



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 \(B-50 ページ\)](#)
- [レガシー ディスカバリ データ構造 \(B-92 ページ\)](#)
- [レガシー接続データ構造 \(B-133 ページ\)](#)
- [レガシー関連イベントのデータ構造 \(B-270 ページ\)](#)
- [レガシー ホスト データ構造 \(B-287 ページ\)](#)

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 \(B-38 ページ\)](#)
- [侵入影響アラート データ \(B-47 ページ\)](#)

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)																															
	Device ID																															
	イベント ID (Event ID)																															
	イベント秒																															
	イベント マイクロ秒																															
	ルール ID (シグネチャ ID)																															
	ジェネレータ ID																															
	ルール リビジョン																															
	分類 ID																															
	プライオリティ ID																															
	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															

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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																																
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
Device ID	uint32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 管理対象 Device レコードのメタデータ (3-37 ページ) を参照してください。
イベント ID (Event ID)	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
イベントマイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒(100 万分の 1 秒)単位の増分。
ルール ID (シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した 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。

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
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。
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">• 0:IP• 1:ICMP• 6:TCP• 17:UDP

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

表 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"> 0: ブロックされていない 1: ブロックされた 2: ブロックされた可能性がある (設定では許可されていない)
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID (User ID)	uint32	ユーザの内部 ID 番号 (該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号 (該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号 (該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号 (該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
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)																															
	Device ID																															
	イベント ID (Event ID)																															
	イベント秒																															
	イベント マイクロ秒																															
	ルール ID (シグネチャ ID)																															
	ジェネレータ ID																															
	ルール リビジョン																															
	分類 ID																															
	プライオリティ ID																															
	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	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 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
Device 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、 管理対象 Device レコードのメタデータ (3-37 ページ) を参照してください。
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"> • 0:IP • 1:ICMP • 6:TCP • 17:UDP

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

表 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"> 0: ブロックされていない 1: ブロックされた 2: ブロックされた可能性がある (設定では許可されていない)
MPLS ラベル	uint32	MPLS ラベル。(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	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(34)																															
	ブロック長																															
	Device ID																															
	イベント ID(Event ID)																															
	イベント秒																															
	イベントマイクロ秒																															
	ルール ID(シグネチャ ID)																															
	ジェネレータ ID																															
	ルールリビジョン																															
	分類 ID																															
	プライオリティ ID																															

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

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															

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)。
Device ID	uint32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 管理対象 Device レコードのメタデータ (3-37 ページ) を参照してください。
イベント ID (Event ID)	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
イベントマイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒(100 万分の 1 秒)単位の増分。
ルール ID (シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した 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"> • 0:IP • 1:ICMP • 6:TCP • 17:UDP

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

表 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"> 0: ブロックされていない 1: ブロックされた 2: ブロックされた可能性がある(設定では許可されていない)
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
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																																
Device ID																																
イベント ID (Event ID)																																
イベント秒																																
イベントマイクロ秒																																

バイト	0								1								2								3										
	0	1	2	3	4	5	6	7	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
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)。
Device ID	uint32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 管理対象 Device レコードのメタデータ (3-37 ページ) を参照してください。
イベント ID (Event ID)	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
イベントマイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒(100 万分の 1 秒)単位の増分。
ルール ID (シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した 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"> • 0:IP • 1:ICMP • 6:TCP • 17:UDP

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

表 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"> 0: ブロックされていない 1: ブロックされた 2: ブロックされた可能性がある(設定では許可されていない)
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
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																															
	Device ID																															
	イベント ID (Event ID)																															
	イベント秒																															
	イベントマイクロ秒																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	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)。
Device ID	uint32	管理対象デバイスの検出の ID 番号が含まれます。バージョン 3 または 4 メタデータを要求すると管理対象デバイス名を入手できます。詳細については、 管理対象 Device レコードのメタデータ (3-37 ページ) を参照してください。
イベント ID (Event ID)	uint32	イベント ID 番号。
イベント秒	uint32	イベント検出の UNIX タイムスタンプ(1970 年 1 月 1 日からの秒数)。
イベントマイクロ秒	uint32	イベント検出のタイムスタンプの、マイクロ秒(100 万分の 1 秒)単位の増分。
ルール ID (シグネチャ ID)	uint32	イベントに対応するルールの ID 番号。
ジェネレータ ID	uint32	イベントを生成した 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"> • 0:IP • 1:ICMP • 6:TCP • 17:UDP

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"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。 <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"> (0、不明):00x00000 赤(1、脆弱):xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx オレンジ(2、潜在的に脆弱):00x00111 黄(3、現在は脆弱でない):00x00011 青(4、不明なターゲット):00x00001
影響	uint8	<p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> 1:レッド(脆弱) 2:オレンジ(脆弱の可能性あり) 3:イエロー(現在は脆弱でない) 4:ブルー(不明なターゲット) 5:グレー(不明なインパクト)

表 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"> 0: ブロックされていない 1: ブロックされた 2: ブロックされた可能性がある(設定では許可されていない)
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
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。
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	32	33	34	35	36	37	38	39
	ヘッダーバージョン(1)																メッセージタイプ(4)																							
	メッセージ長																																							
	Netmap ID																レコードタイプ(400)																							
	レコード長																																							
	eStreamer サーバタイムスタンプ(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)																																							
	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															
	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)																															

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、 管理対象 Device レコードのメタデータ (3-37 ページ) を参照してください。
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"> • 0:IP • 1:ICMP • 6:TCP • 17:UDP

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

表 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"> 0: ブロックされていない 1: ブロックされた 2: ブロックされた可能性がある(設定では許可されていない)
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
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	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。

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、 管理対象 Device レコードのメタデータ (3-37 ページ) を参照してください。
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"> • 0:IP • 1:ICMP • 6:TCP • 17:UDP

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

表 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"> 0: ブロックされていない 1: ブロックされた 2: ブロックされた可能性がある(設定では許可されていない)
MPLS ラベル	uint32	MPLS ラベル。
VLAN ID (Admin. VLAN ID)	uint16	パケットの発信元の VLAN の ID を示します。
パッド	uint16	今後使用するために予約されています。
ポリシー UUID	uint8[16]	侵入ポリシーの固有識別子として機能するポリシー ID 番号。
ユーザ ID (User ID)	uint32	ユーザの内部 ID 番号(該当する場合)。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
アクセスコントロールルール ID	uint32	アクセスコントロールルールの固有識別子として機能するルール ID 番号。
アクセスコントロールポリシー UUID	uint8[16]	アクセスコントロールポリシーの固有識別子として機能するポリシー ID 番号。
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	<p>SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「復号しない」 • 2:「ブロックする」 • 3:「リセットでブロック」 • 4:「復号(既知のキー)」 • 5:「復号(置換キー)」 • 6:「復号(Resign)」

表 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 ステータス	uint16	<p>SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
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	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 (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)																																							
	Device 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。 侵入イベントとメタデータのレコードタイプ(3-1 ページ) を参照してください。
侵入影響アラート ブロック長	uint32	侵入の影響アラートのブロックタイプの長さを示します。後続のすべてのデータ、および侵入の影響アラートのブロックタイプと長さの 8 バイトを含みます。
イベント ID (Event ID)	uint32	イベント ID 番号を表示します。
Device ID	uint32	管理対象デバイス ID 番号を表示します。
イベント秒	uint32	イベントが検出された秒(1970年1月1日からの経過秒数)を示します。

表 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"> 0x01 (ビット 0): 送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02 (ビット 1): 送信元または宛先ホストはネットワークマップ内に存在します。 0x04 (ビット 2): 送信元または宛先ホストはイベントのポート上のサーバを実行しているか (TCP または UDP の場合)、IP プロトコルを使用します。 0x08 (ビット 3): イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10 (ビット 4): イベントで検出されたサーバにマップされた脆弱性があります。 0x20 (ビット 5): イベントが原因で、管理対象デバイスがセッションをドロップしました (デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40 (ビット 6): このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80 (ビット 7): イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) <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"> (0、不明): 00x00000 赤 (1、脆弱): xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx (バージョン 5.0+ のみ) オレンジ (2、潜在的に脆弱): 00x0011x 黄 (3、現在は脆弱でない): 00x0001x 青 (4、不明なターゲット): 00x00001
送信元 IP アドレス	uint8[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、 文字列データブロック (4-73 ページ) を参照してください。

表 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\(B-50 ページ\)](#)
- [マルウェアイベント データ ブロック 5.1.1.x\(B-54 ページ\)](#)
- [マルウェアイベント データ ブロック 5.2.x\(B-60 ページ\)](#)
- [マルウェアイベントのデータ ブロック 5.3\(B-67 ページ\)](#)
- [マルウェア イベント データ ブロック 5.3.1\(B-74 ページ\)](#)
- [マルウェア イベント データ ブロック 5.4.x\(B-82 ページ\)](#)

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)																																

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。
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-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	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。
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。

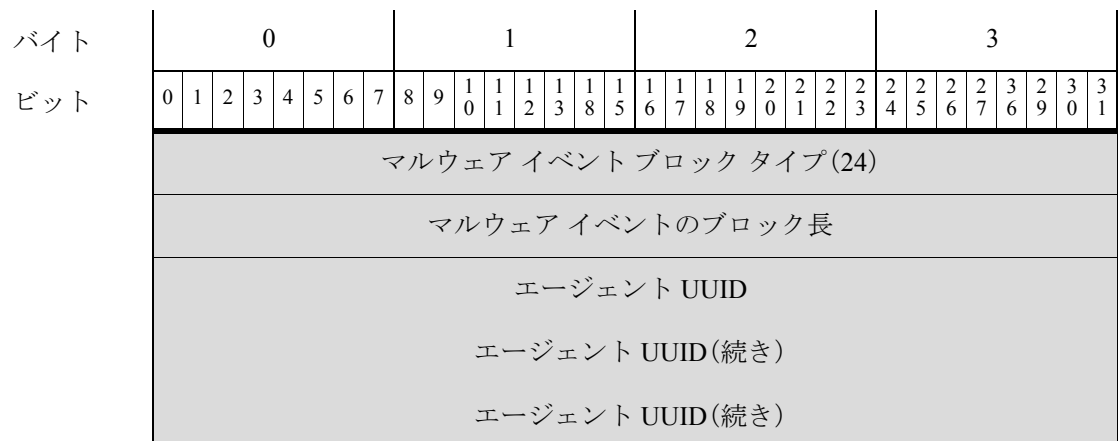
表 B-9 マルウェアイベントデータブロックのフィールド(続き)

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。



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...																															
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(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 アドレス(続き)																								
宛先 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(続き)								宛先 IP アドレス(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)																URI...																							
	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。
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"> • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID(Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
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"> • 1(CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE): ファイルにはマルウェアが含まれています。 • 4(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。 • 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。
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。

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...																															

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
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...																															
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																								

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

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。

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。
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。

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"> 1:ダウンロード 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID(Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
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"> 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 2(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。 3(MALWARE):ファイルにはマルウェアが含まれています。 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。
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。

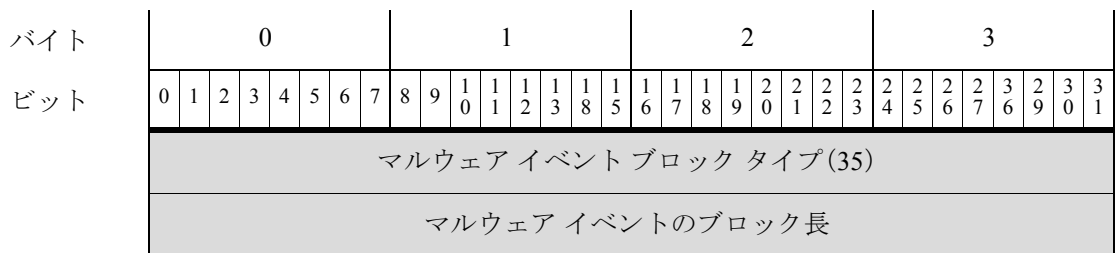
表 B-11 マルウェアイベントデータブロック 5.2.x のフィールド(続き)

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"> • 1:検出 • 2:ブロック • 3:マルウェアクラウドルックアップ • 4:マルウェアブロック • 5:マルウェアホワイトリスト
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"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP 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...																															
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)																																

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							
	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																																							
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)。

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
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、 エンドポイント向け AMP ファイルタイプのメタデータ (3-43 ページ) を参照してください。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
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。
Device ID	uint32	イベントを生成したデバイスの ID。

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
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"> • 1: ダウンロード • 2: アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
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"> • 1 (CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。 • 2 (UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。 • 3 (MALWARE): ファイルにはマルウェアが含まれています。 • 4 (UNAVAILABLE): ソフトウェアから 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。 • 5 (CUSTOM SIGNATURE): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
レトロスペクティブ 特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。

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)。
操作	uint8	ファイルタイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 <ul style="list-style-type: none"> • 1:検出 • 2:ブロック • 3:マルウェアクラウドルックアップ • 4:マルウェアブロック • 5:マルウェアホワイトリスト
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"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ~ 100)。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。

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...																							
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...																															

