syslogの信頼性の高い伝送およびフィルタリング

syslog の信頼性の高い伝送およびフィルタリング機能によって、デバイスを syslog メッセージの受信用にカスタマイズできます。この機能は、ブロック拡張可能交換プロトコル（BEEP）を使用したsyslogメッセージの信頼性の高いセキュアな伝送を提供します。さらに、基盤となる転送方式にかかわらず、1つのロギング ホストへの複数のセッションを可能にし、メッセージ ディスクリミネータと呼ばれるフィルタリング メカニズムを提供します。

この章では、syslog 機能のための信頼性の高い伝送およびフィルタリングの機能と、それらのネットワーク内での設定方法について説明します。

- syslog の信頼性の高い伝送およびフィルタリングの前提条件 （1 ページ）
- syslog の信頼性の高い伝送およびフィルタリングの制約事項 （2 ページ）
- syslog の信頼性の高い伝送およびフィルタリングに関する情報 （2 ページ）
- syslog の信頼性の高い伝送およびフィルタリングの設定方法 （8 ページ）
- syslog の信頼性の高い伝送およびフィルタリングの設定例 （14 ページ）
- syslog トランザクションの VRF 対応送信元インターフェイスに関する追加情報 （15 ページ）
- syslog の信頼性の高い伝送およびフィルタリングの機能情報 （16 ページ）

syslog の信頼性の高い伝送およびフィルタリングの前提条件

- デバイス レベルのレート制限を、ビジネス要件、ネットワーク トラフィック要件、またはパフォーマンス要件を満たすように設定します。
- 各 BEEP セッションには、RFC 3195 準拠の syslog-RAW 交換プロファイルが含まれている必要があります。
- 暗号イメージを使用する場合、プロビジョニング サービスに「DIGEST-MD5」を指定する Simple Authentication and Security Layer（SASL）プロファイルを確立する必要があります。

- syslog サーバは BEEP と互換性がある必要があります。
- syslog の信頼性の高い伝送およびフィルタリング機能の複数セッション機能を使用するには、syslogサーバアプリケーションは、複数のセッションを処理できる必要があります。

syslog の信頼性の高い伝送およびフィルタリングの制約事項

- syslog-RAW、SASL、およびトランスポート層セキュリティ（TLS）プロファイルだけがサポートされています。
- syslog セッションの両端で同じ転送方式を使用する必要があります。
- メッセージ ディスクリミネータを特定の syslog セッションに関連付けるには、事前に定義する必要があります。
- syslog セッションは、1 つのメッセージ ディスクリミネータとだけ関連付けることができます。
- ユーザ データグラム プロトコル（UDP）によるメッセージ伝送は、TCP または BEEP による伝送よりも速くなります。

syslog の信頼性の高い伝送およびフィルタリングに関する情報

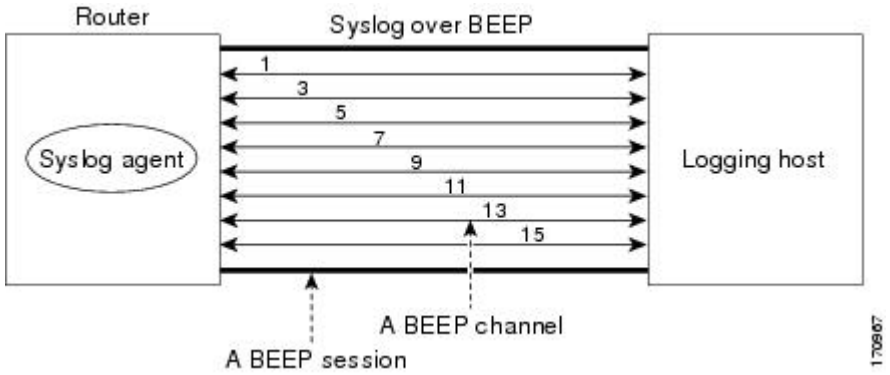
BEEP 転送のサポート

BEEPは、コネクション型非同期相互作用のための汎用アプリケーションプロトコルフレームワークです。これは、従来さまざまなプロトコルの実装で何度も利用されてきた機能を提供することを目的としています。BEEP は一般的に TCP 上で動作し、メッセージの交換が可能です。HTTP および同様のプロトコルとは異なり、接続の両端でいつでもメッセージを送信できます。BEEP には暗号化と認証のファシリティも含まれており、高い拡張性があります。

