CSS のロギング機能の使用

この章では、ロギングの有効化、ログ バッファの設定、アクティビティ情報の送信先の決定、およびログ メッセージの表示方法と内容について説明します。この章の内容は、特に指示のない限り、すべての CSS モデルに適用されます。

この章の主な内容は次のとおりです。

ロギングの概要

CSS では、CSS のデバッグや監視処理を支援するために、ログ メッセージが生成されます。デフォルトで、ブート ログ メッセージおよびサブシステム イベント ログ メッセージが、ハード ディスクまたはフラッシュ ディスクのログ ファイルに保存されます。これらのファイルの内容は、ASCII テキストで記録されます。CSS から、アクティブな CSS セッション、電子メール アドレスまたは別のホスト システムへログ メッセージを送信するように設定することもできます。

ログ ファイルの最大サイズは、ハード ディスクを使用するシステムの場合は 50MB、フラッシュ ディスクを使用するシステムの場合は 10MB です。

ブート ログ メッセージは、ブート プロセスの結果を表します。これらのメッセージは、boot.log ファイルに保存されます。

サブシステム ログ メッセージは、CSS の動作中に発生するサブシステム イベントを表します。このメッセージは、sys.log ファイルに保存されます。このファイルは、ログに記録するサブシステム イベントが初めて発生したときに生成されます。ログに記録するサブシステム メッセージは、CSS に設定したログ レベルによって決ります。デフォルトでは、すべてのサブシステムの、警告（warning）レベルのイベントがログに記録されます。警告レベルでは、サブシステムの fatal、alert、critical、error、および warning の各レベルのメッセージがログに記録されます。

サブシステム メッセージを、デフォルトの警告レベルとは異なるレベルでログに記録することもできます。レベルを指定すると、そのレベルおよびそれより上のレベルで発生したサブシステムのアクティビティが記録されます。

CSS では、informational メッセージの他に、notice、warning、error、critical、alert、および fatal の各メッセージがログに記録されます。

ログ ファイルを表示するには **show log** コマンドを使用し、ログ ファイルをコピーするには **copy log** コマンドを使用します。**show log** コマンドの詳細については、「ログ ファイルの表示」を参照してください。**copy log** コマンドの詳細については、「FTP または TFTP サーバへのログ ファイルのコピー」を参照してください。**show log** コマンドを使用するには、スーパーユーザ権限が必要です。

CSS には、デバッグとシステムの監視を行うためのロギング機能が用意されており、表 4-1 に示すようなログ ファイルが生成されます。

表 4-1　CSS ログ ファイル

ログ ファイル	ログ ファイルの出力先		記録内容
	デフォルトの場所	代替の場所	
boot.log	ハードディスクとコンソール、またはフラッシュ ディスクとコンソール	なし	ブート プロセスの結果
boot.bak	ハードディスクとコンソール、またはフラッシュ ディスクとコンソール	なし	ブート ログ ファイルのバックアップ。CSS が再度ブートされるたびに、現在のブート ログ ファイル名は boot.log.prev に変わり、新しいブート ログ ファイルが開始されます。ブート ログ ファイルの名前が変わると、既存のバックアップ ブート ログ ファイルは上書きされます。
sys.log	ハードディスク または フラッシュ ディスク	コンソール syslogd VTY1 VTY2	ユーザ定義のサブシステムまたは CLI コマンドに関するログ情報。デフォルトで、ロギングは有効に設定され、**warning** レベルでサブシステム **all** のログが記録されます。このログ情報を記録するために sys.log が作成されます。

表 4-1　CSS ログ ファイル（続き）

ログ ファイル	ログ ファイルの出力先		記録内容
	デフォルトの場所	代替の場所	
sys.log.prev	ハード ディスクまたはフラッシュ ディスク	コンソール syslogd VTY1 VTY2	システム ログ ファイルのバックアップ。システム ログ ファイルのサイズが最大（ハード ディスクを使用する CSS の場合は 50MB、フラッシュ ディスクを使用する CSS の場合は 10MB）の大きさに達すると、システム ログ ファイルの名前は sys.log.prev に変わり、新しいシステム ログ ファイルが開始されます。システム ログ ファイルの名前が変わると、既存のバックアップ システム ログ ファイルが上書きされます。CSS を再度ブートしても、ファイルが最大サイズに達するまで、既存のシステム ログ ファイルが使用されます。

CSS ロギングのクイック スタート

CSS のロギング機能を熟知している場合は、表 4-2 を参照して、ロギングを設定および有効にするために必要なコマンドとコマンド オプションを確認してください。

clear log コマンド以外のすべてのロギング コマンドは、設定モードで実行します。**clear log** コマンドは、スーパーユーザ モードのルート プロンプト（#）でだけ実行できます。

表 4-2　ロギングの設定と有効化

手順	ロギング オプション	例
1. ディスクのバッファ サイズを指定します。	*size*：ディスクのバッファ サイズ（0 ～ 64000）	**logging buffer 1000**
2. CSS のサブシステムを選択し、ログを記録するアクティビティのタイプ（デフォルトは **all**）およびレベル（デフォルトは **warning**）を決定します。	**subsystem**：次の有効なサブシステム **acl**、**all**、**app**、**boomerang**、**buffer**、**cdp**、**chassis**、**circuit**、**csdpeer**、**dhcp**、**dql**、**fac**、**flowagent**、**flowmgr**、**fp-driver**、**hfg**、**ipv4**、**keepalive**、**natmgr**、**netman**、**netmgr**、**nql**、**ospf**、**pcm**、**portmapper**、**proximity**、**publish**、**radius**、**redundancy**、**reporter**、**replicate**、**rip**、**security**、**ssl-accel**、**slr**、**sntp**、**sshd**、**syssoft**、**urql**、**vlanmgr**、**vpm**、**vrrp**、**wcc** **level**：次の有効なレベル **fatal-0**、**alert-1**、**critical-2**、**error-3**、**warning-4**、**notice-5**、**info-6**、**debug-7**	**logging subsystem rip level alert-1**

表 4-2　ロギングの設定と有効化（続き）

手順	ロギング オプション	例
3. サブシステム アクティビティのログを記録する場所（ディスク、ホスト、回線）を指定します。	**disk** *filename* : log ディレクトリの新しいファイル名または既存のファイル名 **host** *ip* または *host* : ホストの syslog デーモンの IP アドレスまたはホスト名 **log** *line*:CSS のアクティブ セッション	**logging disk stubs** **logging host 192.168.11.3** **logging host myhost.domain.com** **logging line vty1**
4. （省略可）CSS で指定レベルのログ メッセージを電子メール アドレスに送信できるようにします。	**sendmail** メール受信者の *email address*（電子メール アドレス） SMTP ホストの *IP address*（IP アドレス）または *hostname*（ホスト名） **level** : CSS に有効な次のレベル **fatal-0**、**alert-1**、**critical-2**、**error-3**、**warning-4**、**notice-5**、**info-6**、**debug-7**	**logging sendmail us@arrowpoint.com 172.16.6.58 critical-2**
5. ログ ファイルを表示します。	*filename* : 表示するログ ファイル	**show log stubs**

次の実行設定例は、表 4-2 のコマンドの入力結果を表しています。

```
!************************** GLOBAL ***************************

  logging buffer 1000
  logging subsystem rip level alert-1
  logging disk stubs
  logging sendmail us@cisco.com 172.16.6.58 critical-2
```

ロギング バッファのサイズの指定

ロギング バッファのサイズは、ディスクに出力されるまでメモリ内に格納される情報の量を指します。バッファのサイズを大きく設定すれば、CSS がディスクに内容を出力する回数が少なくなります。バッファのサイズの指定は、記録先をログ ファイルの宛先としてディスクに設定する場合だけに必要です。

ディスクのバッファ サイズを設定するには、**logging buffer** コマンドを使用します。バッファのサイズは、0 ～ 64000 バイトで指定します。デフォルトは 0 で、ログ内容がログ ファイルに直接送信されます。

たとえば、バッファのサイズを 1000 バイトに設定するには、次のように入力します。

```
(config)# logging buffer 1000
```

ログ内容をログ ファイルに直接送信するには、次のように入力します。

```
(config)# no logging buffer
```

サブシステムでのロギングの設定

ここでは、CSS サブシステムを選択して、そのアクティビティをログに記録する方法について説明します。内容は次のとおりです。

サブシステムのロギングの有効化と無効化

デフォルトでは、すべての CSS サブシステムのロギング レベルが warning-4 に設定されます。レベルを指定すると、そのレベルおよびそれより上のレベルで発生したサブシステムのアクティビティが記録されます。たとえば、情報メッセージ（info-6）を記録するよう指定した場合は、notice、warning、error、critical、alert、および fatal のエラー レベルのログも記録されます。

CSS のサブシステムを選択し、ログに記録するアクティビティのタイプを決定するには、**logging subsystem** コマンドを使用します。

サブシステムのロギングをデフォルトのロギング レベル（warning-4）にリセットするには、先頭に **no** を付けて logging コマンドを入力します。たとえば、次のように入力します。

```
(config)# no logging subsystem redundancy
```

次の例では、chassis サブシステムのロギングを critical-2 エラー レベルで有効にしています。この場合は、chassis に関する critical、alert、および fatal エラーがすべて記録されます。

```
(config)# logging subsystem chassis level critical-2
```

表 4-3 に、ロギングを有効にできる CSS サブシステムを定義します。

表 4-3　サブシステムのロギング

サブシステム	定義
acl	Access control list（ACL; アクセス コントロール リスト）
all（デフォルト）	すべての CSS サブシステム
app	Application Peering Protocol（APP）
boomerang	DNS Content Routing Agent（CRA; コンテンツ ルーティング エージェント）
buffer	バッファ マネージャ
cdp	Cisco Discovery Protocol（CDP; シスコ検出プロトコル）
chassis	シャーシ マネージャ
circuit	回線マネージャ
csdpeer	Content Server Database（CSD; コンテンツ サーバ データベース）ピア
dhcp	Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）
dql	Domain Qualifier List（DQL; ドメイン修飾子リスト）
fac	Flow Admission Control（FAC; フロー アドミッション制御）
flowagent	フロー エージェント
flowmgr	フロー マネージャ サブシステム
fp-driver	Fathpath ドライバ
hfg	Header Field Group（HFG; ヘッダー フィールド グループ）
ipv4	Internet Protocol version 4（IPv4; インターネット プロトコル バージョン 4）
keepalive	キープアライブ
natmgr	NAT マネージャ
netman	ネットワーク管理
nql	Network Qualifier List（NQL; ネットワーク修飾子リスト）
ospf	Open Shortest Path First（OSPF）プロトコル

