



## 設定前の作業

---

この章では、Content Switching Module with SSL (CSM-S) の設定を始める前の必要事項について説明します。

- [設定の概要 \(p.3-2\)](#)
- [オペレーティング システムのサポート \(p.3-5\)](#)
- [CSM-S の設定準備 \(p.3-6\)](#)
- [設定の保存および復元 \(p.3-7\)](#)
- [SLB モードの設定 \(p.3-8\)](#)
- [新しいソフトウェア リリースへのアップグレード \(p.3-14\)](#)
- [失われたパスワードの回復 \(p.3-18\)](#)

## 設定の概要

設定プロセスでは、スイッチが Route Processor (RP; ルート プロセッサ) モードであることを前提とします。図 3-1 に、基本的な CSM-S 設定プロセスの必須および任意の作業の概要を示します。図 3-2 に、設定プロセスの SSL 部分の概要を示します。



---

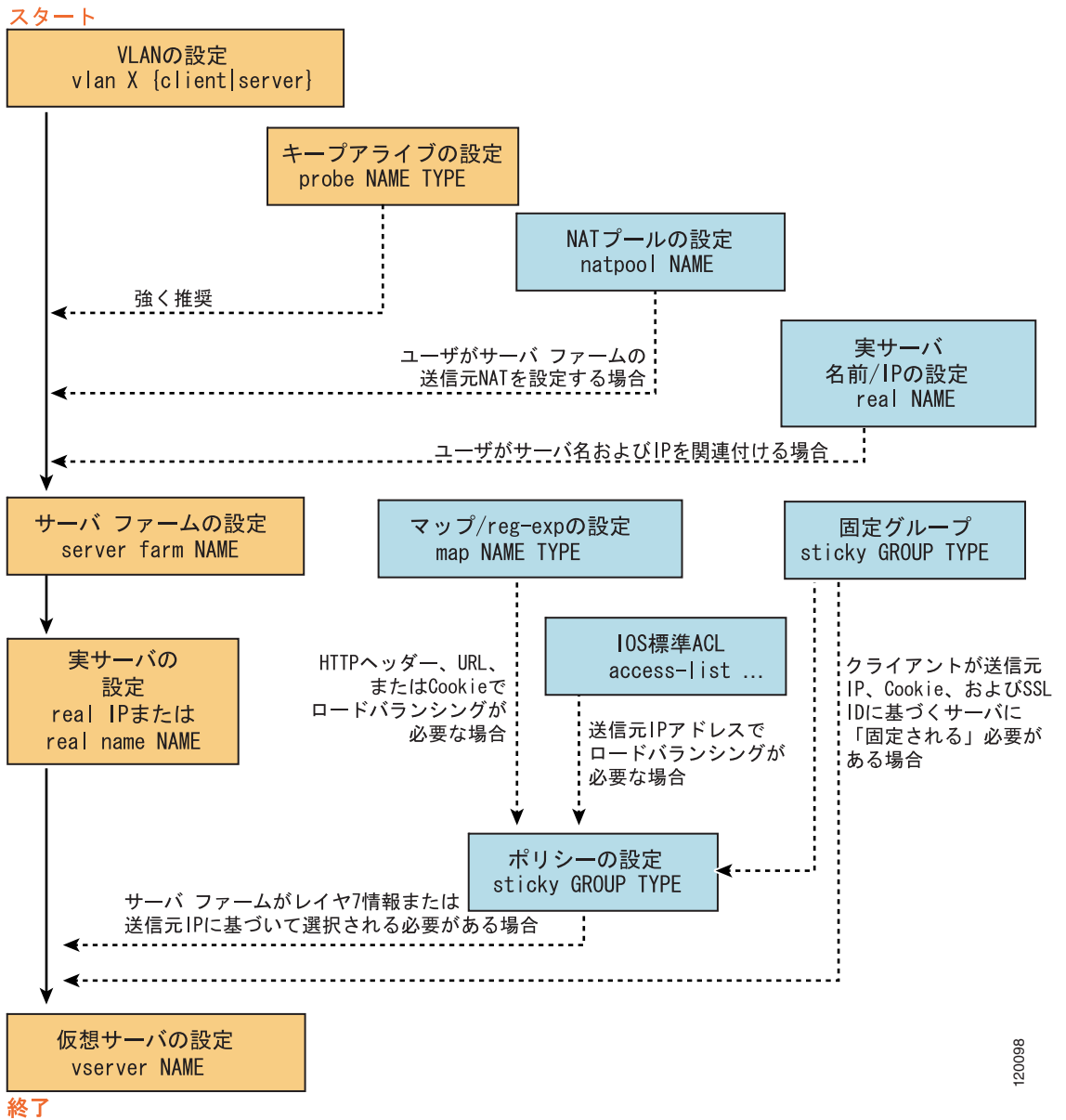
(注) レイヤ 4 ロードバランシングの場合、ポリシーの設定は不要です。

---

