

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。



<u>—</u> (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)
- レガシー相関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 $5.0.x \sim 5.1$ 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 3 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| • | 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 | | |
| | Netma | 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 | i 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 1 1 1 1 1 1 1 5 | $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | IP プロトコル ID 影響フラグ 影響 ブロック | | | | | |
| | | MPLS | ラベル | | | |
| | VLAN ID (Adm | nin. VLAN ID) | パ | ッド | | |
| | | ポリシー | - UUID | | | |
| | | ポリシーU | UID(続き) | | | |
| | | ポリシーU | UID(続き) | | | |
| | | ポリシーU | UID(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 | | | | | |
| | <i>T</i> : | クセス コントロール | ポリシー UUID(続 | <i>き</i>) | | |
| | 7 : | クセス コントロール | ポリシー UUID(続 | <i>a</i>) | | |
| | <i>T</i> : | クセス コントロール | ポリシー UUID(続 | <i>(</i> *) | | |
| | | インターフェイ | 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 | 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) | | | |

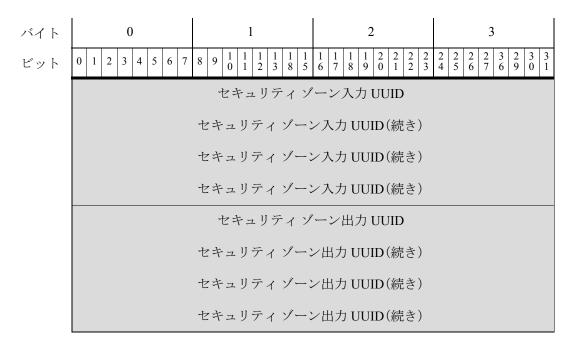


表 B-1 侵入イベント(IPv4)レコードのフィールド

| | データ タ | |
|-----------------------|----------|--|
| フィールド | イプ | 説明 |
| Device ID unit32 | | 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)

| | データ タ | |
|------------------|----------|--|
| フィールド | 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。 |

表 B-1 侵入イベント(IPv4)レコードのフィールド(続き)

| | データ タ | |
|-------|---------|--|
| フィールド | イプ | 説明 |
| 影響フラグ | bits[8] | 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。 |
| | | • 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。 |
| | | 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。 |
| | | • (0、不明):00x00000 |
| | | • 赤(1、脆弱):xxxxxxxxx, xxxxxxxx, xxxxxxxx, xxxxxxxx |
| | | • 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 | イベントの影響フラグ値。値は次のとおりです。 |
| | | • 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。 |
| | | • o: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 $5.0.x \sim 5.1$ 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 3 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| | 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 | | | | |
| | Netma | ap ID | レコードタ | ·イプ(208) | |
| | | レコー | - ド長 | | |
| | eStreamer サーバ タ | マイムスタンプ(イベ 合の | | 設定されている場 | |
| | 将来の使用に備えて | 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 | 卜 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

ビッ

| <u>۲</u> | 0 | 1 | 2 | 3 | |
|----------|--------------------|-----------------------|---|---|--|
| ١ | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| | 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 アト | ドレス(続き) | | |
| | | 宛先 IPv6 アト | ドレス(続き) | | |
| | 送信元ポート/ | TCMP タイプ | 宛先ポート/I | CMP 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 (Adm | in. 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 | | | | |
| | | クライアントアフ | プリケーション ID | | |
| | | アプリケーション | ノプロトコル ID | | |
| | | アクセス コントロ | コールルール ID | | |
| | | アクセス コントロー | | | |
| | | クセス コントロール | | , | |
| | | クセス コントロール | | , | |
| | <i>P</i> / | クセス コントロール | | <u>(</u> f) | |
| | | インターフェイ | | | |
| | | 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | | 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) | |
| | | セキュリティン | デーン入力 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) | |
| | | セキュリティン | ゲーン出力 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) | |

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 | unit32 | 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)

| | データ タ | |
|---------------------|-----------|---|
| フィールド | 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 | uint8 | IANA 指定のプロトコル番号。次に例を示します。 |
| 番号 | | • 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)

| | データ タ | |
|-------|---------|--|
| フィールド | イプ | 説明 |
| 影響フラグ | bits[8] | 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。 |
| | | • 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。 |
| | | 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。 |
| | | • (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 | イベントの影響フラグ値。値は次のとおりです。 |
| | | • 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)

| | データ タ | |
|--------------------------------|-----------|--|
| フィールド | 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。 |
| | | • o: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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | |
| | 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 | | | | |
| | Netm | ap ID | レコードゟ | アイプ(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 | 7イプ(34) | | | | |
| | | ブロッ | ク長 | | | | |
| | | Devic | ee ID | | | | |
| | | イベントID | (Event ID) | | | | |
| | | イベン | ∕卜秒 | | | | |
| | | イベントっ | アイクロ秒 | | | | |
| | | 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 | į 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | | |
| | | 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 7 | アドレス | | | | | |
| | | 宛先 IP アド | レス(続き) | | | | | |
| | | 宛先 IP アド | | | | | | |
| | | 宛先 IP アド | ンス(続き) | | | | | |
| | 送信元ポートまた | こは ICMP タイプ | 送信先ポートまた | こは 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 (Adn | nin. VLAN ID) | パッ | ノド | | | | |
| | | ポリシー | - UUID | | | | | |
| | | ポリシーU | UID(続き) | | | | | |
| | | ポリシーU | UID(続き) | | | | | |
| | | ポリシーU | UID(続き) | | | | | |
| | | ユーザ ID | (User ID) | | | | | |
| | | Web アプリク | 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 | <u>(</u>) | | | | |
| | ア | クセス コントロール | ポリシー UUID(続き | ٤) | | | | |
| | | | | | | | | |

| バイト | 0 | | 1 | | | 2 | | | 3 | | | | | | | | |
|-----|-----------------------|-----|------------|--|-----|----------------|--------------|-------|-----|-------|-----|-------|-----|-----|-----|----------|---|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 | 1 1 0 1 | $\begin{array}{c cccc} 1 & 1 & 1 \\ 2 & 3 & 8 \end{array}$ | 1 5 | 1 1 1 6 7 8 | 3 | 1 2 0 | 2 | 2 2 3 | 2 4 | 2 2 6 | 2 7 | 3 6 | 2 9 | 3 0 1 | - |
| | <i>r</i> : | クセフ | スコン | トロー | ル | ポリシ | /_ | - UI | JID |)(続 | き) | | | | | | |
| | | | インク | ターフュ | -/ | イス入力 | ђ | UUI | D | | | | | | | | |
| | | イン | ンター | フェイ | ス | 入力 U | U] | ID(| 続き | ٤) | | | | | | | |
| | 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 U | U | ID (} | 続き | ٤) | | | | | | | |
| | | イ | ンター | フェイ | ス | 出力 U | U | ID (} | 続き | ٤) | | | | | | | |
| | 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 | ュリラ | ニィゾー | -: | /入力1 | U | JID | (続 | き) | | | | | | | |
| | | セキ | ユリラ | ニィゾー | -: | /入力1 | U | JID | (続 | き) | | | | | | | |
| | | 1 | セキュ | リティ | ゾ | ーン出 | け、 | J UU | JID |) | | | | | | | |
| | | セキ | ユリラ | ニィゾー | - ; | /出力1 | Ul | JID | (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) | | | | | | | | | | | | | | | | |
| | | | 担 | 接続タイ | 1 | スタン | / 7 | プ | | | | | | | | | |
| | 接続インス | タン | スID | | | | | | 接絲 | 売数ス | b ウ | ンタ | 7 | | | | |
| | 送信元 | の国 | | | | | | | | 宛先 | の[| 玉 | | | | | |

表 B-3 侵入イベント レコード 5.2.x のフィールド

| | データ タ | |
|---------------------------|---------------------|--|
| フィールド | ァー <i>ァ ゥ</i> イプ | 説明 |
| ブロック タ イプ | unint32 | 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 | unint32 | 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 | unit32 | 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 | uint8 | IANA 指定のプロトコル番号。次に例を示します。 |
| 番号 | | • 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)

| | データタ | |
|-------|---------|--|
| フィールド | イプ | 説明 |
| 影響フラグ | bits[8] | 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。 |
| | | • 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) |
| | | 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。 |
| | | • (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 | イベントの影響フラグ値。値は次のとおりです。 |
| | | • 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)

| | データ タ | |
|-------------------------------|-----------|--|
| フィールド | 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。 |
| | | • o: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 | uint16 | パケットの発信元の VLAN の ID を示します。 |
| (Admin. VLAN ID) | | |
| 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 <i>侵</i> | スイベン | トレコード5. | .2.x のフィール | ド(続き) |
|----------------|------|---------|------------|-------|
|----------------|------|---------|------------|-------|

| | データ タ | |
|---------|---------|-------------------------------------|
| フィールド | 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 ビット | 0 1 2 3 4 5 6 7 | 1 8 9 1 1 1 1 1 1 1 1 5 8 9 5 1 1 2 3 8 5 | 2 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 3 2 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | | |
|------------|--|---|---|---|--|--|--|--|
| | 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 | | | | | | | |
| | Netm | ap 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 | 7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 | アイクロ秒 | | | | | |

| バイトビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 8 5 | 2 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 3 2 2 2 2 3 2 3 3 3 4 5 6 7 6 9 0 1 | | | | | |
|--------|------------------|-------------------------|---|-------------------------------------|--|--|--|--|--|
| | | ルール ID(ショ | | | | | | | |
| | | ジェネレ | | | | | | | |
| | ルール リビジョン | | | | | | | | |
| | | 分類 | | | | | | | |
| | | プライオ! | | | | | | | |
| | | | アドレス | | | | | | |
| | | 送信元 IP アー | | | | | | | |
| | | 送信元 IP アー | ドレス(続き) | | | | | | |
| | | 送信元 IP アー | ドレス(続き) | | | | | | |
| | <u> </u> | | | | | | | | |
| | | 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 | たは ICMP タイプ | 送信先ポートまた | こは 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 (Adm | nin. 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 | | | | | | |
| | | クライアントアフ | °リケーション ID | | | | | | |
| | | アプリケーション | / プロトコル ID | | | | | | |

| イト 0 1 | | 2 | 3 | | | |
|----------------------------|--|---|---|--|--|--|
| ット 0 1 2 3 4 5 6 7 8 9 1 1 | $\begin{array}{c cccc} 1 & 1 & 1 & 1 \\ 2 & 3 & 8 & 5 \end{array}$ | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | |
| アクセ | スコント | ロールルルID | | | | |
| アクセス | コントロー | ール ポリシー UUID | | | | |
| アクセスコン | トロール | ポリシー UUID(続 |) | | | |
| アクセスコン | アクセス コントロール ポリシー UUID(続き) | | | | | |
| アクセス コン | アクセス コントロール ポリシー UUID(続き) | | | | | |
| イン | 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 | ターフェィ | 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 | 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 | | 接続数次 | カウンタ | | | |
| 送信元の国 | | 宛先 | の国 | | | |
| IOC 番号 | | | | | | |

表 B-4 侵入イベント レコード 5.3 のフィールド

| | データ タ | |
|---------------------------|-----------|--|
| フィールド | イプ | 説明 |
| ブロック タ イプ | unint32 | 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 | unint32 | 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 | unit32 | 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。 • 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)

| 7 | データタ | 光 田 |
|----------------|---------------|--|
| フィールド 影響フラグ | イプ bits[8] | 説明 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。 |
| | | ● 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) |
| | | 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。 |
| | | • (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 | イベントの影響フラグ値。値は次のとおりです。 |
| | | ● 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)

| | データ タ | |
|-------------------------------|-----------|--|
| フィールド | 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。 |
| | | • o: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 | uint16 | パケットの発信元の VLAN の ID を示します。 |
| (Admin. VLAN ID) | | |
| 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) |
|------------------------|---------|---------------------------------------|--|
| <i>3</i> X <i>D</i> ⁻Ŧ | コヌノい・・・ | · · · · · · · · · · · · · · · · · · · | י אוייטער איינייטייטייטייטייטייטיטיטיטיטיטיטיטיטיט |

| | データ タ | |
|---------|---------|---------------------------------|
| フィールド | 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 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | ヘッダーバー | ージョン(1) | メッセージ | タイプ(4) | | |
| | | メッセ | ージ長 | | | |
| | Netma | ap ID | レコードタ | 7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 | 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | | |
| | 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 | į 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 | | | | | | |
| | | 宛先 IP アド | | | | | | |
| | | 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 (Adn | nin. VLAN ID) | パゞ | 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 アフ | プリケーション ID | | | | | |
| | | アプリケーション | ンプロトコル ID | | | | | |

| バイト | 0 | 1 | | 2 | | | 3 | | |
|-----|-----------------------|-----------------|-------|--|--|--|--|-------|--|
| ビット | 0 1 2 3 4 5 6 7 8 | 9 1 1 1 1 1 1 8 | | $\begin{bmatrix} 1 & 1 & 2 \\ 8 & 9 & 0 \end{bmatrix}$ | $\begin{bmatrix} 2 & 2 & 2 \\ 1 & 2 & 3 \end{bmatrix}$ | $\begin{bmatrix} 2 & 2 & 2 \\ 4 & 5 & 6 \end{bmatrix}$ | $\begin{bmatrix} 2 & 3 & 2 \\ 7 & 6 & 9 \end{bmatrix}$ | 3 3 1 | |
| | | アクセスコン | トロール | レルール | / ID | | | | |
| | - | アクセスコント | ロール オ | ポリシー | · UUID | | | | |
| | アク | セス コントロー | -ルポリ | シー UU | JID(続き | <u>\$</u>) | | | |
| | アク | セス コントロー | -ルポリ | シー UU | JID(続き | <u>\$</u>) | | | |
| | アク | セス コントロー | -ルポリ | シー UU | JID(続き | <u>\$</u>) | | | |
| | | インターフ | ェイス入 | 力 UUI | D | | | | |
| | | インターフェイ | ス入力 | UUID (# | 売き) | | | | |
| | | インターフェイ | ス入力 | UUID(# | 売き) | | | | |
| | インターフェイス入力 UUID(続き) | | | | | | | | |
| | | インターフ | ェイス比 | 力 UUI | D | | | | |
| | 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 UU | JID | | | | |
| | | セキュリティゾ | ーン入力 | J UUID | (続き) | | | | |
| | | セキュリティゾ | ーン入力 | J UUID | (続き) | | | | |
| | | セキュリティゾ | ーン入力 | J UUID | (続き) | | | | |
| | | セキュリティ | ゾーン | 出力 UU | JID | | | | |
| | | セキュリティゾ | ーン出力 | J UUID | (続き) | | | | |
| | | セキュリティゾ | ーン出力 | J UUID | (続き) | | | | |
| | セキュリティ ゾーン出力 UUID(続き) | | | | | | | | |
| | | 接続タク | イムスタ | ンプ | | | | | |
| | 接続インスク | アンス ID | | | 接続数プ | カウンタ | • | | |

表 B-5 侵入イベント レコード 5.1.1 のフィールド

| | データ タ | | | | |
|-----------------------|-----------|--|--|--|--|
| フィールド | イプ | 説明 | | | |
| ブロック タ イプ | unint32 | 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 | unint32 | 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 | unit32 | 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 | uint8 | IANA 指定のプロトコル番号。次に例を示します。 | | | |
| 番号 | | • 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)

| | データ タ | |
|-------|---------|--|
| フィールド | イプ | 説明 |
| 影響フラグ | bits[8] | 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。 |
| | | • 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。 |
| | | 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。 |
| | | • (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 | イベントの影響フラグ値。値は次のとおりです。 |
| | | • 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。 |
| | | • 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 | uint16 | パケットの発信元の VLAN の ID を示します。 |
| (Admin. VLAN ID) | | |
| 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 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | |
| | 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 | | | | |
| | Netm | ap ID | レコードタ | 7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 | | | | | | |
| | | イベントっ | 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 | į ID | | | | |
| | | プライオ | リティ ID | | | | |

| バイト ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 8 5 5 | 2 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 3 2 2 2 2 3 3 2 3 3 4 5 6 7 6 9 0 1 | | |
|------------|------------------------------|---------------------------|---|---|--|--|
| | 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 | こは ICMP タイプ | 送信先ポートまた | 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 | | | ノド | | |
| | 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 | | | | |
|-----|--|---|---|--|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 5 | $ \begin{array}{c c c c c c c c c c c c c c c c c c c $ | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | | |
| | 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) | | | | | |
| | インターフェィ | 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 | 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 | | | | | | |
| | 接続タイムスタンプ | | | | | | |
| | 接続インスタンス ID | 接続数划 | 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) | | | | | | |

表 B-6 侵入イベント レコード 5.3.1 のフィールド

| | データ タ | |
|---------------------------|-----------|--|
| フィールド | イプ | 説明 |
| ブロック タ イプ | unint32 | 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 | unint32 | 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) | unit32 | 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。0:IP1: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 イプ 説明 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。 ・ 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ボ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プ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。送行に設定オストは、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)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た脆弱性があります。x は、値が 0 または 1 になることを示しています。 | | データ タ | |
|--|-------|-------|---|
| す。値は次のとおりです。 | - | | 兑明 |
| でモニタされるネットワーク内にあります。 | 影響フラグ | | |
| マップ内に存在します。 | | | |
| 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)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。 | | | |
| 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)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。 | | | ト上のサーバを実行しているか(TCP または UDP の場合)、 |
| 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)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。 | | | |
| 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)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。 | | | |
| 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) 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。 | | | 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 |
| プされた脆弱性があります。 $(バージョン 5.0+ のみ)$ 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。 | | | 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 |
| 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。 | | | |
| (0. 7.111) | | - | |
| ● (0、小明):00x00000 | | | • (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 | | | • オレンジ(2、潜在的に脆弱):00x0011x |
| 黄(3、現在は脆弱でない):00x0001x | | | • 黄(3、現在は脆弱でない):00x0001x |
| ● 青(4、不明なターゲット):00x00001 | | | 青(4、不明なターゲット):00x00001 |
| 影響 uint8 イベントの影響フラグ値。値は次のとおりです。 | 影響 | uint8 | イベントの影響フラグ値。値は次のとおりです。 |
| ● 1:レッド(脆弱) | | | • 1:レッド(脆弱) |
| • 2:オレンジ(脆弱の可能性あり) | | | • 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) | | | • 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) | | | 4:ブルー(不明なターゲット) |
| • 5:グレー(不明なインパクト) | | | 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。 |
| | | • o: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 | uint16 | パケットの発信元の VLAN の ID を示します。 |
| (Admin. VLAN ID) | | |
| 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 | き) | ド(続 | ィール | のフィ | ド5.3.1 | レコー | ベント | 得入っ | 表 B-6 |
|------------------------------------|----|-----|-----|-----|--------|-----|-----|-----|-------|
|------------------------------------|----|-----|-----|-----|--------|-----|-----|-----|-------|

| | データ タ | |
|--------------|-----------|--|
| フィールド | 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | | | | |
| | 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 | | | | | | | |
| | Netma | ap 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 | | | | | | | |
|-----|------------------------------|----------------------|---|---|--|--|--|--|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | | | | | |
| | 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 | į ID | | | | | | | | |
| | | プライオ | リティ ID | | | | | | | | |
| | | 送信元 IP | アドレス | | | | | | | | |
| | | 送信元 IP アー | ドレス(続き) | | | | | | | | |
| | | 送信元 IP アー | | | | | | | | | |
| | | 送信元 IP ア l | ドレス(続き) | | | | | | | | |
| | | 宛先 IP アドレス | | | | | | | | | |
| | | 宛先 IP アド | | | | | | | | | |
| | | 宛先 IP アド 宛先 IP アド | | | | | | | | | |
| | W. I≕ → 10 1 1 1 1 1 | | | | | | | | | | |
| | 送信元ポートまた | | 送信先ポートま7 | | | | | | | | |
| | 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U | | | | | | | | | |
| | | ユーザ ID | | | | | | | | | |
| | | Web アプリケ | ーション ID | | | | | | | | |

| バイト | 0 1 2 3 | | | | | | | | | | |
|-----|---|--|--|--|--|--|--|--|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 2 3 8 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | | | | | | | | | | |
| | 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 | $9 \begin{vmatrix} 1 \\ 0 \end{vmatrix}$ | 1 | 1 1 2 3 | 1 1 8 5 | 1 1 6 7 | 1 1 8 9 | 2 0 | 2 1 | 2 2 3 | 2 4 | 2 5 6 | 2 7 | 3 2 9 | 3 3 1 |
| | 接続イン | ンスク | アンス | ID | | | 接続数カウンタ | | | | | | | | | |
| | 送 | 信元の | の国 | | | | | 3 | 宛先 | の国 | <u></u> | | | | | |
| | IC | | | セコ | ドユ | リラ | ティ | コン | /テ: | キス | , | | | | | |
| | | | セキ | 고ᆝ | リティ | コン | ノテキ | トスト | (続 | き) |) | | | | | |
| | | | セキ | 그 ! | リティ | コン | ノテキ | テスト | (続 | [き) |) | | | | | |
| | | | セキ | リティ | コン | ノテキ | テスト | (続 | [き) |) | | | | | | |
| | セキュリティ | (続き |) | , | SSL i | 正明 | 書 | フィ | ンス | ヺー こ | 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) | | | | | | | | | | | | | | | |
| | | Š | SSL 証 | 明 | 書フィ | ・ンス | ブーフ | ゜リン | ト(| 続き | き) | | | | | |
| | | S | SSL 証 | 明 | 書フィ | ・ンオ | i ーフ | ゜リン | ト(| 続き | き) | | | | | |
| | SSL 証明書フィ | 売 | | j | 実際 | の S | SSL | アク | ラシ | ョン | , | | | | | |
| | SSLフロ | | 77 | ベット | ・ワ・ | 一ク | 分析 | 斤ポ | リシ | / —] | UUII | D | | | | |
| | ネットワーク分析ポリシー UUID(続き) | | | | | | | | | | | | | | | |
| | | 析ポ | リシ | — UU | ЛD | (続 | き) | | | | | | | | | |
| | | 析ポ | リシ | — UU | ЛD | (続 | き) | | | | | | | | | |
| | ネットワーク分 | か析ポ き) | リシー | - U | UID(| 続 | | | | | | | | | | |

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

| | データ タ | |
|--------------|---------|---|
| フィールド | イプ | 説明 |
| ブロック タ イプ | unint32 | 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 | unint32 | 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)

| - | データ タ | |
|---------------------------|-----------|--|
| フィールド | イプ | 説明 |
| デバイス ID (Device ID) | unit32 | 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 | uint8 | IANA 指定のプロトコル番号。次に例を示します。 |
| 番号 | | • 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)

| | データ タ | |
|-------|---------|---|
| フィールド | イプ | 説明 |
| 影響フラグ | bits[8] | 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。 |
| | | • 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) |
| | | 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。 |
| | | 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 | イベントの影響フラグ値。値は次のとおりです。 |
| | | • 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)

| | データ タ | |
|---------------------|------------|---|
| フィールド | 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。 |
| | | • o: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 | uint16 | パケットの発信元の VLAN の ID を示します。 |
| (Admin. VLAN | | |
| ID) | | |
| 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 | uint32 | ユーザの内部 ID 番号(該当する場合)。 |
| ID) | | |
| 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 | 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 | umtsz | クノイナンドナノック・ションのPipi ID 番号(欧ヨッる物ロ)。 |
| ションID | | |
| アプリケー | 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)。 |
| ションプロト | | |
| コル ID | : | |
| アクセス コン トロール ルー | 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。 |
| ルID | | , D H 100 |
| アクセス コン | 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 |
| トロールポリ | | リシー ID 番号。 |
| <i>></i> − UUID | | |
| 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 | 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 UUID | unito[10] | フェイス ID 番号。 |
| 入力セキュリ | 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 |
| ティゾーン | | 番号。 |
| UUID | | |
| 出力セキュリ | 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 |
| ティゾーン UUID | | 番号。 |
| <u>接続タイムス</u> | 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 |
| タンプ | J. 1111.52 | ムスタンプ(1970年1月1日からの経過秒数)。 |
| 接続インスタ | 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 |
| ンス ID | | 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)

| | データ タ | |
|--------------------------|-----------|---|
| フィールド | イプ | 説明 |
| 接続数カウンタ | uint16 | 同じ秒の間に発生する接続イベントを区別するために使用される値。 |
| 送信元の国 | uint16 | 送信元ホストの国のコード。 |
| 宛先の国 | uint 16 | 宛先ホストの国のコード。 |
| IOC 番号 | uint16 | このイベントに関連付けられている侵害 ID 番号。 |
| セキュリティコンテキスト | uint8[16] | トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の ID 番号。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。 |
| SSL 証明書 フィンガープ リント | uint8[20] | SSL サーバ証明書の SHA1 ハッシュ。 |
| 実際の SSL ア クション | uint16 | SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 |

表 B-7 侵入イベント レコード 5.4.x のフィールド(続き)

| | データ タ | |
|--------------------------|-----------|--|
| フィールド | イプ | 説明 |
| SSL フロース テータス | uint16 | SSL フローのステータス。アクションが実行された理由、またはエラーメッセージが出された理由を示す値です。有効な値は次のとおりです。 |
| | | • 0:「不明」 |
| | | • 1:「一致しない」 |
| | | • 2:「成功」 |
| | | • 3:「キャッシュされていないセッション」 |
| | | • 4:「不明の暗号化スイート」 |
| | | 5:「サポートされていない暗号スイート」 |
| | | • 6:「サポートされていない SSL バージョン」 |
| | | 7:「使用される SSL 圧縮」 |
| | | • 8:「パッシブ モードで復号不可のセッション」 |
| | | • 9:「ハンドシェイク エラー」 |
| | | • 10:「復号エラー」 |
| | | • 11:「保留中のサーバ名カテゴリ 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の標準レコードへッダーを使用し、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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | 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 | | | |
| | Netma | ap ID | レコード | タイプ(9) | | |
| | | レコー | - ド長 | | | |
| | | 侵入影響アラートフ | [*] 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) | | | | | |
| DL91 | 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

| | データ タ | |
|-----------------------|--------|--|
| フィールド | 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)

| 7 1. 15 | データタ | ⇒ X µ⊓ |
|----------------|---------------|--|
| フィールド 影響 | イプ bits[8] | 説明 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 |
| 必管 | onstol | ます。値は次のとおりです。 |
| | | • 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) |
| | | 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。 |
| | | • (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 o 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 o 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 | ィー <i>ルド(続き</i>) |
|---------------------|-------------------|
|---------------------|-------------------|

| | データ タ | |
|----------|--------|--|
| フィールド | 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。 |

