



## レガシー データ構造の概要

この付録には、旧バージョンの Firepower システム 製品の eStreamer によってサポートされるデータ構造に関する情報を記載しています。

クライアントが、旧バージョン形式でデータを要求するようにビットが設定されているイベントストリーム要求を使用する場合、この付録の情報を使用して、受け取るデータメッセージのデータ構造を識別できます。

バージョン 5.0 より前は、検出エンジンに個別に ID が割り当てられていたことに注意してください。バージョン 5.0 では、デバイスに ID が割り当てられます。この点は、バージョンに基づいてデータ構造に反映されます。



(注) この付録では、Firepower システム のバージョン 4.9 以降からのデータ構造のみを説明します。以前のデータ構造バージョンによる構造向けの資料が必要な場合は、シスコ カスタマー サポートにお問い合わせください。

詳細については、次の各項を参照してください。

- [レガシー侵入データ構造 \(B-1 ページ\)](#)
- [レガシー マルウェア イベントのデータ構造 \(B-51 ページ\)](#)
- [レガシー ディスカバリ データ構造 \(B-93 ページ\)](#)
- [レガシー接続データ構造 \(B-134 ページ\)](#)
- [レガシー関連イベントのデータ構造 \(B-274 ページ\)](#)
- [レガシー ホスト データ構造 \(B-291 ページ\)](#)

## レガシー侵入データ構造

- [侵入イベント \(IPv4\) レコード 5.0.x ~ 5.1 \(B-2 ページ\)](#)
- [侵入イベント \(IPv6\) レコード 5.0.x ~ 5.1 \(B-8 ページ\)](#)
- [侵入イベント レコード 5.2.x \(B-14 ページ\)](#)
- [侵入イベント レコード 5.3 \(B-20 ページ\)](#)
- [侵入イベント レコード 5.1.1.x \(B-26 ページ\)](#)
- [侵入イベント レコード 5.3.1 \(B-32 ページ\)](#)
- [侵入イベント レコード 5.4.x \(B-39 ページ\)](#)
- [侵入影響アラート データ \(B-48 ページ\)](#)

## 侵入イベント (IPv4) レコード 5.0.x ~ 5.1

侵入イベント (IPv4) レコードのフィールドは、次の図では網掛けされています。レコードの種類は 207 です。

侵入イベント レコードは、要求メッセージに侵入イベント フラグまたは拡張要求フラグを設定して要求します。[要求フラグ \(2-12 ページ\)](#) および [拡張要求の送信 \(2-4 ページ\)](#) を参照してください。

バージョン 5.0.x ~ 5.1 の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン (1)																メッセージタイプ (4)															
	メッセージ長																															
	Netmap ID																レコードタイプ (207)															
	レコード長																															
	eStreamer サーバタイムスタンプ (イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み (イベントでビット 23 が設定されている場合のみ)																															
	デバイス ID																															
	イベント ID (Event ID)																															
	イベント秒																															
	イベントマイクロ秒																															
	ルール ID (シグネチャ ID)																															
	ジェネレータ ID																															
	ルール リビジョン																															
	分類 ID																															
	プライオリティ ID																															
	送信元 IPv4 アドレス																															
	宛先 IPv4 アドレス																															
	送信元ポート (Source Port)																接続先ポート															
	IP プロトコル ID								影響フラグ								影響								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
ビット																																
	MPLS ラベル																															
	VLAN ID (Admin. VLAN ID)																パッド															
	ポリシー UUID																															
	ポリシー UUID (続き)																															
	ポリシー UUID (続き)																															
	ポリシー UUID (続き)																															
	ユーザ ID (User ID)																															
	Web アプリケーション ID																															
	クライアント アプリケーション ID																															
	アプリケーション プロトコル ID																															
	アクセス コントロール ルール ID																															
	アクセス コントロール ポリシー UUID																															
	アクセス コントロール ポリシー UUID (続き)																															
	アクセス コントロール ポリシー UUID (続き)																															
	アクセス コントロール ポリシー UUID (続き)																															
	インターフェイス入力 UUID																															
	インターフェイス入力 UUID (続き)																															
	インターフェイス入力 UUID (続き)																															
	インターフェイス入力 UUID (続き)																															
	インターフェイス出力 UUID																															
	インターフェイス出力 UUID (続き)																															
	インターフェイス出力 UUID (続き)																															
	インターフェイス出力 UUID (続き)																															
	セキュリティ ゾーン入力 UUID																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
セキュリティゾーン入力 UUID(続き)																																
セキュリティゾーン入力 UUID(続き)																																
セキュリティゾーン入力 UUID(続き)																																
セキュリティゾーン出力 UUID																																
セキュリティゾーン出力 UUID(続き)																																
セキュリティゾーン出力 UUID(続き)																																
セキュリティゾーン出力 UUID(続き)																																

次の表は、各侵入イベントレコードデータフィールドについての説明です。

表 B-1 侵入イベント(IPv4)レコードのフィールド

フィールド	データタイプ	説明
デバイス ID	uint32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 <a href="#">管理対象デバイスレコードのメタデータ(3-36 ページ)</a> を参照してください。
イベント ID (Event ID)	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
イベントマイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒(100 万分の 1 秒)単位の増分。
ルール ID (シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルールリビジョン	uint32	ルールリビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IPv4 アドレス	uint8[4]	アドレス オクテットの、イベントで使用される送信元 IPv4 アドレス。
宛先 IPv4 アドレス	uint8[4]	アドレス オクテットの、イベントで使用される宛先 IPv4 アドレス。

表 B-1 侵入イベント (IPv4) レコードのフィールド (続き)

フィールド	データタイプ	説明
送信元ポート	uint16	イベントプロトコルタイプが TCP または UDP の場合は送信元ポート番号。
接続先ポート	uint16	イベントプロトコルタイプが TCP または UDP の場合は宛先ポート番号。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none"><li>• 0:IP</li><li>• 1:ICMP</li><li>• 6:TCP</li><li>• 17:UDP</li></ul>

表 B-1 侵入イベント (IPv4) レコードのフィールド(続き)

フィールド	データタイプ	説明
影響フラグ	bits[8]	<p>イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。</li> <li>0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。</li> <li>0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。</li> <li>0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。</li> <li>0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。</li> <li>0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。</li> <li>0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。</li> <li>0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。</li> </ul> <p>次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。</p> <ul style="list-style-type: none"> <li>(0、不明):00x00000</li> <li>赤(1、脆弱):xxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx</li> <li>オレンジ(2、潜在的に脆弱):00x00111</li> <li>黄(3、現在は脆弱でない):00x00011</li> <li>青(4、不明なターゲット):00x00001</li> </ul>
影響	uint8	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>1:レッド(脆弱)</li> <li>2:オレンジ(脆弱の可能性あり)</li> <li>3:イエロー(現在は脆弱でない)</li> <li>4:ブルー(不明なターゲット)</li> <li>5:グレー(不明なインパクト)</li> </ul>

表 B-1 侵入イベント (IPv4) レコードのフィールド (続き)

フィールド	データタイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 <ul style="list-style-type: none"> <li>0: ブロックされていない</li> <li>1: ブロックされた</li> <li>2: ブロックされた可能性がある (設定では許可されていない)</li> </ul>
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID (User ID)	uint32	ユーザの内部 ID 番号 (該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号 (該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号 (該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号 (該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。

## 侵入イベント (IPv6) レコード 5.0.x ~ 5.1

侵入イベント (IPv6) レコードのフィールドは、次の図では網掛けされています。レコードの種類は 208 です。

侵入イベント レコードは、要求メッセージに侵入イベント フラグまたは拡張要求フラグを設定して要求します。[要求フラグ \(2-12 ページ\)](#) および [拡張要求の送信 \(2-4 ページ\)](#) を参照してください。

バージョン 5.0.x ~ 5.1 の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(208)															
	レコード長																															
	eStreamer サーバ タイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
	デバイス ID																															
	イベント ID(Event ID)																															
	イベント秒																															
	イベント マイクロ秒																															
	ルール ID(シグネチャ ID)																															
	ジェネレータ ID																															
	ルール リビジョン																															
	分類 ID																															
	プライオリティ ID																															
	送信元 IPv6 アドレス																															
	送信元 IPv6 アドレス(続き)																															
	送信元 IPv6 アドレス(続き)																															



バイト	0								1								2								3																										
ビット	0	1	2	3	4	5	6	7	8	9	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
送信元 IPv6 アドレス(続き)																																																			
宛先 IPv6 アドレス																																																			
宛先 IPv6 アドレス(続き)																																																			
宛先 IPv6 アドレス(続き)																																																			
宛先 IPv6 アドレス(続き)																																																			
送信元ポート/ICMP タイプ																		宛先ポート/ICMP コード																																	
IP プロトコル ID									影響フラグ									影響									ブロック																								
MPLS ラベル																																																			
VLAN ID (Admin. VLAN ID)																		パッド																																	
ポリシー UUID																																																			
ポリシー UUID(続き)																																																			
ポリシー UUID(続き)																																																			
ポリシー UUID(続き)																																																			
ユーザ ID (User ID)																																																			
Web アプリケーション ID																																																			
クライアント アプリケーション ID																																																			
アプリケーション プロトコル ID																																																			
アクセス コントロール ルール ID																																																			
アクセス コントロール ポリシー UUID																																																			
アクセス コントロール ポリシー UUID(続き)																																																			
アクセス コントロール ポリシー UUID(続き)																																																			
アクセス コントロール ポリシー UUID(続き)																																																			
インターフェイス入力 UUID																																																			
インターフェイス入力 UUID(続き)																																																			

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	インターフェイス入力 UUID(続き)																															
	インターフェイス入力 UUID(続き)																															
	インターフェイス出力 UUID																															
	インターフェイス出力 UUID(続き)																															
	インターフェイス出力 UUID(続き)																															
	インターフェイス出力 UUID(続き)																															
	セキュリティゾーン入力 UUID																															
	セキュリティゾーン入力 UUID(続き)																															
	セキュリティゾーン入力 UUID(続き)																															
	セキュリティゾーン入力 UUID(続き)																															
	セキュリティゾーン出力 UUID																															
	セキュリティゾーン出力 UUID(続き)																															
	セキュリティゾーン出力 UUID(続き)																															
	セキュリティゾーン出力 UUID(続き)																															

次の表は、各侵入イベントレコードデータフィールドについての説明です。

表 B-2 侵入イベント(IPv6)レコードのフィールド

フィールド	データタイプ	説明
デバイス ID	uint32	検出デバイスの ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 <a href="#">管理対象デバイスレコードのメタデータ(3-36 ページ)</a> を参照してください。
イベント ID (Event ID)	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
イベントマイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒(100 万分の 1 秒)単位の増分。
ルール ID (シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。

表 B-2 侵入イベント (IPv6) レコードのフィールド(続き)

フィールド	データタイプ	説明
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IPv6 アドレス	uint8[16]	アドレス オクテットの、イベントで使用される送信元 IPv6 アドレス。
宛先 IPv6 アドレス	uint8[16]	アドレス オクテットの、イベントで使用される宛先 IPv6 アドレス。
送信元ポート/ ICMP タイプ	uint16	イベント プロトコル タイプが TCP または UDP の場合は送信元ポート番号。プロトコル タイプが ICMP である場合、これは ICMP タイプを示します。
宛先ポート/ ICMP コード	uint16	イベント プロトコル タイプが TCP または UDP の場合は宛先ポート番号。プロトコル タイプが ICMP である場合、これは ICMP コードを示します。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none"> <li>• 0:IP</li> <li>• 1:ICMP</li> <li>• 6:TCP</li> <li>• 17:UDP</li> </ul>

表 B-2 侵入イベント (IPv6) レコードのフィールド(続き)

フィールド	データタイプ	説明
影響フラグ	bits[8]	<p>イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。</li> <li>0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。</li> <li>0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。</li> <li>0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。</li> <li>0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。</li> <li>0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。</li> <li>0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。</li> <li>0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。</li> </ul> <p>次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。</p> <ul style="list-style-type: none"> <li>(0、不明):00x00000</li> <li>赤(1、脆弱):xxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx</li> <li>オレンジ(2、潜在的に脆弱):00x00111</li> <li>黄(3、現在は脆弱でない):00x00011</li> <li>青(4、不明なターゲット):00x00001</li> </ul>
影響	uint8	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>1:レッド(脆弱)</li> <li>2:オレンジ(脆弱の可能性あり)</li> <li>3:イエロー(現在は脆弱でない)</li> <li>4:ブルー(不明なターゲット)</li> <li>5:グレー(不明なインパクト)</li> </ul>

表 B-2 侵入イベント (IPv6) レコードのフィールド (続き)

フィールド	データタイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 <ul style="list-style-type: none"> <li>0: ブロックされていない</li> <li>1: ブロックされた</li> <li>2: ブロックされた可能性がある (設定では許可されていない)</li> </ul>
MPLS ラベル	uint32	MPLS ラベル。(4.9+ のイベントにのみ適用。)
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。(4.9+ のイベントにのみ適用。)
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID (User ID)	uint32	ユーザの内部 ID 番号 (該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号 (該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号 (該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号 (該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。

## 侵入イベント レコード 5.2.x

侵入イベントレコードのフィールドは、次の図で網掛けされています。レコードタイプは400であり、ブロックタイプはシリーズ2セットのデータブロックの34です。

eStreamerからの5.2.x侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベントタイプコード12およびバージョン5を要求します(拡張要求の送信の詳細については、[拡張要求の送信\(2-4ページ\)](#)を参照してください)。

バージョン5.2.xの侵入イベントの場合、イベントID、管理対象デバイスID、イベント秒により固有識別子が形成されます。接続の秒、接続インスタンス、および接続数カウンタは、侵入イベントに関連付けられた接続イベントの、1つの固有識別子を形成します。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	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(400)																							
	レコード長																																							
	eStreamer サーバタイムスタンプ(イベント用、ビット23が設定されている場合のみ)																																							
	将来の使用に備えて予約済み(イベントでビット23が設定されている場合のみ)																																							
	ブロックタイプ(34)																																							
	ブロック長																																							
	デバイスID																																							
	イベントID(Event ID)																																							
	イベント秒																																							
	イベントマイクロ秒																																							
	ルールID(シグネチャID)																																							
	ジェネレータID																																							
	ルールリビジョン																																							
	分類ID																																							
	プライオリティID																																							

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

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	インターフェイス入力 UUID																															
	インターフェイス入力 UUID(続き)																															
	インターフェイス入力 UUID(続き)																															
	インターフェイス入力 UUID(続き)																															
	インターフェイス出力 UUID																															
	インターフェイス出力 UUID(続き)																															
	インターフェイス出力 UUID(続き)																															
	インターフェイス出力 UUID(続き)																															
	セキュリティゾーン入力 UUID																															
	セキュリティゾーン入力 UUID(続き)																															
	セキュリティゾーン入力 UUID(続き)																															
	セキュリティゾーン入力 UUID(続き)																															
	セキュリティゾーン出力 UUID																															
	セキュリティゾーン出力 UUID(続き)																															
	セキュリティゾーン出力 UUID(続き)																															
	セキュリティゾーン出力 UUID(続き)																															
	接続タイムスタンプ																															
	接続インスタンス ID																接続数カウンタ															
	送信元の国																宛先の国															

次の表は、各侵入イベント レコード データ フィールドについての説明です。



表 B-3 侵入イベントレコード 5.2.x のフィールド

フィールド	データタイプ	説明
ブロックタイプ	uint32	侵入イベントデータブロックを開始します。この値は常に 34 です。
ブロック長	uint32	侵入イベントデータブロックのバイトの合計数(侵入イベントブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID	uint32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 <a href="#">管理対象デバイスレコードのメタデータ (3-36 ページ)</a> を参照してください。
イベント ID (Event ID)	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
イベントマイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒(100 万分の 1 秒)単位の増分。
ルール ID (シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルールリビジョン	uint32	ルールリビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポートまたは ICMP タイプ	uint16	イベントプロトコルタイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
送信先ポートまたは ICMP コード	uint16	イベントプロトコルタイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none"> <li>• 0:IP</li> <li>• 1:ICMP</li> <li>• 6:TCP</li> <li>• 17:UDP</li> </ul>

表 B-3 侵入イベント レコード 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
影響フラグ	bits[8]	<p>イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。</li> <li>0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。</li> <li>0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。</li> <li>0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。</li> <li>0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。</li> <li>0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。</li> <li>0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。</li> <li>0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ)</li> </ul> <p>次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。</p> <ul style="list-style-type: none"> <li>(0、不明):00X00000</li> <li>赤(1、脆弱):xxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx(バージョン 5.0+ のみ)</li> <li>オレンジ(2、潜在的に脆弱):00X0011X</li> <li>黄(3、現在は脆弱でない):00X0001X</li> <li>青(4、不明なターゲット):00X00001</li> </ul>
影響	uint8	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>1:レッド(脆弱)</li> <li>2:オレンジ(脆弱の可能性あり)</li> <li>3:イエロー(現在は脆弱でない)</li> <li>4:ブルー(不明なターゲット)</li> <li>5:グレー(不明なインパクト)</li> </ul>

表 B-3 侵入イベントレコード 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 <ul style="list-style-type: none"> <li>0: ブロックされていない</li> <li>1: ブロックされた</li> <li>2: ブロックされた可能性がある(設定では許可されていない)</li> </ul>
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970年1月1日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。

表 B-3 侵入イベント レコード 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。

## 侵入イベント レコード 5.3

侵入イベントレコードのフィールドは、次の図で網掛けされています。レコードタイプは 400 であり、ブロックタイプはデータブロックのシリーズ 2 セットの 41 です。

eStreamer からの 5.3 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベントタイプコード 12 およびバージョン 6 を要求します(拡張要求の送信の詳細については、[拡張要求の送信 \(2-4 ページ\)](#) を参照してください)。

バージョン 5.3 の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。接続の秒、接続インスタンス、および接続数カウンタは、侵入イベントに関連付けられた接続イベントの、1 つの固有識別子を形成します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ヘッダーバージョン(1)																メッセージタイプ(4)																
メッセージ長																																
Netmap ID																レコードタイプ(400)																
レコード長																																
eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																																
将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																																
ブロックタイプ(41)																																
ブロック長																																
デバイス ID																																
イベント ID(Event ID)																																
イベント秒																																
イベントマイクロ秒																																

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	ルール ID (シグネチャ ID)																															
	ジェネレータ ID																															
	ルール リビジョン																															
	分類 ID																															
	プライオリティ ID																															
	送信元 IP アドレス 送信元 IP アドレス (続き) 送信元 IP アドレス (続き) 送信元 IP アドレス (続き)																															
	宛先 IP アドレス 宛先 IP アドレス (続き) 宛先 IP アドレス (続き) 宛先 IP アドレス (続き)																															
	送信元ポートまたは ICMP タイプ																送信先ポートまたは ICMP コード															
	IP プロトコル ID								影響フラグ								影響								ブロック							
	MPLS ラベル																															
	VLAN ID (Admin. VLAN ID)																パッド															
	ポリシー UUID ポリシー UUID (続き) ポリシー UUID (続き) ポリシー UUID (続き)																															
	ユーザ ID (User ID)																															
	Web アプリケーション ID																															
	クライアント アプリケーション ID																															
	アプリケーション プロトコル ID																															

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

次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 B-4 侵入イベント レコード 5.3 のフィールド

フィールド	データタイプ	説明
ブロックタイプ	uint32	侵入イベント データ ブロックを開始します。この値は常に 34 です。
ブロック長	uint32	侵入イベント データ ブロックのバイトの合計数(侵入イベント ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID	uint32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 <a href="#">管理対象デバイス レコードのメタデータ (3-36 ページ)</a> を参照してください。
イベント ID (Event ID)	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
イベント マイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒(100 万分の 1 秒)単位の増分。
ルール ID (シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルール リビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポートまたは ICMP タイプ	uint16	イベントプロトコルタイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
送信先ポートまたは ICMP コード	uint16	イベントプロトコルタイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none"> <li>• 0:IP</li> <li>• 1:ICMP</li> <li>• 6:TCP</li> <li>• 17:UDP</li> </ul>

表 B-4 侵入イベント レコード 5.3 のフィールド(続き)

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



表 B-4 侵入イベントレコード5.3 のフィールド(続き)

フィールド	データタイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 <ul style="list-style-type: none"> <li>0: ブロックされていない</li> <li>1: ブロックされた</li> <li>2: ブロックされた可能性がある(設定では許可されていない)</li> </ul>
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970年1月1日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。

表 B-4 侵入イベントレコード5.3のフィールド(続き)

フィールド	データタイプ	説明
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。

## 侵入イベントレコード 5.1.1.x

侵入イベントレコードのフィールドは、次の図で網掛けされています。レコードタイプは 400 で、ブロックタイプは 25 です。

eStreamer からの 5.1.1 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベントタイプコード 12 およびバージョン 4 を要求します(拡張要求の送信の詳細については、[拡張要求の送信 \(2-4 ページ\)](#)を参照してください)。

バージョン 5.1.1.x の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。接続の秒、接続インスタンス、および接続数カウンタは、侵入イベントに関連付けられた接続イベントの、1 つの固有識別子を形成します。

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ルール ID(シグネチャ ID)																															
	ジェネレータ ID																															
	ルール リビジョン																															
	分類 ID																															
	プライオリティ ID																															
	送信元 IP アドレス																															
	送信元 IP アドレス(続き)																															
	送信元 IP アドレス(続き)																															
	送信元 IP アドレス(続き)																															
	宛先 IP アドレス																															
	宛先 IP アドレス(続き)																															
	宛先 IP アドレス(続き)																															
	宛先 IP アドレス(続き)																															
	送信元ポート/ICMP タイプ																宛先ポート/ICMP コード															
	IP プロトコル ID								影響フラグ								影響								ブロック							
	MPLS ラベル																															
	VLAN ID (Admin. VLAN ID)																パッド															
	ポリシー UUID																															
	ポリシー UUID(続き)																															
	ポリシー UUID(続き)																															
	ポリシー UUID(続き)																															
	ユーザ ID (User ID)																															
	Web アプリケーション ID																															
	クライアント アプリケーション ID																															
	アプリケーション プロトコル ID																															

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

次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 B-5 侵入イベントレコード 5.1.1 のフィールド

フィールド	データタイプ	説明
ブロックタイプ	uint32	侵入イベントデータブロックを開始します。この値は常に 25 です。
ブロック長	uint32	侵入イベントデータブロックのバイトの合計数(侵入イベントブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID	uint32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 <a href="#">管理対象デバイスレコードのメタデータ (3-36 ページ)</a> を参照してください。
イベント ID (Event ID)	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
イベントマイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒(100 万分の 1 秒)単位の増分。
ルール ID (シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システムプリプロセッサの ID 番号。
ルールリビジョン	uint32	ルールリビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポート/ICMP タイプ	uint16	イベントプロトコルタイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
宛先ポート/ICMP コード	uint16	イベントプロトコルタイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none"> <li>• 0:IP</li> <li>• 1:ICMP</li> <li>• 6:TCP</li> <li>• 17:UDP</li> </ul>

表 B-5 侵入イベント レコード 5.1.1 のフィールド(続き)

フィールド	データタイプ	説明
影響フラグ	bits[8]	<p>イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。</li> <li>0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。</li> <li>0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。</li> <li>0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。</li> <li>0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。</li> <li>0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。</li> <li>0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。</li> <li>0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。</li> </ul> <p>次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。</p> <ul style="list-style-type: none"> <li>(0、不明):00x00000</li> <li>赤(1、脆弱):xxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx</li> <li>オレンジ(2、潜在的に脆弱):00x00111</li> <li>黄(3、現在は脆弱でない):00x00011</li> <li>青(4、不明なターゲット):00x00001</li> </ul>
影響	uint8	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>1:レッド(脆弱)</li> <li>2:オレンジ(脆弱の可能性あり)</li> <li>3:イエロー(現在は脆弱でない)</li> <li>4:ブルー(不明なターゲット)</li> <li>5:グレー(不明なインパクト)</li> </ul>

表 B-5 侵入イベントレコード5.1.1のフィールド(続き)

フィールド	データタイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 <ul style="list-style-type: none"> <li>0: ブロックされていない</li> <li>1: ブロックされた</li> <li>2: ブロックされた可能性がある(設定では許可されていない)</li> </ul>
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970年1月1日からの経過秒数)。

表 B-5 侵入イベントレコード5.1.1のフィールド(続き)

フィールド	データタイプ	説明
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数值 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。

## 侵入イベントレコード 5.3.1

侵入イベントレコードのフィールドは、次の図で網掛けされています。レコードタイプは 400 であり、ブロックタイプはシリーズ 2 セットのデータブロックの 42 です。

eStreamer からの 5.3.1 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベントタイプコード 12 およびバージョン 7 を要求します(拡張要求の送信の詳細については、[拡張要求の送信 \(2-4 ページ\)](#)を参照してください)。

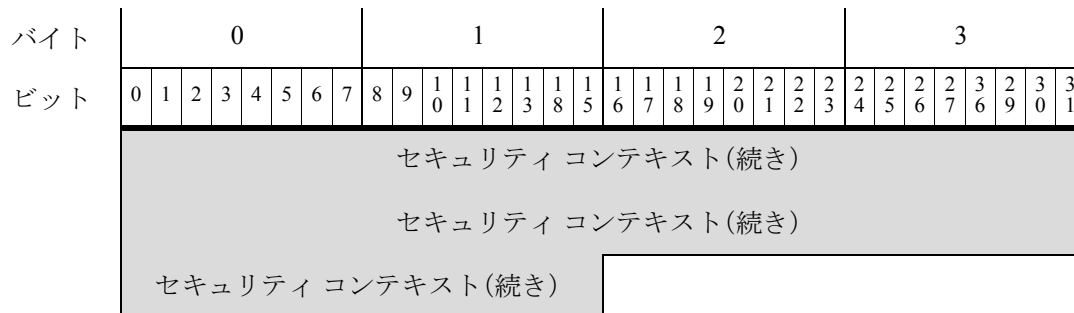
バージョン 5.3.1 の侵入イベントの場合、イベント ID、管理対象デバイス ID、イベント秒により固有識別子が形成されます。接続の秒、接続インスタンス、および接続数カウンタは、侵入イベントに関連付けられた接続イベントの、1 つの固有識別子を形成します。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(400)															
	レコード長																															
	eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
	ブロックタイプ(42)																															
	ブロック長																															
	デバイス ID(Device ID)																															
	イベント ID(Event ID)																															
	イベント秒																															
	イベントマイクロ秒																															
	ルール ID(シグネチャ ID)																															



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ジェネレータ ID																																
ルール リビジョン																																
分類 ID																																
プライオリティ ID																																
送信元 IP アドレス																																
送信元 IP アドレス (続き)																																
送信元 IP アドレス (続き)																																
送信元 IP アドレス (続き)																																
宛先 IP アドレス																																
宛先 IP アドレス (続き)																																
宛先 IP アドレス (続き)																																
宛先 IP アドレス (続き)																																
送信元ポートまたは ICMP タイプ																送信先ポートまたは ICMP コード																
IP プロトコル ID								影響フラグ								影響								ブロック								
MPLS ラベル																																
VLAN ID (Admin. VLAN ID)																パッド																
ポリシー UUID																																
ポリシー UUID (続き)																																
ポリシー UUID (続き)																																
ポリシー UUID (続き)																																
ユーザ ID (User ID)																																
Web アプリケーション ID																																
クライアント アプリケーション ID																																
アプリケーション プロトコル ID																																
アクセス コントロール ルール ID																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
アクセス コントロール ポリシー UUID																																
アクセス コントロール ポリシー UUID (続き)																																
アクセス コントロール ポリシー UUID (続き)																																
アクセス コントロール ポリシー UUID (続き)																																
インターフェイス入力 UUID																																
インターフェイス入力 UUID (続き)																																
インターフェイス入力 UUID (続き)																																
インターフェイス入力 UUID (続き)																																
インターフェイス出力 UUID																																
インターフェイス出力 UUID (続き)																																
インターフェイス出力 UUID (続き)																																
インターフェイス出力 UUID (続き)																																
セキュリティゾーン入力 UUID																																
セキュリティゾーン入力 UUID (続き)																																
セキュリティゾーン入力 UUID (続き)																																
セキュリティゾーン入力 UUID (続き)																																
セキュリティゾーン出力 UUID																																
セキュリティゾーン出力 UUID (続き)																																
セキュリティゾーン出力 UUID (続き)																																
セキュリティゾーン出力 UUID (続き)																																
接続タイムスタンプ																																
接続インスタンス ID																接続数カウンタ																
送信元の国																宛先の国																
IOC 番号																セキュリティ コンテキスト																
セキュリティ コンテキスト (続き)																																



次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 B-6 侵入イベント レコード 5.3.1 のフィールド

フィールド	データタイプ	説明
ブロックタイプ	uint32	侵入イベント データ ブロックを開始します。この値は常に 42 です。
ブロック長	uint32	侵入イベント データ ブロックのバイトの合計数(侵入イベント ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID (Device ID)	uint32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 <a href="#">管理対象デバイス レコードのメタデータ (3-36 ページ)</a> を参照してください。
イベント ID (Event ID)	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
イベントマイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒(100 万分の 1 秒)単位の増分。
ルール ID(シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルールリビジョン	uint32	ルール リビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。

表 B-6 侵入イベントレコード5.3.1のフィールド(続き)

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

表 B-6 侵入イベントレコード 5.3.1 のフィールド(続き)

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

表 B-6 侵入イベントレコード5.3.1のフィールド(続き)

フィールド	データタイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 <ul style="list-style-type: none"> <li>0:ブロックされていない</li> <li>1:ブロックされた</li> <li>2:ブロックされた可能性がある(設定では許可されていない)</li> </ul>
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970年1月1日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。

表 B-6 侵入イベント レコード 5.3.1 のフィールド(続き)

フィールド	データタイプ	説明
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト (仮想ファイアウォール) の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

## 侵入イベント レコード 5.4.x

侵入イベント レコードのフィールドは、次の図で網掛けされています。レコードタイプは 400 であり、ブロックタイプはシリーズ 2 セットのデータブロックの 45 です。これはブロックタイプ 42 に取って代わり、ブロックタイプ 60 により取って代わられます。SSL サポート用およびネットワーク分析ポリシー用のフィールドが追加されました。

eStreamer からの 5.4.x 侵入イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベントタイプコード 12 およびバージョン 8 を要求します (拡張要求の送信の詳細については、[拡張要求の送信 \(2-4 ページ\)](#) を参照してください)。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダー バージョン (1)																メッセージ タイプ (4)															
	メッセージ長																															
	Netmap ID																レコード タイプ (400)															
	レコード長																															
	eStreamer サーバ タイムスタンプ (イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み (イベントでビット 23 が設定されている場合のみ)																															
	ブロック タイプ (45)																															
	ブロック長																															
	デバイス ID (Device ID)																															
	イベント ID (Event ID)																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	イベント秒																															
	イベント マイクロ秒																															
	ルール ID(シグネチャ ID)																															
	ジェネレータ ID																															
	ルール リビジョン																															
	分類 ID																															
	プライオリティ ID																															
	送信元 IP アドレス																															
	送信元 IP アドレス(続き)																															
	送信元 IP アドレス(続き)																															
	送信元 IP アドレス(続き)																															
	宛先 IP アドレス																															
	宛先 IP アドレス(続き)																															
	宛先 IP アドレス(続き)																															
	宛先 IP アドレス(続き)																															
	送信元ポートまたは ICMP タイプ																送信先ポートまたは ICMP コード															
	IP プロトコル ID								影響フラグ								影響								ブロック							
	MPLS ラベル																															
	VLAN ID (Admin. VLAN ID)																パッド															
	ポリシー UUID																															
	ポリシー UUID(続き)																															
	ポリシー UUID(続き)																															
	ポリシー UUID(続き)																															
	ユーザ ID (User ID)																															
	Web アプリケーション ID																															



バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
ビット																																	
	クライアント アプリケーション ID																																
	アプリケーション プロトコル ID																																
	アクセス コントロール ルール ID																																
	アクセス コントロール ポリシー UUID																																
	アクセス コントロール ポリシー UUID (続き)																																
	アクセス コントロール ポリシー UUID (続き)																																
	アクセス コントロール ポリシー UUID (続き)																																
	インターフェイス 入力 UUID																																
	インターフェイス 入力 UUID (続き)																																
	インターフェイス 入力 UUID (続き)																																
	インターフェイス 入力 UUID (続き)																																
	インターフェイス 出力 UUID																																
	インターフェイス 出力 UUID (続き)																																
	インターフェイス 出力 UUID (続き)																																
	インターフェイス 出力 UUID (続き)																																
	セキュリティ ゾーン 入力 UUID																																
	セキュリティ ゾーン 入力 UUID (続き)																																
	セキュリティ ゾーン 入力 UUID (続き)																																
	セキュリティ ゾーン 入力 UUID (続き)																																
	セキュリティ ゾーン 出力 UUID																																
	セキュリティ ゾーン 出力 UUID (続き)																																
	セキュリティ ゾーン 出力 UUID (続き)																																
	セキュリティ ゾーン 出力 UUID (続き)																																
	接続 タイムスタンプ																																

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

次の表は、各侵入イベント レコード データ フィールドについての説明です。

表 B-7 侵入イベント レコード 5.4.x のフィールド

フィールド	データ タイプ	説明
ブロック タイプ	uint32	侵入イベント データ ブロックを開始します。この値は常に 45 です。
ブロック長	uint32	侵入イベント データ ブロックのバイトの合計数(侵入イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。

表 B-7 侵入イベントレコード 5.4.x のフィールド(続き)

フィールド	データタイプ	説明
デバイス ID (Device ID)	uint32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 <a href="#">管理対象デバイスレコードのメタデータ (3-36 ページ)</a> を参照してください。
イベント ID (Event ID)	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
イベントマイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒(100 万分の 1 秒)単位の増分。
ルール ID(シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した Firepower システム プリプロセッサの ID 番号。
ルールリビジョン	uint32	ルールリビジョン番号。
分類 ID	uint32	イベント分類メッセージの ID 番号。
プライオリティ ID	uint32	イベントに関連付けられている優先順位の ID 番号。
送信元 IP アドレス	uint8[16]	イベントで使用される送信元 IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	イベントで使用される宛先 IPv4 または IPv6 アドレス。
送信元ポート または ICMP タイプ	uint16	イベントプロトコルタイプが TCP または UDP の場合は送信元ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のタイプ。
送信先ポート または ICMP コード	uint16	イベントプロトコルタイプが TCP または UDP の場合は宛先ポート番号、またはイベントが ICMP トラフィックによって引き起こされた場合は ICMP のコード。
IP プロトコル 番号	uint8	IANA 指定のプロトコル番号。次に例を示します。 <ul style="list-style-type: none"> <li>• 0:IP</li> <li>• 1:ICMP</li> <li>• 6:TCP</li> <li>• 17:UDP</li> </ul>

表 B-7 侵入イベントレコード5.4.xのフィールド(続き)

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

表 B-7 侵入イベントレコード 5.4.x のフィールド(続き)

フィールド	データタイプ	説明
ブロック	uint8	イベントがブロックされたかどうかを示す値。 <ul style="list-style-type: none"> <li>0: ブロックされていない</li> <li>1: ブロックされた</li> <li>2: ブロックされた可能性がある(設定では許可されていない)</li> </ul>
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
入力インターフェイス UUID	uint8[16]	入力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
出力インターフェイス UUID	uint8[16]	出力インターフェイスの固有識別子として機能するインターフェイス ID 番号。
入力セキュリティゾーン UUID	uint8[16]	入力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
出力セキュリティゾーン UUID	uint8[16]	出力セキュリティゾーンの固有識別子として機能するゾーン ID 番号。
接続タイムスタンプ	uint32	侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(1970年1月1日からの経過秒数)。
接続インスタンス ID	uint16	接続イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。

表 B-7 侵入イベントレコード 5.4.x のフィールド(続き)

フィールド	データタイプ	説明
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティコンテキスト	uint8[16]	トラフィックが通過したセキュリティコンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキストモードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
実際の SSL アクション	uint16	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• 0:「不明」</li> <li>• 1:「復号しない」</li> <li>• 2:「ブロックする」</li> <li>• 3:「リセットでブロック」</li> <li>• 4:「復号(既知のキー)」</li> <li>• 5:「復号(置換キー)」</li> <li>• 6:「復号(Resign)」</li> </ul>

表 B-7 侵入イベントレコード 5.4.x のフィールド(続き)

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

## 侵入影響アラート データ

侵入影響アラート イベントには、影響イベントに関する情報が含まれます。これは、侵入イベントがシステム ネットワーク マップ データと比較され、影響が判別されているときに送信されます。これはレコードタイプ 9 の標準レコードヘッダーを使用し、シリーズ 1 グループのブロックの、データブロックタイプが 20 である侵入影響アラートデータブロックが続きます。(影響アラートデータブロックタイプは、シリーズ 1 データブロックです。シリーズ 1 データブロックの詳細については、[ディスカバリ \(シリーズ 1\) ブロック \(4-63 ページ\)](#) を参照してください。)

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(9)															
	レコード長																															
	侵入影響アラートブロックタイプ(20)																															
	侵入影響アラートブロック長																															
	イベント ID(Event ID)																															
	デバイス ID																															
	イベント秒																															
	影響																															
	送信元 IP アドレス																															
	宛先 IP アドレス																															
影響説明	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	説明...																															

次の表は、影響イベントの各データフィールドについての説明です。



表 B-8 影響イベントデータフィールド

フィールド	データタイプ	説明
侵入影響アラートブロックタイプ	uint32	侵入影響アラートデータブロックが続くことを示します。このフィールドの値は、常に 20 です。 <a href="#">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)</a> を参照してください。
侵入影響アラートブロック長	uint32	侵入の影響アラートのブロックタイプの長さを示します。後続のすべてのデータ、および侵入の影響アラートのブロックタイプと長さの 8 バイトを含みます。
イベント ID (Event ID)	uint32	イベント ID 番号を表示します。
デバイス ID	uint32	管理対象デバイス ID 番号を表示します。
イベント秒	uint32	イベントが検出された秒(1970年1月1日からの経過秒数)を示します。

表 B-8 影響イベントデータフィールド(続き)

フィールド	データタイプ	説明
影響	bits[8]	<p>イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。</li> <li>0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。</li> <li>0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。</li> <li>0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。</li> <li>0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。</li> <li>0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。</li> <li>0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれません。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。</li> <li>0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ)</li> </ul> <p>次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。</p> <ul style="list-style-type: none"> <li>(0、不明):00x00000</li> <li>赤(1、脆弱):xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx (バージョン 5.0+ のみ)</li> <li>オレンジ(2、潜在的に脆弱):00x0011x</li> <li>黄(3、現在は脆弱でない):00x0001x</li> <li>青(4、不明なターゲット):00x00001</li> </ul>
送信元 IP アドレス	uint8[4]	IP アドレス オクテットの、影響イベントに関連付けられているホストの IP アドレス。
宛先 IP アドレス	uint8[4]	IP アドレス オクテットの、影響イベントに関連付けられている宛先 IP アドレスの IP アドレス(該当する場合)。宛先 IP アドレスがない場合、この値は 0 です。
文字列ブロックタイプ	uint32	影響名を含む文字列データのブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、 <a href="#">文字列データブロック(4-73 ページ)</a> を参照してください。

表 B-8 影響イベント データ フィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数。これには文字列ブロックタイプ用の4バイト、文字列ブロック長用の4バイト、および説明のバイト数が含まれます。
説明	string	影響イベントについての説明。

## レガシー マルウェア イベントのデータ構造

- [マルウェア イベントのデータ ブロック 5.1 \(B-51 ページ\)](#)
- [マルウェア イベント データ ブロック 5.1.1.x \(B-55 ページ\)](#)
- [マルウェア イベント データ ブロック 5.2.x \(B-61 ページ\)](#)
- [マルウェア イベントのデータ ブロック 5.3 \(B-68 ページ\)](#)
- [マルウェア イベント データ ブロック 5.3.1 \(B-76 ページ\)](#)
- [マルウェア イベント データ ブロック 5.4.x \(B-83 ページ\)](#)

### マルウェア イベントのデータ ブロック 5.1

eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェア イベント データ ブロックのブロックタイプは、シリーズ 2 グループの 16 です。マルウェア イベント レコードの一部としてイベントを要求するには、イベント バージョン 1 およびイベント コード 101 の要求メッセージ内に、マルウェア イベント フラグ(要求フラグ フィールドのビット 30)を設定します。

次の図は、マルウェア イベント データ ブロックの構造を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
マルウェア イベント ブロック タイプ (16)																																
マルウェア イベントのブロック長																																
エージェント UUID																																
エージェント UUID(続き)																																
エージェント UUID(続き)																																
エージェント UUID(続き)																																

レガシー マルウェア イベントのデータ構造

バイト	0								1								2								3																																												
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31																																					
ビット																																																																					
	クラウド UUID																																																																				
	クラウド UUID(続き)																																																																				
	クラウド UUID(続き)																																																																				
	クラウド UUID(続き)																																																																				
	Timestamp																																																																				
	イベント タイプ ID																																																																				
	イベント サブタイプ ID								ホスト IP アドレス																																																												
検出名	ホスト IP アドレス(続き)								ディテクタ ID								文字列ブロック タイプ(0)																																																				
	文字列ブロック タイプ(0) (続き)																文字列ブロック長																																																				
	文字列ブロック長(続き)																検出名...																																																				
ユーザ(User)	文字列ブロック タイプ(0)																																																																				
	文字列ブロック長																																																																				
	ユーザ...																																																																				
ファイル名	文字列ブロック タイプ(0)																																																																				
	文字列ブロック長																																																																				
	ファイル名...																																																																				
ファイルパス	文字列ブロック タイプ(0)																																																																				
	文字列ブロック長																																																																				
	ファイルパス...																																																																				
ファイル SHA ハッシュ	文字列ブロック タイプ(0)																																																																				
	文字列ブロック長																																																																				
	ファイル SHA ハッシュ...																																																																				
	ファイル サイズ(File size)																																																																				
	ファイル タイプ								ファイルのタイムスタンプ																																																												

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
親ファイル [名前(Name) ]	ファイルのタイムスタンプ (続き)								文字列ブロック タイプ(0)																							
	文字列ブロック タイプ(0) (続き)								文字列ブロック長																							
	文字列ブロック 長(続き)								親ファイル名...																							
親ファイル SHA ハッ シュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル SHA ハッシュ...																															
イベント 説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	イベントの説明...																															