表 4-3　サブシステムのロギング（続き）

サブシステム	定義
pcm	Proximity CAPP Messaging（PCM; プロキシミティ CAPP メッセージング）
portmapper	ポート マッパー
proximity	プロキシミティ
publish	パブリッシュ
radius	Remote Authentication Dial-In User Server（RADIUS）
redundancy	CSS 冗長性
reporter	レポーター
replicate	コンテンツ レプリケーション
rip	Routing Information Protocol（RIP; ルーティング情報プロトコル）
security	セキュリティ マネージャ
slr	セッション レベル冗長性
sntp	Simple Network Time Protocol（SNTP; 簡易ネットワーク タイム プロトコル）
sshd	SSHD
ssl-accel	Secure Socket Layer（SSL）アクセラレーション
syssoft	システム ソフトウェア
urql	Uniform Resource Locator Qualifier List（URQL; URL 修飾子リスト）
vlanmgr	VLAN マネージャ
vpm	仮想パイプ マネージャ
vrrp	仮想ルータ冗長性プロトコル
wcc	Web 対話制御

表 4-4 に、指定した CSS サブシステムで設定できるロギング レベルを示します。このレベルは、最も重大度が高い fatal-0 レベルのエラーから最も低い info-6 レベルのエラーへと、重大度の順にリストされています。

表 4-4　サブシステムのロギング レベル

レベル	定義
fatal-0	重大エラーだけ
alert-1	アラート エラー。重大エラーを含む。
critical-2	クリティカル エラー。アラート エラーと重大エラーを含む。critical レベルでは、次のトラップ イベントが記録されます（リンクの停止、コールド スタート、ウォーム スタート、サービスの停止、サービスの一時停止）。
error-3	一般エラー。クリティカル エラー、アラート エラーおよび重大エラーを含む。
warning-4（デフォルト）	警告メッセージ。このレベルよりも重大なエラーをすべて含む（error、critical、alert、および fatal）。
notice-5	注意メッセージ。すべてのトラップ イベント（critical レベルで記録されるイベントは除く）、および info と debug 以外のこのエラーよりも重大なレベルのエラーをすべて含む。
info-6	通知メッセージ。debug 以外のこのエラーよりも重大なレベルのエラーを含む。
debug-7	デバッグ メッセージ。他のすべてのエラー レベルを含む。debug-7 のログ レベルを指定すると、CSS のパフォーマンスが低下することがあります。このオプションを入力すると、次のようなメッセージが表示されます。 `Logging at the debug level may degrade the CSS performance. Continue, [y/n]:` ログ レベルを debug7 に設定する場合は、**y** を入力します。debug-7 ログ レベルの実行を取り消す場合は **n** を入力します。

ロギング レベルとサブシステムを指定したログ メッセージの設定

サブシステムのログ メッセージを特定のログ レベルに定義するには、**cliLogMessage subsystem** コマンドを使用します。このグローバル設定モードのコマンドのシンタックスは次のとおりです。

cliLogMessage subsystem *name* “*message*” **level** *level*

変数とオプションは次のとおりです。

- *name*：CSS　サブシステムの名前。いずれかのサブシステム名を入力します（表 4-3 参照）。サブシステムのリストを参照するには、次のように入力します。

  ```
  cliLogMessage subsystem ?
  ```

- **level** *level* ：メッセージのログ レベル。0 ～ 7 のいずれかのレベルを入力します（表 4-4 参照）。レベルのリストを参照するには、次のように入力します。

  ```
  cliLogMessage subsystem name “message” level ?
  ```

ACL アクティビティのロギング

ACL アクティビティをロギングするように設定すると、句と ACL に一致するパケットのイベントがロギングされます。ログ情報は、**logging** コマンドで指定した場所に送信されます。

特定の ACL 句にロギングを設定する前に、必ずグローバルな ACL ロギングを有効にしてください。ACL ロギングをグローバルに有効にするには、設定モードで **logging subsystem acl level debug-7** コマンドを使用します。

ACL 句のロギングを設定するには、次の操作を行います。

1. ロギングを有効にする対象の ACL モードに入ります。

   ```
   (config)# acl 7
   (config-acl[7])#
   ```

2. 次の方法でロギングを有効にします。

   - 新しい句に対してロギングを有効にするには、句の最後に **log** オプションを入力します。たとえば、次のように入力します。

     ```
     (config-acl[7])# clause 1 deny udp any eq 3 destination any eq
     3 log
     ```

- 既存の句に対してロギングを有効にするには、**clause log enable** コマンドを入力します。

```
(config-acl[7])# clause 1 log enable
```

特定の句の ACL ロギングを無効にするには、次のように入力します。

```
(config-acl[7])#) clause 1 log disable
```

すべての ACL 句に対するロギングをグローバルに無効にするには、次のように入力します。

```
(config)# no logging subsystem acl
```

電子メール アドレスへのログ メッセージの送信

サブシステムのログ アクティビティを電子メール アドレスに送信するには、**logging sendmail** コマンドを使用します。このグローバル設定モードのコマンドのシンタックスは次のとおりです。

logging sendmail *email_address ip_address level* {*domain*}

変数は次のとおりです。

- *email_address*：受信者の電子メール アドレス。電子メール アドレスは、大文字小文字を区別して、1 ～ 30 文字以内のテキスト文字列を引用符で囲まずに入力します。
- *IP_address*：SMTP ホストの IP アドレス。IP アドレスは、ドット付き 10 進表記（192.168.11.1 など）で入力します。
- *level*：ログを記録する情報の種類。有効なレベルについては、表 4-4 を参照してください。
- *domain*：（省略可）SMTP ホストのドメイン名。64 文字以内のテキスト文字列を引用符で囲まずに入力します（arrowpoint.com など）。ドメイン名の前に @ 記号を挿入しないでください。@ 記号はドメイン名の前に自動で追加されます。

電子メール アドレスへのロギングを停止するには、次のように入力します。

```
(config)# no logging sendmail email_address
```

ログ ファイルの場所の指定

サブシステムのアクティビティのログが記録される場所を指定するには、**logging** コマンドを使用します。ログ ファイルの格納先には、次の場所を指定できます。

- **disk** *filename*：ディスクの log ディレクトリの新しいファイル名または既存のファイル名
- **host** *ip* または *host*：ホストの syslog デーモンの IP アドレスまたはホスト名
- **log** *line*：CSS のアクティブ セッション

CSS ディスクへログを書き込むと、CSS のパフォーマンスが低下することがあります。ログを頻繁に（1 日あたり数百のログ メッセージ）ディスクに書き込む場合には、ログをハード ディスクに出力し、その他の全システム ファイルをフラッシュ ディスクに格納する設定が、信頼性の点で最も確実です。一般に、フラッシュ ディスクは情報を永続的に格納する最も信頼性が高い手段です。一方ハード ディスクは、情報を頻繁に書き込む場合の格納手段として、現時点で利用可能などのフラッシュ ディスクよりも適しています。

CSS ディスクに過剰な書き込みが行われないようにするには、ディスクの sys.log ファイルへのロギングを無効にしてください（「ディスクの sys.log ファイルへのロギングの無効化」参照）。CSS ログ情報を他の場所にある sys.log ファイルに継続的に送ることもできます。この方法を行うには、**logging host** コマンドでログ情報をホスト システムの syslog デーモンへ送信するか（「ログ ファイルの出力先としてのホストの指定」参照）、**logging line** コマンドでログ情報をアクティブな CSS 回線（「ログ ファイルの出力先としての回線の指定」参照）に送ります（この場合には、ログ情報は保存されません）。

ここでは、次の内容について説明します。

ディスク上のログ ファイルの指定

CSS ディスクの特定のファイルにログ情報を送信するには、**logging disk** コマンドを使用します。ログ ファイルの名前を指定します。名前は 0 ～ 32 文字以内のテキスト文字列で入力します。ファイル名は、新しく指定することも、既存の名前を使用することもできます。

たとえば、次のように入力します。

```
(config)# logging disk stubs
```

logging disk コマンドを指定すると、次の処理が行われます。

- sys.log へのデフォルトのログ情報の書き込みが停止する。
- ディスクの log ディレクトリに、指定したファイル名でログ ファイルが作成される。
- 指定したサブシステムおよびレベルの情報がログ ファイルに送信される。

ディスクでは一度に 1 つのログ ファイルしかアクティブにできません。サブシステムの情報をディスクの別のログ ファイルに送信するには、logging disk コマンドを別のファイル名を指定して再度実行します。

注意　CSS ディスクへログを書き込むと、CSS のパフォーマンスが低下することがあります。

指定したファイルへのロギングを停止し、CSS の sys.log ファイルへのロギングを再度有効にするには、次のコマンドを入力します。

```
(config)# no logging disk
```

ディスクの sys.log ファイルへのロギングの無効化

sys.log ファイルへのロギングを無効化すると、CSS ディスク（フラッシュ ディスクなど）に過剰な書き込みを行わないようにする場合や、CSS のパフォーマンスを向上させる場合に役立ちます。CSS ディスク（ハード ディスクまたはフラッシュ ディスク）の sys.log ファイルへのロギングを無効にするには、**logging to-disk** コマンドを使用します。

logging to-disk コマンドには、次のオプションがあります。

- **logging to-disk disable** : CSS ディスクの CSS sys.log ファイルへのデフォルトのログ情報の書き込みを無効にする。**logging to-disk disable** コマンドは sys.log ファイルだけに影響し、**logging disk** コマンドで指定したディスクのログ ファイルには影響しません。このコマンドを実行しても、**logging disk** *filename* コマンドを使用して、CSS ディスクの特定のファイル名にログ情報を送ることができます。CSS ディスクへのロギングをすべて無効にするには、最初に **no logging disk** コマンドを入力してから、**logging to-disk disable** コマンドを入力します。**no logging disk** コマンドを入力しても、sys.log ファイルへのロギングは再度有効になりません。sys.log ファイルを再度アクティブにするには、**logging to-disk enable** コマンドを指定する必要があります。
- **logging to-disk enable** : ディスクへのロギングを元に戻し、CSS sys.log ファイルへのデフォルトのログ情報の書き込みを再開する。

logging to-disk disable または **logging to-disk enable** コマンドを実行すると、コマンドを有効にするために CSS を再度ブートするように指示されます。

