



CHAPTER 31

システム メッセージ ログイングおよびスマート ログイングの設定

この章では、Catalyst 3750 スイッチにシステム メッセージ ログイングを設定する方法について説明します。Cisco IOS Release 12.2(58)SE 以降のスイッチでは、設定されたトリガーに基づいてパケットフローを取り込むスマート ログイングもサポートされます。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.4*』およびこのリリースに対応するコマンドリファレンスを参照してください。

- 「システム メッセージ ログイングの概要」 (P.31-1)
- 「システム メッセージ ログイングの設定」 (P.31-2)
- 「スマート ログイングの設定」 (P.31-14)
- 「ログイング設定の表示」 (P.31-17)



注意

高レートでコンソールへのメッセージを記録すると、CPU の使用率が高くなり、スイッチの動作に悪影響を与える可能性があります。

システム メッセージ ログイングの概要

スイッチはデフォルトで、システム メッセージおよび **debug** 特権 EXEC コマンドの出力をログイングプロセスに送信します。スタック メンバにより、システム メッセージをトリガーできます。システム メッセージを生成するスタック メンバは、ホスト名を *hostname-n* の形式で付加し (*n* は 1 ~ 9 のスイッチ番号)、出力をスタック マスターのログイングプロセスにリダイレクトします。スタック マスターはスタック メンバですが、そのホスト名はシステム メッセージの末尾に追加されません。ログイングプロセスはログ メッセージを各宛先 (設定に応じて、ログ バッファ、端末回線、UNIX Syslog サーバなど) に配信する処理を制御します。ログイングプロセスは、コンソールにもメッセージを送信します。



(注)

Syslog フォーマットは 4.3 Berkeley Standard Distribution (BSD) UNIX と互換性があります。

ログイング プロセスがディセーブルの場合、メッセージはコンソールにのみ送信されます。メッセージは生成時に送信されるため、メッセージおよびデバッグ出力にはプロンプトや他のコマンドの出力が割り込みます。メッセージがアクティブなコンソールに表示されるのは、メッセージを生成したプロセスが終了してからです。

メッセージの重大度を設定して、コンソールおよび各宛先に表示されるメッセージのタイプを制御できます。ログ メッセージにタイム スタンプを設定したり、Syslog 送信元アドレスを設定したりして、リアルタイムのデバッグ機能および管理機能を強化できます。表示されるメッセージについては、このリリースに対応するシステム メッセージ ガイドを参照してください。

ログイングされたシステム メッセージにアクセスするには、スイッチのコマンドライン インターフェイス (CLI) を使用するか、または適切に設定された Syslog サーバにこれらのシステム メッセージを保存します。スイッチ ソフトウェアは、Syslog メッセージをスタンドアロン スイッチ上の内部バッファに保存します。スイッチ スタックの場合は、スタック マスター上に保存します。スタンドアロン スイッチまたはスタック マスターに障害が発生すると、ログをフラッシュ メモリに保存していなかった場合、ログは失われます。

システム メッセージをリモートでモニタするには、Syslog サーバ上でログを表示するか、または Telnet あるいはコンソール ポート経由でスイッチにアクセスします。スイッチ スタックでは、すべてのスタック メンバ コンソールにより、同じコンソール出力が用意されます。

システム メッセージ ログイングの設定

- 「システム ログ メッセージのフォーマット」 (P.31-2)
- 「システム メッセージ ログイングのデフォルト設定」 (P.31-4)
- 「メッセージ ログイングのディセーブル化」 (P.31-4) (任意)
- 「メッセージ表示宛先デバイスの設定」 (P.31-5) (任意)
- 「ログ メッセージの同期化」 (P.31-6) (任意)
- 「ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化」 (P.31-8) (任意)
- 「ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化」 (P.31-8) (任意)
- 「メッセージ重大度の定義」 (P.31-9) (任意)
- 「履歴テーブルおよび SNMP に送信される Syslog メッセージの制限」 (P.31-10) (任意)
- 「設定変更ロガーのイネーブル化」 (P.31-11) (任意)
- 「UNIX Syslog サーバの設定」 (P.31-12) (任意)

システム ログ メッセージのフォーマット

システム ログ メッセージは最大 80 文字とパーセント記号 (%)、およびその前に配置されるオプションのシーケンス番号やタイム スタンプ情報 (設定されている場合) で構成されています。メッセージは、次のフォーマットで表示されます。

```
seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)
```