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

表 B-9 マルウェア イベント データ ブロックのフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 16 です。
マルウェア イベントのブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数 (マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする AMP for Endpoints エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェア イベントの発生元であるマルウェア 認識 ネットワークの、内部の固有 ID。
Timestamp	uint32	マルウェア イベント生成時のタイムスタンプ。
イベント タイプ ID	uint32	マルウェア イベント タイプの内部 ID。
イベント サブタイプ ID	uint8	マルウェア 検出につながったアクションの内部 ID。
ホスト IP アドレス	uint32	マルウェア イベントに関連付けられているホスト IP アドレス。
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。

表 B-9 マルウェアイベントデータブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロックタイプ	uint32	検出名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	検出名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロックタイプ	uint32	ユーザ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびユーザフィールドのバイト数を含む)。
ユーザ (User)	string	シスコ Agent がインストールされ、マルウェアイベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリーには関係ないことに注意してください。
文字列ブロックタイプ	uint32	ファイル名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロックタイプ	uint32	ファイルパスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイルパス文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびファイルパスフィールドのバイト数を含む)。
ファイルパス	string	検出または検疫されたファイルのファイルパス。ファイル名は含まれません。
文字列ブロックタイプ	uint32	ファイル SHA ハッシュを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびファイル SHA ハッシュフィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値。
ファイルサイズ (File size)	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイルタイプ	uint8	検出または検疫されたファイルのファイルタイプ。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成タイムスタンプ。
文字列ブロックタイプ	uint32	親ファイル名を含む文字列データブロックを開始します。この値は常に 0 です。

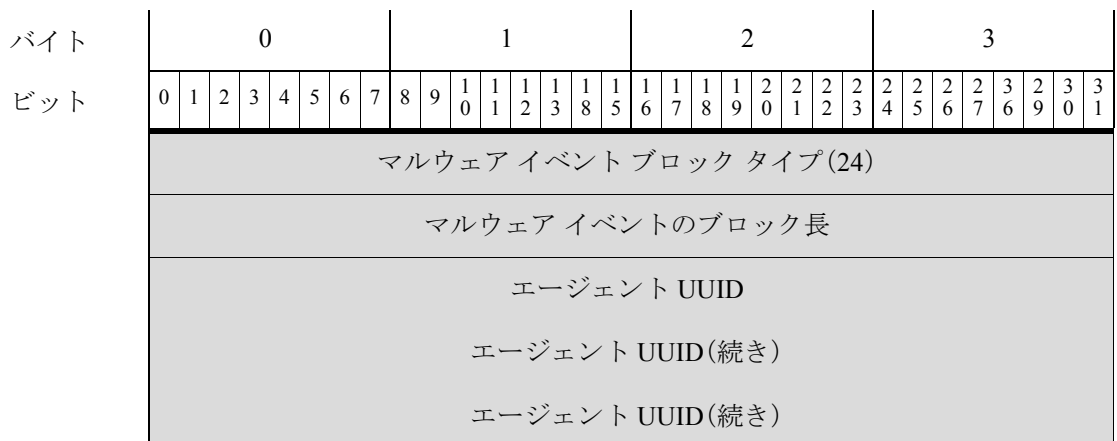
表 B-9 マルウェア イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	親ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロック タイプ	uint32	親ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル SHA ハッシュ フィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロック タイプ	uint32	イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベント タイプに関連付けられている追加イベント情報。

## マルウェア イベント データ ブロック 5.1.1.x

eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザーに関する情報が含まれています。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 24 です。マルウェア イベント レコードの一部として、イベント バージョン 2 およびイベント コード 101 の要求メッセージ内にマルウェア イベント フラグ(要求フラグ フィールドのビット 30)を設定して、イベントを要求します。

次の図は、マルウェア イベント データ ブロックの構造を示しています。



レガシー マルウェア イベントのデータ構造

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



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

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

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

表 B-10 マルウェア イベント データ ブロック 5.1.1.x のフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 24 です。
マルウェア イベント のブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする AMP for Endpoints エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェア イベントの発生元であるマルウェア認識ネットワークの、内部の固有 ID。
マルウェア イベント タイムスタンプ	uint32	マルウェア イベント生成時のタイムスタンプ。
イベント タイプ ID	uint32	マルウェア イベント タイプの内部 ID。
イベント サブタイプ ID	uint8	マルウェア 検出につながったアクションの内部 ID。
ホスト IP アドレス	uint32	マルウェア イベントに関連付けられているホスト IP アドレス。
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。
文字列ブロック タイプ	uint32	検出名を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-10 マルウェア イベント データ ブロック 5.1.1.x のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	検出名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロック タイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ フィールドのバイト数を含む)。
ユーザ (User)	string	シスコ Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリーには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイルパスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイルパス文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイルパス フィールドのバイト数を含む)。
ファイルパス	string	検出または検疫されたファイルのファイルパス。ファイル名は含まれません。
文字列ブロック タイプ	uint32	ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル SHA ハッシュ フィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値のレンダリングされた文字列。
ファイル サイズ (File size)	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイル タイプ	uint8	検出または検疫されたファイルのファイル タイプ。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
文字列ブロック タイプ	uint32	親ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-10 マルウェア イベント データ ブロック 5.1.1.x のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	親ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロック タイプ	uint32	親ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル SHA ハッシュフィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロック タイプ	uint32	イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベント タイプに関連付けられている追加イベント情報。
デバイス ID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または IDS イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続イベント タイムスタンプ	uint32	接続イベントのタイムスタンプ。
方向(Direction)	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示します。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>• 1:ダウンロード</li> <li>• 2:アップロード</li> </ul> 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID(Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID(User ID)	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。

表 B-10 マルウェア イベント データ ブロック 5.1.1.x のフィールド(続き)

フィールド	データ タイプ	説明
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する ID 番号。
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>1 (CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。</li> <li>2 (UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。</li> <li>3 (MALWARE): ファイルにはマルウェアが含まれています。</li> <li>4 (CACHE_MISS): ソフトウェアは シスコ クラウド に特性を確認する要求を送信できませんでした。</li> <li>5 (NO_CLOUD_RESP): シスコ クラウド サービスが 要求に応答しませんでした。</li> </ul>
レトロスペクティブ 特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロック タイプ	uint32	URI を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。

## マルウェア イベント データ ブロック 5.2.x

eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 33 です。マルウェア イベント レコードの一部として、イベント バージョン 3 およびイベント コード 101 の要求メッセージ内にマルウェア イベント フラグ(要求フラグ フィールドのビット 30)を設定して、イベントを要求します。

次の図は、マルウェア イベント データ ブロックの構造を示しています。

レガシー マルウェア イベントのデータ構造

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	マルウェア イベントのブロック タイプ (33)																															
	マルウェア イベントのブロック長																															
	エージェント UUID エージェント UUID (続き) エージェント UUID (続き) エージェント UUID (続き)																															
	クラウド UUID クラウド UUID (続き) クラウド UUID (続き) クラウド UUID (続き)																															
	マルウェア イベント タイムスタンプ																															
	イベント タイプ ID																															
検出名	イベント サブタイプ ID								ディテクタ ID								文字列ブロック タイプ (0)															
	文字列ブロック タイプ (0) (続き)																文字列ブロック長															
	文字列ブロック長 (続き)																検出名...															
ユーザ (User)	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイル名...																															
ファイルパス	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイルパス...																															

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

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

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

表 B-11 マルウェア イベント データ ブロック 5.2.x のフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 33 です。
マルウェア イベント のブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数 (マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。



表 B-11 マルウェア イベント データ ブロック 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
エージェント UUID	uint8[16]	マルウェア イベントをレポートする AMP for Endpoints エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェア イベントの発生元であるマルウェア 認識 ネットワークの、内部の固有 ID。
マルウェア イベント タイムスタンプ	uint32	マルウェア イベント生成時のタイムスタンプ。
イベント タイプ ID	uint32	マルウェア イベント タイプの内部 ID。
イベント サブタイプ ID	uint8	マルウェア 検出につながったアクションの内部 ID。
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。
文字列ブロック タイプ	uint32	検出名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	検出名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダーフィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロック タイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダーフィールド用の 8 バイト、およびユーザ フィールドのバイト数を含む)。
ユーザ (User)	string	シスコ Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダーフィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイル パスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイルパス文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダーフィールド用の 8 バイト、およびファイルパス フィールドのバイト数を含む)。
ファイル パス	string	検出または検疫されたファイルのファイル パス。ファイル名は含まれません。
文字列ブロック タイプ	uint32	ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-11 マルウェア イベント データ ブロック 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル SHA ハッシュ フィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値のレンダリングされた文字列。
ファイル サイズ (File size)	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイル タイプ	uint8	検出または検疫されたファイルのファイル タイプ。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
文字列ブロック タイプ	uint32	親ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロック タイプ	uint32	親ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル SHA ハッシュ フィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロック タイプ	uint32	イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベント タイプに関連付けられている追加イベント情報。
デバイス ID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または IDS イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続イベント タイムスタンプ	uint32	接続イベントのタイムスタンプ。

表 B-11 マルウェア イベント データ ブロック 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
方向 (Direction)	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示します。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>1: ダウンロード</li> <li>2: アップロード</li> </ul> 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID (User ID)	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する ID 番号。
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>1 (CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。</li> <li>2 (NEUTRAL): ファイルにマルウェアが含まれているかどうかは不明です。</li> <li>3 (MALWARE): ファイルにはマルウェアが含まれています。</li> <li>4 (CACHE_MISS): ソフトウェアから シスコ クラウドに対して、特性を確認する要求を送信できなかったか、またはシスコクラウドサービスが要求に応答しませんでした。</li> </ul>
レトロスペクティブ 特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロック タイプ	uint32	URI を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データ ブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。

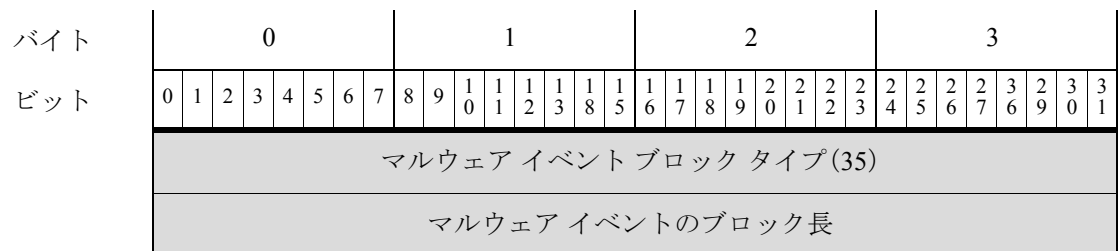
表 B-11 マルウェアイベントデータブロック 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
操作	uint8	ファイルタイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>• 1:検出</li> <li>• 2:ブロック</li> <li>• 3:マルウェアクラウドルックアップ</li> <li>• 4:マルウェアブロック</li> <li>• 5:マルウェアホワイトリスト</li> </ul>
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> <li>• 1:ICMP</li> <li>• 4:IP</li> <li>• 6:TCP</li> <li>• 17:UDP</li> </ul> これは現時点では TCP のみです。

## マルウェアイベントのデータブロック 5.3

eStreamer サービスは、マルウェアイベントに関する情報を保存するために、マルウェアイベントデータブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェアイベントデータブロックのブロックタイプは、シリーズ 2 グループの 35 です。マルウェアイベントレコードの一部として、イベントバージョン 4 およびイベントコード 101 の要求メッセージ内にマルウェアイベントフラグ(要求フラグフィールドのビット 30)を設定して、イベントを要求します。

次の図は、マルウェアイベントデータブロックの構造を示しています。



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

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

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

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

表 B-12 マルウェアイベントデータブロック 5.3 のフィールド

フィールド	データタイプ	説明
マルウェアイベントブロックタイプ	uint32	マルウェアイベントデータブロックを開始します。この値は常に 35 です。
マルウェアイベントのブロック長	uint32	マルウェアイベントデータブロックのバイトの合計数(マルウェアイベントブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェアイベントをレポートする AMP for Endpoints エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェアイベントの発生元であるマルウェア認識ネットワークの、内部の固有 ID。
マルウェアイベントタイムスタンプ	uint32	マルウェアイベント生成時のタイムスタンプ。
イベントタイプ ID	uint32	マルウェアイベントタイプの内部 ID。
イベントサブタイプ ID	uint32	マルウェア検出につながったアクションの内部 ID。
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。
文字列ブロックタイプ	uint32	検出名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	検出名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロックタイプ	uint32	ユーザ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびユーザフィールドのバイト数を含む)。
ユーザ (User)	string	シスコ Agent がインストールされ、マルウェアイベントが発生したコンピュータのユーザ。これらのユーザはユーザディスカバリには関係ないことに注意してください。
文字列ブロックタイプ	uint32	ファイル名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロックタイプ	uint32	ファイルパスを含む文字列データブロックを開始します。この値は常に 0 です。



表 B-12 マルウェア イベント データ ブロック 5.3 のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	ファイルパス文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびファイルパスフィールドのバイト数を含む)。
ファイルパス	string	検出または検疫されたファイルのファイルパス。ファイル名は含まれません。
文字列ブロックタイプ	uint32	ファイルSHAハッシュを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	ファイルSHAハッシュ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびファイルSHAハッシュフィールドのバイト数を含む)。
ファイルSHAハッシュ	string	検出または検疫されたファイルのSHA-256ハッシュ値のレンダリングされた文字列。
ファイルサイズ (File size)	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイルタイプ	uint8	検出または検疫されたファイルのファイルタイプ。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、 <a href="#">エンドポイント向けAMPファイルタイプのメタデータ(3-43ページ)</a> を参照してください。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時のUNIXタイムスタンプ(1970年1月1日からの経過秒数)。
文字列ブロックタイプ	uint32	親ファイル名を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	親ファイル名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロックタイプ	uint32	親ファイルSHAハッシュを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	親ファイルSHAハッシュ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、および親ファイルSHAハッシュフィールドのバイト数を含む)。
親ファイルSHAハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルのSHA-256のハッシュ値。
文字列ブロックタイプ	uint32	イベントの説明を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	イベントの説明文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびイベントの説明フィールドのバイト数を含む)。

表 B-12 マルウェア イベント データ ブロック 5.3 のフィールド(続き)

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

表 B-12 マルウェア イベント データ ブロック 5.3 のフィールド(続き)

フィールド	データ タイプ	説明
レトロスペクティブ 特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロック タ イプ	uint32	URI を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データ ブロックに含まれるバイト数(ブロックタイプとヘッダー フィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
Web アプリケーショ ン ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプ リケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
操作	uint8	ファイルタイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>• 1: 検出</li> <li>• 2: ブロック</li> <li>• 3: マルウェア クラウド ルックアップ</li> <li>• 4: マルウェア ブロック</li> <li>• 5: マルウェア ホワイトリスト</li> </ul>
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> <li>• 1: ICMP</li> <li>• 4: IP</li> <li>• 6: TCP</li> <li>• 17: UDP</li> </ul> これは現時点では TCP のみです。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ~ 100)。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。

## マルウェア イベント データ ブロック 5.3.1

eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 44 です。これはブロック 35 に取って代わります。マルウェア イベント レコードの一部として、イベント バージョン 5 およびイベント コード 101 の要求メッセージ内にマルウェア イベント フラグ (要求フラグ フィールドのビット 30) を設定して、イベントを要求します。

次の図は、マルウェア イベント データ ブロックの構造を示しています。

バイト	0								1					2				3														
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	マルウェア イベント ブロック タイプ (44)																															
	マルウェア イベントのブロック長																															
	エージェント UUID																															
	エージェント UUID (続き)																															
	エージェント UUID (続き)																															
	エージェント UUID (続き)																															
	クラウド UUID																															
	クラウド UUID (続き)																															
	クラウド UUID (続き)																															
	クラウド UUID (続き)																															
	マルウェア イベント タイムスタンプ																															
	イベント タイプ ID																															
	イベント サブタイプ ID																															
検出名	ディテクタ ID								文字列ブロック タイプ (0)																							
	文字列ブロック タイプ (0) (続き)								文字列ブロック長																							
	文字列ブロック長 (続き)								検出名...																							

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ユーザ (User)	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイル名...																															
ファイルパス	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイルパス...																															
ファイル SHA ハッシュ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイル サイズ (File size)																															
	ファイル タイプ																															
	ファイルのタイムスタンプ																															
親ファイル [名前 (Name) ]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	親ファイル名...																															
親ファイル SHA ハッシュ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	親ファイル SHA ハッシュ...																															
イベント説明	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	イベントの説明...																															
デバイス ID (Device ID)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	接続インスタンス																接続数カウンタ															
	接続イベント タイムスタンプ																															
	方向 (Direction)								送信元 IP アドレス																							
									送信元 IP アドレス (続き)																							
									送信元 IP アドレス (続き)																							
									送信元 IP アドレス (続き)																							
	送信元 IP (続き)								宛先 IP アドレス																							
									宛先 IP アドレス (続き)																							
									宛先 IP アドレス (続き)																							
									宛先 IP アドレス (続き)																							
	宛先 IP (続き)								アプリケーション ID (Application ID)																							
	アプリケーション ID (続き)								ユーザ ID (User ID)																							
	ユーザ ID (続き)								アクセス コントロール ポリシー UUID																							
									アクセス コントロール ポリシー UUID (続き)																							
									アクセス コントロール ポリシー UUID (続き)																							
									アクセス コントロール ポリシー UUID (続き)																							
URI	アクセス コントロール ポリシー UUID (続き)								傾向								レトロスペクティブ傾向								文字列ブロックタイプ (0)							
	文字列ブロックタイプ (0) (続き)																文字列ブロック長															
	文字列ブロック長 (続き)																URI...															
	送信元ポート (Source Port)																接続先ポート															
	送信元の国																宛先の国															
	Web アプリケーション ID																															
	クライアント アプリケーション ID																															

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		
	操作								プロトコル								脅威スコア								IOC 番号															
	IOC 番号(続き)								セキュリティ コンテキスト																															
	セキュリティ コンテキスト (続き)								セキュリティ コンテキスト(続き)																															
									セキュリティ コンテキスト(続き)																															
									セキュリティ コンテキスト(続き)																															

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

表 B-13 マルウェア イベント データ ブロック 5.3.1 のフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 44 です。
マルウェア イベントのブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする AMP for Endpoints エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェア イベントの発生元 Cisco Advanced Malware Protection クラウドの、内部の固有 ID。
マルウェア イベント タイムスタンプ	uint32	マルウェア イベント生成時のタイムスタンプ。
イベント タイプ ID	uint32	マルウェア イベント タイプの内部 ID。
イベント サブタイプ ID	uint32	マルウェア 検出につながったアクションの内部 ID。
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。
文字列ブロック タイプ	uint32	検出名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	検出名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。
文字列ブロック タイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。

表 B-13 マルウェア イベント データ ブロック 5.3.1 のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ フィールドのバイト数を含む)。
ユーザ (User)	string	シスコ Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイルパスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイルパス文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイルパス フィールドのバイト数を含む)。
ファイルパス	string	検出または検疫されたファイルのファイルパス。ファイル名は含まれません。
文字列ブロック タイプ	uint32	ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル SHA ハッシュ フィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値のレンダリングされた文字列。
ファイル サイズ (File size)	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイル タイプ	uint8	検出または検疫されたファイルのファイルタイプ。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、 <a href="#">エンドポイント向け AMP ファイル タイプのメタデータ (3-43 ページ)</a> を参照してください。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
文字列ブロック タイプ	uint32	親ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。



表 B-13 マルウェア イベント データ ブロック 5.3.1 のフィールド(続き)

フィールド	データ タイプ	説明
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロック タイプ	uint32	親ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル SHA ハッシュ フィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロック タイプ	uint32	イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベント タイプに関連付けられている追加イベント情報。
デバイス ID (Device ID)	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または IDS イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続イベント タイムスタンプ	uint32	接続イベントのタイムスタンプ。
方向 (Direction)	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示します。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>1: ダウンロード</li> <li>2: アップロード</li> </ul> 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID (User ID)	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する ID 番号。

表 B-13 マルウェア イベント データ ブロック 5.3.1 のフィールド(続き)

フィールド	データ タイプ	説明
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>1(CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。</li> <li>2(UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。</li> <li>3(MALWARE): ファイルにはマルウェアが含まれています。</li> <li>4(UNAVAILABLE): ソフトウェアから シスコ クラウドに対して、特性を確認する要求を送信できなかったか、または シスコ クラウド サービスが要求に応答しませんでした。</li> <li>5(CUSTOM SIGNATURE): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。</li> </ul>
レトロスペクティブ 特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロック タイプ	uint32	URI を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	専用クライアント アプリケーションの内部 ID 番号(該当する場合)。
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>1: 検出</li> <li>2: ブロック</li> <li>3: マルウェア クラウド ルックアップ</li> <li>4: マルウェア ブロック</li> <li>5: マルウェア ホホワイトリスト</li> </ul>

表 B-13 マルウェア イベント データ ブロック 5.3.1 のフィールド(続き)

フィールド	データ タイプ	説明
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> <li>• 1:ICMP</li> <li>• 4:IP</li> <li>• 6:TCP</li> <li>• 17:UDP</li> </ul> これは現時点では TCP のみです。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ~ 100)。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキストモードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

## マルウェア イベント データ ブロック 5.4.x

eStreamer サービスは、マルウェア イベントに関する情報を保存するために、マルウェア イベント データ ブロックを使用します。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれていません。マルウェア イベント データ ブロックのブロック タイプは、シリーズ 2 グループの 47 です。これはブロック 44 に取って代わり、ブロックによって取って代わられます。SSL とファイル アーカイブ サポート用のフィールドが追加されました。

マルウェア イベント レコードの一部としてイベントを要求するには、イベント バージョン 6 およびイベント コード 101 の要求メッセージ内に、マルウェア イベント フラグ(要求フラグ フィールドのビット 30)を設定します。

次の図は、マルウェア イベント データ ブロックの構造を示しています。



レガシー マルウェア イベントのデータ構造

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	クラウド UUID																															
	クラウド UUID(続き)																															
	クラウド UUID(続き)																															
	クラウド UUID(続き)																															
	マルウェア イベント タイムスタンプ																															
	イベント タイプ ID																															
	イベント サブタイプ ID																															
検出名	ディテクタ ID								文字列ブロック タイプ (0)																							
	文字列ブロック タイプ (0) (続き)								文字列ブロック長																							
	文字列ブロック長 (続き)								検出名...																							
ユーザ (User)	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザ...																															
ファイル名	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイル名...																															
ファイルパス	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイルパス...																															
ファイル SHA ハッシュ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイル サイズ (File size)																															
	ファイル 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
	ファイルのタイムスタンプ																															
親ファイル [名前(Name) ]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル名...																															
親ファイル SHA ハッ シュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル SHA ハッシュ...																															
イベント 説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	イベントの説明...																															
デバイス ID(Device ID)																																
接続インスタンス																接続数カウンタ																
接続イベント タイムスタンプ																																
方向(Direction)								送信元 IP アドレス																								
送信元 IP アドレス(続き)																																
送信元 IP アドレス(続き)																																
送信元 IP アドレス(続き)																																
送信元 IP(続き)								宛先 IP アドレス																								
宛先 IP アドレス(続き)																																
宛先 IP アドレス(続き)																																
宛先 IP アドレス(続き)																																
宛先 IP(続き)								アプリケーション ID(Application ID)																								
アプリケーション ID(続き)								ユーザ ID(User ID)																								
ユーザ ID(続き)								アクセス コントロール ポリシー UUID																								

レガシー マルウェア イベントのデータ構造

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
URI	アクセス コントロール ポリシー UUID(続き)								傾向								レトロスペクティブ傾向								文字列ブロック タイプ(0)							
	文字列ブロック タイプ(0)(続き)																文字列ブロック長															
	文字列ブロック長(続き)																URI...															
	送信元ポート (Source Port)																接続先ポート															
	送信元の国																宛先の国															
	Web アプリケーション ID																															
	クライアント アプリケーション ID																															
	操作								プロトコル								脅威スコア								IOC 番号							
	IOC 番号(続き)								セキュリティ コンテキスト																							
	セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト(続き)								SSL 証明書フィンガープリント																							
	SSL 証明書フィンガープリント(続き)																															
	SSL 証明書フィンガープリント(続き)																															
	SSL 証明書フィンガープリント(続き)																															
	SSL 証明書フィンガープリント(続き)																															
	SSL 証明書フィンガープリント(続き)								実際の SSL アクション																SSL フローステータス							

バイト	0							1							2							3																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						
アーカイブ SHA	SSL フロース テータス(続き)							文字列ブロック タイプ(0)																														
	文字列ブロック タイプ(続き)							文字列ブロック タイプ(0)																														
	文字列長さ (続き)							アーカイブ SHA...																														
アーカイ ブ名	文字列ブロック タイプ(0)																																					
	文字列ブロック長																																					
	アーカイブ名...																																					
アーカイブ深度																																						

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

表 B-14 マルウェア イベント データ ブロック 5.4.x のフィールド

フィールド	データ タイプ	説明
マルウェア イベント ブロック タイプ	uint32	マルウェア イベント データ ブロックを開始します。この値は常に 47 です。
マルウェア イベント のブロック長	uint32	マルウェア イベント データ ブロックのバイトの合計数(マルウェア イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
エージェント UUID	uint8[16]	マルウェア イベントをレポートする AMP for Endpoints エージェントの内部固有 ID。
クラウド UUID	uint8[16]	マルウェア イベントの発生元 Cisco Advanced Malware Protection クラウドの、内部の固有 ID。
マルウェア イベント タイムスタンプ	uint32	マルウェア イベント生成時のタイムスタンプ。
イベント タイプ ID	uint32	マルウェア イベント タイプの内部 ID。
イベント サブタイプ ID	uint32	マルウェア 検出につながったアクションの内部 ID。
ディテクタ ID	uint8	マルウェアを検出した検出テクノロジーの内部 ID。
文字列ブロック タ イプ	uint32	検出名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	検出名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および検出名フィールドのバイト数を含む)。
検出名	string	検出または検疫されたマルウェアの名前。

表 B-14 マルウェア イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック タイプ	uint32	ユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびユーザ フィールドのバイト数を含む)。
ユーザ (User)	string	シスコ Agent がインストールされ、マルウェア イベントが発生したコンピュータのユーザ。これらのユーザはユーザ ディスカバリーには関係ないことに注意してください。
文字列ブロック タイプ	uint32	ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル名フィールドのバイト数を含む)。
ファイル名	string	検出または検疫されたファイルの名前。
文字列ブロック タイプ	uint32	ファイル パスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイルパス文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイルパス フィールドのバイト数を含む)。
ファイル パス	string	検出または検疫されたファイルのファイル パス。ファイル名は含まれません。
文字列ブロック タイプ	uint32	ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびファイル SHA ハッシュ フィールドのバイト数を含む)。
ファイル SHA ハッシュ	string	検出または検疫されたファイルの SHA-256 ハッシュ値のレンダリングされた文字列。
ファイル サイズ (File size)	uint32	検出または検疫されたファイルのサイズ(バイト単位)。
ファイル タイプ	uint8	検出または検疫されたファイルのファイル タイプ。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、 <a href="#">エンドポイント向け AMP ファイル タイプのメタデータ (3-43 ページ)</a> を参照してください。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
文字列ブロック タイプ	uint32	親ファイル名を含む文字列データ ブロックを開始します。この値は常に 0 です。



表 B-14 マルウェア イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	親ファイル名文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロック タイプ	uint32	親ファイル SHA ハッシュを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、および親ファイル SHA ハッシュフィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロック タイプ	uint32	イベントの説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データ ブロックに含まれるバイト数(ブロック タイプとヘッダー フィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベント タイプに関連付けられている追加イベント情報。
デバイス ID(Device ID)	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または IDS イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続イベント タイムスタンプ	uint32	接続イベントのタイムスタンプ。
方向(Direction)	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示します。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>• 1: ダウンロード</li> <li>• 2: アップロード</li> </ul> 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID(Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID(User ID)	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。

表 B-14 マルウェアイベントデータブロック 5.4.x のフィールド(続き)

フィールド	データタイプ	説明
アクセスコントロールポリシー UUID	uint8[16]	イベントをトリガーしたアクセスコントロールポリシーの固有識別子として機能する ID 番号。
傾向	uint8	ファイルのマルウェアステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>1(CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。</li> <li>2(UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。</li> <li>3(MALWARE): ファイルにはマルウェアが含まれています。</li> <li>4(UNAVAILABLE): ソフトウェアからシスコクラウドに対して、特性を確認する要求を送信できなかったか、またはシスコクラウドサービスが要求に応答しませんでした。</li> <li>5(CUSTOM SIGNATURE): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。</li> </ul>
レトロスペクティブ特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロックタイプ	uint32	URI を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。

表 B-14 マルウェア イベント データ ブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
操作	uint8	<p>ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。</p> <ul style="list-style-type: none"> <li>• 1: 検出</li> <li>• 2: ブロック</li> <li>• 3: マルウェア クラウド ルックアップ</li> <li>• 4: マルウェア ブロック</li> <li>• 5: マルウェア ホワイトリスト</li> <li>• 6: クラウド ルックアップのタイムアウト</li> <li>• 7: カスタム検出</li> <li>• 8: カスタム検出ブロック</li> <li>• 9: アーカイブ ブロック (深度超過)</li> <li>• 10: アーカイブ ブロック (暗号化されている)</li> <li>• 11: アーカイブ ブロック (調査エラー)</li> </ul>
プロトコル	uint8	<p>ユーザが指定した IANA プロトコル数。次に例を示します。</p> <ul style="list-style-type: none"> <li>• 1: ICMP</li> <li>• 4: IP</li> <li>• 6: TCP</li> <li>• 17: UDP</li> </ul> <p>これは現時点では TCP のみです。</p>
脅威スコア	uint8	<p>動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値 (0 ~ 100)。</p>
IOC 番号	uint16	<p>このイベントに関連付けられている侵害 ID 番号。</p>
セキュリティ コンテキスト	uint8(16)	<p>トラフィックが通過したセキュリティ コンテキスト (仮想ファイアウォール) の ID 番号。マルチコンテキストモードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。</p>
SSL 証明書フィンガープリント	uint8[20]	<p>SSL サーバ証明書の SHA1 ハッシュ。</p>
実際の SSL アクション	uint16	<p>SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 0: 「不明」</li> <li>• 1: 「復号しない」</li> <li>• 2: 「ブロックする」</li> <li>• 3: 「リセットでブロック」</li> <li>• 4: 「復号 (既知のキー)」</li> <li>• 5: 「復号 (置換キー)」</li> <li>• 6: 「復号 (Resign)」</li> </ul>

表 B-14 マルウェア イベント データ ブロック 5.4.x のフィールド(続き)

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

表 B-14 マルウェア イベント データ ブロック 5.4.x のフィールド(続き)

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

## レガシー ディスカバリ データ構造

- [レガシー ディスカバリ イベント ヘッダー \(B-93 ページ\)](#)
- [レガシー サーバ データ ブロック \(B-95 ページ\)](#)
- [レガシー クライアント アプリケーション データ ブロック \(B-96 ページ\)](#)
- [レガシー スキャン結果データ ブロック \(B-98 ページ\)](#)
- [レガシー ホスト プロファイル データ ブロック \(B-125 ページ\)](#)
- [レガシー OS フィンガープリント データ ブロック \(B-133 ページ\)](#)

## レガシー ディスカバリ イベント ヘッダー

### ディスクバリ イベント ヘッダー 5.0 ~ 5.1.1.x

ディスクバリ イベントおよび接続イベントのメッセージには、ディスクバリ 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 \(4-44 ページ\)](#)で説明します。

ディスクバリ 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、ディスクバリ イベント ヘッダーの形式を例示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ															
	レコード長																															
	eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
ディスカバリイベントヘッダー	デバイス ID																															
	[IP アドレス (IP Address)]																															
	MAC アドレス																															
	MAC アドレス(続き)																将来の使用に備えて予約済み															
	イベント秒																															
	イベントマイクロ秒																															
	予約済み(内部使用)																イベントタイプ (Event Type)															
	イベントサブタイプ																															
	ファイル番号(内部使用専用)																															
	ファイルの位置(内部使用専用)																															

次の表は、ディスカバリ イベントヘッダーについての説明です。

表 B-15 ディスカバリ イベントヘッダーのフィールド

フィールド	データ型	説明
デバイス 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、 <a href="#">管理対象デバイスレコードのメタデータ (3-36 ページ)</a> を参照してください。
[IP アドレス (IP Address)]	uint32	イベントに関連するホストの IP アドレス。
MAC アドレス	uint86	イベントに関連するホストの MAC アドレス。

表 B-15 ディスカバリ イベント ヘッダーのフィールド(続き)

フィールド	データ型	説明
将来の使用に備えて予約済み	byte[2]	0 に設定された値による 2 バイトのパディング。
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。
予約済み(内部使用)	バイト	シスコ の内部データであり、無視してかまいません。
イベント タイプ (Event Type)	uint32	イベントのタイプ(新規イベントの場合は 1000、変更イベントの場合は 1001、ユーザ入力イベントの場合は 1002、フルホストプロファイルの場合は 1050)。使用可能なイベント タイプの一覧の詳細については、 <a href="#">イベントタイプ別ホスト ディスカバリ 構造(4-44 ページ)</a> 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、 <a href="#">イベントタイプ別ホスト ディスカバリ 構造(4-44 ページ)</a> 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。

## レガシー サーバデータ ブロック

詳細については、次の項を参照してください。

- [属性アドレス データ ブロック 5.0 ~ 5.1.1.x\(B-95 ページ\)](#)

## 属性アドレス データ ブロック 5.0 ~ 5.1.1.x

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。これはブロック タイプ 38 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 (38)																															
	属性アドレスブロック長																															
	属性 ID																															
	[IP アドレス (IP Address)]																															
	ビット																															

次の表は、属性アドレスデータブロックのフィールドについての説明です。

表 B-16 属性アドレスデータブロックのフィールド

フィールド	データタイプ	説明
属性アドレスブロックタイプ	uint32	属性アドレスブロックデータを開始します。この値は常に 38 です。
属性アドレスブロック長	uint32	属性アドレスデータブロックのバイト数(属性アドレスブロックタイプと長さ用の 8 バイト、およびそれに続く属性アドレスデータのバイト数を含む)。
属性 ID	uint32	影響を受ける属性の ID 番号(該当する場合)。
[IP アドレス (IP Address)]	uint8[4]	IP アドレス オクテットの、ホストの IP アドレス (アドレスが自動的に割り当てられた場合)。
ビット	uint32	IP アドレスが自動的に割り当てられた場合に、ネットマスクを計算するために使用される有効ビットが含まれます。

## レガシークライアントアプリケーションデータブロック

詳細については、次の項を参照してください。

- [ユーザクライアントアプリケーションデータブロック 5.0 ~ 5.1 \(B-96 ページ\)](#)

### ユーザクライアントアプリケーションデータブロック 5.0 ~ 5.1

ユーザクライアントアプリケーションデータブロックには、クライアントアプリケーションデータの送信元に関する情報、データを追加したユーザの ID 番号、および IP アドレス範囲データブロックのリストが含まれます。ユーザクライアントアプリケーションデータブロックのブロックタイプは 59 です。

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



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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(59)																															
	ユーザクライアントアプリケーションブロック長																															
[IP アドレス (IP Address)] 範囲	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	IP 範囲仕様データ ブロック*																															
	アプリケーションプロトコル ID																															
	クライアントアプリケーション ID																															
バージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	バージョン...																															

