Cisco ASA NetFlow 導入ガイド

初版：2014 年 8 月 14 日

Cisco ASA NetFlow 導入ガイド

このガイドでは、NetFlow Secure Event Logging（NSEL）の設定方法、NSEL を介したイベントおよび syslog メッセージの処理方法と、NetFlow コレクタの使用方法について説明します。

NSEL について

Cisco ASA では、NetFlow バージョン 9 サービスがサポートされています。ASA および ASASM の NSEL の実装はステートフルであり、フロー内の重要なイベントを示すレコードだけをエクスポートする IP フローのトラッキング方式です。ステートフル フロー トラッキングでは、追跡されるフローは一連のステートの変更を通過します。

Netflow データを ASA デバイスから手動で抽出し、コレクタに送信することはできません。NSEL イベントはフローステータスについてのデータをエクスポートするために使用され、ステートの変更を引き起こしたイベントによってトリガーされます。

追跡される重要なイベントには、flow-create、flow-teardown、flow-denied（EtherType ACL によって拒否されるフローを除く）および flow-update が含まれます。NSEL の ASA 実装が定期 NSEL イベントと flow-update イベントを生成して、フローの期間の定期的なバイト カウンタを提供します。これらのイベントは通常、タイム ドリブンです。このため、従来の NetFlow でよりインラインとなりますが、これらのイベントはそのフローの状態変更によってもトリガーされます。

（注） flow-update イベント機能は、バージョン 9.0（1）では使用できません。バージョン 8.4(5) および 9.1(2) 以降で使用できます。

ASA はまた、syslog メッセージもエクスポートしますが、これには同じ情報が含まれています。そこで同じイベントに対して NSEL レコードと syslog メッセージが生成されないように、同じ情報を持つsyslogメッセージをディセーブルにすることで、パフォーマンスの低下を防止できます。

各 NSEL レコードにはイベント ID と拡張イベント ID フィールドがあり、これらによってフロー イベントが記述されます。

syslog メッセージと NSEL イベント

次の表に、同等の NSEL イベント、イベント ID、および拡張イベント ID を持つ syslog メッセージを示します。拡張イベント ID は、イベントについての詳細を提供します（入力または出力のどちらの ACL がフローを拒否したかなど）。

（注） NetFlow がフロー情報をエクスポートできるようにすると、対応する syslog メッセージが重複します。パフォーマンスの向上のためには、同じ情報が NetFlow を通してエクスポートされるため、冗長な syslog メッセージをディセーブルにすることをお勧めします。NetFlow 関連の syslog メッセージのディセーブル化と再イネーブル化の手順に従って、個々の Syslog メッセージを有効または無効にできます。

表 *1 : syslog* メッセージと同等の *NSEL* イベント

syslog メッセージ	説明	NSEL イベント ID	NSEL 拡張イベント ID
106100	ACL が発生するたびに生成されます。	1：フローが作成されました（ACL がフローを許可した場合）。 3：フローが拒否されました（ACL がフローを拒否した場合）。	0：ACL がフローを許可した場合。 1001：入力 ACL によってフローが拒否されました。 1002：出力 ACL によってフローが拒否されました。
106015	最初のパケットが SYN パケットではなかったため、TCP フローが拒否されました。	3：フローが拒否されました。	1004：最初のパケットが TCP SYN パケットではなかったため、フローが拒否されました。
106023	**access-group** コマンドによってインターフェイスに接続された ACL によってフローが拒否された場合。	3：フローが拒否されました。	1001：入力 ACL によってフローが拒否されました。 1002：出力 ACL によってフローが拒否されました。
302013、302015、302017、302020	TCP、UDP、GRE、および ICMP 接続の作成。	1：フローが作成されました。	0：無視します。
302014、302016、302018、302021	TCP、UDP、GRE、および ICMP 接続のティアダウン。	2：フローが削除されました。	0：無視します。 >2000：フローが切断されました。
313001	デバイスへの ICMP パケットが拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。

syslog メッセージ	説明	NSEL イベント ID	NSEL 拡張イベント ID
313008	デバイスへの ICMP v6 パケットが拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。
710003	デバイス インターフェイスへの接続の試行が拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。

（注） NSEL メッセージと syslog メッセージの両方がイネーブルにされている場合、2 つのロギング タイプ間が時系列順になる保証はありません。

NSEL コレクタ

各 ASA はコレクタへの独自の接続を確立します。エクスポート パケットのヘッダーのフィールドには、システムのアップ タイム、UNIX タイム（クラスタ間で同期される）が含まれます。これらのフィールドは、すべて個々の ASA に対してローカルです。NSEL コレクタは、パケットの送信元 IP アドレスと送信元ポートの組み合わせを使用して、異なるエクスポータを区切ります。

各 ASA は、テンプレートを個別に管理し、アドバタイズします。ASA がクラスタ内アップグレードをサポートするため、特定の時点で、異なるユニットが異なるイメージバージョンを実行する場合があります。その結果、各 ASA がサポートするテンプレートが異なる可能性があります。

双方向のフロー

双方向のフローのほとんどは、すでに内部でアセンブルされ、単一のフローとして扱われています。NSEL が ASA に関してレポートするフローレコードには、双方向のフローが記載されます。データ レコードでは、発信元（発信側）と送信先（応答側）が明示されるので、コレクタ アプリケーションがフローの方向を区別する必要がある場合は、この情報を使用して判断できます。さらに、一部の NSEL レコードには 2 バイトのカウンタ フィールドである NF_F_FWD_FLOW_DELTA_BYTES と NF_F_REV_FLOW_DELTA_BYTES が含まれ、方向固有のトラフィック データを提供します。

テンプレートの更新

RFC 3954、Cisco Systems NetFlow Services Export バージョン 9 の規定によると、テンプレートは、一定の時間間隔または一定数のデータ レコードがエクスポートされた後、のいずれかの更新間隔でユーザーに送信できます。このような更新間隔は、設定可能である必要があります。この実装では、時間間隔によるテンプレートの更新のみをサポートします。データ レコード数に基づくテンプレート更新は、サポートされていません。

オプションのテンプレートとデータ レコード

オプションのテンプレートとデータ レコードは、エクスポートされません。一部のフィールドは、CLI の **show** コマンドによってサポートされています。コレクタ アプリケーションが特定のフィールドに関する追加情報を取得するには、**show** コマンドを実行する必要があります。また、コレクタには、一意のホスト名と IP アドレスが必要です。そうでなければ、検査動作が予測不可能になります。

観測ポイントと観測ドメイン

ASA は観測ドメインで、各インターフェイスも観測ポイントです。フローは、作成インターフェイスに関係なくすべてエクスポートされます。特定のインターフェイスのセットによって作成されたデータに限定し、またはそれらのデータをフィルタリングしてエクスポートするオプションは存在しません。ASA に外部デバイスが接続されている場合、その外部デバイスによって作成されるフローもエクスポートされます。

フローのフィルタリング

特定のフローのレコードだけをエクスポートする必要が生じることがあります。この場合、たとえば、ASA は、ACE に一致するフローの NSEL イベントを生成できます。この方法を使用すれば、NetFlow 用に生成される NSEL イベントの数を制限できます。この実装では、Modular Policy Framework によってトラフィックやイベント タイプごとに NSEL イベントをフィルタリングし、レコードを異なるコレクタに送信する処理がサポートされます。

たとえば、2 つのコレクタを使用して、次の操作を実行できます。

- すべてのフロー作成イベントをコレクタ 1 にロギングする。
- ACL1 に一致するすべてのフロー拒否イベントをコレクタ 1 にロギングする。
- ACL1 に一致するすべてのイベントをコレクタ 2 にロギングする。

Modular Policy Framework が NetFlow 用に設定されていない場合、NSEL イベントは生成されません。

データ フィールド（**Data Fields**）

次の表に、ASA から NSEL を介してエクスポートされるデータ要素を示します。必須データ要素のリストは、イベントに対して生成された syslog メッセージによってエクスポートされ、NSEL レコードのエクスポートをもたらすデータを集約して作成されました。

（注） NetFlow は、IFC SNMP IF インデックスを使用して、vpifNum に基づくインターフェイスを報告します。ただし、vpifnum には Identity インターフェイスに対する有効な値がありません。したがって、エクスポート済みの NetFlow レコードの場合、ASA バージョン 8.0 のインターフェイス ID 番号は 65535 と表示されます。

各列では、次の情報を示します。

- ID：フィールド タイプを表す一意の名前
- タイプ：このフィールド タイプに割り当てられた値
- LEN：選択した ASA 用にエクスポートされたレコードのフィールドの長さ
- 説明：フィールド タイプの説明

表 *2 : NSEL* によってエクスポートされるデータ レコード

ID	タイプ	長さ	説明
接続 ID フィールド			
NF_F_CONN_ID	148	4	デバイスの一意のフロー用の ID
フロー ID フィールド（L3 IPv4）			
NF_F_SRC_ADDR_IPV4	8	4	発信元 IPv4 アドレス
NF_F_DST_ADDR_IPV4	12	4	送信先 IPv4 アドレス
NF_F_PROTOCOL	4	1	IP 値
フロー ID フィールド（L3 IPv6）			
NF_F_SRC_ADDR_IPV6	27	16	発信元 IPv6 アドレス
NF_F_DST_ADDR_IPV6	28	16	送信先 IPv6 アドレス
フロー ID フィールド（L4）			
NF_F_SRC_PORT	7	2	送信元ポート
NF_F_DST_PORT	11	2	宛先ポート
NF_F_ICMP_TYPE	176	1	ICMP タイプ値
NF_F_ICMP_CODE	177	1	ICMP コード値
NF_F_ICMP_TYPE_IPV6	178	1	ICMP IPv6 タイプ値
NF_F_ICMP_CODE_IPV6	179	1	ICMP IPv6 コード値
フロー ID フィールド（INTF）			
NF_F_SRC_INTF_ID	10	2	入力 IFC SNMP IF インデックス
NF_F_DST_INTF_ID	14	2	出力 IFC SNMP IF インデックス
マッピングされたフロー ID フィールド（L3 IPv4）			

ID	タイプ	長さ	説明
NF_F_XLATE_SRC_ADDR_IPV4	225	4	NAT 後の送信元 IPv4 アドレス
NF_F_XLATE_DST_ADDR_IPV4	226	4	NAT 後の宛先 IPv4 アドレス
NF_F_XLATE_SRC_PORT	227	2	NATT 後の送信元トランスポート ポート
NF_F_XLATE_DST_PORT	228	2	NATT 後の宛先トランスポート ポート
マッピングされたフロー ID フィールド（L3 IPv6）			
NF_F_XLATE_SRC_ADDR_IPV6	281	16	NAT 後の送信元 IPv6 アドレス
NF_F_XLATE_DST_ADDR_IPV6	282	16	NAT 後の宛先 IPv6 アドレス
ステータスまたはイベント フィールド			
NF_F_FW_EVENT	233	1	高レベルのイベント コード。表示される値は次のとおりです。 • 0：デフォルト（無視）。 • 1：フローが作成されました。 • 2：フローが削除されました。 • 3：フローが拒否されました。 • 4：フロー アラート • 5：フロー更新
NF_F_FW_EXT_EVENT	33002	2	拡張イベント コードこれらの値は、イベントに関する詳細情報を提供します。
タイムスタンプおよび統計情報フィールド			
NF_F_EVENT_TIME_MSEC	323	8	IPFIXから取得されたイベントが発生した時刻。マイクロ秒単位の場合は324、ナノ秒単位の場合は 325 を使用します。時刻は、0000 UTC 1970/01/01 からの経過時間をミリ秒単位で表示します。

ID	タイプ	長さ	説明
NF_F_FLOW_CREATE_TIME_MSEC	152	8	フローが作成された時刻。フロー作成イベントが先に送信されなかったフローティアダウン イベントに含まれます。フローの持続時間は、フローティアダウン時刻とフロー作成時刻のイベント時刻を使用して判定できます。
NF_F_FWD_FLOW_DELTA_BYTES	231	4	送信元から宛先への差分バイト数。
NF_F_REV_FLOW_DELTA_BYTES	232	4	宛先から送信元への差分バイト数。
ACL フィールド			
NF_F_INGRESS_ACL_ID	33000	12	フローを許可または拒否した入力 ACL すべての ACL ID は、次の 3 つの 4 バイト値で構成されます。 • ACL 名のハッシュ値または ID • ACL 内の ACE のハッシュ値、ID、または行 • 拡張 ACE 設定のハッシュ値または ID
NF_F_EGRESS_ACL_ID	33001	12	フローを許可または拒否した出力 ACL
AAA フィールド			
NF_F_USERNAME	40000	20	AAA ユーザー名
NF_F_USERNAME_MAX	40000	65	最大許可サイズの AAA ユーザー名

イベント ID フィールド

イベント ID フィールドには、NSEL レコードが発生したイベントが記述されます。次の表に、イベント ID の値を示します。

表 *3:* イベント *ID* の値

イベント ID	説明
[0]	無視：この値は、フィールドを無視する必要があることを示します。現在のリリースでは使用されません。
1	フロー作成：この値は、新しいフローが作成されたことを示します。
2	フロー削除：この値は、フローが削除されたことを意味します。
3	フロー拒否：この値は、フローが拒否されたことを意味します。
5	フロー更新：この値は、フローのタイマーが停止またはフローが切断されたことを示します。

拡張イベント ID フィールド

拡張イベント ID は、特定のイベントに関する追加情報を提供します。このフィールドは、製品固有のフィールド ID（33002）を含みます。次の表に、拡張イベント ID の値を示します。

表 *4:* 拡張イベント *ID* の値

拡張イベント ID	イベント	説明
[0]	無視	この値は、フィールドを無視する必要があることを示します。
> 1000	フロー拒否	1000 を超える値は、フローが拒否された理由を表します。
1001	フロー拒否	フローが入力 ACL から拒否されました。
1002	フロー拒否	フローが出力 ACL によって拒否されました。
1003	フロー拒否	考えられる原因は、次のとおりです。 • ASA インターフェイスへの接続の試みが拒否されました。 • デバイスへの ICMP パケットが拒否されました。 • デバイスへの ICMPv6 パケットが拒否されました。
1004	フロー拒否	TCP の最初のパケットが TCP SYN パケットではありませんでした。
> 2000	フロー削除	2000 を超える値は、フローが終了した理由を表します。