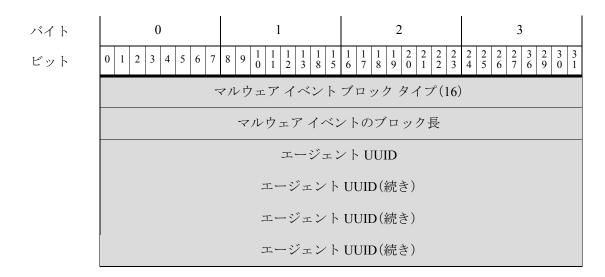
レガシーマルウェアイベントのデータ構造

- 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 2 2 6 7 8 9 0 1 2 3 4 5 | 2 2 3 2 3 3 6 7 6 9 0 1 |
| | | クラウ | F UUID | |
| | | クラウドU | TUID(続き) | |
| | | クラウドU | UID(続き) | |
| | | クラウドU | UID(続き) | |
| | | Times | stamp | |
| | | 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 | 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 | | | |
| 7-71 | ファイル パス 文字列ブロック タイプ(0) | | | |
| ファイル SHA ハッシュ | 文字列プロック タイプ(0) | | | |
| | ステゲリノロック 反 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 | ァイルのタイムスタンプ | |

| バイト | 0 | 1 | 2 | 3 |
|--------------------|-----------------------|---------------------|--------------------------------------|----------------------------------|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 3 3 4 5 6 7 6 9 0 1 |
| 親ファイル [名前(Name) | ファイルのタイム スタンプ(続き) | 文气 | 字列ブロック タイプ | (0) |
| J | 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 | | | クタイプ(0) | |
| シュ | | 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) | | | |
| 100.91 | 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 o 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 o 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 o 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 o 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 o です。 |

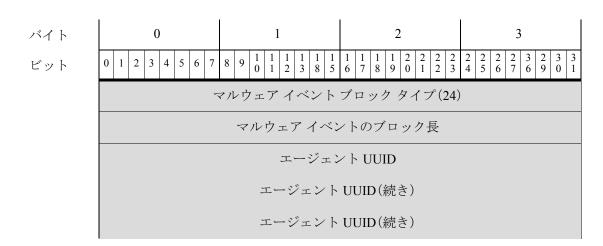
| 表 B-9 | マルワェア イベント テータ フロックのフィールド(続き) |
|-------|-------------------------------|
| | |

| 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 o 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 | | |
|---------------------|-----------------------------|-------------------------|---|--|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 2 3 3 3 6 7 8 9 0 1 2 3 4 5 6 7 6 9 0 1 | | |
| | エージェント UUID(続き) | | | | |
| | | クラウド UUID | | | |
| | | クラウドU | UID(続き) | | |
| | | クラウドU | UID(続き) | | |
| | | クラウド U | UID(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 | 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 | | | |
| | 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 | | | |
| | | ファイル SHA ファイル サイ | | | |
| | | ファイルリイ | (File Size) | | |

| バイト | 0 | 1 | 2 | 3 |
|--------------------|------------------------|-----------------------|---|---|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | ファイル タイプ | ファ | マイルのタイムスタン | ノプ |
| 親ファイル [名前(Name) | ファイルのタイム スタンプ(続き) | 文气 | 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 | | 文字列ブロッ | クタイプ(0) | |
| シュ | | 文字列ブ | ロック長 | |
| | | 親ファイル SF | IA ハッシュ | |
| イベント 説明 | | 文字列ブロッ | ク タイプ(0) | |
| 100.71 | | 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 | | | |
| | 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 (Applic | ation 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 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| | ユーザ ID(続き) | アクセス | コントロール ポリシ | — UUID | |
| | <i>P</i> : | クセス コントロール | ポリシー UUID(続き | <u>(</u>) | |
| | ア: | アクセス コントロール ポリシー UUID(続き) | | | |
| | <i>T</i> : | クセス コントロール | ポリシー UUID(続き | <u>(</u>) | |
| 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 | | | 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 o 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 o 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 o 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 o 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 o 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 o 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。 |
| | | • 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 | 7 5.1.1.x のフィ | 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。 |
| | | • 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 | | |
|-----------|---|------------|----------|-----------|--|--|
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 2 3 8 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 2 3 4 5 6 7 6 9 | | | | | |
| | 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 | 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U | IUID(続き) | | | |
| | | クラウドU | IUID(続き) | | | |
| | | クラウドU | IUID(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 | ック タイプ(0) | | |
| | 文字列ブロック | タイプ(0)(続き) | 文字列フ | 「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) | | | |
| | | | ロック長 | | | |
| | | ファイバ | レパス | | | |

| バイト | 0 | 1 | 2 | 3 | |
|--------------------|----------------------------|-----------------------|------------------------------------|----------------------------------|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 3 3 4 5 6 7 6 9 0 1 | |
| ファイル SHA | 文字列ブロック タイプ(0) | | | | |
| ハッシュ | | 文字列ブ | ロック長 | | |
| | | ファイル SH | Aハッシュ | | |
| 1 | | ファイル サイ | イズ(File size) | | |
| | | ファイバ | レタイプ | | |
| | | 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) | | |
| [治前(Name) | | 文字列ブ | `ロック長 | | |
| | | 親ファ | イル名 | | |
| 親ファイル SHA ハッ | 文字列ブロック タイプ(0) 文字列ブロック長 | | | | |
| シュ | | | | | |
| | | 親ファイル SI | HA ハッシュ | | |
| イベント 説明 | 文字列ブロック タイプ(0) | | | | |
| μ)L 1/21 | 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 | | | 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | | 宛先 IP アド | `レス(続き) | |
| | | 宛先 IP アド | `レス(続き) | |
| | | 宛先 IP アド | ンス(続き) | |
| | 宛先 IP(続き) | アプリケ | ーション ID(Applic | ation 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 | /— UUID |
| | P | 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 | | | |
| | | クライアントアフ | 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 | uint32 | マルウェア イベント データ ブロックを開始します。こ |
| トブロック タイプ | | の値は常に 33 です。 |
| マルウェア イベン | 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 |
| トのブロック長 | | (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 o 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 o 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 o 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 o 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 o 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 o 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。 |
| | | • 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。 |
| | | • 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 o 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。 |

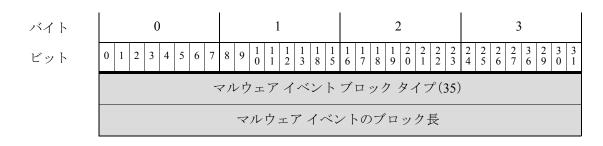
| フィールド | データ タイプ | 説明 |
|------------------------|---------|--|
| Web アプリケーション ID | uint32 | 専用 Web アプリケーションの内部 ID 番号(該当する場合)。 |
| クライアント アプ リケーション ID | uint32 | 専用クライアント アプリケーションの内部 ID 番号(該当する場合)。 |
| 操作 | uint8 | ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 |
| | | • 1:検出 |
| | | • 2:ブロック |
| | | • 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。 |
| | | • 1:ICMP |
| | | • 4:IP |
| | | • 6:TCP |
| | | • 17:UDP |
| | | これは現時点では TCP のみです。 |

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)

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。



| S 2 1 | 0 | 1 | 2 | 3 | | | | | | |
|-----------|-----------------------|-------------|---|-----------------------------------|--|--|--|--|--|--|
| バイト | | | | | | | | | | |
| ビット | 0 1 2 3 4 5 6 7 | | 1 1 1 1 2 2 2 2 3 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 3 4 5 6 7 6 9 0 1 | | | | | | |
| | 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 | F UUID | | | | | | | |
| | | クラウドU | UID(続き) | | | | | | | |
| | | クラウドU | UID(続き) | | | | | | | |
| | | クラウドU | UID(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 | 文气 | 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(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 | レパス | | | | | | | |
| L | | | | | | | | | | |

| バイト | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 8 5 | 2 1 1 1 1 2 2 2 2 2 2 2 6 7 8 9 0 1 2 3 2 | 3 2 2 2 2 3 2 3 3 3 4 5 6 7 6 9 0 1 | | | | | | | | |
|--------------------|---|-------------------------|--|---|--|--|--|--|--|--|--|--|
| ビット ファイル SHA | 0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 | | | | | | | | | | | |
| ハッシュ | 文字列ブロック長 | | | | | | | | | | | |
| | ファイル SHA ハッシュ | | | | | | | | | | | |
| | | ファイル サー | イズ(File size) | | | | | | | | | |
| | | ファイバ | レタイプ | | | | | | | | | |
| | | 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 | | | | | | | | | |
| | | 親ファー | イル名 | | | | | | | | | |
| 親ファイル SHA ハッ | | 文字列ブロッ | クタイプ(0) | | | | | | | | | |
| シュ | 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) | | | | | | | | | |
| W271 | | 文字列プ | ロック長 | | | | | | | | | |
| | | イベント | の説明 | | | | | | | | | |
| | | Devi | ce 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 | 1 0 | 1 1 1 2 | 1 3 | 1 1 8 5 | 16 | 1 7 | 1 1 8 9 | 2 0 | 2 2 1 2 | 2 3 | 2 2 4 5 | 2 | 2 6 2 7 | 3 6 | 2 9 | 3 | 3 |
| | 送信元 IP(続き) | | | 宛先 IP アドレス | | | | | | | | | | | | | | | | | | |
| | | | | | | | 宛先 | i IP | アド | ン | ス | (続き | :) | | | | | | | | | |
| | | | | | | | 宛先 | i IP | アド | ン | ス | (続き | :) | | | | | | | | | |
| | | | | | | | 宛先 | E IP | アド | ン | ス | (続き | :) | | | | | | | | | |
| | 宛先] | P(続 | き) | | | | , | アフ | ゜リク | | シ | ョン | ID | (App | olica | ation | II | D) | | | | |
| | アプリケーショ ン ID(続き) | | | | | | | | | ユ | _ | ザ ID |)(U | ser I | D) | | | | | | | |
| | ユーザ ID(続き) | | | | | | ア | 7ク* | セス | コ | ン | トロ・ | — <i>)</i> 1 | ノポ | リシ | √— [| Д | JID | | | | |
| | | ウセス コントロール ポリシー UUID(続き) | | | | | | | | | | | | | | | | | | | | |
| | | 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 | トロティン | ス・ ブ傾 | ペク j向 | 文字列ブロック タイプ(0) | | | | ク | | | |
| | 文字列 | | | | | ブロック タイプ(0)(続き) | | | | | | 文字列ブロック長 | | | | | į | | | | | |
| | 文字列ブロック長(続き) | | | | | | | | | | UF | RΙ | | | | | | | | | | |
| | 送信元ポート(Sour | | | | | | (Source Port) 接続先 | | | | | | | | 先 | ミポート | | | | | | |
| | 送信元 | | | | | 元の国 宛先の国 | | | | | | | | の国 | D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 | | | | | | | | | | | | | | | | |
| | 1 | 操作 | | | | プロ | 1 | コル | | | 7 | 尊威 ニ | スコ | ア | | |] | IOC | 番- | 号 | | |
| | IOC 番 | 号(約 | 売き) | | | | | | | | | | | | | | | | | | | |

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 o 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-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 o 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 o 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 o 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。 |
| | | • 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。 |
| | | • 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 o 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。 |
| | | • 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。 |
| | | • 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(o ~ 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 1 1 1 1 1 1 8 | 1 1 1 1 5 6 7 8 | 1 2 2 2 2 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| | 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UU | ID | | |
| | | 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 | 1 | | |
| | | クラウト | ドUUID(続 | (き) | | |
| | | クラウト | ドUUID(続 | き) | | |
| | | クラウト | ドUUID(続 | (き) | | |
| | | マルウェアイベ | シト タイ | ムスタンプ | | |
| | | イベント タイプ ID | | | | |
| | | イベント | サブタイプ | プID | | |
| 検出名 | ディテクタ ID | | 文字列ブロ | ュック 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) | | | | | |
| 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 | 1ック タイ | プ(0) | | |
| | | 文字列 | ブロック: | Ę | | |
| | | ファ | ・イル名 | | | |

| バイト | 0 | 1 | 2 3 | | |
|--------------------|--|---------------------|---|-----|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 8 | 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 2 3 5 6 7 8 9 0 1 2 3 4 5 6 7 6 9 0 | 3 3 | |
| 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 | | 文字列ブロッ | ック タイプ(0) | | |
| ハッシュ | | 文字列ス | ブロック長 | | |
| | | ファイル SI | HA 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 | タイムスタンプ | | |
| 親ファイル [名前(Name) | | 文字列ブロッ | 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 | | 文字列ブロッ | ック タイプ(0) | | |
| シュ | 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 | ック タイプ(0) | | |
| 100.01 | | 文字列フ | 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 | 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 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | 送信元 IP(続き) | 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(Applica | ation 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 | — UUID |
| | <i>P</i> : | クセス コントロール | ポリシー UUID(続き | ž) |
| | <i>P</i> : | クセス コントロール | ポリシー UUID(続き | <u>(</u> |
| | P : | クセス コントロール | ポリシー UUID(続き | ٤) |
| 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 | この国 | 宛先 | の国 |
| | | Web アプリケ | ーションID | |
| | | クライアント アフ | 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 | 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 <i>コン</i> 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。 |
| | | • 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。 |
| | | • 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。 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。 • 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 $(0\sim100)$ 。 | | |
| 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| | 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 | ノトのブロック長 | | |
| | | エージェン | ノト 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 | F UUID | | |
| | | クラウドU | UID(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 | |
|--------------------|---------------------|-----------------------|---|---|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| 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 | ノパス | | |
| ファイル SHA | | 文字列ブロッ | ク タイプ(0) | | |
| ハッシュ | 文字列ブロック長 | | | | |
| | | ファイル SHA | A ハッシュ | | |
| | ファイル サイズ(File size) | | | | |
| | ファイルタイプ | | | | |
| | | ファイルのター | 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 | イル名 | | |
| 親ファイル SHA ハッ | 文字列ブロック タイプ(0) | | | | |
| シュ | | 文字列ブ | ロック長 | | |
| | | 親ファイル SH | IA ハッシュ | | |
| イベント 説明 | 文字列ブロック タイプ(0) | | | | |
| 10001 | | 文字列ブ | ロック長 | | |
| | | イベント | の説明 | | |
| | | デバイス ID | (Device ID) | | |

| | 1 | ı | I | 1 1 |
|-----|-------------------------------------|-----------------------|---|---|
| バイト | 0 | 1 | 2 | 3 |
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | 接続イン | スタンス | 接続数分 | カウンタ |
| | | 接続イベント | タイムスタンプ | |
| | 方向(Direction) | | 送信元 IP アドレス | |
| | | 送信元 IP ア | ドレス(続き) | |
| | | 送信元 IP ア | ドレス(続き) | |
| | | 送信元 IP ア | ドレス(続き) | |
| | 送信元 IP(続き) | | 宛先 IP アドレス | |
| | | 宛先 IP アト | シンス(続き) | |
| | | 宛先 IP アト | シンス(続き) | |
| | | 宛先 IP アト | ンス(続き) | |
| | 宛先 IP(続き) | アプリケ | アーション ID(Applica | ation 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 | ∕ — UUID |
| | ア: | ウセス コントロール | ポリシー UUID(続き | <u>*</u>) |
| | <i>T</i> : | クセス コントロール | ポリシー UUID(続き | き) |
| | <i>P</i> : | クセス コントロール | ポリシー UUID(続き | 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 | <u>\$</u>) | URI |
| | 送信元ポート | (Source Port) | 接続先 | ポート |
| | 送信元 | この国 | 宛先 | の国 |
| | Web アプリケーション ID | | | |
| | | クライアントアコ | プリケーション ID | |
| | | | | |

| バイト | 0 | 1 | 2 | 3 |
|--------------|------------------------------|-----------------------|--------------------------------------|------------------------------------|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | 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 | < |
| | | 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 訂 | E明書フィンガープリ | ント |
| | | SSL 証明書フィンス | ブープリント(続き) | |
| | | SSL 証明書フィンス | ブープリント(続き) | |
| | | SSL 証明書フィンス | ブープリント(続き) | |
| | | SSL 証明書フィンス | ブープリント(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) | 文气 | 字列ブロック タイプ (| (0) |
| | 文字列ブロック タイプ(続き) | 文写 | 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 | |
| | | アーカィ | 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 o 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 o 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 o 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 o 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 o 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 o 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。 | |
| | | • 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。 | |
| | | • 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 o 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。 | |
| | | • 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。 | |
| | | • 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 $(0\sim100)$ 。 | |
| 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。 |
| | | • 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 |
|---|-------------------|---|
| フィールド SSL フロー ステー タス | データ タイプ uint16 | SSL フローのステータス。アクションが実行された理由、またはエラーメッセージが出された理由を示す値です。有効な値は次のとおりです。 ・ 0:「不明」 ・ 1:「一致しない」 ・ 2:「成功」 ・ 3:「キャッシュされていないセッション」 ・ 4:「不明の暗号化スイート」 ・ 5:「サポートされていない暗号スイート」 ・ 6:「サポートされていない SSL バージョン」 ・ 7:「使用される SSL 圧縮」 ・ 8:「パッシブ モードで復号不可のセッション」 ・ 9:「ハンドシェイク エラー」 ・ 10:「復号エラー」 |
| | | 11:「保留中のサーバ名カテゴリ 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」 |
| - - - - - - - - - - - - - - - - - - - | uint22 | 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 | 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 o です。 |

| 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 o 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。 |

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)

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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | ヘッダーバ | ージョン(1) | メッセージ | ジタイプ(4) |
| | メッセージ長 | | | |
| | Netma | ap ID | レコート | ドタイプ |
| | | レコー | ード長 | |
| | eStreamer サーバク | 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 | Device ID | | | |
| ヘッダー | [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。 |

| 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] | ο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。 |

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

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。

用のためのものであり、無視してかまいません。

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)

レガシー サーバ データ ブロック

ファイル番号

ファイルの位置

詳細については、次の項を参照してください。

byte[4]

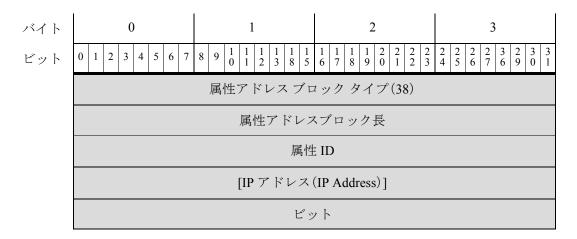
byte[4]

• 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 $5.0 \sim 5.1.1.x$

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。

• $a-m \neq 0$

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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | ユーザク | ライアント アプリケ | ーション ブロック タ | 7イプ(59) |
| | ユーナ | ザ <i>クライアント</i> アプ | リケーションブロッ | ク長 |
| [IP アドレス (IP Address)] | | 汎用リストブロ | ック タイプ(31) | |
| 範囲 | | 汎用リスト | ブロック長 | |
| | | IP 範囲仕様デー | 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 | uint32 | ユーザ クライアント アプリケーション データ ブロックを開始します。この値は常にです。 |
| ロック タイプ | | |
| 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 <i>ブ</i> 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 o 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 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| | | スキャン結果ブロ | ック タイプ (102) | | |
| | | スキャン結果 | 見 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)] | プロー | ヘコル | |
| | 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 | コック タイプ(109) | |
| | スキャン脆弱性ブロ | ュック タイプ (109) | スキャン脆弱 | 性ブロック長 | |
| | スキャン脆弱 | 性ブロック長 | 脆弱性が | データ | |
| | リストブロック タイプ(11) | | | 汎用スキャン 結果リスト | |
| | | リストブ | ロック長 | | ルロント ノ / ・ 「 |
| 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 | | | | |
| | | 汎用スキュ | アン結果… | | |

| バイト | 0 | 1 | 2 | 3 |
|--------------------|-----------------|---------------------|---|---|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| ユーザ(User) 製品リスト | | 汎用リストブロ | ック タイプ(31) | |
| 表面ノハト | | 汎用リスト | ブロック長 | |
| | | ユーザ製品デー | 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

| | データ タ | |
|---------------------------|--------|---|
| フィールド | イプ | 説明 |
| スキャン結果 | 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 |
| ブロック タ イプ | | です。 |
| | 1 | |
| 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 |
| 7 - 7 7 K | | キャン脆弱性データのバイト数を含む)。 |
| ユーザ ID (User | 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 |
| ID) | | 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 | uint32 | 結果がシステムに追加された方法を示します。 |
| イプ | | |
| [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。 |
| | uint16 | |
| [ポート(Port)] | | 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。 |
| | | • 1:ICMP |
| | | • 4:IP |
| | | • 6:TCP |
| | | • 17:UDP |
| フラグ(Flag) | uint16 | 予約済 |
| リストブロッ | 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 |
| ク タイプ | | 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 | 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 |
| ク長 | | 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)

| | データ タ | |
|-------------------------|------------------|---|
| フィールド | 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、 $5.0 \sim 5.0.x$ 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 1 1 1 1 1 1 1 8 | 1 1 1 1 1 2 2 2 5 6 7 8 9 0 1 2 | 2 2 2 2 2 3 2 3 3 3 4 5 6 7 6 9 0 1 | | |
| | コ | 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 | スタイプ | | | |
| [IP アドレス (IP Address)] | | 汎用リストブロ | ュック タイプ(31) | | | |
| 範囲 | | 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)] | プリ | ロトコル | | |
| | | ドロップ | ユーザ製品 | | | |
| カスタム (Custom) | 文字列ブロック タイプ(0) | | | | | |
| ベンダー文 字列 | 文字列ブロック長 | | | | | |
| | | カスタムべい | ンダー文字列 | | | |
| カスタム (Custom) | | 文字列ブロッ | ック タイプ(0) | | | |
| 製品文字列 | 文字列ブロック長 | | | | | |
| | | カスタム | 製品文字列 | | | |
| カスタム (Custom) | | 文字列ブロッ | ック タイプ(0) | | | |
| バージョン 文字列 | | 文字列フ | 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 | | | |
|---------------|---|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 2 3 8 5 6 7 8 9 0 1 3 3 3 3 1 | | | |
| | 製品 ID | | | |
| メジャー | 文字列ブロック タイプ(0) | | | |
| バージョン 文字列 | 文字列ブロック長 | | | |
| | メジャー バージョン文字列 | | | |
| マイナー | 文字列ブロック タイプ(0) | | | |
| バージョン 文字列 | 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 | 文字列ブロック タイプ(0) | | | |
| 文字列 | 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) | | | |
| 文子勿 | 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) | | | |
| 大子グ! | 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) | | | |
| 大子グ! | 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 |
|-------------|-----------------|---------------------|---|---|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| 内線番号 文字列 | | 文字列ブロッ | クタイプ(0) | |
| 7194 | | 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 | 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

| | データ タ | |
|-------------|------------|---|
| フィールド | イプ | 説明 |
| ユーザ製品デー | 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 |
| タブロックタ | | 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。 |
| <u>イプ</u> | | |
| ユーザ製品ブ | 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 |
| ロック長 | | 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 | 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* |
| ロック タイプ | | 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 | 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 |
| ロック長 | | 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 | 変数 | 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 |
| タ ブロック* | (variable) | 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)

| | データ タ | |
|----------------|--------|---|
| フィールド | 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。 |
| | | • 1:ICMP |
| | | • 4:IP |
| | | • 6:TCP |
| | | • 17:UDP |
| ドロップ ユーザ | 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: |
| 製品 | | • 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 o です。 |
| 文字列ブロッ ク長 | uint32 | カスタムベンダー文字列データブロックのバイト数(ブロックタイプと長さのフィールド用の8バイト、およびベンダー名のバイト数を含む)。 |
| カスタム ベン ダー名 | string | ユーザ入力で指定されたカスタム ベンダー名。 |
| 文字列ブロック タイプ | uint32 | ユーザ入力に指定されたカスタム製品名を含む文字列データ ブロックを開始します。この値は常に o 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 o 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リ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)

| | データ タ | | | | |
|----------------|--------|--|--|--|--|
| フィールド | 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 o 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 o 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)

| | データ タ | | | | |
|----------------|--------|---|--|--|--|
| フィールド | 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 o 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 o 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)。 | | | |

| | データ タ | | | | |
|--------------------|------------------|---|--|--|--|
| フィールド | 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。 | | | |

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)

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。

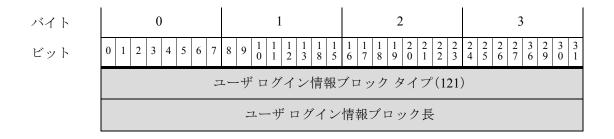
- ユーザ ログイン情報データ ブロック 5.0 ~ 5.0.2(B-106 ページ)
- ユーザ ログイン情報データ ブロック 5.1 ~ 5.4.x(B-108 ページ)
- ユーザ ログイン情報データ ブロック 6.0.x(B-110 ページ)
- ユーザ ログイン情報データ ブロック 6.1.x(B-114 ページ)
- ユーザ情報データ ブロック 5.x(B-121 ページ)

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 $5.0 \sim 5.0.2$ 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 1 1 2 3 8 5 6 7 8 9 0 1 3 2 3 8 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 2 3 4 5 6 7 6 9 0 1 | | | |
| | Timestamp | | | |
| | [IP アドレス (IP Address)] | | | |
| ユーザ (User) | 文字列ブロック タイプ(0) | | | |
| [名前(Name)] | 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

| | データ タ | | | | |
|-----------------|----------|--|--|--|--|
| フィールド | イプ | 説明 | | | |
| ユーザ ログイン | 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、 | | | |
| 情報ブロック タ イプ | | バージョン $5.0 \sim 5.0.2$ の場合は 121 です。 | | | |
| 17 | | | | | |
| 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 | 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 | | | |
| Address)] | | 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 | string | ユーザのユーザ名。 | | | |
| (Username)] | | | | | |
| ユーザ ID(User | uint32 | ユーザの ID 番号。 | | | |
| ID) | | | | | |

| 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) |
|--------|---|
| | |

| | データ タ | |
|-------------------------------------|--------|--|
| フィールド | 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 o 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 $4.7 \sim 4.10.x$ の場合はブロック タイプ 73、バージョン $5.0 \sim 5.0.2$ 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 $5.1 \sim 5.4.x$ 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 | |
|-----------------------------|--|---------------------|---|---|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| | ユーザ ログイン情報ブロック タイプ(127) | | | | |
| | 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) | | | | |
| [治前(Name) | 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) | | | | | |

| バイト | 0 | 1 | 2 | 3 |
|--------|-----------------------|---|------------|-----|
| ビット | 0 1 2 3 4 5 6 7 | 0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 | | |
| 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 | 文章 | 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 | |

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

| | データ タ | |
|---------------------------|--------|--|
| フィールド | 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 o 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。 |

| - | | |
|--------------------------------|-----------|--|
| | データ タ | |
| フィールド | 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 o 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 o 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。 |

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)

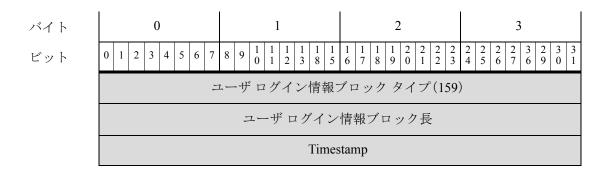
ユーザ ログイン情報データ ブロック 6.0.x

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 $4.7 \sim 4.10.x$ の場合はブロック タイプ 73、バージョン $5.0 \sim 5.0.2$ 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 $5.1 \sim 5.4.x$ (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 1 1 2 3 8 5 6 7 8 9 0 1 3 2 3 8 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 | | | |
| | IPv4 アドレス (IPv4 Address) | | | |
| ユーザ (User) | 文字列ブロック タイプ(0) | | | |
| [名前(Name)] | 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 |
|--------|-----------------|---------------------|---|------------------------------------|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| 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 | 卜基準 |

