ロギング ポリシーの設定

Security Manager には、Cisco IOS ルータでロギングを設定するための次のポリシーが用意されています。

[Syslog Logging Setup]：syslog ロギング機能をイネーブルにし、基本的なロギング パラメータを定義します。詳細については、「Syslog ロギングの設定パラメータの定義」を参照してください。

[Syslog Servers]：syslog メッセージの送信先となるリモート サーバを定義します。詳細については、「Syslog サーバの定義」を参照してください。

[NetFlow]：パラメータおよびインターフェイスを指定して、NetFlow ロギングをイネーブルにします。「NetFlow パラメータの定義」を参照してください。

Cisco IOS ルータにおけるロギング

（注）　バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

Security Manager には、Cisco IOS ルータでロギングを設定するための次のポリシーが用意されています。

- [Syslog Logging Setup]：syslog ロギング機能をイネーブルにし、基本的なロギング パラメータを定義します。詳細については、 Syslog ロギングの設定パラメータの定義　（2 ページ）を参照してください。
- [Syslog Servers]：syslog メッセージの送信先となるリモート サーバを定義します。詳細については、 Syslog サーバの定義　（4 ページ）を参照してください。

- [NetFlow]：パラメータおよびインターフェイスを指定して、NetFlow ロギングをイネーブルにします。詳細については、NetFlow パラメータの定義　（7 ページ）を参照してください。

（注）　ロギングがイネーブルになっているすべてのルータにネットワーク タイム プロトコル（NTP）ポリシーを設定することを強く推奨します。NTP 同期によって、syslog メッセージの正確なタイムスタンプが提供されます。正確なタイムスタンプは、複数のデバイス上のログを比較する場合に不可欠です。

Syslog ロギングの設定パラメータの定義

この手順では、ルータ上で syslog ロギングをイネーブルにし、syslog サーバに送信されるメッセージを定義する方法について説明します。また、オプションで次の項目を定義できます。

- このデバイスから送信されるすべての syslog メッセージの送信元インターフェイス。
- ローカル バッファに保存されるメッセージ。
- 各メッセージに追加される送信元識別子。
- 送信できるメッセージ数に対するレート制限。

（注）　ルータから syslog サーバに syslog メッセージを送信するには、syslog サーバの IP アドレスも定義する必要があります。詳細については、Syslog サーバの定義　（4 ページ）を参照してください。

関連項目

- Syslog サーバの定義　（4 ページ）
- ログ メッセージの重大度について　（5 ページ）
- Cisco IOS ルータにおけるロギング　（1 ページ）

ステップ 1　次のいずれかを実行して、ルータの [Syslogロギングのセットアップ（Syslog Logging Setup）] ページにアクセスします。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslogロギング設定（Syslog Logging Setup）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [ロギング（Logging）] > [Syslogロギングのセットアップ（Syslog Logging Setup）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Syslog Logging Setup] ページが表示されます。このページのフィールドの説明については、表 2 : [Syslog Logging Setup] ページ （11 ページ）を参照してください。

ステップ 2 [ロギングを有効化（Enable Logging）] を選択して、syslog ロギング機能を有効にします。このオプションが選択されていない場合、ログ メッセージは作成されません。

ヒント デバイスのデフォルトロギング設定を使用するか、またはデフォルト設定を復元する場合は、単に [ロギングを有効化（Enable Logging）] を選択し、その他のすべてのフィールドが空白であることを確認してから、[保存（Save）] をクリックします。デフォルト設定は、デバイスごとに異なります。詳細については、ご使用のルータのマニュアルを参照してください。

ステップ 3 （任意）[ソースインターフェイス（Source Interface）] フィールドに、インターフェイスまたはインターフェイスロールの名前を入力します。このインターフェイスまたはインターフェイスロールのアドレスが、syslog サーバに送信されるすべてのログメッセージの送信元インターフェイスとして使用されます。あるいは、[選択（Select）]をクリックしてリストからインターフェイスロールを選択するか、または新しいインターフェイスロールを作成します。送信元インターフェイスには IP アドレスが必要です。

このオプションは、syslog サーバが（たとえばファイアウォールが原因で）接続の発生元のアドレスに到達できない場合に役立ちます。このフィールドに値を入力しない場合は、発信インターフェイスのアドレスが使用されます。

ステップ 4 （任意）syslog サーバにログ メッセージを送信するには、次の手順を実行します。

a) [トラップの有効化（Enable Trap）] を選択します。このオプションは、デフォルトで選択されます。
b) [Trap Level] リストから値を選択します。この重大度以上の（つまり、重大度番号が同じまたはより小さい）すべてのメッセージが、syslog サーバに送信されます。これよりも重大度が低いメッセージは無視されます。重大度の詳細については、表 1を参照してください。