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

表 B-17 ユーザクライアントアプリケーションデータブロックのフィールド

フィールド	バイト数	説明
ユーザクライアントアプリケーションブロック タイプ	uint32	ユーザクライアントアプリケーションデータブロックを開始します。この値は常にです。
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、 <a href="#">表 4-58 ユーザサーバデータブロックのフィールド(4-107 ページ)</a> を参照してください。

表 B-17 ユーザクライアントアプリケーションデータブロックのフィールド(続き)

フィールド	バイト数	説明
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。

## レガシー スキャン結果データ ブロック

詳細については、次の項を参照してください。

- [スキャン結果データブロック 5.0 ~ 5.1.1.x \(B-98 ページ\)](#)
- [ユーザ製品データブロック 5.0.x \(B-101 ページ\)](#)
- [ユーザ情報データブロック 5.x \(B-123 ページ\)](#)

### スキャン結果データ ブロック 5.0 ~ 5.1.1.x

スキャン結果データブロックは、脆弱性を説明し、スキャン結果追加イベント内で使用されます(イベントタイプ 1002、サブタイプ 11)。スキャン結果データブロックのブロックタイプは 102 です。

次の図は、スキャン結果データブロックの形式を示しています。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
	スキャン結果ブロックタイプ(102)																																							
	スキャン結果ブロック長																																							
	ユーザ ID (User ID)																																							
	スキャンタイプ																																							
	[IP アドレス (IP Address)]																																							
	[ポート (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 B-18 スキャン結果データ ブロックのフィールド

フィールド	データタイプ	説明
スキャン結果ブロックタイプ	uint32	スキャン結果データ ブロックを開始します。この値は常に 102 です。
スキャン結果ブロック長	uint32	スキャン脆弱性データ ブロックのバイト数 (接続統計ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くスキャン脆弱性データのバイト数を含む)。
ユーザ ID (User ID)	uint32	スキャン結果をインポートしたユーザ、またはスキャン結果を生成したスキャンを実行したユーザのユーザ ID 番号が含まれます。
スキャンタイプ	uint32	結果がシステムに追加された方法を示します。
[IP アドレス (IP Address)]	uint32	IP アドレス オクテットの、結果の脆弱性によって影響を受けるホストの IP アドレス。
[ポート (Port)]	uint16	結果の脆弱性の影響を受ける、サブサーバで使用されるポート。

表 B-18 スキャン結果データブロックのフィールド(続き)

フィールド	データタイプ	説明
プロトコル	uint16	IANA プロトコル番号。次に例を示します。 <ul style="list-style-type: none"> <li>• 1:ICMP</li> <li>• 4:IP</li> <li>• 6:TCP</li> <li>• 17:UDP</li> </ul>
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。
汎用リストブロックタイプ	uint32	サードパーティアプリケーションからのホスト入力データを伝えるユーザ製品データブロックを構成する、汎用リストデータブロックを開始します。この値は常に 31 です。

表 B-18 スキャン結果データ ブロックのフィールド(続き)

フィールド	データタイプ	説明
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、 <a href="#">ユーザ製品データブロック 5.1+(4-177 ページ)</a> を参照してください。

### ユーザ製品データ ブロック 5.0.x

ユーザ製品データブロックは、サードパーティアプリケーション文字列マッピングを含む、サードパーティアプリケーションからインポートされたホスト入力データを伝えます。このデータブロックは[接続統計データブロック 6.0.x \(B-205 ページ\)](#)と[ユーザサーバメッセージとオペレーティングシステムメッセージ\(4-58 ページ\)](#)で使用します。ユーザ製品データブロックは、4.10.x の場合はブロックタイプ 65、5.0 ~ 5.0.x の場合はブロックタイプ 118 です。それぞれのブロックタイプは同じ構造を持ちます。



(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	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ製品データ ブロック タイプ (65   118)																															
	ユーザ製品ブロック長																															
	ソース																															
	ソースタイプ																															
[IP アドレス (IP Address)] 範囲	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	IP 範囲仕様データ ブロック*																															
	[ポート (Port)]																プロトコル															
	ドロップユーザ製品																															

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

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
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)																															
修正のリスト	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	修正リスト データ ブロック*																															

次の表は、ユーザ製品データ ブロックのコンポーネントについての説明です。

表 B-19 ユーザ製品データブロック 4.10.x、5.0 ~ 5.0.x のフィールド

フィールド	データタイプ	説明
ユーザ製品データブロックタイプ	uint32	ユーザ製品データブロックを開始します。この値はバージョン 4.10.x の場合は 65、バージョン 5.0 ~ 5.0.x の場合は 118 です。
ユーザ製品ブロック長	uint32	ユーザ製品データブロックのバイトの合計数(ユーザ製品ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ製品データのバイト数を含む)。
ソース	uint32	データをインポートした送信元の ID 番号。
ソースタイプ	uint32	データ提供ソースのソースタイプ。
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、 <a href="#">5.2+ の IP アドレス範囲データブロック (4-98 ページ)</a> を参照してください。
[ポート (Port)]	uint16	ユーザが指定するポート。
プロトコル	uint16	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> <li>• 1:ICMP</li> <li>• 4:IP</li> <li>• 6:TCP</li> <li>• 17:UDP</li> </ul>
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"> <li>• 0:いいえ</li> <li>• 1:はい</li> </ul>
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタムベンダー名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタムベンダー文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびベンダー名のバイト数を含む)。
カスタムベンダー名	string	ユーザ入力で指定されたカスタムベンダー名。
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタム製品名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタム製品文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および製品名のバイト数を含む)。
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。



表 B-19 ユーザ製品データブロック 4.10.x、5.0 ~ 5.0.x のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタムバージョンを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタムバージョン文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
カスタムバージョン	string	ユーザ入力に指定されたカスタムバージョン。
ソフトウェア ID	uint32	シスコ データベースの特定のレビジョンのサーバまたはオペレーティング システムの ID。
サーバ ID	uint32	ユーザ入力に指定したホスト サーバのアプリケーションプロトコルの シスコ アプリケーション識別子。
ベンダー ID	uint32	サードパーティ オペレーティング システムが シスコ 3D オペレーティング システム定義にマップされるときに指定される、サードパーティ オペレーティング システムのベンダーの ID。
製品 ID	uint32	サードパーティ オペレーティング システム文字列が シスコ 3D オペレーティング システム定義にマップされるときに指定される、サードパーティ オペレーティング システム文字列の製品 ID 文字列。
文字列ブロックタイプ	uint32	ユーザ入力内のサードパーティ オペレーティング システム文字列がマップされる シスコ 3D オペレーティング システム定義のメジャーバージョン番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	メジャー文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
メジャーバージョン	string	サードパーティ オペレーティング システム文字列がマップされる シスコ 3D オペレーティング システム定義のメジャーバージョン。
文字列ブロックタイプ	uint32	サードパーティ オペレーティング システム文字列がマップされる シスコ 3D オペレーティング システム定義のマイナーバージョン番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	マイナー文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
マイナーバージョン	string	ユーザ入力内のサードパーティ オペレーティング システム文字列がマップされる シスコ 3D オペレーティング システム定義のマイナーバージョン。
文字列ブロックタイプ	uint32	ユーザ入力内のサードパーティ オペレーティング システム文字列がマップされる シスコ オペレーティング システム定義のレ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。

表 B-19 ユーザ製品データブロック 4.10.x, 5.0 ~ 5.0.x のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	メジャー用文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
リビジョン	string	ユーザ入力内のサードパーティオペレーティングシステム文字列がマップされる シスコ 3D オペレーティングシステム定義のリビジョン番号。
文字列ブロックタイプ	uint32	サードパーティオペレーティングシステム文字列がマップされる シスコ 3D オペレーティングシステム定義の最終メジャーバージョン番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにバージョンのバイト数を加えた移行先メジャー文字列データブロックのバイト数。
移行先メジャー	string	ユーザ入力内のサードパーティオペレーティングシステム文字列がマップされる シスコ 3D オペレーティングシステム定義のメジャーバージョン番号の範囲内にある、最終バージョン番号。
文字列ブロックタイプ	uint32	サードパーティオペレーティングシステム文字列がマップされる シスコ 3D オペレーティングシステム定義の最終マイナーバージョン番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにバージョンのバイト数を加えたマイナー用文字列データブロックのバイト数。
マイナー用	string	ユーザ入力内のサードパーティオペレーティングシステム文字列がマップされる シスコ 3D オペレーティングシステム定義のマイナーバージョン番号の範囲内にある、最終バージョン番号。
文字列ブロックタイプ	uint32	サードパーティオペレーティングシステム文字列がマップされる シスコ 3D オペレーティングシステム定義の最終リビジョン番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトにリビジョン番号のバイト数を加えた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	ユーザ入力内のサードパーティオペレーティングシステム文字列がマップされる シスコ 3D オペレーティングシステム定義のリビジョン番号の範囲内にある、最終リビジョン番号。
文字列ブロックタイプ	uint32	サードパーティオペレーティングシステム文字列がマップされる シスコ 3D オペレーティングシステムのビルド番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ビルド文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびビルド番号のバイト数を含む)。

表 B-19 ユーザ製品データブロック 4.10.x, 5.0 ~ 5.0.x のフィールド(続き)

フィールド	データタイプ	説明
ビルド	string	ユーザ入力内のサードパーティ オペレーティング システム文字列がマップされる シスコ 3D オペレーティング システムのビルド番号。
文字列ブロックタイプ	uint32	サードパーティ オペレーティング システム文字列がマップされる シスコ 3D オペレーティング システムのパッチ番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	パッチ文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびパッチ番号のバイト数を含む)。
パッチ	string	ユーザ入力内のサードパーティ オペレーティング システム文字列がマップされる シスコ 3D オペレーティング システムのパッチ番号。
文字列ブロックタイプ	uint32	サードパーティ オペレーティング システム文字列がマップされる シスコ 3D オペレーティング システムの拡張番号を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	拡張文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、および拡張番号のバイト数を含む)。
内線番号	string	ユーザ入力内のサードパーティ オペレーティング システム文字列がマップされる シスコ 3D オペレーティング システムの拡張番号。
UUID	uint8 [x16]	オペレーティング システム用の固有 ID 番号が含まれます。
汎用リストブロックタイプ	uint32	どの修正が特定の IP アドレス範囲内のホストに適用されているかに関するユーザ入力データを伝える修正リストデータ ブロックで構成される、汎用リストデータ ブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータ ブロックのバイト数(リストヘッダーと、カプセル化されたすべての修正リストデータ ブロックを含む)。
修正リストデータブロック*	変数 (variable)	ホストに適用された修正に関する情報を含む修正リストデータ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">フィックス リスト データ ブロック (4-105 ページ)</a> を参照してください。

## レガシー ユーザ ログイン データ ブロック

詳細については、次の各項を参照してください。

- [ユーザ ログイン情報データ ブロック 5.0 ~ 5.0.2 \(B-108 ページ\)](#)
- [ユーザ ログイン情報データ ブロック 5.1 ~ 5.4.x \(B-109 ページ\)](#)
- [ユーザ ログイン情報データ ブロック 6.0.x \(B-111 ページ\)](#)
- [ユーザ ログイン情報データ ブロック 6.1.x \(B-115 ページ\)](#)
- [ユーザ情報データ ブロック 5.x \(B-123 ページ\)](#)

## ユーザログイン情報データブロック 5.0 ~ 5.0.2

ユーザログイン情報データブロックは、ユーザ情報更新メッセージで使用され、検出されたユーザのログイン情報の変更を伝えます。詳細については、[ユーザ情報更新メッセージブロック \(4-62 ページ\)](#)を参照してください。

ユーザログイン情報データブロックは、バージョン 5.0 ~ 5.0.2 の場合は、ブロックタイプ 121 です。

次の図は、ユーザログイン情報データブロックの形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザログイン情報ブロックタイプ(121)																															
	ユーザログイン情報ブロック長																															
	Timestamp																															
	[IP アドレス (IP Address)]																															
ユーザ (User) [名前 (Name) ]	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	ユーザ名...																															
	ユーザ ID (User ID)																															
	アプリケーション ID (Application ID)																															
E メール	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	電子メール...																															

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

表 B-20 ユーザログイン情報データブロック 5.0 ~ 5.0.2 のフィールド

フィールド	データタイプ	説明
ユーザログイン情報ブロックタイプ	uint32	ユーザログイン情報データブロックを開始します。この値は、バージョン 5.0 ~ 5.0.2 の場合は 121 です。
ユーザログイン情報ブロック長	uint32	ユーザログイン情報データブロックのバイトの合計数(ユーザログイン情報ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザログイン情報データのバイト数を含む)。

表 B-20 ユーザログイン情報データブロック 5.0 ~ 5.0.2 のフィールド(続き)

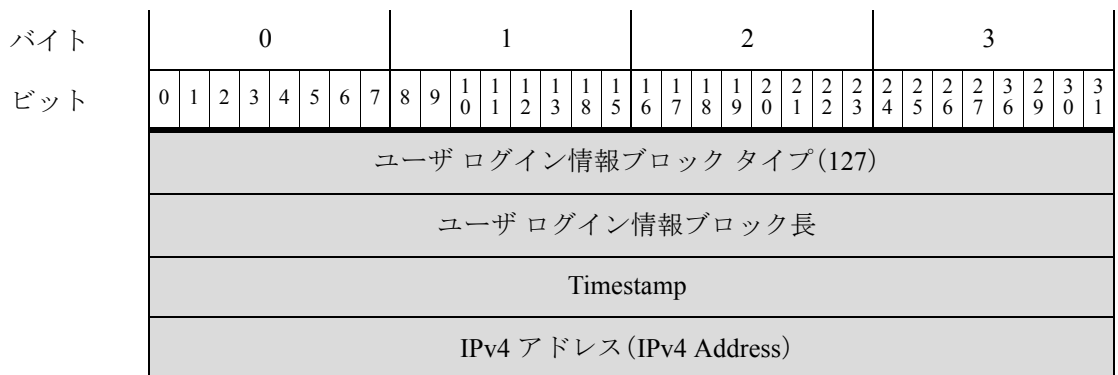
フィールド	データタイプ	説明
Timestamp	uint32	イベントのタイムスタンプ。
[IP アドレス (IP Address)]	uint8[4]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IP アドレス。
文字列ブロックタイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。
アプリケーション ID (Application ID)	uint32	ログイン情報の取得元の、接続に使用されたアプリケーションプロトコルのアプリケーション ID。
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。

### ユーザログイン情報データブロック 5.1 ~ 5.4.x

ユーザログイン情報データブロックは、ユーザ情報更新メッセージで使用され、検出されたユーザのログイン情報の変更を伝えます。詳細については、[ユーザアカウント更新メッセージデータブロック \(4-186 ページ\)](#)を参照してください。

ユーザログイン情報データブロックは、バージョン 4.7 ~ 4.10.x の場合はブロックタイプ 73、バージョン 5.0 ~ 5.0.2 の場合はシリーズ 1 グループのブロックのブロックタイプ 121、バージョン 5.1 ~ 5.4.x の場合はシリーズ 1 グループのブロックのデータタイプ 127 です。

次の図は、ユーザログイン情報データブロックの形式を示しています。



バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	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...																															
	ユーザ ID (User ID)																															
	アプリケーション ID (Application ID)																															
E メール	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	電子メール...																															
	IPv6 アドレス																															
	IPv6 アドレス (続き)																															
	IPv6 アドレス (続き)																															
	IPv6 アドレス (続き)																															
レポート 基準	ログインタイプ	文字列ブロック タイプ (0)																														
	文字列ブロック タイプ (0) (続き)	文字列ブロック長																														
	文字列ブロッ ク長	レポート基準...																														

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

表 B-21 ユーザログイン情報データブロックのフィールド

フィールド	データタイプ	説明
ユーザログイン情報ブロックタイプ	uint32	ユーザログイン情報データブロックを開始します。この値は、バージョン 5.1+ の場合は 127 です。
ユーザログイン情報ブロック長	uint32	ユーザログイン情報データブロックのバイトの合計数 (ユーザログイン情報ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザログイン情報データのバイト数を含む)。
Timestamp	uint32	イベントのタイムスタンプ。

表 B-21 ユーザログイン情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
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、 <a href="#">IP アドレス (1-5 ページ)</a> 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。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。
アプリケーション ID (Application ID)	uint32	ログイン情報の取得元の、接続に使用されたアプリケーション プロトコルのアプリケーション ID。
文字列ブロック タイプ	uint32	ユーザの電子メールアドレスを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データ ブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IPv6 アドレス。
ログイン タイプ	uint8	検出されたユーザ ログインのタイプ。
文字列ブロック タイプ	uint32	レポート基準値を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	レポート基準文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびレポート基準フィールドのバイト数を含む)。
レポート基準	string	ログインをレポートする Active Directory サーバの名前。

## ユーザ ログイン情報データ ブロック 6.0.x

ユーザ ログイン情報データ ブロックは、ユーザ情報更新メッセージで使用され、検出されたユーザのログイン情報の変更を伝えます。詳細については、[ユーザ アカウント更新メッセージ データ ブロック \(4-186 ページ\)](#) を参照してください。

ユーザ ログイン情報データ ブロックは、バージョン 6.0.x の場合は、ブロック タイプ 159 です。これには新しい ISE 統合エンドポイント プロファイル、セキュリティ インテリジェンスのフィールドがあります。

ユーザ ログイン情報データ ブロックは、バージョン 4.7 ~ 4.10.x の場合はブロック タイプ 73、バージョン 5.0 ~ 5.0.2 の場合はシリーズ 1 グループのブロックのブロック タイプ 121、バージョン 5.1+ の場合はシリーズ 1 グループのブロックのデータ タイプ 127 です。詳細については、[ユーザ ログイン情報データ ブロック 5.1 ~ 5.4.x \(B-109 ページ\)](#) 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 (159)																															
	ユーザ ログイン情報ブロック長																															
	Timestamp																															
	IPv4 アドレス (IPv4 Address)																															
ユーザ (User) [名前 (Name) ]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザ名...																															
ドメイン	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ドメイン...																															
	ユーザ ID (User ID)																															
	レルム ID																															
	エンドポイント プロファイル ID																															
	セキュリティ グループ ID																															
	プロトコル																															
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																															



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

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

表 B-22 ユーザ ログイン情報データ ブロックのフィールド

フィールド	データ タイプ	説明
ユーザ ログイン情報 ブロック タイプ	uint32	ユーザ ログイン情報データ ブロックを開始します。この値は、バージョン 6.0.x の場合は 159 です。
ユーザ ログイン情報 ブロック長	uint32	ユーザ ログイン情報データ ブロックのバイトの合計数 (ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ ログイン情報データのバイト数を含む)。
Timestamp	uint32	イベントのタイムスタンプ。
IPv4 アドレス (IPv4 Address)	uint32	このフィールドは予約済みですが、設定されておりません。IPv4 アドレスは IPv6 アドレス フィールドに保存されます。詳細については、 <a href="#">IP アドレス (1-5 ページ)</a> を参照してください。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数 (ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
文字列ブロック タイプ	uint32	ドメインを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにドメインのバイト数を加えたユーザ名文字列データ ブロックのバイト数。
ドメイン	string	ユーザがログインしているドメイン。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。

表 B-22 ユーザログイン情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
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"> <li>• 165:FTP</li> <li>• 426:SIP</li> <li>• 547:AOL Instant Messenger</li> <li>• 683:IMAP</li> <li>• 710:LDAP</li> <li>• 767:NTP</li> <li>• 773:Oracle データベース</li> <li>• 788:POP3</li> <li>• 1755:MDNS</li> </ul>
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IPv6 アドレス。
ロケーション IPv6 アドレス	uint8[16]	ユーザがログインした最新の IP アドレス。IPv4 または IPv6 のどちらかのアドレスになります。
ログインタイプ	uint8	検出されたユーザログインのタイプ。
認証タイプ (Authentication Type)	uint8	ユーザが使用する認証のタイプ。値は次のとおりです。 <ul style="list-style-type: none"> <li>• 0:認証は不要</li> <li>• 1:パッシブ認証、AD エージェント、または ISE セッション</li> <li>• 2:キャプティブポータルの正常な認証</li> <li>• 3:キャプティブポータルのゲスト認証</li> <li>• 4:キャプティブポータルの失敗認証</li> </ul>
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。

表 B-22 ユーザ ログイン情報データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	レポート基準文字列データ ブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびレポート基準フィールドのバイト数を含む)。
レポート基準	string	ログインをレポートする Active Directory サーバの名前。

### ユーザ ログイン情報データ ブロック 6.1.x

バージョン 6.1+ では、ユーザ ログイン情報データ ブロックには、シリーズ 1 グループのブロック内にブロックタイプ 165 が含まれています。ここには新しいポート フィールドとトンネリング フィールドがあります。これはブロックタイプ 159 に置き換わります。詳細については、[ユーザ ログイン情報データ ブロック 6.0.x \(B-111 ページ\)](#) を参照してください。これはブロックタイプ 167 に更新しました。

次の図は、ユーザ ログイン情報データ ブロックの形式を示しています。



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

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

表 B-23 ユーザ ログイン情報データ ブロックのフィールド

フィールド	データ タイプ	説明
ユーザ ログイン情報ブロック タイプ	uint32	ユーザ ログイン情報データ ブロックを開始します。バージョン 6.1+ の場合、この値は 165 です。
ユーザ ログイン情報ブロック長	uint32	ユーザ ログイン情報データ ブロックのバイトの合計数 (ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ ログイン情報データのバイト数を含む)。
Timestamp	uint32	イベントのタイムスタンプ。
IPv4 アドレス (IPv4 Address)	uint32	このフィールドは予約済みですが、設定されていません。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、 <a href="#">IP アドレス (1-5 ページ)</a> を参照してください。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数 (ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
文字列ブロック タイプ	uint32	ドメインを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにドメインのバイト数を加えたユーザ名文字列データ ブロックのバイト数。
ドメイン	string	ユーザがログインしているドメイン。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。
レルム ID	uint32	アイデンティティ レルムに対応する整数 ID。
エンドポイント プロファイル ID	uint32	接続エンドポイントが使用するデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
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。

表 B-23 ユーザログイン情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
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"> <li>• 165:FTP</li> <li>• 426:SIP</li> <li>• 547:AOL Instant Messenger</li> <li>• 683:IMAP</li> <li>• 710:LDAP</li> <li>• 767:NTP</li> <li>• 773:Oracle データベース</li> <li>• 788:POP3</li> <li>• 1755:MDNS</li> </ul>
[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。
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"> <li>• 0:認証は不要</li> <li>• 1:パッシブ認証、AD エージェント、または ISE セッション</li> <li>• 2:キャプティブ ポータルの正常な認証</li> <li>• 3:キャプティブ ポータルのゲスト認証</li> <li>• 4:キャプティブ ポータルの失敗認証</li> </ul>
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。

表 B-23 ユーザ ログイン情報データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	レポート基準文字列データ ブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびレポート基準フィールドのバイト数を含む)。
レポート基準	string	ログインをレポートする Active Directory サーバの名前。

## ユーザ ログイン情報データ ブロック 6.1.x

ユーザ ログイン情報データ ブロックは、ユーザ情報更新メッセージで使用され、検出されたユーザのログイン情報の変更を伝えます。詳細については、[ユーザ情報更新メッセージブロック \(4-62 ページ\)](#)を参照してください。

バージョン 6.1x では、ユーザ ログイン情報データ ブロックには、シリーズ 1 グループのブロック内にブロックタイプ 165 が含まれています。ここには新しいポート フィールドとトンネリング フィールドがあります。これはブロックタイプ 159 に置き換わります。これはブロックタイプ 167 に更新しました。詳細については、[ユーザ ログイン情報データ ブロック 6.0.x \(B-111 ページ\)](#)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 (165)																															
	ユーザ ログイン情報ブロック長																															
	Timestamp																															
	IPv4 アドレス (IPv4 Address)																															
ユーザ (User) [名前 (Name) ]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザ名...																															
ドメイン	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ドメイン...																															
	ユーザ ID (User ID)																															
	レルム ID																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	エンドポイントプロファイル ID																															
	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)																															
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...															
ドメイン	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	説明...																															

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



表 B-24 ユーザ ログイン情報データ ブロックのフィールド

フィールド	データ タイプ	説明
ユーザ ログイン情報ブロック タイプ	uint32	ユーザ ログイン情報データ ブロックを開始します。バージョン 6.2+ の場合、この値は 165 です。
ユーザ ログイン情報ブロック長	uint32	ユーザ ログイン情報データ ブロックのバイトの合計数 (ユーザ ログイン情報ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ ログイン情報データのバイト数を含む)。
Timestamp	uint32	イベントのタイムスタンプ。
IPv4 アドレス (IPv4 Address)	uint32	このフィールドは予約済みですが、設定されておりません。IPv4 アドレスは IPv6 アドレス フィールドに保存されません。詳細については、 <a href="#">IP アドレス (1-5 ページ)</a> を参照してください。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数 (ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
文字列ブロック タイプ	uint32	ドメインを含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロック タイプ フィールドと長さフィールドの 8 バイトにドメインのバイト数を加えたユーザ名文字列データ ブロックのバイト数。
ドメイン	string	ユーザがログインしているドメイン。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。
レルム ID	uint32	アイデンティティ レルムに対応する整数 ID。
エンドポイント プロファイル ID	uint32	接続エンドポイントが使用するデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
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。

表 B-24 ユーザログイン情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
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"> <li>• 165:FTP</li> <li>• 426:SIP</li> <li>• 547:AOL Instant Messenger</li> <li>• 683:IMAP</li> <li>• 710:LDAP</li> <li>• 767:NTP</li> <li>• 773:Oracle データベース</li> <li>• 788:POP3</li> <li>• 1755:MDNS</li> </ul>
[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。
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"> <li>• 0:認証は不要</li> <li>• 1:パッシブ認証、AD エージェント、または ISE セッション</li> <li>• 2:キャプティブポータルでの正常な認証</li> <li>• 3:キャプティブポータルでのゲスト認証</li> <li>• 4:キャプティブポータルでの失敗認証</li> </ul>
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。

表 B-24 ユーザ ログイン情報データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
文字列ブロック長	uint32	レポート基準文字列データ ブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびレポート基準フィールドのバイト数を含む)。
レポート基準	string	ログインをレポートする Active Directory サーバの名前。

## ユーザ情報データ ブロック 5.x

ユーザ情報データ ブロックはユーザ変更メッセージで使用され、検出、削除、またはドロップされたユーザの情報を伝えます。詳細については、[ユーザ変更メッセージ\(4-62 ページ\)](#)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、4.7 ~ 4.10.x のシリーズ 1 ブロック グループのブロックタイプ 75 と、5.x のシリーズ 1 ブロック グループのブロックタイプ 120 です。構成は、ブロックタイプ 75 と 120 で同じです。

次の図は、ユーザ情報データ ブロックの形式を示しています。

バイト	0								1								2								3												
	0	1	2	3	4	5	6	7	8	9	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	ユーザ情報ブロック タイプ (75   120)																																				
	ユーザ情報ブロック長																																				
	ユーザ ID (User ID)																																				
ユーザ (User) [名前 (Name) ]	文字列ブロック タイプ (0)																																				
	文字列ブロック長																																				
	ユーザ名...																																				
	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...																																				

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
E メール	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電子メール...																															
部署名 (Department)	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	部署名...																															
電話	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	電話...																															

次の表は、ユーザ情報データ ブロックのコンポーネントについての説明です。

表 B-25 ユーザ情報データブロックのフィールド

フィールド	データタイプ	説明
ユーザ情報ブロックタイプ	uint32	ユーザ情報データブロックを開始します。この値は、バージョン 4.7 ~ 4.10.x の場合は 75、5.0+ の場合は 120 です。
ユーザ情報ブロック長	uint32	ユーザ情報データブロックのバイトの合計数(ユーザログイン情報ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くユーザ情報データのバイト数を含む)。
ユーザ ID (User ID)	uint32	ユーザの ID 番号。
文字列ブロックタイプ	uint32	ユーザのユーザ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
プロトコル	uint32	ユーザ情報を含むパケットのプロトコル。
文字列ブロックタイプ	uint32	ユーザの名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および名のバイト数を含む)。
名	string	ユーザの名前。

表 B-25 ユーザ情報データブロックのフィールド(続き)

フィールド	データタイプ	説明
文字列ブロックタイプ	uint32	ユーザの姓を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	姓文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および姓のバイト数を含む)。
姓	string	ユーザの姓。
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。
文字列ブロックタイプ	uint32	ユーザの部署を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	部署文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および部署のバイト数を含む)。
部署名 (Department)	string	ユーザの部署名。
文字列ブロックタイプ	uint32	ユーザの電話番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電話番号のバイト数を加えた電話番号文字列データブロックのバイト数。
電話	string	ユーザの電話番号。

## レガシー ホスト プロファイル データ ブロック

詳細については、次の各項を参照してください。

- [ホストプロファイルデータブロック 5.0 ~ 5.0.2 \(B-125 ページ\)](#)

### ホストプロファイルデータブロック 5.0 ~ 5.0.2

次の図は、ホストプロファイルデータブロックのバージョン 5.0 ~ 5.0.2 の形式を示しています。さらに、ホストプロファイルデータブロックには、ホスト重要度値が含まれていませんが、VLAN のプレゼンスインジケータは含まれています。さらに、ホストプロファイルデータブロックは、ホストの NetBIOS 名を伝えることができます。ホストプロファイルデータブロックのブロックタイプは 91 です。



(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。

レガシーディスカバリデータ構造

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ホストプロファイルブロックタイプ(91)																															
	ホストプロファイルブロック長																															
	[IPアドレス(IP Address)]																															
サーバフィンガープリント	ホップ								プライマリ/セカンダリ								汎用リストブロックタイプ(31)															
	汎用リストブロックタイプ(続き)																汎用リストブロック長															
	汎用リストブロック長(続き)																サーバフィンガープリントデータブロック*															
クライアントフィンガープリント	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	クライアントフィンガープリントデータブロック*																															
SMBフィンガープリント	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	SMBフィンガープリントデータブロック*																															
DHCPフィンガープリント	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	DHCPフィンガープリントデータブロック*																															
TCPサーバブロック*	リストブロックタイプ(11)																TCPサーバのリスト															
	リストブロック長																															
	サーバブロックタイプ(36)																															
TCPサーバブロック*	サーバブロック長																															
	TCPサーバデータ...																															

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
	リストブロック タイプ(11)																															UDP サーバ のリスト	
	リストブロック長																																
UDP サーバ ブロック*	サーバブロック タイプ(36)*																																
	サーバブロック長																																
	UDP サーバデータ...																																
	リストブロック タイプ(11)																															ネットワー クプロトコ ルのリスト	
	リストブロック長																																
ネットワー クプロトコ ルブロック*	プロトコルブロック タイプ(4)*																																
	プロトコルブロック長																																
	ネットワーク プロトコルデータ...																																
	リストブロック タイプ(11)																															トランス ポートプロ トコルのリ スト	
	リストブロック長																																
トランス ポート (Transport) プロトコル ブロック*	プロトコルブロック タイプ(4)*																																
	プロトコルブロック長																																
	トランスポート プロトコルデータ...																																
	リストブロック タイプ(11)																															MAC アドレ スのリスト	
	リストブロック長																																
MAC アドレ スブロック*	MAC アドレス ブロック タイプ(95)*																																
	MAC アドレスブロック長																																
	MAC アドレス データ...																																
	最終検出時のホスト																																
	ホスト タイプ																																
	VLAN の有無								VLAN ID (Admin. VLAN ID)																VLAN タイプ								

## レガシー ディスカバリ データ構造

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
	VLAN 優先順位								汎用リストブロック タイプ(31)																								クライアントアプリケーションのリスト							
	汎用リストブロック タイプ (続き)								汎用リストブロック長																															
クライアントアプリケーションデータ	汎用リストブロック長(続き)								クライアントアプリケーションブロック タイプ(112)*																															
									クライアントアプリケーションブロック タイプ (29)*(続き)								クライアントアプリケーションブロック長																							
									クライアントアプリケーションブロック長(続き)								クライアントアプリケーションデータ...																							
NetBIOS [名前(Name) ]	文字列ブロック タイプ(0)																																							
	文字列ブロック長																																							
	NetBIOS 文字列データ...																																							

次の表は、バージョン 4.9 ~ 5.0.2 により返されるホストプロファイルデータブロックのフィールドについての説明です。

表 B-26 ホストプロファイルデータブロック 5.0 ~ 5.0.2 のフィールド

フィールド	データタイプ	説明
ホストプロファイルブロックタイプ	uint32	ホストプロファイルデータブロック 4.9 ~ 5.0.2 を開始します。このデータブロックのブロックタイプは 91 です。
ホストプロファイルブロック長	uint32	ホストプロファイルデータブロックのバイト数(ホストプロファイルブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くホストプロファイルデータに含まれるバイト数を含む)。
[IP アドレス (IP Address)]	uint8[4]	IP アドレス オクテットの、プロファイルに記述されているホストの IP アドレス。
ホップ	uint8	ホストからのデバイスまでのホップ数。
プライマリ/セカンダリ	uint8	ホストがそれを検出したデバイスのプライマリまたはセカンダリのどちらのネットワークにあるかを示します。 <ul style="list-style-type: none"> <li>0:ホストはプライマリ ネットワークにあります。</li> <li>1:ホストはセカンダリ ネットワークにあります。</li> </ul>



表 B-26 ホスト プロファイル データ ブロック 5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
汎用リストブロックタイプ	uint32	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、 <a href="#">オペレーティングシステムフィンガープリントデータブロック 5.0 ~ 5.0.2 (B-133 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	クライアントフィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	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、 <a href="#">オペレーティングシステムフィンガープリントデータブロック 5.0 ~ 5.0.2 (B-133 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	SMB フィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。
オペレーティングシステムフィンガープリント(SMB フィンガープリント)データブロック*	変数(variable)	SMB フィンガープリントを使用して識別されるホスト上のオペレーティングシステムに関する情報が含まれている、オペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレーティングシステムフィンガープリントデータブロック 5.0 ~ 5.0.2 (B-133 ページ)</a> を参照してください。

表 B-26 ホストプロファイルデータブロック 5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
汎用リストブロックタイプ	uint32	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、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.0 ~ 5.0.2 (B-133 ページ)</a> を参照してください。
リストブロックタイプ	uint32	TCP サーバ データを伝えるサーバ データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバ データ ブロックを加えた値です。 このフィールドには、ゼロ以上のサーバ データ ブロックが続きます。
サーバブロックタイプ	uint32	サーバ データ ブロックを開始します。この値は常に 89 です。
サーバブロック長	uint32	サーバ データ ブロックのバイト数(サーバブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く TCP サーバ データのバイト数を含む)。
TCP サーバ データ	変数 (variable)	TCP サーバを記述するデータ フィールド(旧バージョンの製品で説明)。
リストブロックタイプ	uint32	UDP サーバ データを伝えるサーバ データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバ データ ブロックを加えた値です。 このフィールドには、ゼロ以上のサーバ データ ブロックが続きます。
サーバブロックタイプ	uint32	UDP サーバを記述するサーバ データ ブロックを開始します。この値は常に 89 です。
サーバブロック長	uint32	サーバ データ ブロックのバイト数(サーバブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く UDP サーバ データのバイト数を含む)。
UDP サーバ データ	変数 (variable)	UDP サーバを記述するデータ フィールド(旧バージョンの製品で説明)。

表 B-26 ホスト プロファイルデータ ブロック 5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
リストブロックタイプ	uint32	ネットワーク プロトコルデータを伝えるプロトコルデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのプロトコルデータブロックを加えた値です。 このフィールドには、ゼロ以上のプロトコルデータブロックが続きます。
プロトコルブロックタイプ	uint32	ネットワーク プロトコルを記述するプロトコルデータブロックを開始します。この値は常に 4 です。
プロトコルブロック長	uint32	プロトコルデータブロックのバイト数(プロトコルブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くプロトコルデータのバイト数を含む)。
ネットワーク プロトコルデータ	uint16	ネットワーク プロトコル数が含まれるデータ フィールド( <a href="#">プロトコルデータブロック (4-78 ページ)</a> で説明)。
リストブロックタイプ	uint32	トランスポート プロトコルデータを伝えるプロトコルデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのプロトコルデータブロックを加えた値です。 このフィールドには、ゼロ以上のトランスポート プロトコルデータブロックが続きます。
プロトコルブロックタイプ	uint32	トランスポート プロトコルを記述するプロトコルデータブロックを開始します。この値は常に 4 です。
プロトコルブロック長	uint32	プロトコルデータブロックのバイト数(プロトコルブロックタイプと長さ用の 8 バイト、およびそれに続くプロトコルデータのバイト数を含む)。
トランスポート プロトコルデータ	変数 (variable)	トランスポート プロトコル数が含まれるデータ フィールド( <a href="#">プロトコルデータブロック (4-78 ページ)</a> で説明)。
リストブロックタイプ	uint32	MAC アドレスデータブロックを構成するリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リストのバイト数(リストヘッダーと、カプセル化されたすべての MAC アドレスデータブロックを含む)。
ホスト MAC アドレスブロックタイプ	uint32	ホスト MAC アドレスデータブロックを開始します。この値は常に 95 です。
ホスト MAC アドレスブロック長	uint32	ホスト MAC アドレスデータブロックのバイト数(ホスト MAC アドレスブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くホスト MAC アドレスデータのバイト数を含む)。

表 B-26 ホストプロファイルデータブロック 5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
ホスト MAC アドレス データ	変数 (variable)	ホスト MAC アドレス データ フィールド(ホスト MAC アドレス 4.9+(4-119 ページ)で説明)。
最終検出時のホスト	uint32	システムがホスト アクティビティを検出した前回時刻を表す UNIX タイムスタンプ。
ホスト タイプ	uint32	ホスト タイプを示します。表示される可能性がある値は次のとおりです。 <ul style="list-style-type: none"> <li>0:ホスト</li> <li>1:ルータ</li> <li>2:ブリッジ</li> <li>3:NAT デバイス</li> <li>4:LB(ロード バランサ)</li> </ul>
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"> <li>0:はい</li> <li>1:いいえ</li> </ul>
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 タグに含まれるプライオリティ値。
汎用リスト ブロック タイプ	uint32	クライアント アプリケーション データを伝えるクライアント アプリケーション データ ブロックで構成される汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのクライアント アプリケーション データ ブロックを含む)。
クライアント アプリケーション ブロック タイプ	uint32	クライアント アプリケーション ブロックを開始します。この値は常に 5 です。
クライアント アプリケーション ブロック長	uint32	クライアント アプリケーション ブロックのバイト数(クライアント アプリケーション ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くクライアント アプリケーション データのバイト数を含む)。
クライアント アプリケーション データ	変数 (variable)	クライアント アプリケーション を記述するクライアント アプリケーション データ フィールド(5.0+ のホスト クライアント アプリケーション データ ブロック(4-161 ページ)で説明)。
文字列ブロック タイプ	uint32	NetBIOS 名の文字列データ ブロックを開始します。この値は文字列データを示す 0 に設定されます。

表 B-26 ホストプロファイルデータブロック 5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	NetBIOS 名データブロックのバイト数を示します(文字列ブロックタイプと長さのフィールド用の 8 バイト、および NetBIOS 名のバイト数を含む)。
NetBIOS 文字列データ	変数	ホストプロファイルに記述されているホストの NetBIOS 名が含まれます。

## レガシー OS フィンガープリントデータブロック

詳細については、次の各項を参照してください。

- [オペレーティングシステムフィンガープリントデータブロック 5.0 ~ 5.0.2\(B-133 ページ\)](#)

## オペレーティングシステムフィンガープリントデータブロック 5.0 ~ 5.0.2

オペレーティングシステムフィンガープリントデータブロックのブロックタイプは 87 です。このブロックには、フィンガープリント Universally Unique Identifier (UUID) の他、フィンガープリントタイプ、フィンガープリント送信元タイプ、フィンガープリント送信元 ID を格納します。次の図は、オペレーティングシステムフィンガープリントデータブロックのバージョン 5.0 ~ 5.0.2 の形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	オペレーティングシステムフィンガープリントブロックタイプ(87)																															
	オペレーティングシステムフィンガープリントブロック長																															
OS フィンガープリント UUID	フィンガープリント UUID																															
	フィンガープリント UUID(続き)																															
	フィンガープリント UUID(続き)																															
	フィンガープリント UUID(続き)																															
	フィンガープリントタイプ																															
	フィンガープリントソースタイプ																															
	フィンガープリントソース ID																															
	フィンガープリントの最終確認値																															
	TTL 差異																															

次の表は、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の説明です。

表 B-27 オペレーティングシステムフィンガープリントデータブロックのフィールド

フィールド	データタイプ	説明
オペレーティングシステムフィンガープリントデータブロックタイプ	uint32	オペレーティングシステムデータブロックを開始します。この値は常に 87 です。
オペレーティングシステムデータブロック長	uint32	オペレーティングシステムフィンガープリントデータブロックのバイト数。この値は常に 41 です。データブロックタイプと長さのフィールド用の 8 バイト、フィンガープリント UUID 値用の 16 バイト、フィンガープリントのタイプ用の 4 バイト、フィンガープリントソースのタイプ用の 4 バイト、フィンガープリントソース ID 用の 4 バイト、最終確認値用の 4 バイト、および TTL 差異用の 1 バイトです。
フィンガープリント UUID	uint8[16]	オペレーティングシステムの固有識別子として機能するフィンガープリント ID 番号(オクテット)。フィンガープリント UUID は、脆弱性データベース (VDB) 内のオペレーティングシステム名、ベンダー、バージョンにマップされます。
フィンガープリントタイプ	uint32	フィンガープリントのタイプを示します。
フィンガープリントソースタイプ	uint32	オペレーティングシステムフィンガープリントを提供するソースのタイプ(ユーザやスキャナ)を示します。
フィンガープリントソース ID	uint32	オペレーティングシステムフィンガープリントを提供した送信元の ID を示します。
最後の確認日時	uint32	トラフィックで前回フィンガープリントを確認した時刻を示します。
TTL 差異	uint8	フィンガープリントの TTL 値と、ホストのフィンガープリント取得に使用したパケットに表示される TTL 値との間の差異を示します。

## レガシー接続データ構造

詳細については、次の項を参照してください。

- [接続統計データブロック 5.0 ~ 5.0.2 \(B-135 ページ\)](#)
- [接続統計データブロック 5.1 \(B-140 ページ\)](#)
- [接続統計データブロック 5.2.x \(B-146 ページ\)](#)
- [接続チャンクデータブロック 5.0 ~ 5.1 \(B-153 ページ\)](#)
- [接続チャンクデータブロック 5.1.1 ~ 6.0.x \(B-154 ページ\)](#)
- [接続統計データブロック 5.1.1.x \(B-156 ページ\)](#)

- [接続統計データ ブロック 5.3 \(B-162 ページ\)](#)
- [接続統計データ ブロック 5.3.1 \(B-169 ページ\)](#)
- [接続統計データ ブロック 5.4 \(B-177 ページ\)](#)
- [接続統計データ ブロック 5.4.1 \(B-191 ページ\)](#)
- [接続統計データ ブロック 6.0.x \(B-205 ページ\)](#)
- [接続統計データ ブロック 6.1.x \(B-222 ページ\)](#)

## 接続統計データ ブロック 5.0 ~ 5.0.2

接続統計データ ブロックは、接続データ メッセージで使用されます。接続統計データ ブロックバージョン 5.0 ~ 5.0.2 のブロック タイプは 115 です。

接続統計データ メッセージの詳細については、[接続統計データ メッセージ \(4-54 ページ\)](#) を参照してください。

次の図は、接続統計データ ブロック 5.0 ~ 5.0.2 の形式を示しています。

::

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続データ ブロック タイプ (115)																																
接続データ ブロック長																																
デバイス ID																																
入力ゾーン																																
入力ゾーン (続き)																																
入力ゾーン (続き)																																
入力ゾーン (続き)																																
出力ゾーン																																
出力ゾーン (続き)																																
出力ゾーン (続き)																																
出力ゾーン (続き)																																
入力インターフェイス																																
入力インターフェイス (続き)																																
入力インターフェイス (続き)																																
入力インターフェイス (続き)																																

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																																
	出力インターフェイス																															
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	イニシエータ IP アドレス																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	レスポнда IP アドレス																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	ポリシー リビジョン																															
	ポリシー リビジョン(続き)																															
	ポリシー リビジョン(続き)																															
	ポリシー リビジョン(続き)																															
	ルール ID																															
	ルール アクション																															
	イニシエータ ポート																レスポнда ポート															
	TCP フラグ																プロトコル								NetFlow ソース							
	NetFlow ソース(続き)																															
	NetFlow ソース(続き)																															
	NetFlow ソース(続き)																															
	NetFlow ソース(続き)																								最初のパケットの時刻							



バイト ビット	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	最初のパケットのタイムスタンプ(続き)																最終パケットの時刻															
	最終パケットのタイムスタンプ(続き)																送信パケット数															
	送信パケット数(続き)																															
	送信パケット数(続き)																受信パケット数															
	受信パケット数(続き)																															
	受信パケット数(続き)																送信バイト数															
	送信バイト数(続き)																															
	受信パケット数(続き)																受信バイト数															
	受信バイト数(続き)																															
	受信バイト数(続き)																ユーザ ID (User ID)															
	ユーザ ID(続き)																															
	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(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(続き)																Web アプリケーション ID															
	Web アプリケーション ID(続き)																															
クライアントアプリケーション URL	文字列ブロック タイプ(続き)																文字列ブロック長															
	文字列ブロック長(続き)																クライアントアプリケーション URL...															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NetBIOS [名前(Name) ]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	NetBIOS 名...																															
クライアント アプリケーション バージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	クライアントアプリケーションバージョン...																															