syslog メッセージの転送プロトコルとしての BEEP は、複数のチャネルを提供します。各チャネルは、同じホストへの異なるセッションに設定できます。BEEP は信頼性の高い転送を提供します。BEEP 接続を介して送信される syslog メッセージは、順序どおりに伝送されることが保証されます。

syslog の信頼性の高い伝送およびフィルタリング機能に導入されたコマンドライン インターフェイス（CLI）によって、新しい BEEP セッションが最大 8 つのチャネルを持つように設定できます。

次の図は、8 つの異なる syslog セッションを実現する、8 つのチャネルによる BEEP セッションを示しています。



チャネルは1、3、5、7、9、11、13、および15と識別されます。使用できるチャネルの数（8）は、従来の RFC-3164 syslog メッセージ（0 ～ 7）のシビラティ（重大度）の番号に対応して設計されています。メッセージディスクリミネータは、シビラティ（重大度）がBEEPチャネルにマッピングされるように使用できます。インテリジェントな BEEP syslog サーバ（使用する BEEP スタックによって異なる）は、このマッピングを使用して、シビラティ（重大度）の高いメッセージを優先できます（RFC 3081、セクション 3.1.4 を参照）。メッセージディスクリミネータと関連付けられている場合を除いて、すべてのsyslogセッション（チャネル）は、すべての syslog メッセージを受信します。

syslog メッセージ

syslog メッセージには、ホストが番号をメッセージの識別子として使用し、受信されたメッセージにギャップがあるかどうか検出できるようにするシーケンス番号があります。syslog メッセージには連続した番号が付けられます。BEEP の信頼性は、シーケンス番号（次の理由によって必要である）の必要性に代わるものではありません。

- シーケンス番号は、syslog メッセージを識別する簡単な方法を提供します。信頼性に関する問題に関係なく、シーケンス番号はメッセージ識別子として機能します。
- BEEP セッションは、syslog メッセージを送信するデバイスがアップ状態の間ずっと機能しているとは限りません。シーケンス番号は、BEEP セッションの間にメッセージが失われたかどうかを管理アプリケーションが評価する方法を提供します。
- BEEP はいくつかの転送のうちの 1 つにすぎません。信頼性の低い転送も使用されるので、syslog プロトコルは、常に提供されている信頼性の高い転送に依存すべきではありません。

syslog メッセージの既存の番号付け方式は、高度なメッセージの識別機能および複数のホストに対応するために、syslog の拡張で制限されます。メッセージの識別によって、シーケンス番号にギャップが発生します。つまり、ホストは、メッセージを見逃したかどうかを検出する能力を失います。シーケンス番号にギャップが発生しないよう、各セッションでsyslogメッセージに連番が付けられた場合は、シーケンス番号でメッセージが一意に識別されなくなるため、どのメッセージが同じで、どのメッセージが異なるかを簡単に関連付けできなくなります。

識別をシーケンスおよび信頼性から分離するために、syslog メッセージに対して、次の変更が行われました。

- シーケンス番号は、メッセージの識別子として保持されます。低い番号を持つメッセージは、高い番号を持つメッセージよりも優先されますが、連続するように保証されていません。
- シーケンスを保証するために、syslog メッセージの本文の部分に追加フィールドが追加されます。このフィールドの内容には、特定のセッションのシーケンス番号が含まれています。複数のセッションで送信される同じメッセージに、それぞれ異なるシーケンス番号が付けられる可能性があります。

syslog セッション

syslog セッションは、デバイス上の syslog エージェントから syslog メッセージの受信者への論理リンクです。たとえば、syslog エージェントと次のいずれかとの間で syslog セッションを確立できます。