フロー削除された拡張イベント ID（2000 以降）

次の表は、2000 以上の値を持つさまざまなフロー削除拡張イベント ID について説明しています。

表 *5*：フロー削除された拡張イベント *ID*（*2000* 以降）

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2001	NP_FLOW_TUNNEL_TORN_DOWN トンネルが切断されます。 このカウンタは、IPSec セキュリティ アソシエーションの削除中に確立されたフローに関連付けられたパケットをアプライアンスが受信すると増加します。 **推奨事項**： これは、IPSec トンネルが何らかの理由により切断された場合に見られる正常な状態です。	なし
2002	NP_FLOW_NO_IPV6_IPSEC IPv6 を介した IPSec はサポートされていません。 このカウンタは、アプライアンスが IPSec ESP パケット、IPSec NAT-T ESP パケット、または IP バージョン 6 ヘッダーにカプセル化された IPSec over UDP ESP パケットを受信すると増加します。アプライアンスは現在、IP バージョン 6 にカプセル化された IPSec セッションをサポートしていません。 **推奨事項**：なし	なし
2003	NP_FLOW_TUNNEL_PENDING トンネルが起動または切断されています このカウンタは、アプライアンスがセキュリティ ポリシー データベース（つまり暗号マップ）のエントリと一致するパケットを受信したときに増加しますが、セキュリティ アソシエーションはネゴシエート中です。まだ完成していません。 このカウンタは、アプライアンスがセキュリティ ポリシー データベースのエントリと一致するパケットを受信したが、セキュリティ アソシエーションが削除された、または削除中の場合にも増加します。この表示と「トンネルが切断されました」という表示の違いは、後者は確立されたフローに対するものであるということです。 **推奨事項**： これは、IPSec トンネルがネゴシエートまたは削除されているときに見られる正常な状態です。	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2004	NP_FLOW_NEED_IKE IKE ネゴシエーションを開始する必要があります。 このカウンタは、アプライアンスが暗号化を必要とするが確立された IPSec セキュリティアソシエーションを持たないパケットを受信すると、増加します。これは通常、LAN-to-LAN IPSec 設定に見られる正常な状態です。この指示により、アプライアンスは宛先ピアとの ISAKMP ネゴシエーションを開始します。 **推奨事項**： アプライアンスで IPSec LAN-to-LAN を設定している場合、この表示は正常であり、問題を示すものではありません。ただし、このカウンタが急速に増加する場合は、ISAKMP ネゴシエーションの完了を妨げる暗号設定エラーまたはネットワークエラーが発生している可能性があります。 宛先ピアと通信可能であることを確認し、**show running-config** コマンドを使用して、暗号化設定を確認します。	なし
2005	NP_FLOW_VPN_HANDLE_ERROR VPN ハンドルエラーです。 このカウンタは、VPN ハンドルが既に存在するためにアプライアンスが VPN ハンドルを作成できない場合に増分されます。 **推奨事項**： 通常の操作の一部として、このカウンタの増分を確認することができます。ただし、カウンタが急速に増分している場合や、VPN ベースのアプリケーションに著しい不適切動作が見られる場合は、ソフトウェアの欠陥によって発生している可能性があります。次のコマンドを使用して、このカウンタに関する詳細情報を収集し、Cisco TAC に連絡して問題をさらに調査してください。 **capture** *name***type asp-drop vpn-handle-error** **show asp table classify crypto** **show asp table vpn-context detail**	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2006	NP_FLOW_VPN_HANDLE_NOT_FOUND VPN ハンドルが見つかりません。 このカウンタは、データグラムが暗号化または復号操作にヒットし、データグラムが存在するフローの VPN ハンドルが見つからない場合に増分されます。 **推奨事項**： 通常の操作の一部として、このカウンタの増分を確認することができます。ただし、カウンタが急速に増分している場合や、VPNベースのアプリケーションに著しい不適切動作が見られる場合は、ソフトウェアの欠陥によって発生している可能性があります。次のコマンドを使用して、このカウンタに関する詳細情報を収集し、CiscoTACに連絡して問題をさらに調査してください。 **capture** *name***vpn-handle-not-found** **show asp table classify crypto** **show asp table vpn-context detail**	なし
2007	NP_FLOW_IPSEC_SPOOF_DETECT IPSec スプーフィングパケットが検出されました。 このカウンタは、アプライアンスが暗号化されているはずにもかかわらず暗号化されていないパケットを受信すると、増加します。パケットは、アプライアンスで設定および確立された IPSec 接続の内部ヘッダー セキュリティ ポリシー チェックと一致しましたが、暗号化されずに受信されました。これはセキュリティの問題です。 **推奨事項**： ネットワークトラフィックを分析して、スプーフィングされたIPSecトラフィックの送信元を特定します。	402117
2008	NP_FLOW_IPSEC_SP_DETUNNEL_FAIL IPsec のトンネル解除が失敗しました。 このカウンタは、クリアテキストフローがIPSecトンネルフロー処理に失敗すると増加します。 **推奨事項**： **show asp drop** コマンドを使用して、より詳細なパケットドロップを確認できます。	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2009	NP_FLOW_SVC_SPOOF_DETECT SVC スプーフィングパケットが検出されました。 このカウンタは、セキュリティアプライアンスが暗号化されているはずのパケットを受信すると増加しますが、暗号化されていません。パケットは、セキュリティアプライアンスで設定および確立された SVC 接続の内部ヘッダーのセキュリティポリシーチェックと一致しましたが、暗号化されずに受信されました。これはセキュリティの問題です。 **推奨事項**： ネットワークトラフィックを分析して、スプーフィングされたSVCトラフィックの送信元を特定します。	なし
2010	NP_FLOW_SOCKET_SVC_FAILOVER スタンバイユニットで SVC ソケット接続が切断されています。 このカウンタは、アクティブ装置がフェールオーバー遷移の一部としてスタンバイ状態に移行するときに新規の SVC ソケット接続が切断されると、増分します。 これは、現在のデバイスがアクティブからスタンバイに移行しているときの SVC 接続の通常のクリーンアップの一環です。デバイス上の既存の SVC 接続は無効になり、削除する必要があります。 **推奨事項**：なし	なし
2011	NP_FLOW_SOCKET_SVC_CONN_REPLACE SVC 交換接続が確立されました。 このカウンタは、SVC 接続が新しい接続に置き換えられると増加します。 **推奨事項**：なし これは、ユーザーが ASA への接続を維持するのに問題があることを示している可能性があります。ユーザーは、ホームネットワークとインターネット接続の品質を評価する必要があります。	722032
2012	NP_FLOW_VPN_SELECTOR_MISMATCH IPSec VPN 内部ポリシーセレクタの不一致が検出されました。 このカウンタは、トンネルに設定されたポリシーと一致しない内部IPヘッダーを含む IPSec パケットが受信されたときに増分されます。 **推奨事項**： トンネルの暗号 ACL が正しいこと、および許容可能なすべてのパケットがトンネル ID に含まれていることを確認します。このメッセージが繰り返し表示される場合は、ボックスが攻撃を受けていないことを確認してください。	402116

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2013	NP_DROP_FLOW_VPN_EXPIRED VPN コンテキストの期限が切れました。 このカウンタは、セキュリティアプライアンスが暗号化または復号を必要とするパケットを受信し、操作の実行に必要な ASP VPN コンテキストが無効になると増加します。 **推奨事項**： これは、ソフトウェアエラーを Cisco TAC に報告する必要があることを示しています。	なし
2014	NP_DROP_FLOW_VPN_OVERLAP_CONFLICT VPN ネットワークの重複が原因で競合しています。 パケットが復号されると、内部パケットが暗号マップの設定に対して検査されます。パケットが受信したものとは異なる暗号マップエントリと一致する場合、パケットはドロップされ、このカウンタが増加します。これの一般的な原因は、類似または重複するアドレス空間を含む 2 つの暗号マップエントリによるものです。 **推奨事項**： 重複するネットワークがないか VPN 設定を確認してください。暗号マップの順序と ACL での「拒否」ルールの使用を確認します。	なし
2015	NP_DROP_FLOW_VPN_LOCK_ERR IPSec ロックにエラーが発生しました。 このカウンタは、内部ロックエラーにより VPN フローを作成できない場合に増分されます。 **推奨事項**： この状態は通常の操作中には発生しないはずであり、アプライアンスのソフトウェアの問題を示している可能性があります。このエラーが発生した場合は、Cisco Technical Assistance Center（TAC）に連絡してください。	なし
2016	NP_DROP_FLOW_VPN_RECLASSIFY_FAILED 既存の VPN ポリシーに従ってフローを再分類できませんでした。 VPN ポリシーが変更されると、それらのポリシーに一致しなくなったフローは、それらのフローにパケットが到着するときに解放されます。 **推奨事項**：なし このカウンタは情報提供であり、予想される動作です。	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2017 年	NP_DROP_FLOW_VPN_MISSING_DECRYPT 復号ポリシーが利用できなかったため、フローを作成できませんでした。 復号ポリシーが完全に初期化される前に、VPN フローの作成が試行されました。これは一時的な状態であり、復号ポリシーのインストールが完了すると解決されます。 **推奨事項**： 通常の操作の一部として、このカウンタの増分を確認することができます。ただし、カウンタが急速に増加し、トラフィックが中断している場合は、設定の誤りまたはソフトウェアの欠陥が原因である可能性があります。次のコマンドを使用して、このカウンタに関する詳細情報を収集し、Cisco TAC に連絡して問題をさらに調査してください。 **capture** *name***type asp-drop vpn-missing-decrypt** **show asp table classify** **show asp drop** **show tech-support**	なし
2018	NP_DROP_FLOW_VPN_BAD_DECRYPT_RULE 間違った復号ポリシーがヒットしたため、フローを作成できませんでした。 これは、クラスタリングが有効で、VPN モードが分散に設定されている場合の一時的な状態です。 **推奨事項**： 通常の操作の一部として、このカウンタの増分を確認することができます。ただし、カウンタが急速に増加し、トラフィックが中断している場合は、設定の誤りまたはソフトウェアの欠陥が原因である可能性があります。次のコマンドを使用して、このカウンタに関する詳細情報を収集し、Cisco TAC に連絡して問題をさらに調査してください。 **show asp drop** **show tech-support**	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2019	NP_DROP_FLOW_VPN_INVALID_ENCRYPTION_PACKET 暗号化フラグが設定されていないため、フローはドロップされます。 **推奨事項**： 通常の操作の一部として、このカウンタの増分を確認することができます。ただし、カウンタが急速に増加し、トラフィックが中断している場合は、設定の誤りまたはソフトウェアの欠陥が原因である可能性があります。次のコマンドを使用して、このカウンタに関する詳細情報を収集し、Cisco TAC に連絡して問題をさらに調査してください。 **show asp drop** **show tech-support**	なし
2020	NP_FLOW_OUT_OF_MEMORY フローを完了するためのメモリがありません。 このカウンタは、メモリ不足のためにアプライアンスがフローを作成できない場合に増分されます。 **推奨事項**： 現在の接続を確認して、アプライアンスが攻撃を受けていないことを確認します。また、設定したタイムアウト値が大きすぎるために、アイドル状態のフローがメモリに長時間常駐していないかどうかも確認します。 **show memory** コマンドを発行して、使用可能な空きメモリをチェックします。空きメモリが少ない場合は、**show processes memory** コマンドを発行し、どのプロセスがメモリーの大部分を使用しているかを判別してください。	なし
2021	NP_FLOW_PARENT_CLOSED 親フローが終了しました。 従属の親フローが終了すると、従属フローも終了します。たとえば、FTP データフロー（従属フロー）は、その制御フロー（親フロー）が終了すると終了します。セカンダリフロー（ピンホール）がその制御アプリケーションによって終了した場合も同様です。たとえば、BYE メッセージを受信すると、SIP 検査エンジン（制御アプリケーション）により、対応する SIP RTP フロー（セカンダリフロー）は終了します。 **推奨事項**：なし	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2022	NP_FLOW_CLOSED_BY_FIXUP インスペクションによりフローが終了しました。 アプリケーション検査中にエラーが検出されるとフローが終了します。たとえば、H323 メッセージの検査中にエラーが検出された場合、対応する H323 フローは終了します。 **推奨事項**：なし	なし
2023	NP_FLOW_FO_PRIMARY_CLOSED フェールオーバープライマリが終了しました。 スタンバイユニットがアクティブユニットからフロー削除メッセージを受信し、フローを終了しました。 **推奨事項**： アプライアンスがステートフルフェールオーバーを実行している場合、このカウンタは、スタンバイアプライアンスで切断された複製された接続ごとに増分する必要があります。	302014、302016、302018
2024	NP_FLOW_FO_STANDBY フェールオーバースタンバイによってフローが終了しました。 through-the-box パケットがスタンバイ状態のアプライアンスまたはコンテキストに到着し、フローが作成されると、パケットはドロップされ、フローが削除されます。このカウンタは、この方法でフローが削除されるたびに増分します。 **推奨事項**： このカウンタは、アクティブなアプライアンスまたはコンテキストで増分されないようにする必要があります。ただし、スタンバイアプライアンスまたはコンテキストで増分するのは正常です。	302014、302016、302018
2025	NP_FLOW_FO_REP_ERR スタンバイ フロー レプリケーションのエラーが発生しました。 スタンバイユニットがフローの複製に失敗しました。 **推奨事項**： アプライアンスが VPN トラフィックを処理している場合は、IKE SA 情報よりも先にフローが複製されるため、このカウンタはスタンバイ装置上で常に増分しています。この場合、アクションは不要です。アプライアンスが VPN トラフィックを処理していない場合、これはソフトウェアの欠陥を示しています。スタンバイユニットで **debug fover fail** コマンドを使用し、デバッグ出力を収集して、問題を Cisco TAC に報告します。	302014、302016、302018

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2026	NP_FLOW_LOOPBACK フローはループバックです。 次の条件によりフローが終了します：1）フローにUターントラフィックが存在する場合、および 2）**same-security-traffic permit intra-interface** が設定されていない場合。 **推奨事項**： インターフェイスでUターントラフィックを許可するには、**same-security-traffic permit intra-interface** を使用してインターフェイスを設定します。	なし
2027	NP_FLOW_ACL_DROP フローはアクセスルールによって拒否されます。 302014、302016、302018、302021、305010、305012、609002 このルールは、ボックスが表示されたとき、さまざまな機能がオンまたはオフになったとき、ACL がインターフェイスまたはその他の機能に適用されたときに作成されるデフォルトのルールである可能性があります。デフォルトの規則のドロップを除き、フローが拒否される理由は次のとおりです。 • ACL がインターフェイスに設定されている • AAA および AAA 用に設定された ACL によりユーザーが拒否された。 • Through-the-box トラフィックを通過して管理専用インターフェイスに到達した。 • IPSec がイネーブルになっているインターフェイスに、暗号化されていないトラフィックが到達した。 • ACL の末尾で **ip any any** を使用して暗黙的に拒否。 **推奨事項**： パケットとフローのドロップに関連する syslog メッセージを探します。	なし
2028	NP_FLOW_ACL_DROP_RECLASSIFY 再分類後、フローはアクセスルールによって拒否されます。 このカウンタは、ACL ルールの再分類中にドロップルールがパケットにヒットすると増分されます。 **推奨事項**： パケットとフローのドロップに関連する syslog メッセージを探します。	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2029	NP_FLOW_PINHOLE_TIMEOUT ピンホールがタイムアウトしました。 このカウンタは、アプライアンスがセカンダリフローを開いたことを報告するために増分されますが、タイムアウト間隔内にこのフローを通過したパケットがないため、削除されました。セカンダリフローの例は、FTP 制御チャネルでのネゴシエーションが成功した後に作成される FTP データチャネルです。 **推奨事項**：なし	なし
2030	NP_FLOW_HOST_REMOVED ホストが削除されました。 **clear local-host** コマンドに応答してフローが削除されました。 これは情報カウンタです。 **推奨事項**：なし	302014、302016、302018、302021、305010、305012、609002
2031	NP_FLOW_XLATE_REMOVED Xlate がクリアされました。 **clear xlate** または **clear local-host** コマンドに応答してフローが削除されました。 これは情報カウンタです。 **推奨事項**：なし	302014、302016、302018、302021、305010、305012、609002
2032	NP_FLOW_TIMEOUT 接続がタイムアウトされました。 非アクティビティ タイマーの期限切れのためフローが終了した場合、このカウンタが増分します。 **推奨事項**：なし	302014、302016、302018、302021
2033	NP_FLOW_CONN_LIMIT_EXCEEDED 接続制限値を超えました。 接続制限値を超えたためにフローが終了します。接続制限値は **set connection conn-max** コマンドを使用して設定されます。 **推奨事項**：なし	201011

