CHAPTER 1

製品概要

このマニュアルは、次のモジュールをサポートします。

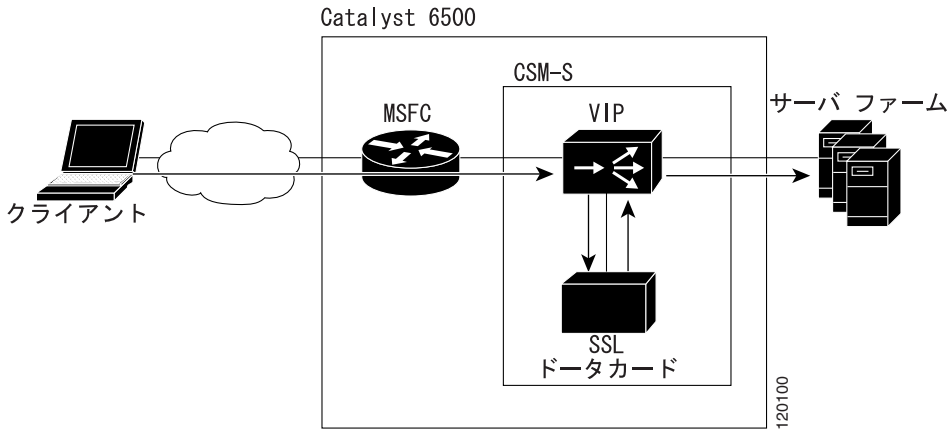
製品番号：WS-X6066-SLB-S-K9

Catalyst 6500 シリーズ Content Switching Module with SSL（CSM-S）は、高性能な Server Load Balancing（SLB）に Secure Socket Layer（SSL）オフロードを組み合わせています。CSM-S は、サーバ ファイアウォール、キャッシュ、Virtual Private Network（VPN; 仮想私設網）終端装置およびその他のネットワーク装置のグループ間でレイヤ 3 ～ 7 の情報を使用して、クライアント要求を分散するのに使用できます。CSM-S は、また CSM-S が優れたロードバランシングを実行しながら、安全なエンドツーエンドの暗号化を確保することができる SSL 暗号化トラフィックを終了および開始できます。

（注） *SSL ドータカード*は、SSL トランザクションを高速化する CSM-S の SSL 終端ドータカードについて言及します。

図 1-1 に、クライアントとサーバ ファーム間の CSM-S を介したトラフィック フローの概要を示します。サーバ ファームは、ロードバランスの対象装置からなるグループです。サーバ ファームを仮想サーバにすることによって、ネットワークのスケーラビリティとサービス アベイラビリティが向上します。仮想サーバのアベイラビリティに影響を与えることなく、いつでも新しいサーバを追加したり、故障したサーバまたは既存のサーバを除去したりできます。

図 1-1　CSM-S トラフィック フローの概要



クライアントを CSM-S に接続するには、仮想サーバの Virtual IP（VIP; 仮想 IP）アドレスに要求を送ります。クライアントが仮想サーバへの接続を開始すると、CSM-S は設定されたロードバランシング アルゴリズムおよびポリシー（アクセス ルール）に基づいて、接続用の実サーバ（サーバ ファームに割り当てられる物理装置）を選択します。ポリシーでは、クライアント接続の送り先を定義することによってトラフィックを管理します。

SSL によって暗号化された要求が届いた場合に、正しい実サーバを選択するために、CSM-S が復号化を実行し、最終的にレイヤ 7 のルールをクリア テキスト要求に適用するように設定できます。実サーバを選択するのにレイヤ 7 情報が必要な場合にだけ、復号化が行われます。エンドツーエンド暗号化が必要な場合、実サーバの選択が行われたあとに CSM-S が接続要求を再び暗号化します。この処理によって、実サーバへの要求が暗号化形式のままになります。

固定（sticky）接続は、送信元 IP アドレス、送信元 IP サブネット、Cookie、および SSL を使用して、同じクライアントからの複数の接続を同じ実サーバに *stick*（固定する）ことによって、または HTTP リダイレクト メッセージを使用してこれらの接続をリダイレクトすることによって、個々のサーバへのトラフィックを制限します。

ここでは、CSM-S について説明します。

機能

今回のソフトウェア リリースには、旧 CSM リリースからの SSL（CSM-S）機能をサポートするフィーチャ セットが含まれます。ここでは、表形式で次のフィーチャ セットを示します。

表 1-1 に、今回のリリースでの新しい CSM 機能を示します。

表 1-1　新しい CSM フィーチャ セットの説明

今回のリリースの新機能	説明
HTTP ヘッダー スティッキ	HTTP ヘッダーの内容（Mobile Station ISDN Number［MSISDN］、サービス キー、セッション ID など）に基づいて、固定処理を実行するように CSM を設定できます。
設定の同期化	フォールト トレラント VLAN（仮想 LAN）上のアクティブCSMおよびスタンバイCSM間の設定の同期化をサポートします。
インターフェイスおよびクリティカル デバイスのフェールオーバー トラッキング	Hot Standby Router Protocol（HSRP）グループ、物理インターフェイス、およびゲートウェイの状態を追跡できます。
Private VLAN（PVLAN; プライベート VLAN）	CSM で PVLAN を使用可能にします。
部分的なサーバ ファーム フェールオーバー	プライマリ サーバ ファームで部分的に障害が発生した場合に CSM がバックアップ サーバ ファームにフェールオーバーするように、バックアップ サーバ ファームの設定時にスレッシュホールド値を定義できます。
サーバ プローブ失敗ステートの改善	プローブに失敗したサーバを復旧するのに必要な再試行回数を指定できます。
実名オプション	エンティティに関する詳細を指定できます。このオプションは、プローブ、vserver、VLAN、およびサーバファームの各モードに適用できます。
Network Address Translation（NAT; ネットワーク アドレス変換）設定の拡張	送信元 NAT（NAT クライアント）設定のルールをポリシー レベルに提供します。
無限アイドル タイムアウト	接続を無期限でオープンのまま維持できます。
VIP の依存関係	複数の VIP を一括してリンクし、指定された VIP が停止するとそれに依存する VIP も自動的に停止させることができます。
ポリシーの順序	特定のポリシーにプライオリティ値を割り当てることができます。
最大解析長に達した場合の動作の変更	CSM は、最大解析長の接続要求をデフォルト ポリシーにロード バランシングします。
スロー スタートの改善	スロースタート タイマー値が期限切れになるか、または conn_count が他の実サーバの conn_count と等しくなるまで、実サーバをスロースタート モードにしておくことができます。
非セキュア ルータ モード	VIP にヒットしない非 SYN パケットに加え、SYN パケットをルーティングするために環境変数が拡張されました。
vserver の制限数の増加	特定の VIP で設定可能な仮想サーバ数を 128 から 1000 に増加しました。