（注） CSS ログ情報を他の場所にある sys.log ファイルに継続的に送ることもできます。ログ情報を他の場所に送るには、**logging host** コマンドでホスト システムの syslog デーモンへ送るか（「ログ ファイルの出力先としてのホストの指定」参照）、**logging line** コマンドでアクティブな CSS 回線へ送ります（この場合には、ログ情報は保存されません）（「ログ ファイルの出力先としての回線の指定」参照）。

CSS ディスク（フラッシュ ディスクまたはハード ディスク）の CSS sys.log ファイルへのロギングを無効にするには、次のコマンドを入力します。

```
(config)# logging to-disk disable
```

CSS ディスクへのロギングを再開するには、次のコマンドを入力します。

```
(config)# logging to-disk enable
```

ログ ファイルの出力先としてのホストの指定

ホスト システムで稼働する syslog デーモンに CSS ログ情報を送信するには、**logging host** コマンドを使用します。syslog デーモンは、ホスト システムで CSS ログ メッセージを受信して表示します。

この設定モードのコマンドのシンタックスは次のとおりです。

logging host *ip_or_host* **facility** *number* **log-level** *number*

このコマンドのオプションと変数は次のとおりです。

- *ip_or_host* : ホストの syslog デーモンのアドレスを指定する。ドット付き 10 進表記の IP アドレス（192.168.11.1 など）またはニーモニック ホスト名（myhost.mydomain.com など）を入力します。
- **facility** *number* : syslog デーモンのファシリティ レベルを指定する。ファシリティは、印刷、電子メール、ネットワークなどのサービス エリアと考えられます。0 ～ 7 の数値を入力します。syslog デーモンとファシリティ レベルの詳細については、使用している syslog デーモンのマニュアルを参照してください。
- **log-level** *number* : ホスト上の syslog デーモンに送られる CSS サブシステム ログ メッセージのレベルを指定する。有効なログ レベルには、fatal-0、alert-1、critical-2、error-3、warning-4（デフォルト）、notice-5、info-6、debug-7 があります。ロギング レベルは、最も重大度が高い fatal-0 レベルのエラーから最も低い info-6 レベルのエラーへと、重大度の順にリストされています。各種のロギング レベルの定義については、表 4-4 を参照してください。

  logging host log-level *number* は、**logging subsystem** コマンドに設定したログ レベルに等しいか、それ以下でなければなりません（詳細は、「サブシステムでのロギングの設定」を参照してください）。ログ レベル値がロギング サブシステム レベルより小さいと、CSS は **log-level** オプションで指定したメッセージ レベルだけを送ります。ログ レベルがロギング サブシステム レベルより大きいと、CSS は **logging subsystem** オプションで指定したメッセージ レベルだけを送ります。

logging host コマンドを入力しても、ログ情報は CSS ディスク（ハード ディスクまたはフラッシュ ディスク）の sys.log ファイルへ継続して送信されます。CSS ディスクの sys.log ファイルへのロギングを無効にするには、**logging to-disk disable** コマンドを使用します（「ディスクの sys.log ファイルへのロギングの無効化」参照）。

たとえば、ファシリティ レベルが 3、ログ レベルが error-3 に設定されている、IP アドレスが 192.168.11.1 のホストへログ情報を送るには、次のように入力します。

```
(config)# logging host 192.168.11.1 facility 3 log-level error-3
```

ホストへのロギングをオフにするには、次のように入力します。

```
(config)# no logging host
```

ログ ファイルの出力先としての回線の指定

ログ情報をアクティブな CSS セッションに送信するには、**logging line** コマンドを使用して、CSS で有効なログ回線を指定します。回線は 32 文字以内の大文字小文字を区別したテキスト文字列で入力します。

logging line コマンドを入力しても、ログ情報は CSS ディスク（ハード ディスクまたはフラッシュ ディスク）の sys.log ファイルへ継続して送信されます。CSS ディスクの sys.log ファイルへのロギングを無効にするには、**logging to-disk disable** コマンドを使用します（「ディスクの sys.log ファイルへのロギングの無効化」参照）。

アクティブな CSS 回線のリストを表示するには、次に示すように **logging line** コマンドを入力します。アスタリスク（*）は、現在のセッションを示しています。

```
(config)# logging line ?

console      Login Name:  Location:local
*vty1        Login Name:  admin Location:10.0.3.35
```

たとえば、サブシステム情報をモニタに送信する場合は、次のように入力します。

```
(config)# logging line vty1
```

ロギングをオフにするには、次のように **no logging line** コマンドを入力します。

```
(config)# no logging line vty1
```

CLI コマンドのロギング

CSS で実行したすべての CLI コマンドを追跡する場合は、sys.log ファイルにログを記録できます。CLI コマンドのログを記録するには、次の手順を実行します。

1. netman サブシステムのロギング レベルを info-6 に設定します。次のように入力します。

   ```
   (config)# logging subsystem netman info-6
   ```

2. **logging commands enable** コマンドを実行し、コマンドのロギングを有効にします。このコマンドを実行すると、それぞれの CLI コマンドの内容が sys.log ファイルに記録されるようになります。次のように入力します。

   ```
   (config)# logging commands enable
   ```

sys.log ファイルへの CLI コマンドのロギングを無効にするには、次のように入力します。

```
(config)# no logging commands
```

ログ ファイルの表示

ログ　ファイルまたはトラップ ログ ファイルの内容、全ログ ファイルのリスト、CSS ファシリティのロギングの状態を表示するには、**show log** コマンドを使用します。ユーザ モードを含むすべてのモードで **show log** コマンドを使用できます。

show log コマンドを使用してログ アクティビティを現在のセッションに送信しているときに、ログ アクティビティの送信を停止するには、端末またはワークステーションでいずれかのキーを押します。**show log** コマンドは、**logging line** コマンドと同じように機能します。この 2 つのコマンドは同時に実行できません。

ここでは、次の内容について説明します。

ログ アクティビティの表示

ログ アクティビティを現在のセッションに送信するには（ログ ファイルまたはトラップ ログ ファイルの内容を表示するには）、**show log** コマンドとオプションを使用します。ユーザ モードを含むすべてのモードで **show log** コマンドを使用できます。

show log コマンドのシンタックスは次のとおりです。

show log {*log_filename*|**traplog** {**tail** *lines*} {**line-numbers**}}

このコマンドのオプションと変数は次のとおりです。

- *log_filename*：ログ　ファイルの名前を指定する。スペースを含まないテキスト文字列を引用符で囲まずに入力します。ログ ファイルとその日付のリストを表示するには、**show log ?** と入力します。
- **traplog**：（省略可）発生したすべての SNMP トラップを表示する。トラップ ログ ファイルは、ログ ディレクトリにある ASCII ファイルで、汎用トラップおよびエンタープライズ トラップが含まれます。デフォルトでは、次のイベントによりレベル critical-2 のメッセージが生成されます。
  - リンク アップ
  - リンク ダウン

- コールド スタート
- ウォーム スタート
- サービスの停止
- サービスの一時停止

上記以外の SNMP トラップでは、レベル notice-5 のメッセージが生成されます。

トラップ ログ ファイルのサイズが最大の大きさ（ハード ディスクを使用する CSS の場合は 50MB、フラッシュ ディスクを使用する CSS の場合は 10MB）に達すると、トラップ ログ ファイルの名前が traplog.prev に変わります。このファイルは、バックアップ ファイルとして保存され、新しいトラップ ログ ファイルが作成されます。トラップ ログ ファイルの名前が変わると、既存のバックアップ トラップ ログ ファイルは上書きされます。CSS を再度ブートしても、最大サイズに達するまで、既存のトラップ ログ ファイルが使用されます。

（注） CSS では、トラップを無効にした状態でも、トラップを通常生成するイベントでログ メッセージが生成されます。

- **tail** *lines*：（省略可）ログ ファイルの最後（最新の部分）を表示する。ログ ファイルの内容は、ファイルの先頭から表示されます。ファイルの先頭には古いメッセージが記録され、最後には最新のメッセージが記録されます。ログ ファイルの最後を開始点として表示する行数（最大 1000 行）を指定できます。1 ～ 1000 の数値を入力します。
- **line-numbers**：（省略可）ログ ファイルの内容を表示するときに行番号が表示されるようにする。

ログ アクティビティを現在のセッションに送信するには、次のように入力します。

```
# show log
Displaying Log events.
Press any key to abort...
APR 14 16:28:09 5/1 2398 NETMAN-7: HTTPC:HTTPC_Open:
ERROR->connect <-1,0> <192.20.1.7> <80>
APR 14 16:28:15 5/1 2399 NETMAN-7: HTTPC:HTTPC_Open:
ERROR->connect <-1,0> <192.20.1.7> <80>
APR 14 16:28:21 5/1 2400 NETMAN-7: HTTPC:HTTPC_Open:
ERROR->connect <-1,0> <192.20.1.7> <80>
APR 14 16:28:27 5/1 2401 NETMAN-7: HTTPC:HTTPC_Open:
ERROR->connect <-1,0> <192.20.1.7> <80>
```

特定のログ ファイルの情報を表示するには、有効なログ ファイル名を指定して **show log** コマンドを入力します。たとえば、次のように入力します。

```
# show log stubs
SEP 22 09:59:18 5/1 918 NETMAN-7: SNMP:SET RSP (3803)
SEP 22 09:59:53 5/1 919 NETMAN-7: SNMP:SET  (3804)
SEP 22 09:59:53 5/1 920 NETMAN-7: SNMP:  1
apLogHostIpAddress.[1.2.3.4] VT_IPADDRESS  <1.2.3.4>
SEP 22 09:59:53 5/1 921 NETMAN-7: SNMP:  2
apLogHostIpAddress.[1.2.3.4] VT_IPADDRESS  <1.2.3.4>
```

たとえば、sys.log ファイルの内容を表示するには、次のように入力します。

```
(config)# show log sys.log
```

ファイル最後の最新部分を表示するには、**show log** コマンドに **tail** オプションを使用します。たとえば、sys.log ファイルの最新 500 行を表示するには、次のように入力します。

```
(config)# show log sys.log tail 500
```

ログ リストの表示

すべてのログ ファイルのリストを表示するには、**show log-list** コマンドを使用します。ユーザ モードを含むすべてのモードで **show log-list** コマンドを使用できます。たとえば、次のように入力します。

```
(config)# show log-list
```

ログ状態の表示

CSS の各種ファシリティのロギング状況を表示するには、**show log-state** コマンドを使用します。ユーザ モードを含むすべてのモードで **show log-state** コマンドを使用できます。たとえば、次のように入力します。

```
(config)# show log-state
```