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
ファイルパス	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイルパス...																															
ファイル SHA ハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	ファイル SHA ハッシュ...																															
	ファイル サイズ (File size)																															
	ファイル タイプ																															
	ファイルのタイムスタンプ																															
親ファイル [名前 (Name)]	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル名...																															
親ファイル SHA ハッシュ	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	親ファイル SHA ハッシュ...																															
イベント 説明	文字列ブロック タイプ(0)																															
	文字列ブロック長																															
	イベントの説明...																															
デバイス ID (Device ID)																																
接続インスタンス																接続数カウンタ																
接続イベント タイムスタンプ																																
方向 (Direction)								送信元 IP アドレス																								
送信元 IP アドレス (続き)																																
送信元 IP アドレス (続き)																																
送信元 IP アドレス (続き)																																

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
	送信元 IP (続き)								宛先 IP アドレス																															
	宛先 IP アドレス (続き)																																							
	宛先 IP アドレス (続き)																																							
	宛先 IP アドレス (続き)																																							
	宛先 IP (続き)								アプリケーション ID (Application ID)																															
	アプリケーション ID (続き)								ユーザ 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)								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。
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。

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	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、 エンドポイント向けAMPファイルタイプのメタデータ(3-43ページ) を参照してください。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時のUNIXタイムスタンプ(1970年1月1日からの経過秒数)。
文字列ブロックタイプ	uint32	親ファイル名を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	親ファイル名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロックタイプ	uint32	親ファイルSHAハッシュを含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	親ファイルSHAハッシュ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、および親ファイルSHAハッシュフィールドのバイト数を含む)。
親ファイルSHAハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルのSHA-256のハッシュ値。
文字列ブロックタイプ	uint32	イベントの説明を含む文字列データブロックを開始します。この値は常に0です。
文字列ブロック長	uint32	イベントの説明文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の8バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベントタイプに関連付けられている追加イベント情報。

表 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
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"> • 1:ダウンロード • 2:アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
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"> • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4(UNAVAILABLE):ソフトウェアから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。 • 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。

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
レトロスペクティブ特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。
文字列ブロックタイプ	uint32	URI を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	URI 文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および URI フィールドのバイト数を含む)。
URI	string	接続の URI。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint 16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	専用 Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
操作	uint8	ファイルタイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 <ul style="list-style-type: none"> • 1:検出 • 2:ブロック • 3:マルウェアクラウドルックアップ • 4:マルウェアブロック • 5:マルウェアホワイトリスト
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"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP これは現時点では TCP のみです。
脅威スコア	uint8	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ~ 100)。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
セキュリティコンテキスト	uint8(16)	トラフィックが通過したセキュリティコンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキストモードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

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 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。

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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 (47)																															
	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 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 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)																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															
	0	1	2	3	4	5	6	7	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																																								
	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															
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。
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)。

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
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、 エンドポイント向け AMP ファイルタイプのメタデータ (3-43 ページ) を参照してください。
ファイルのタイムスタンプ	uint32	検出または検疫されたファイルの作成時の UNIX タイムスタンプ(1970 年 1 月 1 日からの経過秒数)。
文字列ブロックタイプ	uint32	親ファイル名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル名文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および親ファイル名フィールドのバイト数を含む)。
親ファイル名	string	検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。
文字列ブロックタイプ	uint32	親ファイル SHA ハッシュを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	親ファイル SHA ハッシュ文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、および親ファイル SHA ハッシュフィールドのバイト数を含む)。
親ファイル SHA ハッシュ	string	検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。
文字列ブロックタイプ	uint32	イベントの説明を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	イベントの説明文字列データブロックに含まれるバイト数(ブロックタイプとヘッダーフィールド用の 8 バイト、およびイベントの説明フィールドのバイト数を含む)。
イベントの説明	string	イベントタイプに関連付けられている追加イベント情報。
デバイス ID (Device ID)	uint32	イベントを生成したデバイスの ID。

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
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"> 1: ダウンロード 2: アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
送信元 IP アドレス	uint8[16]	接続の送信元の IPv4 または IPv6 アドレス。
宛先 IP アドレス	uint8[16]	接続の宛先の IPv4 または IPv6 アドレス。
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
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"> 1 (CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。 2 (UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。 3 (MALWARE): ファイルにはマルウェアが含まれています。 4 (UNAVAILABLE): ソフトウェアから 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。 5 (CUSTOM SIGNATURE): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
レトロスペクティブ 特性	uint8	特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには特性フィールドと同じ値が格納されます。有効な値は、特性フィールドと同じです。

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	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)。
操作	uint8	ファイルタイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 <ul style="list-style-type: none"> • 1: 検出 • 2: ブロック • 3: マルウェアクラウドルックアップ • 4: マルウェアブロック • 5: マルウェアホワイトリスト • 6: クラウドルックアップのタイムアウト • 7: カスタム検出 • 8: カスタム検出ブロック • 9: アーカイブブロック(深度超過) • 10: アーカイブブロック(暗号化されている) • 11: アーカイブブロック(調査エラー)
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> • 1: ICMP • 4: IP • 6: TCP • 17: UDP これは現時点では TCP のみです。
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。

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

表 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"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
文字列ブロック タイプ	uint32	<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 \(B-92 ページ\)](#)
- [レガシーサーバデータブロック \(B-94 ページ\)](#)
- [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 \(B-95 ページ\)](#)
- [レガシースキャン結果データブロック \(B-97 ページ\)](#)
- [レガシーホストプロファイルデータブロック \(B-123 ページ\)](#)
- [レガシー OS フィンガープリントデータブロック \(B-131 ページ\)](#)

レガシーディスカバリ イベントヘッダー

ディスカバリ イベントヘッダー 5.0 ~ 5.1.1.x

ディスカバリ イベントおよび接続イベントのメッセージには、ディスカバリ イベントヘッダーが含まれます。これは、イベントのタイプおよびサブタイプ、イベントが発生した時刻、イベントが発生したデバイス、およびメッセージ内のイベントデータの構造を伝えます。このヘッダーには、実際のホストディスカバリ、ユーザ、または接続イベントのデータが続きます。さまざまなイベントのタイプ/サブタイプ値に関連付けられる構造の詳細については、[イベントタイプ別ホストディスカバリ構造 \(4-45 ページ\)](#) で説明します。

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	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	Device 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
Device ID	uint32	ディスカバリ イベントを生成したデバイスの ID 番号。バージョン 3 および 4 のメタデータを要求すると、デバイスのメタデータを入手できます。詳細については、 管理対象 Device レコードのメタデータ (3-37 ページ) を参照してください。
[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、 イベント タイプ別ホスト ディスカバリ構造 (4-45 ページ) を参照してください。
イベント サブタイプ	uint32	イベント サブタイプ。使用可能なイベント サブタイプの一覧の詳細については、 イベント タイプ別ホスト ディスカバリ構造 (4-45 ページ) を参照してください。
ファイル番号	byte[4]	シリアル ファイル番号。このフィールドは、シスコ の内部使用のためのものであり、無視してかまいません。
ファイルの位置	byte[4]	シリアル ファイル内のイベントの位置。このフィールドは、シスコ の内部使用のためのものであり、無視してかまいません。

レガシーサーバデータブロック

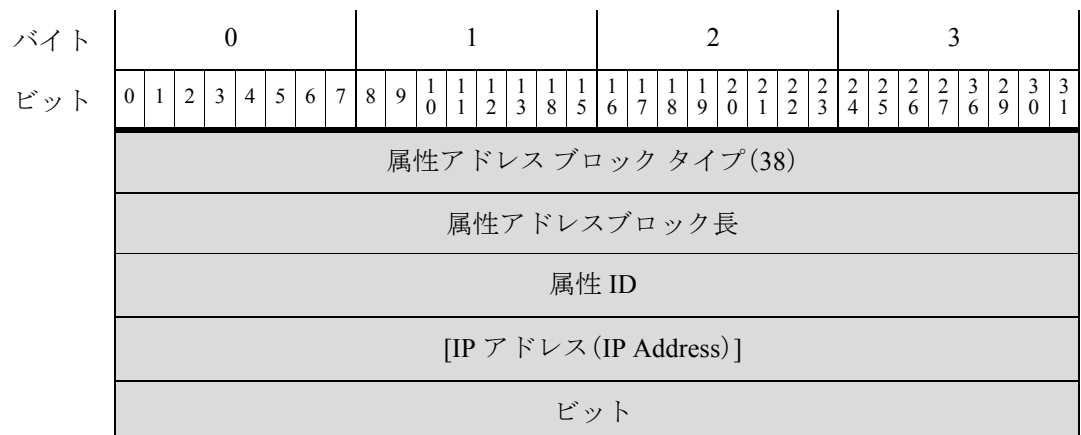
詳細については、次の項を参照してください。

- [属性アドレス データ ブロック 5.0 ~ 5.1.1.x \(B-94 ページ\)](#)

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。



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\(B-95 ページ\)](#)

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	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
	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 0 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、 表 4-58 ユーザサーバデータブロックのフィールド(4-106 ページ) を参照してください。
アプリケーションプロトコル ID	uint32	アプリケーションプロトコルの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	専用クライアントアプリケーションの内部 ID 番号(該当する場合)。
文字列ブロックタイプ	uint32	クライアントアプリケーションバージョンを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	クライアントアプリケーションバージョン文字列データブロックのバイト数(文字列ブロックタイプと長さのフィールド、およびバージョンのバイト数を含む)。
バージョン	string	クライアントアプリケーションバージョン。

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 \(B-97 ページ\)](#)
- [ユーザ製品データ ブロック 5.0.x \(B-99 ページ\)](#)
- [ユーザ情報データ ブロック 5.x \(B-121 ページ\)](#)

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	
	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																
	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																汎用スキャン結果リスト
	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)																																
	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...																																

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
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。
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"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP
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。

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
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。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのユーザ製品データブロックを含む)。
ユーザ製品データブロック*	変数 (variable)	ホスト入力データを含むユーザ製品データブロック。このデータブロックの説明の詳細については、 ユーザ製品データブロック 5.1+(4-176 ページ) を参照してください。

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\(B-204 ページ\)](#)と [ユーザサーバメッセージとオペレーティングシステムメッセージ\(4-59 ページ\)](#)で使用します。ユーザ製品データブロックは、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																															
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																															

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
	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...																															
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...																															

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
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、5.2+ の IP アドレス範囲データ ブロック (4-98 ページ) を参照してください。
[ポート (Port)]	uint16	ユーザが指定するポート。

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
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"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP
ドロップ ユーザ製品	uint32	ユーザ OS 定義がホストから削除されたかどうかを示します: <ul style="list-style-type: none"> • 0:いいえ • 1:はい
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタムベンダー名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタムベンダー文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびベンダー名のバイト数を含む)。
カスタムベンダー名	string	ユーザ入力に指定されたカスタムベンダー名。
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタム製品名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタム製品文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、および製品名のバイト数を含む)。
カスタム製品名	string	ユーザ入力に指定されたカスタム製品名。
文字列ブロックタイプ	uint32	ユーザ入力に指定されたカスタムバージョンを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	カスタムバージョン文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
カスタムバージョン	string	ユーザ入力に指定されたカスタムバージョン。
ソフトウェア ID	uint32	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。

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リビジョン番号を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	メジャー用文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびバージョンのバイト数を含む)。
リビジョン	string	ユーザ入力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。

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	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)。
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)。

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
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、 フィックスリストデータブロック(4-105 ページ) を参照してください。

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。

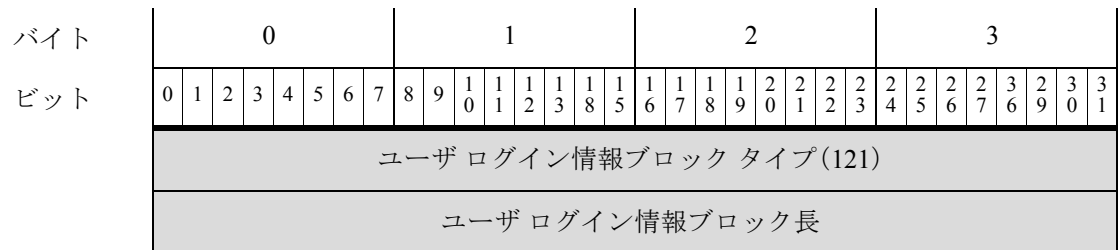
- [ユーザログイン情報データブロック 5.0 ~ 5.0.2\(B-106 ページ\)](#)
- [ユーザログイン情報データブロック 5.1 ~ 5.4.x\(B-108 ページ\)](#)
- [ユーザログイン情報データブロック 6.0.x\(B-110 ページ\)](#)
- [ユーザログイン情報データブロック 6.1.x\(B-114 ページ\)](#)
- [ユーザ情報データブロック 5.x\(B-121 ページ\)](#)

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\(4-63 ページ\)](#)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
	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)。
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。

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)

