーUUIDを合わせると、このレコードの固有キーになります。
アクセスコントロールポリシーUUID	uint8[16]	セキュリティインテリジェンスに設定されたアクセスコントロールポリシーのUUID。このフィールドとセキュリティインテリジェンスリストIDを合わせると、このレコードの固有キーとなります。
文字列ブロックタイプ	uint32	セキュリティインテリジェンスリストに関連付けられたわかりやすい名前を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ブロックタイプフィールドとヘッダーフィールドの8バイトにセキュリティインテリジェンスリスト名フィールドのバイト数を加えた名前文字列データブロックのバイト数。
セキュリティインテリジェンスリスト名	string	接続でトリガーがかかるセキュリティインテリジェンスカテゴリIPカテゴリブラックリストまたはホワイトリストの名前。

ユーザデータブロック

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

次の図は、ユーザデータブロックの構造です。



バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
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 4-95 アクセス コントロール ポリシー データ ブロックのフィールド

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