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

| | データ タ | |
|----------------------------|--------|--|
| フィールド | イプ | 説明 |
| ユーザ ログイン情 | 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 |
| 報ブロック タイプ | | 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。 |
| | | 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 o 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 | string | ユーザのユーザ名。 |
| (Username)] | | |
| 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 o 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 | 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 |
| ロファイル ID | | 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)

| | データ タ | |
|-----------------------------------|-----------|--|
| フィールド | 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。 • 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 o 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。 • 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 o 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 3 3 4 5 6 7 6 9 0 1 | |
| | 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) | | 文字列ブロッ | ク タイプ(0) | | |
| [名前(Name)] | | 文字列ブ | ロック長 | | |
| | | ユーナ | デ名 | | |
| 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 | | | | |
| | 開始才 | ☆ 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 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | | 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 IPvo | 5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 | ック長(続き) | レポー | 卜基準 |

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

| | データタ | TV PIT |
|---------------------------|--------|---|
| フィールド | イプ | 説明 |
| ユーザ ログイン情 | 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 |
| 報ブロック タイプ | | 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 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 o 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)

| | データ タ | |
|----------------------------------|-----------------------------|--|
| フィールド | イプ | 説明 |
| [ユーザ名 | string | ユーザのユーザ名。 |
| (Username)] | | |
| 文字列ブロック タ | 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 |
| イプ | | 値は常にっです。 |
| 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 [ポート(Port)] 範囲の開始 開始ポート | uint32 uint16 uint16 uint16 | 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。 • 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 ユーザを検出したポート番号。 TS エージェントが使用するポート範囲の開始ポート 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 o 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。 |

| | データタ | |
|-----------------------|-----------|--|
| フィールド | イプ | 説明 |
| ロケーション IPv6 | 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 |
| アドレス | | 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 | uint8 | ユーザが使用する認証のタイプ。値は次のとおりです。 |
| (Authentication Type) | | • o:認証は不要 |
| Type) | | • 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 o 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。 |

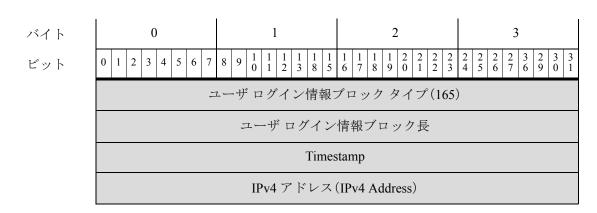
表 B-23 ユーザ ログイン情報データ ブロックのフィールド(続き)

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 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 3 8 5 6 7 8 9 0 1 2 3 2 2 2 2 2 2 2 2 2 2 2 3 4 5 6 7 6 9 0 1 | | | | | | |
| 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 | | | | | | |
| | ユーサ | デ名 | | | | | |
| 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 | ۵ 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)] | [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 | 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 IPve | 5アドレス(続き) | | | | | |
| | ロケーション IPv6 ロケーション IPv6 | | | | | | |

| バイト | 0 | 1 | 2 | 3 | |
|--------|--------------------|-----------------------|---|------------------------------------|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| 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 | 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 | 月 | | |

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

| | データ タ | |
|---------------------------|--------|--|
| フィールド | 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 o 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)

| | データ タ | |
|---------------------|-----------|---|
| フィールド | 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。 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 o 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。 |

| | データタ | ⇒¥ n□ |
|--------------------------|--------|--|
| フィールド | イプ | 説明 |
| 認証タイプ (Authentication | uint8 | ユーザが使用する認証のタイプ。値は次のとおりです。 |
| Type) | | • 0:認証は不要 |
| Турс | | • 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 o 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。 |

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)

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、 $4.7 \sim 4.10.x$ 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 15 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 | | | | |
|------------------------|---|--|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 | | | | |
| | ユーザ情報ブロック タイプ (75 120) | | | | |
| | ユーザ情報ブロック長 | | | | |
| | ユーザ ID (User ID) | | | | |
| ユーザ(User) [名前(Name) | 文字列ブロック タイプ(0) | | | | |
| [And (Name) | 文字列ブロック長 | | | | |
| | ユーザ名 | | | | |
| | プロトコル | | | | |

| バイト | 0 | 1 | 2 | 3 | |
|---------------------|-----------------|---------------------|---|----------------------------------|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 3 3 4 5 6 7 6 9 0 1 | |
| 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) | | |
| [A HI (Name) | | 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) | | |
| (Department) | 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 | | |
| | | 電記 | 括 | | |

表 B-25 ユーザ情報データ ブロックのフィールド

| | データ タ | |
|-------------------|--------|--|
| フィールド | 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 $4.7 \sim 4.10.x$ 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 o 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)

| | データ タ | |
|---------------------|--------|--|
| フィールド | 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 | string | ユーザのユーザ名。 |
| (Username)] | | |
| 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 o 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 | 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 |
| イプ | | 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 o 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 o 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 o 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 $5.0 \sim 5.0.2$ 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。



<u>(注)</u>

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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | ž | 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 | ック タイプ(続き) | 汎用リスト | ブロック長 |
| | 汎用リストブロ | ュック長(続き) | サーバ フィンガー: | |
| クライアント フィンガープ | | 汎用リストブロ | ック タイプ(31) | |
| リント | | 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 | 汎用リストブロック タイプ(31) | | | |
| プリント | 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 | 汎用リスト ブロック タイプ(31) 汎用リスト ブロック長 | | | |
| フィンガー プリント | | | | |
| | DI | HCP フィンガープリ | ントデータ ブロック | * |

| バイト ビット | 0 1 2 3 0 1 2 3 4 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 2 3 4 5 6 7 6 9 0 1 | |
|----------------------|---|-----------------|
| | リストブロック タイプ(11) | TCP サーバ |
| | リストブロック長 | のリスト |
| TCP サーバ | サーバブロック タイプ(36) | |
| ブロック* | 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 | 0) y A F |
| 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 |
| | リストブロック長 | ルのリスト |
| ネットワークプロトコルブ | プロトコルブロック タイプ(4)* | |
| ロック* | 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 |
| | リストブロック長 | トコルのリスト |
| トランスポート | プロトコル ブロック タイプ(4)* | |
| (Transport) プロトコル | プロトコルブロック長 | |
| ブロック* | トランスポート プロトコル データ | |

| バイト ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 8 5 | 2 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 3 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
|-------------------------|--|-------------------------------|---|---|------------------------|
| | | 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 | | 7, 0, 7, 7, T |
| MAC アドレ | | MAC アドレス ブロ | ュック タイプ (95)* | | |
| 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 | 寺のホスト | | |
| | | ホスト | タイプ | | |
| | VLAN の有無 | VLAN ID (Adr | nin. VLAN ID) | VLAN タイプ | |
| | VLAN 優先順位 | VLAN 優先順位 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) | V | l用リスト ブロック♪ | Ē | ト アプリ ケーション のリスト |
| クライアン ト アプリ ケーション | 汎用リストブ ロック長(続き) | クライアントアフ | プリケーション ブロ _う | ック タイプ (112)* | |
| データ | 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 | ノト アプリケーション | ノデータ | |
| NetBIOS [名前(Name) | | | | | |
| | | | | | |
| | | | | | |

次の表は、バージョン $4.9 \sim 5.0.2$ 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 $5.0 \sim 5.0.2$ のフィールド

| フィールド | データ タ イプ | 説明 | | |
|--|------------------|--|--|--|
| ホスト プロファ イル ブロック タイプ | uint32 | ホスト プロファイル データ ブロック 4.9 ~ 5.0.2 を開始します。このデータ ブロックのブロック タイプは 91 です。 | | |
| ホスト プロファ イル ブロック長 | uint32 | ホスト プロファイル データ ブロックのバイト数(ホスト プロファイル ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続くホスト プロファイル データに含まれるバイト数を含む)。 | | |
| [IP アドレス(IP Address)] | uint8[4] | IP アドレス オクテットの、プロファイルに記述されているホストの IP アドレス。 | | |
| ホップ | uint8 | ホストからのデバイスまでのホップ数。 | | |
| プライマリ/セ カンダリ | uint8 | ホストがそれを検出したデバイスのプライマリまたはセカンダ リのどちらのネットワークにあるかを示します。 | | |
| | | • o: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5.0~5.0.2 (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 | 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5.0 ~ 5.0.2(B-131 ページ)を参照してください。 | | |

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

| フィールド | データ タ イプ | 説明 | | |
|--|------------------|---|--|--|
| 汎用リスト <i>ブ</i> 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 | OHCP 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 $ホストプロファイルデータブロック 5.0 \sim 5.0.2 のフィールド(続き)$

| | データ タ | | |
|----------------------|------------------|--|--|
| フィールド | 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 $ホスト プロファイル データ ブロック 5.0 \sim 5.0.2 のフィールド(続き)$

| | データ タ | | | |
|--------------------------------|------------------|--|--|--|
| フィールド | 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。 | | |
| VLAN の有無 | uint8 | VLAN が存在するかどうかを示します。o: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)。 | | |

| | データ タ | |
|---------------------------------|------------------|---|
| フィールド | 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 o 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。 |

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)

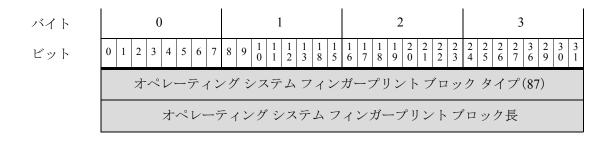
レガシー **OS** フィンガープリント データ ブロック

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 $5.0 \sim 5.0.2$ 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 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| OS フィン ガープリント | | フィンガープ | リント UUID | |
| 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

| | データ タ | |
|---|-----------|--|
| フィールド | 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。 |

| | データ タ | |
|-----------|--------|--|
| フィールド | イプ | 説明 |
| フィンガープリ | 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 |
| ント ソース ID | | 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。 |

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)

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 $5.0 \sim 5.0.2$ 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。

| | | | I I | | | |
|-----|---------------------------------------|---|---|--|--|--|
| バイト | 0 1 | 2 | 3 | | | |
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | |
| | 接続データブロッ | 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 | 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 | 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 I | Pアドレス | | | | |
| | レスポンダ IP ア | 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | | レスポンダ IP : | アドレス(続き) | |
| | | レスポンダ 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 | レスポン | ダ ポート |
| | TCP 7 | 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) | |
| | 1 | NetFlow ソース(続き) |) | 最初のパケット の時刻 |
| | 最初のパク | ァ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) | |
| | Ţ | 送信パケット数(続き |) | 受信パケット数 |
| | | 受信パケッ | | |
| | 5 | を信パケット数(続き | | 送信バイト数 |
| | T. | 送信バイ | .,, , | 五二、八十里。 |
| | Ž | を信パケット数(続き 受信バイ) | | 受信バイト数 |
| | | · 交信バイト数(続き) | SX (NYL C) | 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 1 1 1 1 1 1 1 1 1 1 1 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | 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 | 文字列ブロック タイプ(続き) | 文字列ブロック長 | | |
| ションURL | 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 | 文字列ブロック タイプ(0) | | | |
| ションバージョン | 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

| | データ タ | |
|--------------------------|--------|---|
| フィールド | 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 $5.0 \sim 5.0.2$ 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)

| | データ タ | |
|--------------------------|-----------|---|
| フィールド | 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。 |
| レスポンダ IP アドレス | uint8[16] | IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。 |
| 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 | 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。 |
| レスポンダポート | uint16 | 応答ホストにより使用されるポート。 |
| TCP フラグ | uint16 | 接続イベントのすべての TCP フラグを示します。 |
| プロトコル | uint8 | IANA 指定のプロトコル番号。 |
| NetFlow ソース | uint8[16] | 接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス |
| 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 | ィールド(続き) |
|--------|--------|--------|-------|-------------|----------|
| | | | | | |

| | データ タ | |
|----------------------------------|--------|--|
| フィールド | 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 o 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 o 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 o 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 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。

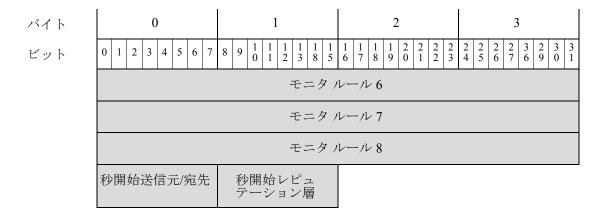
接続統計データメッセージの詳細については、接続統計データメッセージ(4-55ページ)を参照してください。

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。

| | I . |] | 1 | 1 | | |
|-----|--|---------------|------------------|-----------------------|--|--|
| バイト | 0 | 1 | 2 | 3 2 2 2 2 2 2 3 2 3 3 | | |
| ビット | 0 1 2 3 4 5 6 7 | 8 9 0 1 2 3 8 | 8 5 6 7 8 9 0 1 | 2 3 4 5 6 7 6 9 0 1 | | |
| | | | ゛ロック タイプ(126 | 5) | | |
| | | 接続デー | ータブロック長 | | | |
| | | D | Device ID | | | |
| | | 入 | カゾーン | | | |
| | | 入力ン | ブーン(続き) | | | |
| | | 入力ン | ブーン(続き) | | | |
| | | 入力> | バーン(続き) | | | |
| | | 出 | カゾーン | | | |
| | | 出力> | ブーン(続き) | | | |
| | | 出力ン | ブーン(続き) | | | |
| | | 出力ン | ブーン(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 |) | | |
| | | · | ダ IP アドレス | | | |
| | | | ア IP アドレス(続き) | | | |
| | | レスホンダ | Ir テトレハ(就ざ) | | | |

| バイト | 0 | 1 | 2 | 3 |
|-----|-----------------|---------------------|---|---|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | | レスポンダ IP フ | アドレス(続き) | |
| | | レスポンダ IP フ | 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 | rV ID | |
| | ルールア | クション | ルール | の理由 |
| | イニシエー | タ ポート | レスポン | ダポート |
| | TCP 7 | プラグ | 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) | |
| | N | JetFlow ソース(続き) | | 最初のパケット の時刻 |
| | 最初のパク | 「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) | |
| | イニシェ | ニータ送信パケット数 | 女(続き) | レスポンダ送信 パケット数 |
| | | レスポンダ送信ノ | ペケット数(続き) | |
| | レスポ | ンダ送信パケット数 | (続き) | イニシエータ送 信バイト数 |
| | | イニシエータ送信 | 言バイト数(続き) | |
| | イニシ | エータ送信バイト数 | (続き) | レスポンダ送信 バイト数 |

| バイト | 0 | 1 | 2 | 3 | |
|----------------------|-----------------|-----------------------|---|---------------------------------|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| | | | | | |
| | レスオ | ペンダ送信バイト数 | (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 | ーション プロトコル | √ID(続き) | URL カテゴリ | |
| | 1 | 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 7 | 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 | 文字 | 列ブロック タイプ (| 続き) | 文字列ブロック長 | |
| ションURL | 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 | ック タイプ(0) | | |
| | 文字列ブロック長 | | | | |
| | | NetBI | OS 名 | | |
| クライアント アプリケー | | 文字列ブロッ | ック タイプ(0) | | |
| ションバージョン | 文字列ブロック長 | | | | |
| | ク | ライアント アプリケ | アーション バージョン | / | |
| | | モニタ | ルール 1 | | |
| | | モニタ | ノレーノレ 2 | | |
| | | モニタ | ノレーノレ 3 | | |
| | | | <i>ルール4</i> | | |
| | モニタ ルール 5 | | | | |



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

| | データ タ | |
|-------------------|-----------|---|
| フィールド | 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。 |
| レスポンダ IP ア ドレス | uint8[16] | IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。 |
| 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。 |

表 B-29 接続統計データ ブロック 5.1 のフィールド(続き)

| | データ タ | |
|----------------------------|-----------|---|
| フィールド | イプ | 説明 |
| レスポンダ | uint16 | 応答ホストにより使用されるポート。 |
| 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。 |
| レスポンダ送信 パケット数 | uint64 | 応答ホストが送信したパケット数。 |
| イニシエータ送 信バイト数 | uint64 | 開始ホストからの送信バイト数。 |
| レスポンダ送信 バイト数 | uint64 | 応答ホストから送信バイト数。 |
| 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 o 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 o 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)

| - | データ タ | |
|------------------------------|--------|---|
| フィールド | 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 o 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 1 1 1 1 1 1 8 | 1 1 1 1 1 2 2 1 1 5 6 7 8 9 0 1 2 | 2 2 2 2 2 2 3 3 3 3 2 3 4 5 6 7 6 9 0 1 | |
| | | 接続データブロ | 1ック タイプ(144) | | |
| | | 接続データ | マブロック長 | | |
| | | Dev | vice ID | | |
| | | 入力 | ゾーン | | |
| | | 入力ゾ- | ーン(続き) | | |
| | | 入力ゾー | ーン(続き) | | |
| | | 入力ゾー | ーン(続き) | | |
| | 出力ゾーン | | | | |
| | 出力ゾーン(続き) | | | | |
| | | ーン(続き) | | | |
| | 出力ゾーン(続き) | | | | |
| | | 入力インク | ターフェイス | | |
| | | 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 | 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 I | P アドレス(続き) | | |
| | | イニシエータ I | Pアドレス(続き) | | |
| | | イニシエータI | P アドレス(続き) | | |

| | 1 | 1 | 1 | 1 | | |
|-----|---|---|--|---|--|--|
| バイト | 0 | 1 | 2 | 3 | | |
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 8 5 1 1 2 3 8 5 | $ \begin{array}{c ccccccccccccccccccccccccccccccccccc$ | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | | レスポンダ | IP アドレス | | | |
| | レスポンダ IP アドレス(続き) | | | | | |
| | レスポンダ IP アドレス(続き) | | | | | |
| | レスポンダ 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 | レスポン | ダ ポート | | |
| | | | | | | |
| | TCP 7 | フラグ | プロトコル | NetFlow ソース | | |
| | TCP 7 | フラグ NetFlow ソ | | NetFlow ソース | | |
| | TCP > | | 一ス(続き) | NetFlow ソース | | |
| | TCP 7 | NetFlow ソ | ース(続き) ース(続き) | NetFlow ソース | | |
| | | NetFlow ソ NetFlow ソ | 一ス(続き) 一ス(続き) ース(続き) | NetFlow ソース インスタンス ID (Instance ID) | | |
| | | NetFlow ソ NetFlow ソ NetFlow ソ | ース(続き) ース(続き) ース(続き) | インスタンス ID | | |
| | インスタンス ID (続き) | NetFlow ソ NetFlow ソ NetFlow ソ | -ス(続き) -ス(続き) -ス(続き) | インスタンス ID (Instance ID) 最初のパケット | | |
| | ト インスタンス ID (続き) 最初のパク | NetFlow ソ NetFlow ソ NetFlow ソース(続き) 接続数プ | ース(続き) ース(続き) ース(続き)) ウウンタ レプ(続き) | インスタンス ID (Instance ID) 最初のパケットの時刻 最終パケットの | | |
| | ト インスタンス ID (続き) 最初のパク | NetFlow ソ NetFlow ソ NetFlow ソース(続き) 接続数プ | ース(続き) ース(続き) ース(続き)) ウウンタ レプ(続き) プ(続き) | インスタンス ID (Instance ID) 最初のパケット の時刻 最終パケットの 時刻 イニシエータ送 | | |
| | ト インスタンス ID (続き) 最初のパケ 最終パケ | NetFlow ソ NetFlow ソ NetFlow ソース(続き) 接続数プ アットのタイムスタン | ース(続き) ース(続き) ース(続き)) ウウンタ レプ(続き) プ(続き) パケット数(続き) | インスタンス ID (Instance ID) 最初のパケット の時刻 最終パケットの 時刻 イニシエータ送 | | |

| バイト | 0 | 1 | 2 | 3 | | |
|-----------------------|------------------|---------------------------|---|---------------------------------|--|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | レスポ | 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 | レスポンダ Tx Bytes | | | | |
| | | | | | | |
| | レスズ | ユーザ ID(User ID) | | | | |
| | | アプリケーショ ンプロトコル ID | | | | |
| | アプリケ | ーション プロトコル | √ID(続き) | URL カテゴリ | | |
| | | URL レピュテー ション | | | | |
| | URL | 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 7 | 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 | ック タイプ(0) | | | |
| [Hills (Frame)] | | | | | | |
| | | NetBI | OS 名 | | | |
| クライアント アプリケー | | 文字列ブロッ | ック タイプ(0) | | | |
| ションバージョン | | 文字列フ | 「ロック長 | | | |
| | ク | ライアント アプリケ | アーション バージョン | <i>/</i> | | |
| | | モニタ | ルール 1 | | | |

バイト

ビット

1 0 2 3 0 1 2 3 4 5 6 7 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 レスポンダの国

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

| | データ タ | |
|--------------------|-----------|--|
| フィールド | 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。 |
| レスポンダ IP アド レス | uint8[16] | IP アドレス オクテットの、開始ホストに応答したホストの IP アドレス。 |

表 B-30 接続統計データ ブロック 5.2.x のフィールド(続き)

| | データ タ | |
|-------------------------|-----------|--|
| フィールド | 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)。 |
| バール ID | uint32 | イベントをトリガーしたルールの内部 ID(該当する場合)。 |
| ルール アクション | uint16 | そのルールに対してユーザインターフェイスで選択されたアクション(allow、block など)。 |
| ルールの理由 | uint16 | イベントをトリガーしたルールの理由。 |
| イニシエータ ポート | uint16 | 開始ホストにより使用されるポート。 |
| レスポンダ ポート | uint16 | 応答ホストにより使用されるポート。 |
| TCP フラグ | uint16 | 接続イベントのすべての TCP フラグを示します。 |
| プロトコル | uint8 | IANA 指定のプロトコル番号。 |
| NetFlow ソース | uint8[16] | 接続のデータをエクスポートした NetFlow 対応デバイス の IP アドレス。 |
| インスタンス ID (Instance ID) | uint16 | イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。 |
| 接続数カウンタ | uint16 | 同じ秒の間に発生する接続イベントを区別するために使用される値。 |
| 最初のパケット タ イムスタンプ | uint32 | セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。 |
| 最終パケット タイ ムスタンプ | uint32 | セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。 |
| イニシエータ送信パ ケット数 | uint64 | 開始ホストからの送信パケット数。 |
| レスポンダ送信パ ケット数 | uint64 | 応答ホストが送信したパケット数。 |
| イニシエータ送信バ イト数 | uint64 | 開始ホストからの送信バイト数。 |
| レスポンダ送信バイ ト数 | uint64 | 応答ホストから送信バイト数。 |
| 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 | uint32 | アプリケーション プロトコルのアプリケーション ID。 |
| プロトコル 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)

| | データ タ | |
|-------------------------------|-------------|---|
| フィールド | アータ タ イプ | 説明 |
| <u>文字</u> 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 o 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 o 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 o 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。 |

| 表 B-30 接続統計データ ブロック 5.2.x のフィールト | 表 B-30 | 接続統計データ | ブロック | 5.2.x 0 | のフィール | ド(続き) |
|----------------------------------|--------|---------|------|---------|-------|-------|
|----------------------------------|--------|---------|------|---------|-------|-------|

| | データ タ | |
|----------------------|--------|----------------------------------|
| フィールド | 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。 |
| レスポンダの国 | 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 $5.0 \sim 5.1$ の場合、ブロック タイプは 119 です。

次の図は、接続チャンク データ ブロックの形式を示しています。

| バイト | 0 | 2 | 3 | | | | |
|-----|------------------------------|---------------------|---|------------------------------------|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | |
| | 接続チャンク ブロック タイプ(66 119) | | | | | | |
| | 接続チャンク ブロック長 | | | | | | |
| | イニシエータ IP アドレス | | | | | | |
| | レスポンダ IP アドレス | | | | | | |
| | 開始時刻 | | | | | | |
| | アプリケーション ID (Application ID) | | | | | | |
| | レスポンク | ダポート | プロトコル | 接続タイプ | | | |
| | | NetFlow ディテク | カタ IP アドレス | | | | |
| | 送信パケット数 | | | | | | |
| | 受信パケット数 | | | | | | |
| | 送信バイト数 | | | | | | |
| | | 受信バ | イト数 | | | | |
| | | 接 | 続 | | | | |

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

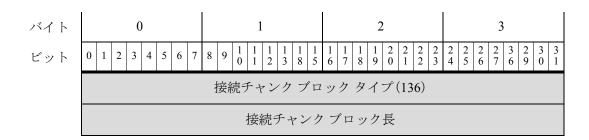
表 B-31 接続チャンク データ ブロックのフィールド

| | データ タ | |
|---------------------|----------|---|
| フィールド | イプ | 説明 |
| 接続チャンク ブ | uint32 | 接続チャンクデータブロックを開始します。この値は、 |
| ロック タイプ | | 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 | 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 |
| ロック長 | | 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 | 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 |
| ドレス | | VX. |
| レスポンダ IP アド | 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 | | 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 | 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 |
| ID (Application ID) | | ケーション ID 番号。 |
| レスポンダ ポート | uint16 | 接続チャンクでレスポンダが使用したポート。 |
| プロトコル | uint8 | ユーザ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 | uint8[4] | IP アドレス オクテットの、接続を検出した NetFlow デバイ |
| ドレス | | 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 2 2 2 2 3 2 3 3 | | | | | |
|-----|---------------------------------------|---|---|--|--|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | | | |
| | イニシエータ IP アドレス | | | | | | | |
| | レスポンダ IP アドレス | | | | | | | |
| | 開始時刻 | | | | | | | |
| | アプリケーション プロトコル | | | | | | | |
| | レスポンダ ポート プロトコル 接続タイプ | | | | | | | |
| | NetFlow ディテクタ IP アドレス | | | | | | | |
| | 送信パク | 「ット数 | | | | | | |
| | 送信パケッ | ト数(続き) | | | | | | |
| | 受信パク | アット数 | | | | | | |
| | 受信パケッ | 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 | ····································· | | | | | | |

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

| | データ タ | |
|---------------------|----------|--|
| フィールド | イプ | 説明 |
| 接続チャンク ブ ロック タイプ | uint32 | 接続チャンク データ ブロックを開始します。この値は常に 136 です。 |
| 接続チャンク ブ ロック長 | uint32 | 接続チャンク データ ブロックのバイト数(接続チャンク ブロック タイプと長さのフィールド用の 8 バイト、およびそれに続く接続チャンク データのバイト数を含む)。 |
| イニシエータ IP アドレス | uint8(4) | この接続タイプのイニシエータの IP アドレス。これはレスポンダ IP アドレスとともに、複数の同じ接続を見分けるために使用されます。 |
| レスポンダ IP アドレス | uint8(4) | この接続タイプのレスポンダの IP アドレス。これはイニシエータ 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: | ルド(続き | r —/I | りフィ | ックの | ブロ | データ | ・ンク | 接続チャ | 表 B-32 |
|---------------------------------|-------|-------|-----|-----|----|-----|-----|------|--------|
|---------------------------------|-------|-------|-----|-----|----|-----|-----|------|--------|

| | データ タ | |
|------------|----------|--------------------------------------|
| フィールド | 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 | uint32 | 接続で使用されたプロトコルの ID 番号。 |
| ンプロトコル | | |
| レスポンダ | uint16 | 接続チャンクでレスポンダが使用したポート。 |
| ポート | | |
| プロトコル | uint8 | ユーザ情報を含むパケットのプロトコル。 |
| 接続タイプ | uint8 | 接続の種類。 |
| NetFlow ディ | 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 |
| テクタ IP アド | | IP アドレス。 |
| 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 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | |
| | 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 1 1 1 1 1 1 8 | 1 1 1 1 1 2 2 5 6 7 8 9 0 1 | 2 2 2 2 2 2 2 3 3 3 3 3 2 3 3 2 3 1 3 3 4 5 6 7 6 9 0 1 | | | |
| | | 入力ゾ [、] | ーン(続き) | | | | |
| | | 出力 | リゾーン | | | | |
| | | 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) | | | | | | |
| | | レスポンク | ダ IP アドレス | | | | |
| | | レスポンダ II | アドレス(続き) | | | | |
| | | レスポンダ II | アドレス(続き) | | | | |
| | | レスポンダ [[| 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) | | | | |
| | | | | | | | |