ここでは、必須パラメータの設定方法について説明します。

- [CSM-S コマンドおよび SSLSM コマンドの相違点 \(p.1-10\)](#)
- [ソフトウェア バージョンの情報 \(p.1-11\)](#)
- [設定の制約事項 \(p.1-13\)](#)
- [失われたパスワードの回復 \(p.3-18\)](#)
- [クライアント側 VLAN の設定 \(p.4-3\)](#)
- [サーバ側 VLAN の設定 \(p.4-4\)](#)
- [サーバファームの設定 \(p.5-2\)](#)
- [実サーバの設定 \(p.5-4\)](#)
- [仮想サーバの設定 \(p.6-2\)](#)

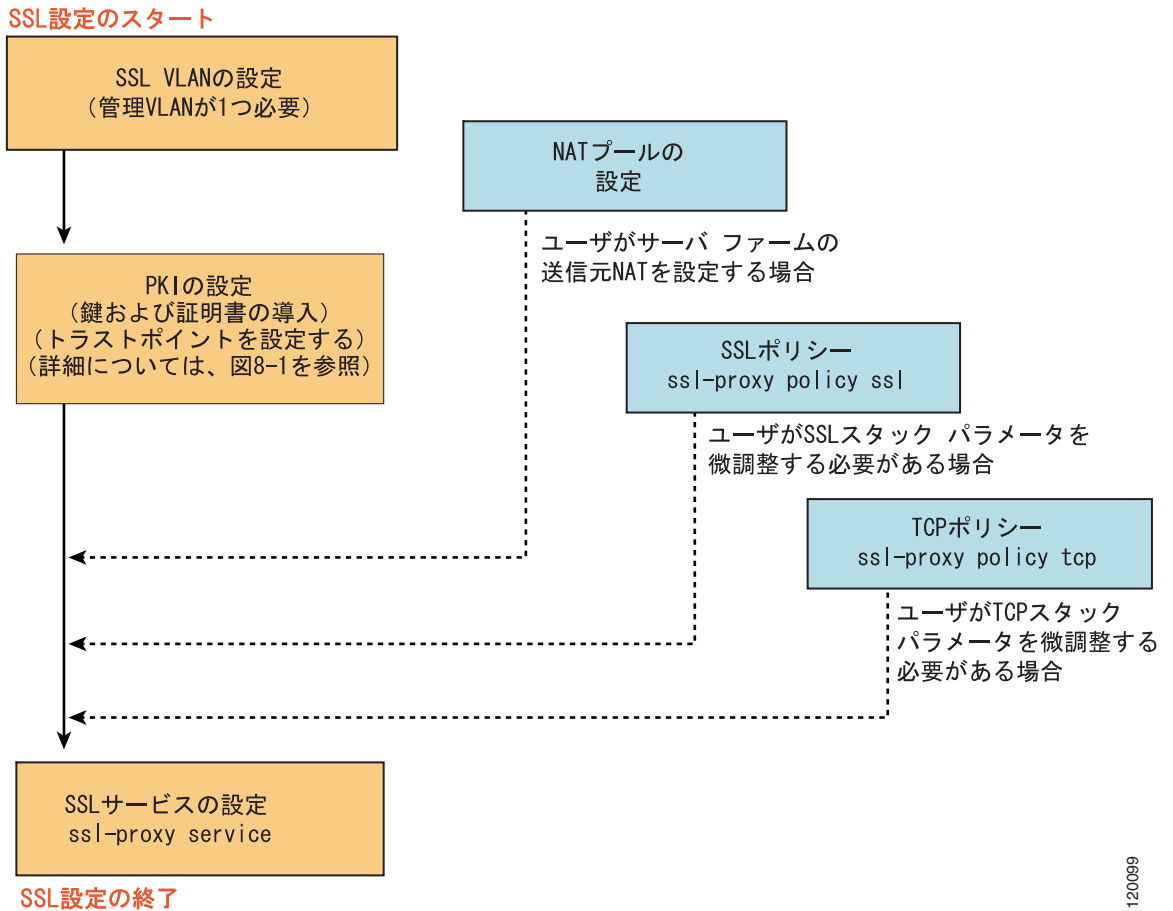
図 3-1 CSM-S の基本設定の概要



必須のロードバランシング パラメータを CSM-S 上で設定すると、任意のパラメータを設定することができます。次の各項を参照してください。

- [リダイレクト仮想サーバの設定 \(p.6-7\)](#)
- [クライアント NAT プールの設定 \(p.5-8\)](#)
- [サーバ開始型接続の設定 \(p.5-9\)](#)
- [TCP パラメータの設定 \(p.6-5\)](#)