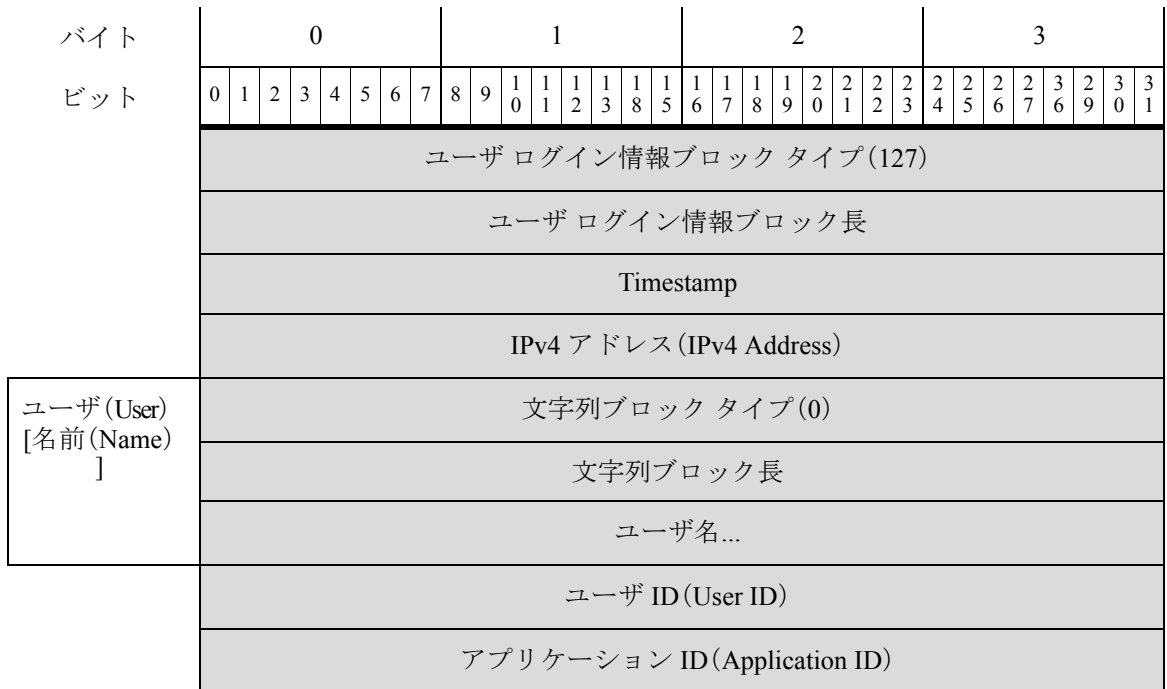
フィールド	データタイプ	説明
アプリケーション ID (Application ID)	uint32	ログイン情報の取得元の、接続に使用されたアプリケーションプロトコルのアプリケーション ID。
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。

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 \(4-185 ページ\)](#)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
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。
IPv4 アドレス (IPv4 Address)	uint32	このフィールドは予約済みですが、設定されておりません。IPv4 アドレスは IPv6 アドレス フィールドに保存されます。詳細については、 IP アドレス(1-5 ページ) を参照してください。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。

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
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 \(4-185 ページ\)](#) 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 \(B-108 ページ\)](#) 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																																

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
	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																															
	ロケーション IPv6 アドレス (続き)																															
	ロケーション IPv6 アドレス (続き)																															
	ロケーション IPv6 アドレス (続き)																															

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

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、 IP アドレス (1-5 ページ) を参照してください。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データブロックのバイト数(ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
文字列ブロック タイプ	uint32	ドメインを含む文字列データブロックを開始します。この値は常に 0 です。
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。

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
セキュリティグループ ID	uint32	ネットワークトラフィックグループの ID 番号。
プロトコル	uint32	ユーザの検出やレポートに使用するプロトコル。値は以下のとおりです。 <ul style="list-style-type: none"> • 165:FTP • 426:SIP • 547:AOL Instant Messenger • 683:IMAP • 710:LDAP • 767:NTP • 773:Oracle データベース • 788:POP3 • 1755:MDNS
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"> • 0:認証は不要 • 1:パッシブ認証、AD エージェント、または ISE セッション • 2:キャプティブポータルの正常な認証 • 3:キャプティブポータルのゲスト認証 • 4:キャプティブポータルの失敗認証
文字列ブロックタイプ	uint32	レポート基準値を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	レポート基準文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびレポート基準フィールドのバイト数を含む)。
レポート基準	string	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 \(B-110 ページ\)](#) 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
	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																															
	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...																															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IPv6 アドレス																																
IPv6 アドレス(続き)																																
IPv6 アドレス(続き)																																
IPv6 アドレス(続き)																																
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、 IP アドレス (1-5 ページ) を参照してください。
文字列ブロック タイプ	uint32	ユーザのユーザ名を含む文字列データ ブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データ ブロックのバイト数 (ブロック タイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。

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
[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。
プロトコル	uint32	ユーザの検出やレポートに使用するプロトコル。値は以下のとおりです。 <ul style="list-style-type: none"> • 165:FTP • 426:SIP • 547:AOL Instant Messenger • 683:IMAP • 710:LDAP • 767:NTP • 773:Oracle データベース • 788:POP3 • 1755:MDNS
[ポート (Port)]	uint16	ユーザを検出したポート番号。
範囲の開始	uint16	TS エージェントが使用するポート範囲の開始ポート
開始ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の開始ポート。
終了ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の最終ポート。
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IPv6 アドレス。

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
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"> 0: 認証は不要 1: パッシブ認証、AD エージェント、または ISE セッション 2: キャプティブポータルでの正常な認証 3: キャプティブポータルでのゲスト認証 4: キャプティブポータルでの失敗認証
文字列ブロックタイプ	uint32	レポート基準値を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	レポート基準文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびレポート基準フィールドのバイト数を含む)。
レポート基準	string	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 \(4-63 ページ\)](#)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 \(B-110 ページ\)](#)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	0	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	3	3	2	3	3	
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)																																			

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...																																
ドメイン	文字列ブロック タイプ (0)																																
	文字列ブロック長																																
	ドメイン...																																
	ユーザ ID (User ID)																																
	レルム ID																																
	エンドポイントプロファイル ID																																
	セキュリティグループ ID																																
	プロトコル																																
	[ポート (Port)]																範囲の開始																
	開始ポート																終了ポート																
	E メール	文字列ブロック タイプ (0)																															
		文字列ブロック長																															
		電子メール...																															
	IPv6 アドレス																																
	IPv6 アドレス (続き)																																
	IPv6 アドレス (続き)																																
	IPv6 アドレス (続き)																																
	ロケーション IPv6 アドレス																																
	ロケーション IPv6 アドレス (続き)																																
	ロケーション IPv6 アドレス (続き)																																
	ロケーション IPv6 アドレス (続き)																																

バイト	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
レポート基準	ログインタイプ								承認タイプ (Type)								文字列ブロックタイプ(0)															
	文字列ブロックタイプ(0) (続き)																文字列ブロック長															
	文字列ブロック長(続き)																レポート基準...															
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す。詳細については、 IP アドレス (1-5 ページ) を参照してください。
文字列ブロックタイプ	uint32	ユーザのユーザ名を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ユーザ名文字列データブロックのバイト数 (ブロックタイプと長さのフィールド用の 8 バイト、およびユーザ名のバイト数を含む)。
[ユーザ名 (Username)]	string	ユーザのユーザ名。
文字列ブロックタイプ	uint32	ドメインを含む文字列データブロックを開始します。この値は常に 0 です。
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-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
レルム ID	uint32	アイデンティティレルムに対応する整数 ID。
エンドポイントプロファイル ID	uint32	接続エンドポイントが使用するデバイスのタイプの ID 番号。この番号は DC ごとに固有であり、メタデータで解決します。
セキュリティグループ ID	uint32	ネットワークトラフィックグループの ID 番号。
プロトコル	uint32	ユーザの検出やレポートに使用するプロトコル。値は以下のとおりです。 <ul style="list-style-type: none"> • 165:FTP • 426:SIP • 547:AOL Instant Messenger • 683:IMAP • 710:LDAP • 767:NTP • 773:Oracle データベース • 788:POP3 • 1755:MDNS
[ポート (Port)]	uint16	ユーザを検出したポート番号。
範囲の開始	uint16	TS エージェントが使用するポート範囲の開始ポート
開始ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の開始ポート。
終了ポート	uint16	TS エージェントが個々のユーザに割り当てられている範囲の最終ポート。
文字列ブロックタイプ	uint32	ユーザの電子メールアドレスを含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	ブロックタイプフィールドと長さフィールドの 8 バイトに電子メールアドレスのバイト数を加えた電子メールアドレス文字列データブロックのバイト数。
E メール	string	ユーザの電子メールアドレス。
IPv6 アドレス	uint8[16]	IP アドレス オクテットの、ユーザのログインが検出されたホストからの IPv6 アドレス。
ロケーション IPv6 アドレス	uint8[16]	ユーザがログインした最新の IP アドレス。IPv4 または IPv6 のどちらかのアドレスになります。
ログインタイプ	uint8	検出されたユーザログインのタイプ。

表 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)

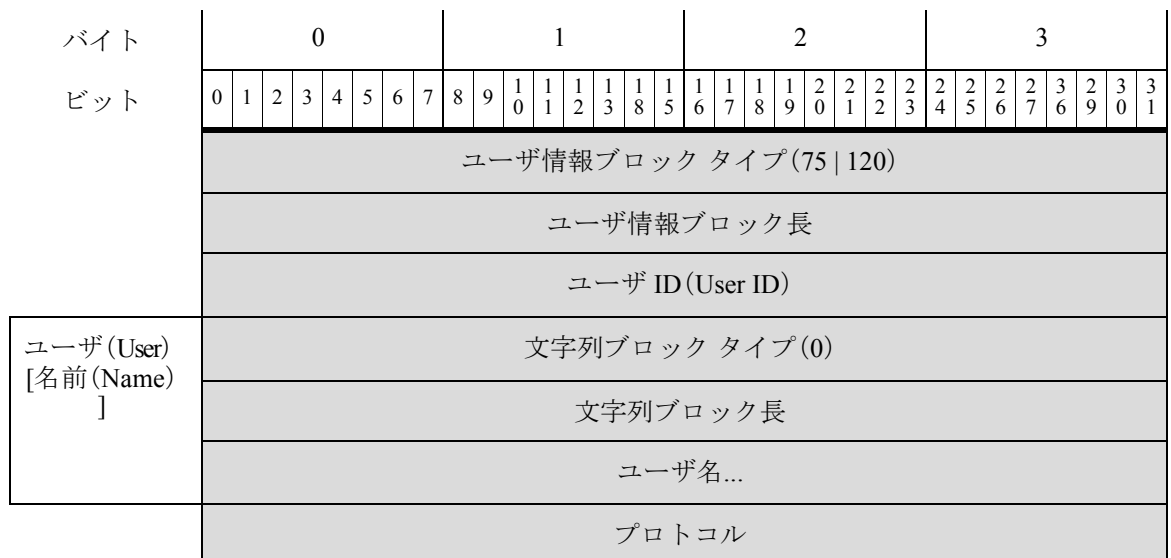
フィールド	データタイプ	説明
認証タイプ (Authentication Type)	uint8	ユーザが使用する認証のタイプ。値は次のとおりです。 <ul style="list-style-type: none"> 0: 認証は不要 1: パッシブ認証、AD エージェント、または ISE セッション 2: キャプティブ ポータルの正常な認証 3: キャプティブ ポータルのゲスト認証 4: キャプティブ ポータルの失敗認証
文字列ブロックタイプ	uint32	レポート基準値を含む文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	レポート基準文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の 8 バイト、およびレポート基準フィールドのバイト数を含む)。
レポート基準	string	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	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ファースト [名前 (Name)]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	名...																															
姓 [名前 (Name)]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	姓...																															
E メール	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	電子メール...																															
部署名 (Department)	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	部署名...																															
電話	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	電話...																															

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。

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。
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 \(B-124 ページ\)](#)

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。

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

バイト	0								1								2								3								
ビット	0	1	2	3	4	5	6	7	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)																															TCP サーバ のリスト	
	リストブロック長																																
TCP 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																																
	TCP サーバデータ...																																
	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...																																