0 1 2 3 バイト 1 2 3 4 5 6 ビット 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 レスポンダ ポート TCP フラグ プロトコル NetFlow ソース NetFlow ソース(続き) NetFlow ソース(続き) NetFlow ソース(続き) NetFlow ソース(続き) インスタンス ID (Instance ID) インスタンス ID 最初のパケット 接続数カウンタ の時刻 (続き) 最終パケットの 最初のパケットのタイムスタンプ(続き) 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) レスポンダ Tx Packets レスポンダ送信パケット数(続き) レスポンダ送信パケット数(続き) イニシエータ送 信バイト数 イニシエータ送信バイト数(続き) レスポンダ Tx イニシエータ送信バイト数(続き) Bytes レスポンダ送信バイト数(続き) ユーザ ID (User レスポンダ送信バイト数(続き) 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

| バイト | 0 | | 1 | | | | 2 | 2 | | | 3 | | | |
|----------------------|------------------------|-------|--------------|-------|-----|---|------------|-----|---------------------|-----|------------|--|-------|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 | 1 1 1 2 | 1 1 8 | 1 5 | $\begin{array}{c c} 1 & 1 \\ 6 & 7 \end{array}$ | 1 1 8 9 | 2 | 2 1 2 2 | 2 3 | 2 2 4 5 | $\begin{bmatrix} 2 & 2 \\ 6 & 7 \end{bmatrix}$ | 3 2 | $\begin{array}{c cccc} 2 & 3 & 3 \\ 0 & 0 & 1 \end{array}$ |
| | URL カテゴリ(続き) | | | | | | | UR | Lレ ショ | ピュラ | テー | | | |
| | URL | レピュラ | テーシ | /ョン | (約 | きき) | | | | | | イア | | アプ ⁄ 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 7 | プリケ | ーショ | ョンII |)(| 続き |) | | | | | 字列: タイ | | |
| | 文字 | 列ブロッ | ッ ク タ | マイプ | (約 | き) | | | | | 文字 | 列ブ | `ロッ | ク長 |
| | 文 | 字列ブロ | コック | '長(続 | き | •) | | | | | | ライフ リケー UR | | |
| NetBIOS [名前(Name) | | 7 | 文字列 | リブロ | ツ | クタ | イプ | (0) | | | | | | |
| | 文字列ブロック長 | | | | | | | | | | | | | |
| | | | | NetB | Ю | S 名. | ••• | | | | | | | |
| クライアント アプリケー | | | 文字列 | リブロ | ツ | クタ | イプ | (0) | | | | | | |
| ションバージョン | | | 文 | (字列) | ブ | ロッ | ク長 | | | | | | | |
| | <i>þ</i> | ライアン | ノトフ | アプリー | ケ | ーシ | ョン | バー | ージョ | ョン. | | | | |
| | | | | モニタ |) | レーバ | V 1 | | | | | | | |
| | | | | モニタ | j | レーバ | レ 2 | | | | | | | |
| | | | • | モニタ | j | レーバ | V 3 | | | | | | | |
| | | | | モニタ | | | | | | | | | | |
| | | | | モニタ | | | | | | | | | | |
| | モニタルール 6 | | | | | | | | | | | | | |
| | | | | モニタ | | | | | | | | | | |
| | 五小目目 4 ヘンチ /⇒ 一 //⇒ /→ | エル ノ | | モニタ | | レーバ | | | n 2 | | 1 | J. L | 1 / 1 | |
| | 砂開始送信元/宛先 | | | 一グ 僧 | | | ノア | 1 | ルイ | ~\; | / h | カウ | ノト | |
| | 侵入イベン | Γルリ↓ | / r | | | | | | | | | | | |

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

| | データ タ | |
|-------------------------|-----------|---|
| フィールド | 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。 |
| レスポンダ IP ア ドレス | uint8[16] | IPアドレスオクテットの、開始ホストに応答したホストのIP アドレス。 |
| 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。 |
| レスポンダ ポート | uint16 | 応答ホストにより使用されるポート。 |
| TCP フラグ | uint16 | 接続イベントのすべての TCP フラグを示します。 |
| プロトコル | uint8 | IANA 指定のプロトコル番号。 |
| NetFlow ソース | uint8[16] | 接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。 |
| インスタンス ID (Instance ID) | uint16 | イベントを生成した管理対象デバイスの Snort インスタンス の数値 ID。 |
| 接続数カウンタ | uint16 | 同じ秒の間に発生する接続イベントを区別するために使用 される値。 |
| 最初のパケット タイムスタンプ | uint32 | セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。 |
| | | |

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)

| | データ タ | |
|----------------------------|--------|--|
| フィールド | 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。 |
| レスポンダ送信 パケット数 | uint64 | 応答ホストが送信したパケット数。 |
| イニシエータ送 信バイト数 | uint64 | 開始ホストからの送信バイト数。 |
| レスポンダ送信 バイト数 | uint64 | 応答ホストから送信バイト数。 |
| 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 o 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 o 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 o 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) |
|--------|---------------------------------|
| | |

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

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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | |
| | | 接続データ ブロ | ック タイプ (152) | | | | |
| | | 接続データ | ブロック長 | | | | |
| | | Devi | ce ID | | | | |
| | | 入力》 | デーン | | | | |
| | 入力ゾーン(続き) | | | | | | |
| | 入力ゾーン(続き) | | | | | | |
| | | 入力ゾー | ン(続き) | | | | |
| | | 出力》 | ブ 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 | フェイス(続き) | | | | |
| | | 出力インタ | ーフェイス | | | | |
| | | 出力インターフ | フェイス(続き) | | | | |
| | | 出力インタース | フェイス(続き) | | | | |
| | | 出力インタース | 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) | | | | |

| | | | 2 |] 2 | | | | | |
|-----|----------------------------------|---------------------|-----------|---------------------------------|--|--|--|--|--|
| バイト | 0 | 1 | 2 | 3 2 2 2 2 3 2 3 3 | | | | | |
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | | | |
| | | レスポンダ | IP アドレス | | | | | | |
| | | レスポンダ IP フ | アドレス(続き) | | | | | | |
| | | レスポンダ IP フ | アドレス(続き) | | | | | | |
| | | レスポンダ IP フ | アドレス(続き) | | | | | | |
| | | ポリシーリ | 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 | レスポン | ダ ポート | | | | | |
| | TCP 7 | フラグ | プロトコル | NetFlow ソース | | | | | |
| | | NetFlow ソー | ース(続き) | | | | | | |
| | | NetFlow ソー | 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) | 接続数力 | リウンタ | 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 | 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) | | | | | | |
| | イニシュ | ニータ送信パケット数 | (続き) | レスポンダ Tx Packets | | | | | |
| | | レスポンダ送信ハ | ペケット数(続き) | | | | | | |

| ビット 0 | バイト | 0 | 1 | 2 | 3 | | | | | | |
|--|-------------|----------|----------------------|-----------------|----------|--|--|--|--|--|--|
| 信バイト数 | ビット | | | | | | | | | | |
| イニシエータ送信バイト数(続き) | | レスポ | レスホンタ送信パケット数(続き) | | | | | | | | |
| Bytes | | | イニシエータ送信バイト数(続き) | | | | | | | | |
| レスポンダ送信バイト数(続き) ユーザ ID(User ID) エーザ ID(続き) エーザ ID(続き) URL カテゴリ URL カテゴリ (続き) URL レピュテーション (続き) リライアント 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 (続き) 文字列ブロック タイプ(の) 文字列ブロック タイプ(の) 文字列ブロック タイプ(の) NetBIOS [名前(Name)] 文字列ブロック タイプ(の) アプリケーション バーション バーション バーション バーション バーション バーション バーション ハーション バーション バーション バーション バーション バージョン | | イニシ | | | | | | | | | |
| ID) | | | レスポンダ送信 | バイト数(続き) | | | | | | | |
| アプリケーションプロトコル ID (続き) URL カテゴリ URL カテゴリ (続き) URL レピュテーション 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) グライアント アプリケーション ID (続き) 文字列ブロック タイプ(の) 文字列ブロック 長 (続き) 文字列ブロック 長 NetBIOS 名 クライアント アプリケーション ID (続き) グ字列ブロック タイプ(の) 文字列ブロック タイプ(の) フ字列ブロック タイプ(の) ファンバージョン バージョン バージョン バージョン バージョン バージョン バージョン バージョン アプリケーション バージョン アプリケーション アプリケーション バージョン バージョン ボージョン アプリケーション アプリケー アプリケーション アプリケー アプリケーション アプリケーション アプリケーション アプリケーション アプリケーション アプリケーション アプリケーション ア | | レスオ | | | | | | | | | |
| 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 (続き) クライアントアプリケーション (の) クライアント URL 文字列ブロック タイプ (続き) 文字列ブロック タイプ (の) 文字列ブロック長 (続き) グ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 (の) フライアントアプリケーション バージョン バージョン バージョン バージョン バージョン バージョン ハージョン グライアントアプリケーション バージョン ハージョン ハージョン ハージョン バージョン ハージョン ハージ | | | | | | | | | | | |
| URL レピュテーション(続き) ウライアント アプリケーション ID クライアント アプリケーション ID Web アプリケーション ID クライアント URL 文字列ブロック タイプ(統き) 文字列ブロック タイプ(統き) 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) ア学列ブロック長 NetBIOS 名 クライアント アプリケーション バージョン バージョン バージョン グライアント アプリケーション バージョン グライアント アプリケーション バージョン | | アプリケー | ーション プロトコル | ID(続き) | URL カテゴリ | | | | | | |
| 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 (続き) 文字列ブロック タイプ(の) 大字列ブロック タイプ(続き) 文字列ブロック長 NetBIOS [名前(Name)] 文字列ブロック タイプ(の) アライアント アプリケーションバーションバージョンバージョン 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 グライアント アプリケーション バージョン グライアント アプリケーション バージョン | | 1 | | | | | | | | | |
| 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) フライアント アプリケーション バー 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 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 | | URL | | | | | | | | | |
| URL 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) ア学列ブロック長 NetBIOS 名 クライアントアプリケーションバージョンバージョン 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 | | クライアン | · ト アプリケーション | / ID(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 文字列ブロック長 NetBIOS 名 文字列ブロック タイプ(0) アプリケーションバーションバージョンバージョン クライアントアプリケーションバージョン | | Web 7 | プリケーション ID(| 続 き) | | | | | | | |
| アリケーション URL NetBIOS | | 文字 | 文字列ブロック長 | | | | | | | | |
| [名前(Name)] 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 グライアント アプリケーション バージョン 文字列ブロック タイプ(0) クライアント アプリケーション バージョン | | 文 | プリケーション | | | | | | | | |
| 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 | | | 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 バー ジョン クライアント アプリケーション バージョン | [A m (Name) | 文字列ブロック長 | | | | | | | | | |
| 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 | | | NetBIO | os 名 | | | | | | | |
| 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 | | | 文字列ブロッ | ク タイプ(0) | | | | | | | |
| | ションバー | | 文字列ブ | ロック長 | | | | | | | |
| モニタ ルール 1 | | ク | ライアント アプリケ | ーション バージョン | <i>′</i> | | | | | | |
| | | | モニタノ | レール1 | | | | | | | |

バイト

ビット

0 1 2 3 0 1 2 3 4 5 6 7 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 レスポンダの国 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

| | データ タ | | |
|---------------------|-----------|---|--|
| フィールド | 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)

| | データ タ | | |
|----------------------------|-------------|--|--|
| フィールド | プータ 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。 | |
| レスポンダ IP ア ドレス | uint8[16] | IPアドレスオクテットの、開始ホストに応答したホストの IP アドレス。 | |
| 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。 | |
| レスポンダ ポート | uint16 | 応答ホストにより使用されるポート。 | |
| TCP フラグ | uint16 | 接続イベントのすべての TCP フラグを示します。 | |
| プロトコル | uint8 | IANA 指定のプロトコル番号。 | |
| NetFlow ソース | uint8[16] | 接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。 | |
| インスタンス ID (Instance ID) | uint16 | イベントを生成した管理対象デバイスの Snort インスタンス の数値 ID。 | |
| 接続数カウンタ | uint16 | 同じ秒の間に発生する接続イベントを区別するために使用 される値。 | |
| 最初のパケット タイムスタンプ | uint32 | セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。 | |
| 最終パケット タ イムスタンプ | uint32 | セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。 | |
| イニシエータ送 信パケット数 | uint64 | 開始ホストからの送信パケット数。 | |
| レスポンダ送信 パケット数 | uint64 | 応答ホストが送信したパケット数。 | |
| イニシエータ送 信バイト数 | uint64 | 開始ホストからの送信バイト数。 | |
| レスポンダ送信 バイト数 | uint64 | 応答ホストから送信バイト数。 | |
| 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)

| - | データ タ | | |
|------------------------------|-------------|---|--|
| フィールド | ブーク ク 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 o 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 o 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 o 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)

| | データ タ | |
|------------------------------|---------|---|
| フィールド | 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。 |
| レスポンダの国 | 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 1 1 2 3 8 5 6 7 8 9 0 1 1 2 3 8 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 2 4 5 6 7 6 9 0 1 | | | |
| | 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 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 3 8 5 6 7 8 9 0 1 2 3 4 5 6 7 6 9 0 1 | |
| | 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| | | レスポンダ | IP アドレス | | |
| | | レスポンダ IP ご | アドレス(続き) | | |
| | | レスポンダ IP アドレス(続き) | | | |
| | | レスポンダ IP 🏾 | アドレス(続き) | | |
| | | ポリシー! | J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 | アレ ID | | |
| | ルールア | クション | ルール | の理由 | |
| | イニシエータ ポート レスポンダ ポート | | | ダ ポート | |
| | TCP 7 | 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) | | |
| | N | NetFlow ソース(続き) |) | インスタンス ID (Instance ID) | |
| | インスタンス ID (続き) | 接続数划 | コウンタ | 最初のパケット の時刻 | |
| | 最初のパク | rットのタイムスタン | 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) | | |
| | イニシコ | ニータ送信パケット数 | 女(続き) | レスポンダ Tx Packets | |
| | | レスポンダ送信ノ | ペケット数(続き) | | |

| ピット 0 | バイト | 0 | 1 | 2 | 3 | |
|--|-----------|------------------------------|-----------------------|---|---|--|
| 信バイト数 | ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| イニシエータ送信バイト数(続き) | | レスポンダ送信パケット数(続き) イニシコ 信バイ | | | | |
| Bytes | | | イニシエータ送信 | 言バイト数(続き) | | |
| レスポンダ送信パイト数(続き) ユーザ ID(User ID) コーザ ID(続き) エーザ ID(続き) URL カテゴリ URL レビュテーション (続き) URL レビュテーション (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) 文字列ブロック タイプ(の) 文字列ブロック タイプ(の) 文字列ブロック長 NetBIOS [名前(Name) 文字列ブロック タイプ(の) NetBIOS 名… クライアント アプリケーションバージョン バージョン バージョン バージョン バージョン アプリケーション アプリケータ | | イニシ | エータ送信バイト数 | (続き) | | |
| ID) | | | レスポンダ送信 | バイト数(続き) | | |
| アプリケーションプロトコル ID (続き) URL カテゴリ URL カテゴリ (続き) URL レピュテーション URL レピュテーション (続き) クライアント アプリケーション ID (続き) Web アプリケーション ID クライアント アプリケーション ID (続き) 文字列ブロック タイプ(の) 文字列ブロック タイプ (続き) グライアント アプリケーション URL NetBIOS [名前 (Name)] 文字列ブロック 長 NetBIOS 名 クライアント アプリケーション バージョン バージョン バージョン グライアント アプリケーション バージョン バージョン バーブリケーション バージョン エー・ジョン ID | | レスオ | ポンダ送信バイト数(約 | 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) グライアント アプリケーション ID (続き) Web アプリケーション ID (続き) 文字列ブロック タイプ (の) クライアント URL 文字列ブロック タイプ (続き) 文字列ブロック長 NetBIOS [名前 (Name)] 文字列ブロック タイプ (の) 文字列ブロック タイプ (の) アプリケーション バーション バーション バージョン バージョン バージョン バージョン パージョン パージ パージョン パージ イン パージ イン パージョン パージョン パージ イン パージョン パージョン パージョン パージョン パージョン パージョン パージョン パージョン パ | | | ユーザ ID(続き) | | | |
| URL レピュテーション (続き) ウライアント 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 (続き) Web アプリケーション ID (続き) 文字列ブロック タイプ (の) クライアント 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 タイプ (の) 文字列ブロック タイプ (の) 文字列ブロック タイプ (の) NetBIOS [名前 (Name)] 文字列ブロック タイプ (の) 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 バージョン バージョン バージョン ハージョン ロース | | アプリケー | ーション プロトコル | ID(続き) | URL カテゴリ | |
| 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 (続き) 文字列プロック タイプ(0) 文字列プロック タイプ(続き) 文字列プロック タイプ(続き) 文字列プロック長 NetBIOS [名前 (Name)] 文字列プロック タイプ(0) アライアント アプリケーションバーションバーションバ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 | | | | | | |
| 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(の) 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(の) フライアント アプリケーション バージョン バージョン バージョン バージョン ハージョン バージョン クライアント アプリケーション バージョン ハージョン ロース | | | | | | |
| URL 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) ア学列ブロック長 NetBIOS 名 クライアントアプリケーションバージョン バージョン バージョン グライアント 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 | | クライアン | · ト アプリケーション | / ID(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) フライアント アプリケーションバー 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 タイプ(0) 文字列ブロック タイプ(0) カライアント 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 | | Web 7 | プリケーション ID(| 続き) | | |
| アリケーション URL NetBIOS | | 文字 | 列ブロック タイプ(約 | 売き) | 文字列ブロック長 | |
| [名前(Name)] 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 文字列ブロック タイプ(0) 文字列ブロック長 文字列ブロック長 クライアント アプリケーション バージョン | | 文 | 字列ブロック長(続き | :) | プリケーション | |
| 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 | | | 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 バー ジョン クライアント アプリケーション バージョン | [治前(Name) | 文字列ブロック長 | | | | |
| 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 | | | NetBIO | OS 名 | | |
| 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 | | 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 バージョン | ションバー | | | | | |
| モニタ ルール 1 | | ク | <i>'</i> | | | |
| | | | モニタノ | レール1 | | |

バイト

ビット

0 1 2 3 0 1 2 3 4 5 6 7 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 レスポンダの国 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

| | データ タ | |
|------------------|--------|---|
| フィールド | 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)

| - | データ タ | | |
|--------------------------|-----------|---|--|
| フィールド | 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。 | |
| レスポンダ IP ア ドレス | uint8[16] | IPアドレス オクテットの、開始ホストに応答したホストの IP アドレス。 | |
| 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。 | |
| レスポンダ ポート | uint16 | 応答ホストにより使用されるポート。 | |
| TCP フラグ | uint16 | 接続イベントのすべての TCP フラグを示します。 | |
| プロトコル | uint8 | IANA 指定のプロトコル番号。 | |
| NetFlow ソース | uint8[16] | 接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。 | |
| インスタンス ID (Instance ID) | uint16 | イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。 | |
| 接続数カウンタ | uint16 | 同じ秒の間に発生する接続イベントを区別するために使用される値。 | |
| 最初のパケット タイムスタンプ | uint32 | セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。 | |
| 最終パケット タ イムスタンプ | uint32 | セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。 | |
| イニシエータ送 信パケット数 | uint64 | 開始ホストからの送信パケット数。 | |
| レスポンダ送信 パケット数 | uint64 | 応答ホストが送信したパケット数。 | |

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)

| | データ タ | |
|------------------------------|--------|---|
| フィールド | イプ | 説明 |
| イニシエータ送 信バイト数 | uint64 | 開始ホストからの送信バイト数。 |
| レスポンダ送信 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)

| | データ タ | | |
|------------------------------|---------|---|--|
| フィールド | 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。 | |
| レスポンダの国 | 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 | 7 ブロック 5.3.1 | のフィールド(続き) |
|---------|-----------------|---------------------|----------------------|
| 2X D-33 | 35スパソレルソレロ ノー・フ | / H / / J.J. I | יטער איר איר איר איר |

| | データ タ | |
|------------------|-------|--|
| フィールド | 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 | | 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 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 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 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | |
| | 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 | 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) | | | | | |
| | レスポンダ IP アドレス(続き) | | | | | |
| | レスポンダ 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) | | | | | |
| | /レー/レ ID | | | | | |
| | ルールアクション ルールの理由 | | | | | |
| | イニシエータ ポート レスポンダ ポート | | | | | |
| | TCP フラグ プロトコル NetFlow ソース | | | | | |

バイ

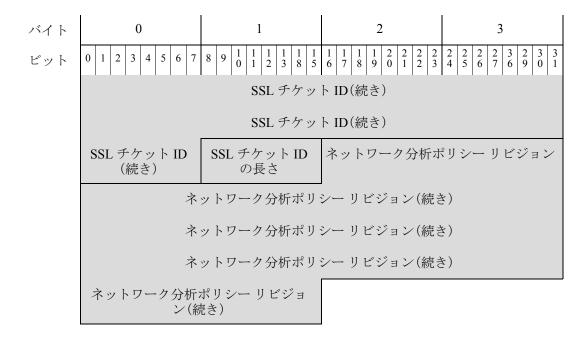
ビッ

| ١ | 0 | 1 2 | 3 | | |
|----------|-------------------|---------------------------------------|---|--|--|
| ١ | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 2 3 8 5 6 7 8 9 0 1 2 2 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | NetFlow ソース(続き) | | | | |
| | | NetFlow ソース(続き) | | | |
| | | NetFlow ソース(続き) | | | |
| | 1 | 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 | | |
| | 最初のパク | 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 | | |
| | | | | | |
| | イニシニ | レスポンダ Tx Packets | | | |
| | レスポンダ送信パケット数(続き) | | | | |
| | レスポ | イニシエータ送 信バイト数 | | | |
| | | | | | |
| | イニシ | レスポンダ Tx Bytes | | | |
| | | | | | |
| | レスス | ユーザ ID (User ID) | | | |
| | | アプリケーショ ンプロトコル ID | | | |
| | アプリケ | ーション プロトコル ID(続き) | URL カテゴリ | | |
| | | URL レピュテー ション | | | |
| | URL | 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 | | |

| バイト | 0 1 | 2 | 3 | | |
|--|---------------------------------------|---|---|--|--|
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | Web アプリケーション ID(続き) 文字列ブロック タイプ(0) | | | | |
| ライアン URL | 文字列ブロック タイプ(続き) | | 文字列ブロック長 | | |
| トライ U | 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 | | | |
| e)] | 文字列ブロック タイプ(0) | | | | |
| NetBIOS [名前(Name)] | 文字列ブ | ロック長 | | | |
| Ne [名 計 | NetBIOS 名 | | | | |
| ~ m , | 文字列ブロック タイプ(0) | | | | |
| | 文字列ブロック長 | | | | |
| ケットアップ・アン・アン・アン・アン・アー・アー・アー・アー・アー・アー・アー・アー・アー・アー・アー・アー・アー・ | 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 | ントカウント | | | |
| | 侵入イベント カウント | ` | イニシエータの国 | | |
| | レスポンダの国 IOC 番号 | | | | |
| | 送信元自律システム | | | | |
| | <u>宛先自律システム</u> | | | | |

| バイト | 0 | 1 | 2 | 3 | |
|---|---|-----------------------|---|------------------------------------|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| | 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) | | | | |
| <u></u> | VLAN ID (Admin. VLAN ID) | | 文字列ブロック タイプ(0) | | |
| 参照ホス | 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 | | |
| # '\ '\ | 文字列ブロック タイプ(0) | | | | |
| サージーグ・イン・イン・イン・イン・イン・イン・イン・イン・イン・イン・イン・イン・イン・ | 文字列ブロック長 | | | | |
| H | ユーザ エージェント | | | | |
| V IV | 文字列ブロック タイプ(0) 文字列ブロック長 HTTP リファラ | | | | |
| 7 | | | | | |
| HTTP J | | | | | |
| | 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 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 3 8 5 6 7 8 9 0 1 2 3 | | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | | SSL /l | 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 SSI | 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 | SSL フローエ ラー | | | |
| | SS | SSL フロー エラー(続き) | | | | |
| | 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) | | | |
| み、 | SS | SSL フロー フラグ(続き) | | | | |
| | 文字列 | ブロック タイプ(0) | (続き) | 文字列ブロック長 | | |
| SSI | 文 | SSL サーバ名 | | | | |
| | | 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) | | | |



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

| | データ タ | |
|------------------------|-----------|---|
| フィールド | 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。 |
| レスポンダ IP ア ドレス | uint8[16] | IPアドレスオクテットの、開始ホストに応答したホストのIP アドレス。 |
| 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)。 |

表 B-36 接続統計データ ブロック 5.4+ のフィールド(続き)

| | データ タ | |
|---------------------------|-------------|---|
| フィールド | リーク ク イプ | 説明 |
| ノレーノレ ID | uint32 | イベントをトリガーしたルールの内部 ID(該当する場合)。 |
| ルール アク ション | uint16 | そのルールに対してユーザ インターフェイスで選択された アクション(allow、block など)。 |
| ルールの理由 | uint16 | イベントをトリガーしたルールの理由。 |
| イニシエータ ポート | uint16 | 開始ホストにより使用されるポート。 |
| レスポンダ ポート | uint16 | 応答ホストにより使用されるポート。 |
| TCP フラグ | uint16 | 接続イベントのすべての TCP フラグを示します。 |
| プロトコル | uint8 | IANA 指定のプロトコル番号。 |
| NetFlow ソース | uint8[16] | 接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。 |
| インスタンス ID (Instance ID) | uint16 | イベントを生成した管理対象デバイスの Snort インスタンス の数値 ID。 |
| 接続数カウンタ | uint16 | 同じ秒の間に発生する接続イベントを区別するために使用 される値。 |
| 最初のパケット タイムスタンプ | uint32 | セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。 |
| 最終パケット タ イムスタンプ | uint32 | セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。 |
| イニシエータ送 信パケット数 | uint64 | 開始ホストからの送信パケット数。 |
| レスポンダ送信 パケット数 | uint64 | 応答ホストが送信したパケット数。 |
| イニシエータ送 信バイト数 | uint64 | 開始ホストからの送信バイト数。 |
| レスポンダ送信 バイト数 | uint64 | 応答ホストから送信バイト数。 |
| 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)

| | データ タ | |
|-------------------------------|-------------|---|
| フィールド | ソーク ク 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 ο 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 o 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 o 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。 |

