



## システム メッセージ ログिंगの設定

この章では、ブリッジにシステム メッセージ ログिंगを設定する方法について説明します。



(注)

---

この章で使用されるコマンドの構文と使用方法の詳細は、リリース 12.2 用の『Cisco IOS Configuration Fundamentals Command Reference』を参照してください。

---

この章の内容は、次のとおりです。

- システム メッセージ ログिंगの概要 (P.19-2)
- システム メッセージ ログिंगの設定 (P.19-3)
- ログング設定の表示 (P.19-13)

## システム メッセージ ログイングの概要

デフォルトでは、ブリッジはシステム メッセージと **debug** イネーブル EXEC コマンドからの出力をログイング プロセスに送信します。ログイング プロセスは、設定に応じてログイング バッファ、端末ライン、UNIX syslog サーバなどのさまざまな宛先へのログイング メッセージの配布を制御します。この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 形式は 4.3 BSD UNIX と互換性を持ちます。

ログイング プロセスを無効にすると、メッセージはコンソールにのみ送信されます。メッセージは生成の途中で送信されるため、メッセージと **debug** の出力はプロンプトや他のコマンドの出力と混在します。メッセージを生成したプロセスが終了した後で、コンソールにメッセージが表示されます。

コンソールと各送信先に表示されるメッセージのタイプを制御する場合、メッセージの重大度レベルを設定できます。ログ メッセージにタイムスタンプを適用したり、syslog 送信元アドレスを設定すると、リアルタイムのデバッグと管理を強化できます。

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、ブリッジの Command-line Interface (CLI; コマンドライン インターフェイス) を使用するか、適切に設定された syslog サーバにメッセージを保存します。ブリッジのソフトウェアは、syslog メッセージを内部バッファに保存します。Telnet を通じてブリッジにアクセスしたり、syslog サーバでログを表示したりすることでシステム メッセージをリモートに監視できます。

## システム メッセージ ログिंगの設定

この項では、システム メッセージ ログिंगを設定する方法について説明します。内容は次のとおりです。

- システム ログ メッセージの形式 (P.19-3)
- システム メッセージ ログिंगのデフォルト設定 (P.19-4)
- メッセージ ログिंगの無効化と有効化 (P.19-5)
- メッセージ表示先デバイスの設定 (P.19-5)
- ログ メッセージへのタイムスタンプの有効化と無効化 (P.19-6)
- ログ メッセージのシーケンス番号の有効化と無効化 (P.19-7)
- メッセージ重大度の定義 (P.19-8)
- 履歴テーブルと SNMP に送信される syslog メッセージの制限 (P.19-9)
- ログング レート制限の設定 (P.19-10)
- UNIX Syslog サーバの設定 (P.19-11)

### システム ログ メッセージの形式

システム ログ メッセージには最大 80 の文字とパーセント記号 (%) が使用できます。設定している場合は、オプション シーケンス番号またはタイムスタンプ情報を文字の前に指定できます。メッセージは次の形式で表示されます。

```
seq no:timestamp:%facility-severity-MNEMONIC:description
```

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** のどのグローバル設定コマンドを設定しているかにより異なります。

表 19-1 では、syslog メッセージの要素について説明します。

表 19-1 システム ログ メッセージの要素

要素	説明
<i>seq no:</i>	グローバル設定コマンド <b>service sequence-numbers</b> が設定されている場合にのみ、ログ メッセージにシーケンス番号がスタンプされます。  詳細は、「ログ メッセージのシーケンス番号の有効化と無効化」の項 (P.19-7) を参照してください。
<i>timestamp formats:</i> <i>mm/dd hh:mm:ss</i>  または <i>hh:mm:ss</i> (短い稼働時間)  または <i>dh</i> (長い稼働時間)	メッセージまたはイベントの日付と時間。この情報が表示されるのは、グローバル設定コマンド <b>service timestamps log [datetime   log]</b> が設定されている場合のみです。  詳細は、「ログ メッセージへのタイムスタンプの有効化と無効化」の項 (P.19-6) を参照してください。
<i>facility</i>	メッセージが参照するファシリティ (SNMP、SYS など)。ファシリティはハードウェア デバイス、プロトコル、システム ソフトウェアのモジュールのいずれかになります。システム メッセージのソースまたは原因を表します。