図 3-2 CSM-S SSL の設定概要



120089

SSL パラメータの設定については、次の各項を参照してください。

- CSM-S コマンドおよび SSLSM コマンドの相違点 (p.1-10)
- SSL ドータカードの初期設定 (p.7-2)
- クライアント側およびサーバ側動作に対する SSL の設定 (p.7-7)

高度な設定と連動するには、第2章から第11章の次の項目を参照してください。

- シングルサブネット (ブリッジ) モードの設定 (p.2-2)
- セキュア (ルータ) モードの設定 (p.2-4)
- URL ハッシュの設定 (p.5-10)
- 一般ヘッダー解析の設定 (p.6-14)
- クライアント側およびサーバ側動作に対する SSL の設定 (p.7-7)
- RHI の設定 (p.10-7)
- フォールトトレランスの設定 (p.9-2)
- 連続 (persistent) 接続の設定 (p.10-15)
- HSRP の設定 (p.9-6)
- 接続の冗長性の設定 (p.9-12)
- 実サーバの SNMP トラップの設定 (p.10-23)
- ヘルス モニタリング用プローブの設定 (p.11-2)

- 帯域内ヘルス モニタリングの概要および設定 (p.11-10)
- HTTP 戻りコードチェックの概要および設定 (p.11-11)
- CSM-S での TCL スクリプトの使用 (p.12-1)
- ステルス ファイアウォール ロードバランシングの設定 (p.13-8)
- 標準ファイアウォール ロードバランシングの設定 (p.13-18)
- ファイアウォール用リバーススティッキの設定 (p.13-27)

## オペレーティング システムのサポート

CSM-S は、Cisco IOS ソフトウェアだけを稼働するスイッチでサポートされます。CSM-S は MSFC CLI (コマンドライン インターフェイス) 経由で設定されるので、MSFC CLI にアクセスするために、最初に MSFC とのセッションを開始する必要があります。Cisco IOS ソフトウェアが稼働するスイッチを使用する場合は、レイヤ 2 の設定 (VLAN およびポート アソシエーションなど) はすべて、スーパーバイザ エンジン上で実行されます。



(注) スイッチ上で CSM-S を実行すると、設定された VLAN (仮想 LAN) が CSM-S とスイッチのバックプレーンを接続するトランクまたはチャンネルに自動的に追加されます。Catalyst オペレーティング システムと Cisco IOS ソフトウェアの両方が稼働するスイッチでは、CSM-S VLAN を手動でトランクまたはチャンネルに追加する必要があります。

## CSM-S の設定準備

CSM-S を設定する前に、次の作業を終えておく必要があります。

- スイッチとモジュールの Cisco IOS バージョンが一致していることを確認します。『*Catalyst 6500 Series Switch Content Switching Module Installation Guide*』を参照してください。
- Server Load Balancing (SLB; サーバ ロードバランシング) を設定するには、次の情報を入手しておく必要があります。
  - 導入先で使用するネットワーク トポロジー
  - 実サーバの IP アドレス
  - Domain Name Server (DNS; ドメイン ネーム サーバ) で使用する CSM-S Virtual IP (VIP; 仮想 IP) 用エントリ (名前を使用して DNS にアクセスする必要がある場合)
  - 各仮想サーバの IP アドレス
- 先に Catalyst 6500 シリーズスイッチで VLAN を設定してから、CSM-S に対して VLAN を設定する必要があります。スイッチとモジュールの VLAN ID は同じでなければなりません。詳細については、『*Catalyst 6500 Series Switch Software Configuration Guide*』を参照してください。

次に、VLAN を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# vlan 130
Router(config-vlan)# name CLIENT_VLAN
Router(config-vlan)# exit
Router(config)# vlan 150
Router(config-vlan)# name SERVER_VLAN
Router(config-vlan)# end
```

- サーバまたはクライアントに接続する物理インターフェイスを、対応する VLAN 内に組み込みます。

次に、物理インターフェイスをレイヤ 2 インターフェイスとして設定して、VLAN に割り当てる例を示します。