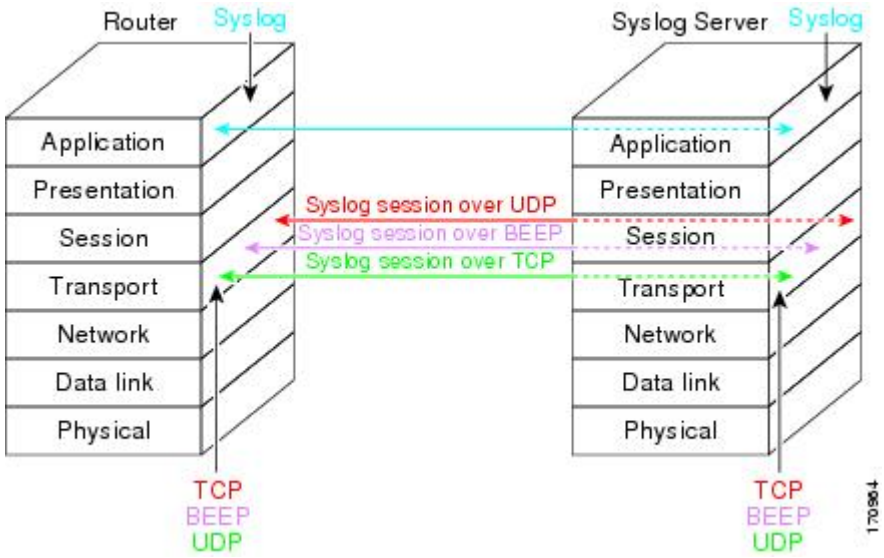
- デバイス コンソール
- デバイスのロギング バッファ
- デバイス モニタ
- 外部 syslog サーバ

syslog セッションは、syslog の送信元と syslog の宛先の間の転送接続で動作します。転送接続では次の任意のプロトコルを使用できます。

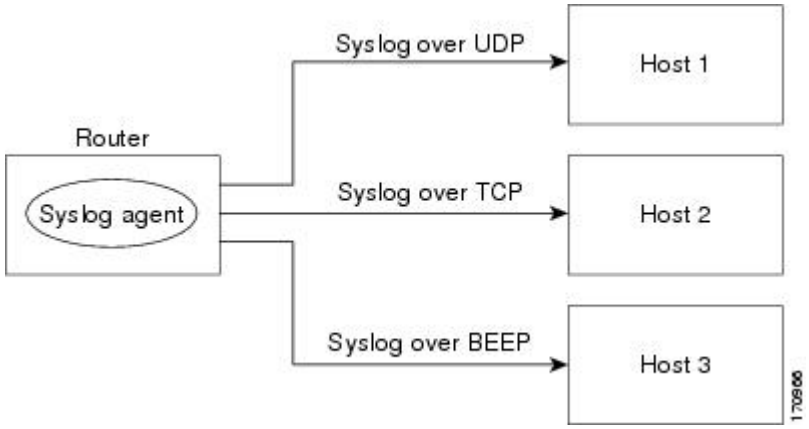
- TCP
- UDP（1 つのリモート アドレスおよびポートとの関連付け）
- BEEP（BEEP セッション内のチャネル）

次の図に、オープン システム相互接続（OSI）モデルを使用したデバイスと syslog サーバ間の syslog セッションおよび転送プロトコルのマッピングを示します。