表 4-5 に、**show log-state** コマンドで表示されるフィールドについて説明します。

表 4-5　show log-state コマンドのフィールド

フィールド	説明
サブシステム：	
acl	アクセス コントロール リスト（ACL）
app	Application Peering Protocol（APP）
boomerang	DNS コンテンツ ルーティング エージェント（CRA）
buffer	バッファ マネージャ
cdp	シスコ検出プロトコル（CDP）
chassis	シャーシ マネージャ
circuit	回線マネージャ
csdpeer	コンテンツ サーバ データベース（CSD）ピア
dhcp	ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）
dql	ドメイン修飾子リスト（DQL）
fac	フロー アドミッション制御（FAC）
flowagent	フロー エージェント
flowmgr	フロー マネージャ サブシステム
fp-driver	Fathpath ドライバ
hfg	ヘッダー フィールド グループ（HFG）
ipv4	インターネット プロトコル バージョン 4（IPv4）
keepalive	キープアライブ
natmgr	NAT マネージャ

表 4-5　show log-state コマンドのフィールド（続き）

フィールド	説明
netman	ネットワーク管理
nql	ネットワーク修飾子リスト（NQL）
ospf	Open Shortest Path First（OSPF）
pcm	プロキシミティ CAPP メッセージング（PCM）
portmapper	ポート マッパー
proximity	プロキシミティ
publish	パブリッシュ
radius	Remote Authentication Dial-In User Server（RADIUS）
redundancy	CSS 冗長性
reporter	レポーター
replicate	コンテンツ レプリケーション
rip	ルーティング情報プロトコル（RIP）
security	セキュリティ マネージャ
slr	セッション レベル冗長性
sntp	簡易ネットワーク タイム プロトコル（SNTP）
sshd	SSHD
ssl-accel	Secure Socket Layer（SSL）アクセラレーション
syssoft	システム ソフトウェア
urql	URL 修飾子リスト（URQL）
vlanmgr	VLAN マネージャ
vpm	仮想パイプ マネージャ
vrrp	仮想ルータ冗長性プロトコル
wcc	Web 対話制御
レベル：	
debug	すべてのエラーとメッセージのログを記録します（詳細）。
info	情報メッセージのログを記録します（notice レベルのエラーを含む）。

表 4-5　show log-state コマンドのフィールド（続き）

フィールド	説明
notice	通知メッセージのログを記録します（warning レベルのエラーを含む）。
warning	（デフォルト）警告エラーのログを記録します（error レベルのエラーを含む）。
error	一般エラーのログを記録します（critical レベルのエラーを含む）。
critical	クリティカル エラーのログを記録します（alert レベルのエラーを含む）。
alert	アラート エラーのログを記録します（fatal レベルのエラーを含む）。
fatal	重大エラーだけのログを記録します（簡略）。
ファイル：	
Filename：	ログ ファイルの名前
Current size：	ログ ファイルの現在のサイズ
Log to Disk	ディスク（フラッシュ ディスクまたはハード ディスク）へのロギングが有効かどうかを示します。

FTP または TFTP サーバへのログ ファイルのコピー

CSS から File Transfer Protocol（FTP; ファイル転送プロトコル）または Trivial File Transfer Protocol（TFTP; トリビアル ファイル転送プロトコル）サーバにログファイルをコピーするには、**copy log** コマンドを使用します。**copy log** コマンドは、スーパーユーザ モードでだけ実行できます。

ここでは、次の内容について説明します。

FTP サーバへのログ ファイルのコピー

ログ ファイルを FTP サーバにコピーするには、**copy log ftp** コマンドを使用します。ログ ファイルを CSS から FTP サーバにコピーする前に、FTP サーバの IP アドレス、ユーザ名、およびパスワードを格納する FTP レコード ファイルを作成します。FTP レコードの設定については、第 1 章「CSS ソフトウェアの管理」を参照してください。

このコマンドのシンタックスは次のとおりです。

copy log *logfilename* **ftp** *ftp_record filename*

このコマンドのオプションと変数は次のとおりです。

- *logfilename*：CSS のログ ファイルの名前。スペースを含まない 32 文字以内の文字列を、引用符で囲まずに指定します。ログ ファイルのリストを表示するには、**copy log ?** コマンドを入力します。
- **ftp**：FTP サーバにログ ファイルをコピーする。
- *ftp_record*：FTP サーバの IP アドレス、ユーザ名、およびパスワードを格納する FTP レコード ファイルの名前を指定します。スペースを含まない 16 文字以内のテキスト文字列を、引用符で囲まずに入力します。FTP レコードを作成する場合は、第 1 章「CSS ソフトウェアの管理」を参照してください。
- *filename*：FTP サーバ上のファイルに割り当てる名前。フルパスで指定します。スペースを含まない 32 文字以内のテキスト文字列を、引用符で囲まずに入力します。

たとえば、*starlog* ログ ファイルを FTP サーバにコピーするには、次のように入力します。

```
# copy log starlog ftp ftpserv1 starlogthurs
```

TFTP サーバへのログ ファイルのコピー

ログ ファイルを TFTP サーバにコピーするには、**copy log tftp** コマンドを使用します。このコマンドのシンタックスは次のとおりです。

copy log *log_filename* [**ftp** *ftp_record*|**tftp** *ip_or_host*] *filename*

このコマンドのオプションと変数は次のとおりです。

- *log_filename* : CSS のログ ファイルの名前。スペースを含まない 32 文字以内の文字列を、引用符で囲まずに指定します。ログ ファイルのリストを表示するには、**copy log ?** コマンドを入力します。
- **tftp** : TFTP サーバにログ ファイルをコピーする。
- *ip_or_host* : ファイルを受信する TFTP サーバの IP アドレスまたはホスト名。ドット付き 10 進表記の IP アドレス（192.168.11.1 など）またはニーモニック ホスト名（myhost.mydomain.com など）を入力します。ホスト名を使用する場合は、その前に **host** コマンドを実行して、ホスト テーブルを設定しておく必要があります。
- *filename* : TFTP サーバ上のファイルに付ける名前。フルパスで指定します。スペースを含まない 32 文字以内のテキスト文字列を、引用符で囲まずに入力します。

たとえば、*starlog* ログ ファイルを TFTP サーバにコピーするには、次のように入力します。

```
# copy log starlog tftp tftpserv1 starlogthurs
```

sys.log ログ メッセージの記述形式

sys.log メッセージの例を次に示します。ここでは、この例を使用してログ メッセージの構成を説明します。

```
FEB 16 14:01:13 5/1 2453 VLANMGR-7: Transmit sfm STP BPDU on bPort 1,
egressLp 0x1f00 VlanLpSend() ret:0
```

ログ メッセージは、次の要素で構成されます。

- タイム スタンプ。ログ メッセージに表されたイベントが発生した日時を示します。上記の例では、タイム スタンプは FEB 16 14:01:13 です。
- 物理インターフェイス。CSS 内でのイベント発生場所を *slot*/*port*（たとえば 3/1）の形式で示します。
- カウンタ。各メッセージの累積発生回数が記録されます。上記のメッセージのカウントは 2,453 です。
- サブシステム名とレベル。メッセージに割り当てられた CSS のサブシステムと、メッセージのレベルを示します。上記の例は、サブシステム メッセージです。サブシステムは VLAN マネージャ、ログ レベルはデバッグ（debug）レベルである 7 です（VLANMGR-7）。CSS サブシステムのリストについては、「サブシステムでのロギングの設定」を参照してください。
- ログ　メッセージ。イベントの発生を示します。上記の例の残りの行は、発生したイベントを示しています。

  ```
  Transmit sfm STP BPDU on bPort 1, egressLp 0x1f00 VlanLpSend()
  ret:0
  ```

cliLogMessage subsystem コマンドを使用すると、特定のログ レベルにおけるサブシステムのログ メッセージを定義できます。詳細については、「ロギング レベルとサブシステムを指定したログ メッセージの設定」を参照してください。

配信不能メッセージの記述形式

IMM、EVENT、LOCAL などの配信不能メッセージは、CSS の特定のキューがいっぱいになった場合や過剰に利用されている場合に、問題の本質を明確にするために CSS のログに記録されます。

配信不能メッセージは、ロギング ヘッダーとロギング メッセージで構成されます（図 4-1 参照）。

図 4-1　　配信不能メッセージの形式

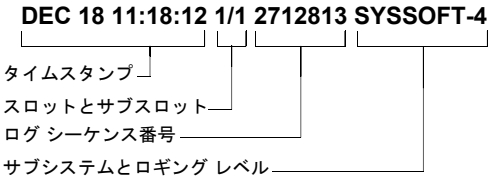
ロギング ヘッダー	ロギング メッセージ
DEC 18 11:18:12 1/1 2712813 SYSOFT-4	Communications- QUEUE FULL- Ipv4arp: Internal Messages Dropped

ロギング ヘッダーは、次の要素で構成されます。

- 日付と時刻付きのタイムスタンプ
- CSS スロットとサブスロットの番号
- 過度のロギングまたは CSS プロセッサの負荷が原因でログ メッセージが廃棄されたことを示すロギング シーケンス カウンタ
- サブシステムとそのログ レベル

図 4-2 に、ロギング ヘッダーの例を示します。

図 4-2　　ログ メッセージのロギング ヘッダー



ロギング ヘッダーに続くロギング メッセージでは、エラー タイプと送信先を定義し、その後に図 4-3 に示すメッセージが続きます。

図 4-3　ロギング メッセージ

エラー タイプは次のいずれかの状態を示します。

- QUEUE FULL：受信キューにはメッセージを受け入れる空きがない。
- QUEUE DELETED：CSS が有効なキューにメッセージを入れようとしたが、キューが破棄されていた。
- QUEUE INVALID：宛先メッセージ キュー ハンドルは有効なオブジェクトではなかった。
- QUEUE UNKNOWN：CSS が宛先キューを確認しようとしたが、検索が失敗した。

宛先は次のいずれかを示します。

- 宛先メッセージ キューの文字列で復号化された名前
- 16 進値（エラー タイプが QUEUE DELETED、QUEUE INVALID、または QUEUE UNKNOWN の場合）
- INTERNAL（同じプロセッサのタスク間で受け渡される LOCAL メッセージ）

ロギング メッセージの *Message...* セクションは、問題に関するその他の情報を提供します。配信不能メッセージのログ レベルによって、ロギング メッセージ内の情報量とログ内のメッセージの生成頻度が変わります。ログ レベルは、warning-4、Info-6、または Debug-7 に設定できます。