表 19-1 システム ログ メッセージの要素 (続き)

要素	説明
<i>severity</i>	メッセージの重大度を表す 0 ~ 7 の 1 桁のコード。重大度レベルの詳細は、表 19-3 (P. 19-9) を参照してください。
<i>MNEMONIC</i>	メッセージを固有に説明するテキスト文字列。
<i>description</i>	レポートされるイベントの詳細な情報を示すテキスト文字列。

次の例はブリッジの部分的なシステム メッセージを示します。

```
Syslog logging:enabled (0 messages dropped, 3 messages rate-limited, 0 flushes,
 0 overruns, xml disabled)
  Console logging:level debugging, 74 messages logged, xml disabled
  Monitor logging:level debugging, 0 messages logged, xml disabled
  Buffer logging:level debugging, 76 messages logged, xml disabled
  Logging Exception size (4096 bytes)
  Count and timestamp logging messages:disabled
  Trap logging:level informational, 78 message lines logged
Log Buffer (4096 bytes):
CHANGED:Interface Dot11Radio0, changed state to reset
*Mar  1 17:02:19.618:%LINK-3-UPDOWN:Interface Dot11Radio0, changed state to up
*Mar  1 17:14:21.520:%SYS-5-CONFIG_I:Configured from console by Cisco on vty0
(10.0.0.42)
*Mar  1 17:36:33.519:%SYS-5-CONFIG_I:Configured from console by Cisco on vty0
(10.0.0.42)
*Mar  1 17:56:48.596:%SYS-5-CONFIG_I:Configured from console by Cisco on vty0
(10.0.0.42)
*Mar  1 18:12:01.670:%SYS-5-CONFIG_I:Configured from console by Cisco on vty0
(10.0.0.42)
*Mar  1 19:35:39.710:%LINK-5-CHANGED:Interface Dot11Radio0, changed state to r
eset
*Mar  1 19:35:39.718:%LINK-3-UPDOWN:Interface Dot11Radio0, changed state to up
*Mar  1 20:52:06.007:%LINK-3-UPDOWN:Interface Dot11Radio0, changed state to do
wn
*Mar  1 20:52:06.022:%LINK-5-CHANGED:Interface Dot11Radio0, changed state to r
eset
*Mar  1 20:52:06.035:%LINK-3-UPDOWN:Interface Dot11Radio0, changed state to up
*Mar  1 23:47:38.851:%DOT11-6-ASSOC:Interface Dot11Radio0, Station 0002.8a29.
82e8 Associated KEY_MGMT [NONE]
*Mar  1 23:48:16.986:%DOT11-6-DISASSOC:Interface Dot11Radio0, Deauthenticating
Station 0002.8a29.82e8 Reason:Previous authentication no longer valid
```

## システム メッセージ ログिंगのデフォルト設定

表 19-2 は、システム メッセージ ログिंगのデフォルト設定を示しています。

表 19-2 システム メッセージ ログिंग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 ログिंग	有効
コンソールの重大度	debugging (および数値の低いレベル。表 19-3 (P. 19-9) を参照)
ログング バッファ サイズ	4096 バイト
ログング履歴サイズ	1 メッセージ
タイムスタンプ	無効
同期ログング	無効

表 19-2 システム メッセージ ログイングのデフォルト設定 (続き)

機能	デフォルト設定
ログイング サーバ	無効
syslog サーバ IP アドレス	設定されていません。
サーバ ファシリティ	Local7 (表 19-4 (P. 19-12) を参照)
サーバ 重大度	informational (および数値の低いレベル。表 19-3 (P. 19-9) を参照)

## メッセージ ログイングの無効化と有効化

メッセージ ログイングはデフォルトで有効に設定されています。コンソール以外の宛先にメッセージを送信する場合は、有効に設定されていなければなりません。有効になっている場合、ログメッセージはログイング プロセスに送信されます。このプロセスはメッセージを生成したプロセスとは非同期に指定された場所にメッセージをログイングします。