（注） 次の図は Internet Explorer を使用すると最適に表示されます。



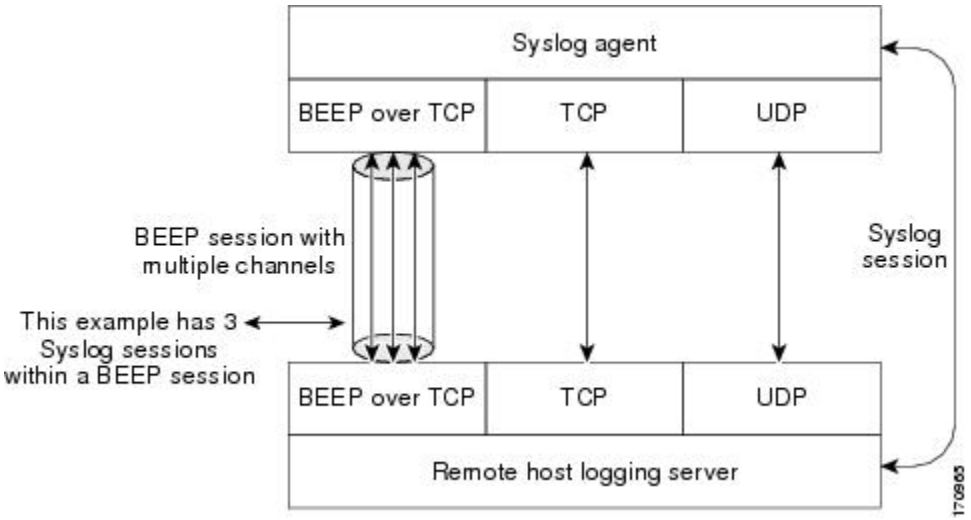
次の図に、UDP、TCP、および BEEP を使用した 1 つの syslog エージェントから複数のホストへの複数の syslog セッションを示します。



複数の syslog セッション

syslogセッションは、転送接続に依存しません。シスコデバイスは、それぞれが独自の転送接続で動作する複数の syslog セッションをサポートできます。複数の syslog セッションで同じ転送接続を共有できませんが、それぞれ独自の転送接続で動作している複数の syslog セッションを、同じリモートホストで終端することはできます。1 つの例として、複数のチャネルが使用される BEEP セッションがあります。

次の図は、エンドツーエンドの syslog セッションを示しています。1 つの BEEP セッションに 3 つの syslog セッションがあることに注目してください。



TCP プロトコルと UDP プロトコルには多重チャネルはありませんが、これらのプロトコルでは複数のポートを使用して、syslog ホストへの複数の syslog セッションを確立できます。UDP および TCP 転送方式が BEEP の複数チャネル機能と同様の機能を持つようにするために、syslog の信頼性の高い伝送およびフィルタリング機能では、UDP および TCP 転送方式によって、同じロギング ホストへの複数の syslog セッションを確立できます。BEEP セッションを経由する syslog セッションもサポートされています。

メッセージ ディスクリミネータ

メッセージ ディスクリミネータは syslog プロセッサです。メッセージ ディスクリミネータは syslog セッションに関連付けられ、セッションを転送接続にバインドします。

メッセージ送信の前に、メッセージは、ユーザが指定した基準リストを持つメッセージディスクリミネータの影響を受けます。最初のフィルタリング基準によってメッセージがブロックされると、フィルタリング チェックが停止します。

（注） CLI の基準の順序は、基準がチェックされる順番には影響しません。

- フィルタリング基準は次のとおりです。これらの基準は、次にリストされている順序でチェックされます。
  - 指定されたシビラティ（重大度）
  - 正規表現と一致するメッセージ本文内のファシリティ
  - 正規表現と一致するニーモニック
  - 正規表現と一致するメッセージ本文の部分

メッセージ ディスクリミネータは、次の機能を提供します。

- オプションのレート制限：超えてはならない、時間間隔あたりのメッセージの転送レートの指定。レート制限を超えた場合、メッセージは、デバイスの判断で遅延するか廃棄され

ます。レート制限の適用は、その syslog セッションでの syslog メッセージの信頼性の高い伝送が保証されなくなったことを意味します。レート制限の目的は、受信者の syslog サーバで、syslog の保証された伝送を必要としないアプリケーションの「フラッディング」が発生する可能性を回避することにあります。

- 相互関連付け：候補となるイベントメッセージを検査し、イベント全体の情報を可能な限り集約して、集約された情報を含む新しいイベントを作成。関連する機能は次のとおりです。
  - メッセージカウントを維持し、特定のタイプの最初のメッセージの送信とそのタイプの次のメッセージの送信の間の特定の時間待機することによる、重複メッセージの除去。
  - 変動するメッセージの除去
  - 単純なメッセージの相互関連付け。たとえば、あるメッセージが別のメッセージによって報告された原因の症状である場合、1 つの統合されたメッセージが報告されます。

