Cisco Secure Network Analytics

情報要素 7.4

Secure Network Analytics v7.4 の情報要素

次に、Flow Collector によって処理される NetFlow/IPFIX 情報要素のリストを示します。

情報要素の詳細については、https://www.iana.org/assignments/ipfix/ipfix.xhtml を参照してください。

Element ID	名前	説明
1	octetDeltaCount	観測ポイントでのこのフローの着信パケットにおける、前のレポート（存在する場合）以降のオクテットの数。オクテットの数には、IP ヘッダーと IP ペイロードが含まれます。
2	packetDeltaCount	観測ポイントでのこのフローの前のレポート（存在する場合）以降の着信パケットの数。
4	protocolIdentifier	IP パケットヘッダーのプロトコル番号の値。プロトコル番号は、IP パケットペイロードタイプを識別します。プロトコル番号は、IANA プロトコル番号レジストリで定義されています。 インターネット プロトコル バージョン 4（IPv4）では、プロトコル番号は［プロトコル（Protocol）］フィールドで伝送されます。インターネット プロトコル バージョン 6（IPv6）では、プロトコル番号はパケットの最後の拡張ヘッダーの［次ヘッダー（Next Header）］フィールドで伝送されます。
5	ipClassOfService	IPv4 パケットの場合、これは IPv4 パケットヘッダーの［TOS］フィールドの値です。 IPv6 パケットの場合、これは IPv6 パケットヘッダーの［トラフィッククラス（Traffic Class）］フィールドの値です。
6	tcpControlBits	このフローのパケットに対して観

Element ID	名前	説明
		測された TCP 制御ビット。この情報はビットフィールドとしてエンコードされます。TCP 制御ビットごとに、このセット内にビットがあります。このフローの観測されたいずれかのパケットで、対応する TCP 制御ビットが 1 に設定されている場合、このビットは 1 に設定されます。ビットは 0 にクリアされます（それ以外の場合）。
7	sourceTransportPort	トランスポートヘッダー内の送信元ポート ID。トランスポートプロトコル（UDP、TCP、および SCTP）の場合、これは、それぞれのヘッダーで指定されている送信元ポート番号です。このフィールドは、16 ビットの送信元ポート ID を持つ今後のトランスポートプロトコルにも使用できます。
8	sourceIPv4Address	IP パケットヘッダー内の IPv4 送信元アドレス。
10	ingressInterface	このフローのパケットが受信されている IP インターフェイスのインデックス。
11	destinationTransportPort	トランスポートヘッダー内の宛先ポート ID。トランスポートプロトコル（UDP、TCP、および SCTP）の場合、これは、それぞれのヘッダーで指定されている宛先ポート番号です。このフィールドは、16 ビットの宛先ポート ID を持つ今後のトランスポートプロトコルにも使用できます。
12	destinationIPv4Address	IP パケットヘッダー内の IPv4 宛先アドレス。
14	egressInterface	このフローのパケットが送信されている IP インターフェイスのインデックス。

Element ID	名前	説明
15	ipNextHopIPv4Address	次の IPv4 ホップの IPv4 アドレス。
16	bgpSourceAsNumber	送信元 IP アドレスの自律システム（AS）番号。このフローの AS パス情報が、（順序どおりの AS シーケンスではなく）順序指定されていない AS セットとしてのみ使用可能な場合、この情報要素の値は 0 になります。
17	bgpDestinationAsNumber	宛先 IP アドレスの自律システム（AS）番号。このフローの AS パス情報が、（順序どおりの AS シーケンスではなく）順序指定されていない AS セットとしてのみ使用可能な場合、この情報要素の値は 0 になります。
18	bgpNextHopIPv4Address	次の（隣接する）BGP ホップの IPv4 アドレス。
21	flowEndSysUpTime	フローの最終パケットの相対タイムスタンプ。これは、IPFIX デバイス（sysUpTime）の最後の（再）初期化以降のミリ秒数を示します。sysUpTime は、systemInitTimeMilliseconds から計算できます。
22	flowStartSysUpTime	フローの先頭パケットの相対タイムスタンプ。これは、IPFIX デバイス（sysUpTime）の最後の（再）初期化以降のミリ秒数を示します。sysUpTime は、systemInitTimeMilliseconds から計算できます。
27	sourceIPv6Address	IP パケットヘッダー内の IPv6 送信元アドレス。
28	destinationIPv6Address	IP パケットヘッダー内の IPv6 宛先アドレス。
32	icmpTypeCodeIPv4	IPv4 ICMP メッセージのタイプとコード。両方の値の組み合わせ