ステップ 5 （任意）ログ メッセージをルータ上のバッファにローカルに保存するには、次の手順を実行します。

a) [バッファの有効化（Enable Buffer）] を選択します。このオプションは、デフォルトで選択されます。
b) バッファ サイズ（バイト単位）を入力します。
c) バッファに保存されるメッセージの最も低い重大度を選択します。その重大度以上のすべてのメッセージが、バッファに保存されます。
d) [XML形式を使用（Use XML Format）] を選択して、メッセージを XML 形式で保存します（同じポリシーで通常のバッファと XML バッファの両方を設定できます）。このオプションを選択する場合は、XML バッファのサイズをバイト単位で入力します。

（注） バッファを大きくしすぎて、ルータで他のタスク用のメモリが不足することがないようにしてください。メモリが不足すると、展開が失敗する場合があります。

ステップ 6 （任意）出力メッセージのフラッドを防止するために、レート制限を定義します。

a) [レート制限の有効化（Enable Rate Limit）] を選択します。このオプションは、デフォルトで選択されます。
b) 1 秒ごとに送信できるメッセージの最大数を入力します。
c) レート制限から除外するシビラティ（重大度）を選択します。たとえば、[2]（クリティカル）を選択すると、重大度が 0 ～ 2 であるすべての syslog メッセージが、定義されているレート制限に関係なく syslog サーバに送信されます。

d) コンソール メッセージを除く（および上で特に除外しているシビラティ（重大度）を除く）すべてのsyslogメッセージにレート制限を適用するには、[すべてのメッセージ（All Messages）] を選択します。
e) コンソールメッセージにだけレート制限を適用するには、[コンソールメッセージ（Console Messages）] を選択します。

（注） レート制限をイネーブルにし、かつ、オプションを指定しないと、デフォルト設定（1秒ごとに 10 メッセージ、コンソール メッセージにだけ適用される）が適用されます。

ステップ 7 （任意）送信元識別子を各 syslog メッセージの先頭に追加するには、次の手順を実行します。

a) 送信する送信元 ID のタイプ（ルータの IP アドレス、ルータのホスト名、または指定するテキスト文字列）を選択します。
b) [String] を選択した場合は、表示されるフィールドに任意のテキストを入力します。スペースを使用できます。

送信元識別子は、複数のデバイスの出力を単一の syslog サーバに送信する場合に、syslog メッセージの送信元の識別に役立ちます。

（注） 送信元識別子は、バッファ、コンソール、モニタなど、ローカルの宛先に送信されるメッセージには追加されません。

Syslog サーバの定義

この手順では、ルータがsyslogメッセージを送信するサーバを定義する方法について説明します。syslog サーバを定義する場合、サーバが受信したロギング メッセージをプレーン テキストとして転送するか、XML 形式で転送するかを選択できます。

複数の syslog サーバを定義した場合、ロギング メッセージはこれらすべてのサーバに送信されます。

はじめる前に

- syslog ロギングをイネーブルにし、[Syslog Logging Setup] ページで基本的なロギング パラメータを定義します。詳細については、Syslog ロギングの設定パラメータの定義 （2 ページ）を参照してください。

関連項目

- Syslog ロギングの設定パラメータの定義 （2 ページ）
- ログ メッセージの重大度について （5 ページ）
- Cisco IOS ルータにおけるロギング （1 ページ）

ステップ 1 次のいずれかの手順を実行して、ルータの [Syslogサーバー（Syslog Servers）] ページにアクセスします。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslogサーバー（Syslog Servers）] を選択します。

- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [ロギング（Logging）] > [Syslogサーバー（Syslog Servers）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Syslog Servers] ページが表示されます。このページのフィールドの説明については、表 3 : [Syslog Servers] ページ （14 ページ）を参照してください。

ステップ 2 ルータから syslog メッセージを受信するサーバーを定義するには、テーブルの下にある [追加（Add）] ボタンをクリックして、[Syslogサーバー（Syslog Server）] ダイアログボックスを開きます。このダイアログボックスの詳細については、表 4 : [Syslog Server] ダイアログボックス （15 ページ）を参照してください。

ステップ 3 [IPアドレス（IP Address）] フィールドで、目的の syslog サーバーのアドレスを入力するか、[選択（Select）] をクリックしてリストからネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。詳細については、ポリシー定義中の IP アドレスの指定を参照してください。

ステップ 4 （任意）[XML形式でメッセージを転送（Forward Messages in XML Format）] を選択して、受信した syslog メッセージをプレーンテキストではなく XML 形式で転送します。