次の表は、接続統計データブロック 5.0 ~ 5.0.2 のフィールドについての説明です。

表 B-28 接続統計データブロック 5.0 ~ 5.0.2 のフィールド

フィールド	データタイプ	説明
接続統計データブロックタイプ	uint32	接続統計データブロック 5.0 ~ 5.0.2 を開始します。値は常に 115 です。
接続統計データブロック長	uint32	接続統計データブロックのバイト数(接続統計ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポнда IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた関連イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルールアクション	uint32	そのルールに対してユーザインターフェイスで選択されたアクション(allow、block など)。
イニシエータポート	uint16	開始ホストにより使用されるポート。

表 B-28 接続統計データブロック 5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
レスポンスポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス
最初のパケットタイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケットタイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
送信パケット数	uint64	開始ホストからの送信パケット数。
受信パケット数	uint64	応答ホストが送信したパケット数。
送信バイト数	uint64	開始ホストからの送信バイト数。
受信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID (User ID)	uint32	トラフィックを生成したホストの最終ログインユーザの内部 ID 番号。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URL レピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロックタイプ	uint32	クライアントアプリケーション URL の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーション URL の文字列データブロックのバイト数(文字列ブロックタイプと長さのフィールド用の 8 バイト、およびクライアントアプリケーション URL 文字列のバイト数を含む)。
クライアントアプリケーション URL	string	クライアントアプリケーションがアクセスする URL (該当する場合) (/files/index.html など)。
文字列ブロックタイプ	uint32	ホスト NetBIOS 名の文字列データブロックを開始します。この値は常に 0 です。

表 B-28 接続統計データブロック 5.0 ~ 5.0.2 のフィールド(続き)

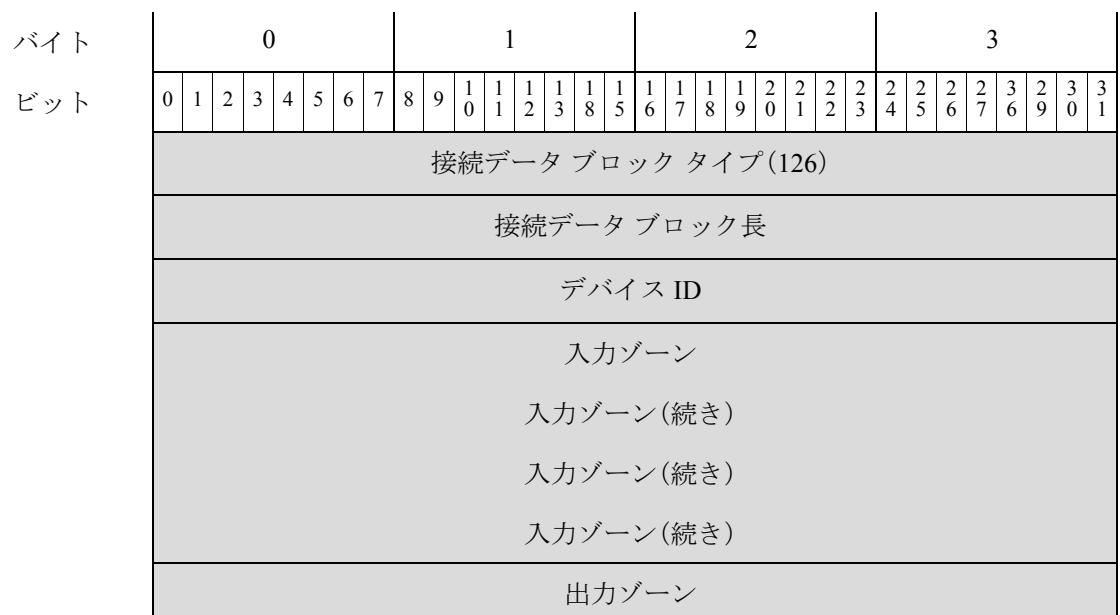
フィールド	データタイプ	説明
文字列ブロック長	uint32	文字列データブロックのバイト数(文字列ブロックタイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロックタイプ	uint32	クライアントアプリケーションバージョンの文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーションバージョンの文字列データブロックのバイト数(文字列ブロックタイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
クライアントアプリケーションバージョン	string	クライアントアプリケーションバージョン。

## 接続統計データ ブロック 5.1

接続統計データブロックは、接続データメッセージで使用されます。バージョン 5.0.2 と 5.1 の間に加えられた接続データブロックの変更には、5.1 で導入された設定パラメータ(ルールアクション理由、モニタールール、セキュリティインテリジェンス送信元/宛先、セキュリティインテリジェンスレイヤ)が指定される新規フィールドの追加が含まれます。接続統計データブロックバージョン 5.1 のブロックタイプは 126 です。

接続統計データメッセージの詳細については、[接続統計データメッセージ\(4-54 ページ\)](#)を参照してください。

次の図は、接続統計データブロック 5.1 の形式を示しています。



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	出力ゾーン(続き)																															
	出力ゾーン(続き)																															
	出力ゾーン(続き)																															
	入力インターフェイス																															
	入力インターフェイス(続き)																															
	入力インターフェイス(続き)																															
	入力インターフェイス(続き)																															
	出力インターフェイス																															
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	イニシエータ IP アドレス																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	レスポнда IP アドレス																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	ポリシー リビジョン																															
	ポリシー リビジョン(続き)																															
	ポリシー リビジョン(続き)																															
	ポリシー リビジョン(続き)																															
	ルール ID																															
	ルール アクション																ルールの理由															

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
	イニシエータ ポート																レスポнда ポート															
	TCP フラグ																プロトコル								NetFlow ソース							
	NetFlow ソース (続き)																															
	NetFlow ソース (続き)																															
	NetFlow ソース (続き)																															
	NetFlow ソース (続き)																								最初のパケットの時刻							
	最初のパケットのタイムスタンプ (続き)																								最終パケットの時刻							
	最終パケットのタイムスタンプ (続き)																								イニシエータ送信パケット数							
	イニシエータ送信パケット数 (続き)																															
	イニシエータ送信パケット数 (続き)																								レスポнда送信パケット数							
	レスポнда送信パケット数 (続き)																															
	レスポнда送信パケット数 (続き)																								イニシエータ送信バイト数							
	イニシエータ送信バイト数 (続き)																															
	イニシエータ送信バイト数 (続き)																								レスポнда送信バイト数							
	レスポнда送信バイト数 (続き)																															
	レスポнда送信バイト数 (続き)																								ユーザ ID (User ID)							
	ユーザ ID (続き)																															
	アプリケーションプロトコル ID (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 (続き)																								URL カテゴリ							
	URL カテゴリ (続き)																															
	URL レピュテーション (続き)																								URL レピュテーション							
	URL レピュテーション (続き)																															
	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							
	URL レピュテーション (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
	クライアントアプリケーション ID(続き)																Web アプリケーション ID															
	Web アプリケーション ID(続き)																文字列ブロック タイプ(0)															
クライアントアプリケーション URL	文字列ブロック タイプ(続き)																文字列ブロック 長															
	文字列ブロック長(続き)																クライアントアプリケーション URL...															
NetBIOS [名前(Name) ]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	NetBIOS 名...																															
クライアントアプリケーションバージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	クライアントアプリケーションバージョン...																															
	モニタ ルール 1																															
	モニタ ルール 2																															
	モニタ ルール 3																															
	モニタ ルール 4																															
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/ 宛先																秒開始レピュ テーション層															

次の表は、接続統計データ ブロック 5.1 のフィールドについての説明です。

表 B-29 接続統計データブロック 5.1 のフィールド

フィールド	データタイプ	説明
接続統計データブロックタイプ	uint32	接続統計データブロック 5.1 を開始します。値は常に 126 です。
接続統計データブロック長	uint32	接続統計データブロックのバイト数(接続統計ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポнда IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに回答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた関連イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルールアクション	uint16	そのルールに対してユーザインターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータポート	uint16	開始ホストにより使用されるポート。
レスポндаポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
最初のパケットタイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケットタイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポнда送信パケット数	uint64	応答ホストが送信したパケット数。



表 B-29 接続統計データブロック 5.1 のフィールド(続き)

フィールド	データタイプ	説明
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポンス送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID (User ID)	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。
アプリケーションプロトコル ID	uint32	アプリケーション プロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URLレピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロックタイプ	uint32	クライアントアプリケーション URL の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーション URL の文字列データブロックのバイト数(文字列ブロックタイプと長さのフィールド用の 8 バイト、およびクライアントアプリケーション URL 文字列のバイト数を含む)。
クライアントアプリケーション URL	string	クライアントアプリケーションがアクセスする URL(該当する場合)(/files/index.html など)。
文字列ブロックタイプ	uint32	ホスト NetBIOS 名の文字列データブロックを開始します。この値は常に 0 です。
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)。
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。

表 B-29 接続統計データブロック 5.1 のフィールド(続き)

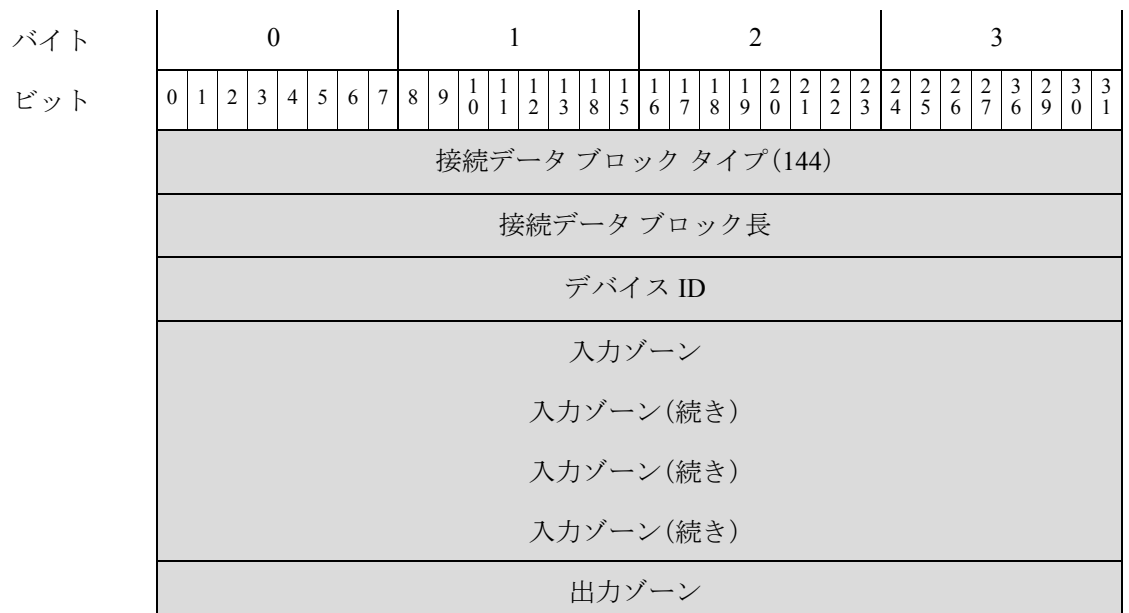
フィールド	データタイプ	説明
モニタールール 3	uint32	接続イベントに関連付けられている 3 番目のモニタールールの ID。
モニタールール 4	uint32	接続イベントに関連付けられている 4 番目のモニタールールの ID。
モニタールール 5	uint32	接続イベントに関連付けられている 5 番目のモニタールールの ID。
モニタールール 6	uint32	接続イベントに関連付けられている 6 番目のモニタールールの ID。
モニタールール 7	uint32	接続イベントに関連付けられている 7 番目のモニタールールの ID。
モニタールール 8	uint32	接続イベントに関連付けられている 8 番目のモニタールールの ID。
セキュリティインテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティインテリジェンス層	uint8	IP ブラックリストに一致した IP 層。

## 接続統計データ ブロック 5.2.x

接続統計データブロックは、接続データメッセージで使用されます。バージョン 5.1.1 と 5.2 の間に加えられた接続データブロックの変更には、地理位置情報をサポートするための新規フィールドの追加が含まれます。バージョン 5.2.x の接続統計データブロックは、シリーズ 1 グループのブロックの、ブロックタイプ 144 です。これにより、ブロックタイプ 137 (接続統計データブロック 5.1.1.x (B-156 ページ)) は廃止されます。

接続統計データメッセージの詳細については、[接続統計データメッセージ \(4-54 ページ\)](#) を参照してください。

次の図は、接続統計データブロック 5.2.x の形式を示しています。



バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	出力ゾーン(続き)																															
	出力ゾーン(続き)																															
	出力ゾーン(続き)																															
	入力インターフェイス																															
	入力インターフェイス(続き)																															
	入力インターフェイス(続き)																															
	入力インターフェイス(続き)																															
	出力インターフェイス																															
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	イニシエータ IP アドレス																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	レスポнда IP アドレス																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	ポリシー リビジョン																															
	ポリシー リビジョン(続き)																															
	ポリシー リビジョン(続き)																															
	ポリシー リビジョン(続き)																															
	ルール ID																															
	ルール アクション																ルールの理由															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	イニシエータ ポート																レスポнда ポート															
	TCP フラグ																プロトコル								NetFlow ソース							
	NetFlow ソース(続き)																															
	NetFlow ソース(続き)																															
	NetFlow ソース(続き)																															
	NetFlow ソース(続き)																								インスタンス ID (Instance ID)							
	インスタンス ID (続き)								接続数カウンタ																最初のパケットの時刻							
	最初のパケットのタイムスタンプ(続き)																								最終パケットの時刻							
	最終パケットのタイムスタンプ(続き)																								イニシエータ送信パケット数							
	イニシエータ送信パケット数(続き)																															
	イニシエータ送信パケット数(続き)																								レスポнда Tx Packets							
	レスポнда送信パケット数(続き)																															
	レスポнда送信パケット数(続き)																								イニシエータ送信バイト数							
	イニシエータ送信バイト数(続き)																															
	イニシエータ送信バイト数(続き)																								レスポнда Tx Bytes							
	レスポнда送信バイト数(続き)																															
	レスポнда送信バイト数(続き)																								ユーザ ID (User ID)							
	ユーザ ID(続き)																															
	アプリケーションプロトコル ID(続き)																								アプリケーションプロトコル ID							
	URL カテゴリ																															
	URL カテゴリ(続き)																								URL レピュテーション							

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																																
	URL レピュテーション(続き)																								クライアント アプリケーション ID							
	クライアントアプリケーションID(続き)																								Web アプリケー ションID							
クライアント URL	Web アプリケーションID(続き)																								文字列ブロック タイプ(0)							
	文字列ブロックタイプ(続き)																								文字列ブロッ ク長							
	文字列ブロック長(続き)																								クライアントア プリケーショ ンURL...							
NetBIOS [名前(Name)]	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	NetBIOS 名...																															
クライアント アプリケー ションバー ジョン	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	クライアントアプリケーションバージョン...																															
	モニタ ルール 1																															
	モニタ ルール 2																															
	モニタ ルール 3																															
	モニタ ルール 4																															
	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															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	侵入イベント カウント																イニシエータの国															
	レスポンドの国																															

次の表は、接続統計データ ブロック 5.2.x のフィールドについての説明です。

表 B-30 接続統計データブロック 5.2.x のフィールド

フィールド	データタイプ	説明
接続統計データブロックタイプ	uint32	接続統計データ ブロック 5.2.x を開始します。値は常に 144 です。
接続統計データブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポンド IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに回答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた関連イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルールアクション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポンド ポート	uint16	回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。

表 B-30 接続統計データブロック 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
インスタンス ID (Instance ID)	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケットタイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケットタイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポнда送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポнда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID (User ID)	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URL レピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロックタイプ	uint32	クライアントアプリケーション URL の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーション URL の文字列データブロックのバイト数(文字列ブロックタイプと長さのフィールド用の 8 バイト、およびクライアントアプリケーション URL 文字列のバイト数を含む)。
クライアントアプリケーション URL	string	クライアントアプリケーションがアクセスする URL (該当する場合) (/files/index.html など)。
文字列ブロックタイプ	uint32	ホスト NetBIOS 名の文字列データブロックを開始します。この値は常に 0 です。
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。

表 B-30 接続統計データブロック 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロックタイプ	uint32	クライアントアプリケーションバージョンの文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーションバージョンの文字列データブロックのバイト数(文字列ブロックタイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
クライアントアプリケーションバージョン	string	クライアントアプリケーションバージョン。
モニタールール 1	uint32	接続イベントに関連付けられている 1 番目のモニタールールの ID。
モニタールール 2	uint32	接続イベントに関連付けられている 2 番目のモニタールールの ID。
モニタールール 3	uint32	接続イベントに関連付けられている 3 番目のモニタールールの ID。
モニタールール 4	uint32	接続イベントに関連付けられている 4 番目のモニタールールの ID。
モニタールール 5	uint32	接続イベントに関連付けられている 5 番目のモニタールールの ID。
モニタールール 6	uint32	接続イベントに関連付けられている 6 番目のモニタールールの ID。
モニタールール 7	uint32	接続イベントに関連付けられている 7 番目のモニタールールの ID。
モニタールール 8	uint32	接続イベントに関連付けられている 8 番目のモニタールールの ID。
セキュリティインテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティインテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイルイベントカウント	uint16	同じ秒で発生するファイルイベントを区別するために使用される値。
侵入イベントカウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポンドの国	uint16	応答ホストの国のコード。



## 接続チャンク データ ブロック 5.0 ~ 5.1

接続チャンク データ ブロックは、NetFlow デバイスによって検出された接続データを伝えます。接続チャンク データ ブロックのブロック タイプは、4.10.1 よりも前のバージョンの場合は 66 です。バージョン 5.0 ~ 5.1 の場合、ブロック タイプは 119 です。

次の図は、接続チャンク データ ブロックの形式を示しています。

バイト	0								1								2								3									
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
接続チャンク ブロック タイプ(66   119)																																		
接続チャンク ブロック長																																		
イニシエータ IP アドレス																																		
レスポнда IP アドレス																																		
開始時刻																																		
アプリケーション ID (Application ID)																																		
レスポнда ポート																プロトコル								接続タイプ										
NetFlow ディテクタ IP アドレス																																		
送信パケット数																																		
受信パケット数																																		
送信バイト数																																		
受信バイト数																																		
接続																																		

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

表 B-31 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、バージョン 4.10.1 以前の場合は 66、バージョン 5.0 の場合は 119 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)。

表 B-31 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
イニシエータ IP アドレス	uint8[4]	IP アドレス オクテットの、接続を開始したホストの IP アドレス。
レスポнда IP アドレス	uint8[4]	IP アドレス オクテットの、接続で応答するホストの IP アドレス。
開始時刻	uint32	接続チャンクの開始時刻。
アプリケーション ID (Application ID)	uint32	接続で使用されるアプリケーション プロトコルのアプリケーション ID 番号。
レスポнда ポート	uint16	接続チャンクでレスポндаが使用したポート。
プロトコル	uint8	ユーザ情報を含むパケットのプロトコル。
接続タイプ	uint8	接続の種類。
送信元 デバイス 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	uint32	接続チャンクで送信されたパケット数。
受信パケット数	uint32	接続チャンクで受信されたパケット数。
送信バイト数	uint32	接続チャンクで送信されたバイト数。
受信バイト数	uint32	接続チャンクで受信されたバイト数。
接続	uint32	接続チャンクで行われたセッション数。

## 接続チャンク データ ブロック 5.1.1 ~ 6.0.x

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。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 グループの 136 です。これはブロック タイプ 119 に取って代わります。

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
	レスポンド ポート																プロトコル								接続タイプ							
	NetFlow ディテクタ IP アドレス																															
	送信パケット数 送信パケット数(続き)																															
	受信パケット数 受信パケット数(続き)																															
	送信バイト数 送信バイト数(続き)																															
	受信バイト数 受信バイト数(続き)																															
	接続																															

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

表 B-32 接続チャンク データ ブロックのフィールド

フィールド	データタイプ	説明
接続チャンク ブロックタイプ	uint32	接続チャンク データ ブロックを開始します。この値は常に 136 です。
接続チャンク ブロック長	uint32	接続チャンク データ ブロックのバイト数(接続チャンク ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く接続チャンク データのバイト数を含む)。
イニシエータ IP アドレス	uint8(4)	この接続タイプのイニシエータの IP アドレス。これはレスポンド IP アドレスとともに、複数の同じ接続を見分けるために使用されます。
レスポンド 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。これはイニシエータ IP アドレスとともに、複数の同じ接続を見分けるために使用されます。
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。

表 B-32 接続チャンク データブロックのフィールド(続き)

フィールド	データタイプ	説明
接続タイプ	uint8	接続の種類。
NetFlow ディテクタ IP アドレス	uint8[4]	IP アドレス オクテットの、接続を検出した NetFlow デバイスの IP アドレス。
送信パケット数	uint64	接続チャンクで送信されたパケット数。
受信パケット数	uint64	接続チャンクで受信されたパケット数。
送信バイト数	uint64	接続チャンクで送信されたバイト数。
受信バイト数	uint64	接続チャンクで受信されたバイト数。
接続	uint32	5 分間の接続数。

## 接続統計データ ブロック 5.1.1.x

接続統計データ ブロックは、接続データ メッセージで使用されます。バージョン 5.1 と 5.1.1 の間に加えられた接続データ ブロックの変更には、関連する侵入イベントを識別するための新規フィールドの追加が含まれます。接続統計データ ブロックバージョン 5.1.1.x のブロックタイプは 137 です。これにより、ブロックタイプ 126 ([接続統計データ ブロック 5.1 \(B-140 ページ\)](#)) は廃止されます。

接続統計データ メッセージの詳細については、[接続統計データ メッセージ \(4-54 ページ\)](#) を参照してください。

次の図は、接続統計データ ブロック 5.1.1 の形式を示しています。



バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	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
	出力ゾーン(続き)																																							
	入力インターフェイス																																							
	入力インターフェイス(続き)																																							
	入力インターフェイス(続き)																																							
	入力インターフェイス(続き)																																							
	出力インターフェイス																																							
	出力インターフェイス(続き)																																							
	出力インターフェイス(続き)																																							
	出力インターフェイス(続き)																																							
	イニシエータ IP アドレス																																							
	イニシエータ IP アドレス(続き)																																							
	イニシエータ IP アドレス(続き)																																							
	イニシエータ IP アドレス(続き)																																							
	レスポнда IP アドレス																																							
	レスポнда IP アドレス(続き)																																							
	レスポнда IP アドレス(続き)																																							
	レスポнда IP アドレス(続き)																																							
	ポリシー リビジョン																																							
	ポリシー リビジョン(続き)																																							
	ポリシー リビジョン(続き)																																							
	ポリシー リビジョン(続き)																																							
	ルール ID																																							
	ルール アクション																				ルールの理由																			
	イニシエータ ポート																				レスポнда ポート																			
	TCP フラグ																				プロトコル										NetFlow ソース									

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	NetFlow ソース (続き)																															
	NetFlow ソース (続き)																															
	NetFlow ソース (続き)																															
	NetFlow ソース (続き)																								インスタンス ID (Instance ID)							
	インスタンス ID (続き)								接続数カウンタ																最初のパケットの時刻							
	最初のパケットのタイムスタンプ (続き)																								最終パケットの時刻							
	最終パケットのタイムスタンプ (続き)																								イニシエータ送信パケット数							
	イニシエータ送信パケット数 (続き)																															
	イニシエータ送信パケット数 (続き)																								レスポнда Tx Packets							
	レスポнда送信パケット数 (続き)																															
	レスポнда送信パケット数 (続き)																								イニシエータ送信バイト数							
	イニシエータ送信バイト数 (続き)																															
	イニシエータ送信バイト数 (続き)																								レスポнда Tx Bytes							
	レスポнда送信バイト数 (続き)																															
	レスポнда送信バイト数 (続き)																								ユーザ ID (User ID)							
	ユーザ ID (続き)																															
	アプリケーションプロトコル ID (続き)																								アプリケーションプロトコル ID							
	URL カテゴリ (続き)																															
	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)																															
	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																															

次の表は、接続統計データ ブロック 5.1.1.x のフィールドについての説明です。

表 B-33 接続統計データブロック 5.1.1.x のフィールド

フィールド	データタイプ	説明
接続統計データブロックタイプ	uint32	接続統計データブロック 5.1.1.x を開始します。値は常に 137 です。
接続統計データブロック長	uint32	接続統計データブロックのバイト数(接続統計ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポнда IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに回答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた関連イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルールアクション	uint16	そのルールに対してユーザインターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータポート	uint16	開始ホストにより使用されるポート。
レスポндаポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID (Instance ID)	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケットタイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケットタイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。



表 B-33 接続統計データブロック 5.1.1.x のフィールド(続き)

フィールド	データタイプ	説明
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポнда送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポнда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID (User ID)	uint32	トラフィックを生成したホストの最終ログインユーザの内部 ID 番号。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URLレピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロックタイプ	uint32	クライアントアプリケーション URL の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーション URL の文字列データブロックのバイト数(文字列ブロックタイプと長さのフィールド用の 8 バイト、およびクライアントアプリケーション URL 文字列のバイト数を含む)。
クライアントアプリケーション URL	string	クライアントアプリケーションがアクセスする URL (該当する場合) (/files/index.html など)。
文字列ブロックタイプ	uint32	ホスト NetBIOS 名の文字列データブロックを開始します。この値は常に 0 です。
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 B-33 接続統計データブロック 5.1.1.x のフィールド(続き)

フィールド	データタイプ	説明
クライアントアプリケーションバージョン	string	クライアントアプリケーションバージョン。
モニタールール 1	uint32	接続イベントに関連付けられている 1 番目のモニタールールの ID。
モニタールール 2	uint32	接続イベントに関連付けられている 2 番目のモニタールールの ID。
モニタールール 3	uint32	接続イベントに関連付けられている 3 番目のモニタールールの ID。
モニタールール 4	uint32	接続イベントに関連付けられている 4 番目のモニタールールの ID。
モニタールール 5	uint32	接続イベントに関連付けられている 5 番目のモニタールールの ID。
モニタールール 6	uint32	接続イベントに関連付けられている 6 番目のモニタールールの ID。
モニタールール 7	uint32	接続イベントに関連付けられている 7 番目のモニタールールの ID。
モニタールール 8	uint32	接続イベントに関連付けられている 8 番目のモニタールールの ID。
セキュリティインテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティインテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイルイベントカウント	uint16	同じ秒で発生するファイルイベントを区別するために使用される値。
侵入イベントカウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。

## 接続統計データ ブロック 5.3

接続統計データブロックは、接続データメッセージで使用されます。バージョン 5.2.x と 5.3 の間に加えられた接続データブロックの変更には、NetFlow 情報用の新規フィールドの追加が含まれます。バージョン 5.3 の接続統計データブロックは、シリーズ 1 グループのブロックの、ブロックタイプ 152 です。これにより、ブロックタイプ 144 ([接続統計データ ブロック 5.2.x \(B-146 ページ\)](#)) は廃止されます。

接続イベントレコードを要求するには、イベントバージョン 10 およびイベントコード 71 の要求メッセージ内に、拡張イベントフラグ (要求フラグフィールドのビット 30) を設定します。[要求フラグ \(2-12 ページ\)](#) 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\(4-54 ページ\)](#) を参照してください。

次の図は、接続統計データ ブロック 5.3+の形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	接続データ ブロック タイプ (152)																															
	接続データ ブロック長																															
	デバイス ID																															
	入力ゾーン 入力ゾーン(続き) 入力ゾーン(続き) 入力ゾーン(続き)																															
	出力ゾーン 出力ゾーン(続き) 出力ゾーン(続き) 出力ゾーン(続き)																															
	入力インターフェイス 入力インターフェイス(続き) 入力インターフェイス(続き) 入力インターフェイス(続き)																															
	出力インターフェイス 出力インターフェイス(続き) 出力インターフェイス(続き) 出力インターフェイス(続き)																															
	イニシエータ IP アドレス イニシエータ IP アドレス(続き) イニシエータ IP アドレス(続き) イニシエータ IP アドレス(続き)																															

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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)																レスポнда Tx Bytes															
	イニシエータ送信バイト数(続き)																レスポнда送信バイト数(続き)															
	レスポнда送信バイト数(続き)																ユーザ ID (User ID)															
	ユーザ ID(続き)																アプリケーションプロトコル ID															
	アプリケーションプロトコル ID(続き)																URL カテゴリ															
	URL カテゴリ(続き)																URL レピュテーション															
	URL レピュテーション(続き)																クライアントアプリケーション ID															
	クライアントアプリケーション ID(続き)																Web アプリケーション ID															
クライアント URL	Web アプリケーション ID(続き)																文字列ブロックタイプ(0)															
	文字列ブロックタイプ(続き)																文字列ブロック長															
	文字列ブロック長(続き)																クライアントアプリケーション URL...															
NetBIOS [名前(Name)]	文字列ブロックタイプ(0)																															
	文字列ブロック長																NetBIOS 名...															
クライアントアプリケーションバージョン	文字列ブロックタイプ(0)																															
	文字列ブロック長																クライアントアプリケーションバージョン...															
	モニターール 1																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	モニタ ルール 2																															
	モニタ ルール 3																															
	モニタ ルール 4																															
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/ 宛先								秒イニシエー タ層								ファイル イベント カウント															
	侵入イベント カウント																イニシエータの国															
	レスポндаの国																IOC 番号															
	送信元自律システム																															
	宛先自律システム																															
	SNMP 入力																SNMP 出力															
	送信元 TOS								宛先 TOS								送信元マスク								宛先マスク							

次の表は、接続統計データ ブロック 5.3 のフィールドについての説明です。

表 B-34 接続統計データ ブロック 5.3+のフィールド

フィールド	データタイプ	説明
接続統計データ ブロックタイプ	uint32	接続統計データ ブロック 5.3 を開始します。値は常に 152 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティゾーン。

表 B-34 接続統計データブロック 5.3+のフィールド(続き)

フィールド	データタイプ	説明
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポнда IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた関連イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アクション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータポート	uint16	開始ホストにより使用されるポート。
レスポндаポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID (Instance ID)	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケットタイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケットタイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポнда送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポнда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID (User ID)	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。

表 B-34 接続統計データブロック 5.3+のフィールド(続き)

フィールド	データタイプ	説明
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)。
クライアントアプリケーションバージョン	string	クライアントアプリケーションバージョン。
モニタールール 1	uint32	接続イベントに関連付けられている 1 番目のモニタールールの ID。
モニタールール 2	uint32	接続イベントに関連付けられている 2 番目のモニタールールの ID。
モニタールール 3	uint32	接続イベントに関連付けられている 3 番目のモニタールールの ID。
モニタールール 4	uint32	接続イベントに関連付けられている 4 番目のモニタールールの ID。



表 B-34 接続統計データブロック 5.3+のフィールド(続き)

フィールド	データタイプ	説明
モニターール 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。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。
SNMP 出力	uint16	出力インターフェイスの SNMP インデックス
送信元 TOS	uint8	着信インターフェイス用のタイプオブサービスバイト設定。
宛先 TOS	uint8	発信インターフェイス用のタイプオブサービスバイト設定。
送信元マスク	uint8	送信元アドレスプレフィックスマスク。
宛先マスク	uint8	宛先アドレスプレフィックスマスク。

## 接続統計データブロック 5.3.1

接続統計データブロックは、接続データメッセージで使用されます。バージョン 5.3 と 5.3.1 との間で加えられた接続データブロックの唯一の変更は、セキュリティコンテキストフィールドの追加です。バージョン 5.3.1 の接続統計データブロックは、シリーズ 1 グループのブロックの、ブロックタイプ 154 です。これにより、ブロックタイプ 152(接続統計データブロック 5.3 (B-162 ページ))は廃止されます。

接続イベントレコードを要求するには、イベントバージョン 11 およびイベントコード 71 の要求メッセージ内に、拡張イベントフラグ(要求フラグフィールドのビット 30)を設定します。[要求フラグ\(2-12 ページ\)](#)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\(4-54 ページ\)](#)を参照してください。

次の図は、接続統計データブロック 5.3.1 の形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続データブロックタイプ(154)																																
接続データブロック長																																
デバイス ID(Device ID)																																
入力ゾーン																																
入力ゾーン(続き)																																
入力ゾーン(続き)																																
入力ゾーン(続き)																																
出力ゾーン																																
出力ゾーン(続き)																																
出力ゾーン(続き)																																
出力ゾーン(続き)																																
入力インターフェイス																																
入力インターフェイス(続き)																																
入力インターフェイス(続き)																																
入力インターフェイス(続き)																																
出力インターフェイス																																
出力インターフェイス(続き)																																
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)																																

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	イニシエータ送信パケット数(続き)																レスポнда Tx Packets															
	レスポнда送信パケット数(続き)																															
	レスポнда送信パケット数(続き)																イニシエータ送信バイト数															
	イニシエータ送信バイト数(続き)																															
	イニシエータ送信バイト数(続き)																レスポнда Tx Bytes															
	レスポнда送信バイト数(続き)																															
	レスポнда送信バイト数(続き)																ユーザ ID (User ID)															
	ユーザ ID(続き)																アプリケーションプロトコル ID															
	アプリケーションプロトコル ID(続き)																URL カテゴリ															
	URL カテゴリ(続き)																URL レピュテーション															
	URL レピュテーション(続き)																クライアントアプリケーション ID															
	クライアントアプリケーション ID(続き)																Web アプリケーション ID															
クライアント URL	Web アプリケーション ID(続き)																文字列ブロックタイプ(0)															
	文字列ブロックタイプ(続き)																文字列ブロック長															
	文字列ブロック長(続き)																クライアントアプリケーション URL...															
NetBIOS [名前(Name)]	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	NetBIOS 名...																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	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バージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	クライアントアプリケーションバージョン...																															
	モニタ ルール 1																															
	モニタ ルール 2																															
	モニタ ルール 3																															
	モニタ ルール 4																															
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/宛先								秒イニシエータ層								ファイル イベント カウント															
	侵入イベント カウント																イニシエータの国															
	レスポндаの国																IOC 番号															
	送信元自律システム																															
	宛先自律システム																															
	SNMP 入力																SNMP 出力															
	送信元 TOS								宛先 TOS								送信元マスク								宛先マスク							
	セキュリティ コンテキスト																															
	セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト(続き)																															

次の表は、接続統計データ ブロック 5.3.1 のフィールドについての説明です。

表 B-35 接続統計データブロック 5.3.1 のフィールド

フィールド	データタイプ	説明
接続統計データブロックタイプ	uint32	接続統計データブロック 5.3.1+ を開始します。値は常に 154 です。
接続統計データブロック長	uint32	接続統計データブロックのバイト数(接続統計ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID (Device ID)	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポнда IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに回答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた関連イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アクション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータポート	uint16	開始ホストにより使用されるポート。
レスポндаポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID (Instance ID)	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケットタイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。

表 B-35 接続統計データブロック 5.3.1 のフィールド(続き)

フィールド	データタイプ	説明
最終パケットタイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポнда送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポнда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID (User ID)	uint32	トラフィックを生成したホストの最終ログインユーザの内部 ID 番号。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URLレピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロックタイプ	uint32	クライアントアプリケーション URL の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーション URL の文字列データブロックのバイト数(文字列ブロックタイプと長さのフィールド用の 8 バイト、およびクライアントアプリケーション URL 文字列のバイト数を含む)。
クライアントアプリケーション URL	string	クライアントアプリケーションがアクセスする URL(該当する場合) (/files/index.html など)。
文字列ブロックタイプ	uint32	ホスト NetBIOS 名の文字列データブロックを開始します。この値は常に 0 です。
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 B-35 接続統計データブロック 5.3.1 のフィールド(続き)

フィールド	データタイプ	説明
クライアントアプリケーションバージョン	string	クライアントアプリケーションバージョン。
モニタールール 1	uint32	接続イベントに関連付けられている 1 番目のモニタールールの ID。
モニタールール 2	uint32	接続イベントに関連付けられている 2 番目のモニタールールの ID。
モニタールール 3	uint32	接続イベントに関連付けられている 3 番目のモニタールールの ID。
モニタールール 4	uint32	接続イベントに関連付けられている 4 番目のモニタールールの ID。
モニタールール 5	uint32	接続イベントに関連付けられている 5 番目のモニタールールの ID。
モニタールール 6	uint32	接続イベントに関連付けられている 6 番目のモニタールールの ID。
モニタールール 7	uint32	接続イベントに関連付けられている 7 番目のモニタールールの ID。
モニタールール 8	uint32	接続イベントに関連付けられている 8 番目のモニタールールの ID。
セキュリティインテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティインテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイルイベントカウント	uint16	同じ秒で発生するファイルイベントを区別するために使用される値。
侵入イベントカウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポンドの国	uint16	応答ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。
SNMP 出力	uint16	出力インターフェイスの SNMP インデックス
送信元 TOS	uint8	着信インターフェイス用のタイプオブサービスバイト設定。
宛先 TOS	uint8	発信インターフェイス用のタイプオブサービスバイト設定。



表 B-35 接続統計データブロック 5.3.1 のフィールド(続き)

フィールド	データタイプ	説明
送信元マスク	uint8	送信元アドレスプレフィックスマスク。
宛先マスク	uint8	宛先アドレスプレフィックスマスク。
セキュリティコンテキスト	uint8(16)	トラフィックが通過したセキュリティコンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキストモードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

## 接続統計データブロック 5.4

接続統計データブロックは、接続データメッセージで使用されます。接続統計データブロック 5.4 には、いくつかの新しいフィールドが追加されました。SSL 接続、HTTP リダイレクション、およびネットワーク分析ポリシーをサポートするためのフィールドが追加されています。バージョン 5.4 の接続統計データブロックは、シリーズ 1 グループのブロックの、ブロックタイプ 155 です。これにより、ブロックタイプ 154(接続統計データブロック 5.3.1(B-169 ページ))は廃止されます。

接続イベントレコードを要求するには、イベントバージョン 12 およびイベントコード 71 の要求メッセージ内に、拡張イベントフラグ(要求フラグフィールドのビット 30)を設定します。要求フラグ(2-12 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(4-54 ページ)を参照してください。

次の図は、接続統計データブロック 5.4 の形式を示しています。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
接続データブロックタイプ(155)																																								
接続データブロック長																																								
デバイス ID(Device ID)																																								
入力ゾーン																																								
入力ゾーン(続き)																																								
入力ゾーン(続き)																																								
入力ゾーン(続き)																																								
出力ゾーン																																								
出力ゾーン(続き)																																								

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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)																															
	入力インターフェイス																															
	入力インターフェイス(続き)																															
	入力インターフェイス(続き)																															
	入力インターフェイス(続き)																															
	出力インターフェイス																															
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	イニシエータ IP アドレス																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	レスポнда IP アドレス																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	ポリシー リビジョン																															
	ポリシー リビジョン(続き)																															
	ポリシー リビジョン(続き)																															
	ポリシー リビジョン(続き)																															
	ルール ID																															
	ルール アクション																ルールの理由															
	イニシエータ ポート																レスポнда ポート															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	TCP フラグ																プロトコル								NetFlow ソース							
	NetFlow ソース (続き)																															
	NetFlow ソース (続き)																															
	NetFlow ソース (続き)																															
	NetFlow ソース (続き)																								インスタンス ID (Instance ID)							
	インスタンス ID (続き)								接続数カウンタ																最初のパケットの時刻							
	最初のパケットのタイムスタンプ (続き)																								最終パケットの時刻							
	最終パケットのタイムスタンプ (続き)																															
	イニシエータ送信パケット数 (続き)																															
	イニシエータ送信パケット数 (続き)																								レスポнда Tx Packets							
	レスポнда送信パケット数 (続き)																															
	レスポнда送信パケット数 (続き)																								イニシエータ送信バイト数							
	イニシエータ送信バイト数 (続き)																															
	イニシエータ送信バイト数 (続き)																								レスポнда Tx Bytes							
	レスポнда送信バイト数 (続き)																															
	レスポнда送信バイト数 (続き)																								ユーザ ID (User ID)							
	ユーザ ID (続き)																															
	アプリケーションプロトコル ID (続き)																								アプリケーションプロトコル ID							
	URL カテゴリ (続き)																															
	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)																															
	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															

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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																															
	SSL ポリシー ID(続き)																															
	SSL ポリシー ID(続き)																															
	SSL ポリシー ID(続き)																															
	SSL ルール ID																															
	SSL 暗号スイート																SSL バージョン								SSL キー証明書統計							
	SSL キー証明書統計(続き)								実際の SSL アクション																予期された SSL アクション							
	予期された SSL アクション(続き)								SSL フロー ステータス																SSL フロー エラー							
	SSL フロー エラー(続き)																SSL フロー メッセージ															
	SSL フロー メッセージ(続き)																SSL フロー フラグ															
	SSL フロー フラグ(続き)																															
SSL サーバー名	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 サーバー名...															
	SSL URL カテゴリ																															
	SSL セッション ID																															
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															
	SSL セッション ID(続き)																															