メッセージディスクリミネータは、特定の宛先および転送と関連付けることができます。つまり、フィルタはホストに依存する可能性があります。このため、メッセージディスクリミネータは、それぞれ異なるディスクリミネータに適用できる複数のセッション、転送、またはチャネルに対して可能なデバイスサポートによって、syslogセッション、転送、またはチャネルに適用されます。

メッセージディスクリミネータの確立は、syslogセッションの確立から分離している必要があります。メッセージディスクリミネータは、適用される syslogセッション、転送、またはチャネルを参照する必要があります。分離の理由は次のとおりです。

- メッセージディスクリミネータは接続から個別に管理でき、メッセージディスクリミネータの設定に使用できる機能の調整を syslog セッションの設定方法に反映させる必要はなく、その逆も同様です。
- 複数の接続を同じメッセージ ディスクリミネータに適用でき、さまざまな syslog 冗長性トポロジが可能です。

明示的なメッセージ ディスクリミネータが syslog セッションと関連付けられていない場合、デバイス全体のグローバル設定から汎用メッセージディスクリミネータが使用されます。属性値を指定せずに、「空の」メッセージディスクリミネータを作成できます（レート制限もフィルタも設定されません）。

レート制限

Cisco IOS XE syslog でのデバイス全体のレート制限機能は、syslog の信頼性の高い伝送およびフィルタリング機能に保存され、「グローバル レート制限」と呼ばれています。グローバル レート制限を使用しない場合、システム リソースがその量をサポートできる場合には、すべてのイベント メッセージがリモート syslog ホストに送信されます。グローバル レート制限が設定されると、すべての宛先に適用されます。この値は、「汎用メッセージ ディスクリミネータ」のレート制限属性（設定されている場合）に設定されます。グローバル レート制限の欠点

は、最も性能の低いリモート syslog ホストのレート制限によって、デバイスが syslog メッセージを送信する速度が設定されることです。

syslog の信頼性の高い伝送およびフィルタリング機能は、syslog セッションベースのレート制限を提供し、グローバル レート制限の影響を回避します。このセッションベースのレート制限は、特定のメッセージ ディスクリミネータと関連付けられており、各 syslog セッションに対して、レート受け入れレベルを別々に設定できます。

セッションベースのレート制限が行われている場合、グローバル レート制限の使用は推奨されません。メッセージディスクリミネータのレート制限は、syslog メッセージの超えてはならないレートを指定しますが、このレートに到達することを保証しません。設定されたグローバル レート制限によって、セッションのレート制限に到達していない場合でも、そのセッションのメッセージが廃棄されることがあります。グローバル レート制限とセッションベースのレート制限が同時に使用される場合、これらの動作について理解することが重要です。

syslog の信頼性の高い伝送およびフィルタリングの利点

- BEEP の認証機能および暗号化機能では、syslog メッセージの信頼性の高いセキュアな伝送が提供されます。
- 基盤となる転送方式に依存しない 1 つのロギング ホストへの複数のセッション
- セッションベースのメッセージ フィルタリングおよびレート制限
- 複数の接続を同じメッセージ ディスクリミネータに適用でき、さまざまな syslog 冗長性トポロジが可能です。
- デフォルトの syslog カウントを無効にする新しい CLI コマンド
- レート制限によって廃棄される syslog メッセージの関連部分の識別に役立つ新しい CLI コマンド

syslog の信頼性の高い伝送およびフィルタリングの設定方法

メッセージ ディスクリミネータの作成

syslog メッセージのメッセージディスクリミネータを作成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **logging discriminator** *discr-name* [[**facility**] [**mnemonics**] [**msg-body**] {**drops** *string*| **includes** *string*}] [**severity** {**drops** *sev-num* | **includes** *sev-num*}] [**rate-limit** *msglimit*]

4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**logging discriminator** *discr-name* [[**facility**] [**mnemonics**] [**msg-body**] {**drops** *string*| **includes** *string*}] [**severity** {**drops** *sev-num* | **includes** *sev-num*}] [**rate-limit** *msglimit*] 例： `Device(config)# logging discriminator pacfltr1 facility includes facl357`	ファシリティ サブフィルタを持つメッセージ ディスクリミネータを作成します。 この例では、ファシリティ フィールドに「facl357」があるすべてのメッセージが伝送されます。
ステップ 4	**end** 例： `Device(config)# end`	CLI を特権 EXEC モードに戻します。