表 1-2 に、以前のリリースで使用可能な CSM 機能を示します。

表 1-2　CSM フィーチャ セットの説明

機能
サポート対象ハードウェア
MSFC2 が搭載された Supervisor Engine 2
サポート対象プロトコル
TCP ロードバランシング
UDP 一般 IP プロトコル ロードバランシング
FTP（ファイル転送プロトコル）および Real Time Streaming Protocol（RTSP）に関する特殊なアプリケーション レイヤ サポート
Server Application State Protocol（SASP）
レイヤ 7 機能
完全正規表現照合
URL、Cookie スイッチング、一般 HTTP ヘッダー解析、HTTP メソッド解析
その他の機能
VIP 接続のウォーターマーク
バックアップ（ソーリー サーバ）およびサーバ ファーム
ヘルス プローブ用のオプション ポート
IP 再組み立て
TCL スクリプト
XML コンフィギュレーション インターフェイス
SNMP（簡易ネットワーク管理プロトコル）
Global Server Load Balancing（GSLB; グローバル サーバ ロードバランシング）— ライセンスが必要です。
リソース使用状況の表示
設定可能なアイドルおよび保留接続タイムアウト
単一方向フローのアイドル タイムアウト
SSL ロードバランシングの SSL サービス モジュール（SSLM）統合
実サーバ名
すべてのタイプのフロー（TCP、UDP、および IP）に関する TCP 接続の冗長性
フォールト トレラント **show** コマンドの拡張
IOS SLB FWLB の相互運用（IP リバーススティッキ）
同一シャーシに複数の CSM
同一シャーシでの CSM および IOS-SLB 機能の同時使用
設定可能な HTTP 1.1 の連続機能（同一サーバにすべての GET が作成される、または複数のサーバにバランシングされる）
全面的に設定可能な NAT
サーバ開始型接続
ルート ヘルス導入
ロードバランシング アルゴリズム
ラウンドロビン
Weighted Round-Robin（WRR; 重み付きラウンドロビン）
最小接続

表 1-2　CSM フィーチャ セットの説明（続き）

機能
重み付き最小接続
URL ハッシュ
送信元 IP ハッシュ（設定可能なマスク）
宛先 IP ハッシュ（設定可能なマスク）
送信元および宛先 IP ハッシュ（設定可能なマスク）
サポート対象ロードバランシング
SLB（TCP、UDP、または総称 IP プロトコル）
ファイアウォール ロードバランシング
Domain Name System（DNS; ドメイン ネーム システム）ロードバランシング
ステルス ファイアウォール ロードバランシング
トランスペアレント キャッシュ リダイレクト
リバース プロキシ キャッシュ
SSL オフロード
VPN-IPSec ロードバランシング
一般的な IP 装置とプロトコル
スティッキ性
設定可能なオフセットおよび長さを持つ Cookie sticky
SSL ID
送信元 IP（設定可能なマスク）
HTTP リダイレクト
冗長性
sticky ステート
完全ステートフル フェールオーバー（接続の冗長性）
ヘルス チェック
HTTP
Internet Control Message Protocol（ICMP）
Telnet
TCP
FTP
SMTP
DNS
戻りエラー コード チェック
帯域内ヘルス チェック
ユーザ定義による TCL スクリプト
管理
SNMP トラップ
SNMP および MIB（管理情報ベース）フルサポート
リモートの CSM 設定用の XML インターフェイス
バックエンド暗号化のサポート
ワークグループ マネージャのサポート
Server Application State Protocol（SASP）

表 1-3 に、今回のリリースの CSM-S 機能を示します。

表 1-3　CSM-S フィーチャ セットの説明

機能
サポート対象ハードウェア
MSFC2 が搭載された Supervisor Engine 2
サポート対象ソフトウェア
Cisco IOS Software Release 12.2(18)SXD（Supervisor Engine 2 および MSFC2 で稼働）
SSL 機能
SSL 開始
SSL version 2.0（SSLv2）転送
URL リライト
HTTP ヘッダー挿入
ワイルドカード プロキシ
ハンドシェイク プロトコル
SSL 3.0
SSL 3.1/TLS 1.0
SSL 2.0（ClientHello のみサポート）
セッション再利用
セッション再ネゴシエーション
セッション タイムアウト
対称アルゴリズム
ARC4
DES
3DES
非対称アルゴリズム
RSA
ハッシュ アルゴリズム
MD5
SHA1
暗号スイート
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_DES_CSC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
公開鍵基盤
最大 2048 ビットの証明書用の RSA 鍵ペア生成
CSM-S フラッシュ メモリ デバイスに鍵を安全に保存
クライアントおよびサーバ タイプのプロキシ サービスの証明書登録
鍵および証明書のインポートおよびエクスポート（PKCS12 および PEM）
鍵および証明書のインポートおよびエクスポート メカニズムを使用したスタンバイ CSM-S での鍵および証明書の複製
手動による鍵のアーカイブ、回復、およびバックアップ
CLI（コマンドライン インターフェイス）を使用した鍵および証明書の更新