Element ID	名前	説明
		は、(ICMP タイプ * 256) + ICMP コードとして報告されます。
34	samplingInterval	サンプリングされた NetFlow を使用する場合、パケットがサンプリングされるレート(たとえば、値 100 は、100 パケットごとに 1 つサンプリングされることを示します)。
48	samplerId	samplerName に関連付けられている固有識別子。
50	samplerRandomInterval	サンプリングするパケット間隔(ランダムサンプリングの場合)。SamplerMode 0x02(ランダムサンプリング)値との接続に使用されます。
52	minimumTTL	このフロー内のパケットに対して観測された最小 TTL 値。
53	maximumTTL	このフロー内のパケットに対して観測された最大 TTL 値。
72	sourceMacAddress	IEEE 802 送信元 MAC アドレスフィールド。
57	postDestinationMacAddress	この情報要素の定義は、情報要素「destinationMacAddress」の定義と同じですが、パケットが観測ポイントに渡された後に middlebox 機能によって変更された可能性のある値を報告する点が異なります。
58	vlanId	入力インターフェイスに関連付けられている仮想 LAN ID。

61	flowDirection	観測ポイントで観測されたフローの方向。次の 2 つの値だけが定義されています。
		`0x00: ingress flow`
		`0x01: egress flow`

Element ID	名前	説明
70	mplsTopLabelStackSection	上位 MPLS ラベルスタックエントリ（つまり、プッシュされた最後のラベル）の [ラベル（Label）]、[Exp]、および [S] フィールド。
71	mplsLabelStackSection2	mplsTopLabelStackSection によって報告されるラベルスタックエントリの直前にプッシュされたラベルスタックエントリの [ラベル（Label）]、[Exp]、および [S] フィールド。
72	mplsLabelStackSection3	mplsLabelStackSection2 によって報告されるラベルスタックエントリの直前にプッシュされたラベルスタックエントリの [ラベル（Label）]、[Exp]、および [S] フィールド。
73	mplsLabelStackSection4	mplsLabelStackSection3 によって報告されるラベルスタックエントリの直前にプッシュされたラベルスタックエントリの [ラベル（Label）]、[Exp]、および [S] フィールド。
74	mplsLabelStackSection5	mplsLabelStackSection4 によって報告されるラベルスタックエントリの直前にプッシュされたラベルスタックエントリの [ラベル（Label）]、[Exp]、および [S] フィールド。
75	mplsLabelStackSection6	mplsLabelStackSection5 によって報告されるラベルスタックエントリの直前にプッシュされたラベルスタックエントリの [ラベル（Label）]、[Exp]、および [S] フィールド。
76	mplsLabelStackSection7	mplsLabelStackSection6 によって報告されるラベルスタックエントリの直前にプッシュされたラベルスタックエントリの [ラベル（Label）]、[Exp]、および [S] フィールド。
77	mplsLabelStackSection8	mplsLabelStackSection7 によって報告されるラベルスタックエントリの直前にプッシュされたラベルス

Element ID	名前	説明
		タックエントリの [ラベル（Label）]、[Exp]、および [S] フィールド。
78	mplsLabelStackSection9	mplsLabelStackSection8 によって報告されるラベルスタックエントリの直前にプッシュされたラベルスタックエントリの [ラベル（Label）]、[Exp]、および [S] フィールド。
79	mplsLabelStackSection10	mplsLabelStackSection9 によって報告されるラベルスタックエントリの直前にプッシュされたラベルスタックエントリの [ラベル（Label）]、[Exp]、および [S] フィールド。
85	octetTotalCount	この観測ポイントの計測プロセス（再）初期化以降、観測ポイントにおけるこのフローに対する着信パケットのオクテットの総数。オクテットの数には、IP ヘッダーと IP ペイロードが含まれます。
95	applicationId	IPFIX におけるアプリケーション情報の Cisco Systems エクスポートごとのアプリケーション ID を指定します。
139	icmpTypeCodeIPv6	IPv6 ICMP メッセージのタイプとコード。両方の値の組み合わせは、(ICMP タイプ * 256) + ICMP コードとして報告されます。
148	flowID	観測されたドメイン内で一意であるフローの識別子。この情報要素は、IP アドレスやポート番号などのフローキーが報告されない場合や、別のレコードで報告されている場合に、異なるフローを区別するために使用できます。
150	flowStartSeconds	フローの先頭パケットの絶対タイムスタンプ。
151	flowEndSeconds	フローの最終パケットの絶対タイムスタンプ。