メッセージ ディスクリミネータのロギング バッファとの関連付け

メッセージディスクリミネータを特定のバッファと関連付けるには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **logging discriminator** *discr-name* [[**facility**] [**mnemonics**] [**msg-body**] {**drops** *string*| **includes** *string*}] [**severity** {**drops** *sev-num* | **includes** *sev-num*}] [**rate-limit** *msglimit*]
4. **logging buffered** [**discriminator** *discr-name* | **xml**] [*buffer-size*] [*severity-level*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**logging discriminator** *discr-name* [[**facility**] [**mnemonics**] [**msg-body**] {**drops** *string*| **includes** *string*}] [**severity** {**drops** *sev-num* | **includes** *sev-num*}] [**rate-limit** *msglimit*] 例： `Device(config)# logging discriminator pacfltr2`	メッセージ ディスクリミネータを作成します。
ステップ 4	**logging buffered** [**discriminator** *discr-name* | **xml**] [*buffer-size*] [*severity-level*] 例： `Device(config)# logging buffered discriminator pacfltr2 5`	ローカルバッファへのロギングをイネーブルにし、メッセージ ディスクリミネータを指定します。
ステップ 5	**end** 例： `Device(config)# end`	CLI を特権 EXEC モードに戻します。

メッセージ ディスクリミネータのコンソール端末との関連付け

メッセージディスクリミネータをコンソール端末と関連付けるには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **logging discriminator** *discr-name* [[**facility**] [**mnemonics**] [**msg-body**] {**drops** *string*| **includes** *string*}] [**severity** {**drops** *sev-num* | **includes** *sev-num*}] [**rate-limit** *msglimit*]
4. **logging console** [**discriminator** *discr-name* | **xml**] [*severity-level*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**logging discriminator** *discr-name* [[**facility**] [**mnemonics**] [**msg-body**] {**drops** *string*| **includes** *string*}] [**severity** {**drops** *sev-num* | **includes** *sev-num*}] [**rate-limit** *msglimit*] 例： `Device(config)# logging discriminator pacfltr3`	メッセージ ディスクリミネータを作成します。
ステップ 4	**logging console** [**discriminator** *discr-name* | **xml**] [*severity-level*] 例： `Device(config)# logging console discriminator pacfltr3 1`	コンソールへのロギングをイネーブルにして、特定のシビラティ（重大度）のメッセージをフィルタリングするメッセージディスクリミネータを指定します。
ステップ 5	**end** 例： `Device(config)# end`	CLI を特権 EXEC モードに戻します。

メッセージ ディスクリミネータの端末回線との関連付け

メッセージディスクリミネータを端末回線に関連付け、モニタにメッセージを表示するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **logging discriminator** *discr-name* [[**facility**] [**mnemonics**] [**msg-body**] {**drops** *string*| **includes** *string*}] [**severity** {**drops** *sev-num* | **includes** *sev-num*}] [**rate-limit** *msglimit*]
4. **logging monitor** [**discriminator** *discr-name*| **xml**] [*severity-level*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**logging discriminator** *discr-name* [[**facility**] [**mnemonics**] [**msg-body**] {**drops** *string*| **includes** *string*}] [**severity** {**drops** *sev-num* | **includes** *sev-num*}] [**rate-limit** *msglimit*] 例： `Device(config)# logging discriminator pacfltr4`	メッセージ ディスクリミネータを作成します。
ステップ 4	**logging monitor** [**discriminator** *discr-name*| **xml**] [*severity-level*] 例： `Device(config)# logging monitor discriminator pacfltr4 2`	pacfltr4 という名前のメッセージ ディスクリミネータを指定し、シビラティ（重大度） 2 以下で端末回線へのメッセージのロギングをイネーブルにします。
ステップ 5	**end** 例： `Device(config)# end`	CLI を特権 EXEC モードに戻します。