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								
	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アドレスブロックタイプ(95)*																																							
MACアドレスブロック*	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																
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データブロックタイプ	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データブロック長	uint32	ホストプロファイルデータブロックのバイト数(ホストプロファイルデータブロックタイプと長さのフィールド用の 8 バイト、およびそれに続くホストプロファイルデータに含まれるバイト数を含む)。
[IP アドレス (IP Address)]	uint8[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かのネットワークにあるかを示します。 <ul style="list-style-type: none"> 0: ホストはプライマリ ネットワークにあります。 1: ホストはセカンダリ ネットワークにあります。
汎用リストデータブロックタイプ	uint32	サーバフィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストデータブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。
オペレーティングシステムフィンガープリント(サーバフィンガープリント)データブロック*	変数 (variable)	サーバフィンガープリントを使用して識別されるホスト上のオペレーティングシステムに関する情報が含まれている、オペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 オペレーティングシステムフィンガープリントデータブロック 5.0 ~ 5.0.2 (B-131 ページ) を参照してください。
汎用リストデータブロックタイプ	uint32	クライアントフィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストデータブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。
オペレーティングシステムフィンガープリント(クライアントフィンガープリント)データブロック*	変数 (variable)	クライアントフィンガープリントを使用して識別されるホスト上のオペレーティングシステムに関する情報が含まれている、オペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 オペレーティングシステムフィンガープリントデータブロック 5.0 ~ 5.0.2 (B-131 ページ) 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	SMB フィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。
オペレーティングシステムフィンガープリント(SMB フィンガープリント)データブロック*	変数(variable)	SMB フィンガープリントを使用して識別されるホスト上のオペレーティングシステムに関する情報が含まれている、オペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 オペレーティングシステムフィンガープリントデータブロック 5.0 ~ 5.0.2 (B-131 ページ) を参照してください。
汎用リストブロックタイプ	uint32	DHCP フィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。
オペレーティングシステムフィンガープリント(DHCP フィンガープリント)データブロック*	変数(variable)	DHCP フィンガープリントを使用して識別されるホスト上のオペレーティングシステムに関する情報が含まれている、オペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 オペレーティングシステムフィンガープリントデータブロック 5.0 ~ 5.0.2 (B-131 ページ) を参照してください。
リストブロックタイプ	uint32	TCP サーバデータを伝えるサーバデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバデータブロックを加えた値です。 このフィールドには、ゼロ以上のサーバデータブロックが続きます。
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。

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)。
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(プロトコルデータブロック (4-78 ページ) 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)。

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
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(プロトコルデータブロック(4-78 ページ)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)。
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"> • 0:ホスト • 1:ルータ • 2:ブリッジ • 3:NAT デバイス • 4:LB(ロード バランサ)
VLAN の有無	uint8	VLAN が存在するかどうかを示します。 <ul style="list-style-type: none"> • 0:はい • 1:いいえ
VLAN ID (Admin. VLAN ID)	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグにカプセル化されたパケットのタイプ。
VLAN 優先順位	uint8	VLAN タグに含まれるプライオリティ値。
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)。

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
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(4-160 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。
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-131 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																																			

レガシーディスカバリデータ構造

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
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。

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(続き)

フィールド	データタイプ	説明
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\(B-133 ページ\)](#)
- [接続統計データ ブロック 5.1\(B-138 ページ\)](#)
- [接続統計データ ブロック 5.2.x\(B-144 ページ\)](#)
- [接続チャンク データ ブロック 5.0 ~ 5.1\(B-151 ページ\)](#)
- [接続チャンク データ ブロック 5.1.1 ~ 6.0.x\(B-152 ページ\)](#)
- [接続統計データ ブロック 5.1.1.x\(B-154 ページ\)](#)
- [接続統計データ ブロック 5.3\(B-160 ページ\)](#)
- [接続統計データ ブロック 5.3.1\(B-167 ページ\)](#)
- [接続統計データ ブロック 5.4\(B-176 ページ\)](#)
- [接続統計データ ブロック 5.4.1\(B-190 ページ\)](#)
- [接続統計データ ブロック 6.0.x\(B-204 ページ\)](#)
- [接続統計データ ブロック 6.1.x\(B-221 ページ\)](#)

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\(4-55 ページ\)](#)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								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
ビット																																	
	接続データ ブロック タイプ (115)																																
	接続データ ブロック長																																
	Device ID																																
	入力ゾーン 入力ゾーン(続き) 入力ゾーン(続き) 入力ゾーン(続き)																																
	出力ゾーン 出力ゾーン(続き) 出力ゾーン(続き) 出力ゾーン(続き)																																
	入力インターフェイス 入力インターフェイス(続き) 入力インターフェイス(続き) 入力インターフェイス(続き)																																
	出力インターフェイス 出力インターフェイス(続き) 出力インターフェイス(続き) 出力インターフェイス(続き)																																
	イニシエータ IP アドレス イニシエータ IP アドレス(続き) イニシエータ IP アドレス(続き) イニシエータ IP アドレス(続き)																																
	レスポンダ IP アドレス レスポンダ IP アドレス(続き)																																

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

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

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)。
Device ID	uint32	接続イベントを検出したデバイス。

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
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	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。
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。
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。

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
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。

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\(4-55 ページ\)](#)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
	接続データ ブロック タイプ (126)																															
	接続データ ブロック長																															
	Device ID																															
	入力ゾーン 入力ゾーン(続き) 入力ゾーン(続き) 入力ゾーン(続き)																															
	出力ゾーン 出力ゾーン(続き) 出力ゾーン(続き) 出力ゾーン(続き)																															
	入力インターフェイス 入力インターフェイス(続き) 入力インターフェイス(続き) 入力インターフェイス(続き)																															
	出力インターフェイス 出力インターフェイス(続き) 出力インターフェイス(続き) 出力インターフェイス(続き)																															
	イニシエータ IP アドレス イニシエータ IP アドレス(続き) イニシエータ IP アドレス(続き) イニシエータ IP アドレス(続き)																															
	レスポンダ IP アドレス レスポンダ IP アドレス(続き)																															

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

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

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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 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)。
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]	トリガーされた相関イベントに関連付けられている規則のリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーした規則の内部 ID(該当する場合)。
ルールアクション	uint16	その規則に対してユーザ 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規則の理由。
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。

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
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。
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。

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
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。
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。

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-154 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\(4-55 ページ\)](#) 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							
ビット	0	1	2	3	4	5	6	7	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(144)																																
接続データ ブロック長																																
Device ID																																
入力ゾーン																																
入力ゾーン(続き)																																
入力ゾーン(続き)																																
入力ゾーン(続き)																																
出力ゾーン																																
出力ゾーン(続き)																																
出力ゾーン(続き)																																
出力ゾーン(続き)																																
入力インターフェイス																																
入力インターフェイス(続き)																																
入力インターフェイス(続き)																																
入力インターフェイス(続き)																																
出力インターフェイス																																
出力インターフェイス(続き)																																
出力インターフェイス(続き)																																
出力インターフェイス(続き)																																
イニシエータ IP アドレス																																
イニシエータ IP アドレス(続き)																																
イニシエータ IP アドレス(続き)																																
イニシエータ IP アドレス(続き)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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							
	0	1	2	3	4	5	6	7	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																																
	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(続き)																レスポнда Tx Bytes															
	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 ルール 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																															

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)。
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。

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
ポリシー リビジョン	uint8[16]	トリガーされた相関イベントに関連付けられているルールのリビジョン番号(該当する場合)。
ルール ID	uint32	イベントをトリガーしたルールの内部 ID(該当する場合)。
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。
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)。

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 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。
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。

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
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。



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。

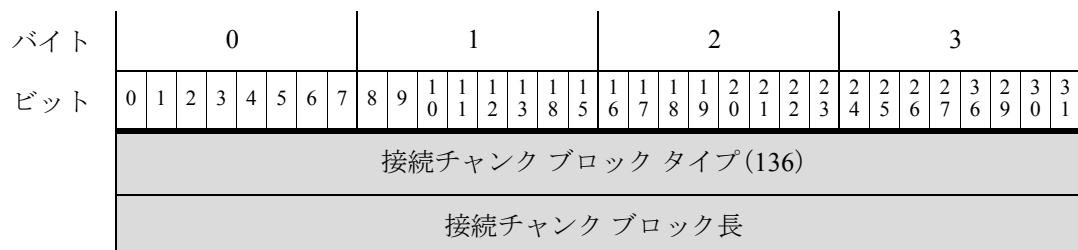
表 B-31 接続チャンク データ ブロックのフィールド

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)。
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 Device 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
	イニシエータ IP アドレス																															
	レスポнда IP アドレス																															
	開始時刻																															
	アプリケーションプロトコル																															
	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 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нда 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нда IP アドレス	uint8(4)	この接続タイプのレスポнда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。

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
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。
NetFlow データ 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 \(B-138 ページ\)](#)) 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 \(4-55 ページ\)](#) 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
接続データ ブロック タイプ (137)																																
接続データ ブロック長																																
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															
	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)																															
	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)																															
	アプリケーションプロトコル ID (続き)																								URL カテゴリ							

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	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...																															
	モニタールール 1																															
	モニタールール 2																															
	モニタールール 3																															
	モニタールール 4																															
	モニタールール 5																															
	モニタールール 6																															
	モニタールール 7																															
	モニタールール 8																															
	秒開始送信元/宛先								秒イニシエータ層								ファイルイベントカウント															
	侵入イベントカウント																															

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)。
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-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
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-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 \(B-144 ページ\)](#)) 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\(4-55 ページ\)](#) 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																																
Device ID																																
入力ゾーン																																
入力ゾーン (続き)																																
入力ゾーン (続き)																																
入力ゾーン (続き)																																
出力ゾーン																																
出力ゾーン (続き)																																
出力ゾーン (続き)																																
出力ゾーン (続き)																																
入力インターフェイス																																
入力インターフェイス (続き)																																
入力インターフェイス (続き)																																
入力インターフェイス (続き)																																
出力インターフェイス																																
出力インターフェイス (続き)																																
出力インターフェイス (続き)																																
出力インターフェイス (続き)																																
イニシエータ IP アドレス																																
イニシエータ IP アドレス (続き)																																
イニシエータ IP アドレス (続き)																																
イニシエータ IP アドレス (続き)																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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)																															
	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															
	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)																															
	クライアントアプリケーション 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)																															
クライアント URL	Web アプリケーション ID(続き)																Web アプリケーション ID															
	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 ルール 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)。
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-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
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。
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。

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
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。
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。

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 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。

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-160 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\(4-55 ページ\)](#)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)																															

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

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

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
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。
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-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
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-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
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。

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
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-167 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(4-55 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	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1				
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)																																			
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)																																
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)																															
	クライアントアプリケーション ID (続き)																								クライアントアプリケーション ID							
	Web アプリケーション 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
クライアント URL	Web アプリケーション ID (続き)																								文字列ブロック タイプ (0)							
	文字列ブロック タイプ (続き)																								文字列ブロック長							
	文字列ブロック長 (続き)																								クライアントア プリケーション URL...							
NetBIOS [名前 (Name)]	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	NetBIOS 名...																															
クライアント アプリケーション バージョン	文字列ブロック タイプ (0)																															
	文字列ブロック長																															
	クライアント アプリケーションバージョン...																															
	モニタ ルール 1																															
	モニタ ルール 2																															
	モニタ ルール 3																															
	モニタ ルール 4																															
	モニタ ルール 5																															
	モニタ ルール 6																															
	モニタ ルール 7																															
	モニタ ルール 8																															
	秒開始送信元/宛先								秒イニシエータ層								ファイル イベント カウント															
	侵入イベント カウント																イニシエータの国															
	レスポндаの国																IOC 番号															
	送信元自律システム																															
	宛先自律システム																															

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

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

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

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。
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)。

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
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。
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)。

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	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。
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。

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
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	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。
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。

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	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、 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
SSL バージョン	uint8	接続の暗号化に使用された SSL または TLS プロトコルバージョン。
SSL サーバ証明書ステータス	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"> 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 1(不明):サーバ証明書のステータスは判別できませんでした。 2(有効):サーバ証明書は有効です。 4(自己署名済み):サーバ証明書は自己署名です。 16(無効な発行者):サーバ証明書に無効な発行者があります。 32(無効な署名):サーバ証明書に無効な署名があります。 64(期限切れ):サーバ証明書は期限切れです。 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 256(取り消し):サーバ証明書は取り消されました。

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

表 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"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブモードで復号不可のセッション」 • 9:「ハンドシェイクエラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL フローエラー	uint32	<p>詳細な SSL エラーコード。これらの値はサポート目的で必要とされる場合があります。</p>

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

表 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 サーバ名	string	SSL Client Hello でサーバ名に指定された名前。
SSL URL カテゴリ	uint32	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできません。
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-167 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 (4-55 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	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
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)																																								

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																																
	入力ゾーン																															
	入力ゾーン(続き)																															
	入力ゾーン(続き)																															
	入力ゾーン(続き)																															
	出力ゾーン																															
	出力ゾーン(続き)																															
	出力ゾーン(続き)																															
	出力ゾーン(続き)																															
	入力インターフェイス																															
	入力インターフェイス(続き)																															
	入力インターフェイス(続き)																															
	入力インターフェイス(続き)																															
	出力インターフェイス																															
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	出力インターフェイス(続き)																															
	イニシエータ IP アドレス																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	イニシエータ IP アドレス(続き)																															
	レスポ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																															

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

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

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

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

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

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。

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
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。
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。

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
レスポンド送信バイト数	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。
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。

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
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。
セキュリティ コンテキスト	uint8(16)	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキストモードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。

表 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
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、 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
SSL バージョン	uint8	接続の暗号化に使用された SSL または TLS プロトコルバージョン。