Element ID	名前	説明
152	flowStartMilliseconds	フローの先頭パケットの絶対タイムスタンプ。
153	flowEndMilliseconds	フローの最終パケットの絶対タイムスタンプ。
154	flowStartMicroseconds	フローの先頭パケットの絶対タイムスタンプ。
155	flowEndMicroseconds	フローの最終パケットの絶対タイムスタンプ。
156	flowStartNanoseconds	フローの先頭パケットの絶対タイムスタンプ。
157	flowEndNanoseconds	フローの最終パケットの絶対タイムスタンプ。
158	flowStartDeltaMicroseconds	これは、単一の IPFIX メッセージの範囲内でのみ有効な相対タイムスタンプです。これには、IPFIX メッセージヘッダーで指定されたエクスポート時間に対して相対的な、このフローの最初に観測されたパケットの負の時間オフセットが含まれています。
159	flowEndDeltaMicroseconds	これは、単一の IPFIX メッセージの範囲内でのみ有効な相対タイムスタンプです。これには、IPFIX メッセージヘッダーで指定されたエクスポート時間に対して相対的な、このフローの最後に観測されたパケットの負の時間オフセットが含まれています。
160	systemInitTimeMilliseconds	IPFIX デバイスの最後の（再）初期化の絶対タイムスタンプ。
176	icmpTypeIPv4	IPv4 ICMP メッセージのタイプ。
177	icmpCodeIPv4	IPv4 ICMP メッセージのコード。
178	icmpTypeIPv6	IPv6 ICMP メッセージのタイプ。

Element ID	名前	説明
179	icmpCodeIPv6	IPv6 ICMP メッセージのコード。
180	udpSourcePort	UDP ヘッダー内の送信元ポート ID。
181	udpDestinationPort	UDP ヘッダー内の宛先ポート ID。
182	tcpSourcePort	TCP ヘッダー内の送信元ポート ID。
183	tcpDestinationPort	TCP ヘッダー内の宛先ポート ID。
192	ipTTL	IPv4 の場合、情報要素の値は、IPv4 パケットヘッダーの [存続可能時間（TTL）（Time-to-Live (TTL)）] フィールドの値と一致します。IPv6 の場合、情報要素の値は、IPv6 パケットヘッダーの [ホップリミット（Hop Limit）] フィールドの値と一致します。
195	ipDiffServCodePoint	差別化サービス（Differentiated Services）フィールドでエンコードされる Differentiated Services Code Point（DSCP; DiffServ コードポイント）の値。差別化サービス（Differentiated Services）フィールドは、IPv4 TOS フィールドまたは IPv6 トラフィック クラス フィールドの最上位 6 ビットになります。 この要素では、差別化サービス（Differentiated Services）フィールドの 6 ビットのみがエンコードされます。したがって、値の範囲は 0 ～ 63 です。
218	tcpSynTotalCount	TCP「Synchronize sequence numbers」（SYN）フラグが設定されている、このフローのパケットの総数。
219	tcpFinTotalCount	TCP「No more data from sender」（FIN）フラグが設定されている、このフローのパケットの総数。

Element ID	名前	説明
220	tcpRstTotalCount	TCP「Reset the connection」（RST）フラグが設定されている、このフローのパケットの総数。
222	tcpAckTotalCount	TCP「Acknowledgment field significant」（ACK）フラグが設定されている、このフローのパケットの総数。
223	tcpUrgTotalCount	TCP「Urgent Pointer field significant」（URG）フラグが設定されている、このフローのパケットの総数。
225	postNATSourceIPv4Address	この情報要素の定義は、情報要素「sourceIPv4Address」の定義と同じですが、パケットが観測ポイントに渡された後に NAT middlebox 機能によって変更された値を報告する点が異なります。
226	postNATDestinationIPv4Address	この情報要素の定義は、情報要素「destinationIPv4Address」の定義と同じですが、パケットが観測ポイントに渡された後に NAT middlebox 機能によって変更された値を報告する点が異なります。
227	postNAPTSourceTransportPort	この情報要素の定義は、情報要素「sourceTransportPort」の定義と同じですが、パケットが観測ポイントに渡された後にネットワークアドレスポート変換（NAPT）middlebox 機能によって変更された値を報告する点が異なります。
228	postNAPTDestinationTransportPort	この情報要素の定義は、情報要素「destinationTransportPort」の定義と同じですが、パケットが観測ポイントに渡された後にネットワークアドレスポート変換（NAPT）middlebox 機能によって変更された値を報告する点が異なります。