```
Router>
Router> enable
Router# config
Router(config)# interface 3/1
Router(config-if)# switchport
Router(config-if)# switchport access vlan 150
Router(config-if)# no shutdown
Router(vlan)# exit
```

- クライアント側またはサーバ側 VLAN 上のネクストホップルータで MSFC を使用する場合は、対応するレイヤ 3 VLAN インターフェイスを設定する必要があります。



### 注意

ポリシー ベース ルーティングまたは送信元 Network Address Translation (NAT; ネットワーク アドレス変換) を使用し、CSM-S をルータ モードとして設定しないかぎり、クライアント側とサーバ側の両方に対して、MSFC をルータとして同時に使用することはできません。このような状況が発生するのは、CSM-S がロードバランスまたは転送する両方向のフローを確認する必要があるためです。ブリッジ (シングル サブネット) モードで CSM-S を使用する場合は、クライアント側とサーバ側の両方に対して、MSFC 上でレイヤ 3 VLAN インターフェイスを設定しないでください。CSM-S をルータ モードで使用する場合は、戻りトラフィックが CSM-S に送り返されるように、ポリシー ベース ルーティングまたは送信元 NAT を適切に設定しないかぎり、クライアント側とサーバ側の両方に対して、MSFC 上でレイヤ 3 VLAN インターフェイスを設定しないでください。

次に、レイヤ 3 VLAN インターフェイスを設定する例を示します。

```
Router>
Router> enable
Router# config
Router(config)# interface vlan 130
Router(config-if)# ip address 10.10.1.10 255.255.255.0
Router(config-if)# no shutdown
Router(vlan)# exit
```

## CLI の使用法

CSM-S のソフトウェア インターフェイスは Cisco IOS CLI (コマンドライン インターフェイス) です。Cisco IOS CLI および Cisco IOS コマンド モードの詳細については、『*Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*』の Chapter 2 を参照してください。



(注) プロンプトに入力できる文字数に制限があるため、プロンプトが切り捨てられる場合があります。たとえば、Router(config-slb-vlan-server)# は Router(config-slb-vlan-serve)# のように表示されます。

## オンライン ヘルプの利用方法

どのコマンド モードでも、疑問符 (?) を入力すると、使用できるコマンドのリストが表示されます。

```
Router> ?
```

または

```
Router(config)# module CSM 5
Router(config-module-CSM)# ?
```



(注) オンライン ヘルプでは、コマンドで使用できるデフォルトのコンフィギュレーション値、および値の範囲が表示されます。

## 設定の保存および復元

設定の保存および復元については、『*Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*』を参照してください。

## SLB モードの設定

Catalyst 6500 シリーズ スイッチの SLB 機能は、2 種類のモードで設定されます。RP モードおよび CSM モードです。スイッチの設定は、CSM-S の動作に影響しません。CSM-S はデフォルトで、RP モードで設定されます。RP モードを使用すると、同一シャーシで 1 つまたは複数の CSM-S モジュールを設定し、同一スイッチで Cisco IOS SLB を実行できます。



(注)

RP モードはデフォルト モードで、推奨されているモードです。CSM モードは、下位互換性を維持するためにリリース 2.1 より前の CSM ソフトウェア イメージでのみ使用されます。新たに CSM または CSM-S イメージを搭載する場合は、RP モードを使用してください。

CSM モードの場合、設定できる CSM-S は 1 つだけです。CSM モードをサポートしているのは、旧ソフトウェア リリースとの下位互換性を維持するためです。単一 CSM-S 設定では、同一スイッチで Cisco IOS SLB を実行できません。

次に、モードについて説明します。

- [モードのコマンド構文 \(p.3-8\)](#)
- [モード間の切り替え \(p.3-9\)](#)
- [CSM モードと RP モードの相違 \(p.3-10\)](#)
- [モードの変更 \(p.3-12\)](#)

## モードのコマンド構文

スイッチに CSM-S コンフィギュレーション コマンドを入力するには、その前に設定対象の CSM-S を指定しなければなりません。設定する CSM-S を指定するには、**module csm slot-number** コマンドを使用します。*slot-number* 値は、設定対象の CSM-S が搭載されているシャーシ スロットです。

**module csm** コマンドによって CSM-S コンフィギュレーション サブモードが開始されます。以後、入力したすべてのコンフィギュレーション コマンドは、指定したスロットの CSM-S に適用されます。



(注)

特に明記していないかぎり、このマニュアルの例はすべて、このコマンドが入力済みで、設定対象の CSM-S に対応するコンフィギュレーション モードがすでに開始されていることが前提です。

CSM-S モードおよび RP モードを設定するコマンドの構文は、次の点を除いて同じです。

- CSM モードで設定する場合、上位レベルのコマンドごとに、プレフィクスとして **ip slb** を指定する必要があります。
- CSM モードの設定と RP モードの設定では、プロンプトが異なります。

スロット 5 の CSM-S に仮想サーバを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Router(config)# <b>module csm 5</b>	設定する CSM-S の位置を指定します。
ステップ 2	Router(config-module-csm)# <b>vserver VS1</b>	仮想サーバを設定します。



次に、`config-module-csm` モードでのすべての CSM-S コマンドのリスト例を表示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# module csm 5
Router(config-module-csm)# ?
SLB CSM module config
  arp          configure a static ARP entry
  capp         configure Content Application Peering Protocol
  default      Set a command to its defaults
  dfp         configure Dynamic Feedback Protocol manager
  exit        exit SLB CSM module submode
  ft          configure CSM fault tolerance (ft) feature
  map         configure an SLB map
  natpool     configure client nat pool
  no          Negate a command or set its defaults
  owner       configure server owner
  policy      configure an SLB policy
  probe       configure an SLB probe
  real        configure module real server
  script      configure script files and tasks
  serverfarm  configure a SLB server farm
  standby
  static      configure static NAT for server initiated connections
  sticky      configure a sticky group
  variable    configure an environment variable
  vlan        configure a vlan
  vserver     configure an SLB virtual server
  xml-config  settings for configuration via XML
```