パーセント記号の前のメッセージ部分は、**service sequence-numbers**、**service timestamps log datetime**、**service timestamps log datetime [localtime] [msec] [show-timezone]**、または **service timestamps log uptime** グローバル コンフィギュレーション コマンドの設定によって変わります。

表 31-1 に、Syslog メッセージの要素を示します。

表 31-1 システム ログ メッセージの要素

要素	説明
<i>seq no:</i>	service sequence-numbers グローバル コンフィギュレーション コマンドが設定されている場合だけ、ログ メッセージにシーケンス番号をスタンプします。 詳細については、「ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化」(P.31-8) を参照してください。
<i>timestamp</i> のフォーマット： <i>mm/dd hh:mm:ss</i> または <i>hh:mm:ss</i> (短時間) または <i>d h</i> (長時間)	メッセージまたはイベントの日時です。 service timestamps log [datetime log] グローバル コンフィギュレーション コマンドが設定されている場合だけ、この情報が表示されます。 詳細については、「ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化」(P.31-8) を参照してください。
<i>facility</i>	メッセージが参照する機能 (SNMP、SYS など) です。サポートされる機能の一覧については、表 31-4 (P.31-14) を参照してください。
<i>severity</i>	メッセージの重大度を示す 0 ~ 7 の 1 桁のコードです。重大度の詳細については、表 31-3 (P.31-10) を参照してください。
<i>MNEMONIC</i>	メッセージを一意に示すテキスト ストリングです。
<i>description</i>	レポートされているイベントの詳細を示すテキスト ストリングです。
<i>hostname-n</i> (ホスト名 -n)	スタック メンバのホスト名およびスタック内のスイッチ番号。スタック マスターはスタック メンバですが、そのホスト名はシステム メッセージの末尾に追加されません。

次の例は、スタック マスターおよびスタック メンバ (ホスト名は *Switch-2*) に対応するスイッチ システム メッセージの一部です。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channell, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed
state to down 2
*Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar 1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