表 B-36 接続統計データ ブロック 5.4+ のフィールド(続き)

| | データ タ | |
|-----------------------|-----------|--|
| フィールド | イプ | 説明 |
| セキュリティ | uint8 | IP ブラックリストに一致した IP 層。 |
| インテリジェ | | |
| ンス層 | :16 | |
| ファイル イベント カウント | uint16 | 同じ秒で発生するファイル イベントを区別するために使用される値。 |
| 侵入イベント カ ウント | uint16 | 同じ秒で発生する侵入イベントを区別するために使用される値。 |
| イニシエータ の国 | uint16 | 開始ホストの国のコード。 |
| レスポンダの国 | uint 16 | 応答ホストの国のコード。 |
| 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 | uint16 | ホストがメンバーである VLAN を示す VLAN ID 番号。 |
| (Admin. VLAN | | |
| ID) 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)

| | データ タ | | |
|----------------------|-----------|--|--|
| フィールド | 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。 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)

| | データ タ | |
|--------------------|--------|--|
| フィールド | イプ | 説明 |
| 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。 |
| | | • o:「不明」 |
| | | • 1:「復号しない」 |
| | | • 2:「ブロックする」 |
| | | • 3:「リセットでブロック」 |
| | | • 4:「復号(既知のキー)」 |
| | | • 5:「復号(置換キー)」 |
| | | • 6:「復号(Resign)」 |
| 予期された SSL アクション | uint16 | SSL ルールに基づいて接続に対して実行する必要があるアクション。有効な値は次のとおりです。 |
| | | • 0:「不明」 |
| | | • 1:「復号しない」 |
| | | • 2:「ブロックする」 |
| | | • 3:「リセットでブロック」 |
| | | • 4:「復号(既知のキー)」 |
| | | • 5:「復号(置換キー)」 |
| | | • 6:「復号(Resign)」 |

表 B-36 接続統計データ ブロック 5.4+ のフィールド(続き)

| - | データ タ | |
|-------------------|--------|--|
| フィールド | イプ | 説明 |
| SSL フロー ス テータス | uint16 | SSL フローのステータス。アクションが実行された理由、またはエラーメッセージが出された理由を示す値です。有効な値は次のとおりです。 |
| | | • o:「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 | 詳細な SSL エラー コード。これらの値はサポート目的で必要とされる場合があります。 |

表 B-36 接続統計データ ブロック 5.4+ のフィールド(続き)

| | データ タ | |
|------------------|--------|---|
| フィールド | イプ | 説明 |
| SSL フローメッ セージ | uint32 | SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。 |
| | | • 0x00000001:NSE_MTHELLO_REQUEST |
| | | • 0x00000002:NSE_MTCLIENT_ALERT |
| | | • 0x00000004:NSE_MTSERVER_ALERT |
| | | • 0x00000008:NSE_MTCLIENT_HELLO |
| | | • 0x00000010:NSE_MTSERVER_HELLO |
| | | • 0x00000020:NSE_MTSERVER_CERTIFICATE |
| | | • 0x00000040:NSE_MTSERVER_KEY_EXCHANGE |
| | | • 0x00000080:NSE_MTCERTIFICATE_REQUEST |
| | | • 0x00000100:NSE_MTSERVER_HELLO_DONE |
| | | • 0x00000200:NSE_MTCLIENT_CERTIFICATE |
| | | • 0x00000400:NSE_MTCLIENT_KEY_EXCHANGE |
| | | 0x00000800:NSE_MTCERTIFICATE_VERIFY |
| | | 0x00001000: NSE_MTCLIENT_CHANGE_CIPHER_SPEC |
| | | • 0x00002000:NSE_MTCLIENT_FINISHED |
| | | • 0x00004000: NSE_MTSERVER_CHANGE_CIPHER_SPEC |
| | | • 0x00008000:NSE_MTSERVER_FINISHED |
| | | • 0x00010000:NSE_MTNEW_SESSION_TICKET |
| | | • 0x00020000:NSE_MTHANDSHAKE_OTHER |
| | | • 0x00040000:NSE_MTAPP_DATA_FROM_CLIENT |
| | | • 0x00080000:NSE_MTAPP_DATA_FROM_SERVER |
| SSL フロー フ ラグ | uint64 | 暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。 |
| | | • 0x00000001 (NSE_FLOWVALID):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_FLOWINITIALIZED):内部構造が処理可能です |
| | | • 0x00000004(NSE_FLOWINTERCEPT):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 o 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)。 |
| | | |

| | データ タ | |
|----------------------------|-----------|--|
| フィールド | 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。 |

表 B-36 接続統計データ ブロック 5.4+ のフィールド(続き)

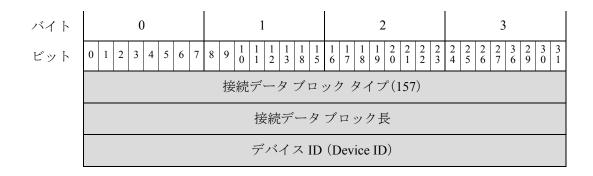
接続統計データ ブロック 5.4.1

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 1 1 1 1 1 1 8 | $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | $\begin{array}{c cccc} 1 & 2 & 2 & 2 \\ 9 & 0 & 1 & 2 \end{array}$ | 2 2 2 2 2 3 2 3 3 3 4 5 6 7 6 9 0 1 | | |
| | 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 | イス | | | |
| | | 入力インター | 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 アト | 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 I | Pアドレス | :(続き) | | | |
| | | レスポンダ I | Pアドレス | :(続き) | | | |
| | | レスポンダ I | P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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| | | 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) | rV ID | | |
| | ルールア | クション | ルール | の理由 | |
| | イニシエー | -タ ポート | レスポン | ダ ポート | |
| | TCP 7 | 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 | 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) | | |
| | イニシコ | レスポンダ Tx Packets | | | |
| | | | | | |
| | レスポ | ンダ送信パケット数 | (続き) | イニシエータ送 信バイト数 | |
| | | イニシエータ送信 | 言バイト数(続き) | | |
| | イニシ | エータ送信バイト数 | (続き) | レスポンダ Tx Bytes | |
| | | レスポンダ送信 | 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 1 1 2 3 8 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | レスポンダ送信バイト数(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 |
| <u>_</u> | Web アプリケーション ID(続き) | 文字列ブロック タイプ(0) |
| ライアント URL | 文字列ブロック タイプ(続き) | 文字列ブロック長 |
| 1 | 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 |
| (e)] | 文字列ブロック タイプ(0) | |
| NetBIOS [名前(Name) | 文字列ブロック長 | |
| Ne 图 | NetBIOS 名 | |
| ~ m \ | 文字列ブロック タイプ(0) | |
| アージョンツッツ | 文字列ブロック長 | |
| ケブケック・ブイング・ブーン・バー・ブーン・ブーン・ブーン・ブーン・ブーン・ブーン・ブーン・ブーン・ブーン・ブー | クライアント アプリケーション バージョン | <i>'</i> |
| | 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 | |

| | | 1 | 2 | | |
|---------|---|---------------|------------|-------------------|--|
| バイト | 0 1 2 3 4 5 6 7 | 1 1 1 1 1 1 1 | 2 | 3 2 2 2 2 3 2 3 3 | |
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 1 2 3 8 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 2 3 4 5 6 7 6 9 0 1 | | | | |
| | | · | | | |
| | | モニタノ | | | |
| | 小田上/、火 /= → /→ /- | モニタノ | | x . 1 2 | |
| | 秒開始送信元/宛先 | | ファイルイベ | | |
| | 侵入イベン | | イニシエ | | |
| | レスポン | · · · · | IOC : | 番号 | |
| | | 送信元自律 | | | |
| | CN II AT | 宛先自律 | | \ 111.£ | |
| | SNMP | | SNMP | | |
| | 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 | | | |
| K K | VLAN ID (Adm | nin. VLAN ID) | 文字列ブロッ | クタイプ(0) | |
| 参照ホスト | 文字列ブロック タイプ(0)(続き) | | 文字列ブ | ロック長 | |
| 160 | 文字列ブロッ | ,ク長(続き) | 参照ホ | スト | |
| л У | 文字列ブロック タイプ(0) | | | | |
| コージー | 文字列ブロック長 | | | | |
| , l | ユーザ エージェント | | | | |
| 1 | 文字列ブロック タイプ(0) | | | | |
| | 文字列ブロック長 | | | | |
| HTTP J7 | 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 3 3 4 5 6 7 6 9 0 1 |
| | SSL 証明書フィンガープリント(続き) | | | |
| | | SSL 証明書フィンプ | ブープリント(続き) | |
| | | SSL 証明書フィンプ | ブープリント(続き) | |
| | | SSL 証明書フィンプ | ブープリント(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 | | | |
| | 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(糸 | 売き) | SSL フロー フラグ |
| | | SSLフローフ | フラグ(続き) | |
| 名が | SS | Lフロー フラグ (続き | <u>\$</u>) | 文字列ブロック タイプ(0) |
| SSL サーバ名 | 文字列 | ブロック タイプ(0) | (続き) | 文字列ブロック長 |
| ISS | 文 | 字列ブロック長(続き | <u>(</u>) | 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 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | | 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 | ネットワーク分析オ | ポリシー リビジョン |
| | ネ | ットワーク分析ポリ | ンー リビジョン(続き | <u>*</u>) |
| | ネ | ットワーク分析ポリ | ンー リビジョン(続き | <u>*</u>) |
| | ネ | ットワーク分析ポリ | ンー リビジョン(続き | <u>*</u>) |
| | ネットワーク分析; ン(約 | | | |

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

| | データ タ | |
|------------------------|--------|---|
| フィールド | 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)

| | データ タ | |
|----------------------------|-----------|--|
| フィールド | 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。 |
| レスポンダ IP ア ドレス | uint8[16] | IPアドレス オクテットの、開始ホストに応答したホストの IP アドレス。 |
| 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。 |
| レスポンダ ポート | uint16 | 応答ホストにより使用されるポート。 |
| TCP フラグ | uint16 | 接続イベントのすべての TCP フラグを示します。 |
| プロトコル | uint8 | IANA 指定のプロトコル番号。 |
| NetFlow ソース | uint8[16] | 接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。 |
| インスタンス ID (Instance ID) | uint16 | イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。 |
| 接続数カウンタ | uint16 | 同じ秒の間に発生する接続イベントを区別するために使用 される値。 |
| 最初のパケット タイムスタンプ | uint32 | セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。 |
| 最終パケット タ イムスタンプ | uint32 | セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。 |
| イニシエータ送 信パケット数 | uint64 | 開始ホストからの送信パケット数。 |
| レスポンダ送信 パケット数 | uint64 | 応答ホストが送信したパケット数。 |
| イニシエータ送 信バイト数 | uint64 | 開始ホストからの送信バイト数。 |

表 B-37 接続統計データ ブロック 5.4+ のフィールド(続き)

| | データ タ | |
|------------------------------|--------|---|
| フィールド | イプ | 説明 |
| レスポンダ送信 バイト数 | uint64 | 応答ホストから送信バイト数。 |
| 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 o 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 o 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 o 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)

| | データ タ | |
|-------------------------------|-----------|--|
| フィールド | 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。 |
| レスポンダの国 | 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)

| | データ タ | |
|--------------------------------|-----------|---|
| フィールド | 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)

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

表 B-37 接続統計データ ブロック 5.4+ のフィールド(続き)

| | データ タ | |
|-------------------|--------|--|
| フィールド | イプ | 説明 |
| SSL フロー ス テータス | uint16 | SSL フローのステータス。アクションが実行された理由、またはエラーメッセージが出された理由を示す値です。有効な値は次のとおりです。 |
| | | • 0:「不明」 |
| | | • 1:「一致しない」 |
| | | • 2:「成功」 |
| | | • 3:「キャッシュされていないセッション」 |
| | | • 4:「不明の暗号化スイート」 |
| | | • 5:「サポートされていない暗号スイート」 |
| | | • 6:「サポートされていない SSL バージョン」 |
| | | 7:「使用される SSL 圧縮」 |
| | | • 8:「パッシブ モードで復号不可のセッション」 |
| | | • 9:「ハンドシェイク エラー」 |
| | | • 10:「復号エラー」 |
| | | • 11:「保留中のサーバ名カテゴリ 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 | 詳細な SSL エラー コード。これらの値はサポート目的で必要とされる場合があります。 |

表 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 イブ 説明 SSL フローメッ uint32 SSL フローメッ uint32 SSL ハンドシェイク時にクラ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。 0x00000001:NSE_MT_HELLO_REQUEST 0x00000002:NSE_MT_CLIENT_ALERT 0x00000001:NSE_MT_SERVER_ALERT 0x00000001:NSE_MT_SERVER_ALERT 0x00000001:NSE_MT_SERVER_HELLO 0x00000001:NSE_MT_SERVER_HELLO 0x00000001:NSE_MT_SERVER_KEY_EXCHANGE 0x00000001:NSE_MT_SERVER_KEY_EXCHANGE 0x00000001:NSE_MT_CLIENT_CERTIFICATE 0x00000001:NSE_MT_CLIENT_CERTIFICATE 0x00000001:NSE_MT_CLIENT_KEY_EXCHANGE 0x000000001:NSE_MT_CLIENT_KEY_EXCHANGE 0x000000001:NSE_MT_CLIENT_FINISHED 0x000000001:NSE_MT_CLIENT_FINISHED 0x000000001:NSE_MT_SERVER_FINISHED 0x000000001:NSE_MT_SERVER_FINISHED 0x000000001:NSE_MT_NEW_SESSION_TICKET 0x000000001:NSE_MT_APP_DATA_FROM_CLIENT 0x000000001:NSE_MT_APP_DATA_FROM_SERVER 0x000000001:NSE_MT_APP_DATA_FROM_SERVER 0x000000001:NSE_MT_APP_DATA_FROM_SERVER 0x000000001:NSE_FLOW_INITIALIZED): 内部構造が処理のです。 0x000000002(NSE_FLOW_INITIALIZED): 内部構造が処理のです。 0x000000002(NSE_FLOW_INITIALIZED): 内部構造が処理のです。 0x0000000002(NSE_FLOW_INITIALIZED): 内部構造が処理のです。 0x0000000002(NSE_FLOW_INITIALIZED): 内部構造が処理のです。 0x0000000000000000000000000000000000 | | データ タ | |
|--|--------------|--------|---|
| 換されたメッセージ。詳細については、 | フィールド | | 説明 |
| ・ 0x00000002:NSE_MTCLIENT_ALERT ・ 0x00000004:NSE_MTSERVER_ALERT ・ 0x00000004:NSE_MTSERVER_ALERT ・ 0x000000010:NSE_MTSERVER_HELLO ・ 0x000000010:NSE_MTSERVER_HELLO ・ 0x000000010:NSE_MTSERVER_CERTIFICATE ・ 0x000000010:NSE_MTSERVER_KEY_EXCHANGE ・ 0x00000010:NSE_MTCERTIFICATE_REQUEST ・ 0x00000100:NSE_MTCLIENT_CERTIFICATE ・ 0x00000000:NSE_MTCLIENT_CERTIFICATE ・ 0x00000000:NSE_MTCLIENT_KEY_EXCHANGE ・ 0x00000000:NSE_MTCLIENT_FINISHED ・ 0x00000000:NSE_MTCLIENT_FINISHED ・ 0x00000000:NSE_MTSERVER_FINISHED ・ 0x00000000:NSE_MTSERVER_FINISHED ・ 0x00000000:NSE_MTHANDSHAKE_OTHER ・ 0x00000000:NSE_MTAPP_DATA_FROM_SERVER SSL_フローフ が は | | uint32 | 換されたメッセージ。詳細については、 |
| 0x00000001:NSE_MT_CLIENT_HELLO | | | • 0x00000001:NSE_MTHELLO_REQUEST |
| 0x00000008:NSE_MT_CLIENT_HELLO | | | • 0x00000002:NSE_MTCLIENT_ALERT |
| 0x00000010:NSE_MT_SERVER_HELLO | | | • 0x00000004:NSE_MTSERVER_ALERT |
| | | | • 0x00000008:NSE_MTCLIENT_HELLO |
| 0x00000040:NSE_MT_SERVER_KEY_EXCHANGE | | | • 0x00000010:NSE_MTSERVER_HELLO |
| 0x00000080:NSE_MT_CERTIFICATE_REQUEST 0x00000100:NSE_MT_SERVER_HELLO_DONE 0x00000200:NSE_MT_CLIENT_CERTIFICATE 0x000000400:NSE_MT_CLIENT_CERTIFICATE 0x000000800:NSE_MT_CLIENT_KEY_EXCHANGE 0x0000000000:NSE_MT_CERTIFICATE_VERIFY 0x0000101000:NSE_MT_CLIENT_CHANGE_CIPHER_SPEC 0x00002000:NSE_MT_CLIENT_FINISHED 0x000010000:NSE_MT_SERVER_FINISHED 0x00010000:NSE_MT_NEW_SESSION_TICKET 0x00010000:NSE_MT_HANDSHAKE_OTHER 0x00010000:NSE_MT_APP_DATA_FROM_CLIENT 0x00010000:NSE_MT_APP_DATA_FROM_SERVER SSL フローフ | | | • 0x00000020:NSE_MTSERVER_CERTIFICATE |
| ・ 0x00000100:NSE_MT_SERVER_HELLO_DONE ・ 0x00000200:NSE_MT_CLIENT_CERTIFICATE ・ 0x000000400:NSE_MT_CLIENT_KEY_EXCHANGE ・ 0x00000000:NSE_MT_CERTIFICATE_VERIFY ・ 0x000001000: NSE_MT_CLIENT_CHANGE_CIPHER_SPEC ・ 0x000002000:NSE_MT_CLIENT_FINISHED ・ 0x00000000:NSE_MT_SERVER_FINISHED ・ 0x0000000:NSE_MT_NEW_SESSION_TICKET ・ 0x000010000:NSE_MT_HANDSHAKE_OTHER ・ 0x00010000:NSE_MT_APP_DATA_FROM_CLIENT ・ 0x00010000:NSE_MT_APP_DATA_FROM_SERVER SSL フロー フ | | | • 0x00000040:NSE_MTSERVER_KEY_EXCHANGE |
| | | | • 0x00000080:NSE_MTCERTIFICATE_REQUEST |
| | | | • 0x00000100:NSE_MTSERVER_HELLO_DONE |
| | | | • 0x00000200:NSE_MTCLIENT_CERTIFICATE |
| ・ 0x00001000: NSE_MT_CLIENT_CHANGE_CIPHER_SPEC | | | • 0x00000400:NSE_MTCLIENT_KEY_EXCHANGE |
| NSE_MTCLIENT_CHANGE_CIPHER_SPEC | | | • 0x00000800:NSE_MTCERTIFICATE_VERIFY |
| 0x000040000: NSE_MT_SERVER_CHANGE_CIPHER_SPEC | | | |
| NSE_MTSERVER_CHANGE_CIPHER_SPEC | | | • 0x00002000:NSE_MTCLIENT_FINISHED |
| 0x00010000:NSE_MTNEW_SESSION_TICKET 0x00020000:NSE_MTHANDSHAKE_OTHER 0x00040000:NSE_MTAPP_DATA_FROM_CLIENT 0x00080000:NSE_MTAPP_DATA_FROM_SERVER SSL フローフ juint64 暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。 0x00000001(NSE_FLOWVALID):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_FLOWINITIALIZED):内部構造が処理可能です 0x00000004(NSE_FLOWINTERCEPT):SSL セッションが代行受信されました 文字列ブロック uint32 文字列ブロック 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 uint32 | | | |
| 0x00020000:NSE_MTHANDSHAKE_OTHER 0x00040000:NSE_MTAPP_DATA_FROM_CLIENT 0x00080000:NSE_MTAPP_DATA_FROM_SERVER SSL フローフラグ。有効な値は次のとおりです。 0x00000001(NSE_FLOWVALID):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_FLOWINITIALIZED):内部構造が処理可能です 0x00000004(NSE_FLOWINTERCEPT):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 立x5列ブロックは言まれるバイト数(ブ | | | • 0x00008000:NSE_MTSERVER_FINISHED |
| ・ 0x00040000:NSE_MT_APP_DATA_FROM_CLIENT・ 0x00080000:NSE_MT_APP_DATA_FROM_SERVERSSL フローフラグ暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。・ 0x00000001 (NSE_FLOW_VALID):他のフィールドを有効にするために設定する必要があります・ 0x00000002 (NSE_FLOW_INITIALIZED):内部構造が処理可能です・ 0x00000004 (NSE_FLOW_INTERCEPT):SSL セッションが代行受信されました文字列ブロックタイプuint32文字列ブロッuint32文字列ブロッuint32以字列ブロッuint32以字列ブロッuint32以字列ブロックに含まれるバイト数(ブ | | | • 0x00010000:NSE_MTNEW_SESSION_TICKET |
| • 0x00080000:NSE_MT_APP_DATA_FROM_SERVERSSL フローフラグ暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。• 0x00000001 (NSE_FLOW_VALID):他のフィールドを有効にするために設定する必要があります• 0x00000002 (NSE_FLOW_INITIALIZED):内部構造が処理可能です• 0x00000004 (NSE_FLOW_INTERCEPT):SSL セッションが代行受信されました文字列ブロックタイプuint32文字列ブロッuint32文字列ブロッuint32女字列ブロッuint32女字列ブロッ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 | | | • 0x00020000:NSE_MTHANDSHAKE_OTHER |
| SSL フローフラグ uint64 暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。 • 0x00000001 (NSE_FLOW_VALID):他のフィールドを有効にするために設定する必要があります • 0x00000002 (NSE_FLOW_INITIALIZED):内部構造が処理可能です • 0x00000004 (NSE_FLOW_INTERCEPT):SSL セッションが代行受信されました 文字列ブロックタイプ uint32 SSL サーバ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 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 | | | • 0x00040000:NSE_MTAPP_DATA_FROM_CLIENT |
| ラグです。• 0x00000001 (NSE_FLOWVALID):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_FLOWINITIALIZED):内部構造が処理可能です• 0x00000004 (NSE_FLOWINTERCEPT):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wint32文字列ブロッuint32文字列ブロッuint32文字列ブロッuint32以字列ブロッuint32 | | | • 0x00080000:NSE_MTAPP_DATA_FROM_SERVER |
| 効にするために設定する必要があります• 0x00000002 (NSE_FLOWINITIALIZED): 内部構造が処理可能です• 0x00000004 (NSE_FLOWINTERCEPT): 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vint32文字列ブロックuint32SSL 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vint32V字列ブロッ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 | | uint64 | |
| 理可能です | | | |
| 文字列ブロック タイプuint32SSL 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 o です。文字列ブロッuint32SSL サーバ名文字列データ ブロックに含まれるバイト数(ブ | | | · |
| タイプ の値は常に o です。 文字列ブロッ 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 | | | |
| | | uint32 | |
| SSL サーバ名フィールドのバイト数を含む)。 | 文字列ブロッ ク長 | uint32 | 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 |

| 表 B-37 接続統計データ | ' ブロック 5.4+ のフィールド(続き) |
|----------------|------------------------|
|----------------|------------------------|

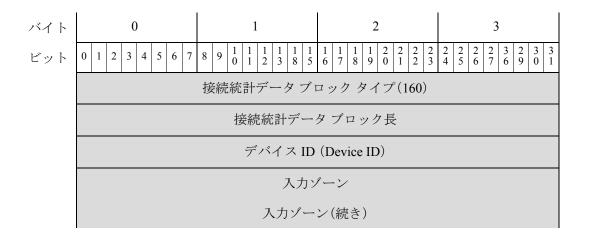
| | データ タ | |
|----------------------------|-----------|---|
| フィールド | イプ | 説明 |
| SSL サーバ名 | string | SSL Client Hello でサーバ名に指定された名前。 |
| SSL URL カテ ゴリ | uint32 | サーバ名と証明書の共通名から識別されるフローのカテゴリ。 |
| SSL セッション ID | uint8[32] | クライアントとサーバがセッションの再利用に同意する場合に、SSLハンドシェイク時に使用されるセッション ID の値 |
| SSL セッション ID の長さ | 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。 |

