



製品概要

Catalyst 6500 シリーズ Content Switching Module (CSM; コンテント スイッチング モジュール) は、レイヤ 3 ～ 7 までのパケット情報に基づき、サーバ グループ、サーバ ファーム、ファイアウォール、キャッシュ、VPN 終端デバイス、およびその他のネットワーク デバイスの間で負荷を分散する高性能な Server Load Balancing (SLB; サーバ ロードバランシング) を提供します。

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ルABILITYとサービス AVAILABILITYが向上します。仮想サーバの AVAILABILITY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。

クライアントを CSM に接続するには、仮想サーバの 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 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。

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 Secure Socket Layer (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 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 について説明します。

- [機能 \(p.1-2\)](#)
- [前面パネル \(p.1-6\)](#)
- [CSM の動作 \(p.1-8\)](#)
- [CSM のトラフィック フロー \(p.1-9\)](#)

機能

今回のソフトウェア リリースには、旧リリースからの CSM 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、このリリースの新しい 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

このリリースの新機能	説明
HTTP ヘッダーの固定	HTTP ヘッダーの内容（たとえば、MSISDN ¹ 番号、サービス キー、セッション ID など）に基づいて固定処理を行うように CSM を設定できます。
設定の同期化	フォールトトレランス VLAN を経由したアクティブ CSM とスタンバイ CSM 間の設定の同期化をサポートします。
インターフェイスと重要なデバイスのフェールオーバー トラッキング	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。
プライベート VLAN	CSM で Private VLAN (PVLAN; プライベート VLAN) 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ホールドの値を定義できます。
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ために必要となる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、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) 設定の拡張機能	送信元 NAT (NAT クライアント) の設定ルールをポリシー レベルにまで向上させることができます。
無限アイドル タイムアウト	無期限で接続をオープンなまま維持できます。
VIP の依存関係	複数の VIP を一括してリンクし、指定した VIP が停止するとそれに従属する VIP も自動的に停止する機能を提供します。
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。
解析可能な最大長に達したときの動作の変更	CSM は、解析可能な最大長の接続要求を複数のデフォルト 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 タイマーが期限切れになるか、conn_count 値がその他の実サーバの conn_count 値と等しくなるまで、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	SYN パケット以外に、VIP にヒットしない非 SYN パケットもルーティングするように環境変数が拡張されました。

表 1-1 新しい CSM フィーチャ セットの説明 (続き)

このリリースの新機能	説明
vserver の制限数を増加	特定の VIP ごとに設定可能な仮想サーバの数が 128 から 1000 に増えています。
リモート デスクトップ プロトコル	MSTS-RDP を設定するための環境変数が追加されています。 ²

1. MSISDN = Mobile Station ISDN; モバイル ステーション ISDN
2. MSTS-RDP = Microsoft Terminal Services Remote Desktop Protocol

表 1-2 に、このリリースと旧リリースに対応している 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
Supervisor 1A (Multilayer Switch Feature Card [MSFC; マルチレイヤ スイッチ フィーチャ カード] および Policy Feature Card [PFC; ポリシー フィーチャ カード] 内蔵)
Supervisor 2 (MSFC および PFC 内蔵)
Supervisor 720 — CSM ソフトウェア Release 3.1(4) 以上が必要です。
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 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 STE 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 リバーススティック)

表 1-2 CSM フィーチャ セットの説明 (続き)

機能
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)
実サーバに対してスロースタートできるようにする最小接続機能
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
DNS 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
スティッキー性
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)

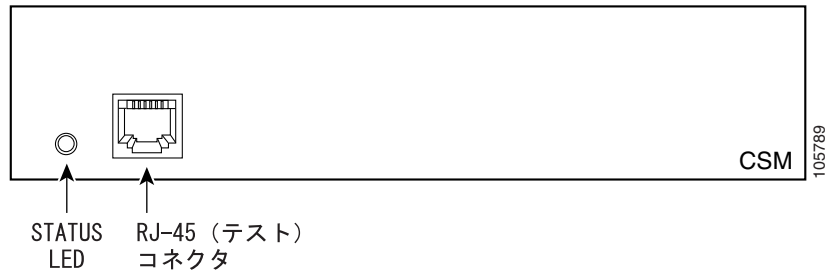
表 1-2 CSM フィーチャ セットの説明 (続き)