ステップ 5 [OK] をクリックして定義を保存し、ダイアログボックスを閉じます。定義した syslog サーバーが、テーブルに表示されます。

（注） syslog サーバーを編集するには、テーブルからサーバーを選択して [編集（Edit）] をクリックします。syslog サーバーを削除するには、そのサーバーを選択し、[削除（Delete）] をクリックします。

ログ メッセージの重大度について

Cisco IOS ルータ上の syslog メッセージは、8 つの重大度に分類されます。各重大度は、番号によって識別され、対応する名前が付けられています。次のテーブルに示すように、この番号が低いほど、重大度は高くなります。

表 *1 : Syslog* メッセージの重大度

レベル番号	重大度の名前	説明
[0]	emergency	システムが使用不可
1	アラート	即時処理が必要
2	critical	クリティカルな状態
3	errors	エラー状態
4	警告	警告状態
5	通知	正常だが注意を要する状態
6	情報	情報メッセージだけ

レベル番号	重大度の名前	説明
7	デバッグ	デバッグ メッセージ

関連項目

- Syslog ロギングの設定パラメータの定義 （2 ページ）
- Syslog サーバの定義 （4 ページ）
- Cisco IOS ルータにおけるロギング （1 ページ）

Cisco IOS ルータにおける NetFlow

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

IP トラフィックの特性を明確化し、IP トラフィックが、どのような方法で、どこを通過するかを把握することが、ネットワークの可用性、パフォーマンス、およびトラブルシューティングにとって重要となります。IP トラフィック フローをモニタリングすることで、正確な容量計画を容易に策定でき、ネットワーク リソースが組織の目標をサポートするために適切に使用されていることを確認できます。

NetFlow は、IOS デバイスで使用できるロギング機能であり、IP トラフィック フロー情報の記録、キャッシュ、および送信をインターフェイス単位で実行します。NetFlow の基本的な出力は、フローレコードです。フローレコードでは、「フロー」が、所定の送信元と宛先（両方とも、ネットワークレイヤの IP アドレスおよびトランスポートレイヤの送信元ポート番号と宛先ポート番号で定義されています）の間の、パケットの単方向ストリームとして定義されています。

IOS デバイス上で、NetFlow は 2 つの主要コンポーネント（IP フロー データを格納する NetFlow キャッシュ、およびデータ レポートのために NetFlow レコードを収集サーバに送信する NetFlow エクスポート メカニズム）で構成されています。このため、NetFlow は、イネーブルである場合、着信トラフィックと発信トラフィックのフローに関する統計情報を記録およびキャッシュし、これらのレコードをデバイスから NetFlow Collector にユーザ データグラム プロトコル（UDP）データグラム形式で定期的に送信します。

NetFlow の成熟に伴い、エクスポート パケットまたはフロー レコード用の複数の異なる形式が作成されました。これらの形式は、一般に NetFlow バージョンと呼ばれています。これらのバージョンは詳細に文書化されています。バージョンには 1、5、7、および 9 が存在します。最も一般的に使用される形式は NetFlow バージョン 5 ですが、バージョン 9 が最新の形式であり、拡張性、セキュリティ、トラフィック分析、およびマルチキャストの点で優れています。

Security Manager では、現在、IOS デバイスでの Traditional NetFlow の使用がサポートされています。Traditional NetFlow では、固定フロー レコードを提供します（バージョン 9 の場合も同

様）。つまり、デバイスでは、フローを生成するとき、フラグと定義済みレコードの特定の組み合わせを使用します。デバイス設定では、エクスポートの宛先、エクスポートインターフェイス、およびバージョン固有の特定の送信オプションを定義します。

トラフィック フローおよび NetFlow の詳細

ルータまたはスイッチを経由する各パケットに対して、IP パケット属性セットが検査されます。これらの属性は、IP パケット ID、つまり「フィンガープリント」であり、パケットが一意であるか、または他のパケットと関連するかを定義します。

送信元/宛先IPアドレス、送信元/宛先ポート、プロトコルインターフェイス、およびサービスクラスが同一であるすべてのパケットは、1 つのフローにグループ化され、これらのパケットおよびバイトが集計されます。このフロー決定の方式（または「フィンガープリント」）では、大量のネットワーク情報を NetFlow キャッシュと呼ばれる NetFlow 情報のデータベースに圧縮できるため、スケーラビリティが高くなります。