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 1 1 1 1 1 1 8 | 1 1 1 1 1 2 2 2 5 6 7 8 9 0 1 2 | 2 2 2 2 2 3 2 3 3 3 4 5 6 7 6 9 0 1 |
| | _ | | | |
| | | 入力ゾ | ーン(続き) | |
| | | 出力 | ウゾーン | |
| | | 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 | ーフェイス(続き) | |
| | | 入力インター | ーフェイス(続き) | |
| | | 入力インター | 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 [] | Pアドレス(続き) | |
| | | レスポンダ [] | Pアドレス(続き) | |
| | | レスポンダ II | P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 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 3 3 4 5 6 7 6 9 0 1 |
| | | ポリシー リビジョン(続き) | | |
| | | ルー | vV ID | |
| | ルールア | クション | ルール | の理由 |
| | ルールの理 | 里由(続き) | イニシエー | -タ ポート |
| | レスポンク | ダポート | TCP 7 | フラグ |
| | プロトコル | | NetFlow ソース | |
| | | NetFlow ソ | | |
| | | NetFlow ソ | | |
| | | NetFlow ソ | | |
| | NetFlow ソース (続き) | インスタンスI | D (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 タイムスク | 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 | 卜数 |
| | | 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) | レフ | スポンダ送信パケット | 、数 |
| | | レスポンダ送信ノ | ペケット数(続き) | |
| | レスポンダ送信パ ケット数(続き) | イニ | ニシエータ送信バイト | 、数 |
| | | イニシエータ送信 | 言バイト数(続き) | |
| | イニシエータ送信 バイト数(続き) | V | スポンダ送信バイト | 数 |
| | | レスポンダ送信 | バイト数(続き) | |
| | レスポンダ送信 バイト数(続き) | | ユーザ ID (User ID) | |

| バイト | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 2 3 2 3 3 8 9 0 1 2 3 4 5 6 7 6 9 0 1 | |
|-----------------------|-------------------------------|---|--|
| ビット | | | |
| | 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 | |
| <u> </u> | Web アプリケー ション ID(続き) | String ブロック タイプ(0) | |
| ライアン URL | 文字列ブロック タイプ(続き) | 文字列ブロック長 | |
| 1 | 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 | |
| (e)] | 文字列ブロック タイプ(0) | | |
| tBIOS (Nam | 文字列ブロック長 | | |
| NetBIOS [名前(Name)] | NetBIOS 名 | | |
| | 文字列ブロック タイプ(0) | | |
| ア ジ ソ ツ ジ | 文字列ブロック長 | | |
| クライアプリケ | 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | モニタ ルール 6 | | | |
| | | モニタノ | レールフ | |
| | | モニタノ | レール8 | |
| | 秒開始送信元/宛先 | 秒イニシエータ層 | ファイルイベ | ントカウント |
| | 侵入イベン | トカウント | イニシエ | ータの国 |
| | レスポン | /ダの国 | IOC : | 番号 |
| | | 送信元自律 | きシステム | |
| | | 宛先自律 | システム | |
| | SNMP | · 入力 | SNMF | 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) | |
| <u>~</u> | VLAN ID (Admin. VLAN ID) 文字列ブロック タイプ (0) | | | クタイプ(0) |
| 照ホス | 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 | ック長(続き) | 参照ホ | スト |
| * > | | 文字列ブロッ | クタイプ(0) | |
| サーガーン・イン・イン・イン・イン・イン・イン・イン・イン・イン・イン・イン・イン・イン | 文字列ブロック長 | | | |
| H | ユーザ エージェント | | | |
| IV Y | 文字列ブロック タイプ(0) | | | |
| Į V | 文字列ブロック長 | | | |
| HTTP | | нттр у | ファラ | |
| | | SSL 証明書フィ | ンガープリント | |
| | | | | |

| E | バイト | 0 | 1 | 2 | 3 |
|---|----------|------------------------------|-----------------------|---|---|
| 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 パージョン SSL キー証明書 | ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| 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 ボー証明書統計(続き) SSL キー証明書 実際の SSL アクション 予期された SSL アクション SSL フローステータス SSL フローエラー(続き) SSL フローメッセージ(続き) SSL フロー フラグ(続き) SSL フローフラグ(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 ポリシー ID (続き) SSL ルール ID SSL 昨号スイート SSL パージョン SSL キー証明書統計 (続き) 字期された 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 SSL フロー エラー (続き) SSL フロー エラー (続き) SSL フロー エラー (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 SSL フロー フラグ (続き) 文字列ブロック タイブ(0) 文字列ブロック タイブ(0) (続き) 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 セッシュ ID SSL セッシュ ID SSL セッション ID SSL セッシュ ID SSL セッシュ ID SSL セッシュ ID SSL セッション ID SSL セッシュ ID SSL セッション ID SSL セッシュ ID | | | SSL 証明書フィンス | ガープリント(続き) | |
| 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 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 (続き) 予期された SSL アクション 予期された SSL アクション SSL フロー ステータス SSL フローエラー (続き) SSL フロー エラー (続き) SSL フロー メッセージ (続き) SSL フロー フラグ (続き) SSL フローフラグ (続き) | | | SSL 証明書フィンス | ガープリント(続き) | |
| 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 ポリシー ID(続き) SSL ルール ID SSL 暗号スイート SSL アクション SSL キー証明書 統計(続き) 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(続き) SSL フロー フラグ(続き) SSL フローフラグ(続き) | | | SSL 証明書フィンス | ガープリント(続き) | |
| 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 (続き) 実際の SSL アクション 予期された SSL アクション アクション SSL フロー エテータス SSL フローエラー (続き) 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 SSL フロー フラグ (続き) SSL フロー フラグ 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) 文字列ブロック長 文字列ブロック長 ※ SSL サーバ名 SSL セッション ID SSL セッシュー ID SSL セッション ID SS | | | SSLポリ | リシー ID | |
| 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 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 予期された SSL アクション SSL フロー エテータス SSL フローエ | | | SSL ポリシ | ー ID(続き) | |
| SSL ルール ID SSL キー証明書統 | | | SSL ポリシ | ー ID(続き) | |
| SSL 暗号スイート | | | SSL ポリシ | ー ID(続き) | |
| 計 | | | SSLル | ール ID | |
| 統計(続き) | | SSL 暗号。 | スイート | SSLバージョン | |
| クション(続き) ラー SSL フローエラー(続き) SSL フローメッセージ(続き) SSL フローフラグ(続き) SSL フローフラグ(続き) X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 セッション ID SSL セッション ID(続き) | | | 実際の SSL | アクション | |
| ヤージ 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) 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 文字列ブロック長 文字列ブロック長 文字列ブロック長 SSL サーバ名 SSL セッション ID SSL セッシュ ID SSL セッション ID SSL セッシュ ID SSL セッ | | | | ステータス | |
| 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 身イプ(0) 文字列ブロック長(続き) 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 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 フローメッセージ(続き) SSL フロー フラグ | | | SSL フロー フラグ |
| グライプ(0) 女字列ブロック 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 フロー フラグ (続き) | | | |
| SSL URL カテゴリ SSL セッション ID SSL セッション ID(続き) | 光 | | | | |
| SSL URL カテゴリ SSL セッション ID SSL セッション ID(続き) | + | 文字列ブロック タイプ(0)(続き) 文字列ブロック: | | | 文字列ブロック長 |
| SSL セッション ID SSL セッション ID(続き) | SSI | 文字列ブロック長(続き) SSL サーバ名 | | | SSL サーバ名 |
| SSL セッション ID(続き) | | 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 | ıンID(続き) | |

| バイト | 0 | 1 | 2 | 3 |
|-----|---------------------|-----------------------|---|---------------------------------|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | | 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 | ネットワーク分析オ | 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 | <u>*</u>) |
| | ネ | ットワーク分析ポリ | シー リビジョン(続き | <u>*</u>) |
| | ネ | ットワーク分析ポリ | シー リビジョン(続き | <u>*</u>) |
| | ネットワーク分析: ン(約 | | エンドポイント | プロファイル ID |
| | エンドポイントプき | | 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 | ∃ 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 V | スポンス |
| | HTTP レスオ | ペンス(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 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | 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 | | | 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

| | データ タ | |
|------------------------|-----------|---|
| フィールド | 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。 |
| レスポンダ IP ア ドレス | uint8[16] | IPアドレスオクテットの、開始ホストに応答したホストのIP アドレス。 |

表 B-38 接続統計データ ブロック 6.0.x のフィールド(続き)

| | データ タ | |
|---------------------------|-------------|--|
| フィールド | ナータ 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 | uint32 | イベントをトリガーしたルールの理由。 |
| イニシエータポート | uint16 | 開始ホストにより使用されるポート。 |
| レスポンダ ポート | uint16 | 応答ホストにより使用されるポート。 |
| TCP フラグ | uint16 | 接続イベントのすべての TCP フラグを示します。 |
| プロトコル | uint8 | IANA 指定のプロトコル番号。 |
| NetFlow ソース | uint8[16] | 接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。 |
| インスタンス ID (Instance ID) | uint16 | イベントを生成した管理対象デバイスの Snort インスタンス の数値 ID。 |
| 接続数カウンタ | uint16 | 同じ秒の間に発生する接続イベントを区別するために使用される値。 |
| 最初のパケット タイムスタンプ | uint32 | セッションで最初のパケットが交換された日時の UNIX タイムスタンプ。 |
| 最終パケット タ イムスタンプ | uint32 | セッションで最後のパケットが交換された日時の UNIX タイムスタンプ。 |
| イニシエータ送 信パケット数 | uint64 | 開始ホストからの送信パケット数。 |
| レスポンダ送信 パケット数 | uint64 | 応答ホストが送信したパケット数。 |
| イニシエータ送 信バイト数 | uint64 | 開始ホストからの送信バイト数。 |
| レスポンダ送信 バイト数 | uint64 | 応答ホストから送信バイト数。 |
| 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)

| | データ タ | |
|------------------------------|--------|---|
| フィールド | 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 o 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 o 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 o 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)

| | データ タ | |
|--------------------------------|-------------|--|
| フィールド | アータ 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。 |
| レスポンダの国 | 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 o 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 o 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)

| | データ タ | |
|----------------------|-----------|--|
| フィールド | 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 o 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。 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)

| | データ タ | |
|--------------------|--------|--|
| フィールド | イプ | 説明 |
| 実際の SSL アクション | uint16 | SSL ルールに基づいて接続に対して実行されたアクション。 ルールに指定されているアクションが不可能なことがある ため、これは予期していたアクションとは異なることがあり ます。有効な値は次のとおりです。 |
| | | • 0:「不明」 |
| | | • 1:「復号しない」 |
| | | • 2:「ブロックする」 |
| | | • 3:「リセットでブロック」 |
| | | • 4:「復号(既知のキー)」 |
| | | • 5:「復号(置換キー)」 |
| | | • 6:「復号(Resign)」 |
| 予期された SSL アクション | uint16 | SSL ルールに基づいて接続に対して実行する必要があるアクション。有効な値は次のとおりです。 |
| | | • 0:「不明」 |
| | | • 1:「復号しない」 |
| | | • 2:「ブロックする」 |
| | | • 3:「リセットでブロック」 |
| | | • 4:「復号(既知のキー)」 |
| | | • 5:「復号(置換キー)」 |
| | | • 6:「復号(Resign)」 |

表 B-38 接続統計データ ブロック 6.0.x のフィールド(続き)

| | データ タ | |
|-------------------|--------|--|
| フィールド | イプ | 説明 |
| SSL フロー ス テータス | uint16 | SSL フローのステータス。アクションが実行された理由、またはエラーメッセージが出された理由を示す値です。有効な値は次のとおりです。 |
| | | • 0:「不明」 |
| | | 1:「一致しない」 |
| | | • 2:「成功」 |
| | | • 3:「キャッシュされていないセッション」 |
| | | • 4:「不明の暗号化スイート」 |
| | | • 5:「サポートされていない暗号スイート」 |
| | | • 6:「サポートされていない SSL バージョン」 |
| | | 7:「使用される SSL 圧縮」 |
| | | • 8:「パッシブ モードで復号不可のセッション」 |
| | | • 9:「ハンドシェイク エラー」 |
| | | • 10:「復号エラー」 |
| | | • 11:「保留中のサーバ名カテゴリ 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 | 詳細な SSL エラー コード。これらの値はサポート目的で必要とされる場合があります。 |

表 B-38 接続統計データ ブロック 6.0.x のフィールド(続き)

| | データ タ | | | | | |
|------------------|--------|---|--|--|--|--|
| フィールド | イプ | 説明 | | | | |
| SSL フローメッ セージ | uint32 | SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。 | | | | |
| | | • 0x00000001:NSE_MTHELLO_REQUEST | | | | |
| | | • 0x00000002:NSE_MTCLIENT_ALERT | | | | |
| | | • 0x00000004:NSE_MTSERVER_ALERT | | | | |
| | | • 0x00000008:NSE_MTCLIENT_HELLO | | | | |
| | | • 0x00000010:NSE_MTSERVER_HELLO | | | | |
| | | • 0x00000020:NSE_MTSERVER_CERTIFICATE | | | | |
| | | • 0x00000040:NSE_MTSERVER_KEY_EXCHANGE | | | | |
| | | • 0x00000080:NSE_MTCERTIFICATE_REQUEST | | | | |
| | | • 0x00000100:NSE_MTSERVER_HELLO_DONE | | | | |
| | | • 0x00000200:NSE_MTCLIENT_CERTIFICATE | | | | |
| | | • 0x00000400:NSE_MTCLIENT_KEY_EXCHANGE | | | | |
| | | • 0x00000800:NSE_MTCERTIFICATE_VERIFY | | | | |
| | | • 0x00001000: NSE_MTCLIENT_CHANGE_CIPHER_SPEC | | | | |
| | | • 0x00002000:NSE_MTCLIENT_FINISHED | | | | |
| | | • 0x00004000: NSE_MTSERVER_CHANGE_CIPHER_SPEC | | | | |
| | | • 0x00008000:NSE_MTSERVER_FINISHED | | | | |
| | | • 0x00010000:NSE_MTNEW_SESSION_TICKET | | | | |
| | | • 0x00020000:NSE_MTHANDSHAKE_OTHER | | | | |
| | | • 0x00040000:NSE_MTAPP_DATA_FROM_CLIENT | | | | |
| | | • 0x00080000:NSE_MTAPP_DATA_FROM_SERVER | | | | |
| SSL フロー フ ラグ | uint64 | 暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。 | | | | |
| | | • 0x00000001 (NSE_FLOWVALID):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_FLOWINITIALIZED):内部構造が処理可能です | | | | |
| | | • 0x00000004(NSE_FLOWINTERCEPT):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 o 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)

| | データ タ | |
|-------------------------------------|-----------|--|
| フィールド | 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 o 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)

| | データ タ | | | | | | | |
|-----------------------------|----------|---|--|--|--|--|--|--|
| フィールド | イプ | 説明 | | | | | | |
| DNS レスポンス | uint16 | o(NoError):エラーなし | | | | | | |
| タイプ | | 1(FormErr):フォーマットエラー | | | | | | |
| | | 2(ServFail):サーバ障害 | | | | | | |
| | | 3(NXDomain):存在していないドメイン | | | | | | |
| | | 4(NotImp):未実装 | | | | | | |
| | | 5(Refused):クエリ拒否 | | | | | | |
| | | 6(YXDomain):名前が存在してはならない状況で存在している | | | | | | |
| | | 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 | | | | | | |
| | | 8(NXRRSet):存在しているべき RR セットが存在していない | | | | | | |
| | | 9(NotAuth):未承認 | | | | | | |
| | | 10(NotZone):名前がゾーンに含まれていない | | | | | | |
| | | 16(BADSIG):TSIG 署名失敗 | | | | | | |
| | | 17(BADKEY):キーが認識されない | | | | | | |
| | | 18(BADTIME):時間範囲外の署名 | | | | | | |
| | | 19 (BADMODE):不適切な TKEY モード | | | | | | |
| | | 20(BADNAME):重複するキー名 | | | | | | |
| | | 21(BADALG):サポートされていないアルゴリズム | | | | | | |
| | | 22(BADTRUNC):不適切な切り捨て | | | | | | |
| | | 3841 (NXDOMAIN) : ファイアウォールからの NXDOMAIN 応答 | | | | | | |
| | | 3842(SINKHOLE):ファイアウォールからのシンクホール 応答 | | | | | | |
| 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 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 | | | | | | | | | |
| | | 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》 | ブーン | | | | | | | |
| | | 入力ゾー | ン(続き) | | | | | | | |
| | | 入力ゾー | ン(続き) | | | | | | | |
| | | 入力ゾー | ン(続き) | | | | | | | |
| | | 出力》 | ブーン | | | | | | | |
| | 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 | フェイス(続き) | | | | | | | |
| | | 出力インタ | ーフェイス | | | | | | | |

| バイト | 0 | 1 | 2 | 3 | | | | | |
|-----|--------------------------|---------------------|--------------------------------------|------------------------------------|--|--|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | | | |
| | | 出力インターフ | フェイス(続き) | | | | | | |
| | | 出力インターフ | 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 フ | アドレス(続き) | | | | | | |
| | | レスポンダ IP フ | アドレス(続き) | | | | | | |
| | | レスポンダ IP フ | 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 | 里由(続き) | イニシエー | ータ ポート | | | | | |
| | レスポン | ダポート | TCP 7 | 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 1 1 2 3 8 5 6 7 8 9 0 1 2 3 4 5 6 7 6 9 0 1 | | | | | | | |
| | 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) | レスポンダ送信パケット数 | | | | | | | |
| | | レスポンダ送信パケット数(続き) | | | | | | | |
| | レスポンダ送信パ ケット数(続き) | イニシエータ送信バイト数 | | | | | | | |
| | | イニシエータ送信バイト数(続き) | | | | | | | |
| | イニシエータ送信 バイト数(続き) | レスポンダ送信パケット数 | | | | | | | |
| | | レスポンダ送信バイト数(続き) | | | | | | | |
| | レスポンダ送信 バイト数(続き) | イニシエータ パケット ドロップ | | | | | | | |
| | | イニシエータ パケット ドロップ(続き) | | | | | | | |
| | イニシエータパ ケットドロップ (続き) | レスポンダ パケット ドロップ | | | | | | | |
| | | レスポンダ パケット ドロップ(続き) | | | | | | | |
| | レスポンダパ ケットドロップ (続き) | ドロップしたイニシエータ バイト数 | | | | | | | |
| | | イニシエータ バイト ドロップ(続き) | | | | | | | |

| バイト | 0 | 1 2 3 | | | | | | | | |
|---------------------|-------------------------------------|---|--|--|--|--|--|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 2 3 8 5 6 7 8 9 0 1 2 3 4 5 6 7 6 9 0 1 | | | | | | | | |
| | イニシエータバイ ト ドロップ(続き) | レスポンダ バイト ドロップ | | | | | | | | |
| | | レスポンダ バイト ドロップ(続き) | | | | | | | | |
| | レスポンダバイト ドロップ(続き) QOS 適用インターフェイス | | | | | | | | | |
| | | QOS 適用インターフェイス (続き) | | | | | | | | |
| | | QOS 適用インターフェイス (続き) | | | | | | | | |
| | | QOS 適用インターフェイス (続き) | | | | | | | | |
| | QOS インター フェイス(続き) | QOS ルール ID | | | | | | | | |
| | QOS ルール ID (続き) ユーザ 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 | | | | | | | | |
| <u> </u> | 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 URL | 文字列ブロック タイプ(続き) | 文字列ブロック長 | | | | | | | | |
| 7 | 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 | | | | | | | | |
| S ne)] | | 文字列ブロック タイプ(0) | | | | | | | | |
| NetBIOS 前 (Name) | | 文字列ブロック長 | | | | | | | | |
| N 經 經 | NetBIOS 名 | | | | | | | | | |

| バイト ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 8 5 | 2 3 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 2 3 3 3 5 6 7 8 9 0 1 2 3 4 5 6 7 6 9 0 1 | | | | | | | | | |
|---|-----------------|-------------------------|--|---------------|--|--|--|--|--|--|--|--|
| | 文字列ブロック タイプ(0) | | | | | | | | | | | |
| \ \frac{\gamma}{\gamma} \gamma \qquad \qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq | | | | | | | | | | | | |
| イヤージージョンジョンジョ | 文字列ブロック長 | | | | | | | | | | | |
| アプレンジング | <i>D</i> | 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 | | | | | | | | | | | |
| | | モニタノ | レール 5 | | | | | | | | | |
| | モニタ ルール 6 | | | | | | | | | | | |
| | | モニタノ | レールフ | | | | | | | | | |
| | | モニタノ | レール8 | | | | | | | | | |
| | 秒開始送信元/宛先 | 秒イニシエータ層 | ファイルイベ | ントカウント | | | | | | | | |
| | 侵入イベン | トカウント | イニシエ | ータの国 | | | | | | | | |
| | レスポン | / ダの国 | クライアントの (Original Cli | | | | | | | | | |
| | IOC | 番号 | 送信元自律 | きシステム | | | | | | | | |
| | 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 | | | | | | | | |
| | SNMF |) 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 | ノテキスト(続き) | VLAN ID (Adn | nin. VLAN ID) | | | | | | | | |

| バイト | 0 1 2 3 4 5 6 7 | 3 2 2 2 2 3 2 3 3 | | | | | |
|-------------|-------------------------------------|-------------------|------------|--|--|--|--|
| ビット | 0 1 2 3 4 3 6 7 | 0 1 2 3 8 3 | | 2 2 2 2 3 3 3 4 5 6 7 6 9 0 1 | | | |
| κ ~ | 文字列ブロック タイプ(0) | | | | | | |
| 参照ホス | | | ロック長 | | | | |
| 160 | | | · スト | | | | |
| サーベイン・サーベート | | | クタイプ(0) | | | | |
| 1 % H | | | `ロック長 | | | | |
| H | | ユーザ エー | -ジェント | | | | |
| V IV | | 文字列ブロッ | クタイプ(0) | | | | |
| U 7 ; | | 文字列ブ | ロック長 | | | | |
| HTTP J 7 | | нттр у | ファラ | | | | |
| | | SSL 証明書フィ | ンガープリント | | | | |
| | | SSL 証明書フィンス | ガープリント(続き) | | | | |
| | | SSL 証明書フィンス | ガープリント(続き) | | | | |
| | | SSL 証明書フィンス | ガープリント(続き) | | | | |
| | | SSL 証明書フィンス | ガープリント(続き) | | | | |
| | | SSLポリ | 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 キー証明書編 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 St | SL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 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 |
| | 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) |
| 分 | SSL フロー フラ グ(続き) | 文字列ブロック タイプ(0) |
| SSL サーバ名 | 文字列ブロック タイプ(0)(続き) | 文字列ブロック長 |
| SS | 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 の長さ | SSL チケット ID |
| | | SSL チケット ID(続き) |

| バイト | 0 | 1 | 2 3 | | | | | | | | | | |
|--------------------------|------------------------|---------------------|------------|----------------|-------------|------|------------|-----|-------|-----|--------|-----|---|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 8 | 1 5 | 1 1 1 8 | 1 2 9 0 | 2 | 2 2 3 | 2 4 | 2 2 6 | 2 7 | 3 2 9 | 3 0 | 3 |
| | SSL チケット ID (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 | J | シーリビ | ゛ジョ | ン | (続 | き) | | | | | |
| | ネ | ットワーク分析ポリ | J | シーリビ | ゛ジョ | ン | (続: | き) | | | | | |
| | ネットワーク分析; ン(約 | | | エン | ドポ | イ | ント | プロ | ロフ | ァイ | ル | D | |
| | エンドポイントプき | | | セ | ビキ コ | ı IJ | ティ | ・ク | ゛ルー | ·プI | D | | |
| | セキュリティグ | ループ ID(続き) | | | 口 | ケ | ーシ | 3 | ≻ IPv | v6 | | | |
| | | 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) | | | Н | ТТ | Pν | スァ | ポンス | ス | | | |
| = IJ ery) | HTTP レスホ | ジス(続き) | | 文字列ブロック タイプ(0) | | | | | | | | | |
| DNS ⅓ ± ⅓ (DNS Query) | 文字列ブロック | タイプ(0)(続き) | | 文字列ブロック長 | | | | | | | | | |
| NO (D) | 文字列ブロッ | ,ク長(続き) | | DNS クエリ | | | | | | | | | |
| | DNS レコードター Typ | | |] | DNS | レ | スポ | シ | スタ | イフ | o O | | |
| | | DN | S | TTL | | | | | | | | | |
| | | シンクオ | ; <u> </u> | ール UUII | D | | | | | | | | |
| | | シンクホー | レ | UUID(約 | 売き) | | | | | | | | |
| | | シンクホー | レ | UUID(約 | 売き) | | | | | | | | |
| | | シンクホー | ル | UUID(約 | 売き) | | | | | | | | |
| | | セキュリティイン | テ | リジェン | /ス! | Jフ | ド 1 | | | | | | |
| | | セキュリティイン | テ | リジェン | /ス! | Jフ | <ト2 | 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

| | データ タ | | | | |
|------------------------------|-----------|---|--|--|--|
| フィールド | 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。 | | | |
| レスポンダ IP ア ドレス | uint8[16] | IPアドレスオクテットの、開始ホストに応答したホストのIP アドレス。 | | | |
| オリジナル クラ イアント IP アド レス | uint8[16] | 要求の送信元であるプロキシの背後にあるホストの IP アドレス(オクテットの IP アドレス)。 | | | |
| ポリシー リビ ジョン | uint8[16] | トリガーされた相関イベントに関連付けられているルールのリビジョン番号(該当する場合)。 | | | |
| ルール ID | uint32 | イベントをトリガーしたルールの内部 ID(該当する場合)。 | | | |
| トンネル ルー ル ID | uint32 | イベントにトリガーをかけたトンネル ルールの内部 ID(該当する場合)。 | | | |
| ルール アク ション | uint16 | そのルールに対してユーザインターフェイスで選択された アクション(allow、block など)。 | | | |
| ルールの理由 | uint32 | イベントをトリガーしたルールの理由。 | | | |
| イニシエータ ポート | uint16 | 開始ホストにより使用されるポート。 | | | |
| レスポンダ ポート | uint16 | 応答ホストにより使用されるポート。 | | | |
| TCP フラグ | uint16 | 接続イベントのすべての TCP フラグを示します。 | | | |
| プロトコル | uint8 | IANA 指定のプロトコル番号。 | | | |
| NetFlow ソース | uint8[16] | 接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。 | | | |

表 B-39 接続統計データ ブロック 6.1+ のフィールド(続き)

| | データ タ | | | | |
|----------------------------|-----------|--|--|--|--|
| フィールド | 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。 | | | |
| レスポンダ送信 パケット数 | uint64 | 応答ホストが送信したパケット数。 | | | |
| イニシエータ送 信バイト数 | uint64 | 開始ホストからの送信バイト数。 | | | |
| レスポンダ送信 バイト数 | uint64 | 応答ホストから送信バイト数。 | | | |
| イニシエータ パ ケット ドロップ | uint64 | レート制限により、セッション イニシエータからドロップしたパケット数。 | | | |
| レスポンダ パ ケット ドロップ | uint64 | レート制限により、セッション レスポンダからドロップした パケット数。 | | | |
| ドロップしたイ ニシエータ バイ ト数 | uint64 | レート制限により、セッション イニシエータからドロップしたバイト数。 | | | |
| レスポンダ バイ ト ドロップ | uint64 | レート制限により、セッション レスポンダからドロップした バイト数。 | | | |
| QOS 適用イン ターフェイス | uint8[16] | レート制限された接続で、レート制限が適用されるインターフェイスの名前。 | | | |
| QOS バール 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)

| | データ タ | | | | |
|-------------------------------|--------|---|--|--|--|
| フィールド | 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 o 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 o 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 o 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。 | | | |

表 B-39 接続統計データ ブロック 6.1+ のフィールド(続き)

| | データ タ | | | |
|---|-----------|--|--|--|
| フィールド | 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。 | | |
| レスポンダの国 | uint 16 | 応答ホストの国のコード。 | | |
| クライアントの オリジナル国 (Original Client Country) | uint 16 | 要求を開始したプロキシの背後にあるホストの国コード。 | | |
| IOC 番号 | uint16 | このイベントに関連付けられている侵害 ID 番号。 | | |
| 送信元自律シス テム | uint32 | 送信元の自律システム番号、起点またはピア。 | | |
| 宛先自律シス テム | uint32 | 宛先の自律システム番号、起点またはピア。 | | |
| SNMP 入力 | uint16 | 入力インターフェイスの SNMP インデックス。 | | |
| SNMP 出力 | uint16 | 出力インターフェイスの SNMP インデックス | | |
| 送信元 TOS | uint8 | 着信インターフェイス用のタイプ オブ サービス バイト設定。 | | |
| 宛先 TOS | uint8 | 発信インターフェイス用のタイプ オブ サービス バイト設定。 | | |
| 送信元マスク | uint8 | 送信元アドレス プレフィックス マスク。 | | |
| 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 | 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 | | |
| ンテキスト | | 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 o 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 o 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)

| | データ タ | | | | |
|----------------------|-----------|--|--|--|--|
| フィールド | 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 o 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。 o(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)

| | データ タ | |
|--------------------|--------|--|
| フィールド | イプ | 説明 |
| 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。 |
| | | • o:「不明」 |
| | | • 1:「復号しない」 |
| | | • 2:「ブロックする」 |
| | | • 3:「リセットでブロック」 |
| | | • 4:「復号(既知のキー)」 |
| | | • 5:「復号(置換キー)」 |
| | | • 6:「復号(Resign)」 |
| 予期された SSL アクション | uint16 | SSL ルールに基づいて接続に対して実行する必要があるアクション。有効な値は次のとおりです。 |
| | | • 0:「不明」 |
| | | • 1:「復号しない」 |
| | | • 2:「ブロックする」 |
| | | • 3:「リセットでブロック」 |
| | | • 4:「復号(既知のキー)」 |
| | | • 5:「復号(置換キー)」 |
| | | • 6:「復号(Resign)」 |