イネーブル EXEC モードから、次の手順に従ってメッセージ ログイングを無効にします。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>no logging on</b>	メッセージ ログイングを無効にします。
ステップ 3	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>  または <b>show logging</b>	入力内容を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。


ログイング プロセスを無効にするとブリッジの速度が遅くなる場合があります。これはメッセージがコンソールに書き込まれるまで待ってからプロセスで次の動作が行われるためです。ログイング プロセスが無効になっている場合、メッセージは生成された直後、多くの場合コマンド出力の途中でコンソールに表示されます。

グローバル設定コマンド **logging synchronous** もコンソールへのメッセージの表示に影響します。このコマンドを有効にすると、メッセージは Return キーを押した後に表示されます。詳細は、「[ログメッセージへのタイムスタンプの有効化と無効化](#)」の項 (P.19-6) を参照してください。

メッセージ ログイングを無効にした後で再度有効にする場合は、グローバル設定コマンド **logging on** を使用します。

## メッセージ表示先デバイスの設定

メッセージ ログイングを有効にしている場合、メッセージをコンソール以外に特定の場所に送信できます。イネーブル EXEC モードから、次のコマンド 1 つまたは複数を使用してメッセージを受信する場所を指定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>logging buffered [size] [level]</b>	<p>メッセージを内部バッファにログイングします。デフォルトのバッファ サイズは 4096 です。範囲は 4096 ~ 2147483647 バイトです。レベルには emergencies 0、alerts 1、critical 2、errors 3、warnings 4、notifications 5、informational 6、debugging 7 を指定します。</p> <p> (注) バッファ サイズは大きくしすぎないでください。これは、ブリッジが他の作業の分のメモリを消費してしまうためです。ブリッジのプロセッサの空きメモリを表示する場合は <b>show memory</b> イネーブル EXEC コマンドを使用します。ただし、この値は使用可能な最大メモリ量です。バッファ サイズをこの数値に設定しないでください。</p>
ステップ 3	<b>logging host</b>	<p>メッセージを UNIX syslog サーバ ホストにログイングします。</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>ログイング メッセージを受信する syslog サーバのリストを作成する場合は、このコマンドを複数回入力します。</p> <p>syslog サーバの設定手順の詳細は、「<a href="#">UNIX Syslog サーバの設定</a>」の項 (P.19-11) を参照してください。</p>
ステップ 4	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b>terminal monitor</b>	<p>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ログイングします。</p> <p>端末パラメータ設定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 メッセージを確認する場合は、各セッションでこの手順を実行する必要があります。</p>
ステップ 6	<b>show running-config</b>	入力内容を確認します。
ステップ 7	<b>copy running-config startup-config</b>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

グローバル設定コマンド **logging buffered** は、ログイング メッセージを内部バッファにコピーします。バッファは循環型であるため、バッファが一杯になると新しいメッセージにより古いメッセージが上書きされます。バッファにログイングされたメッセージを表示する場合は、**show logging** イネーブル EXEC コマンドを使用します。最初に表示されるメッセージは、バッファで最も古いメッセージです。バッファの内容をクリアするには、**clear logging** イネーブル EXEC コマンドを使用します。

コンソールへのログイングを無効にするには、グローバル設定コマンド **no logging console** を使用します。ファイルへのログイングを無効にするには、グローバル設定コマンド **no logging file [severity-level-number | type]** を使用します。

## ログ メッセージへのタイムスタンプの有効化と無効化

デフォルトでは、ログ メッセージにはタイムスタンプが設定されていません。

イネーブル EXEC モードから、次の手順に従ってログ メッセージへのタイムスタンプを有効にします。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>service timestamps log uptime</b>  または <b>service timestamps log datetime [msec] [localtime] [show-timezone]</b>	ログ タイムスタンプを有効にします。  最初のコマンドにより、ログ メッセージへのタイムスタンプが有効になり、システムがリポートしてからの時間が表示されます。  2 番目のコマンドによりログ メッセージへのタイムスタンプが有効になります。選択したオプションに応じて、タイムスタンプに日付、時間（ローカル時間帯を基準、単位 = ミリ秒）、タイムゾーン名を指定できます。
ステップ 3	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>	入力内容を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