00:00:46: %LINK-3-UPDOWN: Interface Port-channell, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/2, changed state to up (Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
(Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/1, changed
state to down 2 (Switch-2)
```

システム メッセージ ログイングのデフォルト設定

表 31-2 システム メッセージ ログイングのデフォルト設定

機能	デフォルト設定
コンソールへのシステム メッセージ ログイング	イネーブル
コンソールの重大度	debugging (および数値的により低いレベル。 表 31-3 (P.31-10) を参照)
ログ ファイル設定	ファイル名の指定なし
ログ バッファ サイズ	4096 バイト
ログ履歴サイズ	1 メッセージ
タイム スタンプ	ディセーブル
同期ログイング	ディセーブル
ログイング サーバ	ディセーブル
Syslog サーバの IP アドレス	未設定
設定変更ロガー	ディセーブル
サーバ機能	Local7 (表 31-4 (P.31-14) を参照)
サーバの重大度	informational (および数値的により低いレベル。 表 31-3 (P.31-10) を参照)

メッセージ ログイングのディセーブル化

メッセージ ログイングはデフォルトでイネーブルに設定されています。コンソール以外のいずれかの宛先にメッセージを送信する場合は、メッセージ ログイングをイネーブルにする必要があります。メッセージ ログイングがイネーブルの場合、ログ メッセージはログイング プロセスに送信されます。ログイング プロセスは、メッセージを生成元プロセスと同期しないで指定場所に記録します。

メッセージ ログイングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	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 2	no logging console	メッセージ ログイングをディセーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config または show logging	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ログイング プロセスをディセーブルにすると、メッセージがコンソールに書き込まれるまでプロセスは処理続行を待機する必要があるため、スイッチの処理速度が低下することがあります。ログイング プロセスがディセーブルの場合、メッセージは生成後すぐに (通常はコマンド出力に割り込む形で) コンソールに表示されます。

logging synchronous グローバル コンフィギュレーション コマンドも、コンソールへのメッセージ表示に影響します。このコマンドをイネーブルにすると、**Return** を押さなければメッセージが表示されません。詳細については、「[ログ メッセージの同期化](#)」(P.31-6) を参照してください。

メッセージ ログイングをディセーブルにした後に再びイネーブルにするには、**logging on** グローバル コンフィギュレーション コマンドを使用します。

メッセージ表示宛先デバイスの設定

メッセージ ログイングがイネーブルの場合、コンソールだけでなく特定の場所にもメッセージを送信できます。メッセージの受信場所を指定するには、特権 EXEC モードで次のコマンドを 1 つまたは複数使用します。この手順は任意です。

	コマンド	目的
ステップ 1	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 2	logging buffered [size]	<p>スタンドアロン スイッチ上か、または、スイッチ スタックの場合はスタック マスター上で、ログ メッセージを内部バッファに保存します。指定できる範囲は 4096 ~ 2147483647 バイトです。デフォルトのバッファサイズは 4096 バイトです。</p> <p>スタンドアロン スイッチまたはスタック マスターに障害が発生すると、ログ ファイルをフラッシュ メモリに保存していなかった場合、ログ ファイルは失われます。ステップ 4 を参照してください。</p> <p>(注) バッファ サイズを大きすぎる値に設定しないでください。他の作業に使用するメモリが不足することがあります。スイッチ上の空きプロセッサ メモリを表示するには、show memory 特権 EXEC コマンドを使用します。ただし、表示される値は使用できる最大値であるため、バッファ サイズをこの値に設定しないでください。</p>
ステップ 3	logging host	<p>UNIX Syslog サーバホストにメッセージを記録します。</p> <p><i>host</i> には、Syslog サーバとして使用するホストの名前または IP アドレスを指定します。</p> <p>ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。</p> <p>Syslog サーバの設定手順については、「UNIX Syslog サーバの設定」(P.31-12) を参照してください。</p>

	コマンド	目的
ステップ 4	logging file flash:filename [max-file-size [min-file-size]] [severity-level-number type]	ログ メッセージをフラッシュ メモリのファイル内にストアします (スタンドアロン スイッチ上、あるいはスイッチ スタックの場合はスタック マスター上)。 <ul style="list-style-type: none"> filename には、ログ メッセージのファイル名を入力します。 (任意) max-file-size には、ログ ファイルの最大サイズを指定します。指定できる範囲は 4096 ~ 2147483647 です。デフォルトは 4096 バイトです。 (任意) min-file-size には、ログ ファイルの最小サイズを指定します。指定できる範囲は 1024 ~ 2147483647 です。デフォルトは 2048 バイトです。 (任意) severity-level-number type には、ログイングの重大度またはログイング タイプを指定します。重大度に指定できる範囲は 0 ~ 7 です。ログイング タイプ キーワードの一覧については、表 31-3 (P.31-10) を参照してください。デフォルトでは、デバッグ メッセージ、および数値的により低いレベルのメッセージがログ ファイルに送信されます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	terminal monitor	現在のセッション中に、コンソール以外の端末にメッセージを記録します。 端末パラメータ コンフィギュレーション コマンドはローカルに設定され、セッションの終了後は無効になります。デバッグ メッセージを表示する場合は、セッションごとにこのステップを実行する必要があります。
ステップ 7	show running-config	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

logging buffered グローバル コンフィギュレーション コマンドを実行すると、ログ メッセージが内部バッファにコピーされます。循環バッファなので、バッファがいっぱいになると、古いメッセージが新しいメッセージで置き換えられます。バッファに記録されたメッセージを表示するには、**show logging** 特権 EXEC コマンドを使用します。バッファ内の最も古いメッセージが最初に表示されます。バッファの内容をクリアするには、**clear logging** 特権 EXEC コマンドを使用します。

特定の PoE に対応したポートで Power over Ethernet (PoE) イベントのログイングをイネーブルにしたりディセーブルにしたりするには、**logging event power-inline-status** インターフェイス コンフィギュレーション コマンドを使用します。これらのポートへのログイングは、デフォルトでイネーブルです。

コンソールへのログイングをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。ファイルへのログイングをディセーブルにするには、**no logging file [severity-level-number | type]** グローバル コンフィギュレーション コマンドを使用します。

ログ メッセージの同期化

特定のコンソール ポート回線または仮想端末回線に対して、非送信請求メッセージおよび **debug** 特権 EXEC コマンドの出力を送信請求デバイスの出力およびプロンプトと同期させることができます。重大度に応じて非同期に出力されるメッセージのタイプを特定できます。また、端末の非同期メッセージが削除されるまで保存しておくバッファの最大数を設定することもできます。

非送信請求メッセージおよび **debug** コマンド出力の同期ログイングがイネーブルの場合、送信請求デバイス出力がコンソールに表示または印刷された後に、非送信請求デバイスからの出力が表示または印刷されます。非送信請求メッセージおよび **debug** コマンドの出力は、ユーザ入力用プロンプトが返された後に、コンソールに表示されます。したがって、非送信請求メッセージおよび **debug** コマンドの出力は、送信請求デバイス出力およびプロンプトに割り込まれることはありません。非送信請求メッセージが表示された後に、コンソールはユーザ プロンプトを再表示します。

同期ログイングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	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 2	line [console vty] line-number [ending-line-number]	<p>メッセージの同期ログイングを行うように、回線を設定します。</p> <ul style="list-style-type: none"> スイッチのコンソール ポートを介して行われる設定には、console キーワードを使用します。 同期ログイングをイネーブルにする vty 回線を指定するには、line vty line-number コマンドを使用します。Telnet セッションを介して行われる設定には、vty 接続を使用します。回線番号に指定できる範囲は 0 ~ 15 です。 <p>16 個の vty 回線の設定をすべて一度に変更するには、次のように入力します。</p> <p>line vty 0 15</p> <p>また、現在の接続に使用されている 1 つの vty 回線の設定を変更することもできます。たとえば、vty 回線 2 の設定を変更するには、次のように入力します。</p> <p>line vty 2</p> <p>このコマンドを入力すると、ライン コンフィギュレーション モードになります。</p>
ステップ 3	logging synchronous [level [severity-level all] limit number-of-buffers]	<p>メッセージの同期ログイングをイネーブルにします。</p> <ul style="list-style-type: none"> (任意) level severity-level には、メッセージの重大度を指定します。重大度がこの値以上であるメッセージは、非同期に出力されます。値が小さいほど重大度は大きく、値が大きいほど重大度は小さくなります。デフォルトは 2 です。 (任意) level all を指定すると、重大度に関係なく、すべてのメッセージが非同期に出力されます。 (任意) limit number-of-buffers には、キューイングされる端末のバッファ数を指定します。これを超える新しいメッセージは廃棄されます。指定できる範囲は 0 ~ 2147483647 です。デフォルトは 20 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

非送信請求メッセージおよびデバッグ出力の同期をディセーブルにするには、**no logging synchronous [level severity-level | all] [limit number-of-buffers]** ライン コンフィギュレーション コマンドを使用します。

ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化

デフォルトでは、ログ メッセージにはタイム スタンプが適用されません。

ログ メッセージのタイム スタンプをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	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 2	service timestamps log uptime または service timestamps log datetime [msec] [localtime] [show-timezone]	ログのタイム スタンプをイネーブルにします。 最初のコマンドを実行するとログ メッセージのタイム スタンプがイネーブルになり、システムを再起動した後の経過時間が表示されます。 2 番目のコマンドを実行すると、ログ メッセージのタイム スタンプがイネーブルになります。選択したオプションに応じて、ローカル タイム ゾーンを基準とした日付、時間 (ミリ秒)、タイム ゾーン名をタイム スタンプとして表示できます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デバッグ メッセージとログ メッセージの両方のタイム スタンプをディセーブルにするには、**no service timestamps** グローバル コンフィギュレーション コマンドを使用します。

次に、**service timestamps log datetime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
*Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
(Switch-2)
```