表 1-3　CSM-S フィーチャ セットの説明（続き）

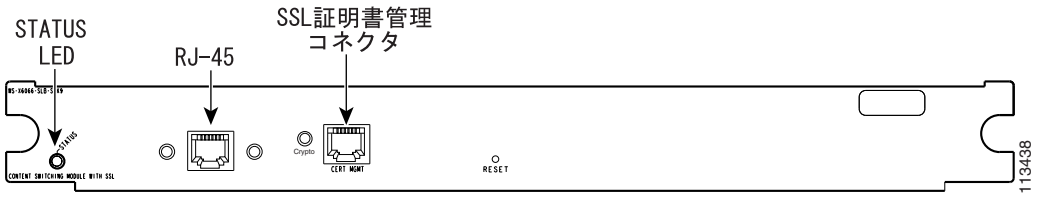
機能
期限切れの鍵および証明書の適正な書き替え
証明書の自動登録および自動更新
カット アンド ペーストまたは Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）による認証局証明書のインポート
最大 8 レベルの証明書チェーンの認証局
自己署名証明書の生成
PKCS10 CSR ファイルのカット アンド ペーストまたは TFTP を使用した手動の証明書登録
ピア（クライアントおよびサーバ）の証明書認証
ピア（クライアントおよびサーバ）の証明書
証明書セキュリティの属性ベース アクセス制御リスト
Certificate Revocation List（CRL; 証明書失効リスト）
証明書の期限切れ警告
TCP 終端
RFC 1323
接続エージング
接続レート
NAT[1] /PAT[2]
クライアントおよびサーバ
冗長性
CSM-S モジュールがスタンバイ状態である場合は、SSL サービスにアクセスできません。
冗長構成にするためには、2 つの CSM または 2 つの CSM-S のどちらかを使用する必要があります。サポート対象の冗長構成に CSM と CSM-S を混在させることはできません。
ハイ アベイラビリティ
障害検知（SLB ヘルス モニタリング方式）
モジュールレベルの冗長性（ステートレス）
サービス性
パスワードの回復
統計情報およびアカウンティング
プロキシ サービスごとの、SSL 接続試行回数の合計
プロキシ サービスごとの、正常に確立された SSL 接続数の合計
プロキシ サービスごとの、失敗した SSL 接続数の合計
プロキシ サービスごとの、SSL 警告エラー数の合計
プロキシ サービスごとの、SSL 再開セッション数の合計
プロキシ サービスごとの、暗号化および復号化されたパケット / バイト数の合計
1 秒、1 分、および 5 分あたりの CPU 利用率に関するトラフィック レートで表示される統計情報、および SSL 固有のカウンタ

1. NAT = Network Address Translation：ネットワーク アドレス変換
2. PAT = Port Address Translation：ポート アドレス変換

前面パネル

図 1-2 に、CSM-S の前面パネルを示します。

図 1-2　CSM の前面パネル



（注）　RJ-45 コネクタは着脱式プレートで覆われています。

（注）　CSM-S 証明書管理ポートに直接接続して、SSL ドータカードの初期設定を行う必要があります。この初期設定の完了後は、Secure Shell（SSH; セキュア シェル）または Telnet 接続を行い、さらに詳細にモジュールを設定できます。「SSL ドータカードの初期設定」（p.2）を参照してください。

LED

CSM-S の電源が入ると、各種ハードウェア コンポーネントが初期化され、スーパバイザ エンジンとの通信が行われます。STATUS LED は、スーパバイザ エンジンの動作と初期化の結果を示します。通常の初期化シーケンスの間に、STATUS LED は消灯状態からレッド、オレンジ、グリーンへと変化します。SSL ドータカードの CRYPTO LED は、今回のリリースでは使用されません。

（注）　スーパバイザ エンジンの LED の詳細については、『*Catalyst 6500 Series Switch Module Installation Guide*』を参照してください。

表 1-4 に、STATUS LED の動作を示します。

表 1-4　CSM の LED

LED	色	説明
STATUS	消灯	• モジュールはスーパバイザ エンジンからの電力供給を待機しています。 • モジュールはオンラインではありません。 • モジュールに電力が供給されていません。次の原因が考えられます。 — CSM-S に電力が供給されていない。 — モジュール温度が制限値を超えている[1]。
	レッド	• スーパバイザ エンジンによるリセットでモジュールが解放され、起動中です。 • ブート コードの実行に失敗した場合、LED は起動後もレッドのままです。
	オレンジ	• モジュールがハードウェアを初期化中、またはスーパバイザ エンジンと通信中です。 • 初期化シーケンス中にエラーが発生しました。 • モジュールは起動時に Field Programmable Gate Array（FPGA）をダウンロードできませんでしたが、初期化シーケンスを続行し、スーパバイザ エンジンからモジュール オンライン ステータスを得ます。 • モジュールはスーパバイザ エンジンからモジュール オンライン ステータスを得ていません。この問題は、CSM-S に発行された外部ループバック テストでスーパバイザ エンジンがエラーを検出した場合に発生します。
	グリーン	• モジュールは動作可能です。スーパバイザ エンジンからモジュールにモジュール オンライン ステータスが与えられています。
	グリーンからオレンジ	• スーパバイザ エンジンの CLI[2] で **set module disable** *mod* コマンドを使用した結果、モジュールがディセーブルになっています。
CRYPTO	なし	• 使用されません。今後のリリース用に確保されています。

1. CSM-S の 4 つの各センサーの温度を表示するには、**show environment temperature** *mod* コマンドを入力します。
2. CLI = コマンドライン インターフェイス

RJ-45 コネクタ

着脱式プレートで覆われた RJ-45 コネクタを使用して、管理ステーションまたはテスト装置を接続します。このコネクタはフィールド エンジニアがテストを行ったり、ダンプ情報を取得したりするために使用します。

SSL コネクタ

証明書管理ポート コネクタは、SSL 証明書管理に使用され、初期設定で SSL ドータカードに接続する必要がある場合に利用できます。この初期設定の完了後は、SSL ドータカードに SSH または Telnet 接続を行い、さらに詳細にモジュールを設定できます。詳細については、『*Catalyst 6500 Series Content Switching Module with SSL Installation and Configuration Note*』の Chapter 5 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

ここでは、SSL Services Module（SSLSM）および CSM-S コマンド機能の相違点について説明します。SSL サービス モジュール ソフトウェアの次のコマンドおよび機能は、CSM-S では利用できません。

- **debug ssl-proxy pc** コマンド
- スタンドアロン モードで HSRP を使用したステートレス冗長機能
- ssl-proxy サービス コンフィギュレーション モードの **virtual ipaddr ...** コマンドには、**secondary** キーワードが必要になります。**secondary** キーワードを使用せずにこのコマンドが設定すると、トラフィックのフローが失敗します。