一般的に、NetFlowキャッシュにはフローが常に入れられ、ルータまたはスイッチのソフトウェアは、終了したフローや期限切れのフローをキャッシュで検索します。これらのフローはNetFlow Collectorにエクスポートされます（SNMP ポーリングとは異なり、NetFlow エクスポートは、情報を NetFlow コレクタに定期的に送信します）。NetFlow Collector には、エクスポートされたフローを収集および整理して、トラフィックとセキュリティの分析に使用されるリアルタイムレポートまたは履歴レポートを生成するジョブがあります。

NetFlow の概要

NetFlow の処理概要は次のとおりです。

- NetFlowは、IP トラフィック フローをキャプチャするために、ルータまたはスイッチ上で設定されます。
- フロー レコードは、ローカル NetFlow キャッシュに格納されます。
- 定期的に、約 30 ～ 50 のフロー レコードがバンドルされ、NetFlow Collector サーバにエクスポートされます。
- NetFlow Collector ソフトウェアによって、NetFlow データからレポートが作成されます。

関連項目

- Cisco IOS ルータにおけるロギング （1 ページ）
- NetFlow パラメータの定義 （7 ページ）
- NetFlow ポリシー ページ （16 ページ）

NetFlow パラメータの定義

この手順では、ルータ上で NetFlow ロギングをイネーブルにする方法について説明します。

関連項目

- Cisco IOS ルータにおける NetFlow （6 ページ）
- NetFlow ポリシー ページ （16 ページ）
- Cisco IOS ルータにおけるロギング （1 ページ）

ステップ 1 ルータの [NetFlow] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] > [NetFlow] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [ロギング（Logging）] > [NetFlow] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ルータの [NetFlow] ページが表示されます。このページのフィールドの詳細な説明については、 NetFlow ポリシー ページ （16 ページ）を参照してください。

ステップ 2 [NetFlow] ページの [セットアップ（Setup）] タブで、ルータのグローバル NetFlow パラメータを指定します。

- [プライマリ宛先（Primary Destination）]：リストから [IPアドレス（IP Address）] または [ホスト名（Hostname）] を選択して NetFlow 収集を有効にし、プライマリ NetFlow Collector の定義方法を指定します。ブランクのエントリを選択して、このオプションをディセーブルにできます。
  - [IPアドレス（IP Address）]：プライマリ NetFlow Collection Engine をホスティングするデバイスの IP アドレスを入力し、そのフローコレクタがモニターする **UDP ポート**の番号を入力します（ポート番号の範囲は 1 ～ 65535 です）。
  - [ホスト名（Hostname）]：プライマリ NetFlow Collection Engine をホスティングするデバイスの完全修飾ドメイン名を入力し、そのフローコレクタがモニターする **UDP ポート**の番号を入力します（ポート番号の範囲は 1 ～ 65535 です）。
- [重複宛先（Redundant Destination）]：リストから [IPアドレス（IP Address）] または [ホスト名（Hostname）] を選択して、バックアップ NetFlow Collector の定義方法を指定します。ブランクのエントリを選択して、このオプションをディセーブルにできます。
  - [IPアドレス（IP Address）]：セカンダリ NetFlow Collection Engine をホスティングするデバイスの IP アドレスを入力し、そのフローコレクタがモニターする **UDP ポート**の番号を入力します（ポート番号の範囲は 1 ～ 65535 です）。
  - [ホスト名（Hostname）]：セカンダリ NetFlow Collection Engine をホスティングするデバイスの完全修飾ドメイン名を入力し、そのフローコレクタがモニターする **UDP ポート**の番号を入力します（ポート番号の範囲は 1 ～ 65535 です）。

（注） プライマリ宛先および重複宛先を定義した場合、フロー データは両方に送信されます。

- [送信元インタフェース（Source Interface）]：ルータインターフェイスを指定します。このインターフェイスを経由してフローデータがコレクタの宛先に送信されます。

- [バージョン（Version）]：ドロップダウンリストから目的の NetFlow バージョン番号を選択して、フローデータに使用するレコード形式を定義します。ブランクのエントリを選択して、このオプションをディセーブルにできます。
  - [1]：元のレコード形式。追加のパラメータは必要ありません。
  - [5]：ボーダー ゲートウェイ プロトコル（BGP）自律システム（AS）情報およびフローシーケンス番号など、最も広く採用されている形式。

ネットワークに BGP が設定されている場合は、NetFlow レコードに送信元またはピア AS 情報を含めることができます。[ASタイプ（AS Type）] ドロップダウンリストから、[origin-as] または [peer-as] を選択します。ブランクのエントリを選択して、このオプションをディセーブルにできます。

[BGPネクストホップの有効化（Enable BGP Nexthop）] をオンにして、BGP ネクストホップ情報をフローキャッシュに含めます。（バージョン 5 では、この情報はキャッシュに表示されますが、エクスポートはされません）。