次に、**service timestamps log uptime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up (Switch-2)
```

ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化

複数のログ メッセージのタイム スタンプが同じになることがあるため、1 つのメッセージを正確に識別できるように、メッセージにシーケンス番号を表示できます。デフォルトでは、ログ メッセージにシーケンス番号は表示されません。

ログ メッセージのシーケンス番号をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	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 2	service sequence-numbers	シーケンス番号をイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ4	show running-config	設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

シーケンス番号をディセーブルにするには、**no service sequence-numbers** グローバル コンフィギュレーション コマンドを使用します。

次に、シーケンス番号をイネーブルにした場合のログイング表示の一部を示します。

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) (Switch-2)
```

メッセージ重大度の定義

選択したデバイスに表示されるメッセージを制限するには、メッセージの重大度を指定します (表 31-3 を参照)。

メッセージの重大度を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	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2	logging console level	コンソールに記録されるメッセージを制限します。 デフォルトで、コンソールはデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します (表 31-3 (P.31-10) を参照)。
ステップ3	logging monitor level	端末回線に記録されるメッセージを制限します。 デフォルトで、端末はデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します (表 31-3 (P.31-10) を参照)。
ステップ4	logging trap level	Syslog サーバに記録されるメッセージを制限します。 デフォルトで、Syslog サーバは通知メッセージ、および数値的により低いレベルのメッセージを受信します (表 31-3 (P.31-10) を参照)。 Syslog サーバの設定手順については、「UNIX Syslog サーバの設定」(P.31-12) を参照してください。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show running-config または show logging	設定を確認します。
ステップ7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) *level* を指定すると、このレベルのメッセージ、および数値的により低いレベルのメッセージが宛先に表示されます。

コンソールへのログイングをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。コンソール以外の端末へのログイングをディセーブルにするには、**no logging monitor** グローバル コンフィギュレーション コマンドを使用します。Syslog サーバへのログイングをディセーブルにするには、**no logging trap** グローバル コンフィギュレーション コマンドを使用します。

表 31-3 に *level* キーワードを示します。また、対応する UNIX Syslog 定義を、重大度の最も高いものから順に示します。

表 31-3 メッセージ ログイング level キーワード

level キーワード	レベル	説明	Syslog 定義
emergencies	0	システムが不安定	LOG_EMERG
alerts	1	即時処理が必要	LOG_ALERT
critical	2	クリティカルな状態	LOG_CRIT
errors	3	エラー状態	LOG_ERR
warnings	4	警告状態	LOG_WARNING
notifications	5	正常だが注意を要する状態	LOG_NOTICE
informational	6	情報メッセージだけ	LOG_INFO
debugging	7	デバッグ メッセージ	LOG_DEBUG

ソフトウェアは、これ以外の 4 つのカテゴリのメッセージを生成します。

- ソフトウェアまたはハードウェアの誤動作に関するエラー メッセージ：**warnings** ~ **emergencies** の重大度で表示されます。このタイプのメッセージは、スイッチの機能に影響があることを示します。この誤動作からの回復手順については、このリリースに対応するシステム メッセージ ガイドを参照してください。
- **debug** コマンドの出力：**debugging** の重大度で表示されます。通常、デバッグ コマンドは Technical Assistance Center (TAC) でのみ使用されます。
- インターフェイスのアップまたはダウン トランジション メッセージおよびシステム再起動メッセージ：**notifications** の重大度で表示されます。このメッセージは単なる情報であり、スイッチの機能には影響がありません。
- リロード要求と低プロセス スタック メッセージ：**informational** の重大度で表示されます。このメッセージは単なる情報であり、スイッチの機能には影響がありません。

履歴テーブルおよび SNMP に送信される Syslog メッセージの制限

snmp-server enable trap グローバル コンフィギュレーション コマンドを使用して、SNMP Network Management Station (NMS; ネットワーク管理ステーション) に送信されるように Syslog メッセージトラップがイネーブルに設定されている場合は、スイッチの履歴テーブルに送信および格納されるメッセージの重大度を変更できます。また、履歴テーブルに格納されるメッセージの数を変更することもできます。

SNMP トラップは宛先への到達が保証されていないため、メッセージは履歴テーブルに格納されます。デフォルトでは、Syslog トラップがイネーブルでない場合も、重大度が **warnings** のメッセージ、および数値的により低いメッセージ (表 31-3 (P.31-10) を参照) が、履歴テーブルに 1 つ格納されます。

重大度および履歴テーブル サイズのデフォルト値を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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 2	<code>logging history level¹</code>	履歴ファイルに格納され、SNMP サーバに送信される Syslog メッセージのデフォルトの重大度を変更します。 <i>level</i> キーワードのリストについては、表 31-3 (P.31-10) を参照してください。 デフォルトでは、 warnings 、 errors 、 critical 、 alerts 、および emergencies のメッセージが送信されます。
ステップ 3	<code>logging history size number</code>	履歴テーブルに格納できる Syslog メッセージ数を指定します。 デフォルトでは 1 つのメッセージが格納されます。指定できる範囲は 0 ~ 500 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

1. 表 31-3 に、*level* キーワードおよび重大度を示します。SNMP を使用している場合は、重大度の値が 1 だけ増えます。たとえば、*emergencies* は 0 ではなく 1 に、*critical* は 2 ではなく 3 になります。

履歴テーブルがいっぱいの場合 (`logging history size` グローバル コンフィギュレーション コマンドで指定した最大メッセージ エントリ数が格納されている場合) は、新しいメッセージ エントリを格納できるように、最も古いエントリがテーブルから削除されます。

Syslog メッセージのログイングをデフォルトの重大度に戻すには、`no logging history` グローバル コンフィギュレーション コマンドを使用します。履歴テーブル内のメッセージ数をデフォルト値に戻すには、`no logging history size` グローバル コンフィギュレーション コマンドを使用します。