  次に、例を示します。

  ```
  'virtual ipaddr 90.1.1.1 protocol tcp port 443'  is NOT supported.
  'virtual ipaddr 90.1.1.1 protocol tcp port 443 secondary'  is supported.
  ```

- SSL サービス モジュールのゲートウェイ転送機能は、CSM-S では機能しません。この機能は SSL サービス モジュールで使用され、SSL サービス モジュールにより多くのトラフィックが流れるようにします。

  次に、例を示します。

  ```
  ssl-proxy vlan 2
  ipaddr 190.1.1.142 255.255.255.0
  gateway 190.1.1.100 forward
  ```

  SSL ドータカードは CSM の VIP が行う接続に対するパケットだけを受信するので、この機能は CSM-S では機能しません。この機能は SSL サービス モジュールで使用され、SSL サービス モジュールにより多くのトラフィックが流れるようにします。

ソフトウェア バージョンの情報

CSM-S は、CSM と SSL サービス モジュールを組み合わせたものです。バージョン番号は、3 つの部分で構成されます。

CSM-S バージョン番号

CSM バージョン番号

SSL サービス モジュール バージョン番号

バージョン番号の形式は、次のようになります。

<CSM-S バージョン> <CSM バージョン> <SSL サービス モジュール バージョン>

たとえば、CSM-S の最初のソフトウェア リリースは次のように表示されます。

```
1.1(1) 4.1(3) 2.1(2
```

（注）　次の例では、バージョン番号が**太字**のテキストで強調されます。利用できる **show version** コマンドは 2 つあります。**show version** コマンドは、スーパバイザ エンジン CLI および SSL ドータカード CLI から利用できます。

（注）　**tech-support processor 0** コマンドは、CSM ソフトウェア バージョン番号を表示します。**show module** コマンドは、CSM と SSL が一緒になったソフトウェア バージョン番号を表示します。

次のような方法で、ソフトウェアのバージョン番号を表示できます。

- ここでは、CSM バージョンを表示するために、スーパバイザ エンジンからテクニカル サポート情報を表示する例を示します。

```
Router# show module csm 4 tech-support processor 0
Software version: 4.1(3)
```

- スーパバイザ エンジンから **show module** コマンドを使用する場合、次のようになります。

```
Router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  1    2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-SUP2-2GE    SAD055104SU
  2    2  Catalyst 6000 supervisor 2 (Hot)       WS-X6K-SUP2-2GE    SAL0702BJKF
  3    3  MWAM Module                            WS-SVC-MWAM-1      SAD071602TZ
  4    3  MWAM Module                            WS-SVC-MWAM-1      SAD071602UT
  5    3  MWAM Module                            WS-SVC-MWAM-1      SAD07200176
  7    0  Switching Fabric Module-136 (Active)   WS-X6500-SFM2      SAL06355FRR
  8   48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD03080474
  9    3  MWAM Module                            WS-SVC-MWAM-1      SAD0649019F
 11    0  CSM with SSL                           WS-X6066-SLB-S-K9  SAD07380300
 12    0  SLB Application Processor Complex      WS-X6066-SLB-APC   SAD061801NA
 13    1  SSL daughter card                             WS-SVC-SSL-1
SAD070303G2

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  0001.6415.ab56 to 0001.6415.ab57   3.2    7.1(1)       12.2(TETONS_ Ok
  2  0006.d65c.5c78 to 0006.d65c.5c79   4.1    7.1(1)       12.2(TETONS_ Ok
  3  0003.feab.9738 to 0003.feab.973f   2.0    7.2(1)       2.1(0.3b)    Ok
  4  0002.fcbe.8500 to 0002.fcbe.8507   2.0    7.2(1)       2.1(0.3b)    Ok
  5  0003.feab.80c8 to 0003.feab.80cf   2.0    7.2(1)       2.1(0.1b)    Ok
  7  0001.0002.0003 to 0001.0002.0003   1.2    6.1(3)       8.3(0.63)TET Ok
  8  0060.09ff.f5c0 to 0060.09ff.f5ef   0.701 4.2(0.24)VAI 8.3(0.63)TET Ok
  9  0005.9a3b.9de8 to 0005.9a3b.9def   0.304 7.2(1)       1.0(0.1)     Ok
 11  0003.feac.a958 to 0003.feac.a95f   1.7                1.1(1)       Ok
 12  00d0.d32f.03f8 to 00d0.d32f.03ff   1.5                3.1(6)       Ok
 13  0040.0bf0.1c04 to 0040.0bf0.1c0b   1.2    7.2(1)       2.1(0.59)    Ok
```

- 次に、SSL ドータカード CLI から SSL プロキシ バージョンを表示する例を示します。

```
ssl-proxy> show ssl-proxy version
Cisco Internetwork Operating System Software
IOS (tm) SVCSSL Software (SVCSSL-K9Y9-M), Version 12.2(14.6)SHK(0.28)  INTERIM TEST
SOFTWARE
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Tue 04-May-04 11:05 by integ
Image text-base: 0x00400078, data-base: 0x00B04000

ROM: System Bootstrap, Version 12.2(15)YS1 RELEASE SOFTWARE

ssl-proxy uptime is 0 minutes
System returned to ROM by power-on
System image file is "tftp://255.255.255.255/unknown"
AP Version 1.1(1) 4.1(1) 2.1(1)
```

設定の制約事項

SSL ドータカードによって処理される SSL フローは、CSM によってのみ処理されるフローです。SSL ドータカードは、CSM によってロードバランシングされないフローをオフロードできません。

SSL ドータカードに設定されるすべての VLAN は、CSM にも設定される必要があります。CSM に設定されていない場合、その VLAN に対するトラフィックは SSL ドータカードに届きません。

（注）　CSM および SSL ドータカード間では、設定の確認が行われません。CSM 部分の設定だけが終了すると、SSL ドータカードがまだ設定されていなくてもローカル実サーバが動作可能な状態で表示されます。ローカル実サーバのステータスは、常に動作可能な状態になります。これらの実サーバはドータカードに設定されるので、常に利用できる状態とみなされます。

CSM-S 動作の概要

特定の VLAN の設定の場合、クライアントおよびサーバは、レイヤ 2 およびレイヤ 3 テクノロジーを使用して、CSM-S を介して通信します（図 1-3 を参照）。単純な SLB では、クライアントはクライアント側 VLAN に、サーバはサーバ側 VLAN に接続します。サーバおよびクライアントは異なるサブネット上に配置できます。レイヤ 3 ホップで 1 つまたは複数離れた位置にサーバを配置し、ルータを介して CSM-S に接続することもできます。