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

次の表は、接続統計データ ブロック 5.4+ のフィールドについての説明です。

表 B-36 接続統計データ ブロック 5.4+ のフィールド

フィールド	データ タイプ	説明
接続統計データ ブロック タイプ	uint32	接続統計データ ブロック 5.4+ を開始します。値は常に 155 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID (Device ID)	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティゾーン。

表 B-36 接続統計データブロック 5.4+ のフィールド(続き)

フィールド	データタイプ	説明
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポнда IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに回答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた関連イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アクション	uint16	そのルールに対してユーザ インターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータポート	uint16	開始ホストにより使用されるポート。
レスポндаポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID (Instance ID)	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケットタイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
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。



表 B-36 接続統計データブロック 5.4+ のフィールド(続き)

フィールド	データタイプ	説明
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)。
クライアントアプリケーションバージョン	string	クライアントアプリケーションバージョン。
モニタールール 1	uint32	接続イベントに関連付けられている 1 番目のモニタールールの ID。
モニタールール 2	uint32	接続イベントに関連付けられている 2 番目のモニタールールの ID。
モニタールール 3	uint32	接続イベントに関連付けられている 3 番目のモニタールールの ID。

表 B-36 接続統計データブロック 5.4+ のフィールド(続き)

フィールド	データタイプ	説明
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス 送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス 層	uint8	IP ブラックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入イベント カウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータ の国	uint16	開始ホストの国のコード。
レスポндаの国	uint 16	応答ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。
SNMP 出力	uint16	出力インターフェイスの SNMP インデックス
送信元 TOS	uint8	着信インターフェイス用のタイプ オブ サービス バイト設定。
宛先 TOS	uint8	発信インターフェイス用のタイプ オブ サービス バイト設定。
送信元マスク	uint8	送信元アドレス プレフィックス マスク。
宛先マスク	uint8	宛先アドレス プレフィックス マスク。
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。

表 B-36 接続統計データブロック 5.4+ のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロックタイプ	uint32	参照ホストを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	参照ホスト文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および参照ホストフィールドのバイト数を含む)。
参照ホスト	string	HTTP または DNS で提供されるホスト名情報。
文字列ブロックタイプ	uint32	ユーザエージェントを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザエージェント文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびユーザエージェントフィールドのバイト数を含む)。
ユーザエージェント	string	セッションのユーザエージェントヘッダーフィールドからの情報。
文字列ブロックタイプ	uint32	HTTP リファラを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	HTTP リファラ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および HTTP リファラフィールドのバイト数を含む)。
HTTP リファラ	string	ページの発生元のサイト。これは HTTP トラフィック内の参照ヘッダー情報にあります。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の SHA1 ハッシュ。
SSL ポリシー ID	uint8[16]	接続を処理した SSL ポリシーの ID 番号。
SSL ルール ID	uint32	接続を処理した SSL ルールまたはデフォルトアクションの ID 番号。
SSL 暗号スイート	uint16	SSL 接続で使用される暗号スイート。値は 10 進形式で保存されます。値により指定されている暗号スイートの詳細については、 <a href="http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml">www.iana.org/assignments/tls-parameters/tls-parameters.xhtml</a> を参照してください。
SSL バージョン	uint8	接続の暗号化に使用された SSL または TLS プロトコルバージョン。

表 B-36 接続統計データブロック 5.4+ のフィールド(続き)

フィールド	データタイプ	説明
SSL サーバ証明書ステータス	uint16	<p>SSL 証明書のステータス。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>2(有効):サーバ証明書は有効です。</li> <li>4(自己署名済み):サーバ証明書は自己署名です。</li> <li>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。</li> <li>32(無効な署名):サーバ証明書に無効な署名があります。</li> <li>64(期限切れ):サーバ証明書は期限切れです。</li> <li>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。</li> <li>256(取り消し):サーバ証明書は取り消されました。</li> </ul>
実際の SSL アクション	uint16	<p>SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>0:「不明」</li> <li>1:「復号しない」</li> <li>2:「ブロックする」</li> <li>3:「リセットでブロック」</li> <li>4:「復号(既知のキー)」</li> <li>5:「復号(置換キー)」</li> <li>6:「復号(Resign)」</li> </ul>
予期された SSL アクション	uint16	<p>SSL ルールに基づいて接続に対して実行する必要があるアクション。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>0:「不明」</li> <li>1:「復号しない」</li> <li>2:「ブロックする」</li> <li>3:「リセットでブロック」</li> <li>4:「復号(既知のキー)」</li> <li>5:「復号(置換キー)」</li> <li>6:「復号(Resign)」</li> </ul>

表 B-36 接続統計データブロック 5.4+ のフィールド(続き)

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

表 B-36 接続統計データブロック 5.4+ のフィールド(続き)

フィールド	データタイプ	説明
SSL フローメッセージ	uint32	<p>SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、<a href="http://tools.ietf.org/html/rfc5246">http://tools.ietf.org/html/rfc5246</a> を参照してください。</p> <ul style="list-style-type: none"> <li>0x00000001:NSE_MT__HELLO_REQUEST</li> <li>0x00000002:NSE_MT__CLIENT_ALERT</li> <li>0x00000004:NSE_MT__SERVER_ALERT</li> <li>0x00000008:NSE_MT__CLIENT_HELLO</li> <li>0x00000010:NSE_MT__SERVER_HELLO</li> <li>0x00000020:NSE_MT__SERVER_CERTIFICATE</li> <li>0x00000040:NSE_MT__SERVER_KEY_EXCHANGE</li> <li>0x00000080:NSE_MT__CERTIFICATE_REQUEST</li> <li>0x00000100:NSE_MT__SERVER_HELLO_DONE</li> <li>0x00000200:NSE_MT__CLIENT_CERTIFICATE</li> <li>0x00000400:NSE_MT__CLIENT_KEY_EXCHANGE</li> <li>0x00000800:NSE_MT__CERTIFICATE_VERIFY</li> <li>0x00001000:NSE_MT__CLIENT_CHANGE_CIPHER_SPEC</li> <li>0x00002000:NSE_MT__CLIENT_FINISHED</li> <li>0x00004000:NSE_MT__SERVER_CHANGE_CIPHER_SPEC</li> <li>0x00008000:NSE_MT__SERVER_FINISHED</li> <li>0x00010000:NSE_MT__NEW_SESSION_TICKET</li> <li>0x00020000:NSE_MT__HANDSHAKE_OTHER</li> <li>0x00040000:NSE_MT__APP_DATA_FROM_CLIENT</li> <li>0x00080000:NSE_MT__APP_DATA_FROM_SERVER</li> </ul>
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"> <li>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</li> <li>0x00000002 (NSE_FLOW__INITIALIZED):内部構造が処理可能です</li> <li>0x00000004 (NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました</li> </ul>
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)。
SSL サーバ名	string	SSL Client Hello でサーバ名に指定された名前。

表 B-36 接続統計データブロック 5.4+ のフィールド(続き)

フィールド	データタイプ	説明
SSL URL カテゴリ	uint32	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできます。
SSL チケット ID	uint8[20]	クライアントとサーバがセッション チケットの使用に同意する場合に使用されるセッション チケットのハッシュ。
SSL チケット ID の長さ	uint8	SSL チケット ID の長さ。チケット ID は 20 バイトより長くすることはできませんが、20 バイト未満であってもかまいません。
ネットワーク分析ポリシー リビジョン	uint8[16]	接続イベントに関連付けられているネットワーク分析ポリシーのリビジョン。

## 接続統計データ ブロック 5.4.1

接続統計データ ブロックは、接続データ メッセージで使用されます。接続統計データ ブロック 5.4 には、いくつかの新しいフィールドが追加されました。SSL 接続、HTTP リダイレクション、およびネットワーク分析ポリシーをサポートするためのフィールドが追加されています。バージョン 5.4+ の接続統計データ ブロックは、シリーズ 1 グループのブロックの、ブロック タイプ 157 です。これにより、ブロック タイプ 155 (接続統計データ ブロック 5.3.1 (B-169 ページ)) は廃止されます。

接続イベント レコードを要求するには、イベント バージョン 12 およびイベント コード 71 の要求メッセージ内に、拡張イベント フラグ (要求フラグ フィールドのビット 30) を設定します。要求フラグ (2-12 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 (4-54 ページ) を参照してください。

次の図は、接続統計データ ブロック 5.4+ の形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	接続データ ブロック タイプ (157)																															
	接続データ ブロック長																															
	デバイス ID (Device ID)																															
	入力ゾーン																															

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



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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ユーザ ID (続き)																								アプリケーション プロトコル ID							
	アプリケーションプロトコル ID (続き)																								URL カテゴリ							
	URL カテゴリ (続き)																								URL レピュテー ション							
	URL レピュテーション (続き)																								クライアント アプリケー ション ID							
	クライアント アプリケーション ID (続き)																								Web アプリケー ション ID							
クライアント URL	Web アプリケーション ID (続き)																								文字列ブロック タイプ (0)							
	文字列ブロック タイプ (続き)																								文字列ブロッ ク長							
	文字列ブロック長 (続き)																								クライアント ア プリケーショ ン URL...							
NetBIOS [名前 (Name)]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	NetBIOS 名...																															
クライアント アプリケーション バージョン	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	クライアントアプリケーションバージョン...																															
	モニタ ルール 1																															
	モニタ ルール 2																															
	モニタ ルール 3																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	モニタ ルール 4																															
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/ 宛先								秒イニシエー タ層								ファイル イベント カウント															
	侵入イベント カウント																イニシエータの国															
	レスポндаの国																IOC 番号															
	送信元自律システム																															
	宛先自律システム																															
	SNMP 入力																SNMP 出力															
	送信元 TOS								宛先 TOS								送信元マスク								宛先マスク							
	セキュリティ コンテキスト																															
	セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト(続き)																															
参照ホスト	VLAN ID (Admin. VLAN ID)																文字列ブロック タイプ (0)															
	文字列ブロック タイプ (0) (続き)																文字列ブロック長															
	文字列ブロック長(続き)																参照ホスト...															
ユーザエージェント	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザ エージェント...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
HTTP リファラ	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	HTTP リファラ...																															
	SSL 証明書フィンガープリント																															
	SSL 証明書フィンガープリント(続き)																															
	SSL 証明書フィンガープリント(続き)																															
	SSL 証明書フィンガープリント(続き)																															
	SSL 証明書フィンガープリント(続き)																															
	SSL ポリシー ID																															
	SSL ポリシー ID(続き)																															
	SSL ポリシー ID(続き)																															
	SSL ポリシー ID(続き)																															
SSL ルール ID																																
SSL 暗号スイート																SSL バージョン								SSL キー証明書統計								
SSL キー証明書統計(続き)								実際の SSL アクション																予期された SSL アクション								
予期された SSL アクション(続き)								SSL フローステータス																SSL フローエラー								
SSL フローエラー(続き)																SSL フローメッセージ																
SSL フローメッセージ(続き)																SSL フローフラグ																
SSL フローフラグ(続き)																																



次の表は、接続統計データ ブロック 5.4+ のフィールドについての説明です。

表 B-37 接続統計データ ブロック 5.4+ のフィールド

フィールド	データタイプ	説明
接続統計データ ブロックタイプ	uint32	接続統計データ ブロック 5.4+を開始します。値は常に 157 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロックタイプ と長さのフィールド用の 8 バイト、およびそれに続く接続 データのバイト数を含む)。
デバイス ID (Device ID)	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティ ゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティ ゾーン。
入力インター フェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インター フェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッション を開始したホストの IP アドレス。
レスポнда IP ア ドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。
ポリシー リビ ジョン	uint8[16]	トリガーされた関連イベントに関連付けられているルール のリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルール アク ション	uint16	そのルールに対してユーザ インターフェイスで選択された アクション(allow、block など)。
ルールの理由	uint16	イベントをトリガーしたルールの理由。
イニシエータ ポート	uint16	開始ホストにより使用されるポート。
レスポнда ポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID (Instance ID)	uint16	イベントを生成した管理対象デバイスの Snort インスタンス の数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用 される値。

表 B-37 接続統計データブロック 5.4+のフィールド(続き)

フィールド	データタイプ	説明
最初のパケットタイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケットタイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポнда送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポнда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID (User ID)	uint32	トラフィックを生成したホストの最終ログインユーザの内部 ID 番号。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URLレピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロックタイプ	uint32	クライアントアプリケーション URL の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーション URL の文字列データブロックのバイト数(文字列ブロックタイプと長さのフィールド用の 8 バイト、およびクライアントアプリケーション URL 文字列のバイト数を含む)。
クライアントアプリケーション URL	string	クライアントアプリケーションがアクセスする URL(該当する場合)(/files/index.html など)。
文字列ブロックタイプ	uint32	ホスト NetBIOS 名の文字列データブロックを開始します。この値は常に 0 です。
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。

表 B-37 接続統計データブロック 5.4+ のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	クライアントアプリケーションバージョンの文字列データブロックのバイト数(文字列ブロックタイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
クライアントアプリケーションバージョン	string	クライアントアプリケーションバージョン。
モニタルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタルールの ID。
モニタルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタルールの ID。
モニタルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタルールの ID。
モニタルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタルールの ID。
モニタルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタルールの ID。
モニタルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタルールの ID。
モニタルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタルールの ID。
モニタルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタルールの ID。
セキュリティインテリジェンス送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティインテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイルイベントカウント	uint16	同じ秒で発生するファイルイベントを区別するために使用される値。
侵入イベントカウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポндаの国	uint16	応答ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。



表 B-37 接続統計データブロック 5.4+のフィールド(続き)

フィールド	データタイプ	説明
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。
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、 <a href="http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml">www.iana.org/assignments/tls-parameters/tls-parameters.xhtml</a> を参照してください。

表 B-37 接続統計データブロック 5.4+ のフィールド (続き)

フィールド	データタイプ	説明
SSL 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	uint16	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"> <li>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。</li> <li>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。</li> <li>2(有効):サーバ証明書は有効です。</li> <li>4(自己署名済み):サーバ証明書は自己署名です。</li> <li>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。</li> <li>32(無効な署名):サーバ証明書に無効な署名があります。</li> <li>64(期限切れ):サーバ証明書は期限切れです。</li> <li>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。</li> <li>256(取り消し):サーバ証明書は取り消されました。</li> </ul>
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"> <li>0:「不明」</li> <li>1:「復号しない」</li> <li>2:「ブロックする」</li> <li>3:「リセットでブロック」</li> <li>4:「復号(既知のキー)」</li> <li>5:「復号(置換キー)」</li> <li>6:「復号(Resign)」</li> </ul>
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"> <li>0:「不明」</li> <li>1:「復号しない」</li> <li>2:「ブロックする」</li> <li>3:「リセットでブロック」</li> <li>4:「復号(既知のキー)」</li> <li>5:「復号(置換キー)」</li> <li>6:「復号(Resign)」</li> </ul>

表 B-37 接続統計データブロック 5.4+のフィールド(続き)

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

表 B-37 接続統計データブロック 5.4+ のフィールド (続き)

フィールド	データタイプ	説明
SSL フローメッセージ	uint32	<p>SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、<a href="http://tools.ietf.org/html/rfc5246">http://tools.ietf.org/html/rfc5246</a> を参照してください。</p> <ul style="list-style-type: none"> <li>0x00000001:NSE_MT__HELLO_REQUEST</li> <li>0x00000002:NSE_MT__CLIENT_ALERT</li> <li>0x00000004:NSE_MT__SERVER_ALERT</li> <li>0x00000008:NSE_MT__CLIENT_HELLO</li> <li>0x00000010:NSE_MT__SERVER_HELLO</li> <li>0x00000020:NSE_MT__SERVER_CERTIFICATE</li> <li>0x00000040:NSE_MT__SERVER_KEY_EXCHANGE</li> <li>0x00000080:NSE_MT__CERTIFICATE_REQUEST</li> <li>0x00000100:NSE_MT__SERVER_HELLO_DONE</li> <li>0x00000200:NSE_MT__CLIENT_CERTIFICATE</li> <li>0x00000400:NSE_MT__CLIENT_KEY_EXCHANGE</li> <li>0x00000800:NSE_MT__CERTIFICATE_VERIFY</li> <li>0x00001000:NSE_MT__CLIENT_CHANGE_CIPHER_SPEC</li> <li>0x00002000:NSE_MT__CLIENT_FINISHED</li> <li>0x00004000:NSE_MT__SERVER_CHANGE_CIPHER_SPEC</li> <li>0x00008000:NSE_MT__SERVER_FINISHED</li> <li>0x00010000:NSE_MT__NEW_SESSION_TICKET</li> <li>0x00020000:NSE_MT__HANDSHAKE_OTHER</li> <li>0x00040000:NSE_MT__APP_DATA_FROM_CLIENT</li> <li>0x00080000:NSE_MT__APP_DATA_FROM_SERVER</li> </ul>
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"> <li>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</li> <li>0x00000002 (NSE_FLOW__INITIALIZED):内部構造が処理可能です</li> <li>0x00000004 (NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました</li> </ul>
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)。
SSL サーバ名	string	SSL Client Hello でサーバ名に指定された名前。

表 B-37 接続統計データブロック 5.4+のフィールド(続き)

フィールド	データタイプ	説明
SSL URL カテゴリ	uint32	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできます。
SSL チケット ID	uint8[20]	クライアントとサーバがセッション チケットの使用に同意する場合に使用されるセッション チケットのハッシュ。
SSL チケット ID の長さ	uint8	SSL チケット ID の長さ。チケット ID は 20 バイトより長くすることはできませんが、20 バイト未満であってもかまいません。
ネットワーク分析ポリシー リビジョン	uint8[16]	接続イベントに関連付けられているネットワーク分析ポリシーのリビジョン。

## 接続統計データ ブロック 6.0.x

接続統計データブロックは、接続データメッセージで使用されます。接続統計データブロック 6.0 には、いくつかの新しいフィールドが追加されました。ISE 統合および複数ネットワークマップをサポートするために、フィールドが追加されました。バージョン 6.0.x の接続統計データブロックは、シリーズ 1 グループのブロックの、ブロックタイプ 160 です。これはブロックタイプ 157(接続統計データブロック 5.4.1 (B-191 ページ)) に取って代わります。DNS ルックアップとセキュリティ インテリジェンスをサポートするため新しいフィールドを追加しました。

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

次の図は、接続統計データブロック 6.0.x の形式を示しています。

7

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接続統計データ ブロック タイプ (160)																																
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)																																

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	レスポнда送信 バイト数(続き)								ユーザ ID (User ID)																							
	ユーザ ID(続き)								アプリケーションプロトコル ID																							
	アプリケーション プロトコル ID (続き)								URL カテゴリ																							
	URL カテゴリ (続き)								URL レピュテーション																							
	URL レピュテー ション(続き)								クライアントアプリケーション ID																							
	クライアントア プリケーション ID(続き)								Web アプリケーション ID																							
クライアント URL	Web アプリケー ション ID(続き)								Stringブロック タイプ(0)																							
	文字列ブロック タイプ(続き)								文字列ブロック長																							
	文字列ブロック 長(続き)								クライアントアプリケーション URL...																							
NetBIOS [名前(Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	NetBIOS 名...																															
クライアント アプリケーション バージョン	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	クライアントアプリケーションバージョン...																															
	モニタールール 1																															
	モニタールール 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
ビット																																
	モニタ ルール 3																															
	モニタ ルール 4																															
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/ 宛先								秒イニシエー タ層								ファイルイベント カウント															
	侵入イベント カウント																イニシエータの国															
	レスポндаの国																IOC 番号															
	送信元自律システム																															
	宛先自律システム																															
	SNMP 入力																SNMP 出力															
	送信元 TOS								宛先 TOS								送信元マスク								宛先マスク							
	セキュリティ コンテキスト																															
	セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト(続き)																															
参照ホスト	VLAN ID (Admin. VLAN ID)																文字列ブロック タイプ (0)															
	文字列ブロック タイプ (0) (続き)																文字列ブロック長															
	文字列ブロック長(続き)																参照ホスト...															
ユーザー エージェント	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	ユーザー エージェント...																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
HTTP リファラ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	HTTP リファラ...																															
SSL 証明書フィンガープリント SSL 証明書フィンガープリント (続き) SSL 証明書フィンガープリント (続き) SSL 証明書フィンガープリント (続き) SSL 証明書フィンガープリント (続き)																																
SSL ポリシー ID SSL ポリシー ID (続き) SSL ポリシー ID (続き) SSL ポリシー ID (続き)																																
SSL ルール ID																																
SSL 暗号スイート																SSL バージョン								SSL キー証明書統計								
SSL キー証明書統計 (続き)								実際の SSL アクション																予期された SSL アクション								
予期された SSL アクション (続き)								SSL フロー ステータス																SSL フロー エラー								
SSL フロー エラー (続き)																SSL フロー メッセージ																
SSL フロー メッセージ (続き)																SSL フロー フラグ																
SSL フロー フラグ (続き)																																

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	エンドポイントプロファイル ID (続き)																セキュリティグループ ID															
	セキュリティグループ ID (続き)																ロケーション IPv6															
	ロケーション IPv6 (続き)																ロケーション IPv6 (続き)															
	ロケーション IPv6 (続き)																ロケーション IPv6 (続き)															
	ロケーション IPv6 (続き)																HTTP レスポンス															
	HTTP レスポンス (続き)																文字列ブロック タイプ (0)															
	文字列ブロック タイプ (0) (続き)																文字列ブロック長															
	文字列ブロック長 (続き)																DNS クエリ...															
	DNS レコードタイプ (DNS Record Type)																DNS レスポンス タイプ															
	DNS TTL																															
	シンクホール UUID																															
	シンクホール UUID (続き)																															
	シンクホール UUID (続き)																															
	シンクホール UUID (続き)																															
	セキュリティインテリジェンス リスト 1																															
	セキュリティインテリジェンス リスト 2																															

次の表は、接続統計データブロック 6.0.x のフィールドについての説明です。

表 B-38 接続統計データブロック 6.0.x のフィールド

フィールド	データタイプ	説明
接続統計データブロックタイプ	uint32	接続統計データブロック 6.0+ を開始します。値は常に 160 です。
接続統計データブロック長	uint32	接続統計データブロックのバイト数(接続統計ブロックタイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。

表 B-38 接続統計データブロック 6.0.x のフィールド(続き)

フィールド	データタイプ	説明
デバイス ID (Device ID)	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティゾーン。
入力インターフェイス	uint8[16]	着信トラフィックのインターフェイス。
出力インターフェイス	uint8[16]	発信トラフィックのインターフェイス。
イニシエータ IP アドレス	uint8[16]	IP アドレス オクテットの、接続イベントを記述するセッションを開始したホストの IP アドレス。
レスポнда IP アドレス	uint8[16]	IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。
ポリシー リビジョン	uint8[16]	トリガーされた関連イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
ルールアクション	uint16	そのルールに対してユーザインターフェイスで選択されたアクション(allow、block など)。
ルールの理由	uint32	イベントをトリガーしたルールの理由。
イニシエータポート	uint16	開始ホストにより使用されるポート。
レスポндаポート	uint16	応答ホストにより使用されるポート。
TCP フラグ	uint16	接続イベントのすべての TCP フラグを示します。
プロトコル	uint8	IANA 指定のプロトコル番号。
NetFlow ソース	uint8[16]	接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。
インスタンス ID (Instance ID)	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケットタイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケットタイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポнда送信パケット数	uint64	応答ホストが送信したパケット数。

表 B-38 接続統計データブロック 6.0.x のフィールド(続き)

フィールド	データタイプ	説明
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポнда送信バイト数	uint64	応答ホストから送信バイト数。
ユーザ ID (User ID)	uint32	トラフィックを生成したホストの最終ログイン ユーザの内部 ID 番号。
アプリケーションプロトコル ID	uint32	アプリケーション プロトコルのアプリケーション ID。
URL カテゴリ	uint32	URL カテゴリの内部 ID 番号。
URLレピュテーション	uint32	URL レピュテーションの内部 ID 番号。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
文字列ブロックタイプ	uint32	クライアントアプリケーション URL の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーション URL の文字列データブロックのバイト数(文字列ブロックタイプと長さのフィールド用の 8 バイト、およびクライアントアプリケーション URL 文字列のバイト数を含む)。
クライアントアプリケーション URL	string	クライアントアプリケーションがアクセスする URL (該当する場合) (/files/index.html など)。
文字列ブロックタイプ	uint32	ホスト 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)。
クライアントアプリケーションバージョン	string	クライアントアプリケーションバージョン。
モニタ ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタ ルールの ID。

表 B-38 接続統計データ ブロック 6.0.x のフィールド(続き)

フィールド	データタイプ	説明
モニタ ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタ ルールの ID。
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス 送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス層	uint8	IP ブラックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入イベント カウント	uint16	同じ秒で発生する侵入イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポндаの国	uint 16	応答ホストの国のコード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
SNMP 入力	uint16	入力インターフェイスの SNMP インデックス。
SNMP 出力	uint16	出力インターフェイスの SNMP インデックス
送信元 TOS	uint8	着信インターフェイス用のタイプ オブ サービス バイト設定。
宛先 TOS	uint8	発信インターフェイス用のタイプ オブ サービス バイト設定。
送信元マスク	uint8	送信元アドレス プレフィックス マスク。
宛先マスク	uint8	宛先アドレス プレフィックス マスク。

表 B-38 接続統計データブロック 6.0.x のフィールド(続き)

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



表 B-38 接続統計データブロック 6.0.x のフィールド(続き)

フィールド	データタイプ	説明
SSL サーバ証明書ステータス	uint16	<p>SSL 証明書のステータス。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>2(有効):サーバ証明書は有効です。</li> <li>4(自己署名済み):サーバ証明書は自己署名です。</li> <li>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。</li> <li>32(無効な署名):サーバ証明書に無効な署名があります。</li> <li>64(期限切れ):サーバ証明書は期限切れです。</li> <li>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。</li> <li>256(取り消し):サーバ証明書は取り消されました。</li> </ul>
実際の SSL アクション	uint16	<p>SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>0:「不明」</li> <li>1:「復号しない」</li> <li>2:「ブロックする」</li> <li>3:「リセットでブロック」</li> <li>4:「復号(既知のキー)」</li> <li>5:「復号(置換キー)」</li> <li>6:「復号(Resign)」</li> </ul>
予期された SSL アクション	uint16	<p>SSL ルールに基づいて接続に対して実行する必要があるアクション。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>0:「不明」</li> <li>1:「復号しない」</li> <li>2:「ブロックする」</li> <li>3:「リセットでブロック」</li> <li>4:「復号(既知のキー)」</li> <li>5:「復号(置換キー)」</li> <li>6:「復号(Resign)」</li> </ul>

表 B-38 接続統計データブロック 6.0.x のフィールド(続き)

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

表 B-38 接続統計データブロック 6.0.x のフィールド(続き)

フィールド	データタイプ	説明
SSL フローメッセージ	uint32	<p>SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、<a href="http://tools.ietf.org/html/rfc5246">http://tools.ietf.org/html/rfc5246</a> を参照してください。</p> <ul style="list-style-type: none"> <li>0x00000001:NSE_MT__HELLO_REQUEST</li> <li>0x00000002:NSE_MT__CLIENT_ALERT</li> <li>0x00000004:NSE_MT__SERVER_ALERT</li> <li>0x00000008:NSE_MT__CLIENT_HELLO</li> <li>0x00000010:NSE_MT__SERVER_HELLO</li> <li>0x00000020:NSE_MT__SERVER_CERTIFICATE</li> <li>0x00000040:NSE_MT__SERVER_KEY_EXCHANGE</li> <li>0x00000080:NSE_MT__CERTIFICATE_REQUEST</li> <li>0x00000100:NSE_MT__SERVER_HELLO_DONE</li> <li>0x00000200:NSE_MT__CLIENT_CERTIFICATE</li> <li>0x00000400:NSE_MT__CLIENT_KEY_EXCHANGE</li> <li>0x00000800:NSE_MT__CERTIFICATE_VERIFY</li> <li>0x00001000:NSE_MT__CLIENT_CHANGE_CIPHER_SPEC</li> <li>0x00002000:NSE_MT__CLIENT_FINISHED</li> <li>0x00004000:NSE_MT__SERVER_CHANGE_CIPHER_SPEC</li> <li>0x00008000:NSE_MT__SERVER_FINISHED</li> <li>0x00010000:NSE_MT__NEW_SESSION_TICKET</li> <li>0x00020000:NSE_MT__HANDSHAKE_OTHER</li> <li>0x00040000:NSE_MT__APP_DATA_FROM_CLIENT</li> <li>0x00080000:NSE_MT__APP_DATA_FROM_SERVER</li> </ul>
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"> <li>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</li> <li>0x00000002 (NSE_FLOW__INITIALIZED):内部構造が処理可能です</li> <li>0x00000004 (NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました</li> </ul>
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)。
SSL サーバ名	string	SSL Client Hello でサーバ名に指定された名前。

表 B-38 接続統計データブロック 6.0.x のフィールド(続き)

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

表 B-38 接続統計データ ブロック 6.0.x のフィールド(続き)

フィールド	データタイプ	説明
DNS レスポンス タイプ	uint16	<p>0 (NoError): エラーなし</p> <p>1 (FormErr): フォーマット エラー</p> <p>2 (ServFail): サーバ障害</p> <p>3 (NXDomain): 存在していないドメイン</p> <p>4 (NotImp): 未実装</p> <p>5 (Refused): クエリ拒否</p> <p>6 (YXDomain): 名前が存在してはならない状況で存在している</p> <p>7 (YXRRSet): RR セットが存在してはならない状況で存在している</p> <p>8 (NXRRSet): 存在しているべき RR セットが存在していない</p> <p>9 (NotAuth): 未承認</p> <p>10 (NotZone): 名前がゾーンに含まれていない</p> <p>16 (BADSIG): TSIG 署名失敗</p> <p>17 (BADKEY): キーが認識されない</p> <p>18 (BADTIME): 時間範囲外の署名</p> <p>19 (BADMODE): 不適切な TKEY モード</p> <p>20 (BADNAME): 重複するキー名</p> <p>21 (BADALG): サポートされていないアルゴリズム</p> <p>22 (BADTRUNC): 不適切な切り捨て</p> <p>3841 (NXDOMAIN): ファイアウォールからの NXDOMAIN 応答</p> <p>3842 (SINKHOLE): ファイアウォールからのシンクホール応答</p>
DNS TTL	uint32	DNS レスポンスの存続期間(秒単位)。
シンクホール UUID	uin8[16]	このシンクホール オブジェクトに関連付けられているリビジョン UUID。
セキュリティ インテリジェンス リスト 1	uint32	イベントに関連付けられているセキュリティ インテリジェンス リスト。これは、関連メタデータのセキュリティ インテリジェンス リストにマップされます。接続には、2つのセキュリティ インテリジェンス リストが関連付けられている場合があります。
セキュリティ インテリジェンス リスト 2	uint32	イベントに関連付けられているセキュリティ インテリジェンス リスト。これは、関連メタデータのセキュリティ インテリジェンス リストにマップされます。接続には、2つのセキュリティ インテリジェンス リストが関連付けられている場合があります。

## 接続統計データ ブロック 6.1.x

接続統計データ ブロックは、接続データ メッセージで使用されます。6.1.x の接続統計情報データ ブロックに複数の新しいフィールドが追加されました。ISE 統合および複数ネットワーク マップをサポートするために、フィールドが追加されました。バージョン 6.1+ の接続統計データ ブロックのブロック タイプは、シリーズ 1 ブロック グループのブロック タイプ 163 です。これはブロック タイプ160 [接続統計データ ブロック 6.0.x \(B-205 ページ\)](#) に置き換わります。DNS ルックアップとセキュリティ インテリジェンスをサポートするため新しいフィールドを追加しました。ブロック タイプ 168 に代わりました ([接続統計データ ブロック 6.2+\(4-123 ページ\)](#))。

接続イベント レコードは、要求メッセージにイベント バージョン 13 とイベント コード 71 とともに拡張イベント フラグを設定して要求します。[要求フラグ \(2-12 ページ\)](#) 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 \(4-54 ページ\)](#) を参照してください。

次の図は、6.1+ の接続統計データ ブロックの形式です。

バイト	0								1								2								3										
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
接続統計データ ブロック タイプ (163)																																			
接続統計データ ブロック 長																																			
デバイス ID (Device ID)																																			
入力ゾーン																																			
入力ゾーン (続き)																																			
入力ゾーン (続き)																																			
入力ゾーン (続き)																																			
出力ゾーン																																			
出力ゾーン (続き)																																			
出力ゾーン (続き)																																			
出力ゾーン (続き)																																			
入力インターフェイス																																			
入力インターフェイス (続き)																																			
入力インターフェイス (続き)																																			
入力インターフェイス (続き)																																			
出力インターフェイス																																			

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	イニシエータ IP アドレス																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	レスポнда IP アドレス																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	レスポнда IP アドレス(続き)																															
	オリジナルクライアント IP アドレス																															
	オリジナルクライアント IP アドレス(続き)																															
	オリジナルクライアント IP アドレス(続き)																															
	オリジナルクライアント IP アドレス(続き)																															
	ポリシー リビジョン																															
	ポリシー リビジョン(続き)																															
	ポリシー リビジョン(続き)																															
	ポリシー リビジョン(続き)																															
	ルール ID																															
	トンネルルール ID																															
	ルールアクション																ルールの理由															
	ルールの理由(続き)																イニシエータ ポート															
	レスポнда ポート																TCP フラグ															
	プロトコル								NetFlow ソース																							

バイト	0							1							2							3										
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	NetFlow ソース(続き)																															
	NetFlow ソース(続き)																															
	NetFlow ソース(続き)																															
NetFlow ソース(続き)	インスタンス ID (Instance ID)														接続数カウンタ																	
接続数カウンタ(続き)	最初の packets タイムスタンプ																															
最初の packets タイムスタンプ(続き)	最終 packets タイムスタンプ																															
最終 packets タイムスタンプ(続き)	イニシエータ送信 packets 数																															
	イニシエータ送信 packets 数(続き)																															
イニシエータ送信 packets 数(続き)	レスポнда送信 packets 数																															
	レスポнда送信 packets 数(続き)																															
レスポнда送信 packets 数(続き)	イニシエータ送信 bytes 数																															
	イニシエータ送信 bytes 数(続き)																															
イニシエータ送信 bytes 数(続き)	レスポнда送信 packets 数																															
	レスポнда送信 bytes 数(続き)																															
レスポнда送信 bytes 数(続き)	イニシエータ packets ドロップ																															
	イニシエータ packets ドロップ(続き)																															
イニシエータ packets ドロップ(続き)	レスポнда packets ドロップ																															
	レスポнда packets ドロップ(続き)																															



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

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

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

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

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

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

次の表では、6.1+ の接続統計データ ブロックのフィールドについて説明します。

表 B-39 接続統計データ ブロック 6.1+ のフィールド

フィールド	データ タイプ	説明
接続統計データ ブロック タイプ	uint32	接続統計データ ブロック 6.1.x を開始します。値は常に 163 です。
接続統計データ ブロック長	uint32	接続統計データ ブロックのバイト数(接続統計ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続データのバイト数を含む)。
デバイス ID (Device ID)	uint32	接続イベントを検出したデバイス。
入力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの入力セキュリティゾーン。
出力ゾーン	uint8[16]	ポリシー違反をトリガーしたイベントの出力セキュリティゾーン。
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。

表 B-39 接続統計データブロック 6.1+ のフィールド(続き)

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

表 B-39 接続統計データブロック 6.1+ のフィールド(続き)

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



表 B-39 接続統計データ ブロック 6.1+ のフィールド(続き)

フィールド	データタイプ	説明
文字列ブロック長	uint32	クライアント アプリケーション バージョンの文字列データブロックのバイト数(文字列ブロックタイプと長さフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
クライアント アプリケーション バージョン	string	クライアント アプリケーション バージョン。
モニタ ルール 1	uint32	接続イベントに関連付けられている 1 番目のモニタ ルールの ID。
モニタ ルール 2	uint32	接続イベントに関連付けられている 2 番目のモニタ ルールの ID。
モニタ ルール 3	uint32	接続イベントに関連付けられている 3 番目のモニタ ルールの ID。
モニタ ルール 4	uint32	接続イベントに関連付けられている 4 番目のモニタ ルールの ID。
モニタ ルール 5	uint32	接続イベントに関連付けられている 5 番目のモニタ ルールの ID。
モニタ ルール 6	uint32	接続イベントに関連付けられている 6 番目のモニタ ルールの ID。
モニタ ルール 7	uint32	接続イベントに関連付けられている 7 番目のモニタ ルールの ID。
モニタ ルール 8	uint32	接続イベントに関連付けられている 8 番目のモニタ ルールの ID。
セキュリティ インテリジェンス 送信元/宛先	uint8	送信元または宛先の IP アドレスを IP ブラックリストに突き合わせるかどうか。
セキュリティ インテリジェンス 層	uint8	IP ブラックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入 イベント カウント	uint16	同じ秒で発生する侵入 イベントを区別するために使用される値。
イニシエータ の国	uint16	開始ホストの国のコード。
レスポンドの国	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。

表 B-39 接続統計データブロック 6.1+ のフィールド(続き)

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

表 B-39 接続統計データブロック 6.1+ のフィールド(続き)

フィールド	データタイプ	説明
SSL 暗号スイート	uint16	SSL 接続で使用される暗号スイート。値は 10 進形式で保存されます。値により指定されている暗号スイートの詳細については、 <a href="http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml">www.iana.org/assignments/tls-parameters/tls-parameters.xhtml</a> 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"> <li>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。</li> <li>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。</li> <li>2(有効):サーバ証明書は有効です。</li> <li>4(自己署名済み):サーバ証明書は自己署名です。</li> <li>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。</li> <li>32(無効な署名):サーバ証明書に無効な署名があります。</li> <li>64(期限切れ):サーバ証明書は期限切れです。</li> <li>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。</li> <li>256(取り消し):サーバ証明書は取り消されました。</li> </ul>
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"> <li>0:「不明」</li> <li>1:「復号しない」</li> <li>2:「ブロックする」</li> <li>3:「リセットでブロック」</li> <li>4:「復号(既知のキー)」</li> <li>5:「復号(置換キー)」</li> <li>6:「復号(Resign)」</li> </ul>

表 B-39 接続統計データブロック 6.1+ のフィールド(続き)

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

表 B-39 接続統計データブロック 6.1+ のフィールド(続き)

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

表 B-39 接続統計データブロック 6.1+ のフィールド(続き)

フィールド	データタイプ	説明
SSL フローメッセージ	uint32	<p>SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、<a href="http://tools.ietf.org/html/rfc5246">http://tools.ietf.org/html/rfc5246</a> を参照してください。</p> <ul style="list-style-type: none"> <li>0x00000001:NSE_MT__HELLO_REQUEST</li> <li>0x00000002:NSE_MT__CLIENT_ALERT</li> <li>0x00000004:NSE_MT__SERVER_ALERT</li> <li>0x00000008:NSE_MT__CLIENT_HELLO</li> <li>0x00000010:NSE_MT__SERVER_HELLO</li> <li>0x00000020:NSE_MT__SERVER_CERTIFICATE</li> <li>0x00000040:NSE_MT__SERVER_KEY_EXCHANGE</li> <li>0x00000080:NSE_MT__CERTIFICATE_REQUEST</li> <li>0x00000100:NSE_MT__SERVER_HELLO_DONE</li> <li>0x00000200:NSE_MT__CLIENT_CERTIFICATE</li> <li>0x00000400:NSE_MT__CLIENT_KEY_EXCHANGE</li> <li>0x00000800:NSE_MT__CERTIFICATE_VERIFY</li> <li>0x00001000:NSE_MT__CLIENT_CHANGE_CIPHER_SPEC</li> <li>0x00002000:NSE_MT__CLIENT_FINISHED</li> <li>0x00004000:NSE_MT__SERVER_CHANGE_CIPHER_SPEC</li> <li>0x00008000:NSE_MT__SERVER_FINISHED</li> <li>0x00010000:NSE_MT__NEW_SESSION_TICKET</li> <li>0x00020000:NSE_MT__HANDSHAKE_OTHER</li> <li>0x00040000:NSE_MT__APP_DATA_FROM_CLIENT</li> <li>0x00080000:NSE_MT__APP_DATA_FROM_SERVER</li> </ul>
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"> <li>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</li> <li>0x00000002 (NSE_FLOW__INITIALIZED):内部構造が処理可能です</li> <li>0x00000004 (NSE_FLOW__INTERCEPT):SSL セッションが代行受信されました</li> </ul>
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)。
SSL サーバ名	string	SSL Client Hello でサーバ名に指定された名前。

表 B-39 接続統計データブロック 6.1+ のフィールド(続き)

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

表 B-39 接続統計データブロック 6.1+ のフィールド(続き)

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

## レガシー ファイル イベントのデータ構造

続くいくつかのトピックでは、他のレガシー ファイル イベント データの構造について説明します。

- [ファイル イベント 5.1.1.x \(B-240 ページ\)](#)
- [ファイル イベント 5.2.x \(B-244 ページ\)](#)
- [ファイル イベント 5.3 \(B-249 ページ\)](#)
- [ファイル イベント 5.3.1 \(B-256 ページ\)](#)
- [ファイル イベント 5.4.x \(B-262 ページ\)](#)
- [ファイル イベント SHA ハッシュ 5.1.1 ~ 5.2.x \(B-273 ページ\)](#)