Element ID	名前	説明
230	natEvent	この情報要素は、NAT イベントを識別します。この IE は、NAT イベントのタイプを識別します。NAT イベントの例としては、NAT 変換の作成、NAT 変換の削除、しきい値到達、しきい値超過などがあります。この情報要素の値は、NAT イベントタイプレジストリに表示されます。
231	initiatorOctets	前のレポート以降の、イニシエータからのフローに含まれているレイヤ 4 ペイロードの合計バイト数。イニシエータは、セッションの作成をトリガーしたデバイスであり、セッションの期間中も同じです。
232	responderOctets	前のレポート以降の、レスポンダからのフローに含まれているレイヤ 4 ペイロードの合計バイト数。レスポンダは、イニシエータに応答するデバイスであり、セッションの期間中も同じです。
233	firewallEvent	ファイアウォールイベントを示します。使用できる値は、次のとおりです。 0:無視(無効) 1:フロー作成 2:フロー削除 3:フロー拒否 4:フローアラート 5:フロー更新
239	biflowDirection	Biflow の送信元と宛先を割り当てるために使用される方向割り当て方式の説明。この情報要素は、フローデータレコード内に存在するか、または IPFIX オプションを使用して、エクスポートプロセスまたは観測ドメインからエクスポートされたすべてのフローに適用される場

Element ID	名前	説明
		合があります。この情報要素がフローレコード内に存在しない場合、または範囲を指定して Biflow に関連付けられている場合、方向割り当て方式の設定はアウトオブバンドで行われることが前提となります。IPFIX オプションを使用して、観測ドメイン内で、またはエクスポートプロセスからすべてのフローにこの情報要素を適用する場合は、オプションを確実に送信する必要があります。信頼性の高い転送を使用できない場合（つまり、UDP を使用している場合）、この情報要素は各フローレコードに表示されます。
281	postNATSourceIPv6Address	この情報要素の定義は、情報要素「sourceIPv6Address」の定義と同じですが、パケットが観測ポイントに渡された後に NAT64 middlebox 機能によって変更された値を報告する点が異なります。
282	postNATDestinationIPv6Address	この情報要素の定義は、情報要素「destinationIPv6Address」の定義と同じですが、パケットが観測ポイントに渡された後に NAT64 middlebox 機能によって変更された値を報告する点が異なります。
313	ipHeaderPacketSection	この情報要素は、サンプリングされたパケットの IP ヘッダーから一連の n 個のオクテットを伝送し、その IP ヘッダーへの sectionOffset オクテットを開始します。
314	ipPayloadPacketSection	この情報要素は、サンプリングされたパケットの IP ペイロードから一連の n 個のオクテットを伝送し、その IP ペイロードへの sectionOffset オクテットを開始します。
323	observationTimeMilliseconds	この情報要素は、観測の絶対時

Element ID	名前	説明
		間をミリ秒単位で指定します。
346	privateEnterpriseNumber	IANA によって割り当てられたプライベート エンタープライズ番号。情報要素タイプレコードのコンテキスト内では、この要素を informationElementId 要素とともに使用して、特定の情報要素に対するプロパティの範囲を設定できます。IANA によって割り当てられた情報要素に関するタイプ情報をエクスポートするには、privateEnterpriseNumber を 0 に設定するか、または privateEnterpriseNumber をタイプレコードにエクスポートしないようにします。企業固有の情報要素に関するタイプ情報をエクスポートするには、privateEnterpriseNumber でエンタープライズ番号をエクスポートし、エンタープライズビットがクリアされた情報要素番号を informationElementId でエクスポートします。関連する informationElementId 情報要素のエンタープライズビットは、収集プロセスでは無視される必要があります。
371	userName	フローに関連付けられているユーザー名。
1232	TrustSecSourceIdentifierIPFIX PEN(9)	送信元ホストの TrustSec ID を含む Cisco PEN（PrivateEnterpriseNumber）フィールド。
1233	TrustSecDestinationIdentifierIPFIX PEN(9)	宛先ホストの TrustSec ID を含む Cisco PEN フィールド。
9292	AVCResponsesCountDeltaIPFIX	IPFIX の AVC（Application Visibility and Control）応答数差分フィールド。RTT と SRT の決定に使用されます。