クライアントはモジュールの VIP アドレスのいずれかに要求を送信します。CSM-S はこの要求を応じることのできるサーバに転送します。サーバはさらに、CSM-S に応答を転送し、CSM-S がクライアントにその応答を転送します。

クライアント側およびサーバ側 VLAN が同じサブネット上にある場合は、CSM-S をシングル サブネット（ブリッジ）モードで設定することができます。詳細については、「シングル サブネット（ブリッジ）モードの設定」（p.2-2）を参照してください。

クライアント側およびサーバ側 VLAN が異なるサブネット上にある場合は、セキュア（ルータ）モードで動作するように CSM-S を設定できます。詳細については、「セキュア（ルータ）モードの設定」（p.2-4）を参照してください。

冗長 CSM-S モジュールを使用して、セキュア（ルータ）モードまたはシングル サブネット（ブリッジ）モードのどちらでもフォールトトレラント構成を設定できます。詳細については、「フォールトトレランスの設定」（p.9-2）を参照してください。

複数の VLAN を使用して、シングル サブネット（ブリッジ）モードおよびセキュア（ルータ）モードを同じ CSM-S で共存させることができます。

図 1-3　CSM-S およびサーバ

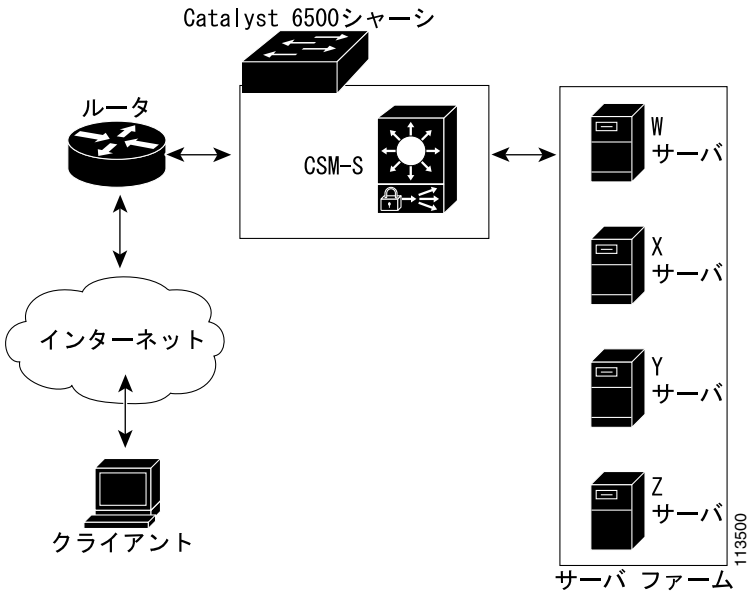
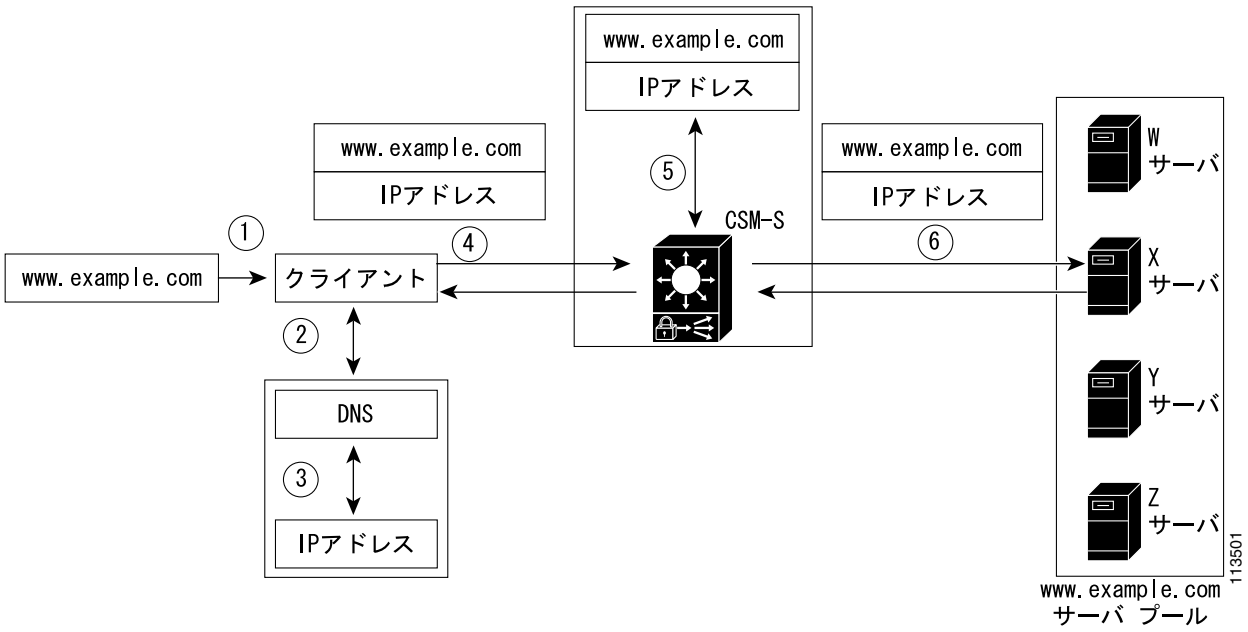


図 1-4 では、CSM-S 環境のクライアントとサーバ間でトラフィックが送信される仕組みについて説明します。

図 1-4　クライアントとサーバ間のトラフィック フロー



（注）　図 1-4 の番号は、次の作業の番号と対応しています。

URL を入力して情報を要求した場合、トラフィック フローは次のようになります。

1. URL を入力します（図 1-4 の例では、www.example.com）。
2. クライアントは DNS サーバにアクセスして、URL に関連付けられている IP アドレスを検索します。
3. DNS サーバは VIP の IP アドレスをクライアントに送信します。
4. クライアントはその IP アドレス（CSM-S VIP）を使用して、HTTP 要求を CSM-S に送信します。
5. CSM は URL と要求を受信し、ロードバランス上の決定を行い、サーバを選択します。