- • [9]：テンプレートベースの最新バージョンであり、まだ完全にはサポートされていません。

ネットワークに BGP が設定されている場合は、NetFlow レコードに送信元またはピア AS 情報を含めることができます。[ASタイプ（AS Type）] ドロップダウンリストから、[origin-as] または [peer-as] を選択します。ブランクのエントリを選択して、このオプションをディセーブルにできます。

[BGPネクストホップの有効化（Enable BGP Nexthop）] をオンにして、BGP ネクストホップ情報をフローレコードに含めます。

（注） AS 情報の収集はリソースを大量に消費します。origin-as の場合は特に消費量が多くなります。ピアリングの配置をモニタする必要がない場合は、AS収集をディセーブルにすると、パフォーマンスが向上する場合があります。

ステップ 3 [インタフェース（Interfaces）] タブで、トラフィックフローをレポートするインターフェイスを定義します。

- インターフェイスを追加するには、[Add Row] ボタンをクリックして [Add NetFlow Interface Settings] ダイアログボックスを開きます。このダイアログボックスについては、NetFlow インターフェイス設定の追加および編集 （19 ページ）で説明しています。
- 既存のインターフェイスを編集するには、[Interfaces] テーブルで目的のエントリを選択し、次に [Edit Row] ボタンをクリックして [Edit NetFlow Interface Settings] ダイアログボックス（NetFlow インターフェイス設定の追加および編集 （19 ページ）で説明しています）を開きます。
- 既存のインターフェイスを削除するには、そのエントリを [Interfaces] テーブルで選択してから [Delete Row] ボタンをクリックし、次に、削除されたことを確認します。

（注） NetFlow データ収集は、削除しないで、インターフェイスでディセーブルにできます。詳細については、NetFlow インターフェイス設定の追加および編集 （19 ページ）を参照してください。

Syslog ロギングの設定ポリシーのページ

[Syslog Logging Setup] ページを使用して、syslog ロギングをイネーブルにし、選択した Cisco IOS ルータ上で基本的なロギング パラメータを定義します。

詳細については、Syslog ロギングの設定パラメータの定義 （2 ページ）を参照してください。

（注） 各ログ メッセージに対して正確なタイムスタンプを作成するために、ロギングがイネーブルになっているすべてのルータで NTP ポリシーを定義することを強く推奨します。詳細については、[NTP Policy] ページを参照してください。

（注） ロギングの設定ポリシーを割り当てていない場合、デフォルトのロギング設定が展開時にデバイス上で復元されます。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslogロギング設定（Syslog Logging Setup）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [ロギング（Logging）] > [Syslogロギングのセットアップ（Syslog Logging Setup）] を選択します。[Syslogロギングのセットアップ（Syslog Logging Setup）] を右クリックしてポリシーを作成するか、共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるロギング （1 ページ）
- Syslog サーバ ポリシーのページ （14 ページ）
- Cisco IOS ルータにおける NTP
- インターフェイス ロール オブジェクトについて

フィールド リファレンス

表 2 : *[Syslog Logging Setup]* ページ

要素	説明
Enable Logging	選択すると、syslog ロギングがデバイス上でイネーブルになります。 選択を解除すると、ロギングがデバイス上でディセーブルになります。これがデフォルトです。 **ヒント** デバイスのデフォルトの syslog ロギング設定を使用するには、[ロギングの有効化（Enable Logging）] チェックボックスをオンにし、次に、追加の値を入力せずに [保存（Save）] をクリックします。
送信元インターフェイス（Source Interface）	syslog サーバに送信される、すべての発信ログ メッセージの送信元アドレス。この設定は、syslog サーバが（たとえばファイアウォールが原因で）ログ メッセージの発生元のアドレスに応答できない場合に必要となることがあります。 このフィールドで値を定義しない場合、発信インターフェイスのアドレスが使用されます。 インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
トラップ	syslog サーバに転送されるログ メッセージを定義します。 • [Enable Trap]：選択すると、ログ メッセージが syslog サーバに送信されます。これがデフォルトです。選択を解除すると、ログ メッセージは送信されません。 • [Trap Level]：記録され、syslog サーバに送信されるメッセージの最も低い重大度。この重大度以上のすべてのメッセージが記録されます。重大度は、名前と番号で識別されます。詳細については、表 1 : Syslog メッセージの重大度 （5 ページ）を参照してください。 **ヒント** ルータのデフォルトのトラップ設定を復元するには、[トラップの有効化（Enable Trap）] を選択し、次に [トラップレベル（Trap Level）] リストから空白の設定を選択します。