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2034	NP_FLOW_TCP_FINS TCP FIN です。 TCP FIN パケットを受信した時に TCP フローが終了します。このカウンタは、FIN で正常に終了する TCP 接続ごとに増分します。 **推奨事項**：なし	302014
2035	NP_FLOW_SYN_TIMEOUT SYN タイムアウトです。 初期接続タイマーの期限が切れたために TCP フローが終了します。 **推奨事項**： これらが接続の確立に時間がかかる有効なセッションである場合は、初期タイムアウトを増分します。	302014
2036	NP_FLOW_FIN_TIMEOUT FIN タイムアウトです。 ハーフクローズ接続タイマーの期限が切れたために TCP フローが終了します。 **推奨事項**： これらが TCP フローを終了するのに時間がかかる有効なセッションがある場合は、ハーフクローズタイムアウトを増分します。	302014
2037	NP_FLOW_RESET_IN TCP Reset-I。 TCP リセットがフロー上で受信され、（セキュリティが低いインターフェイスからセキュリティレベルが同じまたは高いインターフェイスへの）発信フローが終了します。 **推奨事項**：なし	302014
2038	NP_FLOW_RESET_OUT TCP Reset-O。 TCP リセットがフロー上で受信され、（セキュリティが高いインターフェイスからセキュリティレベルが同じまたは低いインターフェイスへの）発信フローが終了します。 **推奨事項**：なし	302014

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2039	NP_FLOW_RESET_APPLIANCE TCP Reset-APPLIANCE。 アプライアンスによって TCP リセットが生成されフローが終了します。 **推奨事項**：なし	302014
2040	NP_FLOW_RECURSE 再帰フローが終了します。 フローが再帰的に解放されました。これは、ペアフロー、マルチキャスト従属フロー、および syslog フローに適用され、これらの従属フローごとに syslog が発行されるのを防ぎます。 **推奨事項**：なし	なし
2041	NP_FLOW_PROXY_SERVER_NOT_RESPOND TCP インターセプト、サーバーからの応答がありません。 1 秒ごとに 3 回試行した後 SYN 再送信タイムアウトになりました。サーバーに到達できず、接続が切断されています。 **推奨事項**： サーバーが ASA から到達可能かどうかを確認します。	なし
2042	NP_FLOW_PROXY_UNEXPECTED TCP は予期しない状態をインターセプトします。 TCP インターセプトモジュールの論理エラーで、発生してはなりません。 **推奨事項**： これは、TCP インターセプトモジュールのメモリ破損またはその他の論理エラーを示しています。	なし
2043	NP_FLOW_TCPNORM_REXMIT_BAD TCP の不正な再送信です。 再送信チェック機能が有効になっており、TCP エンドポイントが元のパケットとは異なるデータを再送信すると、TCP フローが終了します。 **推奨事項**： TCP エンドポイントは、TCP 再送信で異なるデータを送信することによって攻撃している可能性があります。パケットキャプチャ機能を使用して、パケットの発信元の詳細を確認してください。	302014

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2044	NP_FLOW_TCPNORM_WIN_VARIATION TCP の予期しないウィンドウサイズの変動です。 TCP エンドポイントによってアドバタイズされたウィンドウサイズが、それほど多くのデータを受け入れずに大幅に変更されると、TCP フローが終了します。 **推奨事項**： この接続を許可するには、tcp-map の下の window-variation 設定を使用します。	302014
2045	NP_FLOW_TCPNORM_INVALID_SYN 無効な SYN による TCP フローの状態 SYN パケットが無効になると TCP フローが終了します。 **推奨事項**： 無効なチェックサムや無効な TCP ヘッダーなど、さまざまな理由で SYN パケットが無効になる可能性があります。なぜ SYN パケットが無効になるかを理解するには、パケットキャプチャ機能を使用してください。これらの接続を許可する場合は、tcp-map 設定を使用してチェックをバイパスします。	302014
2046	NP_FLOW_SCTP_DROP_INIT_0_TAG SCTP INIT には、0 の値の開始タグが含まれています。 SCTP INIT チャンクに 0 の値の開始タグが含まれている場合、このカウンタは増分され、フローはドロップされます。 **推奨事項**：なし	なし
2047	NP_FLOW_SCTP_DROP_INITACK_0_TAG SCTP INIT ACK には、0 の値の開始タグが含まれています。 SCTP INIT ACK チャンクに 0 の値の開始タグが含まれている場合、このカウンタは増分され、フローはドロップされます。 **推奨事項**：なし	なし
2048	NP_FLOW_SCTP_DROP_INIT_0_STREAM_CNT SCTP INIT には、0 値のインバウンド/アウトバウンド ストリーム カウントが含まれます。 SCTP INIT チャンクにインバウンド/アウトバウンド ストリーム カウントの値が 0 の場合、このカウンタは増分され、パケットはドロップされます。 **推奨事項**：なし	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2049	NP_FLOW_SCTP_DROP_INIT_TIMEOUT SCTP INIT がタイムアウトしました（INIT ACK を受信していません）。 SCTP INIT チャンク タイムアウト カウントが制限に達すると、このカウンタが増分され、フローがドロップされます。 **推奨事項**： このドロップは、INIT チャンクの受信者が INIT ACK に応答しない場合や、クライアントとサーバーの間に冗長パスがあり、INIT が 1 つのパスになり、INITACK が別のパスに入る場合などに、発生する可能性があります。このエラーが多数発生する場合は、パケットキャプチャを使用して問題を特定してください。	なし
2050	NP_FLOW_SCTP_DROP_COOKIE_TIMEOUT SCTP Cookie がタイムアウトしました。 SCTP cookie 状態（INITACK または COOKIEECHO を受信した後）のタイムアウトカウントが制限に達すると、このカウンタが増分され、フローがドロップされます。 **推奨事項**：なし	なし
2051	NP_FLOW_SCTP_DROP_ENDPOINT_ABORT SCTP はエンドポイントから ABORT を受信しました。 SCTP 中断チャンクが受信されると、このカウンタは増分され、フローはドロップされます。 **推奨事項**：なし	なし
2052	NP_FLOW_SCTP_DROP_INITACK_0_STREAM_CNT SCTP INIT ACK には、0 値のインバウンド/アウトバウンド ストリーム カウントが含まれます。 SCTP INIT ACK チャンクにインバウンド/アウトバウンド ストリーム カウントの値が 0 の場合、このカウンタは増分され、パケットはドロップされます。 **推奨事項**：なし	なし
2053	NP_FLOW_SCTP_DROP_SHUTDOWN_TIMEOUT SCTP SHUTDOWN がタイムアウトしました（SHUTDOWN ACK を受信していません）。 SCTP SHUTDOWN タイムアウトカウントが制限に達すると、このカウンタが増分され、フローがドロップされます。 **推奨事項**：なし	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2054	NP_FLOW_MCAST_INTRF_REMOVED マルチキャスト インターフェイスが削除されました。 出力インターフェイスがマルチキャストエントリから削除されたか、すべての出力インターフェイスがマルチキャストエントリから削除されました。 **推奨事項**： インターフェイスを削除しただけの場合は、アクションは必要ありません。 すべての出力インターフェイスを削除する場合は、このグループのレシーバがなくなっていることを確認してください。	なし
2055	NP_FLOW_MCAST_ENTRY_REMOVED マルチキャストエントリが削除されました。 次のいずれかです。 • マルチキャストフローに一致するパケットが着信しましたが、マルチキャストサービスが有効でなくなっていたか、またはマルチキャストフローが作成された後で再度イネーブルにされました。 **推奨事項**：ディセーブルになっているマルチキャストを再びイネーブルにします。 • マルチキャストエントリが削除されたため、フローはクリーンアップされていますが、パケットはデータパスに再注入されます。 **推奨事項**：アクションは不要です。	なし
2056	NP_FLOW_KILLED_BY_TCP_INTERCEPT フローは TCP インターセプトによって終了しました。 これが最初の SYN であり、SYN の接続が作成され、TCP インターセプトが SYN Cookie で応答した場合、TCP インターセプトは接続を切断します。またはクライアントより有効な ACK が確認された後、TCP インターセプトがサーバーに SYN を送信した場合、サーバーは RST で応答します。 **推奨事項**： TCP インターセプトは通常、最初の SYN の接続を作成しません。ただし、ルールが定められている場合、パケットが VPN トンネルを経由する場合、またはクライアントに到達するためのネクストホップ ゲートウェイ アドレスが解決されない場合を除きます。したがって、最初の SYN の場合、これは接続が作成されたことを示します。TCP インターセプトがサーバーから RST を受信すると、対応するポートがサーバーで閉じられている可能性があります。	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2057	NP_FLOW_AUDIT_FAILURE 監査エラーです。 関連するアクションとしてリセットされた **ip audit** シグニチャを照合した後、フローが解放されました。 **推奨事項**： フローの削除がこのシグニチャの一致の望ましい結果ではない場合は、**ip audit** コマンドからリセットアクションを削除します。	なし
2058	NP_FLOW_CX_REQUEST フローは CXSC によって終了しました。 CXSC モジュールによって要求されたフローが終了します。 **推奨事項**： CXSC モジュールの syslog とアラートを確認してください。	429002
2059	NP_FLOW_CX_FAIL_CLOSE CXSC フェールクローズ。 CXSC カードがダウンし、CXSC アクションでフェールクローズオプションが使用されたため、フローが終了します。 **推奨事項**： CXSC モジュールを確認して起動します。	429001
2060	NP_FLOW_CX_BAD_HDL CX からのハンドルが正しくないため、ASA によってフローが終了しました。 CX から受け取ったハンドルが無効であるため、フローはドロップされます。 **推奨事項**： CXSC モジュールの syslog とアラートを確認してください。	421004
2061	NP_FLOW_RESET_BY_CX CXSC によりフローがリセットされました。 CXSC モジュールによって要求された TCP フローが終了します。 **推奨事項**： CXSC モジュールの syslog とアラートを確認してください。	429003

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2062	NP_FLOW_SFR_REQUEST SFR によりフローが終了しました。 ASA FirePOWER モジュールによって要求されたフローが終了します。 **推奨事項**： ASA FirePOWER モジュールの syslog とアラートを確認します。	434002
2063	NP_FLOW_SFR_FAIL_CLOSE SFR フェールクローズ。 ASA FirePOWER モジュールがダウンし、SRF アクションでフェールクローズオプションが使用されたためにフローが終了します。 **推奨事項**： ASA FirePOWER モジュールを確認して起動します。	434001
2064	NP_FLOW_SFR_BAD_HDL SFR からのハンドルが正しくないため、ASA によってフローが終了しました。 ASA FirePOWER から受け取ったハンドルが無効であるため、フローがドロップします。 **推奨事項**： ASA FirePOWER モジュールの syslog とアラートを確認します。	421004
2065	NP_FLOW_RESET_BY_SFR SFR によりフローがリセットされました。 ASA FirePOWER モジュールによって要求された TCP フローが終了します。 **推奨事項**： ASA FirePOWER モジュールの syslog とアラートを確認します。	434003
2066	NP_FLOW_SNORT_FLOW_DROP フローが SNORT によって終了しました。 Snort モジュールによって要求されたフローが終了します。 **推奨事項**： フローを拒否するルールについては、Snort ポリシーを確認してください。	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2067	NP_FLOW_IDS_REQUEST フローは IPS によって終了しました。 IPS モジュールによって要求されたフローが終了します。 **推奨事項**： IPS モジュールの syslog とアラートを確認します。	420002
2068	NP_FLOW_IDS_FAIL_CLOSE IPS がフェールクローズしました。 IPS モジュールがダウンし、IPS 検査でフェールクローズオプションが使用されるとフローが終了します。 **推奨事項**： IPS モジュールを確認して起動します。	420001
2069	NP_FLOW_IDS_LICENSE_FAIL_CLOSE IPS モジュールライセンスが無効になっています。 IPS モジュールライセンスが無効になっていて、IPS 検査でフェールクローズオプションが使用されるとフローが終了します。 **推奨事項**： IPSモジュールライセンスが有効になっているアクティベーションキーを適用してください。	420008
2070	NP_FLOW_REINJECT_PUNT 放棄アクションによってフローが終了しました。 このカウンタは、検査や AAA などの拡張サービスの 1 つで処理するためにパケットが例外パスに破棄され、フローを流れるトラフィックの違反を検出したサービスルーチンが、フローをドロップするよう要求した場合に増分されます。フローはすぐにドロップされます。 **推奨事項**： 詳細については、サービスルーチンによって発行された syslog に注意してください。フロードロップにより、対応する接続が終了します。	なし
2071	NP_FLOW_SHUNNED フローが排除されました。 排除データベース内にあるホストと一致する送信元 IP アドレスを持つパケットを受信した場合、このカウンタが増分します。**shun** コマンドが適用されると、**shun** コマンドに一致する既存のフローごとに増分されます。 **推奨事項**：なし	401004

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2072	NP_FLOW_HOSTLIMIT フローホストが制限されています。 **推奨事項**：なし	なし。
2073	NP_FLOW_NAT_FAILED NAT が失敗しました。 IP またはトランスポートヘッダーを変換するための xlate の作成に失敗しました。 **推奨事項**： NAT が必要ない場合は、NAT コマンドを無効にします。それ以外の場合は、ドロップされたフローの NAT ルールを設定します。	305005、305006、305009、305010、305011、305012
2074	NP_FLOW_NAT_RPF_FAILED NAT リバースパスが失敗しました。 変換されたホストの実際のアドレスを使用して、変換されたホストに接続しようとして拒否されました。 **推奨事項**： NAT 経由のホストと同じインターフェイス上にない場合は、実際のアドレスの代わりにマップされたアドレスを使用してホストに接続します。また、アプリケーションに IP アドレスが埋め込まれている場合は、適切な inspect コマンドを有効にします。	305005
2075	NP_FLOW_INSPECT_FAIL 検査が失敗しました。 このカウンタは、アプライアンスが、接続に対して NP によって実行されるプロトコル検査を有効にできない場合に増加します。これは、メモリ割り当ての失敗が原因であるか、または ICMP エラーメッセージの場合、アプライアンスが、ICMP エラーメッセージに埋め込まれたフレームに関連する確立された接続を検出できないことが原因である可能性があります。 **推奨事項**： システムのメモリ使用量を確認してください。ICMP エラーメッセージの場合、原因が攻撃である場合は、ACL を使用してホストを拒否できます。	313004

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2076	NP_FLOW_NO_INSPECT 検査の割り当てに失敗しました。 このカウンタは、セキュリティアプライアンスが、接続の作成時にランタイム検査のデータ構造を割り当てることができない場合に増加します。接続が切断されます。 **推奨事項**： このエラー状態は、セキュリティアプライアンスのシステムメモリが不足した場合に発生します。**show memory** コマンドを発行して、使用可能な空きメモリをチェックします。	なし
2077	NP_FLOW_RESET_BY_IDS IPS によりフローがリセットされました。 IPS モジュールによって要求された TCP フローが終了します。 **推奨事項**： IPS モジュールの syslog とアラートを確認します。	420003
2078	NP_FLOW_RECLAIMED 非 tcp/udp フローが新しい要求に対して再利用されました。 このカウンタは、新しいフロー用のスペースを確保するために再利用可能なフローが削除されると増分されます。これは、アプライアンスを通過するフローの数が、ソフトウェアによって課された制限により許可されている最大数と等しく、新しいフロー要求が受信された場合にのみ発生します。これが発生した場合、再利用可能なフローの数がアプライアンスで許可されている VPN トンネルの数を超えると、最も古い再利用可能なフローが削除され、新しいフロー用のスペースが確保されます。以下を除くすべてのフローは、再利用可能と見なされます。 • TCP、UDP、GRE およびフェールオーバーフロー • ICMP フロー（ICMP ステートフル検査がイネーブルの場合） • アプライアンスへの ESP フロー **推奨事項**： このカウンタがゆっくりと増加している場合は、アクションは不要です。このカウンタが急速に増加している場合は、アプライアンスが攻撃を受けており、アプライアンスがフローの再利用と再構築により多くの時間を費やしていることを意味している可能性があります。	302021