### ファイル イベント 5.1.1.x

ファイル イベントには、ネットワークを介して送信されるファイルに関する情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントのブロック タイプは、シリーズ 2 グループのブロックの、ブロック タイプ 23 です。

次の図は、ファイル イベント データ ブロックの構造を示しています。





バイト	0								1								2								3													
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
接続タイムスタンプ																																						
ファイル イベント タイムスタンプ (File Event Timestamp)																																						
送信元 IP アドレス																																						
送信元 IP アドレス (続き)																																						
送信元 IP アドレス (続き)																																						
送信元 IP アドレス (続き)																																						
宛先 IP アドレス																																						
宛先 IP アドレス (続き)																																						
宛先 IP アドレス (続き)																																						
宛先 IP アドレス (続き)																																						
傾向								操作								SHA ハッシュ																						
SHA ハッシュ (続き)																																						
SHA ハッシュ (続き)																																						
SHA ハッシュ (続き)																																						
SHA ハッシュ (続き)																																						
SHA ハッシュ (続き)																																						
SHA ハッシュ (続き)																																						
SHA ハッシュ (続き)																																						
SHA ハッシュ (続き)																ファイル タイプ ID																						
ファイル名								ファイル タイプ ID (続き)								文字列ブロック タイプ (0)																						
																文字列ブロック タイプ (0) (続き)								文字列ブロック長														
																文字列ブロック長 (続き)								ファイル名...														
ファイル サイズ (File size)																																						
ファイル サイズ (続き)																																						
方向 (Direction)								アプリケーション ID (Application ID)																														

## レガシー ファイル イベントのデータ構造

バイト	0								1								2								3													
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
	アプリケーション ID (続き)								ユーザ ID (User ID)																													
URI	ユーザ ID (続き)								文字列ブロック タイプ (0)																													
	文字列ブロック タイプ (0) (続き)								文字列ブロック 長																													
	文字列ブロック 長 (続き)								URI...																													
シグネチャ	文字列ブロック タイプ (0)																																					
	文字列ブロック 長																																					
	署名...																																					
	送信元ポート (Source Port)														接続先ポート																							
	プロトコル								アクセス コントロール ポリシー UUID																													
	アクセス コントロール ポリシー UUID (続き)																																					
	アクセス コントロール ポリシー UUID (続き)																																					
アクセス コントロール ポリシー UUID (続き)																																						
アクセス コントロール ポリシー UUID (続き)																																						

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

表 B-40 ファイル イベント データ ブロックのフィールド

フィールド	データ タイプ	説明
ファイル イベント ブロック タイプ	uint32	ファイル イベント データ ブロックを開始します。この値は常に 23 です。
ファイル イベント ブロック 長	uint32	ファイル イベント ブロックのバイトの合計数(ファイル イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または侵入イベントとイベントをリンクするために使用されます。

表 B-40 ファイル イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続タイムスタンプ	uint32	関連する接続イベントの UNIX タイムスタンプ(1970年1月1日からの秒数)。
ファイル イベント タイムスタンプ (File Event Timestamp)	uint32	ファイル タイプが識別されてファイル イベントが生成されたときの UNIX タイムスタンプ(1970年1月1日からの秒数)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
傾向	uint8	<p>ファイルのマルウェア ステータス。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>1(CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。</li> <li>2(UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。</li> <li>3(MALWARE): ファイルにはマルウェアが含まれています。</li> <li>4(CACHE_MISS): ソフトウェアはシスコクラウドに特性を確認する要求を送信できませんでした。</li> <li>5(NO_CLOUD_RESP): シスコクラウド サービスが要求に応答しませんでした。</li> </ul>
操作	uint8	<p>ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。</p> <ul style="list-style-type: none"> <li>1: 検出</li> <li>2: ブロック</li> <li>3: マルウェア クラウド ルックアップ</li> <li>4: マルウェア ブロック</li> <li>5: マルウェア ホワイトリスト</li> </ul>
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
ファイル タイプ ID	uint32	ファイル タイプにマップされている ID 番号。
ファイル名	string	ファイルの名前。
ファイル サイズ (File size)	uint64	ファイルのサイズ(バイト単位)。

表 B-40 ファイル イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
方向 (Direction)	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示す値。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>1: ダウンロード</li> <li>2: アップロード</li> </ul> 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID (User ID)	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
URI	string	接続の Uniform Resource Identifier (URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> <li>1: ICMP</li> <li>4: IP</li> <li>6: TCP</li> <li>17: UDP</li> </ul> これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。

## ファイル イベント 5.2.x

ファイル イベントには、ネットワークを介して送信されるファイルに関する情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントのブロック タイプは、シリーズ 2 グループのブロックの、ブロック タイプ 32 です。これはブロック タイプ 23 に取って代わります。送信元と宛先の国、およびクライアントと Web アプリケーション インスタンスを追跡するために、新しいフィールドが追加されました。

次の図は、ファイル イベント データ ブロックの構造を示しています。

バイト	0								1								2								3													
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
	ファイルイベントブロックタイプ(32)																																					
	ファイルイベントブロック長																																					
	デバイス ID																																					
	接続インスタンス																接続数カウンタ																					
	接続タイムスタンプ																																					
	ファイルイベント タイムスタンプ (File Event Timestamp)																																					
	送信元 IP アドレス																																					
	送信元 IP アドレス(続き)																																					
	送信元 IP アドレス(続き)																																					
	送信元 IP アドレス(続き)																																					
	宛先 IP アドレス																																					
	宛先 IP アドレス(続き)																																					
	宛先 IP アドレス(続き)																																					
	宛先 IP アドレス(続き)																																					
	傾向	操作																SHA ハッシュ																				
		SHA ハッシュ(続き)																																				
		SHA ハッシュ(続き)																																				
		SHA ハッシュ(続き)																																				
		SHA ハッシュ(続き)																																				
		SHA ハッシュ(続き)																																				
		SHA ハッシュ(続き)																																				
		SHA ハッシュ(続き)																																				
	SHA ハッシュ(続き)																ファイルタイプ ID																					

レガシー ファイル イベントのデータ構造

バイト	0								1								2								3													
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
ファイル名	ファイル タイプ ID (続き)																文字列ブロック タイプ (0)																					
	文字列ブロック タイプ (0) (続き)																文字列ブロック長																					
	文字列ブロック長 (続き)																ファイル名...																					
ファイル サイズ (File size)																																						
ファイル サイズ (続き)																																						
方向 (Direction)								アプリケーション ID (Application ID)																														
アプリケーション ID (続き)								ユーザ ID (User ID)																														
URI	ユーザ ID (続き)								文字列ブロック タイプ (0)																													
	文字列ブロック タイプ (0) (続き)								文字列ブロック長																													
	文字列ブロック長 (続き)								URI...																													
シグネチャ	文字列ブロック タイプ (0)																																					
	文字列ブロック長																																					
	署名...																																					
送信元ポート (Source Port)																接続先ポート																						
プロトコル								アクセス コントロール ポリシー UUID																														
アクセス コントロール ポリシー UUID (続き)																																						
アクセス コントロール ポリシー UUID (続き)																																						
アクセス コントロール ポリシー UUID (続き)																																						
アクセス コントロール ポリシー UUID (続き)								送信元の国																宛先の国 (Country)														
宛先の国 (続き)								Web アプリケーション ID																														

バイト	0								1								2								3													
ビット	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
	Web アプリケーション ID(続き)								クライアント アプリケーション ID																													
	クライアント アプリケーション ID(続き)																																					

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

表 B-41 ファイルイベント データ ブロックのフィールド

フィールド	データ タイプ	説明
ファイル イベント ブロック タイプ	uint32	ファイル イベント データ ブロックを開始します。この値は常に 23 です。
ファイル イベント ブロック 長	uint32	ファイル イベント ブロックのバイトの合計数(ファイル イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または侵入イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続タイムスタンプ	uint32	関連する接続イベントの UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
ファイル イベント タイムスタンプ (File Event Timestamp)	uint32	ファイル タイプが識別されてファイル イベントが生成されたときの UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。

表 B-41 ファイルイベントデータブロックのフィールド(続き)

フィールド	データ タイプ	説明
傾向	uint8	ファイルのマルウェア ステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。</li> <li>2(NEUTRAL):ファイルにマルウェアが含まれているかどうかは不明です。</li> <li>3(MALWARE):ファイルにはマルウェアが含まれています。</li> <li>4(CACHE_MISS):ソフトウェアから シスコ クラウドに対して、特性を確認する要求を送信できなかったか、または シスコ クラウド サービスが要求に応答しませんでした。</li> </ul>
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>1:検出</li> <li>2:ブロック</li> <li>3:マルウェア クラウド ルックアップ</li> <li>4:マルウェア ブロック</li> <li>5:マルウェア ホワイトリスト</li> </ul>
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
ファイル タイプ ID	uint32	ファイル タイプにマップされている ID 番号。
ファイル名	string	ファイルの名前。
ファイル サイズ (File size)	uint64	ファイルのサイズ(バイト単位)。
方向 (Direction)	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示す値。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>1:ダウンロード</li> <li>2:アップロード</li> </ul> <p>現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。</p>
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID (User ID)	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
URI	string	接続の Uniform Resource Identifier (URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。



表 B-41 ファイル イベント データ ブロックのフィールド(続き)

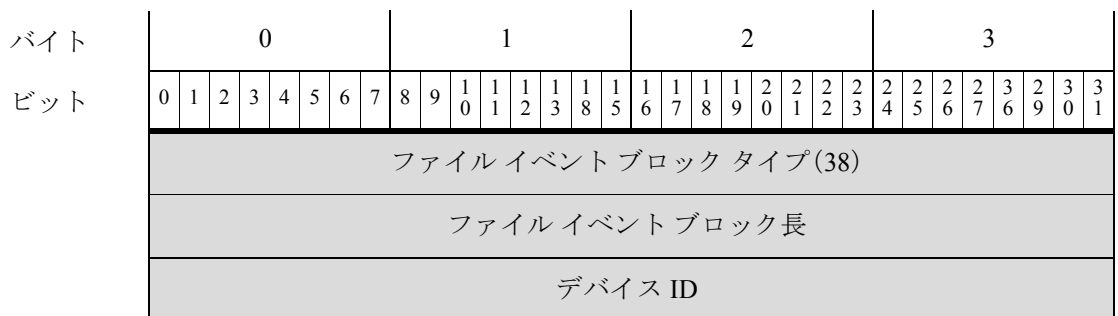
フィールド	データ タイプ	説明
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> <li>• 1:ICMP</li> <li>• 4:IP</li> <li>• 6:TCP</li> <li>• 17:UDP</li> </ul> これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。

### ファイル イベント 5.3

ファイル イベントには、ネットワークを介して送信されるファイルに関する情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントのブロック タイプは、シリーズ 2 グループのブロックの、ブロック タイプ 38 です。これはブロック タイプ 32 に取って代わります。新しいフィールドは、ダイナミック ファイル分析とファイル ストレージを追跡するために追加されました。

ファイル イベント レコードを要求するには、イベント バージョン 3 およびイベント コード 111 の要求メッセージ内に、ファイル イベント フラグ(要求フラグ フィールドのビット 30)を設定します。[要求フラグ\(2-12 ページ\)](#)を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

次の図は、ファイル イベント データ ブロックの構造を示しています。



レガシー ファイル イベントのデータ構造

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	接続インスタンス																接続数カウンタ															
	接続タイムスタンプ																															
	ファイル イベント タイムスタンプ (File Event Timestamp)																															
	送信元 IP アドレス 送信元 IP アドレス(続き) 送信元 IP アドレス(続き) 送信元 IP アドレス(続き)																															
	宛先 IP アドレス 宛先 IP アドレス(続き) 宛先 IP アドレス(続き) 宛先 IP アドレス(続き)																															
	傾向								SPERO 解析結果								ファイル スト レージ ステ ータス								ファイル分析ス テータス							
	アーカイブ ファ イル ステータス								脅威スコア								操作								SHA ハッシュ							
	SHA ハッシュ(続き) SHA ハッシュ(続き) SHA ハッシュ(続き) SHA ハッシュ(続き) SHA ハッシュ(続き) SHA ハッシュ(続き) SHA ハッシュ(続き) SHA ハッシュ(続き)																															
	SHA ハッシュ(続き)																								ファイル タイ プ 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
ファイル名	ファイルタイプ ID(続き)																								文字列ブロック タイプ(0)							
	文字列ブロック タイプ(0)(続き)																								文字列ブロッ ク長							
	文字列ブロック長(続き)																								ファイル名...							
	ファイル サイズ (File size)																															
	ファイル サイズ(続き)																															
	方向(Direction)																アプリケーション ID(Application ID)															
	アプリケーション ID(続き)																ユーザ ID(User ID)															
	ユーザ ID(続き)																文字列ブロック タイプ(0)															
	文字列ブロック タイプ(0)(続き)																文字列ブロック長															
URI	文字列ブロック 長(続き)																URI...															
	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
シグネチャ	署名...																															
	送信元ポート (Source Port)																接続先ポート															
	プロトコル																アクセス コントロール ポリシー UUID															
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コント ロール ポリシー UUID(続き)																送信元の国								宛先の国 (Country)							
宛先の国(続き)																Web アプリケーション ID																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Web アプリケーション ID (続き)								クライアント アプリケーション ID																							
	クライアント アプリケーション ID (続き)																															

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

表 B-42 ファイル イベント データ ブロックのフィールド

フィールド	データ タイプ	説明
ファイル イベント ブロック タイプ	uint32	ファイル イベント データ ブロックを開始します。この値は常に 23 です。
ファイル イベント ブロック 長	uint32	ファイル イベント ブロックのバイトの合計数(ファイル イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または侵入イベントとイベントをリンクするために使用されます。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続タイムスタンプ	uint32	関連する接続イベントの UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
ファイル イベント タイムスタンプ (File Event Timestamp)	uint32	ファイル タイプが識別されてファイル イベントが生成されたときの UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。

表 B-42 ファイルイベント データブロックのフィールド(続き)

フィールド	データ タイプ	説明
傾向	uint8	<p>ファイルのマルウェア ステータス。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>1 (CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。</li> <li>2 (UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。</li> <li>3 (MALWARE): ファイルにはマルウェアが含まれています。</li> <li>4 (UNAVAILABLE): ソフトウェアから シスコ クラウドに対して、特性を確認する要求を送信できなかったか、または シスコ クラウド サービスが要求に応答しませんでした。</li> <li>5 (CUSTOM SIGNATURE): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。</li> </ul>
SPERO 解析結果	uint8	<p>SPERO 署名がファイル分析で使用されたかどうかを示します。値が 1、2、または 3 であれば、SPERO 分析は使用されました。それ以外の値であれば、SPERO 分析は使用されませんでした。</p>
ファイル ストレージ ステータス	uint8	<p>ファイルの保存ステータス。値は以下のとおりです。</p> <ul style="list-style-type: none"> <li>1: ファイルが保存されました</li> <li>2: ファイルが保存されました</li> <li>3: ファイルを保存できません</li> <li>4: ファイルを保存できません</li> <li>5: ファイルを保存できません</li> <li>6: ファイルを保存できません</li> <li>7: ファイルを保存できません</li> <li>8: ファイル サイズが大きすぎます</li> <li>9: ファイル サイズが小さすぎます</li> <li>10: ファイルを保存できません</li> <li>11: ファイルは保存されておらず、解析結果を入力できません</li> </ul>

表 B-42 ファイルイベントデータブロックのフィールド(続き)

フィールド	データタイプ	説明
ファイル分析ステータス	uint8	<p>ファイルが動的分析のために送信されているかどうかを示します。値は以下のとおりです。</p> <ul style="list-style-type: none"> <li>• 0: ファイルが分析のために送信されていません</li> <li>• 1: 分析のために送信されました</li> <li>• 2: 分析のために送信されました</li> <li>• 4: 分析のために送信されました</li> <li>• 5: 送信に失敗しました</li> <li>• 6: 送信に失敗しました</li> <li>• 7: 送信に失敗しました</li> <li>• 8: 送信に失敗しました</li> <li>• 9: ファイルサイズが小さすぎます</li> <li>• 10: ファイルサイズが大きすぎます</li> <li>• 11: 分析のために送信されました</li> <li>• 12: 分析が完了しました</li> <li>• 13: 失敗(ネットワークの問題)</li> <li>• 14: 失敗(レート制限)</li> <li>• 15: 失敗(ファイルが大きすぎます)</li> <li>• 16: 失敗(ファイルの読み取りエラー)</li> <li>• 17: 失敗(内部ライブラリ エラー)</li> <li>• 19: ファイルは送信されておらず、解析結果を入力できません</li> <li>• 20: 失敗(ファイルを実行できません)</li> <li>• 21: 失敗(分析タイムアウト)</li> <li>• 22: 分析のために送信されました</li> <li>• 23: サポートされていないファイル</li> </ul>
アーカイブ ファイルステータス	uint8	この値は常に 0 です。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ~ 100)。
操作	uint8	<p>ファイルタイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。</p> <ul style="list-style-type: none"> <li>• 1: 検出</li> <li>• 2: ブロック</li> <li>• 3: マルウェア クラウドルックアップ</li> <li>• 4: マルウェア ブロック</li> <li>• 5: マルウェア ホワイトリスト</li> </ul>
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。

表 B-42 ファイルイベント データブロックのフィールド(続き)

フィールド	データ タイプ	説明
ファイル タイプ ID	uint32	ファイル タイプにマップされている ID 番号。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、 <a href="#">エンドポイント向け AMP ファイル タイプのメタデータ (3-43 ページ)</a> を参照してください。
ファイル名	string	ファイルの名前。
ファイル サイズ (File size)	uint64	ファイルのサイズ(バイト単位)。
方向 (Direction)	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示す値。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>1: ダウンロード</li> <li>2: アップロード</li> </ul> 現時点では、この値はプロトコルに依存しています (たとえば接続が HTTP の場合はダウンロード)。
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID (User ID)	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
URI	string	接続の Uniform Resource Identifier (URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> <li>1: ICMP</li> <li>4: IP</li> <li>6: TCP</li> <li>17: UDP</li> </ul> これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。

## ファイルイベント 5.3.1

ファイルイベントには、ネットワークを介して送信されるファイルに関する情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントのブロック タイプは、シリーズ 2 グループのブロックの、ブロック タイプ 43 です。これはブロック タイプ 38 に取って代わります。セキュリティ コンテキスト フィールドが追加されました。

ファイル イベント レコードを要求するには、イベント バージョン 4 および イベント コード 111 の要求メッセージ内に、ファイル イベント フラグ (要求フラグ フィールドのビット 30) を設定します。[要求フラグ \(2-12 ページ\)](#) を参照してください。ビット 23 を有効にすると、拡張イベント ヘッダーがレコードに含まれます。

次の図は、ファイル イベント データ ブロックの構造を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファイル イベント ブロック タイプ (43)																																
ファイル イベント ブロック 長																																
デバイス ID (Device ID)																																
接続 インスタンス																接続 数 カウンタ																
接続 タイム スタンプ																																
ファイル イベント タイム スタンプ (File Event Timestamp)																																
送信元 IP アドレス																																
送信元 IP アドレス (続き)																																
送信元 IP アドレス (続き)																																
送信元 IP アドレス (続き)																																
宛先 IP アドレス																																
宛先 IP アドレス (続き)																																
宛先 IP アドレス (続き)																																
宛先 IP アドレス (続き)																																
傾向	SPERO 解析結果								ファイル スト レージ ステータス								ファイル 分析 ステータス															
アーカイブ ファイル ステータス	脅威スコア								操作								SHA ハッシュ															



バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	SHA ハッシュ (続き)																															
	SHA ハッシュ (続き)																															
	SHA ハッシュ (続き)																															
	SHA ハッシュ (続き)																															
	SHA ハッシュ (続き)																															
	SHA ハッシュ (続き)																															
	SHA ハッシュ (続き)																															
	SHA ハッシュ (続き)																								ファイル タイプ ID							
ファイル名	ファイル タイプ ID (続き)																								文字列ブロック タイプ (0)							
	文字列ブロック タイプ (0) (続き)																								文字列ブロック 長							
	文字列ブロック 長 (続き)																								ファイル名...							
	ファイル サイズ (File size)																															
	ファイル サイズ (続き)																															
	方向 (Direction)								アプリケーション ID (Application ID)																							
	アプリケーション ID (続き)								ユーザ ID (User ID)																							
URI	ユーザ ID (続き)								文字列ブロック タイプ (0)																							
	文字列ブロック タイプ (0) (続き)								文字列ブロック 長																							
	文字列ブロック 長 (続き)								URI...																							
シグネチャ	文字列ブロック タイプ (0)																															
	文字列ブロック 長																															
	署名...																															
	送信元ポート (Source Port)																接続先ポート															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	プロトコル								アクセス コントロール ポリシー UUID																							
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
	アクセス コントロール ポリシー UUID(続き)																															
アクセス コントロール ポリシー UUID(続き)	送信元の国																宛先の国 (Country)															
宛先の国(続き)	Web アプリケーション ID																															
Web アプリケーション ID(続き)	クライアント アプリケーション ID																															
クライアント アプリケーション ID(続き)	セキュリティ コンテキスト																															
	セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト(続き)																															
	セキュリティ コンテキスト(続き)																															
セキュリティ コンテキスト(続き)																																

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

表 B-43 ファイル イベント データ ブロックのフィールド

フィールド	データ タイプ	説明
ファイル イベント ブロック タイプ	uint32	ファイル イベント データ ブロックを開始します。この値は常に 43 です。
ファイル イベント ブロック長	uint32	ファイル イベント ブロックのバイトの合計数(ファイル イベント ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
デバイス ID (Device ID)	uint32	イベントを生成したデバイスの ID。
接続インスタンス	uint16	イベントを生成したデバイスの Snort インスタンス。接続または侵入イベントとイベントをリンクするために使用されます。

表 B-43 ファイル イベント データ ブロックのフィールド(続き)

フィールド	データ タイプ	説明
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
接続タイムスタンプ	uint32	関連する接続イベントの UNIX タイムスタンプ (1970 年 1 月 1 日からの秒数)。
ファイル イベント タイムスタンプ (File Event Timestamp)	uint32	ファイル タイプが識別されてファイル イベントが生成されたときの UNIX タイムスタンプ (1970 年 1 月 1 日からの秒数)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
傾向	uint8	<p>ファイルのマルウェア ステータス。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>1 (CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。</li> <li>2 (UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。</li> <li>3 (MALWARE): ファイルにはマルウェアが含まれています。</li> <li>4 (UNAVAILABLE): ソフトウェアから シスコ クラウドに対して、特性を確認する要求を送信できなかったか、または シスコ クラウド サービスが要求に応答しませんでした。</li> <li>5 (CUSTOM SIGNATURE): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。</li> </ul>
SPERO 解析結果	uint8	SPERO 署名がファイル分析で使用されたかどうかを示します。値が 1、2、または 3 であれば、SPERO 分析は使用されました。それ以外の値であれば、SPERO 分析は使用されませんでした。
ファイル ストレージ ステータス	uint8	<p>ファイルの保存ステータス。値は以下のとおりです。</p> <ul style="list-style-type: none"> <li>1: ファイルが保存されました</li> <li>2: ファイルが保存されました</li> <li>3: ファイルを保存できません</li> <li>4: ファイルを保存できません</li> <li>5: ファイルを保存できません</li> <li>6: ファイルを保存できません</li> <li>7: ファイルを保存できません</li> <li>8: ファイル サイズが大きすぎます</li> <li>9: ファイル サイズが小さすぎます</li> <li>10: ファイルを保存できません</li> <li>11: ファイルは保存されておらず、解析結果を入力できません</li> </ul>

表 B-43 ファイルイベントデータブロックのフィールド(続き)

フィールド	データ タイプ	説明
ファイル分析ステータス	uint8	<p>ファイルが動的分析のために送信されているかどうかを示します。値は以下のとおりです。</p> <ul style="list-style-type: none"> <li>• 0: ファイルが分析のために送信されていません</li> <li>• 1: 分析のために送信されました</li> <li>• 2: 分析のために送信されました</li> <li>• 4: 分析のために送信されました</li> <li>• 5: 送信に失敗しました</li> <li>• 6: 送信に失敗しました</li> <li>• 7: 送信に失敗しました</li> <li>• 8: 送信に失敗しました</li> <li>• 9: ファイル サイズが小さすぎます</li> <li>• 10: ファイル サイズが大きすぎます</li> <li>• 11: 分析のために送信されました</li> <li>• 12: 分析が完了しました</li> <li>• 13: 失敗(ネットワークの問題)</li> <li>• 14: 失敗(レート制限)</li> <li>• 15: 失敗(ファイルが大きすぎます)</li> <li>• 16: 失敗(ファイルの読み取りエラー)</li> <li>• 17: 失敗(内部ライブラリ エラー)</li> <li>• 19: ファイルは送信されておらず、解析結果を入力できません</li> <li>• 20: 失敗(ファイルを実行できません)</li> <li>• 21: 失敗(分析タイムアウト)</li> <li>• 22: 分析のために送信されました</li> <li>• 23: サポートされていないファイル</li> <li>• 23(ファイル送信によるファイル キャパシティの処理): 分析のためにファイルをサンドボックスに送信できなかったため、ファイル キャパシティが処理されました(センサーに保存)</li> <li>• 25(ファイル送信サーバ制限超過によるキャパシティの処理): サーバの速度制限が原因でファイル キャパシティが処理されました</li> <li>• 26(通信障害): クラウド接続失敗が原因でファイル キャパシティが処理されました</li> <li>• 27(未送信): 設定が原因でファイルは送信されていません。</li> <li>• 28(事前分類の一致なし): 事前分類でファイル内に埋め込みオブジェクトまたは疑わしいオブジェクトが検出されなかったため、ファイルはダイナミック分析用に送信されませんでした</li> <li>• 29(Transmit Sent Sandbox Private Cloud): ダイナミック分析のためにファイルがプライベートクラウドに送信されました。</li> <li>• 30(送信ボックスはプライベートクラウドに未送信): ファイルは分析のためにプライベートクラウドに送信されませんでした</li> </ul>

表 B-43 ファイルイベント データブロックのフィールド(続き)

フィールド	データ タイプ	説明
アーカイブ ファイル ステータス	uint8	この値は常に 0 です。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ~ 100)。
操作	uint8	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>• 1:検出</li> <li>• 2:ブロック</li> <li>• 3:マルウェア クラウドルックアップ</li> <li>• 4:マルウェア ブロック</li> <li>• 5:マルウェア ホワイトリスト</li> </ul>
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
ファイル タイプ ID	uint32	ファイル タイプにマップされている ID 番号。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、 <a href="#">エンドポイント向け AMP ファイルタイプのメタデータ (3-43 ページ)</a> を参照してください。
ファイル名	string	ファイルの名前。
ファイル サイズ(File size)	uint64	ファイルのサイズ(バイト単位)。
方向(Direction)	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示す値。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>• 1:ダウンロード</li> <li>• 2:アップロード</li> </ul> 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID(User ID)	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
URI	string	接続の Uniform Resource Identifier(URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。

表 B-43 ファイル イベント データ ブロックのフィールド(続き)

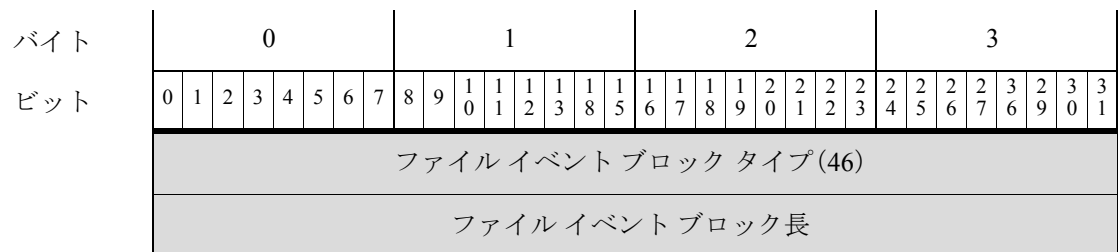
フィールド	データ タイプ	説明
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> <li>1:ICMP</li> <li>4:IP</li> <li>6:TCP</li> <li>17:UDP</li> </ul> これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアント アプリケーション ID	uint32	クライアント アプリケーションの内部 ID 番号(該当する場合)。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト (仮想ファイアウォール) の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

## ファイル イベント 5.4.x

ファイル イベントには、ネットワークを介して送信されるファイルに関する情報が含まれています。これには、接続情報、ファイルがマルウェアであるかどうかの情報、およびファイルを識別するための固有情報が含まれています。ファイル イベントのブロック タイプは、シリーズ 2 グループのブロックの、ブロック タイプ 46 です。これはブロック タイプ 43 に取って代わります。SSL とファイル アーカイブ サポート用のフィールドが追加されました。

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

次の図は、ファイル イベント データ ブロックの構造を示しています。



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

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



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

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

表 B-44 ファイルイベントデータブロック 5.4.x のフィールド

フィールド	データタイプ	説明
ファイル イベント ブロック タイプ	uint32	ファイル イベント データ ブロック を開始 します。この値は常に 46 です。
ファイル イベント ブロック 長	uint32	ファイル イベント ブロック のバイト の合計数 (ファイル イベント ブロック タイプ と長さ のフィールド 用の 8 バイト、および それに 続く データ のバイト 数 を含む)。
デバイス ID (Device ID)	uint32	イベント を生成 した デバイス の ID。
接続 インスタンス	uint16	イベント を生成 した デバイス の Snort インスタンス。接続 または 侵入 イベント と イベント を リンク する ために 使用 されます。
接続 数 カウンタ	uint16	同じ 秒 の間 に 発生 する 接続 イベント を 区別 する ために 使用 される 値。
接続 タイムスタンプ	uint32	関連 する 接続 イベント の UNIX タイムスタンプ (1970 年 1 月 1 日 から の秒数)。
ファイル イベント タイムスタンプ (File Event Timestamp)	uint32	ファイル タイプ が 識別 されて ファイル イベント が 生成 された とき の UNIX タイムスタンプ (1970 年 1 月 1 日 から の秒数)。
送信元 IP アドレス	uint8[16]	接続 の 送信元 の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続 の 宛先 の IPv4 または IPv6 アドレス。
傾向	uint8	<p>ファイル の マルウェア ステータス。有効 な 値 は 次 の と おり です。</p> <ul style="list-style-type: none"> <li>• 1 (CLEAN): ファイル は クリーン であり、マルウェア は 含まれて いません。</li> <li>• 2 (UNKNOWN): ファイル に マルウェア が 含まれて いる か どうか は 不明 です。</li> <li>• 3 (MALWARE): ファイル に は マルウェア が 含まれて います。</li> <li>• 4 (UNAVAILABLE): ソフトウェア から シスコ クラウド に対して、特性 を 確認 する 要求 を 送信 でき なかった か、または シスコ クラウド サービス が 要求 に 応答 し ません でした。</li> <li>• 5 (CUSTOM SIGNATURE): ファイル が ユーザ 定義 の ハッシュ と 一致 する ため、ユーザ が 指定 した 方法 で 処理 され ました。</li> </ul>
SPERO 解析結果	uint8	SPERO 署名 が ファイル 分析 で 使用 された か どうか を 示 します。値 が 1、2、または 3 で あれば、SPERO 分析 は 使用 され ました。それ 以外 の 値 で あれば、SPERO 分析 は 使用 され ません でした。

表 B-44 ファイルイベント データブロック 5.4.x のフィールド(続き)

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

表 B-44 ファイルイベントデータブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
ファイル分析ステータス	uint8	<p>ファイルが動的分析のために送信されているかどうかを示します。値は以下のとおりです。</p> <ul style="list-style-type: none"> <li>• 0: ファイルが分析のために送信されていません</li> <li>• 1: 分析のために送信されました</li> <li>• 2: 分析のために送信されました</li> <li>• 4: 分析のために送信されました</li> <li>• 5: 送信に失敗しました</li> <li>• 6: 送信に失敗しました</li> <li>• 7: 送信に失敗しました</li> <li>• 8: 送信に失敗しました</li> <li>• 9: ファイル サイズが小さすぎます</li> <li>• 10: ファイル サイズが大きすぎます</li> <li>• 11: 分析のために送信されました</li> <li>• 12: 分析が完了しました</li> <li>• 13: 失敗(ネットワークの問題)</li> <li>• 14: 失敗(レート制限)</li> <li>• 15: 失敗(ファイルが大きすぎます)</li> <li>• 16: 失敗(ファイルの読み取りエラー)</li> <li>• 17: 失敗(内部ライブラリ エラー)</li> <li>• 19: ファイルは送信されておらず、解析結果を入力できません</li> <li>• 20: 失敗(ファイルを実行できません)</li> <li>• 21: 失敗(分析タイムアウト)</li> <li>• 22: 分析のために送信されました</li> <li>• 23: サポートされていないファイル</li> </ul>

表 B-44 ファイルイベント データブロック 5.4.x のフィールド(続き)

フィールド	データ タイプ	説明
アーカイブ ファイルステータス	uint8	<p>調査中のアーカイブのステータス。次のいずれかの値になります。</p> <ul style="list-style-type: none"> <li>0 (N/A): ファイルがアーカイブとして検査されていません。</li> <li>1: 保留中。アーカイブは調査中です</li> <li>2: 取得済み。調査が問題なく正常に実行されました</li> <li>3: 失敗。システムのリソース不足のため調査に失敗しました。</li> <li>4: 深度の超過。調査は正常に実行されましたが、アーカイブがネストされた調査の深度を超過しました</li> <li>5: 暗号化。部分的に正常に実行されましたが、アーカイブが暗号化されているか、暗号化されたアーカイブが含まれています</li> <li>6: 調査できませんでした。部分的に正常に実行されましたが、ファイル形式が不正であるか破損しています</li> </ul>
脅威スコア	uint8	<p>動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値 (0 ~ 100)。</p>
操作	uint8	<p>ファイルタイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。</p> <ul style="list-style-type: none"> <li>1: 検出</li> <li>2: ブロック</li> <li>3: マルウェア クラウドルックアップ</li> <li>4: マルウェア ブロック</li> <li>5: マルウェア ホワイトリスト</li> <li>6: クラウドルックアップのタイムアウト</li> <li>7: カスタム検出</li> <li>8: カスタム検出ブロック</li> <li>9: アーカイブ ブロック (深度超過)</li> <li>10: アーカイブ ブロック (暗号化されている)</li> <li>11: アーカイブ ブロック (調査エラー)</li> </ul>
SHA ハッシュ	uint8[32]	<p>バイナリ形式の SHA-256 ハッシュのファイル。</p>
ファイルタイプ ID	uint32	<p>ファイルタイプにマップされている ID 番号。このフィールドの意味は、このイベントと一緒にメタデータで送信されます。詳細については、<a href="#">エンドポイント向け AMP ファイルタイプのメタデータ (3-43 ページ)</a>を参照してください。</p>
ファイル名	string	<p>ファイルの名前。</p>

表 B-44 ファイル イベント データ ブロック 5.4.x のフィールド(続き)

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

表 B-44 ファイルイベント データブロック 5.4.x のフィールド(続き)

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

表 B-44 ファイルイベントデータブロック 5.4.x のフィールド(続き)

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



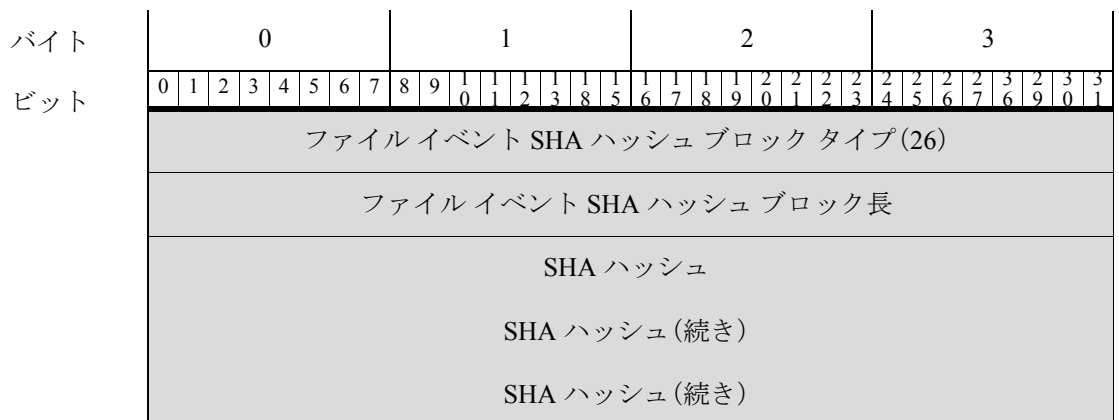
表 B-44 ファイルイベント データ ブロック 5.4.x のフィールド(続き)

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

## ファイル イベント SHA ハッシュ 5.1.1 ~ 5.2.x

eStreamer サービスは、ファイルの SHA ハッシュとそのファイル名とのマッピングのメタデータを含む、ファイル イベント SHA ハッシュ データ ブロックを使用します。ブロック タイプは、シリーズ 2 リストのデータ ブロックの 26 です。これは、ファイル ログ イベントが拡張要求(イベント コード 111)で要求されており、ビット 20 が設定されているかまたはメタデータがイベントバージョン 4 およびイベント コード 21 で要求されているか、要求することができます。

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



	SHA ハッシュ (続き)
	SHA ハッシュ (続き)
	SHA ハッシュ (続き)
	SHA ハッシュ (続き)
	SHA ハッシュ (続き)
ファイル名	文字列ブロック タイプ (0)
	文字列ブロック長
	ファイル名または解析結果...