要素	説明
Logging Buffer	ログ メッセージが、デバイス上のバッファにローカルに保存されるかどうかを指定します。 • [Enable Buffer]：選択すると、ログ メッセージはデバイス上のバッファに保存されます。これがデフォルトです。選択を解除すると、ログ バッファはデバイス上で維持されません。 • [Buffer Size]：バッファのサイズ（バイト単位）。有効値の範囲は 4096 ～ 4294967295 バイト（4 KB ～ 4 GB）です。デフォルトのサイズは、プラットフォームによって異なります。バッファを大きくしすぎて、ルータで他のタスク用のメモリが不足することがないようにしてください。メモリが不足すると、展開が失敗する場合があります。 （注） 一部のデバイスでは最大バッファ サイズがより小さいことがあります。 • [Severity Level]：バッファに保存されるメッセージの最も低い重大度。この重大度以上のすべてのメッセージが保存されます。ほとんどの Cisco IOS ルータにおいて、デフォルトの重大度は 7（[debugging]）です。重大度は、名前と番号で識別されます。詳細については、表 1 : Syslog メッセージの重大度（5 ページ）を参照してください。 • [Use XML Format]：選択すると、ログ メッセージが XML 形式でバッファに保存されます（同じポリシーで通常のバッファと XML バッファの両方を設定できます）。選択を解除すると、XML バッファはデバイス上で維持されません。 • [Buffer Size]：XML バッファのサイズ（バイト単位）。有効値の範囲は 4096 ～ 4294967295 バイト（4 KB ～ 4 GB）です。 （注） 一部のデバイスでは最大バッファ サイズがより小さいことがあります。 ヒント ルータのデフォルトのバッファ設定を復元するには、[トラップの有効化（Enable Trap）] を選択し、バッファサイズ設定を消去し、次に [セキュリティレベル（Security Level）] リストから空白の設定を選択します。

要素	説明
レート制限	syslog サーバに送信されるログ メッセージのレートを制限します。 • [Enable Rate Limit]：選択すると、レート制限がイネーブルになります。選択を解除すると、レート制限がディセーブルになります。 • [Messages per Sec.]：1 秒あたりの送信可能な最大ログ メッセージ数。有効な値の範囲は 1 ～ 10000 です。デフォルトは、1 秒あたり 10 メッセージです。 • [除外（Exclude）]：レート制限から除外するメッセージのタイプ。この設定を適用すると、選択した重大度の、および重大度番号がより低い（つまり、より重大な）メッセージがすべて除外されます。デフォルトは 3（[errors]）です。この場合、重大度が 3、2（[critical]）、1（[alerts]）、または 0（[emergencies]）であるすべてのログ メッセージが、レート制限から除外されます。重大度の詳細については、表 1 : Syslog メッセージの重大度 （5 ページ）を参照してください。 • [All Messages]：選択すると、このレート制限が、コンソール メッセージを除くすべてのメッセージに適用されます。 • [Console Messages]：選択すると、このレート制限が、コンソール メッセージだけに適用されます。 **ヒント** ルータのデフォルトのレート制限設定を復元するには、[レート制限の有効化（Enable Rate Limit）] チェックボックスをオンにして、レート制限値設定を消去します。

Origin ID	デバイスからリモート syslog サーバに送信されるすべての syslog メッセージの先頭に追加される、送信元識別子。送信元識別子は、複数のデバイスから単一の syslog サーバに出力を送信する場合に役立ちます。
	• [ID Type]：各 syslog メッセージに追加される送信元識別子のタイプ。次のオプションがあります。
	  • [IP Address]：送信元デバイスの IP アドレス。
	  • [Hostname]：送信元デバイスのホスト名。
	  • [String]：ユーザ定義のテキスト。
	• [Value]：ID タイプとして [String] を選択した場合にだけ適用されます。ユーザ定義文字列のテキストを入力します。スペースは使用できますが、最初の文字には使用できません。
	（注） 送信元識別子は、バッファ、コンソール、モニタなど、ローカルの宛先に送信されるメッセージには追加されません。

Syslog サーバ ポリシーのページ

[Syslog Servers] ページを使用して、ルータからログ メッセージを収集するサーバを作成、編集、および削除します。

詳細については、Syslog ロギングの設定パラメータの定義 （2 ページ）を参照してください。

（注） このページに定義されている syslog サーバへのロギングをイネーブルにするには、ロギングをイネーブルにし、Syslog ロギングの設定ポリシーのページ （10 ページ）で基本パラメータを定義する必要があります。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslogサーバー（Syslog Servers）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [ロギング（Logging）] > [Syslogサーバー（Syslog Servers）] を選択します。[Syslogサーバー（Syslog Servers）] を右クリックしてポリシーを作成するか、共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるロギング （1 ページ）
- [Syslog Server] ダイアログボックス （15 ページ）
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 *3 : [Syslog Servers]* ページ