表 B-39 接続統計データ ブロック 6.1+ のフィールド(続き)

| | データ タ | |
|-------------------|--------|--|
| フィールド | イプ | 説明 |
| SSL フロー ス テータス | uint16 | SSL フローのステータス。アクションが実行された理由、またはエラーメッセージが出された理由を示す値です。有効な値は次のとおりです。 |
| | | • 0:「不明」 |
| | | 1:「一致しない」 |
| | | • 2:「成功」 |
| | | • 3:「キャッシュされていないセッション」 |
| | | • 4:「不明の暗号化スイート」 |
| | | • 5:「サポートされていない暗号スイート」 |
| | | • 6:「サポートされていない SSL バージョン」 |
| | | 7:「使用される SSL 圧縮」 |
| | | • 8:「パッシブ モードで復号不可のセッション」 |
| | | • 9:「ハンドシェイク エラー」 |
| | | • 10:「復号エラー」 |
| | | • 11:「保留中のサーバ名カテゴリ 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 | 詳細な SSL エラー コード。これらの値はサポート目的で必要とされる場合があります。 |

表 B-39 接続統計データ ブロック 6.1+ のフィールド(続き)

| | データ タ | |
|------------------|--------|--|
| フィールド | イプ | 説明 |
| SSL フローメッ セージ | uint32 | SSL ハンドシェイク時にクライアントとサーバとの間で交換されたメッセージ。詳細については、 |
| | | http://tools.ietf.org/html/rfc5246 を参照してください。 |
| | | • 0x00000001:NSE_MTHELLO_REQUEST |
| | | • 0x00000002:NSE_MTCLIENT_ALERT |
| | | • 0x00000004:NSE_MTSERVER_ALERT |
| | | • 0x00000008:NSE_MTCLIENT_HELLO |
| | | • 0x00000010:NSE_MTSERVER_HELLO |
| | | • 0x00000020:NSE_MTSERVER_CERTIFICATE |
| | | • 0x00000040:NSE_MTSERVER_KEY_EXCHANGE |
| | | • 0x00000080:NSE_MTCERTIFICATE_REQUEST |
| | | • 0x00000100:NSE_MTSERVER_HELLO_DONE |
| | | • 0x00000200:NSE_MTCLIENT_CERTIFICATE |
| | | • 0x00000400:NSE_MTCLIENT_KEY_EXCHANGE |
| | | • 0x00000800:NSE_MTCERTIFICATE_VERIFY |
| | | • 0x00001000: NSE_MTCLIENT_CHANGE_CIPHER_SPEC |
| | | • 0x00002000:NSE_MTCLIENT_FINISHED |
| | | • 0x00004000: NSE_MTSERVER_CHANGE_CIPHER_SPEC |
| | | • 0x00008000:NSE_MTSERVER_FINISHED |
| | | • 0x00010000:NSE_MTNEW_SESSION_TICKET |
| | | • 0x00020000:NSE_MTHANDSHAKE_OTHER |
| | | • 0x00040000:NSE_MTAPP_DATA_FROM_CLIENT |
| | | • 0x00080000:NSE_MTAPP_DATA_FROM_SERVER |
| SSL フロー フ ラグ | uint64 | 暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。 |
| | | 0x00000001 (NSE_FLOWVALID):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_FLOWINITIALIZED): 内部構造が処理可能です |
| | | • 0x00000004 (NSE_FLOWINTERCEPT): 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 o 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)

| - | データ タ | | | | |
|-------------------------------------|-----------|--|--|--|--|
| フィールド | 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 o 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 | 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。 | | | |

| | データ タ | |
|----------------------------|--------|---|
| フィールド | 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。 |

表 B-39 接続統計データ ブロック 6.1+ のフィールド(続き)

レガシー ファイル イベントのデータ構造

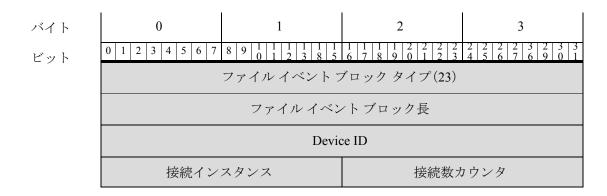
続くいくつかのトピックでは、他のレガシーファイルイベントデータの構造について説明します。

- 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 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 | | | | | |
| | 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 | | | | |
| | | 送信元 IP アー | | | | |
| | | 宛先 IP 7 | | | | |
| | | 宛先 IP アド | | | | |
| | | 宛先 IP アド | | | | |
| | | 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 ハッミ | /ユ(続さ) | | | |
| | SHA ハッミ | ンュ(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 | | | ロック長 | | |
| | 文字列ブロッ | 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 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 | | | |
| | 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 | 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 | | | |
| | <i>P</i> : | 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) | | | | |
| | <i>T</i> : | 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 | 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。 |
| | | • 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 | 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。 |
| | | • 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。 |
| | | • 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 | 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 |
| ションID | | いる ID 番号。 |
| (Application ID) | | |
| ユーザ ID(User | 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 |
| ID) | | 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。 |
| | | • 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 ビット | 0 0 1 2 3 4 5 6 7 | ファイルイベントラ | | | | |
|------------|-------------------|------------------------|----------------------------|--|--|--|
| | | ファイル イベン | /トブロック長 | | | |
| | | Devid | ee 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 | | | | |
| | | 送信元 IP ア | | | | |
| | | 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 ハッミ | /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 | | | |

| バイト | 0 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 | 2 | 3 |
|-------|---|---|-----------------|----------------|
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 | | | |
| | | ファイルサ | イズ(続き) | |
| | 方向(Direction) | 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) | 文写 | 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 | | | 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) | | | () |
| | | | ポリシー UUID(続き | |
| | | | ポリシー UUID(続き | |
| | アクセス コント ロール ポリシー UUID(続き) | | | |
| | 宛先の国(続き) | We | b アプリケーション | ID |
| | Web アプリケー ション ID(続き) | クライン | アントアプリケーシ | ョン ID |
| | クライアント <i>ア</i> 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 | 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。 • 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 | 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。 |
| | | • 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 |

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 | 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。 | |
| | | • 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。 | |
| • | | • 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

バイト

ビット

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。

| 0 | 0 1 | | 3 | | |
|----------------------|--|---|------------------------------------|--|--|
| 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | ファイル イベントコ | ブロック タイプ(38) | | | |
| | ファイル イベン | /トブロック長 | | | |
| | Devid | ce ID | | | |
| 接続イン | スタンス | 接続数划 | コウンタ | | |
| | 接続タイム | ン スタンプ | | | |
| ファイル | ノベント タイムス | タンプ(File Event Tin | nestamp) | | |
| 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 | 傾向 SPERO 解析結果 ファイル ストレー ファイル分析 ジステータス データス | | | | |
| アーカイブ ファ イル ステータス | 脅威スコア | 操作 | SHA ハッシュ | | |

| バイト | 0 | 1 | 2 | 3 | | |
|-------|---|---------------------|---|---------------------------------|--|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | 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 ハッミ | | | | |
| | | SHA ハッミ | | | | |
| | | SHA ハッミ | /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 | 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) | | | | | |
| URI | ユーザ ID(続き) | 文写 | 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 | Z | | | |
| | 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 | /— UUID | | |

バイト

ビット

| 0 | 1 | 2 | 3 | | |
|----------------------------------|---------------------------|--------------------------------------|----------------------------------|--|--|
| 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 3 3 4 5 6 7 6 9 0 1 | | |
| <i>P</i> : | アクセス コントロール ポリシー UUID(続き) | | | | |
| <i>P</i> : | クセス コントロール | ポリシー UUID(続き | ٤) | | |
| 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) | We | ID | | | |
| Web アプリケー ション ID(続き) | クライン | 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 | 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。 |
| | | • 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 | uint8 | ファイルの保存ステータス。値は以下のとおりです。 |
| ステータス | | • 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-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 | 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。 |
| | | 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 |
| アーカイブ ファイル ステータス | uint8 | この値は常に o 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 $(0 \sim 100)$ 。 |
| 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。 |
| | | • 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。 • 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。 • 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

バイト

ビット

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。

| 0 | 1 | 2 | 3 | | | | |
|----------------------|-----------------------|---|----------------------------------|--|--|--|--|
| 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 3 3 4 5 6 7 6 9 0 1 | | | | |
| | ファイルイベントフ | 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 | 接続数な | リウンタ | | | | |
| | 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 Tim | nestamp) | | | | |
| | 送信元 IP アドレス | | | | | | |
| | 送信元 IP ア | ドレス(続き) | | | | | |
| | 送信元 IP ア | ドレス(続き) | | | | | |
| | 送信元 IP ア | ドレス(続き) | | | | | |
| | 宛先 IP 🤇 | アドレス | | | | | |
| | 宛先 IP アド | レス(続き) | | | | | |
| | 宛先 IP アドレス(続き) | | | | | | |
| | 宛先 IP アドレス (続き) | | | | | | |
| 傾向 | SPERO 解析結果 | ファイル ストレー ジ ステータス | ファイル分析ス テータス | | | | |
| アーカイブ ファ イル ステータス | 脅威スコア | 操作 | SHA ハッシュ | | | | |

| バイト | 0 | 1 | 2 | 3 | | | |
|-------|-----------------------|-----------------------|---|------------------------------------|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | |
| | | 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 | | | | | |
| | | SHA ハッシ | | | | | |
| | | SHA ハッシ | /ュ(続き) | | | | |
| | S | SHA ハッシュ(続き) | | ファイル タイプ ID | | | |
| ファイル名 | 7; | ァイル タイプ ID(続き | <u>*</u>) | 文字列ブロック タイプ(0) | | | |
| | 文字列 | 文字列ブロック タイプ(0)(続き) | | | | | |
| | 文 | 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 (Applica | ation 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 | 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 | 7 1 | | | | |
| | 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 | /— UUID | | | |

バイ

ビッ

| ٢ | | | | | 0 | | | | ĺ | 1 | | | | | | | | | | 2 | | | | | | | | | 3 | | | | | |
|---|----------------------------------|---|----|----|-------------------|-----|------------|--------|-----|--------------------|-------------------------|-----|--------|-----|----------|-----|------------|--------|----|--------|----|-------------------|-----|-----|-----|-----|-----|--------|--------|--|------------|--------|---|---|
| ٢ | 0 | 1 | 2 | 3 | 4 | | 5 (| 6 | , | 8 | 9 | 1 0 | 1 1 | 1 2 | 1 1 2 3 | . [| 1 | 1 5 | 16 | 1 7 | 18 | 19 | 2 0 | 2 | 2 2 | 2 3 | 2 4 | 2 5 | 2 6 | | 2 3 7 6 | 2 9 | 3 | 3 |
| | | | | | | | | ア | . / | クセ | セス コントロール ポリシー UUID(続き | | | | | | | ٤) | | | | | | | | | | | | | | | | |
| | | | | | | | | ア | . / | クセ | セス コントロール ポリシー UUID(続き) | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | ア | • / | クセ | 27 | ス | コ、 | ~ | ا | コー | — ј | ル | ポ | リ | シ | <u> </u> | UL | JID | (糸 | 売き | ٤) | | | | | | | |
| | 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) | | | | | | | | | | | | |
| | 3 | 宛 | 走 | の[| 国(; | 続 | き |) | | Web アプリケーション ID | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | プリ D(| | - | | | クライアント アプリケーション ID | | | | | | | | | | | | | | | | | | | | | | | | |
| | | プ | IJ | ケー | アンーシ | / ; | э ` | | | セキュリティ コンテキ | | | | | キン | ス] | ۲ | | | | | | | | | | | | | | | | | |
| | | | | | 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 | ユ | IJ | テ | イ | コ | ン | ⁄テ | キ | ・ス | ト | (綅 | きき |) | | | | | | | | | |
| | | | | | テ.ト(; | | | ン) | | | | | | | | | | | | | | | | | | | | | | | | | | |

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 | 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。 |
| タイプ 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 | 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。 |
| | | • 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 | uint8 | ファイルの保存ステータス。値は以下のとおりです。 |
| トレージ ス テータス | | • 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 |
|---------------------------------|-----------------|---|
| フィールド ファイル分析 ステータス | データタイプ uint8 | 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。 ・ 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ので、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 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 $(0 \sim 100)$ 。 |
| 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。 |
| | | • 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。 |
| | | • 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。 |
| | | • 1:ICMP |
| | | • 4:IP |
| | | • 6:TCP |
| | | • 17:UDP |
| | | これは現時点では TCP のみです。 |

| フィールド | データ タイプ | 説明 |
|----------|-----------|------------------------------------|
| アクセスコン | 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 |
| トロール ポリ | | 有識別子。 |
| シーUUID | | |
| 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 | uint32 | Web アプリケーションの内部 ID 番号(該当する場合)。 |
| ケーション ID | | |
| クライアント | 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 ID | | |
| セキュリティ | 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 |
| コンテキスト | | 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。 |

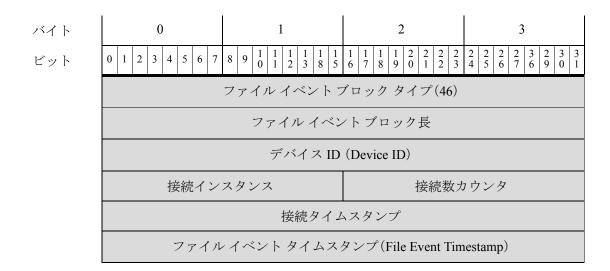
表 B-43 ファイル イベント データ ブロックのフィールド(続き)

ファイルイベント 5.4.x

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

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

次の図は、ファイルイベントデータブロックの構造を示しています。



| バイト | 0 | 1 | 2 | 3 | | | | |
|-------|----------------------|-----------------------|---|---------------------------------|--|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | | |
| | | 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 | | | | | | |
| | | 宛先 IP アド | | | | | | |
| | | 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 ハッミ | ンュ(続き) | | | | | |
| | | SHA ハッミ | ンュ(続き) | | | | | |
| | | SHA ハッミ | ンュ(続き) | | | | | |
| | | SHA ハッミ | ンュ(続き) | | | | | |
| | | SHA ハッミ | ンュ(続き) | | | | | |
| | | SHA ハッミ | ンュ(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 | ž) | 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) | アプリク | ニーション ID(Applica | ation ID) | | | | |
| | | | | | | | | |

| バイト | 0 | 1 | 2 | 3 |
|-------|----------------------------------|-----------------------|---|---|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | アプリケーショ ン ID(続き) | | ユーザ ID (User ID) | |
| URI | ユーザ ID(続き) | 文气 | 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 | 7 | |
| | 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 | /— UUID |
| | r | · クセス コントロール | ポリシー UUID(続き | <u>*</u>) |
| | P | クセス コントロール | ポリシー UUID(続き | <u>*</u>) |
| | P | クセス コントロール | ポリシー UUID(続き | <u>*</u>) |
| | アクセス コント ロール ポリシー UUID(続き) | 送信力 | この国 | 宛先の国 (Country) |
| | 宛先の国(続き) | We | b アプリケーション | ID |
| | Web アプリケー ション ID(続き) | クライン | 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 コンテキン | 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 <i>コン</i> テキスト(続き) | SSL 記 | E明書フィンガープリ | リント |
| | | SSL 証明書フィンス | ブープリント(続き) | |

| バイト | 0 | 1 | 2 | 3 |
|--------------|------------------------------|-----------------------|---|------------------------------------|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | | SSL 証明書フィンス | ブープリント(続き) | |
| | | SSL 証明書フィンス | ブープリント(続き) | |
| | | SSL 証明書フィンス | ブープリント(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) | 文气 | 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 | |
| | | アーカィ | 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 | 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。 |
| | | • 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 | uint8 | ファイルの保存ステータス。値は以下のとおりです。 |
| ステータス | | • 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-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 | 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。 | | | |
| | | 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 | | | |

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 | 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。 |
| | | • o(N/A):ファイルがアーカイブとして検査されていません。 |
| | | • 1:保留中。アーカイブは調査中です |
| | | • 2:取得済み。調査が問題なく正常に実行されま した |
| | | • 3:失敗。システムのリソース不足のため調査に失 敗しました。 |
| | | • 4:深度の超過。調査は正常に実行されましたが、 アーカイブがネストされた調査の深度を超過し ました |
| | | • 5:暗号化。部分的に正常に実行されましたが、 アーカイブが暗号化されているか、暗号化された アーカイブが含まれています |
| | | • 6:調査できませんでした。部分的に正常に実行されましたが、ファイル形式が不正であるか破損しています |
| 脅威スコア | uint8 | 動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値 $(0\sim100)$ 。 |
| 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。 |
| | | • 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] | 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。 |

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。 |
| | | • 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。 • 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 | SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 0:「不明」 |
| | | 1:「復号しない」 2:「ブロックする」 3:「リセットでブロック」 4:「復号(既知のキー)」 |
| | | 5:「復号(置換キー)」6:「復号(Resign)」 |

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 | SSL フローのステータス。アクションが実行された 理由、またはエラーメッセージが出された理由を示 す値です。有効な値は次のとおりです。 |
| | | • 0:「不明」 |
| | | 1:「一致しない」 |
| | | • 2:「成功」 |
| | | • 3:「キャッシュされていないセッション」 |
| | | • 4:「不明の暗号化スイート」 |
| | | • 5:「サポートされていない暗号スイート」 |
| | | • 6:「サポートされていない SSL バージョン」 |
| | | • 7:「使用される SSL 圧縮」 |
| | | • 8:「パッシブ モードで復号不可のセッション」 |
| | | • 9:「ハンドシェイク エラー」 |
| | | • 10:「復号エラー」 |
| | | • 11:「保留中のサーバ名カテゴリ 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 | 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。 |

| 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 o 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。 |

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 で要求されていれば、要求することができます。

次の図は、ファイルイベントハッシュデータブロックの構造を示しています。

| バイト | 0 | 1 | 2 | 3 | | | | |
|-----|---------------------------------|---|-----------------|------------------------------------|--|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | | | |
| | ファイル イベント SHA ハッシュ ブロック タイプ(26) | | | | | | | |
| | ファイル イベント SHA ハッシュ ブロック長 | | | | | | | |
| | SHA ハッシュ | | | | | | | |
| | SHA ハッシュ(続き) | | | | | | | |
| | SHA ハッシュ(続き) | | | | | | | |
| | SHA ハッシュ(続き) | | | | | | | |
| | SHA ハッシュ(続き) | | | | | | | |
| | | SHA ハッシ | /ュ(続き) | | | | | |
| | | SHA ハッシ | /ュ(続き) | | | | | |
| | | SHA ハッシ | /ュ(続き) | | | | | |

| ファイル名 | 文字列ブロック タイプ(0) |
|-------|----------------|
| | 文字列ブロック長 |
| | ファイル名または解析結果 |

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 o 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。 |

レガシー相関イベントのデータ構造

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

- 相関イベント 5.0 ~ 5.0.2(B-270 ページ)
- 相関イベント 5.1 ~ 5.3.x (B-279 ページ)

相関イベント 5.0 ~ 5.0.2

相関イベント(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、相関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、それに相関データ 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 相関イベントは、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 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | ヘッダーバー | ージョン(1) | メッセージ | タイプ(4) | | |
| | | メッセ | ージ長 | | | |
| | Netma | ap 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 合の | ント用、ビット 23 が み) | 設定されている場 | | |
| | 将来の使用に備えて | て予約済み(イベント み | 、でビット 23 が設定) | されている場合の | | |
| | | 相関ブロック | タイプ(116) | | | |
| | 相関ブロック長 | | | | | |
| | Device ID | | | | | |
| | (相関)イベント秒 | | | | | |
| | イベント ID(Event ID) | | | | | |
| | ポリシー ID | | | | | |
| | ルール ID | | | | | |
| | [プライオリティ(Priority)] | | | | | |
| | 文字列ブロック タイプ(0) | | | | イベント 説明 | |
| | 文字列ブロック長 | | | | | |
| | 説明 イベント タイプ (Event Type) | | | | | |
| | | イベント | Device ID | | | |

| バイト | 0 | 1 | 2 | 3 | |
|----------|--|---------------------|---|------------------------------------|----------------------------------|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 3 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| <u>'</u> | 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 | ントマイクロ秒 | | |
| | | イベントID | (Event ID) | | |
| | | イベントで定義 | きされたマスク | | |
| | 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 | |
| | | ソージ | Z IP | | |
| | 送信元ホスト タイプ | 送信元 V | LAN 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 |) | V T CCID |
| | 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 |
| | 宛先 OS フィンガープリント UUID(続き) | | | | 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 き | プリント UUID(続) | 宛先重 | 重要度 | |

| バイト | 0 | 1 | 2 | 3 |
|-----|---------------------|-----------------------|---|------------------------------------|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | | 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 | ノターフェイス UUII |) (続き) | 出力インター フェイス UUID |
| | | 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 |)(続き) | 入力ゾーン UUID | |
| | | 入力ゾー | ン UUID | |
| | | | | |
| | | UUID(続き) | | |
| | 入 | :) | 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 | カゾーン UUID(続き | :) | |

表 B-46 相関イベント データ 5.0 ~ 5.0.2 のフィールド

| | データ タ | |
|-------------------------|--------|---|
| フィールド | イプ | 説明 |
| 相関ブロック タイプ | uint32 | 相関イベント 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。 |
| 相関ブロック長 | uint32 | 相関データ ブロック長(相関ブロック タイプと長さの 8 バイト、およびそれに続く相関データを含む)。 |
| Device ID | uint32 | 相関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。 |
| (相関)イベン ト秒 | uint32 | 相関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 | 相関イベント ID 番号。 |
| ポリシーID | uint32 | 違反された相関ポリシーの 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相関ルールの 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 | 相関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 o 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 | 相関イベントについての説明。 |
| イベントタイプ(Event Type) | uint8 | 相関イベントが、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。 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 | 相関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 o になります。 |

表 B-46 相関イベント 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 | 相関ポリシー 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 口秒 | 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 相関イベント データ 5.0 ~ 5.0.2 のフィールド(続き)

| | データ タ | |
|-----------------|----------|--|
| フィールド | イプ | 説明 |
| イベント影響 フラグ | bits[8] | 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。 |
| | | • 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。 |
| | | 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。 |
| | | • (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 |
| 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 相関イベント データ 5.0 ~ 5.0.2 のフィールド(続き)

| | データ タ | |
|---------------------|-----------|--|
| フィールド | イプ | 説明 |
| 送信元ホスト タイプ | uint8 | 送信元ホストのタイプ: |
| 717 | | • 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 | 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。 |
| ⊦ UUID | | 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: |
| | | • 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 | uint8 | 宛先ホストのタイプ: |
| イプ | | • 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 | 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。 |
| UUID | | 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: |
| | | • 0:なし |
| | | • 1:低 |
| | | • 2:中 |
| | | ● 3:高 |

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

| | データ タ | |
|---------------------|-----------|--|
| フィールド | 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。 |
| | | • o: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] | 相関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] | 相関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] | 相関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] | 相関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 |
| | |

相関イベント 5.1 ~ 5.3.x

相関イベント(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、相関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 相関データ 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 $5.1 \sim 5.3.x$ の相関イベントは、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。

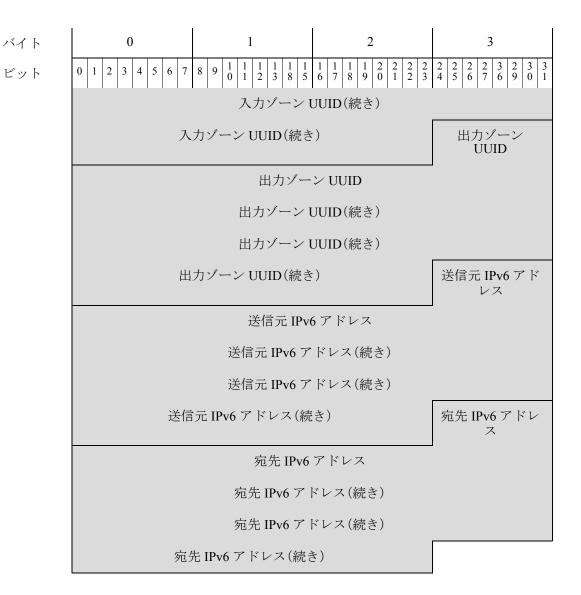
| バイト ビット | | | 2 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | | |
|------------|--|---------|---|--------|--|
| | ヘッダーバー | ージョン(1) | メッセージ | タイプ(4) | |
| | | メッセー | ージ長 | | |
| | Netmap ID レコードタイプ (112) | | | | |
| | レコード長 | | | | |
| | eStreamer サーバ タイムスタンプ(イベント用、ビット 23 が設定されている場合のみ) | | | | |
| | 将来の使用に備えて予約済み(イベントでビット 23 が設定されている場合の み) | | | | |
| | 相関ブロック タイプ(128) | | | | |
| | 相関ブロック長 | | | | |
| | デバイス ID (Device ID) | | | | |

バイト

ビット

| 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 8 5 | 2 1 1 1 1 1 2 2 2 2 2 2 6 7 8 9 0 1 2 3 | 3 2 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
|---------------------------|-------------------------------------|---|-------------------------------------|---------------------------------|--|
| | (相関)イ | ベント秒 | | | |
| | イベントID | (Event ID) | | | |
| | ポリシ | ~— ID | | | |
| | ルー) | r ID | | | |
| | [プライオリテ | イ (Priority)] | | | |
| | 文字列ブロッ | クタイプ(0) | | イベント 説明 | |
| | 文字列ブ | ロック長 | | b)r -⊘ 1 | |
| | 説明 | | イベントタイプ (Event Type) | | |
| | イベント デバイス ID | | | | |
| | シグネラ | チャID | | | |
| | シグネチャジ | ェネレータ ID | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| イベントで定義されたマスク | | | | | |
| イベント影響フ ラグ | イベント影響フ IP プロトコル ネットワーク プロトコル ラグ | | | | |
| | ソー | ス IP | | | |
| 送信元ホスト タイプ | 送信元 V | LAN 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) | | | | OOID | |
| 送 | | | | | |
| 送 | | | | | |
| 送信元 OS フ | 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 | | | | | |

| バイト | 0 1 | 2 | 3 | |
|-----|---|---|---|-------------------|
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| | 送信元ユーザ ID 送信元 (続き) | 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 |
| | 宛先 OS フィンガーフ | プリント UUID(続き) | | ントUUID |
| | 宛先 OS フィンガーフ | °リント UUID(続き) | | |
| | 宛先 OS フィンガーフ | 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 | 重要度 | |
| | 着信ユーザ」 | D(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 | | |
| | 入力ゾーンで | JUID(続き) | | |



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

表 B-48 相関イベント データ 5.1 ~ 5.3.x のフィールド

| | データ タ | |
|---------------|--------|--|
| フィールド | イプ | 説明 |
| 相関ブロック タイプ | uint32 | 相関イベント 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。 |
| 相関ブロッ ク長 | uint32 | 相関データブロック長(相関ブロックタイプと長さの8バイト、およびそれに続く相関データを含む)。 |