メッセージ カウンタのイネーブル化

デバッグ、ログ、またはsyslogメッセージのロギングをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **logging message-counter** {**debug** | **log** | **syslog**}
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**logging message-counter** {**debug** | **log** | **syslog**} 例： `Device(config)# logging message-counter syslog`	syslog メッセージのロギングをイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	CLI を特権 EXEC モードに戻します。

BEEP セッションの追加と削除

BEEP セッションを追加および削除するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **logging host** {{*ip-address* | *hostname*} [**vrf** *vrf-name*] | **ipv6**{*ipv6-address* | *hostname*}} [**discriminator** *discr-name* | [[**filtered** [**stream** *stream-id*] | **xml**]] [**transport** {[**beep** [**audit**] [**channel** *chnl-number*] [**sasl** *profile-name*] [**tls cipher** [*cipher-num*] **trustpoint** *trustpt-name*]]] | **tcp**[**audit**] | **udp**} [**port** *port-num*]] [**sequence-num-session**] [**session-id**{**hostname** | **ipv4** | **ipv6** | **string** *custom-string*}]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**logging host** {{*ip-address* | *hostname*} [**vrf** *vrf-name*] | **ipv6**{*ipv6-address* | *hostname*}} [**discriminator** *discr-name* | [[**filtered** [**stream** *stream-id*] | **xml**]] [**transport** {[**beep** [**audit**] [**channel** *chnl-number*] [**sasl** *profile-name*] [**tls cipher** [*cipher-num*] **trustpoint** *trustpt-name*]]] | **tcp**[**audit**] | **udp**} [**port** *port-num*]] [**sequence-num-session**] [**session-id**{**hostname** | **ipv4** | **ipv6** | **string** *custom-string*}] 例： `Device(config)# logging host host3 transport beep port 600 channel 3`	ロギング ホストを指定し、メッセージのロギングのための転送プロトコル、ポート、およびチャネルを指定します。
ステップ 4	**end** 例： `Device(config)# end`	CLI を特権 EXEC モードに戻します。

syslog の信頼性の高い伝送およびフィルタリングの設定例

転送とロギングの設定例

```
Device(config)# do show running-config
 | include logging
logging buffered xml
logging host 209.165.201.1 transport udp port 601
Device(config)# logging host 209.165.201.1 transport beep port 600 channel 3
Device(config)# logging host 209.165.201.1 transport tcp port 602

Device(config)# show running-config | include logging
logging buffered xml
logging host 209.165.201.1 transport udp port 601
logging host 209.165.201.1 transport beep port 600 channel 3
logging host 209.165.201.1 transport tcp port 602
Device(config)#
```

syslog トランザクションの VRF 対応送信元インターフェイスに関する追加情報

関連資料

関連項目	マニュアル タイトル
ネットワーク管理コマンド（logging コマンドを含む）：コマンド構文の詳細、デフォルト設定、コマンド モード、コマンド履歴、使用上のガイドライン、および例	『*Cisco IOS Network Management Command Reference*』
Syslog ロギング	*Troubleshooting and Fault Management module*

標準および RFC

標準/RFC	タイトル
この機能によりサポートされる新規または変更された標準/RFC はありません。またこの機能による既存の標準/RFC のサポートに変更はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

syslog の信頼性の高い伝送およびフィルタリングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : syslog* の信頼性の高い伝送およびフィルタリングの機能情報

機能名	リリース	機能情報
syslog の信頼性の高い伝送およびフィルタリング	Cisco IOS XE Release 2.1	syslog の信頼性の高い伝送およびフィルタリング機能によって、デバイスを syslog メッセージの受信用にカスタマイズできます。この機能は、BEEP を使用した syslog メッセージの信頼性の高いセキュアな伝送を提供します。さらに、基盤となる転送方式にかかわらず、1 つのロギング ホストへの複数のセッションを可能にし、メッセージディスクリミネータと呼ばれるフィルタリング メカニズムを提供します。 Cisco IOS XE リリース 2.1 では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドが導入または変更されました。**logging buffered**、**logging console**、 **logging discriminator**、 **logging host**、 **logging message-counter**、 **logging monitor**、 **show logging**。

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。