## モード間の切り替え

`ip slb mode` コマンドを使用してモードを CSM から RP に切り替えると、既存の CSM-S 設定が新しい設定に移行します。既存の CSM-S 設定がある場合は、スロット番号を要求されます。

Catalyst 6500 シリーズ スイッチでは、RP モードの設定から CSM モードの設定に移行できます。Cisco IOS SLB の設定から CSM-S の設定への移行は、手動に限って可能です。

## CSM モードと RP モードの相違

CSM モードと RP モードは、CSM-S が CLI から設定される方法に影響するだけで、CSM-S 自体の動作および機能に影響するわけではありません。CSM-S と同一シャーシ内の Cisco IOS SLB の場合と同様に、1 つのシャーシ内の複数の CSM-S モジュールを設定する場合は、RP モードである必要があります。

## CSM モード

**ip slb mode csm** コマンドモードを使用して、1.x リリースの CSM-S を設定することができます。このモードの場合、シャーシに設定できる CSM-S は1つです（他の CSM または Cisco IOS SLB を同一シャーシ内に設定できません）。

このモードでは、すべての CSM-S コンフィギュレーション コマンドは **ip slb** で始まります。

CSM-S の **show** コマンドは、**show ip slb** で始まります。

CSM ソフトウェア 2.1 以降のリリースを使用している場合は、このモードは推奨できません。このモードは、Cisco IOS CLI で下位互換性の維持のためにオプションとして提供されているからです。

次に、シャーシ内の単一の CSM-S の設定例を示します。

```
Cat6k# show running-config
Building configuration...
Current configuration : 5617 bytes

ip slb mode csm
ip slb vlan 110 server
ip address 10.10.110.1 255.255.255.0

ip slb vlan 111 client
ip address 10.10.111.2 255.255.255.0
gateway 10.10.111.1

ip slb probe HTTP_TEST http
request method get url /probe/http_probe.html
expect status 200
interval 5
failed 5

ip slb serverfarm WEBFARM
nat server
no nat client
real 10.10.110.10
inservice
real 10.10.110.20
inservice
probe HTTP_TEST

ip slb vserver HTTPVIP
virtual 10.10.111.100 tcp www
persistent rebalance
serverfarm WEBFARM
inservice
```

## RP モード

Cisco IOS SLB が稼働するシャーシで複数の CSM-S モジュールを設定するには、**ip slb mode rp** コマンドモード (デフォルト) を使用します。このモードで設定できるのは、リリース 2.1 以降の CSM-S だけです。

このモードでは、CSM-S は次のコマンドサブモードから設定されます。

```
mod csm X
```

X は設定する CSM-S のスロット番号です。

CSM-S の **show** コマンドは、**show mod csm X** で始まります。

CSM ソフトウェア リリース 2.1 以降で CSM-S を設定する場合は、RP モードが推奨されます。このモードでも、Cisco IOS SLB に適用されるすべてのコマンドは、シャーシの CSM-S には適用されません。これらのコマンドは、**ip slb** で始まります。

次に、シャーシ内の単一の CSM-S の設定例を示します。

```
Cat6k# show running-config
Building configuration...

Current configuration : 5597 bytes
!---

module ContentSwitchingModule 5
vlan 110 server
ip address 10.10.110.1 255.255.255.0

vlan 111 client
ip address 10.10.111.2 255.255.255.0
gateway 10.10.111.1

probe HTTP_TEST http
request method get url /probe/http_probe.html
expect status 200
interval 5
failed 5

serverfarm WEBFARM
nat server
no nat client
real 10.10.110.10
inservice
real 10.10.110.20
inservice
probe HTTP_TEST

vserver HTTPVIP
virtual 10.10.111.100 tcp www
persistent rebalance
serverfarm WEBFARM
inservice
```