表 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 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"> 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 1(不明):サーバ証明書のステータスは判別できませんでした。 2(有効):サーバ証明書は有効です。 4(自己署名済み):サーバ証明書は自己署名です。 16(無効な発行者):サーバ証明書に無効な発行者があります。 32(無効な署名):サーバ証明書に無効な署名があります。 64(期限切れ):サーバ証明書は期限切れです。 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 256(取り消し):サーバ証明書は取り消されました。
実際の SSL アクション	uint16	<p>SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> 0:「不明」 1:「復号しない」 2:「ブロックする」 3:「リセットでブロック」 4:「復号(既知のキー)」 5:「復号(置換キー)」 6:「復号(Resign)」
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"> 0:「不明」 1:「復号しない」 2:「ブロックする」 3:「リセットでブロック」 4:「復号(既知のキー)」 5:「復号(置換キー)」 6:「復号(Resign)」

表 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"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL フローエラー	uint32	<p>詳細な SSL エラー コード。これらの値はサポート目的で必要とされる場合があります。</p>

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

表 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 サーバ名	string	SSL Client Hello でサーバ名に指定された名前。
SSL URL カテゴリ	uint32	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
SSL セッション ID	uint8[32]	クライアントとサーバがセッションの再利用に同意する場合に、SSL ハンドシェイク時に使用されるセッション ID の値
SSL セッション ID の長さ	uint8	SSL セッション ID の長さ。セッション ID は 32 バイトより長くすることはできませんが、32 バイト未満にすることはできません。
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-190 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。

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

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

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

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 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...																															
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																															

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

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

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

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
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。
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)。

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
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。
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。

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。
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。

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
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、 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
SSL バージョン	uint8	接続の暗号化に使用されたSSL または TLS プロトコルバージョン。
SSL サーバ証明書ステータス	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"> 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 1(不明):サーバ証明書のステータスは判別できませんでした。 2(有効):サーバ証明書は有効です。 4(自己署名済み):サーバ証明書は自己署名です。 16(無効な発行者):サーバ証明書に無効な発行者があります。 32(無効な署名):サーバ証明書に無効な署名があります。 64(期限切れ):サーバ証明書は期限切れです。 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 256(取り消し):サーバ証明書は取り消されました。

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

表 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"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL フローエラー	uint32	<p>詳細な SSL エラー コード。これらの値はサポート目的で必要とされる場合があります。</p>

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

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

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 \(B-204 ページ\)](#) 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+ \(4-122 ページ\)](#))。

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 \(4-55 ページ\)](#) 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																																

レガシー接続データ構造

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
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)	最初のパケット タイムスタンプ																															
最初のパケット タイムスタンプ (続き)	最終パケット タイムスタンプ																															
最終パケット タイムスタンプ (続き)	イニシエータ送信パケット数																															
	イニシエータ送信パケット数 (続き)																															
イニシエータ送信パケット数 (続き)	レスポнда送信パケット数																															
	レスポнда送信パケット数 (続き)																															
レスポнда送信パケット数 (続き)	イニシエータ送信バイト数																															
	イニシエータ送信バイト数 (続き)																															
イニシエータ送信バイト数 (続き)	レスポнда送信パケット数																															
	レスポнда送信バイト数 (続き)																															
レスポнда送信バイト数 (続き)	イニシエータ パケット ドロップ																															
	イニシエータ パケット ドロップ (続き)																															
イニシエータパケットドロップ (続き)	レスポнда パケット ドロップ																															
	レスポнда パケット ドロップ (続き)																															
レスポндаパケットドロップ (続き)	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)																															

バイト	0							1							2							3																
ビット	0	1	2	3	4	5	6	7	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)																														
	レスポндаバイトドロップ(続き)							QOS 適用インターフェイス																														
	QOS インターフェイス(続き)							QOS 適用インターフェイス(続き)																														
	QOS インターフェイス(続き)							QOS 適用インターフェイス(続き)																														
	QOS インターフェイス(続き)							QOS 適用インターフェイス(続き)																														
	QOS インターフェイス(続き)							QOS ルール ID																														
	QOS ルール ID(続き)							ユーザ ID(User ID)																														
	ユーザ ID(続き)							アプリケーションプロトコル ID																														
	アプリケーションプロトコル ID(続き)							URL カテゴリ																														
	URL カテゴリ(続き)							URL レピュテーション																														
	URL レピュテーション(続き)							クライアントアプリケーション ID																														
	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]	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																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)																

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							
参照ホスト	文字列ブロック タイプ(0)																																						
	文字列ブロック長																																						
	参照ホスト...																																						
ユーザエージェント	文字列ブロック タイプ(0)																																						
	文字列ブロック長																																						
	ユーザ エージェント...																																						
HTTP リファラ	文字列ブロック タイプ(0)																																						
	文字列ブロック長																																						
	HTTP リファラ...																																						
SSL 証明書フィンガープリント																																							
SSL 証明書フィンガープリント(続き)																																							
SSL 証明書フィンガープリント(続き)																																							
SSL 証明書フィンガープリント(続き)																																							
SSL 証明書フィンガープリント(続き)																																							
SSL ポリシー ID																																							
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)							

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	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 フロー ステータス(続き)								SSL フロー エラー																															
	SSL フロー エラー(続き)								SSL フロー メッセージ																															
	SSL フロー メッセージ(続き)								SSL フロー フラグ																															
									SSL フロー フラグ(続き)																															
SSL サーバ名	SSL フロー フラグ(続き)								文字列ブロック タイプ(0)																															
	文字列ブロック タイプ(0)(続き)								文字列ブロック長																															
	文字列ブロック 長(続き)								SSL サーバ名...																															
	SSL URL カテゴリ																																							
	SSL セッション ID																																							
	SSL セッション ID(続き)																																							
	SSL セッション ID(続き)																																							
	SSL セッション ID(続き)																																							
	SSL セッション ID(続き)																																							
	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)																																							

バイト	0								1								2								3																							
ビット	0	1	2	3	4	5	6	7	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 チケット ID (続き)								SSL チケット ID の長さ								ネットワーク分析ポリシー リビジョン																															
	ネットワーク分析ポリシー リビジョン (続き)																ネットワーク分析ポリシー リビジョン (続き)																ネットワーク分析ポリシー リビジョン (続き)															
	ネットワーク分析ポリシー リビジョン (続き)																エンドポイント プロファイル ID																															
	エンドポイント プロファイル ID (続き)																セキュリティ グループ ID																															
	セキュリティ グループ ID (続き)																ロケーション IPv6																															
	ロケーション IPv6 (続き)																ロケーション IPv6 (続き)																ロケーション IPv6 (続き)															
	ロケーション IPv6 (続き)																HTTP レスポンス																															
DNS クエリ (DNS Query)	HTTP レスポンス (続き)																文字列ブロック タイプ (0)																															
	文字列ブロック タイプ (0) (続き)																文字列ブロック長																															
	文字列ブロック長 (続き)																DNS クエリ...																															
	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。
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。
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。

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
インスタンス ID (Instance ID)	uint16	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。
接続数カウンタ	uint16	同じ秒の間に発生する接続イベントを区別するために使用される値。
最初のパケットタイムスタンプ	uint32	セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。
最終パケットタイムスタンプ	uint32	セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。
イニシエータ送信パケット数	uint64	開始ホストからの送信パケット数。
レスポнда送信パケット数	uint64	応答ホストが送信したパケット数。
イニシエータ送信バイト数	uint64	開始ホストからの送信バイト数。
レスポнда送信バイト数	uint64	応答ホストから送信バイト数。
イニシエータパケットドロップ	uint64	レート制限により、セッションイニシエータからドロップしたパケット数。
レスポндаパケットドロップ	uint64	レート制限により、セッションレスポндаからドロップしたパケット数。
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)。

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

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層	uint8	IP ブラックリストに一致した IP 層。
ファイル イベント カウント	uint16	同じ秒で発生するファイル イベントを区別するために使用される値。
侵入 イベント カウント	uint16	同じ秒で発生する侵入 イベントを区別するために使用される値。
イニシエータの国	uint16	開始ホストの国のコード。
レスポンドの国	uint16	応答ホストの国のコード。
クライアントのオリジナル国 (Original Client Country)	uint16	要求を開始したプロキシの背後にあるホストの国コード。
IOC 番号	uint16	このイベントに関連付けられている侵害 ID 番号。
送信元自律システム	uint32	送信元の自律システム番号、起点またはピア。
宛先自律システム	uint32	宛先の自律システム番号、起点またはピア。
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。

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	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、 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
SSL バージョン	uint8	接続の暗号化に使用されたSSL または TLS プロトコルバージョン。
SSL サーバ証明書ステータス	uint32	SSL 証明書のステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> 0(チェックなし):サーバ証明書のステータスは評価されませんでした。 1(不明):サーバ証明書のステータスは判別できませんでした。 2(有効):サーバ証明書は有効です。 4(自己署名済み):サーバ証明書は自己署名です。 16(無効な発行者):サーバ証明書に無効な発行者があります。 32(無効な署名):サーバ証明書に無効な署名があります。 64(期限切れ):サーバ証明書は期限切れです。 128(まだ有効でない):サーバ証明書はまだ有効ではありません。 256(取り消し):サーバ証明書は取り消されました。

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

表 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"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
SSL フローエラー	uint32	<p>詳細な SSL エラー コード。これらの値はサポート目的で必要とされる場合があります。</p>

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

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

表 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

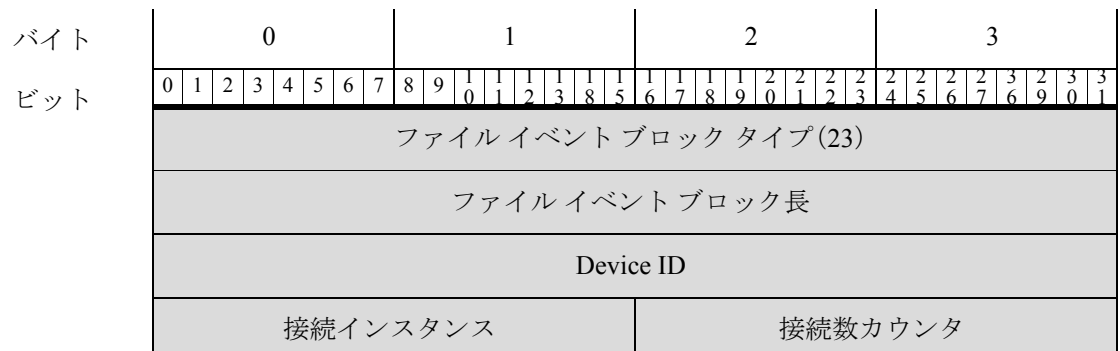
続くいくつかのトピックでは、他のレガシーファイルイベントデータの構造について説明します。

- [ファイルイベント 5.1.1.x \(B-238 ページ\)](#)
- [ファイルイベント 5.2.x \(B-242 ページ\)](#)
- [ファイルイベント 5.3 \(B-247 ページ\)](#)
- [ファイルイベント 5.3.1 \(B-253 ページ\)](#)
- [ファイルイベント 5.4.x \(B-259 ページ\)](#)
- [ファイルイベント SHA ハッシュ 5.1.1 ~ 5.2.x \(B-269 ページ\)](#)

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)																																				
		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)。
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-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"> 1(CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。 2(UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。 3(MALWARE): ファイルにはマルウェアが含まれています。 4(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。 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。
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"> 1: 検出 2: ブロック 3: マルウェアクラウドルックアップ 4: マルウェアブロック 5: マルウェアホワイトリスト
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"> 1: ダウンロード 2: アップロード 現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID (User ID)	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
URI	string	接続の Uniform Resource Identifier (URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> 1: ICMP 4: IP 6: TCP 17: UDP これは現時点では TCP のみです。
アクセス コントロール ポリシー UUID	uint8[16]	イベントをトリガーするアクセス コントロール ポリシーの固有識別子。

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	2	2	2	2	2	2	2	2	2	2	3	2	3	3
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																																					
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									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...																		