デフォルトでは、配信不能メッセージのログ レベルは warning-4 です。このメッセージは、問題の発生しているメッセージ キューで 2 秒ごとに発生します。ロギング メッセージ内のメッセージが提供するのは、次の情報だけです。

```
Internal Messages Dropped.
```

ログ レベルを Info-6 に変更すると、配信不能メッセージは引き続き問題の発生しているメッセージ キューで 2 秒ごとに発生します。ただし、ロギング メッセージで表示されるメッセージは次のようなものです。

```
Internal Messages dropped 5 times since the previous log for a total
of 21 times since bootup.
```

このメッセージは、さらに次のような情報を提供します。

- 前回のメッセージのロギング以降に内部メッセージが廃棄された回数
- CSS の起動以降に廃棄されたメッセージの合計数

詳細な情報が必要な場合は、ログ レベルを Debug-7 に設定します。配信不能メッセージは、発生するたびにログに記録され、識別子がメッセージ本文に表示されます。ロギング メッセージには、次のようなメッセージが表示されます。

```
Message (IMM:Base Class-IPV4_ARP, Identifier 1) from 1/1 (the other
CSS) failed to reach destination 'Ipv4Arp' on 1/1 (this CSS)
```

（注） Debug-7 ログ レベルでは、デバッグ メッセージとその他すべてのエラー レベルが表示されます。Debug-7 ログ レベルを選択すると、CSS のパフォーマンスが低下することがあります。

このメッセージのフィールドは、メッセージ タイプ、メッセージ タイプに基づく詳細情報、送信元情報、および宛先情報で構成されます。図 4-4 は、上記のロギング メッセージのフィールドを表しています。

図 4-4　ロギング メッセージのフィールド

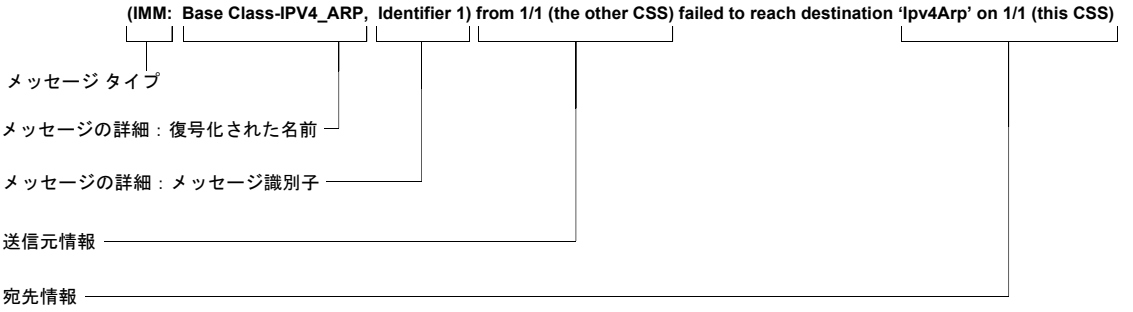


表 4-6 にロギング メッセージのフィールドを示します。

表 4-6　ログ レベルが Debug-7 であるロギング メッセージのフィールド

メッセージ フィールド	エントリと説明
メッセージ タイプ	**IMM**：プロセッサ間およびプロセッサ内の両方のメッセージとして渡されるメッセージ **LOCAL**：同じプロセッサのタスク間で受け渡されるメッセージ **EVENT**：CSS 全体を通じて登録済みの受信者群に配信されるメッセージ

メッセージの詳細	LOCAL メッセージ タイプの場合には、詳細情報はありません。
	
	EVENT メッセージ タイプの場合には、詳細情報は次のいずれかです。
	• イベントが認識されたときのイベントの文字列で復号化された名前。たとえば、次のように表示されます。
	`(Event:Ipv4ArpChangeEvent)`
	• イベントが範囲外のときの 16 進数で復号化された名前。たとえば、次のように表示されます。
	`(Event:unknown type-0x00a00005)`
	
	IMM メッセージ タイプの場合には、詳細情報として、Base Class とその後に次のいずれかが続きます。
	• 基本クラスの IMM メッセージの文字列で復号化された名前、およびそのクラス内の 10 進数で表したメッセージ識別子。たとえば、次のように表示されます。
	`(IMM:Base Class-IPV4_ARP, Identifier 1)`
	• Unknown、およびメッセージ タイプ フィールドの 16 進数値。たとえば、次のように表示されます。
	`(IMM:Base Class- Unknown, unknown type-0x00a00005)`

表 4-6　ログ レベルが Debug-7 であるロギング メッセージのフィールド（続き）

メッセージ フィールド	エントリと説明
送信元情報	メッセージの送信元。この情報には、スロット番号とサブスロット番号、および Adaptive Session Redundancy（ASR; 適応型セッションの冗長性）設定などでスロットまたはサブスロットが ローカルの CSS とリモートの CSS のどちらにあるかが示されます。たとえば、`from 1/1 (other CSS)` のように表示されます。 LOCAL メッセージ タイプの場合、文字列形式でのローカル プロセッサの情報も表示されます。たとえば、`from 1/1-'EventAgent' (this CSS)` のように表示されます。
宛先情報	ロギング メッセージの先頭に表示される宛先と同じ宛先。宛先情報とはメッセージの送信先です。この情報には、ロギング ヘッダーに表示されるスロットとサブスロットの番号があります。たとえば、`failed to reach destination Ipv4Arp on 1/1 (this CSS)` のように表示されます。

表 4-7 は、ユーザからの問い合わせが多い IMM 基本クラスのメッセージと識別子をまとめた表です。これらのメッセージと識別子は、別の CSS サブシステムの詳細メッセージとして表示されることがあります。

表 4-7　IMM メッセージ識別子

復号化された基本クラスの名前	説明とメッセージ識別子	サブシステム
CHASSIS	IMM 配信不能メッセージ、または、Chassis Manager Presence キューから廃棄されたメッセージ。このキューに送信されたログ メッセージは、ボードのブート処理中に CSS の Chassis Manager サブシステムおよび Online Diagnostic Monitor サブシステムによって発生します。宛先に指定できるのは、マスター SCM だけです。 割り当てられた各メッセージ タイプの識別子は、次のとおりです。 • 0 : ブート処理中に発生し、処理対象のボードがあることを表す。 • 1 : ブート処理中に各モジュールに対して一度だけ発生し、処理の準備ができているボードがあることを表す。 • 2 : Chassis Manager サブシステムおよび Online Diagnostic Monitor サブシステムから通知されるモジュールの状態変化に関するメッセージ。この識別子は、ブート処理中または特定のモジュールでエラーが発生した場合に表示されます。 • 3 : Chassis Manager サブシステムおよび Online Diagnostic Monitor サブシステムから通知されるサブモジュールの状態変化に関するメッセージ。この識別子は、ブート処理中またはサブモジュールでエラーが発生した場合に表示されます。 • 4 : モジュールを運用可能にするために Chassis Manager のタイムアウトを開始する。タイムアウトは、Chassis Manager から送信されます。この識別子が、ブート中に表示されます。	Chassis Manager

表 4-7　IMM メッセージ識別子（続き）

復号化された基本クラスの名前	説明とメッセージ識別子	サブシステム
DHCP	SCM にあるメインのダイナミック ホスト コンフィギュレーション プロトコル（DHCP）受信キューでメッセージがオーバーフローしていることを表すログ メッセージ このメッセージ タイプの識別子は、1 です。	DHCP Task
IPV4_ARP	IMM 配信不能メッセージ、または、SCM にある ARP_Q キューから廃棄されたメッセージ 割り当てられた各メッセージ タイプの識別子は、次のとおりです。 • 0：セッション プロセッサから受信した更新 • 1：セッション プロセッサから送信された ARP 要求	IPv4ARP Task
IPV4_RDNMGR_TID	IMM 配信不能メッセージ、または、SCM にある IP Redundancy Manager キューから廃棄されたメッセージ 割り当てられた各メッセージ タイプの識別子は、次のとおりです。 • 0：VRRP ソフトウェア コールバック • 1：VRRP 1 秒タイマー • 2：仮想ルータからの削除サービス • 3：仮想ルータからの冗長 VIP	IP Redundancy Manager
IPV4_SLAVE_RX	IMM 配信不能メッセージ、または、Session Manager にある SfmForwRx_Q キューから廃棄されたメッセージ。このキューでは、ブロードキャスト / マルチキャスト トラフィック、ICMP キープアライブ、および UDP/TCP フラグメントを受信します。 このメッセージ タイプの識別子は、1 です。	IPv4 Slave Forwarding Rx Task

表 4-7　IMM メッセージ識別子（続き）

復号化された基本クラスの名前	説明とメッセージ識別子	サブシステム
SYS_IMM	IMM 配信不能メッセージ、または、ping 用の ImmRxQ キューおよび ping 確認応答用の SysImmPing キューから廃棄されたメッセージ。SysImmPing キューは、永続的に存在するわけではなく、SysImmPing コマンドが実行されるたびに動的に作成および削除されます。 割り当てられた各メッセージ タイプの識別子は、次のとおりです。 • 0：ping • 1：ping の確認応答	Syssoft IMM

ログ メッセージの例

表 4-8 は、ユーザからの問い合わせが多い Cisco CSS 11500 シリーズのログ メッセージをまとめた表です。必要に応じて、考えられる原因と解決方法も説明します。ログ メッセージは、ロギング サブシステム別に、アルファベット順になっています。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
acl サブシステム	

`ACL-7: ACL match 2:254 Discarding`
`ACL-7: TCP SrcPort: 1043 DestPort: 21`
`ACL-7: Source: 172.20.57.2`
`ACL-7: Dest: 172.20.48.35`
	着信トラフィックが ACL 文と一致しています。CSS は、そのパケットを調べて廃棄します。
	
	このログ メッセージは、フロー マネージャから適用された ACL 文を含むパケットについて表示されます。このログ メッセージは、ロード バランシングが行われる可能性があることを表しています。