設定変更ロガーのイネーブル化

コマンドライン インターフェイス (CLI) で行った設定変更をトラッキングするために設定ロガーをイネーブルにすることができます。`logging enable` 設定変更ロガー コンフィギュレーション コマンドを入力すると、設定変更用に入力されたセッション、ユーザおよびコマンドがログに記録されます。設定ログのサイズは 1 ~ 1000 エントリの間で設定することができます (デフォルトは 100)。`no logging enable` コマンドの後に `logging enable` コマンドを入力してログイングをディセーブルにして再びイネーブルにすることで、いつでもログをクリアすることができます。

`show archive log config {all | number [end-number] | user username [session number] number [end-number] | statistics} [provisioning]` 特権 EXEC コマンドを使用して、設定ログ全体または指定したパラメータのログを表示します。

デフォルトで設定ログイングはディセーブルになっています。

コマンドの詳細については、次の URL にある『Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3 T』を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3/configfun/command/reference/cfr_1g04.html

設定ログイングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	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 2	archive	アーカイブ 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	log config	設定変更ロガー コンフィギュレーション モードを開始します。
ステップ 4	logging enable	設定変更ログイングをイネーブルにします。
ステップ 5	logging size entries	(任意) 設定ログで取得するエントリ数を設定します。指定できる範囲は 1 ~ 1000 です。デフォルトは 100 です。 (注) 設定ログがいっぱいになると、新規エントリが入力されるたびに最も古いログ エントリが削除されます。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show archive log config	設定ログを表示することでエントリを確認します。

次に、設定変更ロガーをイネーブルにして、ログのエントリ数を 500 に設定する例を示します。

```
Switch(config)# archive
Switch(config-archive)# log config
Switch(config-archive-log-cfg)# logging enable
Switch(config-archive-log-cfg)# logging size 500
Switch(config-archive-log-cfg)# end
```

設定ログの出力例は次のとおりです。

```
Switch# show archive log config all
idx  sess      user@line   Logged command
 38   11   unknown user@vty3 |no aaa authorization config-commands
 39   12   unknown user@vty3 |no aaa authorization network default group radius
 40   12   unknown user@vty3 |no aaa accounting dotlx default start-stop group
radius
 41   13   unknown user@vty3 |no aaa accounting system default
 42   14       temi@vty4   |interface GigabitEthernet4/0/1
 43   14       temi@vty4   | switchport mode trunk
 44   14       temi@vty4   | exit
 45   16       temi@vty5   |interface FastEthernet5/0/1
 46   16       temi@vty5   | switchport mode trunk
 47   16       temi@vty5   | exit
```

UNIX Syslog サーバの設定

次に、UNIX サーバの Syslog デーモンを設定し、UNIX システム ログイング機能を定義する手順について説明します。

UNIX Syslog デーモンへのログ メッセージ

システム ログ メッセージを UNIX Syslog サーバに送信する前に、UNIX サーバ上で Syslog デーモンを設定する必要があります。この手順は任意です。

root としてログインし、次のステップを実行します。



(注)

最新バージョンの UNIX Syslog デーモンの中には、デフォルトでネットワークからの Syslog パケットを受け入れないものがあります。このようなシステムの場合に、Syslog メッセージのリモート ログイングをイネーブルにするには、Syslog コマンドラインに追加または削除する必要があるオプションを、UNIX の **man syslogd** コマンドを使用して判別します。

ステップ 1 /etc/syslog.conf ファイルに次のような行を 1 行追加します。

```
local7.debug /usr/adm/logs/cisco.log
```

local7 キーワードは、使用するログイング機能を指定します。機能の詳細については、表 31-4 (P.31-14) を参照してください。**debug** キーワードは、Syslog の重大度を指定します。重大度の詳細については、表 31-3 (P.31-10) を参照してください。Syslog デーモンは、これ以上の重大度の場合に、次のフィールドで指定されたファイルにメッセージを送信します。このファイルは、Syslog デーモンに書き込み権限がある既存ファイルでなければなりません。

ステップ 2 UNIX シェル プロンプトに次のコマンドを入力して、ログ ファイルを作成します。

```
$ touch /var/log/cisco.log
$ chmod 666 /var/log/cisco.log
```

ステップ 3 Syslog デーモンに新しい設定を認識させます。

```
$ kill -HUP `cat /etc/syslog.pid`
```

詳細については、ご使用の UNIX システムの **man syslog.conf** および **man syslogd** コマンドを参照してください。

UNIX システム ログイング機能の設定

システム ログ メッセージを外部デバイスに送信する場合は、メッセージを UNIX Syslog 機能から送信されたメッセージとして特定するようにシステムを設定できます。