## モードの変更

CSM の動作モードを CSM モードから RP モードに、または RP モードから CSM モードに変更することができます。次に、モードの変更方法を示します。

### CSM モードから RP モード

CSM モードから RP モードに変更する例を示します。これは CSM 1.x から 2.1 以降のリリースへの一般的な移行例で、モジュールのリセットは必要ありません。

```
Cat6k# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Cat6k(config)# ip slb mode ?
    csm  SLB in Content Switching Module
    rp   SLB in IOS system

Cat6k(config)# ip slb mode rp
% The current SLB mode is CSM-SLB.
% You are selecting RP-SLB mode.
% All configuration for CSM-SLB will be moved to module submode.
% Confirm switch to RP-SLB mode? [no]: yes
% Enter slot number for CSM module configuration, 0 for none [5]: 5
% Please save the configuration.
Cat6k(config)# end

Cat6k# write
Building configuration...
[OK]
Cat6k#
```

### RP モードから CSM モード

これは RP モードから CSM モードへの移行例で、モジュールのリセットが必要です。

```
Cat6k# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Cat6k(config)# ip slb mode ?
    csm  SLB in Content Switching Module
    rp   SLB in IOS system

Cat6k(config)# ip slb mode csm
% The current SLB mode is RP-SLB.
% You are selecting CSM-SLB.
% All SLB configurations for RP will be ERASED.
% After execution of this command, you must
% write the configuration to memory and reload.
% CSM-SLB module configuration will be moved to ip slb submodes.
% Confirm switch to CSM-SLB mode? [no]: yes
% Enter slot number for CSM module configuration, 0 for none [5]: 5
% Please save the configuration and reload.

Cat6k(config)# end
Cat6k# write
Building configuration...
Cat6k# reload
Proceed with reload? [confirm] y
Verify Mode Operation
```

## 設定の確認

設定が適切に機能するかどうかを確認するには、RP モードで次のコマンドを使用します。

```
Cat6k# show ip slb mode
      SLB configured mode = rp

Cat6k# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Cat6k-1(config)# ip slb ?
  dfp          configure Dynamic Feedback Protocol manager
  entries      initial and maximum SLB entries
  firewallfarm configure an SLB firewall farm
  mode         configure SLB system mode
  natpool      define client nat pool
  probe        configure an SLB probe
  serverfarm   configure an SLB server farm
  vserver      configure an SLB virtual server
```

設定が適切に機能するかどうかを確認するには、Cisco IOS SLB モードで次のコマンドを使用します。

```
Cat6k(config)# module csm 5
Cat6k(config-module-csm)# ?
SLB CSM module config
  default      Set a command to its defaults
  dfp          configure Dynamic Feedback Protocol manager
  exit         exit SLB CSM module submenu
  ft           configure CSM fault tolerance (ft) feature
  map          configure an SLB map
  natpool      configure client nat pool
  no           Negate a command or set its defaults
  policy       configure an SLB policy
  probe        configure an SLB probe
  serverfarm   configure an SLB server farm
  static       configure static NAT for server initiated connections
  sticky       configure a sticky group
  vlan         configure a vlan
  vserver      configure an SLB virtual server
```

シャーシ内の単一の CSM-S 設定が適切に機能するかどうかを確認するには、CSM モードで次のコマンドを使用します。

```
Cat6k# show ip slb mode
      SLB configured mode = csm

Cat6k-1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Cat6k(config)# ip slb ?
  dfp          configure Dynamic Feedback Protocol manager
  ft           configure CSM fault tolerance (ft) feature
  map          configure an SLB map
  mode         configure SLB system mode
  natpool      configure client nat pool
  policy       configure an SLB policy
  probe        configure an SLB probe
  serverfarm   configure an SLB server farm
  static       configure static NAT for server initiated connections
  sticky       configure a sticky group
  vlan         configure a vlan
  vserver      configure an SLB virtual server
```

## 新しいソフトウェア リリースへのアップグレード

ここでは、Content Switching Module with SSL をアップグレードする 3 種類の方法について説明します。

- [スーパーバイザ エンジン ブートフラッシュからのアップグレード \(p.3-15\)](#)
- [PCMCIA カードからのアップグレード \(p.3-16\)](#)
- [外部 TFTP サーバからのアップグレード \(p.3-17\)](#)



(注)

新しいソフトウェア リリースにアップグレードする場合は、CSM-S イメージをアップグレードしてから Cisco IOS イメージをアップグレードする必要があります。そうしないと、スーパーバイザ エンジンが CSM-S を認識しません。スーパーバイザ エンジンが CSM-S を認識しない場合は、Cisco IOS イメージをダウングレードし、CSM-S イメージをアップグレードしてから、Cisco IOS イメージをアップグレードする必要があります。



(注)