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2079	NP_FLOW_NON_TCP_SYN TCP が非同期です。 最初のパケットが SYN パケットではない場合に TCP フローが終了します。 **推奨事項**：なし	なし
2080	NP_FLOW_RM_XLATE_LIMIT RMxlate の制限に達しました。 このカウンタは、コンテキストまたはシステムの xlate の最大数に達して、新しい接続が試行されると増分されます。 **推奨事項**： コマンド **show resource usage** および **show resource usage system** を使用して、コンテキストおよびシステムリソースの制限と拒否されたカウントを表示し、必要に応じてリソース制限を調整します。	321001
2081	NP_FLOW_RM_HOST_LIMIT RM ホストの制限に達しました。 このカウンタは、コンテキストまたはシステムのホストの最大数に達し、新しい接続が試行されると増分されます。 **推奨事項**： コマンド **show resource usage** および **show resource usage system** を使用して、コンテキストおよびシステムリソースの制限と拒否されたカウントを表示し、必要に応じてリソース制限を調整します。	321001
2082	NP_FLOW_RM_INSPECT_RATE_LIMIT RM インスペクションレート制限に達しました。 このカウンタは、コンテキストまたはシステムの最大検査レートに到達し、新しい接続が試行されると増分されます。 **推奨事項**： コマンド **show resource usage** および **show resource usage system** を使用して、コンテキストおよびシステムリソースの制限と拒否されたカウントを表示し、必要に応じてリソース制限を調整します。	321002

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2083	NP_FLOW_TCPMOD_CONNECT_CLASHED クライアントとサーバー間での TCP モジュールポートのコリジョンです。 セルフソース TCP 接続は、既存のリスニングサーバーのポートと競合するポートを使用します。 **推奨事項**： ゼロ以外の場合、このカウンタはシステム整合性チェックが失敗したことを示します。TAC にお問い合わせください。	なし
2084	NP_FLOW_SSM_APP_REQUEST フローはサービスモジュールによって終了しました。 このカウンタは、ASA5500 シリーズ適応型セキュリティアプライアンスにのみ適用されます。SSM で実行されているアプリケーションがセキュリティアプライアンスに接続の終了を要求すると、増分されます。 **推奨事項**： SSM 自体によって生成されたインシデントレポートまたはシステムメッセージを照会することにより、より多くの情報を取得できます。手順については、SSM に付属のドキュメントを参照してください。	なし
2085	NP_FLOW_SSM_APP_FAIL サービスモジュールに障害が発生しました。 このカウンタは、ASA5500 シリーズ適応型セキュリティアプライアンスにのみ適用されます。SSM に障害が発生したために、SSM によって検査されている接続が終了すると増分されます。 **推奨事項**： セキュリティアプライアンスのコントロールプレーンで実行されているカードマネージャプロセスは、システムメッセージと CLI 警告を発行して障害を通知しました。SSM の障害をトラブルシューティングするには、SSM に付属のドキュメントを参照してください。	421001
2086	NP_FLOW_SSM_APP_INCOMPETENT サービスモジュールが機能していません。 このカウンタは、ASA5500 シリーズ適応型セキュリティアプライアンスにのみ適用されます。接続が SSM によって検査されることになっているときに増分されますが、SSM はそれを検査できません。このカウンタは今後使用するために予約されています。常に 0 である必要があります。 **推奨事項**：なし	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2087	NP_FLOW_SSL_BAD_RECORD SSL 不良レコードが検出されました。 このカウンタは、リモートピアから受信した不明な SSL レコードタイプごとに増分されます。ピアから受信した不明なレコードタイプは致命的なエラーとして扱われ、このエラーが発生した SSL 接続を終了する必要があります。 **推奨事項**： このカウンタの増分がいつでも見られるのは正常ではありません。このカウンタが増加する場合は、通常、SSL プロトコルの状態がクライアントソフトウェアと同期していないことを意味します。この問題の最も可能性の高い原因は、クライアントソフトウェアのソフトウェアの欠陥にあります。この問題のトラブルシューティングを行うには、クライアントソフトウェアまたは Web ブラウザバージョンを使用して Cisco TAC に連絡し、SSL データ交換のネットワークトレースを提供してください。	なし
2088	NP_FLOW_SSL_HANDSHAKE_FAILED SSL のハンドシェイクに失敗しました。 このカウンタは、SSL ハンドシェイクが失敗したために TCP 接続が切断されたときに増分されます。 **推奨事項**： これは、SSL ハンドシェイクが失敗したために TCP 接続が切断されたことを示しています。ハンドシェイク障害状態によって生成された syslog 情報に基づいて問題を解決できない場合は、Cisco TAC に連絡するときに関連する syslog 情報を含めてください。	725006、725014
2089	NP_FLOW_DTLS_HELLO_CLOSE DTLS hello が終了しました。 このカウンタは、DTLS クライアントの hello メッセージ処理が終了した後に UDP 接続がドロップされると増分されます。これはエラーを示すものではありません。 **推奨事項**：なし	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2090	NP_FLOW_SSL_MALLOC_ERROR SSL malloc エラーです。 このカウンタは、SSL ライブラリで発生する malloc 障害ごとに増分されます。これは、SSL がメモリバッファまたはパケットブロックを割り当てることができないメモリ不足状態に遭遇したことを示します。 **推奨事項**： セキュリティアプライアンスのメモリとパケットブロックの状態を確認し、Cisco TAC に連絡してください。	なし
2091	NP_FLOW_DROP_SEND_CTM_ERROR CTM 暗号要求エラーです。 このカウンタは、CTM が暗号化要求を受け入れることができないたびに増分されます。これは通常、暗号ハードウェア要求キューがいっぱいであることを意味します。 **推奨事項**： **show crypto protocol statistics ssl** コマンドを発行し、Cisco TAC に連絡してください。	なし
2092	NP_FLOW_DROP_SSL_DECRYPT_ERROR SSL レコードの復号に失敗しました。 このカウンタは、SSL データの受信中に復号エラーが発生した場合に増分されます。これは通常、ASA またはピアの SSL コードにバグがあるか、攻撃者がデータストリームを変更している可能性があることを意味します。SSL 接続が終了しました。 **推奨事項**： ASA との間の SSL データストリームを調査します。攻撃者がいない場合、これは Cisco TAC に報告する必要のあるソフトウェアエラーを示しています。	なし
2093	NP_FLOW_SOCKET_NOT_ACCEPTED 新しいソケット接続は受け入れられませんでした。 このカウンタは、セキュリティアプライアンスによって受け入れられない新しいソケット接続ごとに増分されます。 **推奨事項**： 通常の操作の一部として、このカウンタの増分を確認することができます。ただし、カウンタが急速に増加し、ソケットベースのアプリケーションに大きな誤動作がある場合は、ソフトウェアの欠陥が原因である可能性があります。問題をさらに調査するには、Cisco TAC に連絡してください。	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2094	NP_FLOW_SOCKET_FAILURE NP ソケット障害です。 これは、重大なソケット処理エラーの一般的なカウンタです。 **推奨事項**： これは、ソフトウェアエラーを Cisco TAC に報告する必要があることを示しています。	なし
2095	NP_FLOW_SOCKET_RELAY_FAILURE NP ソケットリレー障害です。 これは、ソケットリレー処理エラーの一般的なカウンタです。 **推奨事項**： 通常の操作の一部として、このカウンタの増分を確認することができます。ただし、カウンタが急速に増加し、ソケットベースのアプリケーションに大きな誤動作がある場合は、ソフトウェアの欠陥が原因である可能性があります。問題をさらに調査するには、Cisco TAC に連絡してください。	なし
2096	NP_FLOW_SOCKET_DATA_MOVE_FAILED NP ソケットデータ移動が失敗しました。 このカウンタは、ソケットデータ移動エラーのために増分されます。 **推奨事項**： これは、ソフトウェアエラーを Cisco TAC に報告する必要があることを示しています。	なし
2097	NP_FLOW_SOCKET_NEW_CONN_FAILED NP ソケットの新しい接続におけるエラーです。 このカウンタは、新しいソケット接続の失敗に対して増分されます。 **推奨事項**： これは、ソフトウェアエラーを Cisco TAC に報告する必要があることを示しています。	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2098	NP_FLOW_SOCKET_TRANSP_CLOSED NP ソケットトランスポートが閉じました。 このカウンタは、ソケットに接続されているトランスポートが突然閉じられたときに増分されます。 **推奨事項**： 通常の操作の一部として、このカウンタの増分を確認することができます。ただし、カウンタが急速に増加し、ソケットベースのアプリケーションに大きな誤動作がある場合は、ソフトウェアの欠陥が原因である可能性があります。問題をさらに調査するには、Cisco TAC に連絡してください。	なし
2099	NP_FLOW_SOCKET_BLK_CONV_FAILED NP ソケットブロック変換に失敗しました。 このカウンタは、ソケットブロック変換の失敗に対して増分されます。 **推奨事項**： これは、ソフトウェアエラーを Cisco TAC に報告する必要があることを示しています。	なし
2100	NP_FLOW_SSL_ALERT SSL よりクローズアラートが受信されました。 このカウンタは、セキュリティアプライアンスがリモートクライアントからクローズアラートを受信するたびに増分されます。これは、クライアントが接続を切断することを通知したことを示しています。これは通常の切断プロセスの一環です。 **推奨事項**：なし	725007
2101	NP_FLOW_CHILDREN_LIMIT フローごとに子の最大制限が超えました。 1 つの親フローに関連付けられている子フローの数が内部制限の 200 を超えています。 **推奨事項**： このメッセージは、アプリケーションの動作に問題があるか、ファイアウォールメモリを使い果たしようとしていることを示しています。**set connection per-client-max** コマンドを使用して、制限をさらに微調整します。FTP の場合は、さらに **inspect ftp** の **strict** オプションを有効化します。	210005