   たとえば、図 1-4 では、CSM-S は www.example.com サーバ プールからサーバ（X サーバ）を選択し、その VIP アドレスを X サーバのアドレスで置き換えて（directed モード）、トラフィックを X サーバに転送します。NAT サーバ オプションがディセーブルの場合、VIP アドレスは変わりません（dispatch モード）。
6. CSM-S は NAT を実行し、最終的に TCP シーケンス番号変換を行います。

SSL を統合した CSM-S の動作

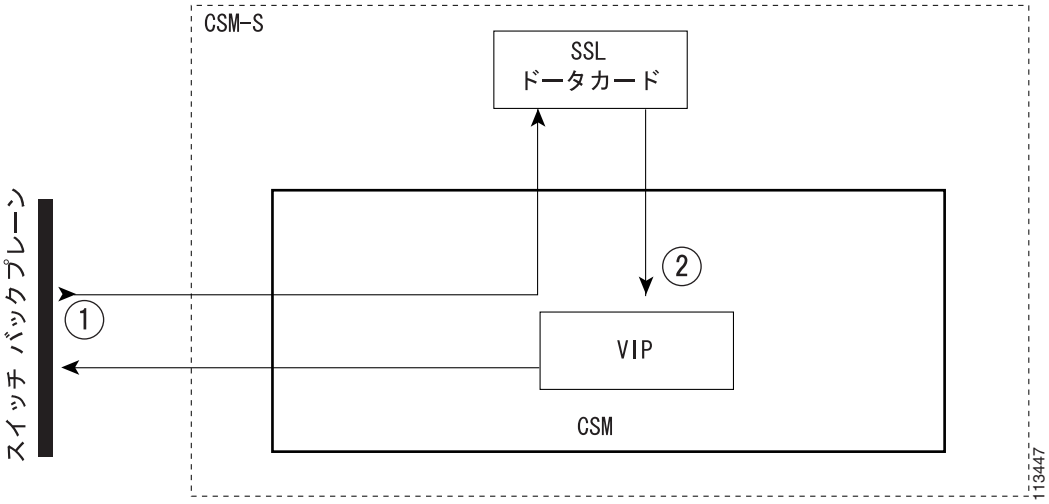
CSM-S は、内蔵ドータカードで統合的な SSL のサポートを行う CSM であるので、ロードバランシングと SSL モジュールとの通信は、CSM-S に対してローカルです。CSM-S の構成は、CSM と SSL サービス モジュールの組み合わせになります。図 1-5 を参照してください。

（注）　仮想サーバが SSL 処理に設定されており、モジュール上に VLAN が設定されている場合にだけ、SSL サービスを利用することができます。

ドータカード間のすべてのパケットは、CSM を介してルーティングされます。

CSM ハードウェアおよび SSL ドータカードは疎結合ですが、CSM はローカルに接続されていることを認識した特別な実サーバとして SSL ドータカードを扱います。

図 1-5　CSM-S のハードウェア構成



ドータカードは、Cisco IOS Software Release 12.2(18)SXD がサポートする SSL Release 2.1 を含む SSL リリースまでの SSL ソフトウェア機能を実行します。CSM-S のサポート対象機能のリストについては、「機能」（p.1-3）を参照してください。

ソフトウェアは CSM および SSL ドータカードの両方で独立して稼働します。CSM-S ソフトウェアを使用すると、SSL を設定し、ドータカード間のフローを処理できます。Cisco IOS ソフトウェアは、Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）をイネーブルにし、CSM-S が SSL データ フローを処理するために証明書および鍵をロードおよび生成し、SSL ソフトウェアを設定できるようにします。

SSL 機能を設定するには、証明書管理ポートからドータカードにアクセスする必要があります。CSM-S ベースボードには、ドータカードの起動要求に応じて、IP アドレスおよびロードする SSL イメージを含む起動情報を提供する BOOTP サーバが含まれます。

（注）　CSM-S を初めて起動すると、時間が 1970 年 1 月 1 日から開始します。CSM と SSL ドータカード（CSM-S システム）がアップの状態になると、スイッチ スーパバイザ エンジンの時間に同期します。

初起動時の時間の同期化条件によって証明書の期限が切れたことを示す Syslog メッセージが SSL ドータカードのコンソールに表示される場合があります。スーパバイザ エンジンからクロックの同期化が行われると（Syslog メッセージの生成後、数秒以内に行われる）、CSM-S がトラフィックを送れるようになります。

CSM-S がトラフィックを送れるかどうかを判別するには、Router# **show module csm** *slot* # **status** コマンドを使用します。

show module csm *slot* # **status** コマンドを入力すると、2 つのタイプの Syslog メッセージが表示されます。

1. モジュールがトラフィックを送ることができる場合は、次のメッセージが表示されます。

```
SLB Module is online in slot 4.
Configuration Download state: COMPLETE, SUCCESS
```

2. モジュールがトラフィックを送ることができない場合は、次のメッセージが表示されます。

```
SLB Module is offline.
Requires CSM module version 3.1.
```