要素	説明
IPアドレス	syslog サーバの名前。ネットワーク/ホスト オブジェクト、または IP アドレスとして表されます。
XML	syslog サーバが、ログ メッセージを XML 形式で受信するかどうかを指定します。

要素	説明
[追加（Add）] ボタン	[Syslog Server] ダイアログボックス （15 ページ）が開きます。ここから、syslog サーバを定義できます。
[編集（Edit）] ボタン	[Syslog Server] ダイアログボックス （15 ページ）が開きます。ここから、選択した syslog サーバを編集できます。
[削除（Delete）]ボタン	選択した syslog サーバをテーブルから削除します。

[Syslog Server] ダイアログボックス

[Syslog Server] ダイアログボックスを使用して、ルータから syslog メッセージを収集するサーバを定義します。サーバがログメッセージを XML 形式またはプレーンテキストのどちらで受信するかを定義することもできます。

（注） このページに定義されている syslog サーバへのロギングをイネーブルにするには、ロギングをイネーブルにし、 Syslog ロギングの設定ポリシーのページ （10 ページ）で基本パラメータを定義する必要があります。

ナビゲーション パス

Syslog サーバ ポリシーのページ （14 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- Syslog サーバの定義 （4 ページ）
- Cisco IOS ルータにおけるロギング （1 ページ）
- ネットワーク/ホストオブジェクトについて

フィールド リファレンス

表 *4 : [Syslog Server]* ダイアログボックス

要素	説明
IPアドレス	syslog サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
Forward Messages in XML Format	選択すると、ログ メッセージが XML 形式で syslog サーバに送信されます。 選択を解除すると、ログ メッセージはプレーンテキストとして syslog サーバに送信されます。

NetFlow ポリシー ページ

[NetFlow] ページを使用して、NetFlow 記録をイネーブルにし、選択した Cisco IOS ルータ上でそのパラメータを定義します。

[NetFlow] ページは、2 つのタブ パネル（[Setup] と [Interfaces]）で構成されています。[Setup] タブには、ルータ上の NetFlow 収集のグローバル設定パラメータが表示されます。[Interfaces] タブには、NetFlow データ収集を設定するルータ インターフェイスが表示されます。このタブを使用して、入力アカウンティングと出力アカウンティングをインターフェイスごとにイネーブルおよびディセーブルにできます。

（注） 各ログ メッセージに対して正確なタイムスタンプを作成するために、ロギングがイネーブルになっているすべてのルータで NTP ポリシーを定義することを強く推奨します。詳細については、[NTP Policy] ページを参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [NetFlow]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [ロギング（Logging）] > [NetFlow]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または [NetFlow] を右クリックして新しいポリシーを作成します。

関連項目

- Cisco IOS ルータにおける NetFlow （6 ページ）
- NetFlow パラメータの定義 （7 ページ）
- NetFlow インターフェイス設定の追加および編集 （19 ページ）
- Cisco IOS ルータにおけるロギング （1 ページ）
- Cisco IOS ルータにおける NTP

フィールド リファレンス

表 *5 : [NetFlow]* ページ

要素	説明
[Setup] タブ	
Primary Destination Redundant Destination	プライマリおよびセカンダリ NetFlow Collector。プライマリ コレクタを選択して、このデバイスでの NetFlow データ収集をイネーブルにする必要があります。これらのいずれかのコレクタへの NetFlow データの送信をディセーブルにするには、ドロップダウン リストから空白のエントリを選択します。 NetFlow Collector の IP アドレスまたはホスト名を使用して NetFlow Collector を指定するかどうかを選択してから、各オプションの次の必須フィールドを設定します。 • [IPアドレス（IP Address）] : プライマリ NetFlow Collection Engine をホスティングしているデバイスの IP アドレスを入力します。また、IP アドレスを指定するネットワーク/ホストオブジェクトを指定するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成できます。 [UDPポート（UDP Port）] フィールドに、フローコレクタがモニターするポート番号を入力します（ポート番号の範囲は 1 ～ 65535）。ポートリスト オブジェクトの番号または名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成できます。 • [ホスト名（Hostname）] : プライマリ NetFlow Collection Engine をホスティングするデバイスの完全修飾ドメイン名を入力します。IP アドレスを指定するときと同様、UDP ポートを指定する必要もあります。
送信元インターフェイス（Source Interface）	フロー データがコレクタ宛先に送信されるときに経由するルータ インターフェイス。インターフェイスまたはインターフェイスロール名を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。