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2102	NP_FLOW_TRACER_DROP パケットトレーサーのトレースフローがドロップしました。 このカウンタは、トレースが完了すると、解放されたフローに対して、packet-tracer により内部的に使用されます。 **推奨事項**：なし	なし
2103	NP_FLOW_SP_LOOPING_ADDRESS ルーピングアドレスです。 このカウンタは、フロー内の送信元アドレスと宛先アドレスが同じ場合に増分されます。アドレスプライバシーが有効になっている SIP フローは除外されます。これは、これらのフローが同じ送信元アドレスと宛先アドレスを持つのが通常であるためです。 **推奨事項**： このカウンタは、次の 2 つの条件下で増分する可能性があります。1 つは、アプライアンスが送信元アドレスが宛先と等しいパケットを受信した場合です。これは、DoS 攻撃の一種を表しています。2 つ目は、アプライアンスの NAT 設定が送信元アドレスを宛先のアドレスと等しくなるように設定する場合です。syslog メッセージ 106017 を調べて、カウンタが増加する原因となっている IP アドレスを特定し、パケットキャプチャを有効にして、問題のあるパケットをキャプチャし、追加の分析を実行します。	106017
2104	NP_FLOW_FP_DROP_NO_ADJACENCY 有効な隣接関係がありません。 有効な出力隣接情報がない既存のフローのパケットをセキュリティアプライアンスが受信すると、このカウンタが増分します。これは、ネクストホップに到達できなくなった場合、またはルーティングの変更が発生した場合に発生する可能性があります。通常、動的ルーティング環境で発生します。 **推奨事項**：なし	なし
2105	NP_FLOW_MIDPATH_SERVICE_FAILURE NP ミッドパスサービスの障害です。 これは、重大なミッドパスサービスエラーの一般的なカウンタです。 **推奨事項**： これは、ソフトウェアエラーを Cisco TAC に報告する必要があることを示しています。	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2106	NP_FLOW_MIDPATH_CP_EVENT_FAILURE NP ミッドパス CP イベント障害です。 これは、CP に送信できなかった重要な midpath イベントに対するカウンタです。 **推奨事項**： これは、ソフトウェアエラーを Cisco TAC に報告する必要があることを示しています。	なし
2107	NP_FLOW_CONTEXT_REMOVED NP 仮想コンテキストが削除されました。 フローに関連付ける仮想コンテキストが削除された場合、このカウンタが増分します。これは、マルチコア環境で 1 つのコア CPU が仮想コンテキストを破壊中に、もう 1 つのコア CPU がコンテキストにフローを作成しようとした場合に発生する可能性があります。 **推奨事項**：なし	なし
2108	NP_FLOW_FAILOVER_IDLE_TIMEOUT アイドルタイムアウトのため、フローがスタンバイユニットから削除されました。 スタンバイユニットがアクティブユニットから定期的な更新を受信しなくなった場合、フローはアイドル状態であると見なされます。これは、フローが動作しているときに内部で固定されていると想定されます。このカウンタは、フローがスタンバイユニットから削除されると増分されます。 **推奨事項**：なし	なし
2109	NP_FLOW_L4TM_BLACKLIST フローが動的フィルタのブラックリストに一致しました。 フローは、トラフィックをドロップするように設定された脅威レベルのしきい値よりも高い脅威レベルを持つダイナミック フィルタ ブラックリストまたはグレーリストエントリと一致しました。 **推奨事項**： 内部 IP アドレスを使用して、感染したホストを追跡します。感染を取り除くための修復手順を実行します。	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2110	NP_FLOW_ASA_TEARDOWN ASA は、フローを破棄するように要求しました。 ASA は、フローの削除を要求しました。 **推奨事項**：なし	なし
2111	NP_FLOW_PDTS_PUNT_DROP インスペクタにキューに入れられたセグメントの数が制限に達しました。 このフローでは、インスペクタにキューイングされるパケットの数が制限に達しました。したがって、フローを終了します。 **推奨事項**：なし	なし
2112	NP_FLOW_DROP_PDTS_RULE_META_FAILED PDTS ルールメタの割り当てに失敗しました。 このカウンタは、ルールメタの割り当てに失敗すると増分され、フローが終了します。 **推奨事項**：なし	なし
2113	NP_FLOW_TCP_FULL_PROXY_REQD 完全なTCPプロキシが必要ですが、モニター専用モードでは使用できません。 このフローには完全な TCP プロキシが必要ですが、この機能はモニター専用モードでは使用できません。 **推奨事項**：なし	なし
2114	NP_FLOW_ROUTE_CHANGE ルート変更によりフローが終了しました。 システムがより低コスト（より良いメトリック）のルートを追加すると、新しいルートに一致する着信パケットにより、ユーザーが設定したタイムアウト（floating-conn）値の後に、既存の接続が切断されます。後続のパケットは、より適切なメトリックを使用してインターフェイスから接続を再構築します。 **推奨事項**： 低コストのルートの追加がアクティブフローに影響を与えるのを防ぐために、floating-conn 設定のタイムアウト値を 0:0:0 に設定できます。	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2115	NP_FLOW_SVC_SELECTOR_MISMATCH SVC VPN 内部ポリシーセレクタの不一致が検出されました。 このカウンタは、トンネルのポリシーと一致しない内部 IP ヘッダーを持つ SVC パケットが受信されたときに増分されます。 **推奨事項**：なし	なし
2116	NP_FLOW_VPATH_LICENSE_FAILURE vPath ライセンスの失敗により、フローが終了しました。 ASA 1000V のライセンス障害が原因で、フローがドロップされます。 **推奨事項**： Nexus 1000V をチェックし、使用中のすべての ASA1000V 仮想マシンをサポートするのに十分な ASA1000V ライセンスがインストールされていることを確認します。	4450002
2117	NP_FLOW_SVC_CONN_TIMER_CB_FAIL SVC 接続タイマーのコールバック障害です。 この状態は、その接続の非同期ロックキューにイベントを配置する試みが失敗した場合に発生します。 **推奨事項**：なし	なし
2118	NP_FLOW_SVC_UDP_CONN_TIMER_CB_FAIL SVC UDP 接続タイマーのコールバック障害です。 この状態は、その接続の非同期ロックキューにイベントを配置する試みが失敗した場合に発生します。 **推奨事項**：なし	なし
2119	NP_FLOW_NAT64_OR_NAT46_CONVERSION_FAIL IPv6 から IPv4 への変換またはその逆の変換が失敗しました。 この状態は、IPv6 トラフィックから IPv4 への変換、またはその逆の変換に失敗した場合に発生します。 **推奨事項**：なし	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2120	NP_FLOW_CLUSTER_CFLOW_CLU_OWNER_CLOSED CLU を使用したクラスタフローは所有者で終了します。 ディレクタ/バックアップユニットは、所有者ユニットからクラスタフローclu削除メッセージを受信し、フローを終了しました。 このカウンタは、所有者ユニットで破棄される複製された CLU ごとに増分する必要があります。 **推奨事項**：なし	なし
2121	NP_FLOW_CLUSTER_CFLOW_STALE_CLU_CLOSED 所有者が古くなったため、CLUを使用したクラスタフローが削除されました。 所有者情報が古いため、クラスタフローが削除されました。通常、これは信頼できるメッセージではないため、CLU_DELETEが欠落しているために古い情報が発生する可能性があります。 **推奨事項**：なし	なし
2122	NP_FLOW_CLUSTER_CFLOW_CLU_TIMEOUT CLU を使用したクラスタフローがアイドルタイムアウトのため削除されました。 ディレクター/バックアップユニットが所有者から定期的な更新を受信しなくなった場合、CLUを使用したクラスタフローはアイドル状態と見なされます。これは、フローが稼働しているときに一定の間隔で発生するはずです。 **推奨事項**：なし	なし
2123	NP_FLOW_CLUSTER_REDIRECT フローがクラスタリダイレクト分類ルールに一致しました。 その後、スタブ転送フローは、フローを所有するクラスタユニットにパケットを転送します。 このカウンタは情報提供であり、動作は予想されます。パケットは、クラスタ制御リンクを介して所有者に転送されました。 **推奨事項**：なし	なし
2124	NP_FLOW_CLUSTER_DROP_ON_SLAVE フローは、クラスタのドロップオンスレーブ分類ルールと一致しました。 これは、レベル3サブネットからのパケットがすべてのユニットに表示され、マスターユニットのみがそれらを処理する必要がある場合です。 このカウンタは情報提供であり、予想される動作です。 **推奨事項**：なし	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2125	NP_FLOW_CLUSTER_DIR_CHANGE クラスタ参加イベントによりフローダイレクタが変更されました。 新しいユニットがクラスタに加わり、現在はフローのディレクタになっています。古いダイレクタ/バックアップはそのフローを削除し、フローの所有者は新しいダイレクタを更新します。 このカウンタは情報提供であり、予想される動作です。 **推奨事項**：なし	なし
2126	NP_FLOW_CLUSTER_MCAST_OWNER_CHANGE 古いダイレクタ/バックアップはそのフローを削除し、フローの所有者は新しいダイレクタを更新します。 フローは、新しい所有者ユニットで作成されます。このカウンタは情報提供であり、予想される動作です。 **推奨事項**：なし	なし
2127	NP_FLOW_CLUSTER_CONVERT_TO_DIR_OR_BAK 転送またはリダイレクトフローは、ダイレクタまたはバックアップフローに変換されます。 転送またはリダイレクトフローが削除され、ディレクタまたはバックアップフローを作成できるようになります。このカウンタは情報提供であり、予想される動作です。 **推奨事項**：なし	なし
2128	NP_FLOW_CLUSTER_MOBILITY_OWNER_REMOVED フローモビリティにより古い所有者が削除されました。 フローモビリティにより、このフローは別のユニットに移動しました。古い所有者は削除されます。このカウンタは情報提供であり、予想される動作です。 **推奨事項**：なし	なし
2129	NP_FLOW_CLUSTER_MOBILITY_FWDER_REMOVED フローモビリティでは、古いフォワーダが削除されています。 フローモビリティにより、このフローは別のユニットに移動しました。この古いフォワーダはバックアップになるため、削除されます。このカウンタは情報提供であり、動作は予想されます。 **推奨事項**：なし	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2130	NP_FLOW_CLUSTER_MOBILITY_BACKUP_REMOVED フローモビリティのバックアップが削除されました。 フローモビリティにより、このフローは別のユニットに移動しました。新しい所有者とディレクターが異なるノードにいるため、このバックアップは削除されます。このカウンタは情報提供であり、動作は予想されます。 **推奨事項**：なし	なし
2131	NP_FLOW_CLUSTER_MOBILITY_OWNER_2_DIR フローモビリティでは、古い所有者/ディレクターがディレクターのみに変更されました。 フローモビリティにより、このフローは別のユニットに移動しました。このユニットは、以前は所有者とディレクタの両方でしたが、現在はディレクタフローのみをホストします。このカウンタは情報提供であり、動作は予想されます。 **推奨事項**：なし	なし
2132	NP_FLOW_SCANSAFE_SERVER_NOT_REACHABLE Scansafe サーバーが構成されていないか、クラウドがダウンしています。 scansafe サーバーの IP が scansafe\ 一般オプションで指定されていないか、scansafe サーバーに到達できません。 **推奨事項**：クラウド Web セキュリティはサポートされなくなりました。	なし
2133	NP_FLOW_REMOVED_BY_CLU_ADD_FORCE 別の所有者によりフローが上書きされ、後でディレクタフローが作成されます。 別のユニットがフローを所有しており、後でその場所にディレクタフローを作成するために、フローを削除するように要求されます。このカウンタは情報提供であり、動作は予想されます。 **推奨事項**：なし	なし
2134	NP_FLOW_REMOVED_BY_CLU_FWD_FORCE 別の所有者により上書きされ、後にフォワーダになります。 別のユニットがフローを所有しており、後でその場所に転送フローを作成するために、フローを削除するように要求されます。このカウンタは情報提供であり、動作は予想されます。 **推奨事項**：なし	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2135	NP_FLOW_REMOVED_DIRECTOR_CLOSED フローが削除され、ディレクタが閉じられます。 **推奨事項**：なし	なし
2136	NP_FLOW_PINHOLE_MASTER_CHANGE マスターの変更により、バルク同期時にマスターのみのピンホールフローが削除されました。 このカウンタは情報提供であり、動作は予想されます。 **推奨事項**：なし	302014
2137	NP_FLOW_PARENT_OWNER_LEFT 親フローがなくなったため、一括同期時にフローが削除されました。 親フローの所有者がクラスタを離れたため、一括同期中にフローが削除されます。このカウンタは情報提供であり、動作は予想されます。 **推奨事項**：なし	302014
2138	NP_FLOW_CLUSTER_CTP_PUNT_CHANNEL_MISSING CTP パントチャネルが欠落しているため、一括同期時にフローが削除されました。 クラスタで復元されたフローに CTP パントチャネルがないため、バルク同期中にフローが削除されます。 **推奨事項**： クラスタマスターがクラスタを離れたばかりである可能性があります。また、クラスタ制御リンクでパケットドロップが発生する可能性があります。	302014
2139	NP_FLOW_DROP_INVALID_VNID VXLAN セグメント ID が無効です。 このカウンタは、セキュリティアプライアンスがフローに付加された無効な VXLAN セグメント ID を検出すると増分されます。 **推奨事項**：なし	なし
2140	NP_FLOW_DROP_NO_VALID_NVE_IFC 有効な NVE インターフェイスがありません。 このカウンタは、セキュリティアプライアンスがフローの VNI インターフェイスの NVE インターフェイスを識別できない場合に増分されます。 **推奨事項**： NVE がすべてのインターフェイスに設定されていることを確認します。	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2141	NP_FLOW_DROP_INVALID_PEER_NVE ピア NVE が無効です。 このカウンタは、セキュリティアプライアンスがフローのピア NVE の IP アドレスと MAC アドレスを取得できなかった場合に増分されます。 **推奨事項**： ピア NVE が NVE 用に構成または学習されていることを確認します。	なし
2142	NP_FLOW_DROP_VXLAN_ENCAP_ERROR VXLAN でカプセル化できません。 このカウンタは、セキュリティアプライアンスがフローの VXLAN でパケットをカプセル化できなかった場合に増分されます。 **推奨事項**：なし	なし
2143	NP_FLOW_DROP_NO_ROUTE_TO_PEER_NVE ピア NVE へのルートはありません。 このカウンタは、セキュリティアプライアンスがピア NVE へのネクストホップを見つけられなかった場合に増分されます。 **推奨事項**： ピア NVE が送信元インターフェイスを介して到達可能であることを確認します。	なし
2144	NP_FLOW_DROP_INVALID_VNI_MCAST_IP VNI インターフェイスのマルチキャスト IP が無効です。 このカウンタは、セキュリティアプライアンスが VNI インターフェイスからマルチキャストグループ IP を取得できなかった場合に増分されます。 **推奨事項**： 設定されたピア NVE がない場合、VNI インターフェイスに有効なマルチキャストグループ IP が設定されていることを確認します。	なし
2145	NP_FLOW_DROP_MISSING_PEER_VTEP_IP ピア VTEP IP が見つかりません。 このカウンタは、セキュリティアプライアンスが VXLAN カプセル化の内部宛先 IP のピア VTEP IP を見つけられなかった場合に増分されます。 **推奨事項**： **show arp vtep-mapping**、**show mac-address-table vtep-mapping**、**show ipv6 neighbor vtep-mapping** 出力で、目的のリモート内部ホストに VTEP IP が存在することを確認します。	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2146	NP_FLOW_IFC_ZN_CHG インターフェイスでゾーンが変更されました。 親インターフェイスがゾーンに参加またはゾーンから離脱したためにフローが終了します。 **推奨事項**：なし	302014、302016、302018、302021、302304
2147	NP_FLOW_DROP_PDTS_SNORT_INFO_MISSING Snort は、pdts snort 情報が欠落しているフローを検査しました。 接続に Snort 関連の構造がないためにフローが終了します。 **推奨事項**：なし	なし
2148	NP_FLOW_IFC_VRF_CHG インターフェイスで VRF が変更されました。 親インターフェイスの VRF から別の VRF に移動したためにフローが終了します。 **推奨事項**：なし	なし
2149	NP_FLOW_CLEAN_FOR_VPN_STUB 新しい VPN スタブを作成するためにクリーンアップします。 新しい VPN スタブ接続の準備として競合する接続が破棄されます。 **推奨事項**：なし	なし
2150	NP_FLOW_CLUSTER_CFLOW_ISAKMP_OWNER_CLOSED クラスタフローは ISAKMP 所有者のユニットで終了しました。 ダイレクタ/バックアップユニットは、転送ユニットから ISAKMP リダイレクトパケットを受信し、フローを終了しました。 このカウンタは、ISAKMP 所有者ユニットで ISAKMP リダイレクトパケットによって破棄されたフローごとに増加する必要があります。 **推奨事項**：なし	なし
2151	NP_FLOW_UNABLE_TO_ASSOCIATE_VPN_CONTEXT VPN コンテキストの関連付けが失敗です。 このカウンタは、システムが VPN コンテキストをクラスタフローに関連付けることができない場合に増加します。 **推奨事項**：なし	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2152	NP_FLOW_DROP_IKE_PKT_BAD_SPI SPI が破損または期限切れの IKE パケットのフローが削除されました。 SPI が破損または期限切れになったために、このフローの IKE パケットがドロップされると、このカウンタは増分され、フローはドロップされます。 **推奨事項**： パケットの発信元に関する詳細情報を取得するには、syslog メッセージを確認してください。この状況は正常であり、一時的である場合があります。ドロップが続く場合は、TAC に連絡してさらに調査してください。	753001
2153	NP_FLOW_TEAR_CONN_RETRANSMIT_TIMEOUT 再送信の最大再試行回数を超えました。 TCP パケットが再送信の最大再試行回数を超え、ピアからの応答がなく、接続が切断されたため、接続が切断されました。 **推奨事項**：なし	302014
2154	NP_FLOW_PROBE_TEAR_CONN_MAX_RETRANSMITS 再送信のプローブの最大再試行回数を超えました TCP パケットが再送信の最大プローブ再試行回数を超え、ピアからの応答がなく、接続が切断されたため、接続が切断されました。 **推奨事項**：なし	302014
2155	NP_FLOW_PROBE_TEAR_CONN_RETRANSMIT_TIMEOUT プローブの最大再送時間が経過しました。 TCP パケットの最大プローブ時間が経過し、ピアからの応答がなく、接続が切断されたため、接続が切断されました。 **推奨事項**：なし	302014
2156	NP_FLOW_PROBE_TEAR_CONN_RST プローブは RST を受信しました。 プローブ接続がサーバーから RST を受信し、接続が切断されたため、接続が切断されました。 **推奨事項**：なし	302014

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2157	NP_FLOW_PROBE_TEAR_CONN_FIN プローブは FIN を受信しました。 プローブ接続がサーバーから FIN を受信し、接続が切断されたため、接続が切断されました。 **推奨事項**：なし	302014
2158	NP_FLOW_PROBE_TEAR_CONN_COMPLETE プローブが完了しました。 プローブ接続が成功したため、接続が切断され、接続が切断されました。 **推奨事項**：なし	302014
2159	NP_FLOW_CLU_REMOVED_DUP_OWNER 重複した所有者フローが検出されました。後でディレクタフローが作成されます。 別のユニットによりフローが所有されているため、後でその場所にディレクターフローを作成するため、フローを削除する必要があります。このカウンタは情報提供であり、動作は予想されます。 **推奨事項**：なし	なし
2160	NP_FLOW_CLU_REMOVED_DUP_OWNER_BY_DIR 重複した所有者フローがディレクタによって削除されました。 別のユニットがフローを所有しているため、ディレクタはこのユニットのフローを削除しました。このカウンタは情報提供であり、動作は予想されます。 **推奨事項**：なし	なし
2161	NP_FLOW_CLU_REMOVED_STALE_STUB 古いスタブフローが所有者によって削除されました。 これは古いスタブフローであるため、所有者はこのユニットのフローを削除しました。このカウンタは情報提供であり、動作は予想されます。 **推奨事項**：なし	なし

拡張イベント ID	ENUM 値、説明、および推奨事項	Syslog ID
2162	NP_FLOW_INVALID_MAP_ADDR_PORT MAP アドレス/ポートの組み合わせが無効です。 MAP（アドレスとポートのマッピング）ドメインの基本マッピングルールに一致するアドレスを持つパケットのエンコーディングに一貫性がないか、使用されているポート番号が割り当てられた範囲内にありません。 **推奨事項**： MAP BR と CE の設定をチェックして、同じ MAP ドメイン内で一貫していることを確認します。これは、割り当てられていないポートを悪意を持って使用しようとする不正な MAPCE によっても発生する可能性があることに注意してください。	305019, 305020

イベント時間フィールド

各 NSEL データ レコードには、イベント時間フィールド（NF_F_EVENT_TIME_MSEC）があります。これは、ミリ秒単位でのイベント発生時刻です。NetFlow パケットは、複数のイベントを入れて作成することができます。ただし、NetFlowサービスが複数のイベントの発生を待ってNetFlowパケットを作成するので、パケットの送信時刻がイベント発生時刻と必ずしも一致しません。

（注） フローの寿命の中で、異なるイベントが別々のNetFlowパケットによって発行され、発生順とは逆の順序でコレクタに届くことがあります。たとえば、フローティアダウンイベントが入ったパケットが、フロー作成イベントの入ったパケットより先に到着することもあります。そのため、コレクタアプリケーションが、イベント時間フィールドを使用してイベントの前後関係を判断することが重要です。

データ レコードとテンプレート

テンプレートは、NetFlow経由でエクスポートされたデータ レコードの形式を記述します。各フロー イベントには、それぞれに関連付けられているいくつかのレコード形式またはテンプレートがあります。

- テンプレートは、イベントによって異なります。
- IPv4 フローと IPv6 フローの各イベント タイプには、異なるテンプレートが用意されています。
- IPV44、IPV46、IPV64 および IPV66 フローの各イベント タイプには、異なるテンプレートが用意されています。
- フロー作成イベントには、フローに関連付けられたユーザー名フィールドのサイズに基づいて、さまざまなテンプレートがあります。NetFlow の文字列フィールドのサイズは固定