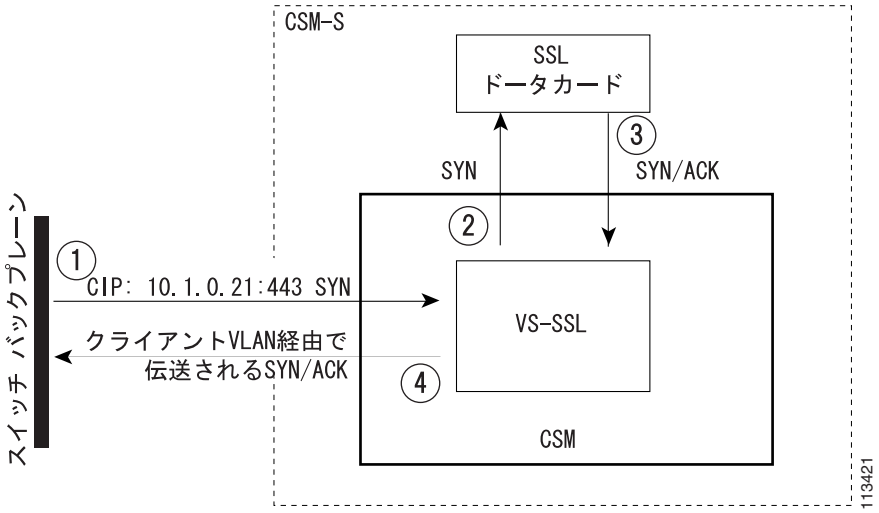
CSM-S の実行時の起動シーケンスは、次のとおりです。

1. CSM-S が起動します。
2. CSM-S がドータカードをリセットします。ドータカードがメモリ テストを実行します。
3. メモリ テストが完了すると、ドータカードの ROMMON が BOOTP 要求を CSM-S に送信します。
4. CSM-S は、MAC（メディア アクセス制御）アドレス、EOBC IP アドレス、およびドータカードのランタイム イメージをロードするフラッシュ ロケーションを含む BOOTP 応答を送信します。
5. SSL Cisco IOS ランタイムが開始すると、SSL コンソールがアクティブになります。
6. SSL ソフトウェアは、CSM に時間要求を送信します。
7. CSM-S は、オンライン状態にできることをスイッチ スーパバイザ エンジンに伝えます。

クライアント側の設定によるトラフィック フロー

図 1-6 では、ポート 443 でクライアントのトラフィックを受け入れるように、レイヤ 4 仮想サーバを CSM に設定する必要があります。この仮想サーバに関連付けられたサーバ ファームには、仮想サーバと同じ VIP アドレスが設定され、ローカルとしてマーキングされる必要があります。仮想サーバをローカルとしてマーキングすることは、このサーバが SSL ドータカード上にあることを CSM に示します。トラフィックをドータカードに正常に転送するために、テーブルが更新されます。

図 1-6　CSM-S のクライアント側の構成



（注）　図 1-6 の番号は、次の作業の番号と対応しています。

クライアント側の設定によるトラフィック フローは、次のとおりです。

1. クライアントの SYN フレームが CSM で受信され、SSL 仮想サーバに一致すると、CSM はレイヤ 4 仮想サーバと同じように処理します。
2. 宛先の決定によって、この接続の後続のすべてのクライアント トラフィックが SSL ドータカードに送られるように内部の CSM テーブルが設定されます。ドータカードからクライアントにトラフィックを送り返すために、リバース タプルも設定されます。SYN パケットが、処理するために SSL ドータカードに送られます。
3. SSL ドータカードは、SYN フレームを処理し、接続用の内部テーブルを設定します。次に、SSL ドータカードは SYN/ACK でクライアントに応答します。
4. SYN/ACK は、CSM によって受信され、リバース タプルで処理されます。次に、SYN/ACK がクライアント VLAN 経由でクライアントに伝送されます。

次に、クライアント側の CSM の設定例を示します。

```
 vlan 420 client
  ip address 192.168.15.109 255.255.255.0
!
 serverfarm SSL
  nat server
  no nat client
  real 192.168.15.100 local
   inservice
!
 vserver V-SSL
  virtual 192.168.15.200 tcp https
  serverfarm SSL
  persistent rebalance
  inservice
```

次に、クライアント側の SSL ドータカードの設定例を示します。

```
ssl-proxy service server_proxy
 virtual ipaddr 192.168.15.100 protocol tcp port 443 secondary
 server ipaddr 192.168.15.200 protocol tcp port 80
 certificate rsa general-purpose trustpoint tier1_tp
 inservice
ssl-proxy vlan 420
 ipaddr 192.168.15.108 255.255.255.0
```

サーバ側の設定によるトラフィック フロー

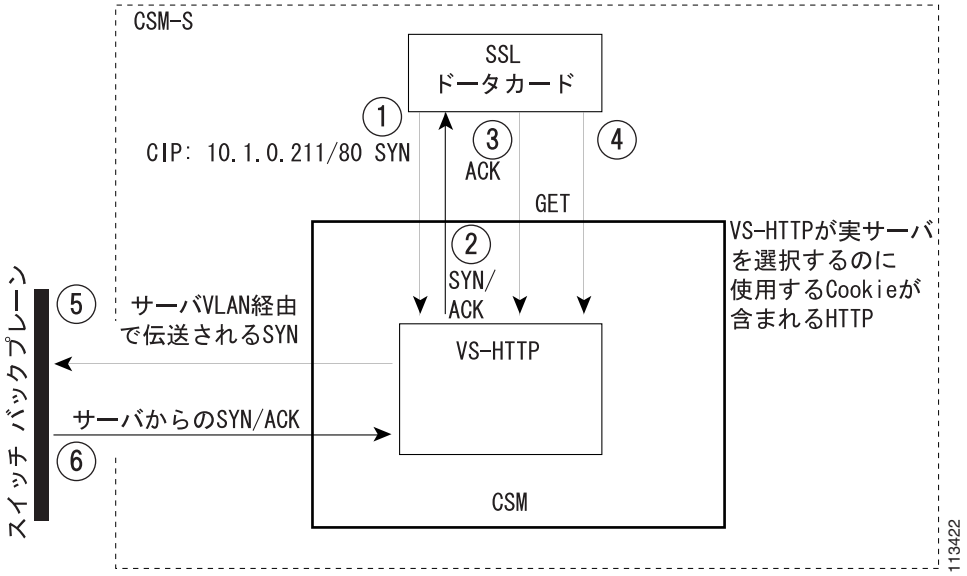
SSL ドータカードが SSL 接続を終了する場合、SSL ドータカードは要求に対応するバックエンド サーバへの接続を確立する必要があります。サーバは、ネットワーク内の実サーバ、または CSM に設定された仮想サーバのどちらでも構いません。

（注）　CSM および SSL ドータカード間では、設定の確認が行われません。CSM と SSL ドータカードが正しく設定されていることを確認し、SSL ドータカードがレイヤ 7 のロードバランシング用に CSM の仮想サーバを使用できるようにする必要があります。

バックエンド サーバとしての CSM の設定

図 1-7 に、バックエンド サーバがレイヤ 7 仮想サーバである場合の構成を示します。VS2 の仮想サーバは、SSL ドータカードの ssl-proxy サーバ設定に一致するように設定されます。