要素	説明
バージョン	NetFlowのバージョン番号。この番号によって、フローに使用されるレコード形式が定義されます。ブランクのエントリを選択して、このオプションをディセーブルにできます。 • [1]：元のレコード形式。追加のパラメータは必要ありません。 • [5]：ボーダー ゲートウェイ プロトコル（BGP）自律システム（AS）情報およびフローシーケンス番号など、最も広く採用されている形式。 ネットワークに BGP が設定されている場合は、NetFlow レコードに送信元またはピア AS 情報を含めることができます。[ASタイプ（AS Type）] ドロップダウンリストから、[origin-as] または [peer-as] を選択します。ブランクのエントリを選択して、このオプションをディセーブルにできます。 [BGPネクストホップの有効化（Enable BGP Nexthop）] をオンにして、BGPネクストホップ情報をフローキャッシュに含めます。（バージョン5では、この情報はキャッシュに表示されますが、エクスポートはされません）。 • [9]：テンプレートベースの最新バージョンであり、まだ完全にはサポートされていません。 ネットワークに BGP が設定されている場合は、NetFlow レコードに送信元またはピア AS 情報を含めることができます。[ASタイプ（AS Type）] ドロップダウンリストから、[origin-as] または [peer-as] を選択します。ブランクのエントリを選択して、このオプションをディセーブルにできます。 [BGPネクストホップの有効化（Enable BGP Nexthop）] をオンにして、BGPネクストホップ情報をフローレコードに含めます。 （注） AS 情報の収集はリソースを大量に消費します。origin-as の場合は特に消費量が多くなります。ピアリングの配置をモニタする必要がない場合は、AS収集をディセーブルにすると、パフォーマンスが向上する場合があります。
[インターフェイス（Interfaces）] タブ	
インターフェイス	NetFlow 収集が設定されるインターフェイスの名前。
Enable Ingress	[有効（Enabled）] は、このインターフェイスで着信トラフィックのフロー記録が有効になっていることを示します。[無効（Disabled）] は、このインターフェイスでは着信トラフィックが記録されないことを示します。
Enable Egress	[有効（Enabled）] は、このインターフェイスで発信トラフィックのフロー記録が有効になっていることを示します。[無効（Disabled）] は、このインターフェイスでは発信トラフィックが記録されないことを示します。

要素	説明
行を追加（Add Row）	このボタンをクリックして、[Add NetFlow Interface Settings] ダイアログボックスを開きます。NetFlow インターフェイスの追加については、NetFlow インターフェイス設定の追加および編集 （19 ページ）で説明しています。
Edit Row	このボタンをクリックして、選択したインターフェイスの [Edit NetFlow Interface Settings] ダイアログボックスを開きます。NetFlow インターフェイスの編集については、NetFlow インターフェイス設定の追加および編集（19 ページ）で説明しています。
Delete Row	選択したインターフェイスを削除するには、このボタンをクリックします。削除の確認が求められます。

NetFlow インターフェイス設定の追加および編集

[Add NetFlow Interface Settings]/[Edit NetFlow Interface Settings] ダイアログボックスを使用して、特定のルータ インターフェイスの NetFlow 入力レポートおよび出力レポートをイネーブルおよびディセーブルにします。

（注） タイトルを除き、これら 2 つのダイアログボックスは同一です。次の情報は、両方に適用されます。

ナビゲーション パス

NetFlow ポリシー ページ （16 ページ）に移動してから、テーブルの下にある [行の追加（Add Row）] ボタンまたは [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- NetFlow パラメータの定義 （7 ページ）
- Cisco IOS ルータにおけるロギング （1 ページ）

フィールド リファレンス

表 6 : [Add NetFlow Interface Settings]/[Edit NetFlow Interface Settings] ダイアログボックス

要素	説明
インターフェイス（Interface）	インターフェイスまたはインターフェイス ロールの名前。名前を入力します。または、[選択（Select）] をクリックしてリストからインターフェイスロールを選択するか、新たに作成します。

要素	説明
Enable Ingress Accounting	このオプションを選択すると、このインターフェイスに到着するトラフィックの NetFlow レコードが収集されます。 このオプションを選択解除すると、このインターフェイスでの着信トラフィックのデータ収集が停止されます。
Enable Egress Accounting	このオプションを選択すると、このインターフェイスを出るトラフィックの NetFlow レコードが収集されます。 このオプションを選択解除すると、このインターフェイスでの発信トラフィックのデータ収集が停止されます。

翻訳について
このドキュメントは、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。