



概要

この章では、Syslog プロトコル (RFC 3164) によって定義されているシステム メッセージについて説明します。Syslog メッセージの形式の解説、および検討のためにシステム メッセージを取り込む方法について説明します。

この章の内容は、次のとおりです。

- [システム ログ メッセージの形式 \(p.1-2\)](#)
- [システム メッセージおよび履歴の取り込み \(p.1-6\)](#)

システム ログ メッセージの形式

システム ログ メッセージはパーセント記号 (%) から始まり、次の形式で表示されます。

- 常駐スイッチの Syslog 形式 (p.1-2)
- リモート ロギング サーバの Syslog 形式 (p.1-4)

常駐スイッチの Syslog 形式

常駐スイッチの Syslog の形式は、次のとおりです。

```
month dd hh:mm:ss switchname facility-severity-MNEMONIC description
```

または

```
month dd hh:mm:ss switchname facility-SLOTnumber-severity-MNEMONIC description
```

または

```
month dd hh:mm:ss switchname facility-STANDBY-severity-MNEMONIC description
```

例：

```
Nov 1 14:07:58 excal-113 %MODULE-5-MOD_OK: Module 1 is online
Nov 1 14:07:58 excal-113 %PORT-3-IF_UNSUPPORTED_TRANSCEIVER: Transceiver for interface
fc1/13 is not supported
.
```

表 1-1 システム ログ メッセージの形式の説明

要素	説明
month dd	エラーまたはイベントが発生した月日
hh:mm:ss	エラーまたはイベントが発生した時刻
switchname	スイッチ名
facility	エラーまたはイベントが発生したファシリティ (デーモン、カーネル、VSHD、または他のファシリティ)
severity	メッセージの重大度を表す 1 桁のコード (0 ~ 7)
MNEMONIC	システム メッセージを固有のものとして記述する文字列
#\$VDC #\$\$	Virtual Device Context (VDC; 仮想デバイス コンテキスト) ID を必要とするメッセージの説明に表示される、オプションの VDC ID
#\$VRF #\$\$	Virtual Routing and Forwarding (VRF; 仮想ルーティングおよび転送) ID を必要とするメッセージの説明に表示される、オプションの VRF ID
description	報告されているイベントの詳細を示す文字列

FACILITY は 2 つ以上の大文字から構成されるコードであり、システム メッセージが参照するファシリティを表します。ファシリティとは、ハードウェア デバイス、プロトコル、機能、またはシステム ソフトウェアのモジュールのことです。

システム メッセージの SEVERITY コードの範囲は 0 ~ 7 であり、状態の重大度を表します。0 が最も重度であり、3 が最も軽度です。表 1-2 に、重大度を示します。

表 1-2 システム メッセージの重大度

重大度	説明
0—緊急	システムは使用不能
1—アラート	ただちに対処が必要
2—クリティカル	クリティカルな状態
3—エラー	エラー状態
4—警告	警告状態
5—通告	正常であるが注意を要する状態
6—通知	通知メッセージのみ
7—デバッグ	デバッグ時にのみ表示

MNEMONIC は、システム メッセージを一意に識別するコードです。

Message-text は、システムの状態を表す文字列です。メッセージのこの部分には、端末ポート番号、ネットワーク アドレス、システム メモリのアドレス領域内の位置に対応するアドレスなど、発生したイベントに関する詳細情報が含まれることがあります。このような変数フィールドに含まれる情報はメッセージごとに異なるため、ここでは角括弧 ([]) で囲んだ短い文字列で表記します。たとえば 10 進数は [dec] のように表します。

表 1-3 に、変数フィールドの表記法、およびそのフィールド内の情報のタイプを示します。

表 1-3 システム メッセージの変数フィールドの表記法

表記	情報のタイプ
[dec]	10 進数
[hex]	16 進数
[char]	1 文字
[chars]	文字列

次のシステム メッセージは、変数フィールドの表記例です。

```
%MODULE-5-MOD_MINORSWFAIL: Module [dec] reported a failure in service [chars]
```

この例では、次が適用されます。

- ファシリティ コード = MODULE (モジュール固有のエラーであることを示します)
- 重大度 = 5 (通告)
- アラーム / イベント コード = MOD_MINORSWFAIL
- 問題の説明 = Module [dec] reported a failure in service [chars]
- [dec] は、このメッセージに関連するモジュール スロット番号です。
- [chars] は、この障害が発生しているサービス名です。

システム ログ メッセージはパーセント記号 (%) から始まり、次の形式で表示されます (表 1-4 を参照)。

リモート ロギング サーバの Syslog 形式

リモート ロギング サーバでの Syslog 形式は、次のとおりです。

```
month dd hh:mm:ss IP-addr-switch : year month day hh:mm:ss Timezone:
facility-severity-MNEMONIC description
```

または

```
month dd hh:mm:ss IP-addr-switch : year month day hh:mm:ssTimezone:
facility-SLOTnumber-severity-MNEMONIC description
```

または

```
month dd hh:mm:ss IP-addr-switch : year month day hh:mm:ss Timezone:
facility-STANDBY-severity-MNEMONIC description
```