Element ID	名前	説明
9303	AVCSummaryResponseTimeIPFIX	IPFIX の AVC サマリー応答時間フィールド。SRT フィールド。このフィールドを AVCResponsesCountDeltaIPFIX フィールドで割ると、RTT が生成されます。
9306	AVCSummaryServerResponseTime	IPFIX の AVC サマリーサーバー応答時間フィールド。このフィールドを AVCResponsesCountDeltaIPFIX フィールドで割ると、SRT が生成されます。
12235	AVCSubApplicationValueIPFIX PEN(9)	フローで使用されるアプリケーションを識別する Cisco NBAR2 フィールド。Flow Collector がプルして Secure Network Analytics フローにアタッチするホストおよび URL の情報を含めることもできます。
12172	NF_F_ETTA_INITIAL_DATA_PACKET_IPFIX	フローで送信された初期データパケットのペイロードを含む ETA IDP フィールド。接続が暗号化される前に URL およびその他の情報を取得するために使用されます。
12173	NF_F_ETTA_SEQUENCE_OF_PACKET_LENGTHS_AND_TIMES_IPFIX	暗号化されたセッションのパケット長と時間を含む ETA SPLT フィールド。
12174	NF_F_ETTA_SEQUENCE_OF_APPLICATION_LENGTHS_AND_TIMES_IPFIX	暗号化されたセッションのアプリケーション長と時間を含む ETA SALT フィールド。
12177	NF_F_ETTA_TLS_RECORDS_IPFIX	TLS フローの最初の N 件のレコードを記述する配列を含む ETA TLS レコードフィールド。
12178	NF_F_ETTA_TLS_CIPHER_SUITES_IPFIX	クライアントによって提供、または TLS フローでサーバーによって選択された最大 N 個の暗号スイートのリストを含む ETA TLS 暗号スイートフィールド。

Element ID	名前	説明
12179	NF_F_ETTA_TLS_EXTENSIONS_IPFIX	TLS フローの Hello メッセージで確認された TLS 拡張を記述する ETA TLS 拡張フィールド。
12180	NF_F_ETTA_TLS_VERSION_IPFIX	フローの TLS Hello メッセージで確認された TLS バージョン番号を含む ETA TLS バージョンフィールド。
12181	NF_F_ETTA_TLS_KEY_LENGTH_IPFIX	TLS ClientKeyExchange メッセージで確認されたクライアントキーの長さを含む ETA TLS キー長フィールド。
12182	NF_F_ETTA_TLS_SESSION_ID_IPFIX	フローの TLS Hello メッセージで確認された（存在する場合）セッション ID 値を含む ETA TLS セッション ID フィールド。
12183	NF_F_ETTA_TLS_RANDOM_IPFIX	このフローの TLS Hello メッセージで確認されたランダム値を含む ETA TLS ランダムフィールド。
12192	NF_F_ETTA_TLS_EXTENSION_LENGTHS_IPFIX	フローの TLS Hello メッセージで確認された最初の N 個の TLS 拡張の拡張の長さのリストを含む ETA TLS 拡張の長さフィールド。
12193	NF_F_ETTA_TLS_EXTENSION_TYPES_IPFIX	フローの TLS Hello メッセージで確認された最初の N 個の TLS 拡張の拡張タイプのリストを含む ETA TLS 拡張タイプフィールド。
16386	ETAInitialDataPacket	ETA（暗号化トラフィック分析）IDP（初期データパケット）フィールド。このフィールドには、フローで送信された初期データパケットのペイロードが含まれています。接続が暗号化される前に URL およびその他の情報を取得するために使用されます。
16387	ETASequenceofPktLengthsandTimes	ETA SLPT（パケット長と時間のシーケンス）フィールド。暗号化されたセッションのパケット長と時