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																													
	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)。
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"> 1(CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。 2(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。 3(MALWARE): ファイルにはマルウェアが含まれています。 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。
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"> 1: 検出 2: ブロック 3: マルウェア クラウドルックアップ 4: マルウェア ブロック 5: マルウェア ホワइटリスト

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
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	<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す値。次のいずれかの値になります。</p> <ul style="list-style-type: none"> • 1:ダウンロード • 2:アップロード <p>現時点では、この値はプロトコルに依存しています(たとえば接続が HTTP の場合はダウンロード)。</p>
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	<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"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP <p>これは現時点では TCP のみです。</p>
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。

バイト	0								1								2								3															
ビット	0	1	2	3	4	5	6	7	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
ファイル イベント ブロック タイプ (38)																																								
ファイル イベント ブロック 長																																								
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																			

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							
	0	1	2	3	4	5	6	7	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	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															
	プロトコル								アクセスコントロールポリシー UUID																							

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

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)。
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。

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"> • 1(CLEAN):ファイルはクリーンであり、マルウェアは含まれていません。 • 2(UNKNOWN):ファイルにマルウェアが含まれているかどうかは不明です。 • 3(MALWARE):ファイルにはマルウェアが含まれています。 • 4(UNAVAILABLE):ソフトウェアから 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。 • 5(CUSTOM SIGNATURE):ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
SPERO 解析結果	uint8	<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"> • 1:ファイルが保存されました • 2:ファイルが保存されました • 3:ファイルを保存できません • 4:ファイルを保存できません • 5:ファイルを保存できません • 6:ファイルを保存できません • 7:ファイルを保存できません • 8:ファイル サイズが大きすぎます • 9:ファイル サイズが小さすぎます • 10:ファイルを保存できません • 11:ファイルは保存されておらず、解析結果を入力できません

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"> 0: ファイルが分析のために送信されていません 1: 分析のために送信されました 2: 分析のために送信されました 4: 分析のために送信されました 5: 送信に失敗しました 6: 送信に失敗しました 7: 送信に失敗しました 8: 送信に失敗しました 9: ファイル サイズが小さすぎます 10: ファイル サイズが大きすぎます 11: 分析のために送信されました 12: 分析が完了しました 13: 失敗(ネットワークの問題) 14: 失敗(レート制限) 15: 失敗(ファイルが大きすぎます) 16: 失敗(ファイルの読み取りエラー) 17: 失敗(内部ライブラリ エラー) 19: ファイルは送信されておらず、解析結果を入力できません 20: 失敗(ファイルを実行できません) 21: 失敗(分析タイムアウト) 22: 分析のために送信されました 23: サポートされていないファイル
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"> 1: 検出 2: ブロック 3: マルウェア クラウドルックアップ 4: マルウェア ブロック 5: マルウェア ホワイトリスト
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、 エンドポイント向け AMP ファイルタイプのメタデータ (3-43 ページ) を参照してください。
ファイル名	string	ファイルの名前。
ファイルサイズ (File size)	uint64	ファイルのサイズ(バイト単位)。
方向 (Direction)	uint8	ファイルのアップロードとダウンロードのどちらが行われたかを示す値。次のいずれかの値になります。 <ul style="list-style-type: none"> 1: ダウンロード 2: アップロード 現時点では、この値はプロトコルに依存しています (たとえば接続が HTTP の場合はダウンロード)。
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ 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"> 1: ICMP 4: IP 6: TCP 17: UDP これは現時点では TCP のみです。
アクセスコントロールポリシー UUID	uint8[16]	イベントをトリガーするアクセスコントロールポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号(該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号(該当する場合)。

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															

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							
	0	1	2	3	4	5	6	7	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	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															
	プロトコル								アクセス コントロール ポリシー UUID																							

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

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 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"> • 1 (CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。 • 2 (UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。 • 3 (MALWARE): ファイルにはマルウェアが含まれています。 • 4 (UNAVAILABLE): ソフトウェアから 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。 • 5 (CUSTOM SIGNATURE): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
SPERO 解析結果	uint8	SPERO 署名がファイル分析で使用されたかどうかを示します。値が 1、2、または 3 であれば、SPERO 分析は使用されました。それ以外の値であれば、SPERO 分析は使用されませんでした。
ファイル ストレージ ステータス	uint8	<p>ファイルの保存ステータス。値は以下のとおりです。</p> <ul style="list-style-type: none"> • 1: ファイルが保存されました • 2: ファイルが保存されました • 3: ファイルを保存できません • 4: ファイルを保存できません • 5: ファイルを保存できません • 6: ファイルを保存できません • 7: ファイルを保存できません • 8: ファイル サイズが大きすぎます • 9: ファイル サイズが小さすぎます • 10: ファイルを保存できません • 11: ファイルは保存されておらず、解析結果を入手できません

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

表 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"> • 1:検出 • 2:ブロック • 3:マルウェアクラウドルックアップ • 4:マルウェアブロック • 5:マルウェアホワイトリスト
SHA ハッシュ	uint8[32]	バイナリ形式の SHA-256 ハッシュのファイル。
ファイルタイ プ ID	uint32	ファイルタイプにマップされている ID 番号。このフィール ドの意味は、このイベントと一緒にメタデータで送信されます。 詳細については、 エンドポイント向け AMP ファイルタイプの メタデータ(3-43 ページ) を参照してください。
ファイル名	string	ファイルの名前。
ファイルサイ ズ(File size)	uint64	ファイルのサイズ(バイト単位)。
方向 (Direction)	uint8	ファイルのアップロードとダウンロードのどちらが行われた かを示す値。次のいずれかの値になります。 <ul style="list-style-type: none"> • 1:ダウンロード • 2:アップロード <p>現時点では、この値はプロトコルに依存しています(たとえば 接続が HTTP の場合はダウンロード)。</p>
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"> • 1:ICMP • 4:IP • 6:TCP • 17:UDP <p>これは現時点では TCP のみです。</p>

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。



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
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)																								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)																															

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

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								
	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)。

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"> 1 (CLEAN): ファイルはクリーンであり、マルウェアは含まれていません。 2 (UNKNOWN): ファイルにマルウェアが含まれているかどうかは不明です。 3 (MALWARE): ファイルにはマルウェアが含まれています。 4 (UNAVAILABLE): ソフトウェアから 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。 5 (CUSTOM SIGNATURE): ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理されました。
SPERO 解析結果	uint8	SPERO 署名がファイル分析で使用されたかどうかを示します。値が 1、2、または 3 であれば、SPERO 分析は使用されました。それ以外の値であれば、SPERO 分析は使用されませんでした。
ファイルストレージステータス	uint8	<p>ファイルの保存ステータス。値は以下のとおりです。</p> <ul style="list-style-type: none"> 1: ファイルが保存されました 2: ファイルが保存されました 3: ファイルを保存できません 4: ファイルを保存できません 5: ファイルを保存できません 6: ファイルを保存できません 7: ファイルを保存できません 8: ファイル サイズが大きすぎます 9: ファイル サイズが小さすぎます 10: ファイルを保存できません 11: ファイルは保存されておらず、解析結果を入力できません

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"> • 0: ファイルが分析のために送信されていません • 1: 分析のために送信されました • 2: 分析のために送信されました • 4: 分析のために送信されました • 5: 送信に失敗しました • 6: 送信に失敗しました • 7: 送信に失敗しました • 8: 送信に失敗しました • 9: ファイルサイズが小さすぎます • 10: ファイルサイズが大きすぎます • 11: 分析のために送信されました • 12: 分析が完了しました • 13: 失敗(ネットワークの問題) • 14: 失敗(レート制限) • 15: 失敗(ファイルが大きすぎます) • 16: 失敗(ファイルの読み取りエラー) • 17: 失敗(内部ライブラリエラー) • 19: ファイルは送信されておらず、解析結果を入力できません • 20: 失敗(ファイルを実行できません) • 21: 失敗(分析タイムアウト) • 22: 分析のために送信されました • 23: サポートされていないファイル

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"> 0 (N/A): ファイルがアーカイブとして検査されていません。 1: 保留中。アーカイブは調査中です 2: 取得済み。調査が問題なく正常に実行されました 3: 失敗。システムのリソース不足のため調査に失敗しました。 4: 深度の超過。調査は正常に実行されましたが、アーカイブがネストされた調査の深度を超過しました 5: 暗号化。部分的に正常に実行されましたが、アーカイブが暗号化されているか、暗号化されたアーカイブが含まれています 6: 調査できませんでした。部分的に正常に実行されましたが、ファイル形式が不正であるか破損しています
脅威スコア	uint8	<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"> 1: 検出 2: ブロック 3: マルウェア クラウドルックアップ 4: マルウェア ブロック 5: マルウェア ホワイトリスト 6: クラウドルックアップのタイムアウト 7: カスタム検出 8: カスタム検出ブロック 9: アーカイブ ブロック (深度超過) 10: アーカイブ ブロック (暗号化されている) 11: アーカイブ ブロック (調査エラー)
SHA ハッシュ	uint8[32]	<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、エンドポイント向け AMP ファイルタイプのメタデータ (3-43 ページ)を参照してください。</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"> 1: ダウンロード 2: アップロード 現時点では、この値はプロトコルに依存しています (たとえば接続が HTTP の場合はダウンロード)。
アプリケーション ID (Application ID)	uint32	ファイル転送を使用するアプリケーションにマップされている ID 番号。
ユーザ ID (User ID)	uint32	システムにより識別される、宛先ホストにログインしたユーザの ID 番号。
URI	string	接続の Uniform Resource Identifier (URI)。
シグネチャ	string	文字列形式の SHA-256 ハッシュのファイル。
送信元ポート	uint16	接続の送信元のポート番号。
接続先ポート	uint16	接続の宛先のポート番号。
プロトコル	uint8	ユーザが指定した IANA プロトコル数。次に例を示します。 <ul style="list-style-type: none"> 1: ICMP 4: IP 6: TCP 17: UDP これは現時点では TCP のみです。
アクセスコントロールポリシー UUID	uint8[16]	イベントをトリガーするアクセスコントロールポリシーの固有識別子。
送信元の国	uint16	送信元ホストの国のコード。
宛先の国	uint16	宛先ホストの国のコード。
Web アプリケーション ID	uint32	Web アプリケーションの内部 ID 番号 (該当する場合)。
クライアントアプリケーション ID	uint32	クライアントアプリケーションの内部 ID 番号 (該当する場合)。
セキュリティコンテキスト	uint8(16)	トラフィックが通過したセキュリティコンテキスト (仮想ファイアウォール) の ID 番号。マルチコンテキストモードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
SSL 証明書フィンガープリント	uint8[20]	SSL サーバ証明書の 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">0:「不明」1:「復号しない」2:「ブロックする」3:「リセットでブロック」4:「復号(既知のキー)」5:「復号(置換キー)」6:「復号(Resign)」

表 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"> • 0:「不明」 • 1:「一致しない」 • 2:「成功」 • 3:「キャッシュされていないセッション」 • 4:「不明の暗号化スイート」 • 5:「サポートされていない暗号スイート」 • 6:「サポートされていない SSL バージョン」 • 7:「使用される SSL 圧縮」 • 8:「パッシブ モードで復号不可のセッション」 • 9:「ハンドシェイク エラー」 • 10:「復号エラー」 • 11:「保留中のサーバ名カテゴリ ルックアップ」 • 12:「保留中の共通名カテゴリ ルックアップ」 • 13:「内部エラー」 • 14:「使用できないネットワーク パラメータ」 • 15:「無効なサーバの証明書の処理」 • 16:「サーバ証明書フィンガープリントが使用不可」 • 17:「サブジェクト DN をキャッシュできません」 • 18:「発行者 DN をキャッシュできません」 • 19:「不明な SSL バージョン」 • 20:「外部証明書のリストが使用できません」 • 21:「外部証明書のフィンガープリントが使用できません」 • 22:「内部証明書リストが無効」 • 23:「内部証明書のリストが使用できません」 • 24:「内部証明書が使用できません」 • 25:「内部証明書のフィンガープリントが使用できません」 • 26:「サーバ証明書の検証が使用できません」 • 27:「サーバ証明書の検証エラー」 • 28:「無効な操作」
文字列ブロックタイプ	uint32	<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>

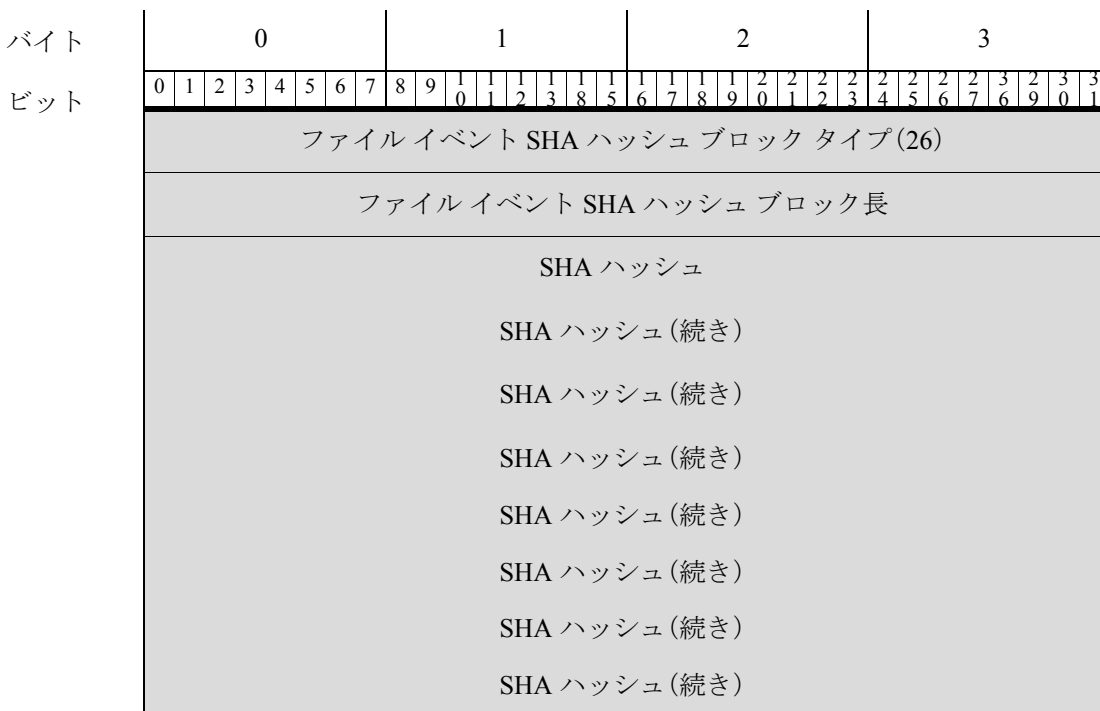
表 B-44 ファイルイベント データ ブロック 5.4.x のフィールド(続き)