デバッグとログ メッセージの両方に対してタイムスタンプを無効にするには、グローバル設定コマンド **no service timestamps** を使用します。

次の例は、グローバル設定コマンド **service timestamps log datetime** を有効にした場合のログイング表示の一部を示しています。

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

次の例は、グローバル設定コマンド **service timestamps log uptime** を有効にした場合のログイング表示の一部を示しています。

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

## ログ メッセージのシーケンス番号の有効化と無効化

複数のログ メッセージに同じタイムスタンプが付く可能性があるため、特定のメッセージを明確に参照する場合はメッセージにシーケンス番号を表示します。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。

イネーブル EXEC モードから、次の手順に従ってログ メッセージへのシーケンス番号を有効にします。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>service sequence-numbers</b>	シーケンス番号を有効にします。
ステップ 3	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>	入力内容を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

シーケンス番号を無効にする場合は、グローバル設定コマンド **no service sequence-numbers** を使用します。

次の例は、sequence numbers を有効にしたログイング表示の一部を示しています。

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

## メッセージ重大度の定義

メッセージの表示を特定のデバイスに制限できます。この場合、表 19-3 で説明するメッセージの重大度を指定します。

イネーブル EXEC モードから、次の手順に従ってメッセージの重大度を定義します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>logging console level</b>	メッセージのログイングをコンソールに制限します。  デフォルトでは、コンソールは数値の低いレベルのデバッグ メッセージを受け取ります (表 19-3 (P. 19-9) を参照)。
ステップ 3	<b>logging monitor level</b>	メッセージのログイングを端末回線に制限します。  デフォルトでは、端末回線は数値の低いレベルのデバッグ メッセージを受け取ります (表 19-3 (P. 19-9) を参照)。
ステップ 4	<b>logging trap level</b>	メッセージのログイングを syslog サーバに制限します。  デフォルトでは、syslog サーバは数値の低いレベルのデバッグ メッセージを受け取ります (表 19-3 (P. 19-9) を参照)。  syslog サーバの設定手順の詳細は、「UNIX Syslog サーバの設定」の項 (P.19-11) を参照してください。
ステップ 5	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 6	<b>show running-config</b>  または <b>show logging</b>	入力内容を確認します。
ステップ 7	<b>copy running-config startup-config</b>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。



(注) *level* を指定すると、そのレベルおよび数値的により低いレベルのメッセージがログイング先に表示されます。

コンソールへのログイングを無効にするには、グローバル設定コマンド **no logging console** を使用します。コンソールへのログイングを無効にするには、グローバル設定コマンド **no logging monitor** を使用します。syslog サーバへのログイングを無効にするには、グローバル設定コマンド **no logging trap** を使用します。

表 19-3 は、*level* キーワードを示しています。また最も重大なものから最も重大度の低いものまで対応する UNIX syslog 定義を並べています。



表 19-3 メッセージ ログिंगの level キーワード

level キーワード	レベル	説明	syslog 定義
<b>emergencies</b>	0	システムが不安定	LOG_EMERG
<b>alerts</b>	1	緊急の措置が必要	LOG_ALERT
<b>critical</b>	2	クリティカルな状況	LOG_CRIT
<b>errors</b>	3	エラー状態	LOG_ERR
<b>warnings</b>	4	警告状態	LOG_WARNING
<b>notifications</b>	5	通常だが重大な状態	LOG_NOTICE
<b>informational</b>	6	情報メッセージ	LOG_INFO
<b>debugging</b>	7	デバッグ メッセージ	LOG_DEBUG