CSM-S のアップグレードの際に、CSM および SSL ドータカード イメージの両方がアップグレードされます。CSM-S 上で CSM イメージを使用、または CSM 上で CSM-S イメージを使用することができません。

CSM-S をアップグレードするには、アップグレードする CSM-S モジュールとのセッションを開始する必要があります。アップグレード中は、スーパーバイザ エンジンに接続されたコンソールにすべてのコマンドを入力します。コンフィギュレーション コマンドは、それぞれ異なるコマンドラインに入力してください。アップグレードを完了するには、**exit** コマンドを入力して、スーパーバイザ エンジン プロンプトに戻ります。「[SLB モードの設定](#)」(p.3-8) を参照してください。



注意

アップグレードしている CSM-S とのセッションを終了するには、**exit** コマンドを入力する必要があります。セッションを終了しないで CSM-S を Catalyst 6500 シリーズ シャーシから取り外した場合は、CSM-S にコンフィギュレーション コマンドを入力するために、**Ctrl + ^** を押して、**x** を入力し、プロンプトに **disconnect** コマンドを入力する必要があります。

## スーパーバイザ エンジン ブートフラッシュからのアップグレード



(注) ブートフラッシュにイメージをロードする手順については、『*Catalyst 6500 Series Supervisor Engine Flash PC Card Installation Note*』を参照してください。

スーパーバイザ エンジンのブートフラッシュから CSM-S をアップグレードする手順は、次のとおりです。

- ステップ 1** Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバをイネーブルにして、次のようにブートフラッシュからイメージを供給します。

```
Router>
Router> enable
Router# configure terminal
Router(config)# tftp-server sup-bootflash:c6s1b-apc.revision-num.bin
Router(config)
```

- ステップ 2** スーパーバイザ エンジンと CSM-S 間のセッションを確立します。

```
Router# session slot csm-slot-number processor 0
```

- ステップ 3** スーパーバイザ エンジンから CSM-S にイメージをロードします。

```
CSM> upgrade 127.0.0.zz c6s1b-apc.revision-num.bin
```

スーパーバイザ エンジンがシャーシのスロット 1 に搭載されている場合、*zz* は 12 です。  
スーパーバイザ エンジンがシャーシのスロット 2 に搭載されている場合、*zz* は 22 です。



(注) スーパーバイザ エンジンを搭載できるのは、シャーシのスロット 1 またはスロット 2 だけです。

- ステップ 4** CSM-S とのセッションを終了し、Cisco IOS プロンプトに戻ります。

```
CSM> exit
```

- ステップ 5** CSM-S の電源を切断して再投入するか、またはスーパーバイザ エンジンのコンソールから次のコマンドを入力して、CSM-S を再起動します。

```
Router(config)# hw-module module csm-slot-number reset
```

## PCMCIA カードからのアップグレード



(注) このマニュアルでは全体を通して、*PCMCIA* カードの代わりにフラッシュ *PC* カードという言葉を使用します。

スーパーバイザ エンジンに装着された着脱式フラッシュ *PC* カードから *CSM-S* をアップグレードする手順は、次のとおりです。

**ステップ 1** TFTP サーバをイネーブルにして、着脱式フラッシュ *PC* カードからイメージを供給します。

```
Router>
Router> enable
Router# configure terminal
Router(config)# tftp-server slotx:c6slb-apc.revision-num.bin
```

*x*値=0(フラッシュ *PC* カードがスーパーバイザ エンジンの *PCMCIA* スロット0に搭載されている場合)

**ステップ 2** スーパーバイザ エンジンと *CSM-S* 間のセッションを確立します。

```
Router# session slot csm-slot-number processor 0
```

**ステップ 3** スーパーバイザ エンジンから *CSM-S* にイメージをロードします。

```
CSM> upgrade slot0: c6slb-apc.revision-num.bin
```



(注) スーパーバイザ エンジンを搭載できるのはシャーシのスロット 1 またはスロット 2 だけです。

**ステップ 4** *CSM-S* とのセッションを終了し、Cisco IOS プロンプトに戻ります。

```
CSM> exit
```

**ステップ 5** *CSM-S* の電源を切断して再投入するか、またはスーパーバイザ エンジンのコンソールから次のコマンドを入力して、*CSM-S* を再起動します。

```
Router# hw-module module csm-slot-number reset
```