Element ID	名前	説明
		間。
29794	FlowSensorInitiator PEN(8712:Lancope)	メッセージ交換を開始したフローの側を示す Lancope FlowSensor PEN フィールド。0x00：イニシエータ不明 0x01：イニシエータは IP0 0x02：イニシエータは IP1
29795	FlowSensorTCPSYNACKTotalCount PEN (8712:Lancope)	フロー内で発生した SYN/ACK パケットの数を含む Lancope FlowSensor PEN フィールド。
29796	FlowSensorTCPSRSTotalCount PEN (8712:Lancope)	フロー内で発生したソフトリセットの数を含む Lancope FlowSensor PEN フィールド。ソフトリセットは、通常の FIN アプローチとの対比で、セッションを終了するために使用されるリセットです。
29797	FlowSensorRoundTripTime PEN (8712:Lancope)	フローで計算されたラウンドトリップ時間を含む Lancope FlowSensor PEN フィールド。
29798	FlowSensorServerResponseTime PEN (8712:Lancope)	フローで計算されたサーバー応答時間を含む Lancope FlowSensor PEN フィールド。
29799	FlowSensorRetransmits PEN(8712:Lancope)	フローで確認された再送信の数を含む Lancope FlowSensor PEN フィールド。
29800	FlowSensorTCPBadTotalCount PEN (8712:Lancope)	フローで確認された不正フラグの組み合わせの数を含む Lancope FlowSensor PEN フィールド。
29801	FlowSensorTCPFragTotalCount PEN (8712:Lancope)	フローで確認されたフラグメント化されたパケットの数を含む Lancope FlowSensor PEN フィールド。
29802	FlowSensorSourceEmailIn PEN (8712:Lancope)	フローの送信元ホストが受信した電子メールアドレスの数を含む Lancope FlowSensor PEN フィール

Element ID	名前	説明
		ド。
29803	FlowSensorSourceEmailOut PEN (8712:Lancope)	フローの送信元ホストが送信した電子メールアドレスの数を含む Lancope FlowSensor PEN フィールド。
29804	FlowSensorSourceEmailInMessages PEN (8712:Lancope)	フローの送信元ホストが正常に受信した電子メールメッセージの数を含む Lancope FlowSensor PEN フィールド。
29805	FlowSensorSourceEmailOutMessages PEN (8712:Lancope)	フローの送信元ホストが正常に送信した電子メールメッセージの数を含む Lancope FlowSensor PEN フィールド。
29806	FlowSensorSourceEmailInTrys PEN (8712:Lancope)	フローの送信元ホストが受信を試みた電子メールメッセージの数を含む Lancope FlowSensor PEN フィールド。
29807	FlowSensorSourceEmailOutTrys PEN (8712:Lancope)	フローの送信元ホストが送信を試みた電子メールメッセージの数を含む Lancope FlowSensor PEN フィールド。
29808	FlowSensorDestinationEmailIn PEN (8712:Lancope)	フローの宛先ホストが受信した電子メールアドレスの数を含む Lancope FlowSensor PEN フィールド。
29809	FlowSensorDestinationEmailOut PEN (8712:Lancope)	フローの宛先ホストが送信した電子メールアドレスの数を含む Lancope FlowSensor PEN フィールド。
29810	FlowSensorDestinationEmailInMessages PEN (8712:Lancope)	フローの宛先ホストが正常に受信した電子メールメッセージの数を含む Lancope FlowSensor PEN フィールド。
29811	FlowSensorDestinationEmailOutMessages PEN(8712:Lancope)	フローの宛先ホストが正常に送信した電子メールメッセージの数を含む Lancope FlowSensor PEN