ソフトウェアはその他に 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不具合に関するエラー メッセージ。**warnings** から **emergencies** の間のレベルで表示されます。これらのタイプのメッセージは、ブリッジの機能に影響することを意味しています。
- debug** コマンドの出力。**debugging** レベルで表示されます。debug コマンドは通常は、Technical Assistance Center (TAC) でのみ使用されます。
- インターフェイスの起動または停止への移行とシステムの再起動メッセージ。**notifications** レベルで表示されます。このメッセージは情報専用です。ブリッジの機能には影響しません。
- リロード要求と低プロセス スタック メッセージ。**informational** レベルで表示されます。このメッセージは情報専用です。ブリッジの機能には影響しません。

## 履歴テーブルと SNMP に送信される syslog メッセージの制限

グローバル設定コマンド **snmp-server enable trap** を使用して、syslog メッセージトラップの SNMP ネットワーク管理ステーションへの送信を設定している場合は、ブリッジ履歴テーブルに送信され、保存されるメッセージのレベルを変更できます。また履歴テーブルに保存されるメッセージ数も変更できます。

SNMP トラップは宛先への到着が保証されていないため、メッセージは履歴テーブルに保存されません。デフォルトでは、syslog トラップが有効になっていない場合でも、レベル **warning** および数値的に低いレベル (表 19-3 (P. 19-9) を参照) のメッセージが 1 つ、履歴テーブルに保存されます。

イネーブル EXEC モードから、次の手順に従ってレベルと履歴テーブルのサイズをデフォルトに変更します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>logging history level<sup>1</sup></b>	履歴ファイルに保存され、SNMP サーバに送信される syslog メッセージのデフォルト レベルを変更します。  level キーワードのリストは、表 19-3 (P. 19-9) を参照してください。  デフォルトでは、 <b>warnings</b> 、 <b>errors</b> 、 <b>critical</b> 、 <b>alerts</b> 、および <b>emergencies</b> のメッセージが送信されます。

	コマンド	目的
ステップ 3	<b>logging history size number</b>	履歴テーブルに保存できる syslog メッセージの数を指定します。  デフォルトでは 1 つのメッセージを保存します。指定範囲は 1 ~ 500 メッセージです。
ステップ 4	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	入力内容を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

1. 表 19-3 に、level キーワードと重大度を示します。SNMP を使用する場合、重大度の値は 1 ずつ増えます。たとえば、emergencies は 0 ではなく 1、critical は 2 ではなく 3 です。

履歴テーブルが一杯になると（グローバル設定コマンド **logging history size** で指定された最大メッセージ エントリ数に達すると）、最も古いメッセージがテーブルから削除され、新しいメッセージ エントリが保存できるようになります。

syslog メッセージのログिंगをデフォルト レベルに戻すには、グローバル設定コマンド **no logging history** 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に戻すには、グローバル設定コマンド **no logging history size** を使用します。

## ログング レート制限の設定

ブリッジが 1 秒あたりにログングするメッセージ数への制限を有効にできます。すべてのメッセージ、またはコンソールに送信されるメッセージに対して制限を有効にできます。また特定の重大度のメッセージを制限から除外することを指定できます。

イネーブル EXEC モードから、次の手順に従ってログング レート制限を有効にします。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>logging rate-limit seconds</b>  [all   console]  [except severity]	ログング レート制限を秒単位で有効にします。  • (オプション) すべてのログング、またはコンソールにログングされるメッセージにのみ制限を適用します。 • (オプション) 特定の重大度を制限から除外します。
ステップ 3	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b>copy running-config startup-config</b>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

レート制限を無効にするには、グローバル設定コマンド **no logging rate-limit** を使用します。

## UNIX Syslog サーバの設定

次の項では、4.3 BSD UNIX サーバの `syslog` デーモンを設定し、UNIX システム ログング ファシリティを定義する方法を説明します。

### メッセージの UNIX syslog デーモンへのログング

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 サーバに `syslog` デーモンを設定する必要があります。root でログインし、次の手順を実行します。



(注) UNIX syslog デーモンの最近のバージョンには、デフォルトでネットワークからデフォルトの `syslog` パケットを受け取らないものがあります。ご使用のシステムがこれに該当する場合、UNIX の `man syslogd` コマンドを使用して、リモート `syslog` メッセージのログングを有効にするために `syslog` コマンドラインに追加または削除する必要のあるオプションを確認してください。