UNIX システム機能メッセージ ログイングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	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2	logging host	IP アドレスを入力して、UNIX Syslog サーバ ホストにメッセージを記録します。 ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。

	コマンド	目的
ステップ 3	<code>logging trap level</code>	Syslog サーバに記録されるメッセージを制限します。 デフォルトでは、Syslog サーバは通知メッセージおよびそれより下のレベルのメッセージを受信します。 <i>level</i> キーワードについては、表 31-3 (P.31-10) を参照してください。
ステップ 4	<code>logging facility facility-type</code>	Syslog 機能を設定します。 <i>facility-type</i> キーワードについては、表 31-4 (P.31-14) を参照してください。 デフォルトは <code>local7</code> です。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

Syslog サーバを削除するには、`no logging host` グローバル コンフィギュレーション コマンドを使用して、Syslog サーバの IP アドレスを指定します。Syslog サーバへのログイングをディセーブルにするには、`no logging trap` グローバル コンフィギュレーション コマンドを入力します。

表 31-4 に、ソフトウェアでサポートされている UNIX システム機能を示します。これらの機能の詳細については、ご使用の UNIX オペレーティング システムの操作マニュアルを参照してください。

表 31-4 ログイング *facility-type* キーワード

<i>facility-type</i> キーワード	説明
<code>auth</code>	許可システム
<code>cron</code>	<code>cron</code> 機能
<code>daemon</code>	システム デーモン
<code>kern</code>	カーネル
<code>local0 ~ local7</code>	ローカルに定義されたメッセージ
<code>lpr</code>	ライン プリンタ システム
<code>mail</code>	メール システム
<code>news</code>	USENET ニュース
<code>sys9 ~ sys14</code>	システムで使用
<code>syslog</code>	システム ログ
<code>user</code>	ユーザ プロセス
<code>uucp</code>	UNIX から UNIX へのコピー システム

スマート ログイングの設定

スマート ログイングは、あらかじめ定義されているトリガーまたはユーザによって設定されたトリガーに基づいてパケット フローを取り込み、エクスポートするメカニズムを提供します。Cisco IOS Release 12.2(58)SE 以降のスイッチでは、次のイベントに対してスマート ログイングがサポートされています。

- DHCP スヌーピング違反
- ダイナミック ARP インスペクション違反
- IP ソース ガードで拒否されたトラフィック

- ACL で許可または拒否されたトラフィック

スマート ログイングを使用するには、スマート ログイングをイネーブルにする際に指定する NetFlow エクスポートを先に設定しておく必要があります。Cisco Flexible NetFlow の設定方法については、『Cisco IOS Flexible NetFlow Configuration Guide, Release 12.4T』を参照してください。

http://www.cisco.com.do/en/US/docs/ios/fnetflow/configuration/guide/12_4t/fnf_12_4t_book.html

スマート ログイング処理により、設定されたイベントに対して NetFlow パケットが作成され、外部の NetFlow 収集装置にそのパケットが送信されます。スマート ログイング カウンタは、記録されたパケットの数を表します。スイッチと NetFlow 収集装置の間でパケットが 1 つもドロップされなければ、この数は、収集装置に送信されたパケットの数と同じになります。

スマート ログイングは、スイッチ上でグローバルにイネーブルにします。その後、スマート ログイングされる個別のイベントを設定できます。

スマート ログイングのイネーブル化

スマート ログイングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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 2	<code>logging smartlog</code>	スマート ログイング機能をオンにします。
ステップ 3	<code>logging smartlog exporter exporter_name</code>	スマート ログ エクスポートを指定します。Flexible NetFlow CLI を使用して、あらかじめエクスポートを設定しておく必要があります。エクスポート名が存在しない場合、エラー メッセージが表示されます。デフォルトでは、スイッチが 60 秒ごとにデータを収集装置に送信します。
ステップ 4	<code>logging packet capture size packet_size</code>	(任意) エクスポートに送信されるパケットのサイズを設定します。指定できる範囲は 64 ~ 1024 バイト (4 バイト単位) です。デフォルトのサイズは 64 バイトです。 (注) パケット キャプチャ サイズを増やすと、1 パケットあたりのフロー レコード数が減少します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show logging smartlog</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP スヌーピング違反のスマート ログイングのイネーブル化