なので、サイズに応じて異なるテンプレートが必要になります。ほとんどの文字列は、最大文字列よりはるかに短いため、考えられる最大文字列に対応するテンプレートをすべての場合に使用すると、帯域幅が無駄になります。ユーザー名フィールドは、2 つのタイプが定義されているため、各カテゴリに 2 つのタイプのテンプレートが存在します。

– 20 文字未満のユーザー名に対応する一般的なユーザー名サイズ

– ユーザー名は最大 65 文字まで対応します。

– 各テンプレートには、イベントタイプフィールドと拡張イベントタイプフィールドがあります。

- フロー拒否イベントとフロー削除イベントには、IPV46 と IPV64 のテンプレートがあり、宛先 IP アドレスは NAT ルールにより変換されているが、送信元 IP アドレスが NAT ルールにより変換されていないため、送信元と宛先の IP アドレスの IP バージョンが異なります。送信元と宛先の NAT ルールは同時に適用されません（宛先 NAT ルールが最初に適用されます）。このため、両方の NAT ルールが適用される前か、どちらか 1 つの NAT ルールだけが使用可能なときに NetFlow レコードが生成される可能性があります。

  フローを作成するには、送信元と宛先の IP アドレスの IP バージョンが同じである必要があるため、これらの断片的な NAT 変換テンプレートは、フロー作成イベントと遅延フロー作成イベントには必要ではありません。

（注） テンプレート定義は、すべてのコレクタに送信され、データ レコードの解析には、これらの ID と定義を使用する必要があります。

フロー作成イベント用テンプレート

フロー作成イベントは、フローが ASA によって作成されたことを示します。このイベントは、ASA が許可するフローのログでもあります。次の表で、フロー作成イベントに使用するテンプレートについて説明します。

表 *6 :* フロー作成イベント用テンプレート

説明	フィールド
一般的なユーザー名サイズ（20 文字）の IPv44 フロー作成イベント	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、 NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE、NF_F_ICMP_CODE、 NF_F_XLATE_SRC_ADDR_IPV4、 NF_F_XLATE_DST_ADDR_IPV4、 NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、 NF_F_FW_EVENT, NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、 NF_F_FLOW_CREATE_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、 NF_F_USERNAME
最大ユーザー名サイズ（65 文字）の IPv44 フロー作成イベント	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、 NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE、NF_F_ICMP_CODE、 NF_F_XLATE_SRC_ADDR_IPV4、 NF_F_XLATE_DST_ADDR_IPV4、 NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、 NF_F_FW_EVENT, NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、 NF_F_FLOW_CREATE_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、 NF_F_USERNAME_MAX

説明	フィールド
一般的なユーザー名サイズ（20 文字）の IPv66 フロー作成	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、 NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、 NF_F_XLATE_SRC_ADDR_IPV6、 NF_F_XLATE_DST_ADDR_IPV6、 NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、 NF_F_FW_EVENT, NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、 NF_FLOW_CREATE_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、 NF_F_USERNAME
最大ユーザー名サイズ（65 文字）の IPv66 フロー作成	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、 NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、 NF_F_XLATE_SRC_ADDR_IPV6、 NF_F_XLATE_DST_ADDR_IPV6、 NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、 NF_F_FW_EVENT, NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、 NF_FLOW_CREATE_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、 NF_F_USERNAME_MAX

説明	フィールド
一般的なユーザー名サイズ（20 文字）の IPv46 フロー作成イベント	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、 NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE、NF_F_ICMP_CODE、 NF_F_XLATE_SRC_ADDR_IPV6、 NF_F_XLATE_DST_ADDR_IPV6、 NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、 NF_F_FW_EVENT, NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、 NF_F_FLOW_CREATE_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、 NF_F_USERNAME
最大ユーザー名サイズ（65 文字）の IPv46 フロー作成イベント	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、 NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE、NF_F_ICMP_CODE、 NF_F_XLATE_SRC_ADDR_IPV6、 NF_F_XLATE_DST_ADDR_IPV6、 NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、 NF_F_FW_EVENT, NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、 NF_F_FLOW_CREATE_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、 NF_F_USERNAME_MAX

説明	フィールド
一般的なユーザー名サイズ（20 文字）の IPv64 フロー作成	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、 NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、 NF_F_XLATE_SRC_ADDR_IPV4、 NF_F_XLATE_DST_ADDR_IPV4、 NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、 NF_F_FW_EVENT, NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、 NF_FLOW_CREATE_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、 NF_F_USERNAME
最大ユーザー名サイズ（65 文字）の IPv64 フロー作成	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、 NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、 NF_F_XLATE_SRC_ADDR_IPV4、 NF_F_XLATE_DST_ADDR_IPV4、 NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、 NF_F_FW_EVENT, NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、 NF_FLOW_CREATE_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、 NF_F_USERNAME_MAX

フロー作成イベントのための遅延

存続期間が短いフローの場合、NSEL コレクションデバイスは、フロー作成とフローティアダウンを 2 つのイベントとして処理するよりも、単一のイベントとして処理する方が好都合です。そこで、フロー作成イベントの送信を遅らせるための設定可能な CLI パラメータが用意さ

れています。タイマーが切れると、フロー作成イベントが送信されます。しかし、タイマーの期限が切れる前にフローがティアダウンされると、フローティアダウンイベントのみが送信され、フロー作成イベントが送信されません。

フローティアダウンイベントが拡張され、フローに関するすべての情報が入っていれば、情報が失われることはありません。拡張フローティアダウンイベントに対応する新しいテンプレートが導入されています。

拡張フロー ティアダウン イベント用テンプレート

次の表で、拡張フローティアダウンイベントに使用されるテンプレートについて説明します。

表 7: 拡張フロー ティアダウン イベント用テンプレート

説明	フィールド
一般的なユーザー名サイズ（20 文字）の拡張 IPv44 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME

説明	フィールド
最大ユーザー名サイズ（65 文字）の拡張 IPv44 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME_MAX
一般的なユーザー名サイズ（20 文字）の拡張 IPv66 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME

説明	フィールド
最大ユーザー名サイズ（65 文字）の拡張 IPv66 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME_MAX
一般的なユーザー名サイズ（20 文字）の拡張 IPv46 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME

説明	フィールド
最大ユーザー名サイズ（65 文字）の拡張 IPv46 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME_MAX
一般的なユーザー名サイズ（20 文字）の拡張 IPv64 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME

説明	フィールド
最大ユーザー名サイズ（65 文字）の拡張 IPv64 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、 NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE_IPV6、 NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV4、 NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、 NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、 NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、 NF_F_FWD_FLOW_DELTA_BYTES、 NF_F_REV_FLOW_DELTA_BYTES、 NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、 NF_F_EGRESS_ACL_ID、NF_F_USERNAME_MAX

フロー拒否イベント用テンプレート

フロー拒否イベントは、フローが拒否されたことを示します。次の表に、フロー拒否イベントに使用されるテンプレートを示します。

表 *8 :* フロー拒否イベント用テンプレート

説明	フィールド
IPv44 フロー拒否	NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、 NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、 NF_F_XLATE_SRC_ADDR_IPV4、 NF_F_XLATE_DST_ADDR_IPV4、 NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、 NF_F_FW_EVENT, NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、NF_F_INGRESS_ACL_ID、 NF_F_EGRESS_ACL_ID

説明	フィールド
IPv4 フロー拒否（xlate フィールドなし）	NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、 NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、 NF_F_FW_EVENT, NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、NF_F_INGRESS_ACL_ID、 NF_F_EGRESS_ACL_ID
IPv66 フロー拒否	NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、 NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、 NF_F_XLATE_SRC_ADDR_IPV6、 NF_F_XLATE_DST_ADDR_IPV6、 NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、 NF_F_ICMP_CODE_IPV6、NF_F_FW_EVENT、 NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID
IPv6 フロー拒否（xlate フィールドなし）	NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、 NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、 NF_F_ICMP_CODE_IPV6、NF_F_FW_EVENT、 NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID
IPv46 フロー拒否	NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、 NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、 NF_F_XLATE_SRC_ADDR_IPV6、 NF_F_XLATE_DST_ADDR_IPV6、 NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、 NF_F_FW_EVENT, NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、NF_F_INGRESS_ACL_ID、 NF_F_EGRESS_ACL_ID

説明	フィールド
IPv46 フロー拒否（送信元が未変換）	NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT, NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID
IPv64 フロー拒否	NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID
IPv64 フロー拒否（送信元が未変換）	NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID

フロー ティアダウン イベント用テンプレート

フロー ティアダウン イベントは、フローが終了したことを示します。次の表で、フローティアダウンイベントに使用されるテンプレートについて説明します。

表 *9:* フロー ティアダウン イベント用テンプレート

説明	フィールド
IPv44 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、 NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、 NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV4、 NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、 NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、 NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、 NF_F_FWD_FLOW_DELTA_BYTES、 NF_F_REV_FLOW_DELTA_BYTES、 NF_F_FLOW_CREATE_TIME_MSEC
IPv66 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、 NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE_IPV6、 NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV6、 NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、 NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、 NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、 NF_F_FWD_FLOW_DELTA_BYTES、 NF_F_REV_FLOW_DELTA_BYTES、 NF_F_FLOW_CREATE_TIME_MSEC

説明	フィールド
IPv46 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC
IPv46 フロー ティアダウン（送信元が未変換）	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC

説明	フィールド
IPv64 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、 NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE_IPV6、 NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV4、 NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、 NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、 NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、 NF_F_FWD_FLOW_DELTA_BYTES、 NF_F_REV_FLOW_DELTA_BYTES、 NF_F_FLOW_CREATE_TIME_MSEC
IPv64 フロー ティアダウン（送信元が未変換）	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、 NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE_IPV6、 NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV6、 NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、 NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、 NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、 NF_F_FWD_FLOW_DELTA_BYTES、 NF_F_REV_FLOW_DELTA_BYTES、 NF_F_FLOW_CREATE_TIME_MSEC

フローの更新イベント用テンプレート

フロー更新イベントは、フローのフロー更新タイマーが停止したか、フローが切断されたことを示します。このイベントは、フロー トラフィックの定期的バイト カウンタとして機能します。フロー更新イベントは、断片的な NAT 変換のテンプレートを除き、フロー ティアダウン イベントと同じテンプレートを使用します。NF_F_FWD_FLOW_DELTA_BYTES と NF_F_REV_FLOW_DELTA_BYTES フィールドには、最後のタイマー インターバル以降のバイト数が含まれます。NF_F_FW_EXT_EVENT フィールドは未使用であり、フロー更新レコードで無視されます。フローティアダウンイベントに使用されるテンプレートについては、表 8 を参照してください。

フローの更新（タイマー）とフロー更新（ティアダウン）イベント

ASAを通過するフローにはフロー更新タイマーが設定され、タイマーが停止すると、NSELがフロー更新（タイマー）レコードを発行します。設定された時間間隔にフローのアクティビティが存在しない場合、その間隔のフロー更新（タイマー）レコードは送信されません。フロー ティアダウン レコードを伴ったフロー更新（ティアダウン）レコードが送信され、最後の時間間隔のトラフィックが検出されます。最後のインターバルにフローのトラフィックがなかった場合、フロー更新（ティアダウン）レコードは送信されません。また、フローが短期間であった場合（つまり、最初のフロー更新（タイマー）イベントが発生する前にティアダウンが発生した場合）、フロー更新（ティアダウン）レコードは送信されません。

フローの作成時にフロー更新コレクタが設定されていないか、フロー更新イベント中にフロー更新コレクタが削除された場合、フロー更新タイマーは設定されず、再び設定されることもありません。このような状況で、フロー更新（タイマー）イベントやフロー更新（ティアダウン）イベントが再び発生することはありません。

フロー更新レコードとフェールオーバー

フェールオーバーの前後に、フロー更新レコードの一貫性の維持が試行されます。フェールオーバー発生後のすべてのフロー更新レコードは、直前のアクティブな ASA からの最新の更新に基づいています。この更新は 15 秒ごとにトラフィックが流れている限り発生します。フェールオーバーペアの生成に時間差が生じた場合、またはアクティブな ASA が定期更新をスタンバイ ASA に送信する前にフェールオーバーが発生した場合、フロー更新レコードは正確でない場合があります。

フロー更新イベントとクラスタリング

1 つの大きな相違が、フェールオーバーおよびクラスタ処理とフロー更新イベントとの相互作用から生じます。クラスタ処理では、所有権の変更前は、フローディレクタがアクティブなリフレッシュ タイマーの設定されていない元のフローのスタブ フローコピーを所持しています。アクティブなリフレッシュ タイマーが設定された完全なフローのコピーは、元のフローの所有者がダウンした後に生成されます。したがって、元のフロー所有者と新しいフロー所有者の間で、フロー更新タイマーの停止時間に顕著な時間オフセットが発生する可能性が高くなります。

クラスタ内でフロー所有権が変更された後、すべてのフロー更新レコードは、フローディレクタが受信した最新の更新に基づいています。フロー情報はトラフィックがある限り 15 秒ごとに更新されます。最新のフロー情報を維持するための方法は、フェールオーバー用に提供された方法と同じです。

NetFlow とフェールオーバー

NetFlow データ レコードおよびテンプレートは、アクティブ/スタンバイ フェールオーバー ペアのアクティブ（プライマリ）ASA からのみ送信されます。スタンバイ（セカンダリ）ASA は、NetFlow関連の情報を送信しません。ただし、フェールオーバー後、セカンダリASAは、複製または新規のフローに対するテンプレートとNetFlowレコードの送信を開始します。この 2 つの ASA では、各 NetFlow コレクタの接続元 IP アドレスは同じですが、送信元ポートは異

なります。これはNetFlowコレクタがプライマリ装置とセカンダリ装置から送信されるパケットを区別できることを意味します。

アクティブ/アクティブ フェールオーバー ペアでは、両方の ASA が NetFlow データ レコードとテンプレートを同時に送信することがあります。コンテキストごとのアクティブ装置だけがNetFlowパケットを送信し、スタンバイ装置は送信しません。これはアクティブ/スタンバイのシナリオとほぼ同じです。ASAコンテキストとそのコピーでは、NetFlowコレクタの接続元IPアドレスは同一ですが、送信元ポートは異なります。

フェールオーバー ペアの各 ASA ノード（コンテキスト）は、NetFlow コレクタへの独自の接続を確立し、テンプレートを個別にアドバタイズします。コレクタはNetFlowエクスポータを区別するためにパケットの送信元 IP アドレスと送信元ポートを使用します。

NetFlow とクラスタリング

NetFlow は、管理と通常の両方のデータ インターフェイスでサポートされますが、管理インターフェイスを使用することを推奨します。NetFlow コレクタの接続が管理専用インターフェイスで設定されている場合、クラスタ内の各ASAは、NetFlowパケットの送信に独自のユニットごとの送信元IPアドレスと送信元ポートを使用します。NetFlowは、レイヤ2モードおよびレイヤ 3 モードでは両方のデータ インターフェイスで使用される場合があります。レイヤ 2 モードのデータ インターフェイスでは、クラスタ内の各 ASA の送信元 IP アドレスは同一ですが、送信元ポートは異なります。レイヤ2モードではクラスタを1つのデバイスとして認識するように設計されていますが、NetFlow コレクタはクラスタの各ノードを区別できます。レイヤ3モードのデータ インターフェイスでは、NetFlow は管理専用インターフェイスと同じ方法で動作します。

クラスタ内の各ASAノードは、NetFlowコレクタへの独自の接続を確立し、テンプレートを個別にアドバタイズします。コレクタはNetFlowエクスポータを区別するためにパケットの送信元 IP アドレスと送信元ポートを使用します。