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

表 B-45 ファイルイベント SHA ハッシュ データ ブロック 5.1.1 ~ 5.2.x のフィールド

フィールド	データ タイプ	説明
ファイル イベント SHA ハッシュ ブロック タイプ	uint32	ファイル イベント SHA ハッシュ ブロックを開始します。この値は常に 26 です。
ファイル イベント SHA ハッシュ ブロック長	uint32	ファイル イベント SHA ハッシュ ブロックのバイトの合計数 (ファイル イベント SHA ハッシュ ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
文字列ブロック タイプ	uint32	ファイルに関連付けられている記述名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと名前フィールドのバイト数が含まれます。
ファイル名または解析結果	string	ファイルの記述名または解析結果。ファイルがクリーンである場合、この値は Clean です。ファイルの解析結果が不明の場合、この値は Neutral です。ファイルにマルウェアが含まれている場合、ファイル名が示されます。

## レガシー関連イベントのデータ構造

続くいくつかのトピックでは、他のレガシー関連(コンプライアンス)データの構造について説明します。

- [関連イベント 5.0 ~ 5.0.2 \(B-275 ページ\)](#)
- [関連イベント 5.1 ~ 5.3.x \(B-283 ページ\)](#)

## 関連イベント 5.0 ~ 5.0.2

関連イベント(5.0 よりも前のバージョンではコンプライアンス イベントと呼ばれていた)には、関連ポリシー違反に関する情報が含まれます。このメッセージは、標準 eStreamer メッセージヘッダーを使用し、レコードタイプ 112 を指定し、それに関連データ ブロック タイプ 116 が続きます。データ ブロック タイプ 116 は、関連するセキュリティゾーンとインターフェイスに関する追加情報が含まれるという点で、その先行するもの(ブロック タイプ 107)とは異なります。

eStreamer からの 5.0 関連イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベントタイプコード 31 およびバージョン 7 を要求します(拡張要求の送信の詳細については、[拡張要求の送信\(2-4 ページ\)](#)を参照してください)。オプションで、最初のイベントストリーム要求メッセージのフラグフィールドでビット 23 を有効にして、拡張イベントヘッダーを含めることができます。また、フラグフィールドでビット 20 を有効にして、ユーザメタデータを含めることもできます。

レコード構造には、シリーズ 1 のブロックである、文字列ブロックタイプが含まれることに注目してください。シリーズ 1 ブロックの詳細については、[ディスカバリ\(シリーズ 1\)ブロック\(4-63 ページ\)](#)を参照してください。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ヘッダーバージョン(1)																メッセージタイプ(4)															
	メッセージ長																															
	Netmap ID																レコードタイプ(112)															
	レコード長																															
	eStreamer サーバタイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																															
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																															
	関連ブロックタイプ(116)																															
	関連ブロック長																															
	デバイス ID																															
	(関連)イベント秒																															
	イベント ID(Event ID)																															
	ポリシー ID																															
	ルール ID																															
	[プライオリティ(Priority)]																															

レガシー関連イベントのデータ構造

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	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																																	
	文字列ブロック タイプ (0)																															イベント 説明	
	文字列ブロック長																																
	説明...																							イベント タイプ (Event Type)									
	イベント デバイス ID																																
	シグネチャ ID																																
	シグネチャ ジェネレータ ID																																
	(トリガー) イベント秒																																
	(トリガー) イベント マイクロ秒																																
	イベント ID (Event ID)																																
	イベントで定義されたマスク																																
	イベント影響フラグ								IP プロトコル								ネットワーク プロトコル																
	ソース IP																																
	送信元ホストタイプ								送信元 VLAN ID																送信元 OS フィンガープリント UUID								送信元 OS フィンガープリント UUID
	送信元 OS フィンガープリント UUID (続き)																																
	送信元 OS フィンガープリント UUID (続き)																																
	送信元 OS フィンガープリント UUID (続き)																							送信元重要度									
	送信元重要度 (続き)								送信元ユーザ ID																								
	送信元ユーザ ID (続き)								送信元ポート																送信元サーバ ID								
	送信元サーバ ID (続き)																							宛先 IP (Destination IP)									
	宛先 IP (続き)																							着信ホストタイプ									

バイト	0								1								2								3								
	0	1	2	3	4	5	6	7	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																																	
	着信 VLAN ID (Admin. VLAN ID)																宛先 OS フィンガープリント UUID																宛先 OS フィン ガープリ ント UUID
	宛先 OS フィンガープリント UUID (続き)																																
	宛先 OS フィンガープリント UUID (続き)																																
	宛先 OS フィンガープリント UUID (続き)																																
	宛先 OS フィンガープリント UUID (続き)																宛先重要度																
	着信ユーザ ID (User ID)																																
	接続先ポート																宛先サーバ ID																
	宛先サーバ ID (続き)																ブロック								入力インター フェイス UUID								
	入力インターフェイス UUID (続き)																																
	入力インターフェイス UUID (続き)																																
	入力インターフェイス UUID (続き)																																
	入力インターフェイス UUID (続き)																								出力インター フェイス UUID								
	出力インターフェイス UUID (続き)																																
	出力インターフェイス UUID (続き)																																
	出力インターフェイス UUID (続き)																																
	出力インターフェイス UUID (続き)																								入力ゾーン UUID								
	入力ゾーン UUID																																
	入力ゾーン UUID (続き)																																
	入力ゾーン UUID (続き)																																
	入力ゾーン UUID (続き)																								出力ゾーン UUID								
	出力ゾーン UUID																																
	出力ゾーン UUID (続き)																																

## レガシー関連イベントのデータ構造

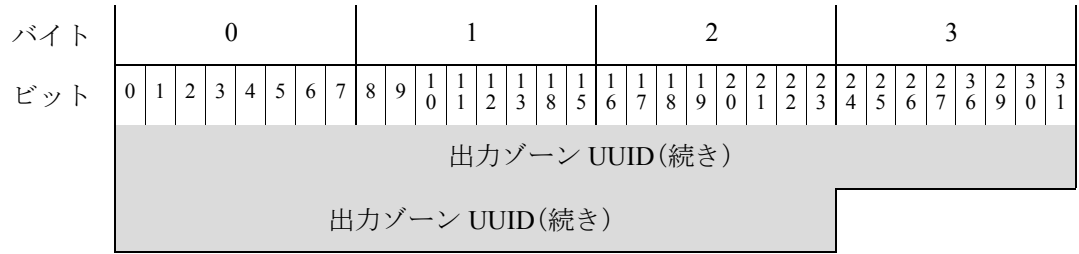


表 B-46 関連イベント データ 5.0 ~ 5.0.2 のフィールド

フィールド	データタイプ	説明
関連ブロックタイプ	uint32	関連イベントデータブロックが続くことを示します。このフィールドの値は、常に 107 です。 <a href="#">ディスカバリ (シリーズ 1) ブロック (4-63 ページ)</a> を参照してください。
関連ブロック長	uint32	関連データブロック長(関連ブロックタイプと長さの 8 バイト、およびそれに続く関連データを含む)。
デバイス ID	uint32	関連イベントを生成した管理対象デバイスまたは Defense Center の内部 ID 番号。値 0 は Defense Center を示します。バージョン 3 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 <a href="#">管理対象デバイスレコードのメタデータ (3-36 ページ)</a> を参照してください。
(関連) イベント秒	uint32	関連イベントが生成された時刻を示す UNIX タイムスタンプ (1970 年 1 月 1 日からの秒数)。
イベント ID (Event ID)	uint32	関連イベント ID 番号。
ポリシー ID	uint32	違反された関連ポリシーの ID 番号。データベースからのポリシー ID 番号を入手する方法の詳細については、 <a href="#">サーバレコード (4-16 ページ)</a> を参照してください。
ルール ID	uint32	トリガーしてポリシー違反となった関連ルールの ID 番号。データベースからのポリシー ID 番号を入手する方法の詳細については、 <a href="#">サーバレコード (4-16 ページ)</a> を参照してください。
[プライオリティ (Priority)]	uint32	イベントに割り当てられた優先順位。これは、0 ~ 5 の整数値です。
文字列ブロックタイプ	uint32	関連違反イベントの説明を含む文字列データブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、 <a href="#">文字列データブロック (4-73 ページ)</a> を参照してください。
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数(文字列のブロックタイプのための 4 バイト、文字列ブロック長のための 4 バイト、説明のバイト数を含む)。
説明	string	関連イベントについての説明。

表 B-46 関連イベント データ 5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
イベントタイプ (Event Type)	uint8	<p>関連イベントが、侵入、ホスト検出、またはユーザ イベントによってトリガーされたかどうかを示します。</p> <ul style="list-style-type: none"> <li>• 1: 侵入</li> <li>• 2: ホストのディスカバリ</li> <li>• 3: ユーザ</li> </ul>
イベントデバイス ID	uint32	<p>関連イベントをトリガーしたイベントを生成したデバイスの ID 番号。バージョン 3 メタデータを要求するとデバイス名を入手できます。詳細については、<a href="#">管理対象デバイス レコードのメタデータ (3-36 ページ)</a> を参照してください。</p>
シグネチャ ID	uint32	<p>イベントが侵入イベントであった場合、イベントに対応するルール ID 番号を示します。そうでない場合、この値は 0 になります。</p>
シグネチャジェネレータ ID	uint32	<p>イベントが侵入イベントであった場合、イベントを生成した Firepower システム プリプロセッサまたはルール エンジンの ID 番号を示します。</p>
(トリガー) イベント秒	uint32	<p>関連ポリシー ルールをトリガーしたイベントの時刻を示す UNIX タイムスタンプ (1970 年 1 月 1 日からの秒数)。</p>
(トリガー) イベント マイクロ秒	uint32	<p>イベントが検出されたタイムスタンプの、マイクロ秒 (100 万分の 1 秒) の増分。</p>
イベント ID (Event ID)	uint32	<p>デバイスによって生成されたイベントの ID 番号。</p>
イベントで定義されたマスク	bits[32]	<p>このフィールドに設定されたビットは、メッセージ内の続くどのフィールドが有効であるかを示します。各ビット値のリストの詳細については、<a href="#">表 B-47 (B-282 ページ)</a> を参照してください。</p>

表 B-46 関連イベント データ 5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
イベント影響フラグ	bits[8]	<p>イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。</li> <li>0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。</li> <li>0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。</li> <li>0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。</li> <li>0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。</li> <li>0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。</li> <li>0x40:このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます(ビット 6)。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。</li> <li>0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。</li> </ul> <p>次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。</p> <ul style="list-style-type: none"> <li>(0、不明):00x00000</li> <li>赤(1、脆弱):xxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx</li> <li>オレンジ(2、潜在的に脆弱):00x00111</li> <li>黄(3、現在は脆弱でない):00x00011</li> <li>青(4、不明なターゲット):00x00001</li> </ul>
IP プロトコル	uint8	イベントに関連付けられている IP プロトコルの ID(該当する場合)。
ネットワークプロトコル	uint16	イベントに関連付けられているネットワークプロトコル(該当する場合)。
ソース IP	uint8[4]	IP アドレス オクテットの、イベントの送信元ホストの IP アドレス。



表 B-46 関連イベント データ 5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
送信元ホストタイプ	uint8	送信元ホストのタイプ: <ul style="list-style-type: none"> <li>0: ホスト</li> <li>1: ルータ</li> <li>2: ブリッジ</li> </ul>
送信元 VLAN ID	uint16	送信元ホストの VLAN ID 番号(該当する場合)。
送信元 OS フィンガープリント UUID	uint8[16]	送信元ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID。 フィンガープリント ID にマップする値の取得の詳細については、 <a href="#">サーバレコード(4-16 ページ)</a> を参照してください。
送信元重要度	uint16	送信元ホストの、ユーザ定義の重要度値: <ul style="list-style-type: none"> <li>0: なし</li> <li>1: 低</li> <li>2: 中</li> <li>3: 高</li> </ul>
送信元ユーザ ID	uint32	システムにより識別される、送信元ホストにログインしたユーザの ID 番号。
送信元ポート	uint16	イベントの送信元ポート。
送信元サーバ ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
宛先 IP アドレス	uint8[4]	ポリシー違反に関連付けられた宛先ホストの IP アドレス(該当する場合)。宛先 IP アドレスがない場合、この値は 0 になります。
宛先ホストタイプ	uint8	宛先ホストのタイプ: <ul style="list-style-type: none"> <li>0: ホスト</li> <li>1: ルータ</li> <li>2: ブリッジ</li> </ul>
宛先 VLAN ID	uint16	宛先ホストの VLAN ID 番号(該当する場合)。
宛先 OS フィンガープリント UUID	uint8[16]	宛先ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID 番号。 フィンガープリント ID にマップする値の取得の詳細については、 <a href="#">サーバレコード(4-16 ページ)</a> を参照してください。
宛先重要度	uint16	宛先ホストの、ユーザ定義の重要度値: <ul style="list-style-type: none"> <li>0: なし</li> <li>1: 低</li> <li>2: 中</li> <li>3: 高</li> </ul>

表 B-46 関連イベントデータ 5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
宛先ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
接続先ポート	uint16	イベントの宛先ポート。
宛先サービス ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
ブロック	uint8	侵入イベントをトリガーしたパケットの処理を示す値。 <ul style="list-style-type: none"> <li>0: 侵入イベントがドロップされていない</li> <li>1: 侵入イベントがドロップされている (展開がインライン型、スイッチ型、またはルーティング型である場合はドロップ)</li> <li>2: 侵入ポリシーが、インライン型、スイッチ型、またはルーティング型展開のデバイスに適用されている場合は、イベントをトリガーしたパケットがドロップされている可能性がある。</li> </ul>
入力インターフェイス UUID	uint8[16]	関連イベントに関連付けられている入力インターフェイスの固有識別子として機能するインターフェイス ID。
出力インターフェイス UUID	uint8[16]	関連イベントに関連付けられている出力インターフェイスの固有識別子として機能するインターフェイス ID。
入力ゾーン UUID	uint8[16]	関連イベントに関連付けられている入力セキュリティゾーンの固有識別子として機能するゾーン ID。
出力ゾーン UUID	uint8[16]	関連イベントに関連付けられている出力セキュリティゾーンの固有識別子として機能するゾーン ID。

次の表は、各イベント定義マスク値についての説明です。

表 B-47 イベントで定義された値

説明	マスク値
イベント影響フラグ	0x00000001
IP プロトコル	0x00000002
ネットワーク プロトコル	0x00000004
ソース IP	0x00000008
送信元ホスト タイプ	0x00000010
送信元 VLAN ID	0x00000020
送信元フィンガープリント ID	0x00000040
送信元重要度	0x00000080
送信元ポート	0x00000100
送信元サーバ	0x00000200
宛先 IP (Destination IP)	0x00000400
宛先ホスト タイプ	0x00000800

表 B-47 イベントで定義された値(続き)

説明	マスク値
宛先 VLAN ID	0x00001000
宛先フィンガープリント ID	0x00002000
宛先重要度	0x00004000
接続先ポート	0x00008000
宛先サーバ	0x00010000
送信元ユーザ	0x00020000
宛先ユーザ	0x00040000

## 関連イベント 5.1 ~ 5.3.x

関連イベント(5.0 よりも前のバージョンではコンプライアンス イベントと呼ばれていた)には、関連ポリシー違反に関する情報が含まれます。このメッセージは、標準 eStreamer メッセージ ヘッダーを使用し、レコードタイプ 112 を指定し、それにシリーズ 1 セットのデータブロックの関連データブロック タイプ 128 が続きます。データブロック タイプ 128 は、IPv6 サポートが含まれるという点で、その先行するもの(ブロック タイプ 116)とは異なります。

eStreamer からの 5.1 ~ 5.3.x の関連イベントは、拡張要求によってのみ要求できます。これに対してはストリーム要求メッセージでイベントタイプコード 31 およびバージョン 8 を要求します(拡張要求の送信の詳細については、[拡張要求の送信\(2-4 ページ\)](#)を参照してください)。オプションで、最初のイベントストリーム要求メッセージのフラグフィールドでビット 23 を有効にして、拡張イベントヘッダーを含めることができます。また、フラグフィールドでビット 20 を有効にして、ユーザ メタデータを含めることもできます。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	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(112)																							
	レコード長																																							
	eStreamer サーバ タイムスタンプ(イベント用、ビット 23 が設定されている場合のみ)																																							
	将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合のみ)																																							
	関連ブロック タイプ(128)																																							
	関連ブロック長																																							
	デバイス ID (Device ID)																																							

レガシー関連イベントのデータ構造

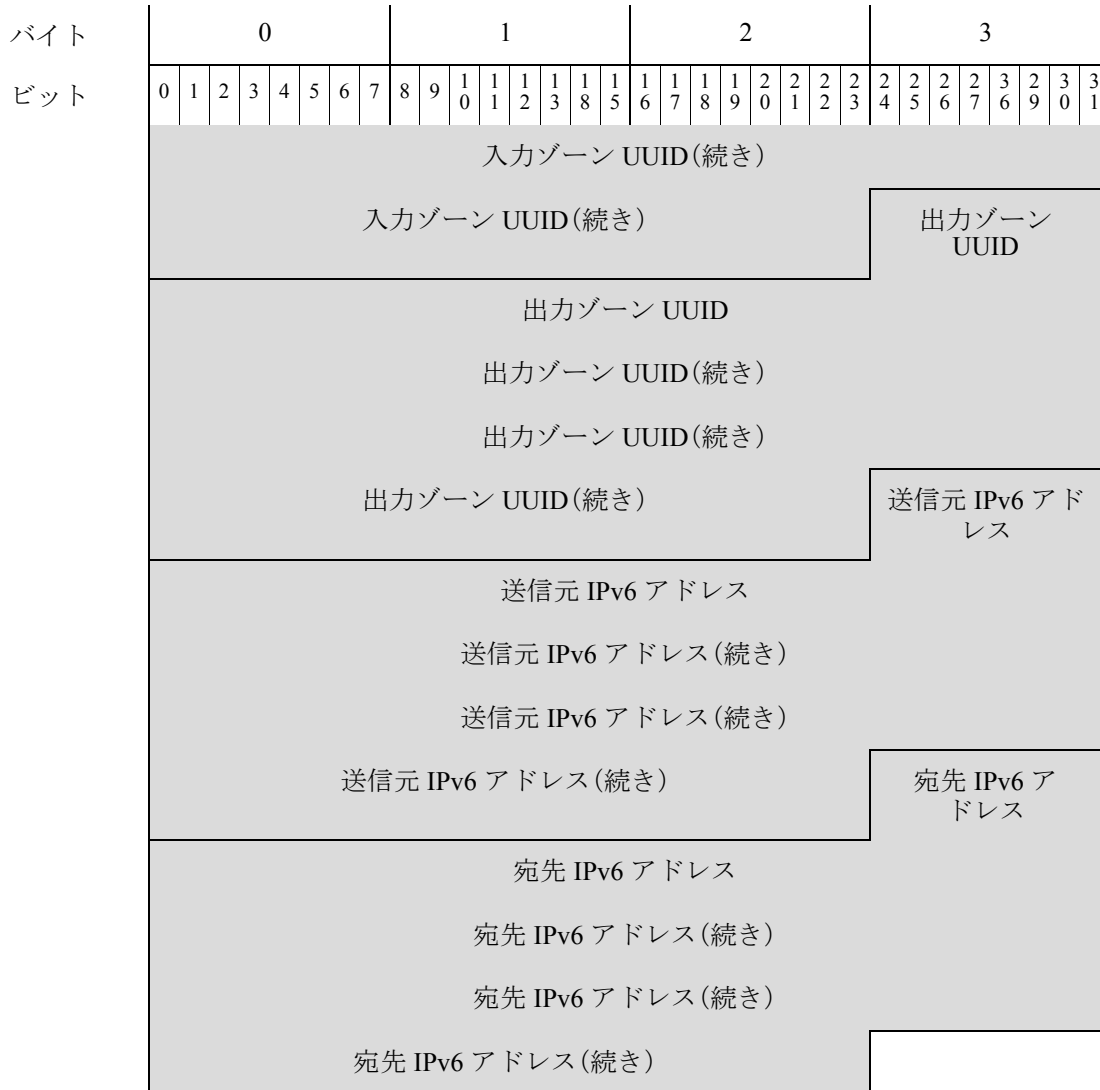
バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	(関連)イベント秒																															
	イベント ID (Event ID)																															
	ポリシー ID																															
	ルール ID																															
	[プライオリティ (Priority)]																															
	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	説明...																								イベントタイプ (Event Type)							
	イベント デバイス ID																															
	シグネチャ ID																															
	シグネチャ ジェネレータ ID																															
	(トリガー)イベント秒																															
	(トリガー)イベント マイクロ秒																															
	イベント ID (Event ID)																															
	イベントで定義されたマスク																															
	イベント影響フラグ								IPプロトコル								ネットワーク プロトコル															
	ソース IP																															
	送信元ホストタイプ								送信元 VLAN ID																送信元 OS フィンガープリント UUID							
	送信元 OS フィンガープリント UUID (続き)																															
	送信元 OS フィンガープリント UUID (続き)																															
	送信元 OS フィンガープリント UUID (続き)																															
	送信元 OS フィンガープリント UUID (続き)																								送信元重要度							
	送信元重要度 (続き)								送信元ユーザ ID																							

イベント  
説明

送信元 OS  
フィンガー  
プリント  
UUID

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	送信元ユーザ ID (続き)								送信元ポート								送信元サーバ ID															
	送信元サーバ ID (続き)																宛先 IP (Destination IP)															
	宛先 IP (続き)																着信ホストタイプ															
	着信 VLAN ID (Admin. VLAN ID)								宛先 OS フィンガープリント UUID								宛先 OS フィンガープリント UUID															
	宛先 OS フィンガープリント UUID (続き)																															
	宛先 OS フィンガープリント UUID (続き)																															
	宛先 OS フィンガープリント UUID (続き)																															
	宛先 OS フィンガープリント UUID (続き)								宛先重要度																							
	着信ユーザ ID (User ID)																															
	接続先ポート																宛先サーバ ID															
	宛先サーバ ID (続き)																ブロック								入カインターフェイス UUID							
	入カインターフェイス UUID (続き)																出カインターフェイス UUID															
	入カインターフェイス UUID (続き)																															
	入カインターフェイス UUID (続き)																															
	入カインターフェイス UUID (続き)																入カゾーン UUID															
	出カインターフェイス UUID (続き)																															
	出カインターフェイス UUID (続き)																															
	出カインターフェイス UUID (続き)																入カゾーン UUID															
	入カゾーン UUID																															
	入カゾーン UUID (続き)																															

## レガシー関連イベントのデータ構造



レコード構造には、シリーズ 1 のブロックである、文字列ブロック タイプが含まれることに注目してください。シリーズ 1 ブロックの詳細については、[ディスカバリ \(シリーズ 1\) ブロック \(4-63 ページ\)](#)を参照してください。

表 B-48 関連イベント データ 5.1 ~ 5.3.x のフィールド

フィールド	データタイプ	説明
関連ブロックタイプ	uint32	関連イベント データ ブロックが続くことを示します。このフィールドの値は、常に 128 です。 <a href="#">ディスカバリ (シリーズ 1) ブロック (4-63 ページ)</a> を参照してください。
関連ブロック長	uint32	関連データ ブロック長 (関連ブロック タイプと長さの 8 バイト、およびそれに続く関連データを含む)。

表 B-48 関連イベントデータ 5.1 ~ 5.3.x のフィールド(続き)

フィールド	データタイプ	説明
デバイス ID (Device ID)	uint32	関連イベントを生成した管理対象デバイスまたは Defense Center の内部 ID 番号。値 0 は Defense Center を示します。バージョン 3 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 <a href="#">管理対象デバイスレコードのメタデータ (3-36 ページ)</a> を参照してください。
(関連) イベント秒	uint32	関連イベントが生成された時刻を示す UNIX タイムスタンプ (1970 年 1 月 1 日からの秒数)。
イベント ID (Event ID)	uint32	関連イベント ID 番号。
ポリシー ID	uint32	違反された関連ポリシーの ID 番号。データベースからのポリシー ID 番号を入手する方法の詳細については、 <a href="#">サーバレコード (4-16 ページ)</a> を参照してください。
ルール ID	uint32	トリガーしてポリシー違反となった関連ルールの ID 番号。データベースからのポリシー ID 番号を入手する方法の詳細については、 <a href="#">サーバレコード (4-16 ページ)</a> を参照してください。
[プライオリティ (Priority)]	uint32	イベントに割り当てられた優先順位。これは、0 ~ 5 の整数値です。
文字列ブロックタイプ	uint32	関連違反イベントの説明を含む文字列データブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、 <a href="#">文字列データブロック (4-73 ページ)</a> を参照してください。
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数(文字列のブロックタイプのための 4 バイト、文字列ブロック長のための 4 バイト、説明のバイト数を含む)。
説明	string	関連イベントについての説明。
イベントタイプ (Event Type)	uint8	関連イベントが、侵入、ホスト検出、またはユーザイベントによってトリガーされたかどうかを示します。 <ul style="list-style-type: none"> <li>• 1: 侵入</li> <li>• 2: ホストのディスカバリ</li> <li>• 3: ユーザ</li> </ul>
イベントデバイス ID	uint32	関連イベントをトリガーしたイベントを生成したデバイスの ID 番号。バージョン 3 メタデータを要求するとデバイス名を入手できます。詳細については、 <a href="#">管理対象デバイスレコードのメタデータ (3-36 ページ)</a> を参照してください。
シグネチャ ID	uint32	イベントが侵入イベントであった場合、イベントに対応するルール ID 番号を示します。そうでない場合、この値は 0 になります。
シグネチャジェネレータ ID	uint32	イベントが侵入イベントであった場合、イベントを生成した Firepower システム プリプロセッサまたはルールエンジンの ID 番号を示します。
(トリガー) イベント秒	uint32	関連ポリシールールをトリガーしたイベントの時刻を示す UNIX タイムスタンプ (1970 年 1 月 1 日からの秒数)。

表 B-48 関連イベント データ 5.1 ~ 5.3.x のフィールド(続き)

フィールド	データタイプ	説明
(トリガー)イベントマイクロ秒	uint32	イベントが検出されたタイムスタンプの、マイクロ秒(100 万分の 1 秒)の増分。
イベント ID (Event ID)	uint32	シスコ デバイスによって生成されたイベントの ID 番号。
イベントで定義されたマスク	bits[32]	このフィールドに設定されたビットは、メッセージ内の続くどのフィールドが有効であるかを示します。各ビット値のリストの詳細については、表 B-47(B-282 ページ)を参照してください。
イベント影響フラグ	bits[8]	<p>イベントの影響フラグ値。下位 8 ビットは影響レベルを示します。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。</li> <li>0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。</li> <li>0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。</li> <li>0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。</li> <li>0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。</li> <li>0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。</li> <li>0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。</li> <li>0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ)</li> </ul> <p>次の影響レベル値は、Defense Center の特定の優先順位にマップされます。x は、値が 0 または 1 になることを示しています。</p> <ul style="list-style-type: none"> <li>(0、不明):00x00000</li> <li>赤(1、脆弱):xxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx(バージョン 5.0+ のみ)</li> <li>オレンジ(2、潜在的に脆弱):00x0011x</li> <li>黄(3、現在は脆弱でない):00x0001x</li> <li>青(4、不明なターゲット):00x00001</li> </ul>



表 B-48 関連イベント データ 5.1 ~ 5.3.x のフィールド(続き)

フィールド	データタイプ	説明
IP プロトコル	uint8	イベントに関連付けられている IP プロトコルの ID(該当する場合)。
ネットワーク プロトコル	uint16	イベントに関連付けられているネットワーク プロトコル(該当する場合)。
送信元 IP アドレス	uint8[4]	このフィールドは予約済みですが、設定されておりません。送信元 IPv4 アドレスは、送信元 IPv6 アドレス フィールドに保存されます。詳細については、 <a href="#">IP アドレス(1-5 ページ)</a> を参照してください。
送信元ホストタイプ	uint8	送信元ホストのタイプ: <ul style="list-style-type: none"> <li>0: ホスト</li> <li>1: ルータ</li> <li>2: ブリッジ</li> </ul>
送信元 VLAN ID	uint16	送信元ホストの VLAN ID 番号(該当する場合)。
送信元 OS フィンガープリント UUID	uint8[16]	送信元ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID。 フィンガープリント ID にマップする値の取得の詳細については、 <a href="#">サーバ レコード(4-16 ページ)</a> を参照してください。
送信元重要度	uint16	送信元ホストの、ユーザ定義の重要度値: <ul style="list-style-type: none"> <li>0: なし</li> <li>1: 低</li> <li>2: 中</li> <li>3: 高</li> </ul>
送信元ユーザ ID	uint32	システムにより識別される、送信元ホストにログインしたユーザの ID 番号。
送信元ポート	uint16	イベントの送信元ポート。
送信元サーバ ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
宛先 IP アドレス	uint8[4]	このフィールドは予約済みですが、設定されておりません。宛先 IPv4 アドレスは、宛先 IPv6 アドレス フィールドに保存されます。詳細については、 <a href="#">IP アドレス(1-5 ページ)</a> を参照してください。
宛先ホストタイプ	uint8	宛先ホストのタイプ: <ul style="list-style-type: none"> <li>0: ホスト</li> <li>1: ルータ</li> <li>2: ブリッジ</li> </ul>
宛先 VLAN ID	uint16	宛先ホストの VLAN ID 番号(該当する場合)。

表 B-48 関連イベント データ 5.1 ~ 5.3.x のフィールド(続き)

フィールド	データタイプ	説明
宛先 OS フィンガープリント UUID	uint8[16]	宛先ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID 番号。 フィンガープリント ID にマップする値の取得の詳細については、 <a href="#">サーバ レコード(4-16 ページ)</a> を参照してください。
宛先重要度	uint16	宛先ホストの、ユーザ定義の重要度値: <ul style="list-style-type: none"> <li>• 0:なし</li> <li>• 1:低</li> <li>• 2:中</li> <li>• 3:高</li> </ul>
宛先ユーザ ID	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
接続先ポート	uint16	イベントの宛先ポート。
宛先サービス ID	uint32	送信元ホスト上で実行するサーバの ID 番号。
ブロック	uint8	侵入イベントをトリガーしたパケットの処理を示す値。 <ul style="list-style-type: none"> <li>• 0:侵入イベントがドロップされていない</li> <li>• 1:侵入イベントがドロップされている(展開がインライン型、スイッチ型、またはルーティング型である場合はドロップ)</li> <li>• 2:侵入ポリシーが、インライン型、スイッチ型、またはルーティング型展開のデバイスに適用されている場合は、イベントをトリガーしたパケットがドロップされている可能性がある。</li> </ul>
入力インターフェイス UUID	uint8[16]	関連イベントに関連付けられている入力インターフェイスの固有識別子として機能するインターフェイス ID。
出力インターフェイス UUID	uint8[16]	関連イベントに関連付けられている出力インターフェイスの固有識別子として機能するインターフェイス ID。
入力ゾーン UUID	uint8[16]	関連イベントに関連付けられている入力セキュリティ ゾーンの固有識別子として機能するゾーン ID。
出力ゾーン UUID	uint8[16]	関連イベントに関連付けられている出力セキュリティ ゾーンの固有識別子として機能するゾーン ID。
送信元 IPv6 アドレス	uint8[16]	IPv6 アドレス オクテットの、イベントの送信元ホストの IP アドレス。
宛先 IPv6 アドレス	uint8[16]	IPv6 アドレス オクテットの、イベントの宛先ホストの IP アドレス。

## レガシー ホスト データ構造

これらの構造を要求するには、ホスト要求メッセージを使用する必要があります。レガシー構造を要求するには、古い形式のホスト要求メッセージを使用する必要があります。詳細については、[ホスト要求メッセージの形式\(2-27 ページ\)](#)を参照してください。

続くいくつかのトピックでは、ホストプロファイルとフルホストプロファイルの両方の構造を含む、レガシーホストデータ構造について説明します。

- フルホストプロファイルデータブロック 5.0 ~ 5.0.2 (B-292 ページ)
- フルホストプロファイルデータブロック 5.1.1 (B-302 ページ)
- フルホストプロファイルデータブロック 5.2.x (B-313 ページ)
- ホストプロファイルデータブロック 5.1.x (B-327 ページ)
- IP 範囲仕様データブロック 5.0 ~ 5.1.1.x (B-334 ページ)
- アクセスコントロールポリシールール理由データブロック (B-334 ページ)

## フルホストプロファイルデータブロック 5.0 ~ 5.0.2

フルホストプロファイルデータブロックバージョン 5.0 ~ 5.0.2 には、1つのホストを記述するフルセットのデータが含まれています。このデータセットの形式を次の図に示し、次表で説明します。図には、リストデータブロックを除き、カプセル化データブロックフィールドを提示していない点にご注意ください。これらのカプセル化データブロックは、[検出と接続データ構造の概要 \(4-1 ページ\)](#) で別途説明します。フルホストプロファイルデータブロックのブロックタイプ値は、111 です。



(注)

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

バイト	0								1							2							3									
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	フルホストプロファイルデータブロック (111)																															
	データブロック長																															
	[IP アドレス (IP Address)]																															
	ホップ							汎用リストブロックタイプ (31)																								
	汎用リストブロックタイプ (続き)							汎用リストブロック長																								

バイト	0							1							2							3																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						
OS から取得したフィンガープリント	汎用リストブロック長(続き)							オペレーティングシステムフィンガープリントブロックタイプ(130)*																														
	OSフィンガープリントブロックタイプ(130)*(続き)							オペレーティングシステムフィンガープリントブロック長																														
	OSフィンガープリントブロック長(続き)							オペレーティングシステムから取得したフィンガープリントデータ...																														
	汎用リストブロックタイプ(31)																																					
	汎用リストブロック長																																					
サーバフィンガープリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																																					
	オペレーティングシステムフィンガープリントブロック長																																					
	オペレーティングシステムサーバフィンガープリントデータ																																					
	汎用リストブロックタイプ(31)																																					
	汎用リストブロック長																																					
クライアントフィンガープリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																																					
	オペレーティングシステムフィンガープリントブロック長																																					
	オペレーティングシステムクライアントフィンガープリントデータ...																																					
	汎用リストブロックタイプ(31)																																					
	汎用リストブロック長																																					
VDB ネイティブフィンガープリント1	オペレーティングシステムフィンガープリントブロックタイプ(130)*																																					
	オペレーティングシステムフィンガープリントブロック長																																					
	オペレーティングシステムVDBフィンガープリントデータ...																																					
	汎用リストブロックタイプ(31)																																					
	汎用リストブロック長																																					

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
VDB ネイティブフィンガープリント2	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムVDBフィンガープリントデータ...																															
汎用リストブロックタイプ(31)																																
汎用リストブロック長																																
ユーザ(User)フィンガープリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムユーザフィンガープリントデータ...																															
汎用リストブロックタイプ(31)																																
汎用リストブロック長																																
スキャン(Scan)フィンガープリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムスキャンフィンガープリントデータ...																															
汎用リストブロックタイプ(31)																																
汎用リストブロック長																																
Applicationフィンガープリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムアプリケーションフィンガープリントデータ...																															
汎用リストブロックタイプ(31)																																
汎用リストブロック長																																
競合フィンガープリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステム競合のフィンガープリントデータ...																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
(TCP)フルサーバデータ	リストブロック タイプ(11)...																															
	リストブロック長...																															
	(TCP)全サーバデータ ブロック (104)*																															
(UDP)全サーバデータ	リストブロック タイプ(11)																															
	リストブロック長																															
	(UDP)全サーバデータ ブロック (104)*																															
ネットワークプロトコルデータ	リストブロック タイプ(11)																															
	リストブロック長																															
	(ネットワーク)プロトコルデータ ブロック (4)*																															
トランスポート (Transport) プロトコル データ	リストブロック タイプ(11)																															
	リストブロック長																															
	(トランスポート)プロトコルデータ ブロック (4)*																															
MAC アドレス データ	リストブロック タイプ(11)																															
	リストブロック長																															
	ホスト MAC アドレス データ ブロック (95)*																															
	Last Seen																															
	ホスト タイプ																															
	ビジネス上の重要度																VLAN ID (Admin. VLAN ID)															
	VLAN タイプ								VLAN 優先順位								汎用リストブロック タイプ(31)															
ホストクライアントデータ	汎用リストブロック タイプ(続き)																汎用リストブロック長															
	汎用リストブロック長(続き)																フルホストクライアントアプリケーションデータブロック (112)*															
NetBIOS [名前(Name) ]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	NetBIOS 名文字列																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
注記 (Notes) データ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	Notes 文字列....																															
(VDB)ホスト Vulns	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	(VDB)ホスト脆弱性データ ブロック (85)*																															
(サードパー ティ/VDB) Host Vulns	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	(サードパーティ/VDB)ホスト脆弱性データ ブロック (85)*																															
サードパー ティ スキャン Host Vulns	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	(サードパーティ スキャン)元の Vuln ID によるホスト脆弱性データ ブロック (85)*																															
属性 (Attribute) 値データ	リストブロック タイプ (11)																															
	リストブロック長																															
	属性値データ ブロック*																															

次の表は、フル ホスト プロファイル 5.0 ~ 5.0.2 レコードのコンポーネントについての説明です。

表 B-49 フルホスト プロファイル レコード 5.0 ~ 5.0.2 のフィールド

フィールド	データタイプ	説明
[IP アドレス (IP Address)]	uint8[4]	IP アドレス オクテットの、ホストの IP アドレス。
ホップ	uint8	ホストからデバイスへのネットワーク ホップ数。
汎用リストブ ロック タイプ	uint32	ホストの既存のフィンガープリントから取得したフィンガープリント データを送送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。



表 B-49 フルホストプロファイルレコード5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムから取得したフィンガープリントデータブロック*	変数 (variable)	ホストの既存のフィンガープリントから取得したホストでのオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	サーバフィンガープリントを使用して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(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、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	クライアントフィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	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、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。

表 B-49 フルホスト プロファイル レコード 5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
オペレーティングシステムフィンガープリント(VDB)ネイティブフィンガープリント1)データブロック*	変数(variable)	シスコ 脆弱性データベース(VDB)のフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリント データを送信するオペレーティングシステムフィンガープリント データブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(VDB)ネイティブフィンガープリント2)データブロック*	変数(variable)	シスコ 脆弱性データベース(VDB)のフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	ユーザが追加したフィンガープリント データを送信するオペレーティングシステムフィンガープリント データブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(ユーザフィンガープリント)データブロック*	変数(variable)	ユーザが追加したホストのオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	脆弱性スキャナによって追加されたフィンガープリント データを送信するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。

表 B-49 フルホストプロファイルレコード5.0～5.0.2のフィールド(続き)

フィールド	データタイプ	説明
オペレーティングシステムフィンガープリント(スキャンフィンガープリント)データブロック*	変数 (variable)	脆弱性スキャナによって追加されたホストのオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	アプリケーションによって追加されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(アプリケーションフィンガープリント)データブロック*	変数 (variable)	アプリケーションによって追加されたホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	フィンガープリント競合解決から選択したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(競合フィンガープリント)データブロック*	変数 (variable)	フィンガープリント競合解決から選択したホストのオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
リストブロックタイプ	uint32	TCP サービスデータを伝送する全サーバデータブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リストブロックタイプフィールド、リストブロック長フィールド、すべてのカプセル化全サーバデータブロック長から成る 8 バイトを含みます。
(TCP)全サーバデータブロック*	変数 (variable)	ホストで TCP サービスに関するデータを伝送する全サーバデータブロックのリスト。このデータブロックの説明の詳細については、 <a href="#">フルホストサーバデータブロック 4.10.0+(4-146 ページ)</a> を参照してください。

表 B-49 フルホスト プロファイル レコード 5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
リストブロックタイプ	uint32	UDP サービス データを伝送する全サーバデータ ブロックを含むリスト データ ブロックを表示します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値には、リスト ブロック タイプ フィールド、リスト ブロック 長 フィールド、すべてのカプセル化全サーバデータ ブロック 長から成る 8 バイトを含みます。
(UDP) 全サーバデータ ブロック*	変数 (variable)	ホストで UDP サブサービスに関するデータを伝送する全サーバデータ ブロックのリスト。このデータ ブロックの説明の詳細については、フルホスト サーバデータ ブロック 4.10.0+ (4-146 ページ) を参照してください。
リストブロックタイプ	uint32	ネットワーク プロトコル データを伝えるプロトコル データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック長	uint32	リスト内のバイト数。この数値には、リスト ブロック タイプ フィールド、リスト ブロック 長 フィールド、すべてのカプセル化プロトコル データ ブロック 長から成る 8 バイトを含みます。
(ネットワーク) プロトコル データ ブロック*	変数 (variable)	ホストでネットワーク プロトコルに関するデータを伝送するプロトコル データ ブロックのリスト。このデータ ブロックの説明の詳細については、プロトコル データ ブロック (4-78 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。
リスト ブロック長	uint32	リスト内のバイト数。この数値には、リスト ブロック タイプ フィールド、リスト ブロック 長 フィールド、すべてのカプセル化プロトコル データ ブロック 長から成る 8 バイトを含みます。
(トランスポート) プロトコル データ ブロック*	変数 (variable)	ホストでトランスポート プロトコルに関するデータを伝送するプロトコル データ ブロックのリスト。このデータ ブロックの説明の詳細については、プロトコル データ ブロック (4-78 ページ) を参照してください。
リストブロックタイプ	uint32	ホスト MAC アドレス データ ブロックを含むリスト データ ブロックを表示します。この値は常に 11 です。
リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化ホスト MAC アドレス データ ブロックを含むリストのバイト数。
ホスト MAC アドレス データ ブロック*	変数 (variable)	ホスト MAC アドレス データ ブロックのリスト。このデータ ブロックの詳細については、ホスト MAC アドレス 4.9+ (4-119 ページ) を参照してください。
最後の確認日時	uint32	システムがホスト アクティビティを検出した前回時刻を表す UNIX タイムスタンプ。

表 B-49 フルホストプロファイルレコード5.0 ~ 5.0.2 のフィールド(続き)

フィールド	データタイプ	説明
ホストタイプ	uint32	ホストのタイプを示します。次の値を指定します。 <ul style="list-style-type: none"> <li>0 — ホスト</li> <li>1: ルータ</li> <li>2 — ブリッジ</li> <li>3 — NAT(ネットワーク アドレス変換デバイス)</li> <li>4 — LB(ロード バランサー)</li> </ul>
ビジネス上の重要度	uint16	ビジネスに対するホストの重要度を示します。
VLAN ID (Admin. VLAN ID)	uint16	ホストがメンバーである 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 タグに含まれるプライオリティ値。
汎用リストブロックタイプ	uint32	クライアントアプリケーションデータを伝える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	リストヘッダーやすべてのカプセル化クライアントアプリケーションデータブロックを含む汎用リストデータブロック内のバイト数。
全ホストクライアントアプリケーションデータブロック*	変数 (variable)	クライアントアプリケーションデータ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、 <a href="#">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+(4-159 ページ)</a> 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。
文字列ブロックタイプ	uint32	ホストの注記の文字列データブロックを表示します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロックタイプフィールドおよび文字列ブロック長フィールドの 8 バイトを含む注記文字列データブロックのバイト数および注記文字列のバイト数。
注記(Notes)	string	ホストの注記ホスト属性の内容を含みます。
汎用リストブロックタイプ	uint32	VDB 脆弱性データを伝送するホスト脆弱性データブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化データブロックを含む汎用リストデータブロック内のバイト数。

表 B-49 フルホスト プロファイル レコード 5.0 ~ 5.0.2 のフィールド (続き)

フィールド	データタイプ	説明
(VDB) ホスト脆弱性データ ブロック*	変数 (variable)	シスコ 脆弱性データベース (VDB) で特定された脆弱性に関するホスト脆弱性データ ブロックのリスト。このデータ ブロックの説明の詳細については、 <a href="#">ホスト脆弱性データ ブロック 4.9.0+ (4-116 ページ)</a> を参照してください。
汎用リスト ブロック タイプ	uint32	サードパーティ スキャン脆弱性データを伝送するホスト脆弱性データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化データ ブロックを含む汎用リスト データ ブロック内のバイト数。
(サードパーティ/VDB) ホスト脆弱性データ ブロック*	変数 (variable)	サードパーティのスキナから送信され、シスコ 脆弱性データベース (VDB) でカタログされているホストの脆弱性に関する情報を含むホスト脆弱性データ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">ホスト脆弱性データ ブロック 4.9.0+ (4-116 ページ)</a> を参照してください。
汎用リスト ブロック タイプ	uint32	サードパーティ スキャン脆弱性データを伝送するホスト脆弱性データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化データ ブロックを含む汎用リスト データ ブロック内のバイト数。
(サードパーティ スキャン) ホスト脆弱性データ ブロック*	変数 (variable)	サードパーティのスキナから送信されたホスト脆弱性データ ブロック。これらのデータ ブロックのホスト脆弱性 ID は、サードパーティのスキナ ID であり、シスコ によって検出された ID ではない点にご注意ください。このデータ ブロックの説明の詳細については、 <a href="#">ホスト脆弱性データ ブロック 4.9.0+ (4-116 ページ)</a> を参照してください。
リスト ブロック タイプ	uint32	属性データを伝送する属性値データ ブロックを含むリスト データ ブロックを表示します。この値は常に 11 です。
リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化データ ブロックを含むリスト データ ブロック内のバイト数。
属性値データ ブロック*	変数 (variable)	属性値データ ブロックのリスト。このリストのデータ ブロックの詳細については、 <a href="#">属性値データ ブロック (4-84 ページ)</a> を参照してください。