`ACL-7: ACL rule match 2:254` `Discarding packet, Log Enabled`	着信トラフィックが ACL 文と一致しています。CSS は、そのパケットを調べて廃棄します。 このログ メッセージは、IPV4 モジュールから適用された ACL 文を含むパケットについて表示されます。また、このログ メッセージは、CSS がこのパケットについてフローを設定しない場合があることを表します（特定の発信元ポートまたは宛先ポートではフローが作成されません）。このログ メッセージは、ICMP や RIP の障害とも関連する場合もあります。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
chassis サブシステム	
`CHMGR: Missing backup power supply.`	AC 給電部から電源装置に給電されていません。CSS 11501 と CSS 11503 には、電源装置が 1 台取り付けられています。CSS 11506 には 3 台まで電源装置を取り付けることができますが、適切なサービスを行うには、機能している電源装置が 2 台必要です。次に示すメッセージが先に表示されている場合は、電源装置ではなく、AC 給電部に問題が発生している可能性があります。 `CHMGR: Cannot locate power supply: PS`*`number`*`.` *PSnumber* 変数は、見つからない、または障害が発生している電源装置を示します。 各電源装置の前面にある 2 つの LED が点灯していれば、Cisco 11500 シリーズ CSS の電源装置は適切に動作しています。
`CHMGR: Cannot locate power supply: PS`*`number`*`.`	CSS シャーシに電源が見つかりません。CSS 11501 と CSS 11503 には、電源装置が 1 台取り付けられています。CSS 11506 には 3 台まで電源装置を取り付けることができますが、適切なサービスを行うには、機能している電源装置が 2 台必要です。PS*number* 変数は、認識できない、または障害が発生した電源装置を示します。給電部がシャーシに接続され、問題なく給電されていることが確実な場合は、電源装置に問題がある可能性があります。 各電源装置の前面にある 2 つの LED が点灯していれば、CSS 11500 シリーズの電源装置は適切に動作しています。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
circuit サブシステム	
CIRCUIT-7: Circuit status message for circuit 1023 sent to CE 20202c01 cause code is 7	コードは、VLAN 内のインターフェイスの状態を示します。論理ポートの原因コードおよびコマンドのコードは次のとおりです。 原因 コード CM_CIRCUIT_CREATED 1 CM_IP_REGISTER 2 CM_IP_NOT_REGISTER 3 CM_IP_MODIFIED 4 CM_LP_STATE_CHG 5 CM_CIRCUIT_REMOVED 6 CM_LP_ADDED 7 CM_LP_REMOVED 8 CM_LP_MODIFIED 9 CM_LP_FAILOVER 10 CM_CIRCUIT_DOWN 11 このログ メッセージは、VLAN にポートが追加されたことを示します。このログ メッセージは、ポートがアップ状態からダウン状態に変化するたびに VLAN への関連付けが変更されるため発生します。 VLAN のリストを表示するには、**show circuit** コマンドを使用します（『*Cisco Content Services Switch Routing and Bridging Guide*』参照）。VLAN のポートの状態、または VLAN がアクティブであるかどうかを確認してください。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
csdpeer サブシステム	
CSDPEER-7: LR Send list too small !!!	ピアから送信されるドメイン名の数が CSS リストのサイズを超えています。このパラメータは、**(config) dns-peer** コマンドで設定できます（『*Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*』参照）。受信スロットと送信スロットには同じ値を設定することをお勧めします。デフォルトのスロット数は 255 です。
flowmgr サブシステム	
FLOWMGR-4: Flow manager received an illegal message with code 10	いずれかのイーサネット ポートで無効なパケットを大量に受信したために、ファーストパスがオーバーフローしました。この場合は、フロー マネージャが無効な制御メッセージをファーストパスから受信しています。この問題は、ハードウェアが故障して中断したためにファーストパスでパケットが破損したこと、または、ファーストパスが無効なパケットのストリームを受信し、それらの一部が漏れてフロー マネージャに到達したことを表します。 多くのエラーが発生しているポートの情報を表示するには、**show ether-errors** コマンドを使用します（『*Cisco Content Services Switch Routing and Bridging Guide*』参照）。そのポートを接続解除するか、またはポートを変更してみて、エラーが発生しなくなるか調べます。
FLOWMGR-4: Flow manager received an illegal message with code 255	CSS のいずれかのイーサネット ポートで多数のエラーが発生し、いくつかの無効なパケットがフローマネージャに到達しています。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
FLOWMGR-4: Flow manager received an illegal message with code 194	ファーストパスから送信された無効なメッセージをフロー マネージャが受信しています。このログ メッセージは、ハードウェア障害が発生している場合、または、ポートで多数の無効なパケットを受信している場合に生成されます。CSS のポートで発生しているエラーを検索するには、**show mibii** コマンドまたは **show ether-errors** コマンドを使用します。
FLOWMGR-6: FM_Tcp: Handling generic FMTCP flow Re-Transmit ERROR FLOWMGR-6: FM_ReTransTimeout: Re-Transmit timeout ERROR FLOWMGR-6: FM_Tcp: Handling generic FMTCP flow Re-Transmit ERROR FLOWMGR-6: FM_ReTransTimeout: Re-Transmit timeout ERROR FLOWMGR-6: FM_Tcp: Handling generic FMTCP flow Re-Transmit ERROR	CSS が 4 つ以上の TCP パケットにまたがるレイヤ 5 ルールのコンテンツ要求を処理する場合は、CSS は、使用するサーバを決定した後に TCP のスロー スタート形式で TCP パケットを送信します。5 つのセグメントから成る TCP コンテンツ要求の例を次に示します。 Segment 1 --> Segment 2 --> (wait for an ACK) <--- ACK Segment3 -> Segment4 -> Segment5 -> <-- Content CSS は、3 秒以内にサーバから ACK を受信しない場合に、それ以降のパケットの受信を拒否し、接続をリセットして終了します。その時点でログ メッセージが生成されます。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
FLOWMGR-6: \n FM_UtilGenericTcpFlowReject: Handling Generic Flow REJECT	クライアント側またはサーバ側の接続障害が原因で、CSS が接続を拒否しています。 クライアント側の接続が原因でこのログ メッセージが生成された場合は、コンテンツ要求が、設定された最大数（デフォルトは 6）より多くのパケットにまたがっていることが、この問題の原因と考えられます。その他に考えられる理由は、次のとおりです。 • 遅延 ACK をクライアントに送信できない（200 ミリ秒で）。 • 遅延 ACK をクライアントに送信したが、クライアントから TCP SYN/FIN/RST ハンドシェイク シーケンスが返された。 • クライアント側が接続を突然閉じた。 サーバ側の接続が原因でこのログ メッセージが生成された場合は、CSS が複数のパケットにまたがるコンテンツ要求をサーバに送信したときに、そのサーバから応答確認が返らないこと、または、予期しない応答が返ったこと（クライアント側へのフローが切断されたことなど）が、この問題の原因と考えられます。 このメッセージがログに多数記録される場合は、製品を購入された弊社販売代理店へご連絡ください。
FLOWMGR-7: Allocation for a vector-loaded flow, where theFlow = 840ef5b0	これは情報メッセージです。対策は必要ありません。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
FLOWMGR-7: Exceeded outflow SYN count	レイヤ 5 ルールのために、CSS はバックエンド サーバへの接続を確立しようとしています。CSS は、バックエンド サーバへ SYN を 4 回送信しましたが、応答がありません。 CSS がバックエンド サーバとの接続を確立するには、次の TCP/IP ハンドシェイクを受信する必要があります。 SYN-> <-SYN/ACK ACK-> GET-> GET メッセージの受信後、CSS はバックエンド接続を開きます。その時点でログ メッセージが生成されます。 このようなログメッセージが数回発生する場合は、サーバに問題がある可能性があります。また、サーバのキープアライブや、通常の TCP HTTP トラフィックが原因であることもあります。サーバのポート 80 ソケットがいっぱいでないことを確認してください。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
fp-driver	
`FP_DRV-4: PrismImmFastPath::Send: Could not allocate an MCID. Remote message send aborted.`	CSS の MIPS プロセッサがグループ メッセージを送信しようとしましたが、プロセッサは Multicast ID Module（MID）から multicast ID （MCID; マルチキャスト ID）を取得できませんでした。MID は、CSS が複数の場所にパケットを送信する場合に、バッファの基準数を追跡します。ファーストパスでは、MCID を、VLAN のすべてのポートに過分に配信されるパケットを含むバッファの基準数として使用します。 CSS では、ハードウェア キューとソフトウェア キューを合わせて 1024 個のパケットがキューに待っている状態で MCID が足りなくなります。 ハードウェア キューがいっぱいになるのは、CSS が大量のパケットを受信し、すべてのポートに向けてパケットを過分に配信する場合です。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
FP_DRV-4: PrismImmFastPath::Send: Could not allocate an MCID. Remote message send aborted. （前のページの続き）	ソフトウェア キューの場合は、MIPS プロセッサのいずれかのタスクで、ローカル メンバーとリモート メンバーの両方を含むグループに大量のメッセージを送信して、MCID の基準値を超えたことが考えられます。ローカル メンバーに非常に大きなキューがある場合、ソフトウェア キューはすぐにいっぱいになり、受信側のタスクを実行し、メッセージを処理して、バッファを解放できないことがあります。 これらの 2 つの原因のうち、最も可能性が高いのは、CSS が、すべてのポートにフラッディングする必要がある大量のパケットを受信した場合です。 このログ メッセージは、通常、CSS が特定のルートを失い、デフォルト ゲートウェイへフローを転送した場合に生成されます。デフォルト ゲートウェイでは、ルーティング テーブルに CSS がネクストホップとしてリストされているために、この転送されたフローを CSS に戻します。その結果、このパケットが CSS からデフォルト ゲートウェイに送信され、デフォルト ゲートウェイから CSS に返されるという処理が繰り返されます。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