図 1-7　CSM-S のサーバ側の構成（バックエンド サーバとして CSM を設定する場合）



（注）　図 1-7 の番号は、次の作業の番号と対応しています。

サーバ側の設定によるトラフィック フロー（バックエンド サーバとして CSM を設定する場合）は、次のとおりです。

1. SSL ドータカードは、ssl-proxy サービスのターゲット アドレスに TCP SYN フレームを伝送します。
2. CSM は、VS-HTTP に送信された SYN に対して SYN/ACK でクライアント IP アドレスに応答し、SYN/ACK が SSL ドータカードに送信されます。
3. SSL ドータカードは、CSM 仮想サーバ VS-HTTP に TCP ACK を送信して、TCP ハンドシェイクを完了します。
4. SSL ドータカードは、復号化された HTTP GET 要求を CSM 仮想サーバ VS-HTTP に送信します。CSM がこの要求を受信すると、CSM はこの Cookie 値を使用して、実際の実サーバを判別します。
5. CSM は、クライアントとして実サーバに TCP SYN を送信します。
6. 実サーバは、TCP SYN/ACK で応答します。
7. CSM は、システムのレイヤ 5 およびレイヤ 7 のフローに対して行う動作と同じ動作を継続します。

次に、サーバ側の CSM の設定例を示します。

```
vlan 421 server
  ip address 192.168.17.109 255.255.255.0
!
 serverfarm SLB
  nat server
  no nat client
  real 192.168.17.13
   inservice
!
 vserver VS-HTTP
  virtual 192.168.15.200 tcp www
  serverfarm SLB
  persistent rebalance
  inservice
```

次に、サーバ側の SSL ドータカードの設定例を示します。

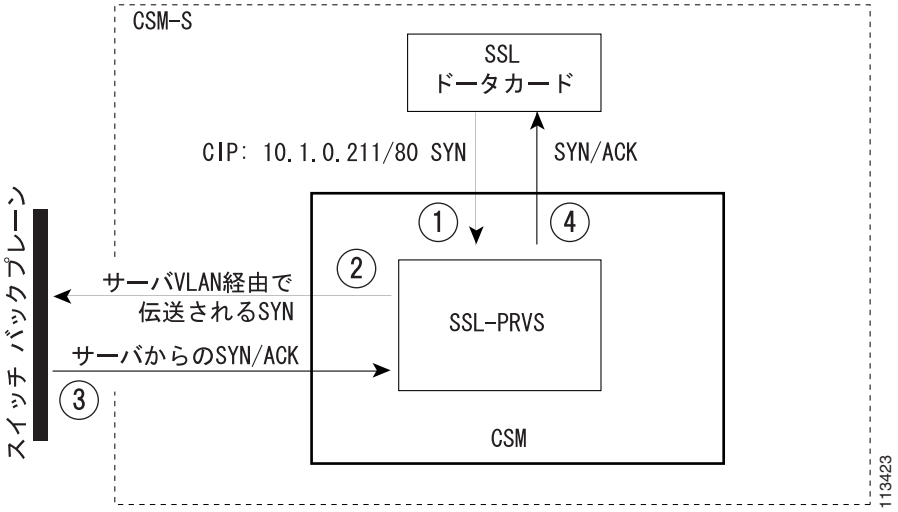
```
ssl-proxy service server_proxy
 virtual ipaddr 192.168.15.100 protocol tcp port 443 secondary
 server ipaddr 192.168.15.200 protocol tcp port 80
 certificate rsa general-purpose trustpoint tier1_tp
 inservice
```

バックエンド サーバとしての実サーバの設定

バックエンド サーバとして実サーバを設定する場合、SSL ドータカードには、ssl-proxy サーバ アドレスとして実サーバの IP アドレスが設定されます。トラフィックの送信元は実サーバとなり、CSM が SSL ドータカードからのトラフィックを実サーバとの間でやりとりします。

図 1-8 に表示されるように、CSM には、プレディクタ転送オプションを設定したサーバ ファームを使用して、仮想サーバ SSL-PRVS が設定されています。実サーバの IP アドレスにトラフィックを正常に転送するには、CSM は可能なすべての実サーバに対して Address Resolution Protocol（ARP）を実行する必要があります。ARP 解決が正しく実行されるには、サーバ ファームの SSL 実サーバに可能なすべての実サーバの IP アドレスが含まれており、CSM 上の仮想サーバに関連付けられないようにする必要があります。ヘルス プローブを実サーバに関連付けることもできます。

図 1-8　CSM-S のサーバ側の構成（バックエンド サーバとして実サーバを設定する場合）



（注）　図 1-8 の番号は、次の作業の番号と対応しています。

サーバ側の設定によるトラフィック フロー（バックエンド サーバとして実サーバを設定する場合）は、次のとおりです。

1. SSL ドータカードが ssl-proxy サービスのサーバ アドレスに TCP SYN フレームを伝送し、仮想サーバ SSL-PRVS に照合するために、CSM でそのフレームが受信されます。
2. ロードバランシングの決定が行われ、プレディクタ転送のサーバ ファーム設定に基づいて、フレームがサーバに転送されます。サーバからの SSL ドータカード宛てのトラフィックを取得するために、リバース タプルがプログラムされます。フレームがサーバ VLAN 経由で伝送されます。
3. サーバ VLAN で SYN/ACK フレームが受信されると、リバース タプル設定と照合し、SSL ドータカードであるクライアントにフレームが送り返されます。
4. SYN/ACK が SSL ドータカードに送信されます。

```
vlan 421 server
ip address 192.168.17.109 255.255.255.0
serverfarm SSLPF
  nat server
  no nat client
  predictor forward
vserver SSL-PFVS
  virtual 0.0.0.0 0.0.0.0 tcp 8888
  vlan local
  serverfarm SSLPF
  persistent rebalance
  inservice
```

次に、クライアント側とサーバ側の SSL ドータカードの設定例を示します。

```
ssl-proxy service server_proxy
 virtual ipaddr 192.168.15.100 protocol tcp port 443 secondary
 server ipaddr 192.168.17.13 protocol tcp port 8888
 certificate rsa general-purpose trustpoint tier1_tp
 inservice
ssl-proxy vlan 420
 ipaddr 192.168.15.108 255.255.255.0
ssl-proxy vlan 421
 ipaddr 192.168.17.108 255.255.255.0
```