Element ID	名前	説明
		フィールド。
29812	FlowSensorDestinationEmailInTrys PEN (8712:Lancope)	フローの宛先ホストが送信を試みた電子メールメッセージの数を含む Lancope FlowSensor PEN フィールド。
29813	FlowSensorDestinationEmailOutTrys PEN (8712:Lancope)	フローの宛先ホストが送信を試みた電子メールメッセージの数を含む Lancope FlowSensor PEN フィールド。
29814	FlowSensorTraces PEN(8712:Lancope)	TTL が 2 未満で、ICMP タイムアウトが発生したフローで発生したパケットの数を含む Lancope FlowSensor PEN フィールド。
29817	FlowSensorEmbeddedICMPProtocol PEN (8712:Lancope)	フロー内で発生した組み込み ICMP パケットのプロトコルを含む Lancope FlowSensor PEN フィールド。
29818	FlowSensorEmbeddedICMPType PEN (8712:Lancope)	フロー内で発生した組み込み ICMP パケットの ICMP タイプフィールドを含む Lancope FlowSensor PEN フィールド。
29819	FlowSensorEmbeddedICMPCode PEN (8712:Lancope)	フロー内で発生した組み込み ICMP パケットの ICMP コードフィールドを含む Lancope FlowSensor PEN フィールド。
29820	FlowSensorApplicationIdentifier PEN (8712:Lancope)	フローで検出されたアプリケーションのアプリケーション ID を含む Lancope FlowSensor PEN フィールド。
29821	FlowSensorBadFlagXmas PEN(8712:Lancope)	フローで確認された Xmas（すべてのフラグを設定）フラグの組み合わせの数を含む Lancope FlowSensor PEN フィールド。
29822	FlowSensorBadFlagSYNFIN PEN (8712:Lancope)	フローで確認された SYN および FIN フラグの両方が設定されているパケットの数を含む Lancope

Element ID	名前	説明
		FlowSensor PEN フィールド。
29823	FlowSensorBadFlagBadRST PEN (8712:Lancope)	フロー内の無効な状況において RST フラグが設定されているパケットの数を含む Lancope FlowSensor PEN フィールド。
29824	FlowSensorBadFlagNoACK PEN (8712:Lancope)	フロー内に設定されている必要がある ACK フラグが設定されていないパケットの数を含む Lancope FlowSensor PEN フィールド。
29825	FlowSensorBadFlagURG PEN(8712:Lancope)	フロー内の無効な状況において URG フラグが設定されているパケットの数を含む Lancope FlowSensor PEN フィールド。
29826	FlowSensorBadFlagNoFlag PEN (8712:Lancope)	フロー内のフラグが設定されていないパケットの数を含む Lancope FlowSensor PEN フィールド。
29828	FlowSensorShortFragAttack PEN (8712:Lancope)	フロー内の短いフラグメントの数を含む Lancope FlowSensor PEN フィールド。
29829	FlowSensorFragPacketTooShort PEN (8712:Lancope)	フロー内の短すぎるフラグメントの数を含む Lancope FlowSensor PEN フィールド。
29830	FlowSensorFragPacketTooLong PEN (8712:Lancope)	フロー内の長すぎるフラグメントの数を含む Lancope FlowSensor PEN フィールド。
29831	FlowSensorFragPacketDifferentSizes PEN (8712:Lancope)	フローで使用されているさまざまなサイズのフラグメントの数を含む Lancope FlowSensor PEN フィールド。
29832	FlowSensorApplicationDetails PEN (8712:Lancope)	フローで使用されている最初のパケットペイロード情報または検出されたアプリケーションの詳細のいずれかを含む、Lancope FlowSensor PEN オーバーロードフィールド。

Element ID	名前	説明
29833	FlowSensorTrustSecSourceIdentifier PEN (8712:Lancope)	送信元ホストの TrustSec ID を含む Lancope FlowSensor PEN フィールド。
29844	EndpointFlowProcessAccount	EndpointFlowProcessName を実行しているユーザーアカウントを含むエンドポイントフィールド。
29845	EndpointFlowProcessName	現在実行中のプロセスの名前を含むエンドポイントフィールド。
29846	EndpointFlowProcessHash	現在実行中のプロセスのハッシュを含むエンドポイントフィールド。
29847	EndpointFlowParentProcessAccount	EndpointFlowProcessName を実行しているプロセスの親のユーザーアカウントを含むエンドポイントフィールド。
29848	EndpointFlowParentProcessName	EndpointFlowProcessName を実行しているプロセスの親の名前を含むエンドポイントフィールド。
29849	EndpointFlowParentProcessHash	EndpointFlowProcessName を実行しているプロセスの親のハッシュを含むエンドポイントフィールド。
33002	ASAFirewallExtendedEvent	Cisco ASA ファイアウォール拡張イベント 0：無視 1001：フロー拒否（入力 ACL による） 1002：フロー拒否（出力 ACL による） 1003：フロー拒否（インターフェイスサービスへの接続の試み） 1004：フロー拒否（最初のパケットが TCP SYN ではないため） 1005 ～ 1999：文書化されていない 2000+：フロー削除