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

| | データ タ | | | |
|-------------------------|--------|---|--|--|
| フィールド | イプ | 説明 | | |
| デバイス ID (Device ID) | uint32 | 相関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。 | | |
| (相関)イベン ト秒 | uint32 | 相関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 | 相関イベント ID 番号。 | | |
| ポリシー ID | uint32 | 違反された相関ポリシーの 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相関ルールの 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、 $0 \sim 5$ の整数値です。 | | |
| 文字列ブロック タイプ | uint32 | 相関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 | 相関イベントについての説明。 | | |
| イベントタイ プ(Event Type) | uint8 | 相関イベントが、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。 | | |
| | | • 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 | 相関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 | 相関ポリシー 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 相関イベント データ 5.1 ~ 5.3.x のフィールド(続き)

| _ | データ タ | | |
|--------------------------|----------|---|--|
| フィールド | 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] | 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。 | |
| | | • 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) | |
| | | 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。 | |
| | | • (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 | |

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

| | データ タ | | | | |
|-------------------------------|-----------|--|--|--|--|
| フィールド | イプ | 説明 | | | |
| IPプロトコル | uint8 | イベントに関連付けられている IP プロトコルの ID(該当する場合)。 | | | |
| ネットワーク プロトコル | uint16 | イベントに関連付けられているネットワーク プロトコル(該当 する場合)。 | | | |
| 送信元 IP アド レス | uint8[4] | このフィールドは予約済みですが、設定されておりません。送信元 IPv4 アドレスは、送信元 IPv6 アドレス フィールドに保存されます。詳細については、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 | uint8 | 送信元ホストのタイプ: | | | |
| タイプ | | • 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: | | | |
| | | • 0:なし | | | |
| | | • 1:低 | | | |
| | | • 2:中 | | | |
| | | • 3:高 | | | |
| 送信元ユーザ ID | | | | | |
| 送信元ポート | uint16 | イベントの送信元ポート。 | | | |
| 送信元サーバ ID | uint32 | 送信元ホスト上で実行するサーバの ID 番号。 | | | |
| 宛先 IP アド レス | uint8[4] | このフィールドは予約済みですが、設定されておりません。宛先 IPv4 アドレスは、宛先 IPv6 アドレス フィールドに保存されます。 詳細については、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 | uint8 | 宛先ホストのタイプ: | | | |
| イプ | | • 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 相関イベント データ 5.1 ~ 5.3.x のフィールド(続き)

| _ | データ タ | | | |
|---------------------|-----------|--|--|--|
| フィールド | イプ | 説明 | | |
| 宛先 OS フィン ガープリント | 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。 | | |
| UUID | | 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: | | |
| | | • 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。 | | |
| | | • 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] | 相関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] | 相関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] | 相関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] | 相関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。



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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | 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 タイン | プ(31) | | |
| | 汎用リストブ ロック タイプ (続き) | Ì | L用リスト ブロック♪ | <u></u> | | |

| バイト | 0 | 1 | 2 | 3 | |
|--------------------------------|--|-----------------------------------|---|------------------------------------|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 2 3 3 3 4 5 6 7 6 9 0 1 | |
| 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 ントデータ | <i>、たフィンガー</i> プリ | |
| | 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 | 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)* | | | | |
| 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 | 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)* | | | | |
| 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 | 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)* | | | | |
| ンガープリ ンカープリ 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 | | | |
|------------------------|----------------------------------|---------------------------------|---|--|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 8 | 1 1 1 1 2 2 2 6 7 8 9 0 1 2 | 2 2 2 2 2 3 2 3 3 3 4 5 6 7 6 9 0 1 | | | |
| VDB ネイ ティブフィ | 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)* | | | |
| ンガープリ ンカープリ ント 2 | オペレーラ | ティング システム フ | フィンガープリント | ブロック長 | | | |
| | オペレーテ | 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 | コック タイプ(31) | | | | |
| | | 汎用リスト | ブロック長 | | | | |
| ユーザ(User) フィンガー | 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)* | | | |
| プリント | オペレーラ | ティング システム こ | フィンガープリント | ブロック長 | | | |
| | オペレーティ | 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) | 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)* | | | |
| フィンガープリント | オペレーラ | ティング システム フ | 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 | オペレーティン | グ システム フィン | ガープリントブロッ | ック タイプ (130)* | | | |
| プリント | オペレーラ | ティング システム こ | 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 | オペレーティン | グ システム フィン | ガープリントブロッ | ック タイプ (130)* | | | |
| フィンガープリント | オペレーラ | ティング システム フ | フィンガープリント | ブロック長 | | | |
| | オペレーテ | イング システム競合 | iのフィンガープリ: | ノトデータ | | | |

| バイト | 0 | 1 | 2 3 | | | |
|----------------------|-----------------------------|-------------------|---|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 8 | 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 2 3 3 5 6 7 8 9 0 1 2 3 4 5 6 7 6 9 0 1 | | | |
| (TCP)フル サーバ データ | リストブロック タイプ(11) | | | | | |
| リーハブータ | | リストフ | 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 | | リストブロ | ック タイプ(11) | | | |
| データ | | 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 | | リストブロ | ック タイプ(11) | | | |
| (Transport) プロトコル | | リスト | ブロック長 | | | |
| データ | (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 | リスト ブロック タイプ(11) | | | | | |
| データ | リストブロック長 | | | | | |
| | ホ | スト MAC アドレン | ス データ ブロック (95)* | | | |
| | | Las | st 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 | 汎用リストブロッ | ック タイプ(続き) | 汎用リストブロック長 | | | |
| データ | 汎用リストブロ | コック長(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 | | | |
| | | NetBIO | S名文字列 | | | |

| バイト | 0 | 1 | 2 | 3 | | |
|-------------------|---|-----------------------|---|---|--|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| 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 ブ | 文字列 | | | |
| (VDB)ホス ト | | 汎用リストブロ | ック タイプ(31) | | | |
| Vulns | | 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) | 汎用リスト ブロック タイプ(31) | | | | | |
| Host Vulns | 汎用リストブロック長 | | | | | |
| | (サード/ | ペーティ/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 | 汎用リスト ブロック タイプ(31) | | | | | |
| Host Vulns | 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) | リスト ブロック タイプ(11) | | | | | |
| 値データ | 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 $5.0 \sim 5.0.2$ 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

| | データ タ | |
|---------------------------|----------|---|
| フィールド | 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。 |

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

| | データ タ | |
|---|---------------------|---|
| フィールド | ブー <i>タ タ</i> 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 $5.0 \sim 5.0.2$ のフィールド(続き)

| | データ タ | |
|---|------------------|--|
| フィールド | 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 $5.0 \sim 5.0.2$ のフィールド(続き)

| | データ タ | |
|---|------------------|--|
| フィールド | アータ 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 | 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 $5.0 \sim 5.0.2$ のフィールド(続き)

| | データ タ | |
|---------------------------------|------------------|---|
| フィールド | 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 $5.0 \sim 5.0.2$ のフィールド(続き)

| | データ タ | |
|--|------------------|--|
| フィールド | 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。 |
| | | • 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 o 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 o 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 $5.0 \sim 5.0.2$ 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ャナから送信され、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 <i>ブ</i> 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ャナから送信されたホスト脆弱性データブロック。これらのデータブロックのホスト脆弱性 ID は、サードパーティのスキャナ ID であり、シスコによって検出された ID ではない点にご注意ください。このデータブロックの説明の詳細については、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 | | | | |
|------------------------|---|--|--------------------------|------------|--|--|--|--|
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 3 6 | | | | | | | |
| | 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) | Ţ | L用リスト ブロック l | E V | | | | |
| OS から取得 した フィンガー | 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 タイプ (130)* | プリントブロック | | | | |
| プリント | 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 ント データ | たフィンガープリ | | | | |
| | 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 | オペレーティン | 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)* | | | | | | |
| フィンガー プリント | オペレーラ | ティング システム フ | ィンガープリントフ | 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 | オペレーティン | グ システム フィンカ | ブ ープリント ブロッ: | クタイプ(130)* | | | | |
| フィンガープリント | オペレー | ティング システム フ | ィンガープリントフ | ブロック長 | | | | |
| | オペレーティン | グ システム クライア | 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 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 3 3 4 5 6 7 6 9 0 1 | |
| | 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 | 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)* | | | | |
| ンガープリ ンガープリ ント1 | オペレーテ | イング システム フ | ィンガープリントフ | ブロック長 | |
| | オペレーティ | ィング システム VD | B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 | オペレーティング | ゲシステム フィンカ | ガープリントブロッ | クタイプ(130)* | |
| ンガープリント 2 | オペレーテ | イング システム フ | ィンガープリントフ | 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 | 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 | | | | |
| プリント | | | | | |
| | 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) | 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)* | | | | |
| 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 ブロック長 | | | | |
| | オペレーティン | ノグ システム スキャ | ァンフィンガープリ | 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 | | |

| バイト | 0 | 1 | 2 | 3 |
|----------------------|--|-------------------|---|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 8 | 1 1 1 1 1 2 2 2 5 6 7 8 9 0 1 2 | 2 2 2 2 2 3 2 3 3 3 4 5 6 7 6 9 0 1 |
| Application フィンガー | 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)* | | | |
| 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 | ブロック長 |
| | オペレーティング | システム アプリク | ーション フィンガー | 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 | オペレーティン | グ システム フィン | /ガープリント ブロ _ッ | ック タイプ (130)* |
| 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 | ブロック長 |
| | オペレーテ | ィング システム競 | 合のフィンガープリン | ントデータ |
| (TCP)フル サーバデータ | | リストブロッ | ック タイプ (11) | |
| | | リストラ | ブロック長 | |
| | | (TCP)全サーバテ | 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)全サーバラ | ータ ブロック (104) | * |
| ネットワークプロトコル | | リストブロ | ック タイプ(11) | |
| データ | | 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 | 7 (4)* |
| トランスポート | | リストブロ | ック タイプ(11) | |
| (Transport) プロトコル | | リスト | ブロック長 | |
| データ | (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 | | リストブロ | ック タイプ(11) | |
| データ | | リスト | ブロック長 | |
| | 办 | スト MAC アドレ | ス データ ブロック(9 | 95)* |
| | | La | st Seen | |

| バイト | 0 | 1 | 2 | 3 |
|----------------------|---|-----------------------|--------------------------------------|------------------------------------|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | | ホストタイプ | | |
| | ビジネス」 | この重要度 | VLAN ID (Adn | nin. 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 | 汎用リストブロッ | ック タイプ(続き) | 汎用リスト | ブロック長 |
| データ | 汎用リストブロ | コック長(続き) | フル ホスト クライ 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 | 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 | 汎用リストブロック タイプ(31) | | | |
| Vulns | 汎用リスト ブロック長 | | | |
| | (| VDB) ホスト脆弱性ラ | データ ブロック(85): | * |
| (サードパー ティ/VDB) | 汎用リスト ブロック タイプ(31) | | | |
| Host Vulns | | 汎用リスト | ブロック長 | |
| | (サード/ | ペーティ/VDB) ホスト | 脆弱性データブロッ | ック (85)* |
| サードパー ティ スキャン | 汎用リストブロック タイプ(31) | | | |
| Host Vulns | 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)* | | | 性データ ブロック |
| 属性 (Attribute) | リストブロック タイプ(11) | | | |
| 値データ | 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

| | データ タ | |
|---|------------------|--|
| フィールド | 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)

| - | データ タ | |
|---|------------------|--|
| フィールド | 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)

| - | データ タ | |
|--|------------------|--|
| フィールド | 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(アプリントンヨンフィンガープリンガープリント)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)

| | データ タ | |
|--|------------------|---|
| フィールド | 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)

| | データ タ | |
|--|------------------|--|
| フィールド | 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。 |
| | | • 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 | uint16 | ホストがメンバーである VLAN を示す VLAN ID 番号。 |
| (Admin. VLAN ID) | | |
| 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)

| | データ タ | |
|---|------------------|---|
| フィールド | 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 o 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ャナから送信され、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ャナから送信されたホスト脆弱性データブロック。これらのデータブロックのホスト脆弱性 ID は、サードパーティのスキャナ ID であり、シスコによって検出された ID ではない点にご注意ください。このデータブロックの説明の詳細については、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 | アイルレコー | ド5.1.1 のフィ | ィールド(続き) |
|--------|------------|--------|------------|----------|
|--------|------------|--------|------------|----------|

| | データ タ | |
|--------------|------------------|---|
| フィールド | 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。 |
| | | o: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。



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 1 1 2 3 8 5 6 7 8 9 0 1 3 2 3 8 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 2 3 4 5 6 7 6 9 0 1 | | |
| | 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 | |
|------------------------|---|---|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 | |
| 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 | 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)* | |
| プリント | 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 | 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 | | |
| 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 | 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)* | | |
| 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 |
|-----------------------|---|
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 |
| VDB ネイ ティブフィ | 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)* |
| ンガープリ ンカープリ 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 | 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)* |
| 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 | 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)* |
| 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) | 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)* |
| 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 | 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)* |
| 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 |
|--------------------|---|
| ビット | 0 1 2 3 4 5 6 7 8 9 1 1 2 3 8 5 6 7 8 9 0 1 3 2 3 8 5 6 7 8 9 0 1 2 3 8 5 6 7 8 9 0 1 2 3 4 5 6 7 6 9 0 1 |
| | 汎用リスト ブロック長 |
| 競合 フィンガー | 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)* |
| 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 | 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)* |
| 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 | 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)* |
| 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 | 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)* |
| 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 | 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)* |
| 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 |

| バイト | 0 | 1 | 2 | 3 | |
|----------------------|--------------------------------------|-----------------------|---|---|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | |
| | 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 | オペレーティン | グ システム フィンカ | ガープリントブロッ | クタイプ(130)* | |
| フィンガープリント | オペレーラ | ティング システム フ | ィンガープリントフ | ブロック長 | |
| | オペレーティング | システム ユーザ エー | 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 | カタイプ(11) | | |
| | | リストブロ | コック長 | | |
| | | (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 | | リストブロッ | ク タイプ(11) | | |
| (Transport) プロトコル | | リストブ | `ロック長 | | |
| データ | (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 | リストブロック タイプ(11) | | | | |
| データ | | 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」 | この重要度 | VLAN ID (Adr | min. VLAN ID) | |
| | VLAN タイプ VLAN 優先順位 汎用リスト ブロック タイプ (3 | | | | |

| バイト | 0 | 1 | 2 | 3 |
|------------------------|-------------------|------------------------|---|------------------------------------|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| ホストクラ イアント | 汎用リストブロッ | ック タイプ(続き) | 汎用リスト | ブロック長 |
| データ | 汎用リストブロ | コック長(続き) | 全ホスト クライフ ション データ | アントアプリケー ブロック(112)* |
| NetBIOS 名 [名前(Name) | | 文字列ブロッ | ク タイプ(0) | |
| [%] Fig (Name) | | 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 | | 汎用リストブロ | ック タイプ(31) | |
| Vulns | 汎用リストブロック長 | | | |
| | (| VDB) ホスト脆弱性ラ | データ ブロック(85) | * |
| (サードパー ティ/VDB) | | 汎用リストブロ | ック タイプ(31) | |
| Host Vulns | | 汎用リスト | ブロック長 | |
| | (サード/ | ペーティ/VDB) ホスト | 脆弱性データブロッ | ック (85)* |
| サードパーティスキャン | 汎用リストブロック タイプ(31) | | | |
| Host Vulns | 汎用リストブロック長 | | | |
| | (サードパーティン | スキャン)元の Vuln II (85 | | 性データ ブロック |
| 属性 (Attribute) | | リストブロッ | ク タイプ(11) | |
| 値データ | リストブロック長 | | | |
| | | 属性値データ | 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

| | データ タ | |
|---|------------------|---|
| フィールド | 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 フィンガー フトフィンガープリ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)

| | データ タ | |
|--|------------------|--|
| フィールド | 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(アプリントンヨンフィンガー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)

| | データ タ | |
|--|------------------|--|
| フィールド | 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)

| - | データ タ | |
|---|------------------|--|
| フィールド | 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 <i>データ ブ</i> 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)

| - | データ タ | |
|--------------------------------|------------------|---|
| フィールド | 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)

| - | データ タ | |
|---------------------------|------------|--|
| フィールド | 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。 |
| | | • 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 | uint16 | ビジネスに対するホストの重要度を示します。 |
| 要度 | | |
| VLAN ID | uint16 | ホストがメンバーである VLAN を示す VLAN ID 番号。 |
| (Admin. VLAN ID) | | |
| ID) 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。 |
| N用リストブ | 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 |
| が用サベトラ ロック タイプ | umtsz | ブライナンドナブリケーションナ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 | 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 |
| ロック長 | | 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 | 変数 | 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 |
| アントアプリ | (variable) | 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 |
| ケーション デー タ ブロック* | | 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。 |
| <u>グラロック*</u> 文字列ブロック | 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 |
| タイプ | unit32 | 値は常 C_0 です。 |
| 文字列ブロッ | 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 |
| ク長 | | 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 | 水スト NetBIOS 名の文字列。 |
| 文字列ブロック | 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 |
| メナ州ノロック タイプ | umt32 | 常にのです。 |
| 文字列ブロッ | 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 |
| 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 <i>ブ</i> 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 |
| н <i>)</i> | | す。 |
| 汎用リストブ | 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 |
| ロック長 | | 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)

| - | データ タ | |
|---|------------------|--|
| フィールド | イプ | 説明 |
| (VDB)ホスト脆 弱性データブ | 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 |
| ロック* | (variable) | 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ャナから送信され、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ャナから送信されたホスト脆弱性データブロック。これらのデータブロックのホスト脆弱性 ID は、サードパーティのスキャナ ID であり、シスコ によって検出された ID ではない点にご注意ください。このデータブロックの説明の詳細については、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 | 0 1 | | 3 | | |
|----------------------|---------------------------------|-------------------------------------|---|------------------------------------|-----|--|
| ビット | 0 1 2 3 4 5 6 7 | 8 9 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 | | |
| | 本 | ホスト プロファイル ブロック タイプ(132) | | | | |
| | | | | | | |
| | | [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 | ック タイプ(続き) | 汎用リスト | ブロック長 | | |
| | 汎用リストブロ | 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 | | 汎用リストブロ | ック タイプ(31) | | | |
| リント | | 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 | 汎用リスト ブロック タイプ(31) | | | | | |
| フィンガー プリント | | 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 | 汎用リスト ブロック タイプ(31) | | | | | |
| 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* | | | | | |
| モバイル Device | 汎用リスト ブロック タイプ(31) | | | | | |
| フィンガープリント | 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 | | |
| 7 4 7 7 . | | リストブ | ロック長 | | サーバ | |
| | | TCP サーバ デ | ータブロック | | | |

| ビット 0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 | バイト | 0 | 1 | 2 | 3 | |
|---|-----------------|-----------------------|------------|-----------|---------|----------------|
| プロック* | ビット | 0 1 2 3 4 5 6 7 | | | | |
| リストプロック長 | | リストブロック タイプ(11) | | | | UDPのリス |
| ネットワーク プロトコルブロック* 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 ボート (Transport) プロトコル ブロック* リスト ブロック タイプ(II) トランスポート リスト ブロック長 ブロック MAC アドレス プロック* リスト ブロック タイプ(II) MAC のリストプロック タイプ(II) メスト ガロック タイプ(II) MAC のリストア・レスデータ ブロック カーション プロック* リスト ブロック タイプ(II) MAC のリストア・レス データ ブロック タイプ(II) ルスト グロック タイプ(II) MAC のリストア・ドレス データ ブロック タイプ(II) MAC のリストア・ドレス データ ブロック タイプ(II) ルスト グロック タイプ (II) MAC のリストア・ドレス データ ブロック タイプ(II) MAC のリストア・ドレス データ ブロック タイプ (II) ルート グロック タイプ (II) MAC のリストア・ドレス データ ブロック タイプ (II) MAC のリストア・ドレス トア・リストア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ | 7497* | | リストフ | 「ロック長 | | サーバ |
| プロトコルプ ロック* 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 ボート (Transport) プロトコル プロック* MAC アドレ ス ブロック* MAC アドレ ス ブロック* MAC アドレス ボート リスト ブロック タイプ(II) リスト ブロック タイプ(II) メスト ブロック タイプ(II) メスト ブロック タイプ(II) メスト ブロック タイプ (II) MAC のリスト アドレス ボスト 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 VLAN ID(統き) VLAN ID(統き) VLAN 優先順位 汎用リスト ブロック タイプ(31) パカーション データ 汎用リスト ブロック タイプ(31)(続き) ハ用リスト ブロック タイアントア ブリケーション データ ブロック タイプ(31)(続き) ハ用リスト ブロック タイプ(30) NetBIOS [名前(Name) | | | UDP サーバラ | ータ ブロック | | |
| ロック* 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 トランスポートリストブロック タイプ(II) ボート (Transport) プロトコル ブロック* リスト ブロック長 MAC アドレス フロック タイプ(II) MAC のリストアドレス データ ブロック メニュー カー・アドレス データ ブロック 展終検出時のホスト ホスト MAC アドレス データ ブロック タイプ (II) 水スト MAC アドレス データ ブロック 展終検出時のホスト ホスト タイプ サーション データ VLAN ID (続き) メリスト ブロック タイプ (31) (続き) ル用リスト ブロック タイプ (31) (続き) ル用リスト ブロック 展 (続き) カライアントア ブリケーション データ ブロック NetBIOS [名前(Name) 文字列ブロック タイプ(0) | | リストブロック タイプ(11) | | | | |
| トランスポート (Transport) ブロトコル ブロック* リストブロック長 トランスポート ブロトコルデータ ブロック MAC アドレスアロック* リストブロックタイプ(11) MAC のリストプロックを メニスト MAC アドレスデータ ブロック サストブロック長 アドレス カライアントアプリケーションデータ VLAN ID(総き) VLAN 優先順位 汎用リストプロックタイプ(31)(総き) ル用リスト プロック長(総き) ルカイブ (31)(総き) ルカリストプロック長のアントアプリケーションデータブロック NetBIOS [名前(Name) 文字列プロックタイプ(0) | | | リストフ | 「ロック長 | | |
| ポート (Transport) プロトコル プロック* MAC アドレ ス プロック* MAC アドレ ス プロック* MAC アドレス プロック* Dyah 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 ひ造 VLAN ID(統き) アプリケーション データ 汎用リスト ブロック タイプ(31)(続き) 汎用リスト ブロック タイプ(31)(続き) 汎用リスト ブロック タイプ(31)(続き) ハラライアント アプリケーション データ NetBIOS [名前(Name) | | ý | ネットワーク プロト | コルデータブロック | 7 | |
| (Transport) | | | リストブロッ | クタイプ(11) | | |
| MAC アドレス | (Transport) | | リストフ | 「ロック長 | | |
| フェーク フェーク | ブロック* | <u>۲</u> | ランスポート プロ | トコルデータブロッ | ク | |
| ブロック* リストブロック長 アドレス プロック* 最終検出時のホスト カライアントアプリケーションデータ VLAN ID(続き) VLAN Øイプ VLAN 優先順位 以用リストブロック タイプ (31) グ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 タイプ(31) (続き) 汎用リストブロック長 NetBIOS [名前 (Name) 文字列プロック タイプ(0) | | リストブロック タイプ(11) | | | MAC のリス | |
| 最終検出時のホスト | | リストブロック長 | | | アドレス | |
| 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 汎用リストブロックタイプ (31) (続き) 汎用リストブロックタイプ (31) (続き) 汎用リストブロックタイプ 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 VLAN 優先順位 八田リストブロックタイプ (31) ハ田リストブロック長 八田リストブロック長 八田リストブロック グライアントアプリケーションデータブロック アプリケーションデータブロック マ字列ブロックタイプ (0) 文字列ブロックタイプ (0) 文字列ブロックタイプ (0) イン・アータブロック アン・アータブロック アン・アース・アース・アース・アース・アース・アース・アース・アース・アース・アース | | ホスト MAC アドレス データ ブロック | | | | |
| 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 優先順位 汎用リストブロックタイプ (31) カライアントのリストアプリケーション アリケーション アリケーションデータ ブロック長 汎用リスト ブロック長(続き) カライアントア プリケーションデータ ブロック アプリケーションデータ ブロック マ字列ブロック タイプ(0) NetBIOS [名前 (Name)] 文字列ブロック タイプ(0) マタイプ(0) | | 最終検出時のホスト | | | | |
| 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) グレスト アプリケーション トのリストアプリケーション ロック長 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(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) | | ホストタイプ | | | | |
| トアプリケーション データ 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) | | Mobile | 改造 | VLAN の有無 | | |
| 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 文字列ブロック タイプ(0) | トアプリ ケーション | VLAN ID(続き) | VLAN タイプ | VLAN 優先順位 | ロック タイプ | トのリスト アプリケー |
| プリケーション データ ブロック 文字列ブロック タイプ(0) | | | | | | |
| [名前(Name) | | プリケーション | | | | |
| | | 文字列ブロック タイプ(0) | | | | |
| 文字列ブロック長 | [AT Hil (Maine) | | 文字列ブロック長 | | | |
| NetBIOS 文字列データ | | | 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

| | データ タ | |
|---|------------------|--|
| フィールド | 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。 |
| | | 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)

| | データ タ | |
|--|------------------|---|
| フィールド | 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 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)

| | データ タ | |
|--|------------------|--|
| フィールド | 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)

| | データ タ | |
|--------------------------------|--------|---|
| フィールド | 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。 • 0:ホスト • 1:ルータ • 2:ブリッジ • 3:NAT デバイス • 4:LB(ロード バランサ) |
| Mobile | uint8 | 検出したホストがモバイル デバイスであるかどうかを示す true/false フラグ。 |
| 改造 | uint8 | ホストが(ジェイルブレイクされていない)モバイル デバイスであるかどうかを示す true/false フラグ。 |
| VLAN の有無 | uint8 | VLAN が存在するかどうかを示します。0:はい1:いいえ |
| VLAN ID (Admin. VLAN ID) | uint16 | ホストがメンバーである VLAN を示す VLAN ID 番号。 |
| VLAN タイプ | uint8 | VLAN タグ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。 |

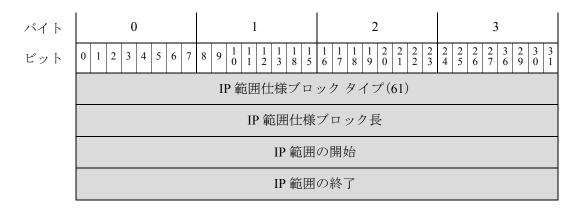
| フィールド | データ タ イプ | 説明 |
|---------------------------------|-------------|--|
| 汎用リストブ ロック長 | uint32 | 汎用リスト データ ブロックのバイト数(リスト ヘッダーと、カプセル化されたすべてのクライアント アプリケーション データ ブロックを含む)。 |
| クライアント ア プリケーション データ ブロック | uint32 | クライアント アプリケーションを記述するクライアント アプリケーション データ ブロック。このデータ ブロックの説明の詳細については、フル クライアント アプリケーション 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。 |

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)

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。



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 | · B-53 | IP 範囲仕様データ ブロックのフィール | バ |
|---------------------------|--------|----------------------|---|
|---------------------------|--------|----------------------|---|

| | データ タ | |
|------------------------|--------|--|
| フィールド | 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 1 1 1 1 1 1 1 1 5 | 1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3 | 2 2 2 2 3 2 3 3 4 5 6 7 6 9 0 1 |
| | 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 | ールの理由のデータ | ブロックの長さ |
| 説明 | 理由(Re | eason) | 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 | 月 |

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 o 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。 |