CLI による デバイス フィールドのデコード

ASAによって入力された一部のフィールド値をデコードするには、デバイスを直接操作する必要があります。これには、expectスクリプトなどのダイナミック メカニズムを使用し、イベントを発行したデバイスの CLI から必要な情報を取得することを推奨します。

デバイスは、コンソール、Telnet、およびSSHセキュア シェルアクセスをサポートしますが、パフォーマンスとセキュリティの点から、SSH を推奨します。

インターフェイス ID フィールド

インターフェイス ID フィールドは、デバイス インターフェイス MIB から SNMP GET 要求を使用してデコードすることもできます。インターフェイス ID フィールドは、MIB をサポートする唯一のフィールドです。

show interface detail コマンドを使用して、デバイス上のすべてのインターフェイスのリストを取得することもできます。この出力には、NetFlow フィールドに送信されたインターフェイス ID の値に対応する、各インターフェイスの下の行が含まれます。次の例で、インターフェイス番号は 8 です。

```
ciscoasa(config)# show interface filter-outside detail
Interface GigabitEthernet4/3 "filter-outside", is up, line protocol is up
Hardware is i82571EB 4CU rev06, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
MAC address 0015.1715.59c7, MTU 1500
IP address 209.165.200.254, subnet mask 255.255.255.224
532594 packets input, 88376018 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
675393 packets output, 53208679 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (curr/max packets): hardware (36/511) software (0/0)
output queue (curr/max packets): hardware (59/68) software (0/0)
Traffic Statistics for "filter-outside":
532594 packets input, 78636500 bytes
675393 packets output, 40866215 bytes
10837 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 0 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
Control Point Interface States:
Interface number is 8
Interface config status is active
Interface state is active
```

ACL ID フィールド

12 バイトの未加工の ACL ID は、次のように、 3 つの構成部分に分割する必要があります。

- 最初の 4 バイトは、ACL 名 ID
- 次の 4 バイトは、ACL エントリ ID（ACE）/オブジェクト グループ ID
- 最後の 4 バイトは、拡張 ACL エントリ ID

これらの個別の値は、ASA から **show access-list** コマンドを実行した出力によって確認できます。ACL 名 ID は、この出力の ACL の最初の行の末尾にあります。ACE ID は、個別の各 ACL エントリ行の末尾にあります。

（注） アクセス リストでオブジェクト グループを使用している場合、2 番目の 4 バイト ID は実際には ACE ID ではなく、オブジェクトグループ ID です。拡張 ACE ID（最後の 4 バイト部分）は、実際の個別の ACL エントリ ID を表します。次の例では、これらのエントリを示します。

```
ciscoasa(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list foo; 2 elements; name hash: 0x102154c1
access-list foo line 1 extended permit tcp object-group host_grp_1 any eq www 0xd0e5806e
access-list foo line 1 extended permit tcp host 209.165.200.254 any eq www (hitcnt=4)
```

```
0x7e5ad93b
access-list foo line 1 extended permit tcp host 209.165.201.1 any eq www (hitcnt=0)
0xe0c1846b
access-list bar; 1 elements; name hash: 0x5da9bb69
access-list bar line 1 extended deny tcp any any (hitcnt=41) 0x84434b4b
```

この例は、例 2：PAT インターフェイスを持つ、出力時に拒否されたフロー （76 ページ） の例と似ています。拒否されたフローの例では、ACL ID が、次のように各構成部分に分割されています。

- NF_F_INGRESS_ACL_ID: InAcl: 0x102154c1d0e5806e7e5ad93b

  ここで、0x102154c1 が最初の 4 バイト、0xd0e5806e が 2 番目の 4 バイト、0x7e5ad93b が最後の 4 バイトです。

- NF_F_EGRESS_ACL_ID: 0x5da9bb6984434b4b00000000

  ここで、0x5da9bb69 が最初の 4 バイト、0x84434b4b が 2 番目の 4 バイト、0x00000000 が最後の 4 バイトです。

（注） これらの ID はそれぞれ、**show access-list** コマンドの例の各行に対応しています。

これらの ID から、アクセス リスト foo は入力インターフェイスに適用され、アクセス リスト bar は出力インターフェイスに適用されたと推定できます。この情報は、**show run access-group** コマンドによっても入手できますが、ACL ID の方が許可または拒否アクションの原因となった個別の ACE を特定できる点で優れています。（拡張イベント コードから判断して）このフローは出力で拒否されているので、入力 ACL ID が特定する ACE 行はフローを許可し、出力 ACL ID が特定する ACE はフローを拒否することがわかります。

イベントおよび拡張イベントコード

ASA は、高レベルのイベントタイプを 4 種類（作成、ティアダウン、拒否、更新）しか発行しないので、イベントコードをコレクタにハードコードする必要があります。

これら 4 つの高レベルのイベント コードのうち、拡張イベント コードがあるのは、フロー拒否とフロー ティアダウンの 2 つのイベント タイプのみです。フロー拒否およびフローティアダウン拡張イベントコードについては、「拡張イベント ID フィールド （8 ページ）」 で説明します。

NSEL のガイドライン

サポートされる機能

- **class-map**、**match access-list**、および **match any** コマンドで IPv6 がサポートされています。
- UDP ペイロードのみ。

その他のガイドライン

- **flow-export enable** コマンドを使用して flow-export アクションを以前に設定していて、以降のバージョンにアップグレードしている場合、**policy-map** コマンドで説明されているように、設定は自動的に新しいモジュラ ポリシー フレームワーク **flow-export event-type** コマンドに変換されます。
- **flow-export event-type all** コマンドを使用して flow-export アクションを以前に設定していて、以降のバージョンにアップグレードしている場合、NSEL は必要に応じて flow-update レコードの発行を自動的に開始します。
- flow-export アクションはインターフェイス ベースのポリシーではサポートされていません。flow-export アクションは class-map で **match access-list**、**match any**、または **class-default** コマンドだけを使用して設定できます。flow-export アクションはグローバル サービス ポリシーでのみ適用できます。
- NetFlow レコードの帯域幅使用状況を表示するには（リアルタイムには利用できません）、脅威検出機能を使用する必要があります。
- NetFlow コンフィギュレーション全体で IP アドレスとホスト名の割り当てが一意であることを確認してください。
- 実装の詳細については、次の記事を参照してください。
  - https://supportforums.cisco.com/docs/DOC-6113
  - https://supportforums.cisco.com/docs/DOC-6114

NSEL コレクタの設定（CLI）

NSEL を使用するには、少なくとも 1 つのコレクタを設定しておく必要があり、モジュラ ポリシー フレームワークを経由してフィルタを設定するには、NSEL コレクタを設定する必要があります。

NSEL コレクタを設定するには、次の手順を実行します。

手順

ステップ 1 NetFlow パケットの送信先となる NSEL コレクタを追加します。

flow-export destination *interface-name ipv4-address | hostname udp-port*

例：

```
ciscoasa(config)# flow-export destination inside 209.165.200.225 2002
```

destination キーワードは NSEL コレクタが設定されていることを示します。*interface-name* 引数は、コレクタに到達するための ASA および ASA サービス モジュール インターフェイスの名前です。*ipv4-address* 引数は、コレクタ アプリケーションを実行しているマシンの IP アドレスです。*hostname* 引数は、コレクタの宛先 IP アドレスまたは名前です。*udp-port* 引数は NetFlow パケットの送信先である UDP ポート番号です。

最大 5 つのコレクタを設定できます。コレクタを設定すると、すべての設定した NSEL コレクタにテンプレート レコードが自動的に送信されます。

（注） コレクタ アプリケーションが Event Time フィールドを使用してイベントを相互に関連付けていることを確認してください。

ステップ 2 さらに多くのコレクタを設定するには、最初の手順を繰り返します。

モジュラ ポリシー フレームワークを使用した flow-export アクションの設定

モジュラ ポリシー フレームワークを使用して flow-export アクションを設定するには、次の手順を実行します。

手順

ステップ 1 NSELイベントをエクスポートする必要があるトラフィックを識別するクラスマップを定義します。

class-map *flow_export_class*

例：

```
ciscoasa(config-pmap)# class-map flow_export_class
```

flow_export_class 引数は、クラス マップの名前です。

ステップ 2 次のいずれかのオプションを選択します。

- 特定のトラフィックと照合する ACL を設定します。

  match access-list *flow_export_acl*

例：

```
ciscoasa(config-cmap)# match access-list flow_export_acl
```

flow_export_acl 引数は、ACL の名前です。

- 任意のトラフィックと照合します。

match any

例：

```
ciscoasa(config-cmap)# match any
```

ステップ 3 定義されたクラスに対する flow-export アクションを適用するポリシー マップを定義します。

policy-map *flow_export_policy*

例：

```
ciscoasa(config)# policy-map flow_export_policy
```

flow_export_policy 引数は、ポリシー マップの名前です。

ステップ6に従って新しいポリシーマップを作成してグローバルに適用するには、残りのインスペクションポリシーを無効にする必要があります。

または、**policy-map global_policy** コマンドの後に **class flow_export_class** コマンドを入力し、NetFlow クラスを既存のポリシーに挿入します。

モジュラ ポリシー フレームワークの作成または変更については、ファイアウォール コンフィギュレーション ガイドまたは詳細情報を参照してください。

ステップ 4 flow-export アクションを適用するクラスを定義します。

class *flow_export_class*

例：

```
ciscoasa(config-pmap)# class flow_export_class
```

flow_export_class 引数はクラスの名前です。

ステップ 5 flow-export アクションを設定します。

flow-export event-type *event-type* **destination** *flow_export_host1* [*flow_export_host2*]

例：

```
ciscoasa(config-pmap-c)# flow-export event-type all destination 209.165.200.230
```

event_type キーワードはフィルタリングされるサポートされているイベントの名前です。**destination** キーワードは設定されたコレクタの IP アドレスです。flow_export_host 引数は、ホストの IP アドレスです。

ステップ 6 サービス ポリシーをグローバルに追加します。

service-policy *flow_export_policy* **global**

例：

```
ciscoasa(config)# service-policy flow_export_policy global
```

flow_export_policy 引数は、ポリシー マップの名前です。

テンプレート タイムアウト間隔の設定

テンプレート タイムアウト間隔を設定するには、次の手順を実行します。

手順

テンプレート レコードがすべての設定された出力先に送信される間隔を指定します。

flow-export template timeout-rate *minutes*

例：

```
ciscoasa(config)# flow-export template timeout-rate 15
```

template キーワードは、テンプレート固有の設定を示します。**timeout-rate** キーワードは、テンプレートが再送信されるまでの時間を指定します。*minutes* 引数には、テンプレートが再送信されるときの分単位の時間間隔を指定します。デフォルト値は 30 分です。

flow-update イベントをコレクタに送信する時間間隔を変更する

flow-updateイベントをコレクタに送信する時間間隔を変更するには、次の手順を実行します。

手順

アクティブな接続の NetFlow パラメータを設定します。

flow-export active refresh-interval *value*

例：

```
ciscoasa(config)# flow-export active refresh-interval 30
```

value 引数は、flow-update イベント間の間隔を分単位で指定します。有効な値は、1 ～ 60 分です。デフォルト値は 1 分です。

flow-export delay flow-create コマンドを設定した後で、遅延値より 5 秒以上長くはない間隔値を使用して flow-export active refresh-interval コマンドを設定した場合、コンソールに次の警告メッセージが表示されます。

```
WARNING: The current delay flow-create value configuration may cause flow-update events
 to
appear before flow-creation events.
```

flow-export active refresh-interval コマンドを設定した後で、間隔値より 5 秒以上短くはない遅延値を使用して **flow-export delay flow-create** コマンドを設定した場合、コンソールに次の警告メッセージが表示されます。

```
WARNING: The current delay flow-create value configuration may cause flow-update events
 to
appear before flow-creation events.
```

flow-create イベント送信の遅延

flow-create イベントの送信を遅延させるには、次の手順を実行します。

手順

flow-create イベントの送信を指定した秒数遅らせます。

flow-export delay flow-create *seconds*

例：

```
ciscoasa(config)# flow-export delay flow-create 10
```

seconds 引数は、遅延として許可された時間を秒単位で示します。このコマンドが設定されていない場合は、遅延はなく、flow-create イベントはフローが作成された時点でエクスポートされます。設定されている遅延よりも前にフローが切断された場合は、flow-create イベントは送信されません。その代わりに拡張フロー ティアダウン イベントが送信されます。

NetFlow 関連の syslog メッセージのディセーブル化と再イネーブル化

NetFlow 関連の syslog メッセージをディセーブルにしてから再度イネーブルにするには、次の手順を実行します。

手順

ステップ 1 NSEL のために冗長になった syslog メッセージをディセーブルにします。

logging flow-export-syslogs disable

例：

```
ciscoasa(config)# logging flow-export-syslogs disable
```

（注） グローバル コンフィギュレーション モードでこのコマンドを実行しても、設定には保存されません。**no logging message** *xxxxxx* コマンドだけが設定に格納されます。

ステップ 2 個別に syslog メッセージを再イネーブルにします。*xxxxxx* は再イネーブルする指定した syslog メッセージです。

logging message*xxxxxx*

例：

```
ciscoasa(config)# logging message 302013
```

ステップ 3 すべての NSEL イベントを同時に再イネーブルにします。

logging flow-export-syslogs enable

例：

```
ciscoasa(config)# logging flow-export-syslogs enable
```

ランタイム カウンタのリセット

ランタイム カウンタをリセットするには、次の手順を実行します。

手順

NSEL のすべてのランタイム カウンタをゼロにリセットします。

clear flow-export counters

例：

```
ciscoasa# clear flow-export counters
```

NetFlow（ASDM）の有効化

NetFlow を有効化するには、次の手順を実行します。

手順

ステップ 1 **[設定（Configuration）] > [デバイス管理（Device Management）] > [ロギング（Logging）] > [NetFlow]** を選択します。

ステップ 2 テンプレート タイムアウト レートを分単位で入力します。テンプレート タイムアウト レートとは、設定されたすべてのコレクタにテンプレート レコードが送信される時間間隔です。デフォルト値は 30 分です。

ステップ 3 フロー更新間隔を入力します。これは、フロー更新イベント間の時間間隔を分単位に指定するものです。有効な値は、1 ～ 60 分です。デフォルト値は 1 分です。

ステップ 4 flow-creation イベントのエクスポートを遅延させ、flow-teardown イベントを flow-creation イベントとは別に単独で処理する場合は、[短時間フローのフロー作成イベントの遅延エクスポート（Delay export of flow creation events for short-lived flows）] チェックボックスをオンにし、遅延の秒数を [遅延（Delay By）] フィールドに入力します。

ステップ 5 NetFlow パケットの送信先となるコレクタを指定します。最大 5 つのコレクタを設定できます。コレクタを設定するには、[Add] をクリックして [Add NetFlow Collector] ダイアログボックスを表示し、次の手順を実行します。

a) NetFlow パケットの送信先となるインターフェイスを、ドロップダウン リストから選択します。

b) IP アドレスまたはホスト名、および UDP ポート番号を、それぞれ該当するフィールドに入力します。

c) [OK] をクリックします。

これらの手順を繰り返して、追加のコレクタを作成します。

ステップ 6 NetFlow がイネーブルになっている場合、一部の syslog メッセージに重複が生じます。これは、同一の情報が NetFlow を介してエクスポートされるためです。システムのパフォーマンスを維持するためにも、重複により不要となった syslog メッセージはすべてディセーブルにすることをお勧めします。不要な syslog メッセージをすべてディセーブルにする場合は、[Disable redundant syslog messages] チェックボックスをオンにします。不要な syslog メッセージおよびそのステータスを表示する場合は、[冗長な syslog メッセージの表示（Show Redundant Syslog Messages）] をクリックします。

[Redundant Syslog Messages] ダイアログボックスが表示されます。不要な syslog メッセージの番号が、[Syslog ID] フィールドに表示されます。[Disabled] フィールドには、指定した syslog メッセージがディセーブルになっているかどうかが表示されます。[OK] をクリックして、このダイアログボックスを閉じます。