DHCP スヌーピングは、信頼できないポートで受信した DHCP パケットを代行受信して検査し、パケットを転送またはドロップします。ドロップされたパケットの内容を NetFlow 収集装置に送信するために、DHCP スヌーピング スマート ログイングをイネーブルにできます。DHCP スヌーピング スマート ログイングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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 2	<code>ip dhcp snooping vlan vlan-range smartlog</code>	DHCP スヌーピング スマート ログイングをイネーブルにする VLAN ID または VLAN 範囲を指定します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。

■ スマート ログイングの設定

	コマンド	目的
ステップ 4	<code>show ip dhcp snooping</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ダイナミック ARP インспекション違反のスマート ログイングのイネーブル化

ダイナミック ARP インспекションは、信頼できないポート上の ARP パケットを代行受信し、それらを転送する前に検証します。この機能は、ARP パケットが対象であること以外は DHCP スヌーピングと同じです。ダイナミック ARP インспекション ログイングは、`ip arp inspection log-buffer` グローバル コンフィギュレーション コマンドを使用して設定できます。デフォルトでは、ドロップされたすべてのパケットが記録されます。さらに、ログイング対象となっている同じパケットにスマート ログイングも適用するようにスイッチを設定して、それらのパケットの内容を NetFlow 収集装置に送信することもできます。

ダイナミック ARP インспекション スマート ログイングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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 2	<code>ip arp inspection smartlog</code>	現在ログイング対象となっているすべてのパケット (デフォルトはすべてのドロップ パケット) がスマート ログイングの対象でもあることを指定します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ip arp inspection</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

IP ソース ガード違反のスマート ログイングのイネーブル化

IP ソース ガードは、DHCP スヌーピングに関連したセキュリティ機能です。IP ソース ガードを使用して、トラフィックを IP 送信元アドレスまたは MAC アドレスに基づいてフィルタリングできます。指定されたアドレスや DHCP スヌーピングによって学習されたアドレス以外の送信元アドレスを持つ IP パケットはすべて拒否されます。IP ソース ガード スマート ログイングをイネーブルにして、拒否されたパケットの内容を NetFlow 収集装置に送信できます。

IP ソース ガード スマート ログイングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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 2	<code>interface interface-id</code>	インターフェイスを指定し、インターフェイス 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	<code>ip verify source smartlog</code>	IP ソース ガードによって拒否されるすべてのパケットに対して IP ソース ガード スマート ログイングをイネーブルにします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	<code>show ip verify source</code>	設定を確認します。出力には、スマート ログイングがこのインターフェイス上でイネーブルになっているかどうかを示されます。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート ACL の拒否または許可アクションのスマート ログイングのイネーブル化

スイッチでは、ポート ACL、ルータ ACL、および VLAN ACL がサポートされます。

- ポート ACL は、レイヤ 2 ポートに適用される IP または MAC ACL です。ポート ACL ではログイングはサポートされませんが、レイヤ 2 ポートに適用される IP ACL ではスマート ログイングがサポートされます。
- ルータ ACL は、レイヤ 3 ポートに適用される ACL です。ルータ ACL ではログイングがサポートされますが、スマート ログイングはサポートされません。
- VLAN ACL または VLAN マップは、VLAN に適用される ACL です。VLAN マップではログイングを設定できますが、スマート ログイングは設定できません。

許可または拒否 ACL を設定するとき、ログイングまたはスマート ログイングをアクセス リストの一部として設定できます。それにより、その ACL で許可または拒否されるすべてのトラフィックに対して適用されます。ログイングのタイプは、ACL を付加するポートのタイプによって決まります。スマート ログが設定された ACL をルータまたは VLAN に付加すると、ACL は付加されますが、スマート ログイングは有効になりません。レイヤ 2 ポートに付加された ACL にログイングを設定すると、そのログイング キーワードは無視されます。

ACL の許可条件や拒否条件を作成する際に、スマート ログ設定オプションを追加します。次に、番号制アクセス リストでスマート ログイングをイネーブルにする例を示します。

```
Switch(config)# access-list 199 permit ip any any smartlog
```

次に、名前付きアクセス リストでスマート ログイングをイネーブルにする例を示します。

```
Switch(config)# ip access-list extended test1
Switch(config-ext-nacl)# deny ip host 10.1.1.3 any smartlog
```

ログイング設定の表示

ログイング設定およびログ バッファの内容を表示するには、**show logging** 特権 EXEC コマンドを使用します。この場合に表示されるフィールドの詳細については、Cisco.com にある『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.4*』を参照してください。

スマート ログイング情報を表示するには、**show logging smartlog** コマンドを使用します。このコマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