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 で要求されている場合は、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。



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 \(B-270 ページ\)](#)
- [関連イベント 5.1 ~ 5.3.x \(B-279 ページ\)](#)

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																															
	Device ID																															
	(関連)イベント秒																															
	イベント ID(Event ID)																															
	ポリシー ID																															
	ルール ID																															
	[プライオリティ(Priority)]																															
	文字列ブロックタイプ(0)																															
	文字列ブロック長																															
	説明...																イベントタイプ(Event Type)															
	イベント Device ID																															

イベント
説明

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
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 OS フィンガープリント UUID (続き)																								送信元重要度								
送信元重要度 (続き)								送信元ユーザ ID																								
送信元ユーザ ID (続き)								送信元ポート																送信元サーバ ID								
送信元サーバ ID (続き)																								宛先 IP (Destination IP)								
宛先 IP (続き)																								着信ホストタイプ								
着信 VLAN ID (Admin. VLAN ID)																宛先 OS フィンガープリント UUID																宛先 OS フィン ガープリ ント UUID
宛先 OS フィンガープリント UUID (続き)																																
宛先 OS フィンガープリント UUID (続き)																																
宛先 OS フィンガープリント UUID (続き)																																
宛先 OS フィンガープリント UUID (続き)																宛先重要度																

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

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。 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。
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)。
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、 管理対象 Device レコードのメタデータ (3-37 ページ) を参照してください。
(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。データベースからポリシー ID 番号を入手する方法の詳細については、 サービス レコード (4-16 ページ) を参照してください。
ルール ID	uint32	トリガーしてポリシー違反となった関連ルールの ID 番号。データベースからポリシー ID 番号を入手する方法の詳細については、 サービス レコード (4-16 ページ) を参照してください。
[プライオリティ (Priority)]	uint32	イベントに割り当てられた優先順位。これは、0 ~ 5 の整数値です。
文字列ブロックタイプ	uint32	関連違反イベントの説明を含む文字列データブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、 文字列データ ブロック (4-73 ページ) を参照してください。
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数(文字列のブロックタイプのための 4 バイト、文字列ブロック長のための 4 バイト、説明のバイト数を含む)。
説明	string	関連イベントについての説明。
イベントタイプ (Event Type)	uint8	<p>関連イベントが、侵入、ホスト検出、またはユーザ イベントによってトリガーされたかどうかを示します。</p> <ul style="list-style-type: none"> • 1: 侵入 • 2: ホストのディスカバリ • 3: ユーザ
イベント Device ID	uint32	関連イベントをトリガーしたイベントを生成したデバイスの ID 番号。バージョン 3 メタデータを要求するとデバイス名を入手できます。詳細については、 管理対象 Device レコードのメタデータ (3-37 ページ) を参照してください。
シグネチャ ID	uint32	イベントが侵入イベントであった場合、イベントに対応するルール ID 番号を示します。そうでない場合、この値は 0 になります。

表 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
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)。
(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	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-278 ページ)を参照してください。

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"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40: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。 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。 <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"> (0、不明):00x00000 赤(1、脆弱):xxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx オレンジ(2、潜在的に脆弱):00x00111 黄(3、現在は脆弱でない):00x00011 青(4、不明なターゲット):00x00001
IP プロトコル	uint8	イベントに関連付けられている IP プロトコルの ID(該当する場合)。
ネットワークプロトコル	uint16	イベントに関連付けられているネットワークプロトコル(該当する場合)。
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"> 0: ホスト 1: ルータ 2: ブリッジ
送信元 VLAN ID	uint16	送信元ホストの VLAN ID 番号(該当する場合)。
送信元 OS フィンガープリント UUID	uint8[16]	送信元ホストのオペレーティングシステムの固有識別子として機能するフィンガープリント ID。 フィンガープリント ID にマップする値の取得の詳細については、 サービスレコード(4-16 ページ) を参照してください。
送信元重要度	uint16	送信元ホストの、ユーザ定義の重要度値: <ul style="list-style-type: none"> 0: なし 1: 低 2: 中 3: 高
送信元ユーザ 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"> 0: ホスト 1: ルータ 2: ブリッジ
宛先 VLAN ID	uint16	宛先ホストの VLAN ID 番号(該当する場合)。
宛先 OS フィンガープリント UUID	uint8[16]	宛先ホストのオペレーティングシステムの固有識別子として機能するフィンガープリント ID 番号。 フィンガープリント ID にマップする値の取得の詳細については、 サービスレコード(4-16 ページ) を参照してください。
宛先重要度	uint16	宛先ホストの、ユーザ定義の重要度値: <ul style="list-style-type: none"> 0: なし 1: 低 2: 中 3: 高

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"> 0: 侵入イベントがドロップされていない 1: 侵入イベントがドロップされている (展開がインライン型、スイッチ型、またはルーティング型である場合はドロップ) 2: 侵入ポリシーが、インライン型、スイッチ型、またはルーティング型展開のデバイスに適用されている場合は、イベントをトリガーしたパケットがドロップされている可能性がある。
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
	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)																																	

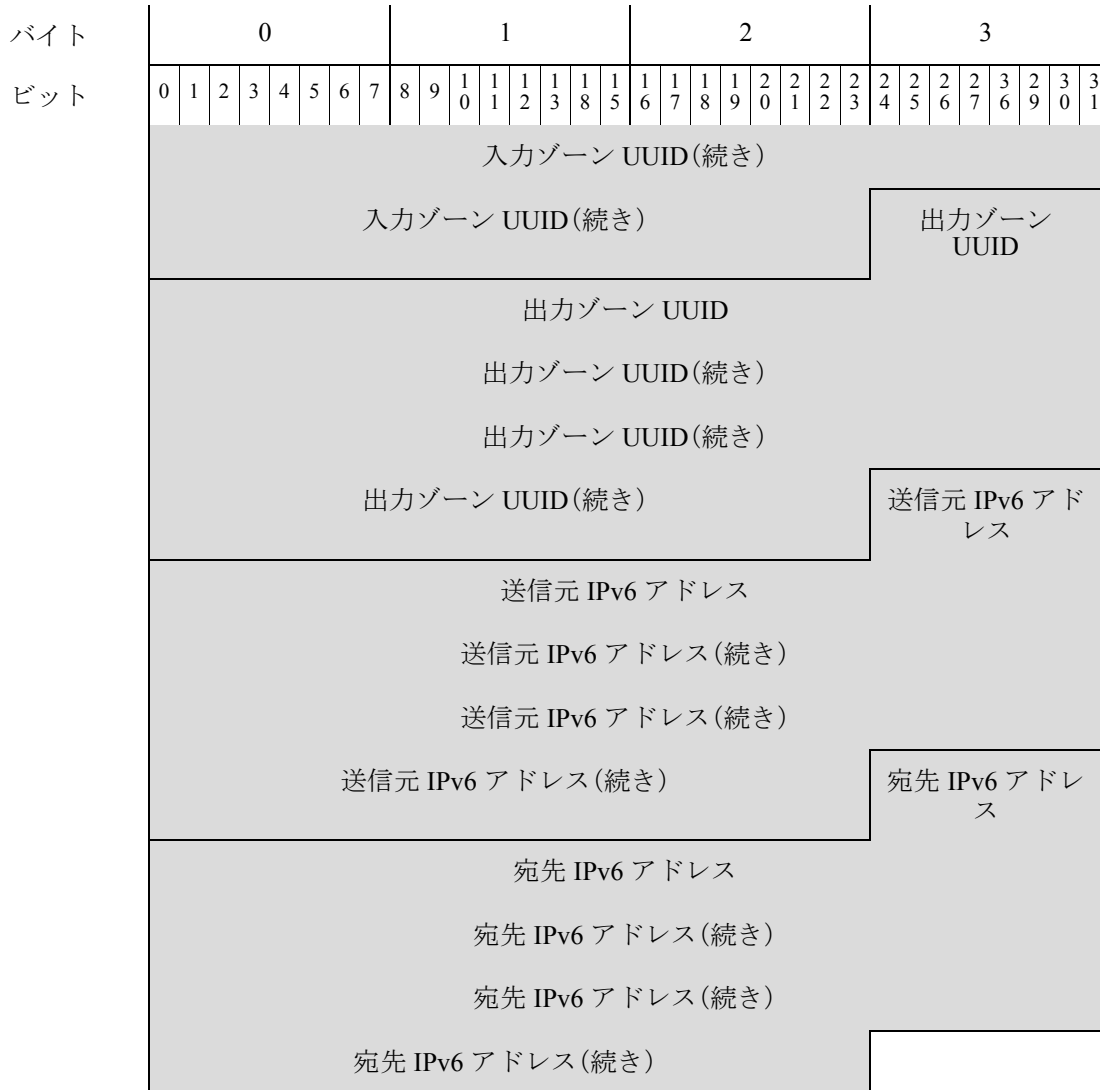
レガシー関連イベントのデータ構造

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								入力インターフェイス UUID															
	入力インターフェイス UUID (続き)																出力インターフェイス UUID															
	入力インターフェイス UUID (続き)																															
	入力インターフェイス UUID (続き)																															
	入力インターフェイス UUID (続き)								出力インターフェイス UUID (続き)								入力ゾーン UUID															
	出力インターフェイス UUID (続き)																															
	出力インターフェイス UUID (続き)																															
	出力インターフェイス UUID (続き)								入力ゾーン UUID																							
	入力ゾーン UUID (続き)																															

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。 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。
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、 管理対象 Device レコードのメタデータ (3-37 ページ) を参照してください。
(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。データベースからポリシー ID 番号を入手する方法の詳細については、 サービス レコード (4-16 ページ) を参照してください。
ルール ID	uint32	トリガーしてポリシー違反となった関連ルールの ID 番号。データベースからポリシー ID 番号を入手する方法の詳細については、 サービス レコード (4-16 ページ) を参照してください。
[プライオリティ (Priority)]	uint32	イベントに割り当てられた優先順位。これは、0 ~ 5 の整数値です。
文字列ブロックタイプ	uint32	関連違反イベントの説明を含む文字列データブロックを開始します。この値は常に 0 に設定されます。文字列ブロックの詳細については、 文字列データブロック (4-73 ページ) を参照してください。
文字列ブロック長	uint32	イベント説明文字列ブロックのバイト数(文字列のブロックタイプのための 4 バイト、文字列ブロック長のための 4 バイト、説明のバイト数を含む)。
説明	string	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"> • 1: 侵入 • 2: ホストのディスカバリ • 3: ユーザ
イベントデバイス ID	uint32	関連イベントをトリガーしたイベントを生成したデバイスの ID 番号。バージョン 3 メタデータを要求するとデバイス名を入手できます。詳細については、 管理対象 Device レコードのメタデータ (3-37 ページ) を参照してください。
シグネチャ ID	uint32	イベントが侵入イベントであった場合、イベントに対応するルール ID 番号を示します。そうでない場合、この値は 0 になります。
シグネチャジェネレータ ID	uint32	イベントが侵入イベントであった場合、イベントを生成した Firepower システム プリプロセッサまたはルールエンジンの ID 番号を示します。
(トリガー) イベント秒	uint32	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-278 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"> 0x01(ビット 0):送信元または宛先ホストはシステムによってモニタされるネットワーク内にあります。 0x02(ビット 1):送信元または宛先ホストはネットワークマップ内に存在します。 0x04(ビット 2):送信元または宛先ホストはイベントのポート上のサーバを実行しているか(TCP または UDP の場合)、IP プロトコルを使用します。 0x08(ビット 3):イベントの送信元または宛先ホストのオペレーティングシステムにマップされた脆弱性があります。 0x10(ビット 4):イベントで検出されたサーバにマップされた脆弱性があります。 0x20(ビット 5):イベントが原因で、管理対象デバイスがセッションをドロップしました(デバイスがインライン、スイッチド、またはルーテッド展開で実行している場合にのみ使用されます)。Firepower システム Web インターフェイスのブロックされた状態に対応します。 0x40(ビット 6):このイベントを生成するルールに、影響フラグを赤色に設定するルールのメタデータが含まれます。送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵入される可能性があります。 0x80(ビット 7):イベントで検出されたクライアントにマップされた脆弱性があります。(バージョン 5.0+ のみ) <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"> (0、不明):00x00000 赤(1、脆弱):xxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx(バージョン 5.0+ のみ) オレンジ(2、潜在的に脆弱):00x0011x 黄(3、現在は脆弱でない):00x0001x 青(4、不明なターゲット):00x00001