## フルホスト プロファイル データ ブロック 5.1.1

フルホスト プロファイル データ ブロック バージョン 5.1.1 には、1つのホストを記述するフルセットのデータが含まれています。このデータセットの形式を次の図に示し、次表で説明します。図には、リストデータ ブロックを除き、カプセル化データ ブロック フィールドを提示していない点にご注意ください。これらのカプセル化データ ブロックは、[検出と接続データ構造の概要 \(4-1 ページ\)](#)で別途説明します。フルホスト プロファイル データ ブロックのブロックタイプ値は、135 です。これによりデータ ブロック 111 は廃止されます。



(注)

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	フル ホスト プロファイル データ ブロック (135)																															
	データ ブロック 長																															
	[IP アドレス (IP Address)]																															
	ホップ								汎用リストブロック タイプ (31)																							
	汎用リストブロック タイプ (続き)								汎用リストブロック 長																							
OS から取得したフィンガープリント	汎用リストブロック 長 (続き)								オペレーティング システム フィンガープリント ブロック タイプ (130)*																							
	OS フィンガープリント ブロック タイプ (130)* (続き)								オペレーティング システム フィンガープリント ブロック 長																							
	OS フィンガープリント ブロック 長 (続き)								オペレーティング システム から取得した フィンガープリント データ...																							
	汎用リストブロック タイプ (31)																															
	汎用リストブロック 長																															
サーバフィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ (130)*																															
	オペレーティング システム フィンガープリント ブロック 長																															
	オペレーティング システム サーバ フィンガープリント データ																															
	汎用リストブロック タイプ (31)																															
	汎用リストブロック 長																															

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
クライアントフィンガープリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムクライアントフィンガープリントデータ...																															
	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
VDB ネイティブフィンガープリント1	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムVDBフィンガープリントデータ...																															
	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
VDB ネイティブフィンガープリント2	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムVDBフィンガープリントデータ...																															
	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
ユーザ(User)フィンガープリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムユーザフィンガープリントデータ...																															
	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
スキャン(Scan)フィンガープリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムスキャンフィンガープリントデータ...																															
	汎用リストブロックタイプ(31)																															



バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ビット																																
	汎用リストブロック長																															
Application フィンガー プリント	オペレーティング システム フィンガープリントブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム アプリケーション フィンガープリント データ...																															
	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
競合 フィンガー プリント	オペレーティング システム フィンガープリントブロック タイプ(130)*																															
	オペレーティング システム フィンガープリント ブロック長																															
	オペレーティング システム 競合のフィンガープリント データ...																															
(TCP)フルサーバ データ	リストブロック タイプ(11)...																															
	リストブロック長...																															
	(TCP)全サーバデータ ブロック (104)*																															
(UDP)全サーバデー タ	リストブロック タイプ(11)																															
	リストブロック長																															
	(UDP)全サーバデータ ブロック (104)*																															
ネットワー クプロトコ ルデータ	リストブロック タイプ(11)																															
	リストブロック長																															
	(ネットワーク)プロトコルデータ ブロック (4)*																															
トランス ポート (Transport) プロトコル データ	リストブロック タイプ(11)																															
	リストブロック長																															
	(トランスポート)プロトコルデータ ブロック (4)*																															
MAC アドレス データ	リストブロック タイプ(11)																															
	リストブロック長																															
	ホスト MAC アドレス データ ブロック (95)*																															

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																																
	Last Seen																															
	ホスト タイプ																															
	ビジネス上の重要度																VLAN ID (Admin. VLAN ID)															
	VLAN タイプ								VLAN 優先順位								汎用リストブロック タイプ (31)															
ホストクライアントデータ	汎用リストブロック タイプ (続き)																汎用リストブロック長															
	汎用リストブロック長 (続き)																フル ホストクライアントアプリケーションデータブロック (112)*															
NetBIOS [名前 (Name)]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	NetBIOS 名文字列																															
注記 (Notes) データ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	Notes 文字列...																															
(VDB) ホスト Vulns	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	(VDB) ホスト脆弱性データ ブロック (85)*																															
(サードパーティ/VDB) Host Vulns	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	(サードパーティ/VDB) ホスト脆弱性データ ブロック (85)*																															
サードパーティ スキャン Host Vulns	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	(サードパーティ スキャン) 元の Vuln ID によるホスト脆弱性データ ブロック (85)*																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
属性 (Attribute) 値データ	リストブロック タイプ(11)																															
	リストブロック長																															
	属性値データ ブロック*																															
	Mobile								改造								VLAN の有無															

次の表は、フル ホスト プロファイル 5.1.1 レコードのコンポーネントについての説明です。

表 B-50 フルホストプロファイルレコード5.1.1のフィールド

フィールド	データタイプ	説明
[IP アドレス (IP Address)]	uint8[4]	IP アドレス オクテットの、ホストの IP アドレス。
ホップ	uint8	ホストからデバイスへのネットワーク ホップ数。
汎用リストブロック タイプ	uint32	ホストの既存のフィンガープリントから取得したフィンガープリント データを送送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システムから取得したフィンガープリント データ ブロック*	変数 (variable)	ホストの既存のフィンガープリントから取得したホストでのオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> を参照してください。
汎用リストブロック タイプ	uint32	サーバフィンガープリントを使用して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 (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、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> を参照してください。

表 B-50 フルホストプロファイルレコード5.1.1のフィールド(続き)

フィールド	データタイプ	説明
汎用リストブロックタイプ	uint32	クライアントフィンガープリントを使用して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(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、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(VDB)ネイティブフィンガープリント1)データブロック*	変数(variable)	シスコ脆弱性データベース(VDB)のフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(VDB)ネイティブフィンガープリント2)データブロック*	変数(variable)	シスコ脆弱性データベース(VDB)のフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。

表 B-50 フルホストプロファイルレコード5.1.1のフィールド(続き)

フィールド	データタイプ	説明
汎用リストブロックタイプ	uint32	ユーザが追加したフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント(ユーザ フィンガープリント)データ ブロック*	変数 (variable)	ユーザが追加したホストのオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	脆弱性スキャナによって追加されたフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント(スキャン フィンガープリント)データ ブロック*	変数 (variable)	脆弱性スキャナによって追加されたホストのオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	アプリケーションによって追加されたフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント(アプリケーション フィンガープリント)データ ブロック*	変数 (variable)	アプリケーションによって追加されたホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> を参照してください。

表 B-50 フルホストプロファイルレコード5.1.1のフィールド(続き)

フィールド	データタイプ	説明
汎用リストブロックタイプ	uint32	フィンガープリント競合解決から選択したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(競合フィンガープリント)データブロック*	変数(variable)	フィンガープリント競合解決から選択したホストのオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
リストブロックタイプ	uint32	TCP サービスデータを伝送する全サーバデータブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リストブロックタイプフィールド、リストブロック長フィールド、すべてのカプセル化全サーバデータブロック長から成る 8 バイトを含みます。
(TCP)全サーバデータブロック*	変数(variable)	ホストで TCP サービスに関するデータを伝送する全サーバデータブロックのリスト。このデータブロックの説明の詳細については、 <a href="#">フルホストサーバデータブロック 4.10.0+(4-146 ページ)</a> を参照してください。
リストブロックタイプ	uint32	UDP サービスデータを伝送する全サーバデータブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リストブロックタイプフィールド、リストブロック長フィールド、すべてのカプセル化全サーバデータブロック長から成る 8 バイトを含みます。
(UDP)全サーバデータブロック*	変数(variable)	ホストで UDP サブサービスに関するデータを伝送する全サーバデータブロックのリスト。このデータブロックの説明の詳細については、 <a href="#">フルホストサーバデータブロック 4.10.0+(4-146 ページ)</a> を参照してください。
リストブロックタイプ	uint32	ネットワークプロトコルデータを伝えるプロトコルデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リストブロックタイプフィールド、リストブロック長フィールド、すべてのカプセル化プロトコルデータブロック長から成る 8 バイトを含みます。
(ネットワーク)プロトコルデータブロック*	変数(variable)	ホストでネットワークプロトコルに関するデータを伝送するプロトコルデータブロックのリスト。このデータブロックの説明の詳細については、 <a href="#">プロトコルデータブロック (4-78 ページ)</a> を参照してください。

表 B-50 フルホストプロファイルレコード5.1.1のフィールド(続き)

フィールド	データタイプ	説明
リストブロックタイプ	uint32	トランスポート プロトコル データを伝えるプロトコル データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック 長	uint32	リスト内のバイト数。この数値には、リスト ブロック タイプ フィールド、リスト ブロック 長 フィールド、すべてのカプセル化 プロトコル データ ブロック 長 から成る 8 バイトを含みます。
(トランスポート)プロトコル データ ブロック*	変数 (variable)	ホストでトランスポート プロトコルに関するデータを伝送するプロトコル データ ブロックのリスト。このデータ ブロックの説明の詳細については、 <a href="#">プロトコル データ ブロック (4-78 ページ)</a> を参照してください。
リストブロックタイプ	uint32	ホスト MAC アドレス データ ブロックを含むリスト データ ブロックを表示します。この値は常に 11 です。
リスト ブロック 長	uint32	リスト ヘッダーやすべてのカプセル化ホスト MAC アドレス データ ブロックを含むリストのバイト数。
ホスト MAC アドレス データ ブロック*	変数 (variable)	ホスト MAC アドレス データ ブロックのリスト。このデータ ブロックの詳細については、 <a href="#">ホスト MAC アドレス 4.9+(4-119 ページ)</a> を参照してください。
最後の確認日時	uint32	システムがホスト アクティビティを検出した前回時刻を表す UNIX タイムスタンプ。
ホスト タイプ	uint32	ホストのタイプを示します。次の値を指定します。 <ul style="list-style-type: none"> <li>• 0 — ホスト</li> <li>• 1: ルータ</li> <li>• 2 — ブリッジ</li> <li>• 3 — NAT(ネットワーク アドレス変換デバイス)</li> <li>• 4 — LB(ロード バランサー)</li> </ul>
ビジネス上の重要度	uint16	ビジネスに対するホストの重要度を示します。
VLAN ID (Admin. VLAN ID)	uint16	ホストがメンバーである 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 タグに含まれるプライオリティ値。
汎用リスト ブロック タイプ	uint32	クライアント アプリケーション データを伝送するホスト脆弱性 データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック 長	uint32	リスト ヘッダーやすべてのカプセル化クライアント アプリケーション データ ブロックを含む汎用リスト データ ブロック内のバイト数。

表 B-50 フルホスト プロファイル レコード 5.1.1 のフィールド(続き)

フィールド	データ タイプ	説明
全ホスト クライアント アプリケーション データ ブロック*	変数 (variable)	クライアント アプリケーション データ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、 <a href="#">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+(4-159 ページ)</a> 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。
文字列ブロック タイプ	uint32	ホストの注記の文字列データ ブロックを表示します。この値は常に 0 です。
文字列ブロック 長	uint32	文字列ブロック タイプ フィールドおよび文字列ブロック 長 フィールドの 8 バイトを含む注記文字列データ ブロックのバイト数および注記文字列のバイト数。
注記(Notes)	string	ホストの注記ホスト属性の内容を含みます。
汎用リスト ブロック タイプ	uint32	VDB 脆弱性データを伝送するホスト脆弱性データ ブロックを含む汎用リストデータ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック 長	uint32	リスト ヘッダーやすべてのカプセル化データ ブロックを含む汎用リストデータ ブロック内のバイト数。
(VDB)ホスト脆弱性データ ブロック*	変数 (variable)	シスコ 脆弱性データベース (VDB) で特定された脆弱性に関するホスト脆弱性データ ブロックのリスト。このデータ ブロックの説明の詳細については、 <a href="#">ホスト脆弱性データ ブロック 4.9.0+(4-116 ページ)</a> を参照してください。
汎用リスト ブロック タイプ	uint32	サードパーティ スキャン脆弱性データを伝送するホスト脆弱性データ ブロックを含む汎用リストデータ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック 長	uint32	リスト ヘッダーやすべてのカプセル化データ ブロックを含む汎用リストデータ ブロック内のバイト数。
(サードパーティ/VDB)ホスト脆弱性データ ブロック*	変数 (variable)	サードパーティのスキナから送信され、シスコ 脆弱性データベース (VDB) でカタログされているホストの脆弱性に関する情報を含むホスト脆弱性データ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">ホスト脆弱性データ ブロック 4.9.0+(4-116 ページ)</a> を参照してください。
汎用リスト ブロック タイプ	uint32	サードパーティ スキャン脆弱性データを伝送するホスト脆弱性データ ブロックを含む汎用リストデータ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック 長	uint32	リスト ヘッダーやすべてのカプセル化データ ブロックを含む汎用リストデータ ブロック内のバイト数。



表 B-50 フルホストプロファイルレコード5.1.1のフィールド(続き)

フィールド	データタイプ	説明
(サードパーティスキャン)ホスト脆弱性データブロック*	変数 (variable)	サードパーティのスキャナから送信されたホスト脆弱性データブロック。これらのデータブロックのホスト脆弱性 ID は、サードパーティのスキャナ ID であり、シスコによって検出された ID ではない点にご注意ください。このデータブロックの説明の詳細については、 <a href="#">ホスト脆弱性データブロック 4.9.0+(4-116 ページ)</a> を参照してください。
リストブロックタイプ	uint32	属性データを伝送する属性値データブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リストヘッダーやすべてのカプセル化データブロックを含むリストデータブロック内のバイト数。
属性値データブロック*	変数 (variable)	属性値データブロックのリスト。このリストのデータブロックの詳細については、 <a href="#">属性値データブロック (4-84 ページ)</a> を参照してください。
Mobile	uint8	オペレーティングシステムがモバイルデバイスで動作しているかどうかを示す true/false フラグ。
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。
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"> <li>0:はい</li> <li>1:いいえ</li> </ul>

## フルホストプロファイルデータブロック 5.2.x

フルホストプロファイルデータブロックバージョン 5.2.x には、1つのホストを記述するフルセットのデータが含まれています。このデータセットの形式を次の図に示し、次表で説明します。図には、リストデータブロックを除き、カプセル化データブロックフィールドを提示していない点にご注意ください。これらのカプセル化データブロックは、[検出と接続データ構造の概要 \(4-1 ページ\)](#)で別途説明します。フルホストプロファイルデータブロックのブロックタイプ値は、140 です。これは以前のバージョン(ブロックタイプが 135 である)に取って代わります。



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

バイト	0							1							2							3																		
ビット	0	1	2	3	4	5	6	7	8	9	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
フルホストプロファイルデータブロック (140)																																								
データブロック長																																								

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

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
クライアントフィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ (130)*																															
	オペレーティング システム フィンガープリント ブロック 長																															
	オペレーティング システム クライアント フィンガープリント データ...																															
	汎用リスト ブロック タイプ (31)																															
	汎用リスト ブロック 長																															
VDB ネイティブフィンガープリント 1	オペレーティング システム フィンガープリント ブロック タイプ (130)*																															
	オペレーティング システム フィンガープリント ブロック 長																															
	オペレーティング システム VDB フィンガープリント データ...																															
	汎用リスト ブロック タイプ (31)																															
	汎用リスト ブロック 長																															
VDB ネイティブフィンガープリント 2	オペレーティング システム フィンガープリント ブロック タイプ (130)*																															
	オペレーティング システム フィンガープリント ブロック 長																															
	オペレーティング システム VDB フィンガープリント データ...																															
	汎用リスト ブロック タイプ (31)																															
	汎用リスト ブロック 長																															
ユーザ (User) フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ (130)*																															
	オペレーティング システム フィンガープリント ブロック 長																															
	オペレーティング システム ユーザ フィンガープリント データ...																															
	汎用リスト ブロック タイプ (31)																															
	汎用リスト ブロック 長																															
スキャン (Scan) フィンガープリント	オペレーティング システム フィンガープリント ブロック タイプ (130)*																															
	オペレーティング システム フィンガープリント ブロック 長																															
	オペレーティング システム スキャン フィンガープリント データ...																															
	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																															
Application フィンガー プリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムアプリケーションフィンガープリントデータ...																															
	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
競合 フィンガー プリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステム競合フィンガープリントデータ...																															
	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
Mobile フィンガー プリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムモバイルフィンガープリントデータ...																															
	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
IPv6 サーバ フィンガー プリント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムIPv6サーバフィンガープリントデータ...																															
	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
Ipv6 クラ イアント フィン ガープリ ント	オペレーティングシステムフィンガープリントブロックタイプ(130)*																															
	オペレーティングシステムフィンガープリントブロック長																															
	オペレーティングシステムIpv6クライアントフィンガープリントデータ...																															

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MAC アドレス データ	リストブロック タイプ (11)																															
	リストブロック長																															
	ホスト MAC アドレス データ ブロック (95)*																															
	Last Seen																															
	ホスト タイプ																															
	ビジネス上の重要度																VLAN ID (Admin. VLAN ID)															
	VLAN タイプ								VLAN 優先順位								汎用リストブロック タイプ (31)															
ホストクラ イアント データ	汎用リストブロック タイプ (続き)																汎用リストブロック長															
	汎用リストブロック長 (続き)																全ホストクライアントアプリケーションデータブロック (112)*															
NetBIOS 名  [名前 (Name) ]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	NetBIOS 名文字列																															
注記 (Notes) データ	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	Notes 文字列...																															
(VDB)ホス ト Vulns	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	(VDB)ホスト脆弱性データ ブロック (85)*																															
(サードパー ティ/VDB) Host Vulns	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	(サードパーティ/VDB)ホスト脆弱性データ ブロック (85)*																															
サードパー ティ スキャン Host Vulns	汎用リストブロック タイプ (31)																															
	汎用リストブロック長																															
	(サードパーティ スキャン)元の Vuln ID によるホスト脆弱性データ ブロック (85)*																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
属性 (Attribute) 値データ	リストブロック タイプ(11)																															
	リストブロック長																															
	属性値データ ブロック*																															
	Mobile																改造															

次の表は、フル ホスト プロファイル 5.2.x レコードのコンポーネントについての説明です。

表 B-51 フルホストプロファイルレコード5.2.x のフィールド

フィールド	データタイプ	説明
ホスト ID (Host ID)	uint8[16]	ホストの一意の ID 番号。これは UUID です。
リストブロックタイプ	uint32	TCP サービスデータを伝送する IP アドレス データ ブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リストブロックタイプフィールド、リストブロック長フィールド、すべてのカプセル化 IP アドレス データ ブロック長から成る 8 バイトを含みます。
[IP アドレス (IP Address)]	変数 (variable)	ホストの IP アドレスおよび各 IP アドレスが最後に表示されたときの IP アドレス。このデータブロックの詳細については、 <a href="#">ホスト IP アドレス データ ブロック (4-100 ページ)</a> を参照してください。
ホップ	uint8	ホストからデバイスへのネットワーク ホップ数。
汎用リストブロックタイプ	uint32	ホストの既存のフィンガープリントから取得したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムから取得したフィンガープリントデータブロック*	変数 (variable)	ホストの既存のフィンガープリントから取得したホストでのオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	サーバフィンガープリントを使用して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 B-51 フルホスト プロファイル レコード 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
汎用リスト ブロック長	uint32	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、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> を参照してください。
汎用リスト ブロック タイプ	uint32	クライアント フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	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、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> を参照してください。
汎用リスト ブロック タイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリント データを送信するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント (VDB) ネイティブ フィンガープリント 1) データ ブロック*	変数 (variable)	シスコ 脆弱性データベース (VDB) のフィンガープリントを使用して特定したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> を参照してください。
汎用リスト ブロック タイプ	uint32	シスコ VDB フィンガープリントを使用して特定したフィンガープリント データを送信するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。



表 B-51 フルホストプロファイルレコード5.2.x のフィールド(続き)

フィールド	データタイプ	説明
オペレーティングシステムフィンガープリント(VDB)ネイティブフィンガープリント2)データブロック*	変数(variable)	シスコ 脆弱性データベース(VDB)のフィンガープリントを使用して特定したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	ユーザが追加したフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(ユーザフィンガープリント)データブロック*	変数(variable)	ユーザが追加したホストのオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	脆弱性スキャナによって追加されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(スキャンフィンガープリント)データブロック*	変数(variable)	脆弱性スキャナによって追加されたホストのオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	アプリケーションによって追加されたフィンガープリントデータを伝送するオペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。

表 B-51 フルホスト プロファイル レコード 5.2.x のフィールド(続き)

フィールド	データ タイプ	説明
オペレーティング システム フィンガープリント(アプリケーション フィンガープリント)データ ブロック*	変数 (variable)	アプリケーションによって追加されたホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリントデータ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> を参照してください。
汎用リスト ブロック タイプ	uint32	フィンガープリント競合解決から選択したフィンガープリント データを伝送するオペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックを表示します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント(競合フィンガープリント)データ ブロック*	変数 (variable)	フィンガープリント競合解決から選択したホストのオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> を参照してください。
汎用リスト ブロック タイプ	uint32	モバイル デバイス フィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。
オペレーティング システム フィンガープリント(モバイル)データ ブロック*	変数 (variable)	モバイル デバイス ホストのオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> 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。
汎用リスト ブロック長	uint32	リスト ヘッダーやすべてのカプセル化オペレーティング システム フィンガープリント データ ブロックを含む汎用リスト データ ブロックのバイト数。

表 B-51 フルホストプロファイルレコード5.2.xのフィールド(続き)

フィールド	データタイプ	説明
オペレーティングシステムフィンガープリント(IPv6サーバフィンガープリント)データブロック*	変数(variable)	IPv6サーバフィンガープリントを使用して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、 <a href="#">オペレー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+(4-166 ページ)</a> 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	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(IPv6クライアントフィンガープリント)データブロック*	変数(variable)	IPv6クライアントフィンガープリントで識別したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	IPv6 DHCP フィンガープリントで識別するフィンガープリントデータを搬送するオペレーティングシステムフィンガープリントデータブロックで構成される汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。
オペレーティングシステムフィンガープリント(IPv6 DHCP)データブロック*	変数(variable)	IPv6 DHCP フィンガープリントで識別したホスト上のオペレーティングシステムに関する情報を含むオペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	ユーザエージェントフィンガープリントで識別するフィンガープリントデータを搬送するオペレーティングシステムフィンガープリントデータブロックで構成される汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化オペレーティングシステムフィンガープリントデータブロックを含む汎用リストデータブロックのバイト数。

表 B-51 フルホスト プロファイル レコード 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
オペレーティングシステムフィンガープリント(ユーザエージェント)データブロック*	変数 (variable)	ユーザ エージェント フィンガープリントで識別したホスト上のオペレーティング システムに関する情報を含むオペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> を参照してください。
リストブロックタイプ	uint32	TCP サービス データを伝送する全サーバ データ ブロックを含むリスト データ ブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リスト ブロック タイプ フィールド、リスト ブロック 長 フィールド、すべてのカプセル化全サーバ データ ブロック 長から成る 8 バイトを含みます。
(TCP)全サーバ データ ブロック*	変数 (variable)	ホストで TCP サービスに関するデータを伝送する全サーバ データ ブロックのリスト。このデータ ブロックの説明の詳細については、 <a href="#">フルホスト サーバ データ ブロック 4.10.0+(4-146 ページ)</a> を参照してください。
リストブロックタイプ	uint32	UDP サービス データを伝送する全サーバ データ ブロックを含むリスト データ ブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リスト ブロック タイプ フィールド、リスト ブロック 長 フィールド、すべてのカプセル化全サーバ データ ブロック 長から成る 8 バイトを含みます。
(UDP)全サーバ データ ブロック*	変数 (variable)	ホストで UDP サブサービスに関するデータを伝送する全サーバ データ ブロックのリスト。このデータ ブロックの説明の詳細については、 <a href="#">フルホスト サーバ データ ブロック 4.10.0+(4-146 ページ)</a> を参照してください。
リストブロックタイプ	uint32	ネットワーク プロトコル データを伝えるプロトコル データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リスト ブロック タイプ フィールド、リスト ブロック 長 フィールド、すべてのカプセル化プロトコル データ ブロック 長から成る 8 バイトを含みます。
(ネットワーク)プロトコル データ ブロック*	変数 (variable)	ホストでネットワーク プロトコルに関するデータを伝送するプロトコル データ ブロックのリスト。このデータ ブロックの説明の詳細については、 <a href="#">プロトコル データ ブロック (4-78 ページ)</a> を参照してください。
リストブロックタイプ	uint32	トランスポート プロトコル データを伝えるプロトコル データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値には、リスト ブロック タイプ フィールド、リスト ブロック 長 フィールド、すべてのカプセル化プロトコル データ ブロック 長から成る 8 バイトを含みます。

表 B-51 フルホストプロファイルレコード 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
(トランスポート)プロトコルデータブロック*	変数 (variable)	ホストでトランスポートプロトコルに関するデータを伝送するプロトコルデータブロックのリスト。このデータブロックの説明の詳細については、 <a href="#">プロトコルデータブロック (4-78 ページ)</a> を参照してください。
リストブロックタイプ	uint32	ホスト MAC アドレス データ ブロックを含むリスト データ ブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リストヘッダーやすべてのカプセル化ホスト MAC アドレス データ ブロックを含むリストのバイト数。
ホスト MAC アドレス データ ブロック*	変数 (variable)	ホスト MAC アドレス データ ブロックのリスト。このデータブロックの詳細については、 <a href="#">ホスト MAC アドレス 4.9+(4-119 ページ)</a> を参照してください。
最後の確認日時	uint32	システムがホスト アクティビティを検出した前回時刻を表す UNIX タイムスタンプ。
ホストタイプ	uint32	ホストのタイプを示します。次の値を指定します。 <ul style="list-style-type: none"> <li>• 0 — ホスト</li> <li>• 1: ルータ</li> <li>• 2 — ブリッジ</li> <li>• 3 — NAT (ネットワーク アドレス変換デバイス)</li> <li>• 4 — LB (ロード バランサー)</li> </ul>
ビジネス上の重要度	uint16	ビジネスに対するホストの重要度を示します。
VLAN ID (Admin. VLAN ID)	uint16	ホストがメンバーである 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 タグに含まれるプライオリティ値。
汎用リストブロックタイプ	uint32	クライアントアプリケーション データを伝える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	リストヘッダーやすべてのカプセル化クライアントアプリケーションデータブロックを含む汎用リストデータブロック内のバイト数。
全ホストクライアントアプリケーションデータブロック*	変数 (variable)	クライアントアプリケーションデータ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、 <a href="#">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+(4-159 ページ)</a> 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)。

表 B-51 フルホスト プロファイル レコード 5.2.x のフィールド(続き)

フィールド	データタイプ	説明
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
文字列ブロックタイプ	uint32	ホストの注記の文字列データブロックを表示します。この値は常に 0 です。
文字列ブロック長	uint32	文字列ブロックタイプフィールドおよび文字列ブロック長フィールドの 8 バイトを含む注記文字列データブロックのバイト数および注記文字列のバイト数。
注記(Notes)	string	ホストの注記ホスト属性の内容を含みます。
汎用リストブロックタイプ	uint32	VDB 脆弱性データを伝送するホスト脆弱性データブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化データブロックを含む汎用リストデータブロック内のバイト数。
(VDB)ホスト脆弱性データブロック*	変数(variable)	シスコ脆弱性データベース(VDB)で特定された脆弱性に関するホスト脆弱性データブロックのリスト。このデータブロックの説明の詳細については、 <a href="#">ホスト脆弱性データブロック 4.9.0+(4-116 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	サードパーティ スキャン脆弱性データを伝送するホスト脆弱性データブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化データブロックを含む汎用リストデータブロック内のバイト数。
(サードパーティ/VDB)ホスト脆弱性データブロック*	変数(variable)	サードパーティのスキナから送信され、シスコ脆弱性データベース(VDB)でカタログされているホストの脆弱性に関する情報を含むホスト脆弱性データブロック。このデータブロックの説明の詳細については、 <a href="#">ホスト脆弱性データブロック 4.9.0+(4-116 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	サードパーティ スキャン脆弱性データを伝送するホスト脆弱性データブロックを含む汎用リストデータブロックを表示します。この値は常に 31 です。
汎用リストブロック長	uint32	リストヘッダーやすべてのカプセル化データブロックを含む汎用リストデータブロック内のバイト数。
(サードパーティ スキャン)ホスト脆弱性データブロック*	変数(variable)	サードパーティのスキナから送信されたホスト脆弱性データブロック。これらのデータブロックのホスト脆弱性 ID は、サードパーティのスキナ ID であり、シスコによって検出された ID ではない点にご注意ください。このデータブロックの説明の詳細については、 <a href="#">ホスト脆弱性データブロック 4.9.0+(4-116 ページ)</a> を参照してください。
リストブロックタイプ	uint32	属性データを伝送する属性値データブロックを含むリストデータブロックを表示します。この値は常に 11 です。
リストブロック長	uint32	リストヘッダーやすべてのカプセル化データブロックを含むリストデータブロック内のバイト数。

表 B-51 フルホストプロファイルレコード5.2.xのフィールド(続き)

フィールド	データタイプ	説明
属性値データブロック*	変数 (variable)	属性値データブロックのリスト。このリストのデータブロックの詳細については、 <a href="#">属性値データブロック (4-84 ページ)</a> を参照してください。
Mobile	uint8	オペレーティングシステムがモバイルデバイスで動作しているかどうかを示す true/false フラグ。
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。

## ホストプロファイルデータブロック 5.1.x

次の図は、ホストプロファイルデータブロックの形式を示しています。さらに、このデータブロックには、ホスト重要度値が含まれていませんが、VLAN プレゼンス インジケータは含まれています。さらに、このデータブロックは、ホストの NetBIOS 名を伝えることができます。ホストプロファイルデータブロックのブロックタイプは 132 です。



(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	38	39
	ホストプロファイルブロックタイプ(132)																																							
	ホストプロファイルブロック長																																							
	[IP アドレス (IP Address)]																																							
サーバフィンガープリント	ホップ								プライマリ/セカンダリ								汎用リストブロックタイプ(31)																							
	汎用リストブロックタイプ(続き)																				汎用リストブロック長																			
	汎用リストブロック長(続き)																サーバフィンガープリントデータブロック*																							
クライアントフィンガープリント	汎用リストブロックタイプ(31)																																							
	汎用リストブロック長																																							
	クライアントフィンガープリントデータブロック*																																							

レガシー ホスト データ構造

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
SMB フィンガー プリント	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	SMB フィンガープリント データ ブロック*																															
DHCP フィンガー プリント	汎用リストブロック タイプ(31)																															
	汎用リストブロック長																															
	DHCP フィンガープリント データ ブロック*																															
モバイルデ バイス 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																															
	モバイルデバイス フィンガープリント データ ブロック*																															
TCP サーバ ブロック*	リストブロック タイプ(11)																TCP のリス ト サーバ															
	リストブロック長																															
	TCP サーバデータ ブロック																															
UDP サーバ ブロック*	リストブロック タイプ(11)																UDP のリス ト サーバ															
	リストブロック長																															
	UDP サーバデータ ブロック																															
ネットワー クプロトコ ルブロック*	リストブロック タイプ(11)																ネットワー クのリス ト プロトコ ル															
	リストブロック長																															
	ネットワーク プロトコル データ ブロック																															
トランス ポート (Transport) プロトコ ル ブロック*	リストブロック タイプ(11)																トランス ポート リ ストプロ トコ ル															
	リストブロック長																															
	トランスポート プロトコル データ ブロック																															
MAC アドレ ス ブロック*	リストブロック タイプ(11)																MAC のリス ト アドレス															
	リストブロック長																															
	ホスト MAC アドレス データ ブロック																															



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

次の表は、バージョン 5.1.x により返されるホスト プロファイル データ ブロックのフィールドについての説明です。

表 B-52 ホスト プロファイルデータ ブロック 5.1.x のフィールド

フィールド	データタイプ	説明
ホスト プロファイル ブロック タイプ	uint32	ホスト プロファイル データ ブロック 5.1.x を開始します。この値は常に 132 です。
ホスト プロファイル ブロック長	uint32	ホスト プロファイル データ ブロックのバイト数(ホスト プロファイル ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くホスト プロファイル データに含まれるバイト数を含む)。
[IP アドレス (IP Address)]	uint8[4]	IP アドレス オクテットの、プロファイルに記述されているホストの IP アドレス。
ホップ	uint8	ホストからのデバイスまでのホップ数。
プライマリ/セカンダリ	uint8	ホストがそれを検出したデバイスのプライマリまたはセカンダリのどちらのネットワークにあるかを示します。 <ul style="list-style-type: none"> <li>0: ホストはプライマリ ネットワークにあります。</li> <li>1: ホストはセカンダリ ネットワークにあります。</li> </ul>

表 B-52 ホストプロファイルデータブロック 5.1.x のフィールド(続き)

フィールド	データタイプ	説明
汎用リストブロックタイプ	uint32	サーバフィンガープリントを使用して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(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、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	クライアントフィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	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、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。
汎用リストブロックタイプ	uint32	<b>SMB</b> 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)	<b>SMB</b> 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、 <a href="#">オペレー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+(4-166 ページ)</a> を参照してください。

表 B-52 ホスト プロファイル データ ブロック 5.1.x のフィールド (続き)

フィールド	データ タイプ	説明
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、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> を参照してください。
汎用リスト ブロック タイプ	uint32	DHCP フィンガープリントを使用して識別されるフィンガープリント データを伝える、オペレーティング システム フィンガープリント データ ブロックを構成する汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック 長	uint32	汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのオペレーティング システム フィンガープリント データ ブロックを含む)。
オペレーティング システム フィンガープリント (モバイル デバイス フィンガープリント) データ ブロック*	変数 (variable)	モバイル デバイス フィンガープリントを使用して識別されるホスト上のオペレーティング システムに関する情報が含まれている、オペレーティング システム フィンガープリント データ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">オペレーティング システム フィンガープリント データ ブロック 5.1+(4-166 ページ)</a> を参照してください。
リスト ブロック タイプ	uint32	TCP サーバ データを伝えるサーバ データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。
リスト ブロック 長	uint32	リスト内のバイト数。この数値は、リスト ブロック タイプ フィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバ データ ブロックを加えた値です。  このフィールドには、ゼロ以上のサーバ データ ブロックが続きます。
TCP サーバ データ ブロック	変数 (variable)	TCP サーバを記述するホスト サーバ データ ブロック (旧バージョンの製品で説明)。
リスト ブロック タイプ	uint32	UDP サーバ データを伝えるサーバ データ ブロックで構成されたリスト データ ブロックを開始します。この値は常に 11 です。

表 B-52 ホストプロファイルデータブロック 5.1.x のフィールド(続き)

フィールド	データタイプ	説明
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバデータブロックを加えた値です。 このフィールドには、ゼロ以上のサーバデータブロックが続きます。
UDP サーバデータブロック	uint32	UDP サーバを記述するホストサーバデータブロック(旧バージョンの製品で説明)。
リストブロックタイプ	uint32	ネットワークプロトコルデータを伝えるプロトコルデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
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、 <a href="#">プロトコルデータブロック(4-78 ページ)</a> を参照してください。
リストブロックタイプ	uint32	トランスポートプロトコルデータを伝えるプロトコルデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのプロトコルデータブロックを加えた値です。 このフィールドには、ゼロ以上のトランスポートプロトコルデータブロックが続きます。
トランスポートプロトコルデータブロック	uint32	トランスポートプロトコルを記述するプロトコルデータブロック。このデータブロックの説明の詳細については、 <a href="#">プロトコルデータブロック(4-78 ページ)</a> 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、 <a href="#">ホスト MAC アドレス 4.9+(4-119 ページ)</a> 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。

表 B-52 ホスト プロファイル データ ブロック 5.1.x のフィールド (続き)

フィールド	データ タイプ	説明
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"> <li>0: ホスト</li> <li>1: ルータ</li> <li>2: ブリッジ</li> <li>3: NAT デバイス</li> <li>4: LB (ロード バランサ)</li> </ul>
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"> <li>0: はい</li> <li>1: いいえ</li> </ul>
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 タグに含まれるプライオリティ値。
汎用リスト ブロック タイプ	uint32	クライアント アプリケーション データ を伝えるクライアント アプリケーション データ ブロックで構成される汎用リスト データ ブロックを開始します。この値は常に 31 です。
汎用リスト ブロック 長	uint32	汎用リスト データ ブロックのバイト数 (リスト ヘッダーと、カプセル化されたすべてのクライアント アプリケーション データ ブロックを含む)。
クライアント アプリケーション データ ブロック	uint32	クライアント アプリケーション を記述するクライアント アプリケーション データ ブロック。このデータ ブロックの説明の詳細については、 <a href="#">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+(4-159 ページ)</a> を参照してください。
文字列 ブロック タイプ	uint32	NetBIOS 名の文字列 データ ブロックを開始します。この値は文字列 データ を示す 0 に設定されます。
文字列 ブロック 長	uint32	NetBIOS 名 データ ブロックのバイト数を示します (文字列 ブロック タイプ と長さのフィールド用の 8 バイト、および NetBIOS 名のバイト数を含む)。
NetBIOS 文字列 データ	変数	ホスト プロファイル に記述されているホストの NetBIOS 名が含まれます。

## IP 範囲仕様データ ブロック 5.0 ~ 5.1.1.x

IP 範囲仕様データ ブロックは、一定範囲内の IP アドレスを伝えます。IP 範囲仕様データ ブロックは、ユーザ プロトコル、ユーザ クライアント アプリケーション、アドレス指定、ユーザ 製品、ユーザ サーバ、ユーザ ホスト、ユーザ 脆弱性、ユーザ 重要度、およびユーザ 属性値の各データ ブロックで使用されます。IP 範囲仕様データ ブロックのブロック タイプは 61 です。

次の図は、IP 範囲仕様データ ブロックの形式を示しています。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IP 範囲仕様ブロック タイプ (61)																																
IP 範囲仕様ブロック長																																
IP 範囲の開始																																
IP 範囲の終了																																

次の表は、IP 範囲仕様データ ブロックのコンポーネントについての説明です。

表 B-53 IP 範囲仕様データ ブロックのフィールド

フィールド	データ タイプ	説明
IP 範囲仕様データ ブロック タイプ	uint32	IP 範囲仕様データ ブロックを開始します。この値は常に 61 です。
IP 範囲仕様ブロック長	uint32	IP 範囲仕様データ ブロックのバイトの合計数 (IP 範囲仕様ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く IP 範囲仕様データのバイト数を含む)。
IP 範囲仕様の開始	uint32	IP アドレス範囲の開始 IP アドレス。
IP 範囲仕様の終了	uint32	IP アドレス範囲の最終 IP アドレス。

## アクセス コントロール ポリシー ルール理由データ ブロック

eStreamer サービスは、アクセス コントロール ルールのポリシー ルールの理由のデータ ブロックを使用して、アクセス コントロール ポリシー ルール ID に関する情報を表示します。このデータ ブロックは、シリーズ 2 のブロック タイプ 21 です。

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	アクセス コントロール ポリシー ルールの理由のデータ ブロック タイプ(21)																															
	アクセス コントロール ポリシー ルールの理由のデータ ブロックの長さ																															
説明	理由 (Reason)																文字列ブロック タイプ(0)															
	文字列ブロック タイプ(0) (続き)																文字列ブロック長															
	文字列ブロック長(続き)																説明...															

次の表に、アクセス コントロール ポリシー ルール ID のメタデータ ブロックのフィールドの説明を示します。

表 B-54 アクセス コントロール ポリシー ルール理由データ ブロックのフィールド

フィールド	データ タイプ	説明
アクセス コントロール ポリシー ルール理由データ ブロック タイプ	uint32	アクセス コントロール ポリシー ルール理由データ ブロックを開始します。この値は常に 21 です。
アクセス コントロール ポリシー ルールの理由のデータ ブロックの長さ	uint32	アクセス コントロール ポリシー ルール理由データ ブロックのバイトの合計数(アクセス コントロール ポリシー ルール理由データ ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くデータのバイト数を含む)。
理由 (Reason)	uint16	イベントをトリガーしたルールの理由の番号。
文字列ブロック タイプ	uint32	アクセス コントロール ポリシー ルール理由の説明を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	名前の文字列データ ブロックのバイト数です。ブロック タイプとヘッダー フィールドの 8 バイトと説明フィールドのバイト数が含まれます。
説明	string	ルールの理由の説明。