ipv4 サブシステム	
IPV4-4:Ipv4IfMgrCctUpdateMsg: IF config for circuit 1015 not found CIRCUIT-4: Error, Circuit 1015 does not exist.	削除された回線が、ACL またはその他の設定パラメータによって参照されています。CSS 設定を確認し、削除された回線の参照を削除するようにこの設定を変更します。
IPV4-4: Ipv4ReceivePacket: out of mbufs[, count *number*, current ingress ce 0x120fa00]	*mbuf* は、BSD UNIX ベースの IP スタック（VxWorks スタックなど）のデータ構造であり、バッファリングに使用されます。このログ メッセージは、CSS が自身のいずれかの IP アドレス宛てのパケットを受信し、それを VxWorks IP スタックへ送信しようとしたときに、このスタックに、使用可能なバッファが CSS に残っていなかったことを示します。 これらのバッファは、フロー設定および転送に使用されるバッファとは別のバッファです。トラフィックを CSS 自体に送信する場合（Telenet セッション時など）だけに使用されます。 CSS では、1 秒間にドロップされたメッセージの数を含むメッセージが、その 1 秒間に対して 1 つだけログに記録されます。 デバッグ モードでフラグを設定することにより、mbuf 不足状態でドロップされたメッセージのパケット ヘッダーと入力論理ポートに関する詳細ロギング（角かっこ内に表示）を有効にできます。 このメッセージが生成された場合は、製品を購入された弊社販売代理店へご連絡ください。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
IPV4-4: Ipv4SfmArpTx: unknown circuit in buffer (2001)	SFM では ARP 送信タスクが実行されています。SFM から受信したパケットは、適切な出力ポートに送信されます。このメッセージには、回線番号が示されます（この例では、2001）。SFM で ARP が待ち行列に置かれている間に、ARP の回線がダウンまたは非アクティブになると、このメッセージと回線番号がログに記録されます。この回線のデータがバッファに残っているときに、何らかの理由で回線が削除されました。 回線 VLAN のすべての物理インターフェイスで、アップ / ダウンを繰り返していないか確認してください。または、このメッセージが生成されたときに VLAN に設定変更が行われていなかったか確認してください。
IPV4-4: Ipv4SfmForwRx: bad IP version received (0)	IPV4 受信タスクがパケットを受信し、パケットの IP バージョンがカッコ () に示されています。CSS は、Ipv4 バージョン 4 以外のパケットを廃棄します。この例では、IP バージョンは 0 です。このメッセージが多く生成される場合は、装置の設定が正しくないか、または DoS 攻撃の可能性があります。
IPV4-4: Ipv4SfmForwTx: No VC for buffer (0x00000000)	IPV4 転送タスクには、スイッチ ファブリック プロセッサに転送するためのバッファがありますが、CSS は、ファーストパスへの仮想回線を作成する必要があります。このメッセージは、通常、CSS のイーサネット ポートの状態が変化すると生成されます。 これは情報メッセージです。対策は必要ありません。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
IPV4-4 Ipv4SfmForwTx: unknown logical port in buffer <0x05c01f00>	ARP パケットまたはその他の IPV4 パケットの中継中に、リンクが使用不能になりました。このエラーが発生すると、CSS は、転送元の論理ポートを選択し、パケットをフォーマットして、パケットの転送を試行します。CSS がパケットの送信を試行した時点で、論理ポートは使用できなくなります。 これは情報メッセージです。対策は必要ありません。
IPV4-4: Ipv4ApIoctl: unknown command: 1074031872	これは情報メッセージです。対策は必要ありません。
IPV4-4: Ipv4SfmForwRx: buffer length (872) less than IP length (1004)	IP パケットが破損しています。IP ヘッダーにある合計の長さを表す値が、パケットの実際の長さと一致しません。この場合は、SFP で受信したパケットの合計の長さ（バイト単位）が 、IP ヘッダーにある合計の長さを表す値より短くなっています。このメッセージは、ハードウェア障害または回線エラー（破損パケット）と関係がある場合があります。CSS のポートで発生しているエラーを検索するには、**show mibii** コマンドまたは **show ether-errors** コマンドを使用します。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
IPV4-4: (RIP) VIP Redundancy callback on unregistered address 0.0.0.0 range 0	CSS は 冗長 VIP を実行し、グローバル ルーティング情報プロトコル（RIP）を使用して、CSS の VIP を他のルータにアドバタイズしています（**rip advertise** コマンドを使用して設定）。この場合、RIP は CSS 内の冗長マネージャに、VIP とその範囲を送信し、冗長 VIP に状態変化があったら通知するように要求します。 冗長マネージャは、冗長 VIP の状態変化を監視する場合、VIP アドレスとその範囲を使用して RIP とやりとりします。VIP を正しくアドバタイズするために、RIP は VIP アドレスとその範囲を検証します。このログ メッセージは、RIP が冗長マネージャからのコールバック メッセージで受信した VIP アドレスを検出できない場合に生成されます。 **rip advertise** コマンドで指定した IP アドレスをチェックし、VIP と仮想インターフェイスの冗長性について VIP が正しく設定されているかを確認します。
IPV4-0: Ipv4SfmProcessArpFrame: ARP packet with unknown ingress port 0x0fc01f00	ファーストパスから IPV4 の宛先に ARP パケットを中継している間に、CSS イーサネット ポートが使用不能になりました。その結果、ARP パケットが廃棄されました。 これは情報メッセージです。対策は必要ありません。
IPV4-4: Ipv4SfmCmDeleteFlow: -1 response from VccRemoveVc, egress 0x09c01f00	CSS イーサネット ポートが使用不能になりました。その結果、IPV4 モジュールが、スイッチ ファブリック経由でファーストパスに確立された仮想回線を削除できなくなりました。これは情報メッセージです。対策は必要ありません。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
IPV4-4: Ipv4SfmProcessArpFrame: bad ARP packet received	CSS が、無効な ARP パケットを受信したことを検知しました。CSS が無効な ARP パケットの受信をログに記録した理由を示す、次のようなメッセージがログに記録されます。 IPV4-4: ffff53ff01ff ff0077fa6503 0806 IPV4-4: HW type: 0x0000 Proto type: 0x0000 IPV4-4: HLEN 0x00 PLEN 0x00 OPTPA-TSI-CSS1# 0x0000 IPV4-4: Sender HA 000000000000 IPV4-4: Sender IP 0.0.0.0 IPV4-4: Target HA 000000000000 IPV4-4: Target IP 0.0.0.0 ログ メッセージの最初の行は、パケットの宛先の MAC アドレス、パケットの送信元アドレス、および IP パケットのタイプを表します。この例では、宛先の MAC アドレスは ff-ff-53-ff-01-ff、送信元の MAC アドレスは ff-00-77-e7-65-03 です。また、0806 は ETHERTYPE_ARP を表します。 このメッセージの 2 行目は、ハードウェア タイプとプロトコル タイプを表します。この例では、ハードウェア タイプとプロトコル タイプがともに **0000** なので、メッセージがログに記録されています。CSS はこの値を無効なパケットを表す値と解釈します。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
IPV4-4: Duplicate IP address detected: 192.168.163.129 00-08-e2-10-38-54 IPV4-4: Incoming CE 0x3001f04, incoming (0 based) SLP 0xc	CSS が IP アドレスの重複を検出しています。通常は、CSS で検出された重複 IP アドレスを検索しやすいように、レベル 4 の IPV4 メッセージが 2 つ表示されます。 最初のメッセージは、CSS にも設定されている送信元 IP アドレスを持つパケットを CSS が受信したことを表します。重複する IP アドレスを持つデバイスを探しやすいように、このメッセージでは、重複する送信元 IP アドレスと対応する MAC アドレスが表示されます。 2 つ目のメッセージは、重複した IP アドレスを受信した CSS のポートを検出するためのメッセージです。CSS 上のインターフェイスを探すには、**flow statistics** コマンドを使用します。**flow statistics** コマンドは、そのポートに関してログ メッセージ内にリストされた CE の値を表示します。
keepalive サブシステム	
KAL-7: kal_ServiceNotify: kalIndex = 24 kalSvcEvent=3 KAL-7: kal_ServiceNotify: kalIndex = 31 kalSvcEvent=4 KAL-7: kal_ServiceNotify: kalIndex = 49 kalSvcEvent=5	CSS で HTTP キープアライブ（HEAD または GET）が設定されている場合に、サーバの状態が変化すると生成されます。サービス イベント（kalSvcEvent）の値は次のとおりです。 • 3 = Alive • 4 = Dying • 5 = Dead サーバの状態を確認してください。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
netman サブシステム	
NETMAN-1: TRAP:Authentication:Generated by: 192.168.36.252	CSS が SNMP トラップ メッセージを転送するように設定されており、ユーザが誤った SNMP コミュニティ ストリングを使用して CSS にアクセスしようとしています。この例では、CSS が、設定された SNMP トラップの受信側にトラップを送信し、IP アドレスが 192.168.36.252 のクライアントが誤ったコミュニティ ストリングを使用して CSS にアクセスしようとしていることを通知します。 このログ メッセージは、CSS に SNMP が設定されていないにもかかわらず、ユーザが SNMP を使用してその CSS にアクセスしようとした場合にも表示されます。設定の詳細については、第 5 章「SNMP の設定」を参照してください。
NETMAN-2: Sshd:do_authenticated:ERROR->TSM Rejects connection	CSS の CLI へのリモート アクセスが試みられました。CSS のセキュリティ マネージャがログインを拒否すると、セッションが終了します。 セキュリティ マネージャがログインを拒否するのは、次のような場合です。 • セキュリティ マネージャを同時に使用できるユーザの最大数（最大 128 ユーザ）を超えた場合 • CSS が再登録できなかった場合（セッションが終了したばかりで、フローのクリーンアップが実行されていないにもかかわらず、再登録を試行した場合） • CSS にメモリが不足しており、制御ブロックを割り当てられなかった場合