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、設定されていません。送信元 IPv4 アドレスは、送信元 IPv6 アドレス フィールドに保存されます。詳細については、 IP アドレス(1-5 ページ) を参照してください。
送信元ホストタイプ	uint8	送信元ホストのタイプ: <ul style="list-style-type: none"> • 0: ホスト • 1: ルータ • 2: ブリッジ
送信元 VLAN ID	uint16	送信元ホストの VLAN ID 番号(該当する場合)。
送信元 OS フィンガープリント UUID	uint8[16]	送信元ホストのオペレーティング システムの固有識別子として機能するフィンガープリント ID。 フィンガープリント ID にマップする値の取得の詳細については、 サービス レコード(4-16 ページ) を参照してください。
送信元重要度	uint16	送信元ホストの、ユーザ定義の重要度値: <ul style="list-style-type: none"> • 0: なし • 1: 低 • 2: 中 • 3: 高
送信元ユーザ 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、設定されていません。宛先 IPv4 アドレスは、宛先 IPv6 アドレス フィールドに保存されます。詳細については、 IP アドレス(1-5 ページ) を参照してください。
宛先ホストタイプ	uint8	宛先ホストのタイプ: <ul style="list-style-type: none"> • 0: ホスト • 1: ルータ • 2: ブリッジ
宛先 VLAN ID	uint16	宛先ホストの VLAN ID 番号(該当する場合)。

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、 サービス レコード(4-16 ページ) を参照してください。
宛先重要度	uint16	宛先ホストの、ユーザ定義の重要度値: <ul style="list-style-type: none"> • 0:なし • 1:低 • 2:中 • 3:高
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"> • 0:侵入イベントがドロップされていない • 1:侵入イベントがドロップされている(展開がインライン型、スイッチ型、またはルーティング型である場合はドロップ) • 2:侵入ポリシーが、インライン型、スイッチ型、またはルーティング型展開のデバイスに適用されている場合は、イベントをトリガーしたパケットがドロップされている可能性がある。
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\(2-28 ページ\)](#)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\(B-287 ページ\)](#)
- [フルホストプロファイルデータブロック 5.1.1\(B-297 ページ\)](#)
- [フルホストプロファイルデータブロック 5.2.x\(B-308 ページ\)](#)
- [ホストプロファイルデータブロック 5.1.x\(B-321 ページ\)](#)
- [IP 範囲仕様データブロック 5.0 ~ 5.1.1.x\(B-328 ページ\)](#)
- [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\(B-329 ページ\)](#)

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	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
フル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 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																						

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							
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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	ユーザ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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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。

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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
リストブロックタイプ	uint32	TCP サー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、 フルホストサーバデータブロック 4.10.0+(4-145 ページ) を参照してください。

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+ (4-145 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"> 0 — ホスト 1: ルータ 2 — ブリッジ 3 — NAT(ネットワークアドレス変換デバイス) 4 — LB(ロードバランサー)
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、 フルクライアントアプリケーションデータブロック 5.0+(4-158 ページ) を参照してください。
文字列ブロックタイプ	uint32	ホスト NetBIOS 名の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データブロックのバイト数(文字列ブロックタイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
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、 ホスト脆弱性データブロック 4.9.0+(4-116 ページ) を参照してください。
汎用リストブロックタイプ	uint32	サードパーティスキャン脆弱性データを伝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、 ホスト脆弱性データブロック 4.9.0+(4-116 ページ) を参照してください。
汎用リストブロックタイプ	uint32	サードパーティスキャン脆弱性データを伝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、 ホスト脆弱性データブロック 4.9.0+(4-116 ページ) を参照してください。
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、 属性値データブロック (4-84 ページ) 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								
	0	1	2	3	4	5	6	7	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																																	
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																																	
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...																																

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	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																															
VDB ネイ ティブフィン 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 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																															

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
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)*																															
	Last Seen																															

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)*																															
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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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)。

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
オペレーティングシステムフィンガープリント(クライアントフィンガープリント)データブロック*	変数(variable)	クライアントフィンガープリントを使用して識別されるホスト上のオペレーティングシステムに関する情報が含まれている、オペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	ユーザ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。

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
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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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。

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
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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
リストブロックタイプ	uint32	TCP サービス 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、 フルホストサーバデータブロック 4.10.0+(4-145 ページ) を参照してください。
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+(4-145 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。

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
(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。
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"> • 0 — ホスト • 1: ルータ • 2 — ブリッジ • 3 — NAT(ネットワークアドレス変換デバイス) • 4 — LB(ロードバランサー)
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。
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、 フルクライアントアプリケーションデータブロック 5.0+(4-158 ページ) を参照してください。
文字列ブロックタイプ	uint32	ホスト NetBIOS 名の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データブロックのバイト数(文字列ブロックタイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。

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
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、 ホスト脆弱性データブロック 4.9.0+ (4-116 ページ) を参照してください。
汎用リストブロックタイプ	uint32	サードパーティ スキャン脆弱性データを伝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、 ホスト脆弱性データブロック 4.9.0+ (4-116 ページ) を参照してください。
汎用リストブロックタイプ	uint32	サードパーティ スキャン脆弱性データを伝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、 ホスト脆弱性データブロック 4.9.0+ (4-116 ページ) を参照してください。
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-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
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、 属性値データブロック (4-84 ページ) 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"> 0: はい 1: いいえ

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 (140)																															
	データブロック長																															
	ホスト ID (Host ID)																															
	ホスト ID (続き)																															
	ホスト ID (続き)																															
	ホスト ID (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
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																															
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																															

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)																															
	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)																															

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																															
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...																															
	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...																															

レガシーホストデータ構造

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
	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)*																															
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)															

バイト	0								1								2								3							
ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ホストクライアントデータ	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)*																															
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、 ホスト IP アドレス データ ブロック (4-100 ページ) を参照してください。
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、 オペレーティングシステムフィンガープリント データ ブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリント データ ブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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。

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(クライアントフィンガープリント)データブロック*	変数(variable)	クライアントフィンガープリントを使用して識別されるホスト上のオペレーティングシステムに関する情報が含まれている、オペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	ユーザ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。

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	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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。

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	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	モバイルデバイスフィンガープリントデータを伝える、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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	IPv6 サーバフィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
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 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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	IPv6 クライアントフィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	IPv6 DHCP フィンガープリントで識別するフィンガープリントデータを搬送するオペレーティングシステムフィンガープリントデータブロックで構成される汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	ユーザエージェントフィンガープリントで識別するフィンガープリントデータを搬送するオペレーティングシステムフィンガープリントデータブロックで構成される汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
リストブロックタイプ	uint32	TCP サー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、 フルホストサーバデータブロック 4.10.0+(4-145 ページ) を参照してください。

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
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+(4-145 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-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
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"> 0 — ホスト 1: ルータ 2 — ブリッジ 3 — NAT(ネットワークアドレス変換デバイス) 4 — LB(ロードバランサー)
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、 フルクライアントアプリケーションデータブロック 5.0+(4-158 ページ) を参照してください。
文字列ブロックタイプ	uint32	ホスト NetBIOS 名の文字列データブロックを開始します。この値は常に 0 です。
文字列ブロック長	uint32	文字列データブロックのバイト数(文字列ブロックタイプと長さフィールド用の 8 バイト、および NetBIOS 名文字列のバイト数を含む)。
NetBIOS 名	string	ホスト NetBIOS 名の文字列。
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-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
(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、 ホスト脆弱性データブロック 4.9.0+ (4-116 ページ) を参照してください。
汎用リストブロックタイプ	uint32	サードパーティスキャン脆弱性データを伝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、 ホスト脆弱性データブロック 4.9.0+ (4-116 ページ) を参照してください。
汎用リストブロックタイプ	uint32	サードパーティスキャン脆弱性データを伝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、 ホスト脆弱性データブロック 4.9.0+ (4-116 ページ) を参照してください。
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、 属性値データブロック (4-84 ページ) 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							
	0	1	2	3	4	5	6	7	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*																															
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Deviceフィンガープリント	汎用リストブロックタイプ(31)																															
	汎用リストブロック長																															
	モバイルDeviceフィンガープリントデータブロック*																															
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																															

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	
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																																
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"> 0:ホストはプライマリ ネットワークにあります。 1:ホストはセカンダリ ネットワークにあります。
汎用リストブロックタイプ	uint32	サーバ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、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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)。

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
オペレーティングシステムフィンガープリント(クライアントフィンガープリント)データブロック*	変数 (variable)	クライアントフィンガープリントを使用して識別されるホスト上のオペレーティングシステムに関する情報が含まれている、オペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 オペレーティングシステムフィンガープリントデータブロック 5.1+ (4-165 ページ)を参照してください。
汎用リストブロックタイプ	uint32	SMB フィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。
オペレーティングシステムフィンガープリント(SMB フィンガープリント)データブロック*	変数 (variable)	SMB フィンガープリントを使用して識別されるホスト上のオペレーティングシステムに関する情報が含まれている、オペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	DHCP フィンガープリントを使用して識別されるフィンガープリントデータを伝える、オペレーティングシステムフィンガープリントデータブロックを構成する汎用リストデータブロックを開始します。この値は常に 31 です。
汎用リストブロック長	uint32	汎用リストデータブロックのバイト数(リストヘッダーと、カプセル化されたすべてのオペレーティングシステムフィンガープリントデータブロックを含む)。
オペレーティングシステムフィンガープリント(DHCP フィンガープリント)データブロック*	変数 (variable)	DHCP フィンガープリントを使用して識別されるホスト上のオペレーティングシステムに関する情報が含まれている、オペレーティングシステムフィンガープリントデータブロック。このデータブロックの説明の詳細については、 オペレーティングシステムフィンガープリントデータブロック 5.1+(4-165 ページ) を参照してください。
汎用リストブロックタイプ	uint32	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)。

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
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 Device 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、 オペレーティングシステムフィンガープリントデータブロック 5.1+ (4-165 ページ) を参照してください。
リストブロックタイプ	uint32	TCP サーバデータを伝えるサーバデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リスト内のバイト数。この数値は、リストブロックタイプフィールドと長さフィールドの 8 バイトに、カプセル化されたすべてのサーバデータブロックを加えた値です。 このフィールドには、ゼロ以上のサーバデータブロックが続きます。
TCP サーバデータブロック	変数 (variable)	TCP サーバを記述するホストサーバデータブロック(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。
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、 プロトコルデータブロック (4-78 ページ) を参照してください。
リストブロックタイプ	uint32	トランスポートプロトコルデータを伝えるプロトコルデータブロックで構成されたリストデータブロックを開始します。この値は常に 11 です。

表 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プロトコルデータブロックを加えた値です。 このフィールドには、ゼロ以上のトランスポートプロトコルデータブロックが続きます。
トランスポートプロトコルデータブロック	uint32	トランスポートプロトコルを記述するプロトコルデータブロック。このデータブロックの説明の詳細については、 プロトコルデータブロック (4-78 ページ) を参照してください。
リストブロックタイプ	uint32	MAC アドレスデータブロックを構成するリストデータブロックを開始します。この値は常に 11 です。
リストブロック長	uint32	リストのバイト数(リストヘッダーと、カプセル化されたすべての MAC アドレスデータブロックを含む)。
ホスト MAC アドレスデータブロック	uint32	ホスト MAC アドレスを記述するホスト MAC アドレスデータブロック。このデータブロックの説明の詳細については、 ホスト MAC アドレス 4.9+(4-119 ページ) を参照してください。
最終検出時のホスト	uint32	システムがホストアクティビティを検出した前回時刻を表す UNIX タイムスタンプ。
ホストタイプ	uint32	ホストタイプを示します。表示される可能性がある値は次のとおりです。 <ul style="list-style-type: none"> 0: ホスト 1: ルータ 2: ブリッジ 3: NAT デバイス 4: LB(ロードバランサ)
Mobile	uint8	検出したホストがモバイルデバイスであるかどうかを示す true/false フラグ。
改造	uint8	ホストが(ジェイルブレイクされていない)モバイルデバイスであるかどうかを示す true/false フラグ。
VLAN の有無	uint8	VLAN が存在するかどうかを示します。 <ul style="list-style-type: none"> 0: はい 1: いいえ
VLAN ID (Admin. VLAN ID)	uint16	ホストがメンバーである VLAN を示す VLAN ID 番号。
VLAN タイプ	uint8	VLAN タグにカプセル化されたパケットのタイプ。
VLAN 優先順位	uint8	VLAN タグに含まれるプライオリティ値。
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。

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、 フルクライアントアプリケーションデータブロック 5.0+(4-158 ページ) を参照してください。
文字列ブロックタイプ	uint32	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。