## 外部 TFTP サーバからのアップグレード

外部 TFTP サーバから CSM-S をアップグレードする手順は、次のとおりです。

- ステップ 1** TFTP CSM-S ランタイム イメージダウンロード用の VLAN をスーパーバイザ エンジン上に作成します。



(注) 既存の VLAN も使用できますが、確実にダウンロードするには、TFTP 接続専用の VLAN を作成する必要があります。

- ステップ 2** TFTP サーバに接続するインターフェイスを設定します。

- ステップ 3** インターフェイスを VLAN に追加します。

- ステップ 4** CSM-S の `vlan` コマンドを入力します。

詳細については、[第4章「VLAN の設定」](#)を参照してください。

- ステップ 5** CSM-S 用 VLAN に IP アドレスを追加します。

- ステップ 6** `show csm slot vlan detail` コマンドを入力し、設定を確認します。

詳細については、[第4章「VLAN の設定」](#)を参照してください。

- ステップ 7** CSM-S から TFTP サーバに接続できるかどうかを確認します。

```
Router# ping module csm csm-slot-number TFTP-server-IP-address
```

- ステップ 8** スーパーバイザ エンジンと CSM-S 間のセッションを確立します。

```
Router# session slot csm-slot-number processor 0
```

- ステップ 9** イメージをアップグレードします。

```
CSM> upgrade TFTP-server-IP-address c6slb-apc.rev-number.bin
```

- ステップ 10** CSM-S とのセッションを終了し、Cisco IOS プロンプトに戻ります。

```
CSM> exit
```

- ステップ 11** CSM-S の電源を切断して再投入するか、またはスーパーバイザ エンジンのコンソールから次のコマンドを入力して、CSM-S を再起動します。

```
Router# hw-module module csm-slot-number reset
```


## 失われたパスワードの回復

CSM-S 上の SSL のパスワードを回復する際は、システムに別のソフトウェア イメージをロードする必要がありません。パスワードを回復するには、CSM-S 前面パネル上の証明書管理ポートから、特別のコマンドを使用します。セキュリティ上の理由から、パスワードの回復はこのポートを介してのみ行われます。

失われた SSL パスワードを回復する場合、次の条件が適用されます。

- CSM および SSL ドータカードの両方にコンソール接続を行える必要があります。
- パスワードの回復処理中に SSL ドータカードが再起動されると、SSL ドータカード間のすべてのトラフィックが中断されます。
- 失われたパスワードを回復するには、次のプロンプトを使用します。
  - CSM> または VENUS (CSM コンソール用)
  - ssl-proxy# (SSL ドータカード用)

SSL ドータカード パスワードを回復する手順は、次のとおりです。

	コマンド	目的
ステップ 1	CSM> <b>venus</b>	Venus CLI をイネーブルにします。
ステップ 2	VENUS# <b>set_ssl_password_recovery 1</b>	SSL ドータカードがパスワード回復モードで再起動するようにします。このモードでは、SSL ドータカードに、イネーブル モードを開始するためのパスワードは必要ありません。
ステップ 3	ssl-proxy# <b>enable</b>	モジュール上でイネーブル モードを開始します。
ステップ 4	ssl-proxy# <b>copy nvram:startup-config running-config</b>	スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
ステップ 5	ssl-proxy# <b>configure terminal</b>	コンフィギュレーション モードを開始します。
ステップ 6	ssl-proxy(config)# <b>enable password password</b>	パスワードをイネーブルにします。   (注) このパスワードは、SSL ドータカードのイネーブル パスワードとして所有する新しいパスワードです。イネーブル パスワードが必要ない場合は、 <b>no enable password</b> コマンドを入力することができます。
ステップ 7	ssl-proxy(config)# <b>line vty start_line end_line</b>	イネーブル パスワードをリセットする仮想端末の開始 / 停止コンソール回線番号を設定します。
ステップ 8	ssl-proxy(config-line)# <b>login</b>	ログインします。
ステップ 9	ssl-proxy(config-line)# <b>password password</b>	仮想端末に設定する新しいイネーブル パスワードを入力します。
ステップ 10	ssl-proxy(config-line)# <b>end</b>	セッションを終了します。



注意

セキュリティの理由から、パスワードの回復後はすべての秘密鍵が使用できなくなります。

次に、SSL ドータカードの証明書管理コンソール ポートから、スロット 4 に搭載された SSL ドータカードの失われたパスワードを回復する例を示します。

```
CSM> venus
VENUS# set_ssl_password_recovery 4
ssl-proxy# enable
ssl-proxy# copy nvram:startup-config running-config
ssl-proxy# configure terminal
ssl-proxy(config)# enable password cisco
```



(注) **enable password cisco** コマンドを入力して、パスワードを **cisco** に設定します。

```
ssl-proxy(config)# line vty 0 4
ssl-proxy(config-line)# login
ssl-proxy(config-line)# password cisco
ssl-proxy(config-line)# end
```

SSL ドータカードのコンソール ポートから、バックアップ イメージからの鍵をインポートするか、鍵を再生成します。

鍵の生成およびインポートについては、「[鍵および証明書の設定](#)」(p.8-3) を参照してください。