Element ID	名前	説明
34000	TrustSecSourceIdentifier	送信元ホストの TrustSec ID を含む Cisco フィールド。
34001	TrustSecDestinationIdentifier	宛先ホストの TrustSec ID を含む Cisco フィールド。
34002	TrustSecSourceName	送信元ホストの TrustSec 名を含む Cisco フィールド。
34003	TrustSecDestinationName	宛先ホストの TrustSec 名を含む Cisco フィールド。
40000	ASAUsername	フロー内のユーザー名を示す Cisco ASA ファイアウォールユーザー名フィールド。
40001	ASAXlateSourceAddressIPV4	Cisco ASA NAT 送信元アドレス IPV4。
40002	ASAXlateDestinationAddressIPV4	Cisco ASA NAT 宛先アドレス IPV4。
40003	ASAXlateSourcePort	Cisco ASA NAT 変換後の送信元ポート。
40004	ASAXlateDestinationPort	Cisco ASA NAT 変換後の宛先ポート。
41105	ART_Server_Bytes	すべてのサーバーパケットのバイトおよびパケット数（レイヤ 3）。
41106	ART_Client_Bytes	すべてのクライアントパケットのバイトおよびパケット数（レイヤ 3）。
42040	AVCResponsesCountDelta	AVC 応答数差分フィールド。RTT と SRT の決定に使用されます。
42071	AVCSummaryResponseTime	AVC サマリー応答時間フィールド。このフィールドを AVCResponsesCountDelta フィールドで割ると、RTT が生成されます。
42074	AVCSummaryServerResponseTime	AVC サマリーサーバーの応答時間フィールド。このフィールドを

Element ID	名前	説明
		AVCResponsesCountDelta フィールドで割ると、SRT が生成されます。
44940	ETAInitialDataPacket	ETA IDP フィールド。フローで送信された初期データパケットのペイロードを含むフィールド。接続が暗号化される前に URL およびその他の情報を取得するために使用されます。
44941	ETASequenceofPktLengthsandTimes	ETA SLPT フィールド。暗号化されたセッションのパケット長と時間。
44944	ETAByteDistribution	ETA BD（バイト分布）フィールド。暗号化されたセッションのバイト分布。
45003	AVCSubApplicationValue	フローで使用されるアプリケーションを識別する Cisco NBAR2 フィールド。FlowCollector がプルして Secure Network Analytics フローにアタッチするホストおよび URL の情報を含めることもできます。
45004	AVC_Client_IPV4_Address	IP パケットヘッダー内の IPv4 クライアントアドレス。これは、接続の最初のパケットに応じて、送信元または宛先の IP アドレスになります。クライアントは、セッションの作成をトリガーしたデバイスであり、セッションの期間中も同じです。
45005	AVC_Server_IPV4_Address	IP パケットヘッダーの IPv4 サーバーアドレス。サーバーは、クライアントに応答するデバイスであり、セッションの期間中も同じです。
45006	AVC_Client_IPV6_Address	IP パケットヘッダー内の IPv6 クライアントアドレス。クライアントは、セッションの作成をトリガーしたデバイスであり、セッションの期間中も同じです。
45007	AVC_Server_IPV6_Address	IP パッカーヘッダー内の IPv6

Element ID	名前	説明
		サーバーアドレス。サーバーは、クライアントに応答するデバイスであり、セッションの期間中も同じです。
45008	AVC_Client_Transport_Port	クライアントの転送ポート ID。これは、送信元または宛先の転送ポートになります。クライアントは、セッションの作成をトリガーしたデバイスであり、セッションの期間中も同じです。
45009	AVC_Server_Transport_Port	サーバーの転送ポート ID。これは、送信元または宛先の転送ポートになります。サーバーは、クライアントに応答するデバイスであり、セッションの期間中も同じです。
56701	PaloAltoApplicationIdentifier PEN(25461)	フローで使用されている Palo Alto アプリケーション ID を含む Palo Alto PEN フィールド。
56702	PaloAltoUserIdentifier PEN(25461)	フロー内の Palo Alto ユーザー名を含む Palo Alto PEN フィールド。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

著作権情報