**ステップ 1** ファイル `/etc/syslog.conf` に次のようなラインを追加します。

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

`local7` キーワードは、使用するログング ファシリティを指定します。ファシリティの詳細は、表 19-4 (P. 19-12) を参照してください。`debug` キーワードは `syslog` レベルを指定します。重大度についての詳細は、表 19-3 (P. 19-9) を参照してください。`syslog` デーモンはこのレベル、またはより重大なレベルのメッセージを次のフィールドで指定するファイルに送信します。ファイルはすでに存在している必要があり、`syslog` デーモンにはそのファイルへの書き込み権限が必要です。

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

```
$ touch /usr/adm/log/cisco.log
$ chmod 666 /usr/adm/log/cisco.log
```

**ステップ 3** 次のコマンドを入力して、`syslog` デーモンが新しい変更を読み取ることを確認します。

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

詳細は、UNIX システムの `man syslog.conf` と `man syslogd` コマンドを参照してください。

## UNIX システム ログング ファシリティの設定

外部デバイスにシステム ログ メッセージを送信するときに、そのメッセージを UNIX `syslog` ファシリティのいずれかから発信されたものとしてブリッジが特定するように設定できます。

イネーブル EXEC モードから、次の手順に従って UNIX システム ファシリティのメッセージ ログングを設定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>logging host</b>	UNIX syslog サーバの IP アドレスを入力すると、メッセージをそのサーバにログイングします。  ログイングメッセージを受信する syslog サーバのリストを作成する場合は、このコマンドを複数回入力します。
ステップ 3	<b>logging trap level</b>	メッセージのログイングを syslog サーバに制限します。  デフォルトでは、syslog サーバは informational 以下のレベルのメッセージを受信します。level キーワードは、表 19-3 (P. 19-9) を参照してください。
ステップ 4	<b>logging facility facility-type</b>	syslog ファシリティを設定します。facility-type キーワードは、表 19-4 (P. 19-12) を参照してください。  デフォルトは local7 です。
ステップ 5	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 6	<b>show running-config</b>	入力内容を確認します。
ステップ 7	<b>copy running-config startup-config</b>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

syslog サーバを削除するには、グローバル設定コマンド **no logging host** を使用して、syslog サーバ IP アドレスを指定します。syslog サーバへのログイングを無効にするには、グローバル設定コマンド **no logging trap** を入力します。

表 19-4 に Cisco IOS ソフトウェアでサポートされる 4.3 BSD UNIX システム ファシリティを示します。これらのファシリティの詳細は、UNIX オペレーティング システムのオペレーターズ マニュアルを参照してください。

表 19-4 ファシリティタイプキーワードのログイング

ファシリティタイプ キーワード	説明
<b>auth</b>	許可システム
<b>cron</b>	Cron ファシリティ
<b>daemon</b>	システム デーモン
<b>kern</b>	カーネル
<b>local0-7</b>	ローカルに定義されたメッセージ
<b>lpr</b>	ラインプリンタ システム
<b>mail</b>	メール システム
<b>news</b>	USENET ニュース
<b>sys9</b>	システム使用
<b>sys10</b>	システム使用
<b>sys11</b>	システム使用
<b>sys12</b>	システム使用
<b>sys13</b>	システム使用
<b>sys14</b>	システム使用
<b>syslog</b>	システム ログ

表 19-4 ファシリティタイプキーワードのログ (続き)

ファシリティタイプ キーワード	説明
<b>user</b>	ユーザ プロセス
<b>uucp</b>	UNIX 間コピー システム

## ログ設定の表示

現在のログ設定とログ バッファの内容を表示する場合は、**show logging** イネーブル EXEC コマンドを使用します。この表示のフィールドは、『Cisco IOS Configuration Fundamentals Command Reference for Release 12.2』を参照してください。

ログ履歴ファイルを表示するには、**show logging history** イネーブル EXEC コマンドを使用します。