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
NETMAN-2: Generic:LINK DOWN for 13/1 CIRCUIT-6: Port 13/1 is down for circuit VLAN1 NETMAN-2: Generic:LINK DOWN for 13/2 CIRCUIT-6: Port 13/2 is down for circuit VLAN1 NETMAN-2: Generic:LINK DOWN for 13/3 CIRCUIT-6: Port 13/3 is down for circuit VLAN1 NETMAN-2: Generic:LINK DOWN for 13/4 CIRCUIT-6: Port 13/4 is down for circuit VLAN1 SYSSOFT-3: ONDM: Timeout downloading image to EPIF 0 from the switch. SYSSOFT-3: ONDM: Timeout downloading image to EPIF 0 from the switch.	EPIF 0 は、FEM の最初の 4 つのポートに属します。このログ メッセージは、通常、SFM が FEM へのコードを受信していない場合、または FEM が SFM を適切に読み取っていない場合に発生する問題に関連します。 次の場合、SFM 9/2 と FEM の間の通信に問題があります。 JAN 5 00:31:43 arrowpoint1.com 9/2 385390 SYSSOFT-3: ONDM: Timeout downloading image to EPIF 0 from the switch. JAN 5 00:31:45 arrowpoint1.com 9/2 385407 SYSSOFT-3: ONDM: Timeout downloading image to EPIF 0 from the switch. スロット 9 の SFM 、次にこの SFM が制御するスロット 13 の FEM を装着し直します。CSS の電源をいったん切ってから再投入します。
NETMAN-2: Enterprise:Service Transition:ServerA -> down NETMAN-5: Enterprise:Service Transition:ServerA -> alive	サービスの状態が変更されたときの情報メッセージです。キープアライブのパラメータに応じて、サーバの状態を確認してください。
NETMAN-4: SNMPAPI:SNMPAPI_Set:SET failure	コンソールまたは Telnet 経由で CSS に接続されている CLI のユーザが、誤ったコマンドを入力しました。Telnet またはコンソールのセッションでこのメッセージが表示され、コマンドが誤っていたことが示されます。
NETMAN-5: Enterprise: Login Failure:vty2 10.6.3.171 Mandy	SNMP のエンタープライズ ログイン失敗トラップが有効になっており、ユーザが入力したユーザ名とパスワードが無効でした。SNMP と CSS の詳細については、第 5 章「SNMP の設定」を参照してください。
NETMAN-5: Generic:SNMP Authentication > Failure from x.x.x.x	ユーザが SNMP を使用して CSS をポーリングしようとしましたが、入力したコミュニティ ストリングが誤っています。コミュニティ ストリングの指定の詳細については、第 5 章「SNMP の設定」を参照してください。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
NETMAN-5: Enterprise:Service > Transition:nexthop00001 -> down	CSS からネクスト ホップの IP アドレスに到達できません。スタティック ルートを設定すると、CSS によって内部サービスが自動的に作成されます。このサービスがアクティブになると、スタティック ルートがルーティング テーブルにリストされます。サービスが使用できなくなると、このサービスはルーティング テーブルから削除されます。 CSS のルーティング テーブルのすべてのルートが使用できることを確認してください。一部のルートの状態が変化している可能性があります。
NETMAN-5: Generic:LINK UP for 3/1 SYSSOFT-7: NP55_connection.c 512: Connection already open or reserved SYSSOFT-3: NP55 Driver: Connection already open or reserved SYSSOFT-2: VccAddVc:open conn failed w/ stat = -1; iVc 320; eVc 290 FLOWMGR-7: FM_GetIpv4Vc: Warning VCC_FP_IPV4_DC failed	フロー マネージャが、すでに確立されている仮想回線を再度割り当てようとしています。 このメッセージは、ポートがアップしようとする際に生成されます。このメッセージは問題を示すものではありません。このメッセージは、コンソールから接続した場合にブート プロセスの最後に頻繁に生成されます。
NETMAN-7: clm_ProcessStdAction:ERROR->Action<clms_dir>not found NETMAN-7: CLM:ERROR from clm_DispatchActionRoutine()	入力された CLI コマンドが無効です。この例では、デバッグ モードで **dir** コマンドが実行されましたが、無効なディレクトリが指定されました。たとえば、次のように指定しました。 (debug)# **dir d:**
NETMAN-7: SNMP:UNKNOWN RSP (493512 NETMAN-7: SNMP:(493512) Index = 1 <NO_SUCH_NAME>	有効な SNMP エージェント（コミュニティ ストリングが一致）が、無効なオブジェクトを設定しようとしています。CSS は、そのオブジェクトを認識できません。
NETMAN-7: TSM:tsm_SendToCLA:ERROR->Write	このセキュリティ マネージャのメッセージは、回線が切断された後（Telnet アプリケーションの接続解除後）に、スタック経由で送信される回線データに関する問題を表しています。このメッセージは、DEBUG レベルのメッセージであり、開発者用の情報メッセージです。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
NETMAN-7: ASUPPORT:as_SyncTask:ERROR->No registered reciever for MT:5/1.0 W	これは情報メッセージです。対策は必要ありません。
portmapper サブシステム	
PORTMAPPER-5: PortUnmap no Port mapping found.	ソース グループでポートマッパーが不足しています。**portmap** コマンドを使用して、このメッセージがログに記録されなくなるまで、また、ユーザ側やサービス側で性能上またはネットワーク アドレス変換上の問題が発生しなくなるまで、ソース グループのポートマッパーの数を増やします。
publish サブシステム	
PUBLISH-1: Unable to allocate tree memory <4150000>	CSS が約 4150000 バイトのメモリ セグメントを検索しましたが、使用可能なメモリ ブロックが検出されませんでした。このメッセージは、ファイルの複製の設定が誤っている場合に発生することがあります。設定が適切かどうか確認してください。ファイルが正しく複製されることを確認します。 非常に小さいメモリを要求したにもかかわらず、このメッセージが記録される場合は、システムのメモリのサイズが設定の要件を満たしていない可能性があります。問題を切り分けるには、まず、複製しないように設定して使用可能なメモリを監視し、ベースラインを判断します。次に、複製するように設定してこの手順を繰り返します。 CSS の実メモリと空きメモリの情報を表示するには、**show system-resources** コマンドを使用します。さらに多くのメモリを使用可能にするには、CSS を再度ブートします。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
radius サブシステム	
RADIUS-7: Auth Primary RADIUS-7: The id is 63 RADIUS-7: Return Auth Primary RADIUS-7: RADIUS no memory available	CSS の RADIUS サーバに関するアトリビュートの設定が誤っています。ACS radius サーバ設定の基本情報については、『*Cisco Content Services Switch Security Configuration Guide*』を参照してください。
RADIUS-4: RADIUS Authentication failed with reason code 2	このメッセージでは、次のコードが使用されます。 #define PW_ACCESS_REQUEST 1 #define PW_ACCESS_ACCEPT 2 #define PW_ACCESS_REJECT 3 #define PW_ACCOUNTING_REQUEST 4 #define PW_ACCOUNTING_RESPONSE 5 #define PW_ACCOUNTING_STATUS 6 #define PW_ACCESS_CHALLENGE 11 この例の原因はコード 2 であり、「CSS が RADIUS サーバから Accept 応答を受けているにもかかわらず、たぶんユーザ名かパスワードが誤まっていたために、この Accept 応答の受信を拒否したこと」を表しています。 このログ メッセージは、radius サブシステムに関するデバッグ メッセージ（debug-7）をロギングする場合にだけ表示されます。
sntp サブシステム	
SNTP-6: Sntp Server has incorrect mode 29	このメッセージは、SNTP サーバに障害がある可能性を表しています。SNTP サーバが「サーバ」として時刻のアップデートを CSS に送信していることを確認します。SNTP サーバ アップデートが、CSS がサポートする唯一のサーバ アップデートです。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
syssoft サブシステム	
SYSSOFT-2: VccAddVc:open conn failed w/ stat = -1; iVc 320; eVc 290	このメッセージは、ポートがアップ状態からダウン状態に遷移した場合に生成されます。自動ネゴシエーションについて、ケーブルの欠陥やハードウェア障害がないかを調べます。
SYSSOFT-3: ONDM: Could not open file <wsscm.sys> SYSSOFT-3: ONDM: Could not download Sub-module 8/1. SYSSOFT-3: ONDM: Could not open file <wssfm.sys> SYSSOFT-3: ONDM: Could not download Sub-module 6/2. SYSSOFT-3: ONDM: Could not download Sub-module 6/1. SYSSOFT-3: ONDM: Could not download Sub-module 5/2 SYSSOFT-3: ONDM: Could not download Sub-module 5/1. SYSSOFT-3: ONDM:No Sfm proxy for Slot 2. SYSSOFT-3: ONDM:No Sfm proxy for Slot 1.	ディスクにロードするイメージ ファイルが見つかりません。ディスクに異常があるか、またはディレクトリからファイルが削除されています。 製品を購入された弊社販売代理店へご連絡ください。
SYSSOFT-4: SYS:SysImmBind:Bind Collision TSM:5/1.1 W	これは情報メッセージです。対策は必要ありません。
SYSSOFT-4: Invalid Target(0x03087a01) for Chassis Type, Message being dropped.	CSS は、シャーシ内に存在しないスロットとサブスロットへのメッセージ送信を要求しようとしています。ログ メッセージは、16 進の誤ったアドレスとメッセージが廃棄されたことを示します。CSS 11503 のスロット 4、サブスロット 1 にコマンドを発行した場合に、このメッセージが表示される可能性が高くなります。 対処は必要ありません。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
SYSSOFT-4: Event not deliverable, msgq id =0x8cc48980, event id = 29, event name = BridgeMacAddrEvent	キューがいっぱいであるため、CSS が特定のプロセスを実行できませんでした。すべてのメッセージは、キューがいっぱいなためにイベントが廃棄されたことを示します。このメッセージは、ファーストパス（ネットワーク プロセッサ）が送信元 MAC アドレスの検索を実行し、エントリを検出できなかった場合に表示されます。ファーストパスは、MAC アドレス学習メッセージを SCM に送信します。SCM が処理しきれないほど大量のメッセージを受信した場合、キューがこれらのメッセージでいっぱいになります。
SYSSOFT-4: Event not deliverable, msgq id = 0x865c2110, event id = 4, event name = Ipv4RouteChangeEvent	キューがいっぱいであるため、CSS が特定のプロセスを実行できませんでした。すべてのメッセージは、キューがいっぱいなためにイベントが廃棄されたことを示します。このメッセージは、ルートの変更が検出されるといつでも表示されます。RIP プロセス、OSPF プロセス、代行管理プロセス（各 SFM につき生成されるプロセスで、SFM ルート テーブルと SCM ルート テーブルの同期を担当）、スタティック ルート プロセス、ARP プロセスで、このイベントを登録します。 ルートの状態変化、頻繁に起動および停止するローカルに接続されたステーションまたはサーバ、同時に大量の ARP 要求があったかどうかを調査してください。
SYSSOFT-7: MPOOL:mpoolAutoAlloc:WARN->Overrun on MPOOL 3 321	このメッセージは、通常、ブート時に情報メッセージとして表示され、CSS に追加メモリを割り当てることを示します。対策は必要ありません。

表 4-8　Cisco CSS 11500 シリーズのログ メッセージ（続き）

ログ メッセージ（sys.log: サブシステム名、レベル、メッセージ）	原因と解決方法
vlanmgr サブシステム	
`VLANMGR-4: DeleteMacAddr() called with VlanID = 0 for MacAddr 0- 0- 0- 0- 0- 0`	VLAN ID が 0 で MAC アドレスがすべて 0 のエントリを転送テーブルから削除するように、VLAN マネージャに要求しています。
vpm サブシステム	
`VPM removed Vc 8000b00 based on failure of port 3401f00.<010>`	特定のポートが使用不能なために、CSS がこのイーサネット ポートで使用するリソースを再要求しています。CSS は、ポートが内部検査に応答しない場合、または回線が使用不能な場合に、リソースを再要求します。このイーサネット ポートのアドレス情報は表示されません。**show interface** コマンドを使用してイーサネット ポートの情報を表示し、障害があるポートを特定します。
wcc サブシステム	
`WCC-7: Route Change for IP Address ( x.x.x.x)`	情報メッセージです。ARP が別のポートに着信したことを示します。

以降の内容について

第 5 章「SNMP の設定」では、CSS の Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）機能について説明します。