例 :

```
sep 21 11:09:50 172.22.22.45 : 2005 Sep 04 18:18:22 UTC: %AUTHPRIV-3-SYSTEM_MSG:
ttyS1:
togetatrr: Input/output error - getty[28224]
switch resident syslog 2005 Sep 4 18:18:22 switch %AUTHPRIV-3-SYSTEM_MSG: ttyS1:
togetatrr: Input/output error - getty[28224]
time on switch : 2005 Sep 4 18:18:22 time on Loggng Server : Sep 21 11:09:50
fcl/13 is not supported
.
```

表 1-4 システム ログ メッセージの形式の説明

要素	説明
month dd	エラーまたはイベントが発生した月日
hh:mm:ss	エラーまたはイベントが発生した時刻
IP-addr-switch	スイッチの IP アドレス
facility	エラーまたはイベントが発生したファシリティ (デーモン、カーネル、VSHD、または他のファシリティ)
severity	メッセージの重大度を表す 1 桁のコード (0 ~ 3)
MNEMONIC	システム メッセージを固有のものとして記述する文字列
%%\$VDC #%%\$	Virtual Device Context (VDC; 仮想デバイス コンテキスト) ID を必要とするメッセージの説明に表示される、オプションの VDC ID
%%\$VRF #%%\$	Virtual Routing and Forwarding (VRF; 仮想ルーティングおよび転送) ID を必要とするメッセージの説明に表示される、オプションの VRF ID
description	報告されているイベントの詳細を示す文字列

FACILITY は 2 つ以上の大文字から構成されるコードであり、システム メッセージが参照するファシリティを表します。ファシリティとは、ハードウェア デバイス、プロトコル、機能、またはシステム ソフトウェアのモジュールのことです。

システム メッセージの SEVERITY コードの範囲は 0 ~ 3 であり、状態の重大度を表します。0 が最も重度であり、3 が最も軽度です。表 1-5 に、重大度を示します。

表 1-5 システム ログ メッセージの形式の説明

重大度	説明
0—緊急	システムは使用不能
1—アラート	ただちに対処が必要
2—クリティカル	クリティカルな状態
3—通告	正常であるが注意を要する状態

MNEMONIC は、システム メッセージを一意に識別するコードです。

Message-text は、システムの状態を表す文字列です。メッセージのこの部分には、端末ポート番号、ネットワーク アドレス、システム メモリのアドレス領域内の位置に対応するアドレスなど、発生したイベントに関する詳細情報が含まれることがあります。このような変数フィールドに含まれる情報はメッセージごとに異なるため、ここでは角括弧 ([]) で囲んだ短い文字列で表記します。たとえば 10 進数は [dec] のように表します。

表 1-6 に、変数フィールドの表記法、およびそのフィールド内の情報のタイプを示します。

表 1-6 システム メッセージの変数フィールドの表記法

表記	情報のタイプ
[dec]	10 進数
[hex]	16 進数
[char]	1 文字
[chars]	文字列

次のシステム メッセージは、変数フィールドの表記例です。

```
%AUTHPRIV-3-SYSTEM_MSG: AUTHPRIV [dec] reported a failure in service [chars]
```

この例では、次が適用されます。

- ファシリティ コード = AUTHPRIV (authpriv 固有のエラーであることを示します)
- 重大度 = 3 (通告)
- アラーム / イベント コード = SYSTEM_MSG
- 問題の説明 = Authpriv [dec] reported a failure in service [chars]
- [dec] は、このメッセージに関連するモジュール スロット番号です。
- [chars] は、この障害が発生しているサービス名です。

システム メッセージおよび履歴の取り込み

システム メッセージは、デフォルトでコンソールにすぐに表示されますが、内部ログ ファイルまたは Syslog サーバに転送することもできます。システム メッセージの重大度は、**logging** グローバル コンフィギュレーション コマンドによって割り当てられたキーワードに対応します。これらのキーワードによって、メッセージがどこに、どのレベルで出力されるのかが定義されます。設定したログ レベル以上の重大度に該当するシステム メッセージのみが記録されます。たとえばログ レベルを 3 (エラー) に設定すると、エラー、クリティカル、アラート、緊急のシステム メッセージが取得されますが、警告、通告、通知、デバッグのシステム メッセージは取得されません。

システム メッセージ ログの保存

logging logfile グローバル コンフィギュレーション コマンドではシステム メッセージを内部ログ ファイルにコピーし、ファイル サイズを任意に設定できます。ファイルに記録されたメッセージを表示するには、EXEC コマンド **show logging** を使用します。最初に表示されるメッセージは、バッファ内で最も古いメッセージです。バッファの現在の内容をクリアするには、**clear debug-logfile** コマンドを使用します。

Syslog サーバへのシステム メッセージのログ

logging host-name コマンドでは、ログ メッセージを受信する Syslog サーバ ホストを識別します。引数 *host-name* は、ホストの名前またはインターネット アドレスです。このコマンドを複数回実行すると、ログ メッセージを受信する Syslog サーバのリストを構築できます。**no logging host-name** コマンドでは、指定したアドレスの Syslog サーバが Syslog サーバのリストから削除されます。