不要な syslog メッセージを個別にディセーブルにする場合は、**[構成（Configuration）] > [デバイス管理（Device Management）] > [ロギング（Logging）] > [Syslongセットアップ（Syslog Setup）]**を選択します。

ステップ 7 変更を保存するには [Apply] をクリックし、変更を破棄して新しい設定値を入力するには [Reset] をクリックします。

NetFlow イベントと設定済みコレクタとの対応付け

NetFlow イベントを設定済みのコレクタと対応付けるには、次の手順を実行します。

手順

ステップ 1 **[Configuration] > [Firewall] > [Service Policy Rules]** の順に選択します。

ステップ 2 サービス ポリシー ルールを追加するには、次の手順を実行します。

1. [Add] をクリックして、[Add Service Policy Rule Wizard] を表示します。サービスポリシー ルールの詳細については、ファイアウォール コンフィギュレーション ガイドを参照してください。
2. [グローバル：任意のインターフェイスに適用（Global - applies to all interfaces）] オプションボタンをクリックして、ルールをグローバルポリシーに適用します。[Next] をクリックします。
3. [Source and Destination IP Address (uses ACL)] チェックボックスまたは [Any traffic] チェックボックスをトラフィック一致基準としてオンにするか、[Use class-default as traffic class] オプション ボタンをクリックします。[Next] をクリックして、[Rule Actions] 画面に進みます。

（注） NetFlow のアクションは、グローバル サービス ポリシー ルールに対してだけ使用可能で、その適用対象は class-default トラフィック クラス、およびトラフィック照合基準として「Source and Destination IP Address (uses ACL)」または「Any Traffic」が選択されているトラフィック クラスに限定されます。

ステップ 3 [Rule Actions] 画面で、[NetFlow] タブをクリックします。

ステップ 4 フローイベントを設定する場合は、[追加（Add）] をクリックして [フローイベントを追加（Add Flow Event）] ダイアログボックスを表示し、次の手順を実行します。

1. ドロップダウン リストから、フロー イベント タイプを選択します。選択できるイベントは、[created]、[torn down]、[denied]、[updated]、[all] です。

（注） flow-update イベント機能は、バージョン 9.0（1）では使用できません。バージョン 8.4(5) および 9.1(2) 以降で使用できます。

2. [Send] カラムで、イベントの宛先となるコレクタを選択します。コレクタは、対応するチェックボックスをオンにすると選択できます。
3. [Manage] をクリックして、コレクタの追加、編集、または削除や他の NetFlow 設定値（syslog メッセージなど）の設定ができる [Manage NetFlow Collectors] ダイアログボックスを表示します。[OK] をクリックして [Manage NetFlow Collectors] ダイアログボックスを閉じ、[Add Flow Event] ダイアログボックスに戻ります。コレクタの設定の詳細については、NetFlow（ASDM）の有効化のステップ 5 を参照してください。

ステップ 5 [OK] をクリックして [フローイベントを追加（Add Flow Event）] ダイアログボックスを閉じ、[NetFlow] タブに戻ります。

ステップ 6 [Finish] をクリックして、ウィザードを終了します。

ステップ 7 NetFlow サービス ポリシー ルールを編集するには、次の手順を実行します。

1. [Service Policy Rules] テーブルで選択し、[Edit] をクリックします。
2. [Rule Actions] タブをクリックし、さらに [NetFlow] タブをクリックします。

NSEL のモニタリング

syslog メッセージを使用して、エラーのトラブルシューティングやシステムの使用状況とパフォーマンスの監視に役立てることができます。ログバッファに保存されたリアルタイムの syslog メッセージを別のウィンドウで表示できます。これには、メッセージの説明、メッセージの詳細、およびエラーを解決するために必要な場合に実行する推奨アクションが含まれます。詳細については、syslog メッセージと NSEL イベントを参照してください。

次のコマンドを使用して NSEL を監視できます。

手順

	コマンドまたはアクション	目的
ステップ 1	ASDM で、**[ツール（Tools）] > [コマンドライン インターフェイス（Command Line Interface）]** を選択してコマンドを入力します。	• **show flow-export counters** NSEL に対する統計データとエラーデータを含む、ランタイム カウンタを表示します。 • **show logging flow-export-syslogs** NSEL イベントによってキャプチャされたすべての syslog メッセージを表示します。

	コマンドまたはアクション	目的
		• **show running-config flow-export** 現在設定されている NetFlow コマンドを示します。 • **show running-config logging** ディセーブル化された syslog メッセージを表示します。ディセーブル化された syslog メッセージは NetFlow を経由して同じ情報をエクスポートするため、冗長な syslog メッセージです。

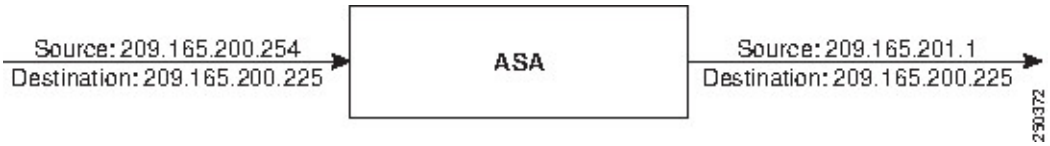
NSEL の例（CLI）

以下の例では、イベントを生成するフローを示し、ASA の新しい NSEL フィールドをサポートするコレクタの実装方法について説明します。

例 1：PAT インターフェイスを持つ許可されたフロー

次の例では、PAT インターフェイスを使用する、許可されたフローを示します。出力インターフェイスの IP アドレスは、209.165.200.225 です。ユーザーは User A として認証されています。ACL は指定されていませんが、フローは発信なので、デフォルトで許可されています。次の図と提供された説明に従って、フロー作成イベントが発行されます。

図 *1 : PAT* インターフェイスを持つ許可されたフローの例



作成された NSEL レコードには、次のフィールドと値が含まれます。

フィールド	値
NF_F_CONN_ID	xxxx
NF_F_SRC_ADDR_IPV4	209.165.200.254
NF_F_SRC_PORT	56789
NF_F_SRC_INTF_ID	1
NF_F_DST_ADDR_IPV4	209.165.200.225
NF_F_DST_PORT	80

フィールド	値
NF_F_DST_INTF_ID	0
NF_F_PROTOCOL	6
NF_F_ICMP_TYPE	0
NF_F_ICMP_CODE	0
NF_F_XLATE_SRC_ADDR_IPV4	209.165.201.1
NF_F_XLATE_DST_ADDR_IPV4	209.165.200.225
NF_F_XLATE_SRC_PORT	1024
NF_F_XLATE_DST_PORT	80
NF_F_FW_EVENT	1
NF_F_FW_EXT_EVENT	0
NF_F_EVENT_TIME_MSEC	YYYYYYYY
NF_F_INGRESS_ACL_ID	0
NF_F_EGRESS_ACL_ID	0
NF_F_USERNAME	User A

例 2：PAT インターフェイスを持つ、出力時に拒否されたフロー

次の例では、PAT インターフェイスを使用し、出力 ACL によって拒否されたフローを示します。出力インターフェイスの IP アドレスは、209.165.200.225 です。ユーザーは User A として認証されています。入力 ACL（foo）はフローを許可しますが、出力 ACL（bar）がフローを拒否します。入力 ACL（foo）は、オブジェクト グループを使用して指定されています。

```
ciscoasa# object-group network host_grp_1
 network-object host 209.165.200.254
 network-object host 209.165.201.1
ciscoasa(config)# access-list foo extended permit tcp
object-group host_grp_1 any eq www
ciscoasa(config)# access-list bar extended deny tcp any any
ciscoasa(config)# access-group foo in interface inside
ciscoasa(config)# access-group bar out interface outside
```

図 1 および記載された説明に従い、フロー拒否イベントが発行されます。

作成された NSEL レコードには、次のフィールドと値が含まれます。

フィールド	値
NF_F_SRC_ADDR_IPV4	209.165.200.254
NF_F_SRC_PORT	37518

フィールド	値
NF_F_SRC_INTF_ID	7
NF_F_DST_ADDR_IPV4	209.165.200.225
NF_F_DST_PORT	80
NF_F_DST_INTF_ID	8
NF_F_PROTOCOL	6
NF_F_ICMP_TYPE	0
NF_F_ICMP_CODE	0
NF_F_XLATE_SRC_ADDR_IPV4	209.165.201.1
NF_F_XLATE_DST_ADDR_IPV4	209.165.200.225
NF_F_XLATE_SRC_PORT	48264
NF_F_XLATE_DST_PORT	80
NF_F_FW_EVENT	3
NF_F_FW_EXT_EVENT	1002（出力 ACL）
NF_F_EVENT_TIME_MSEC	1187374131808
NF_F_INGRESS_ACL_ID	0x102154c1d0e5806e7e5ad93b
NF_F_EGRESS_ACL_ID	0x5da9bb6984434b4b00000000
NF_F_USERNAME	User A

例 3：NSEL イベントのフィルタリング

次の例では、すでに設定されている指定コレクタを使用してNSELイベントをフィルタリングする方法を示しています。

- **flow-export destination inside 209.165.200.2055**
- **flow-export destination outside 209.165.201.29 2055**
- **flow-export destination outside 209.165.201.27 2055**

ホスト 209.165.200.224 と 209.165.201.224 から 209.165.200.230 までの間のすべてのイベントのログを記録し、209.165.201.29 へのその他のすべてのイベントのログを記録します。

```
ciscoasa(config)# access-list flow_export_acl permit ip
host 209.165.200.224 host 209.165.201.224
ciscoasa(config)# class-map flow_export_class
ciscoasa(config-cmap)# match access-list flow_export_acl
ciscoasa(config)# policy-map flow_export_policy
```

```
ciscoasa(config-pmap)# class flow_export_class
ciscoasa(config-pmap-c)# flow-export event-type all destination 209.165.200.230
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# flow-export event-type all destination 209.165.201.29
ciscoasa(config)# service-policy flow_export_policy global
```

flow-creation イベントを 209.165.200.230 に、flow-teardown イベントを 209.165.201.29 に、flow-denied イベントを 209.165.201.27 に、flow-update イベントを 209.165.200.230 にそれぞれ記録します。

```
ciscoasa(config)# policy-map flow_export_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# flow-export event-type flow-creation destination 209.165.200.230
ciscoasa(config-pmap-c)# flow-export event-type flow-teardown destination 209.165.201.29
ciscoasa(config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
ciscoasa(config-pmap-c)# flow-export event-type flow-update destination 209.165.200.230
ciscoasa(config)# service-policy flow_export_policy global
```

ホスト 209.165.200.224 と 209.165.200.230 から 209.165.201.29 までの間の flow-create イベントのログを記録し、209.165.201.27 へのすべての flow-denied イベントのログを記録します。

```
ciscoasa(config)# access-list flow_export_acl permit ip
host 209.165.200.224 host 209.165.200.230
ciscoasa(config)# class-map flow_export_class
ciscoasa(config)# match access-list flow_export_acl
ciscoasa(config)# policy-map flow_export_policy
ciscoasa(config-pmap)# class flow_export_class
ciscoasa(config-pmap-c)# flow-export event-type flow-creation destination 209.165.200.29
ciscoasa(config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
ciscoasa(config)# service-policy flow_export_policy global
```

（注） flow_export_acl については次のコマンドを入力する必要があります。

```
ciscoasa(config-pmap-c)# flow-export event-type flow-denied
destination 209.165.201.27
```

flow_export_acl の場合は、最初の一致が検出された後トラフィックがチェックされないからです。*flow_export_acl* に一致する flow-denied イベントを記録するには、アクションを明示的に定義する必要があります。

ホスト 209.165.201.27 と 209.165.201.50 から 209.165.201.27 までの間のトラフィックを除くすべてのトラフィックのログを記録します。

```
ciscoasa(config)# access-list flow_export_acl deny ip
host 209.165.201.27 host 209.165.201.50
ciscoasa(config)# access-list flow_export_acl permit ip any any
ciscoasa(config)# class-map flow_export_class
ciscoasa(config-cmap)# match access-list flow_export_acl
ciscoasa(config)# policy-map flow_export_policy
ciscoasa(config-pmap)# class flow_export_class
ciscoasa(config-pmap-c)# flow-export event-type all destination 209.165.201.27
ciscoasa(config)# service-policy flow_export_policy global
```

NSEL の履歴

表 *10 : NSEL* の履歴

機能名	プラットフォームリリース	機能情報
NetFlow	8.1(1)	NetFlow 機能では ASA のロギング機能を拡張し、NetFlow プロトコルを介したフローベースのイベントをロギングします。NetFlow バージョン 9 サービスは、開始から終了までのフローの進行についての情報をエクスポートするために使用されます。NetFlow の実装はフローの有効期間における重要なイベントを示すレコードをエクスポートします。この実装は定期的にフローに関するデータをエクスポートする従来の NetFlow とは異なります。NetFlow モジュールは、ACL によって拒否されたフローについてのレコードもエクスポートします。ASA 5580 を設定すると、NetFlow を使用して flow create、flow teardown、および flow denied（ACL によって拒否されたフローだけがレポートされます）イベントを送信できます。 **clear flow-export counters**、**flow-export enable**、**flow-export destination**、**flow-export template timeout-rate**、**logging flow-export syslogs enable**、**logging flow-export syslogs disable**、**show flow-export counters**、**show logging flow-export-syslogs** コマンドが導入されました。 次の画面が導入されました：[構成（Configuration）] > [デバイス管理（Device Management）] > [ロギング（Logging）] > [NetFlow]。
NetFlow フィルタリング	8.1(2)	トラフィックとイベント タイプに基づいて NetFlow イベントをフィルタリングしてから、さまざまなコレクタにレコードを送信できます。たとえば、すべての flow-create イベントのログを 1 つのコレクタに記録し、flow-denied イベントのログを別のコレクタに記録できます。 **class**、**class-map**、**flow-export event-type destination**、**match access-list**、**policy-map**、**service-policy** コマンドが変更されました。 有効期間が短いフローの場合、NetFlow コレクタは、2 つのイベント（flow create イベントと flow teardown イベント）の代わりに 1 つのイベントを処理できるという利点があります。flow-create イベントを送信する前に遅延を設定できます。タイマーの期限が切れる前にフローが切断された場合は、flow teardown イベントだけが送信されます。teardown イベントには、そのフローに関するすべての情報が含まれ、情報の損失は発生しません。 **flow-export delay flow-create** コマンドが導入されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules]。
NSEL	8.2(1)	NetFlow 機能は、ASA のすべての使用可能なモデルに移植されました。
クラスタ	9.0(1)	NetFlow 機能は、クラスタリングをサポートします。

機能名	プラットフォームリリース	機能情報
NSEL	9.0(1)	新しい NetFlow エラー カウンタ（送信元ポート割り当ての失敗）が追加されました。 **show flow-export counters** コマンドが変更されました。 （注） flow-update イベント機能は、バージョン 9.0(1) では使用できません。
NSEL	9.1(2)	フロー トラフィックの定期的なバイト カウンタを提供するために flow-update イベントが導入されました。flow-update イベントが NetFlow コレクタに送信される時間間隔を変更できます。flow-update レコードを送信するコレクタをフィルタリングできます。 次のコマンドが導入されました。**flow-export active refresh-interval** 次のコマンドが変更されました。**flow-export event-type** 次の画面が変更になりました：[構成（Configuration）] > [ファイアウォール（Firewall）] > [サービスポリシールール（Service Policy Rules）] > [サービスポリシールールの追加ウィザード：ルールアクション（Add Service Policy Rule Wizard - Rule Actions）] > [NetFlow] > [フローイベントの追加（Add Flow Event Configuration）]>[デバイス管理（Device Management）]>[ロギング（Logging）] > [NetFlow]。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。