機能
ヘルス チェック
HTTP
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 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)

前面パネル

図 1-1 に、CSM の前面パネルを示します。

図 1-1 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。

STATUS LED

CSM 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、スーパーバイザ エンジンとの通信が行われます。STATUS LED は、スーパーバイザ 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。



(注) スーパーバイザ 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 1-3 に、STATUS LED の動作を示します。

表 1-3 CSM の STATUS LED

色	説明
消灯	<ul style="list-style-type: none"> モジュールはスーパーバイザ 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。 <ul style="list-style-type: none"> CSM 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	<ul style="list-style-type: none"> スーパーバイザ 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。

表 1-3 CSM の STATUS LED (続き)

色	説明
オレンジ	<ul style="list-style-type: none"> モジュールがハードウェアを初期化中、またはスーパーバイザ 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 FPGA² 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、スーパーバイザ 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ーバイザ 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 に発行された外部ループバック テストでスーパーバイザ 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	<ul style="list-style-type: none"> モジュールは動作可能です。スーパーバイザ 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	<ul style="list-style-type: none"> スーパーバイザ エンジンの CLI³ 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。

1. CSM 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. FPGA = Field Programmable Gate Arrays
3. 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。

CSM の動作

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 を介して通信します (図 1-2 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 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 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 に応答を転送し、CSM がクライアントにその応答を転送します。

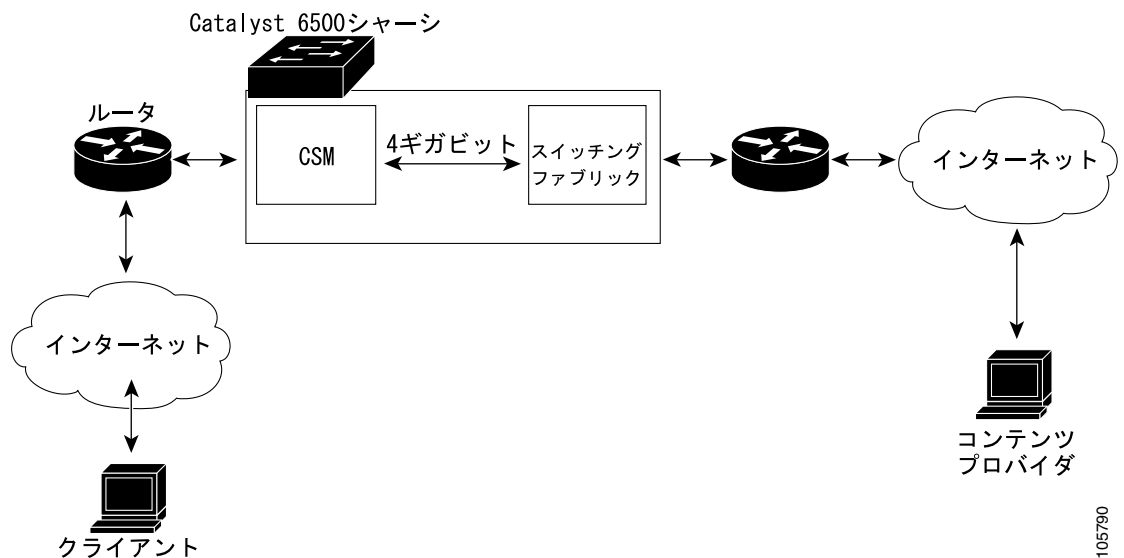
クライアント側およびサーバ側 VLAN が同じサブネット上にある場合は、CSM をシングルサブネット (ブリッジ) モードで設定することができます。詳細については、「[シングルサブネット \(ブリッジ\) モードの設定](#)」(p.2-2) を参照してください。

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 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 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.7-2) 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 で共存させることができます。

図 1-2 CSM およびサーバ

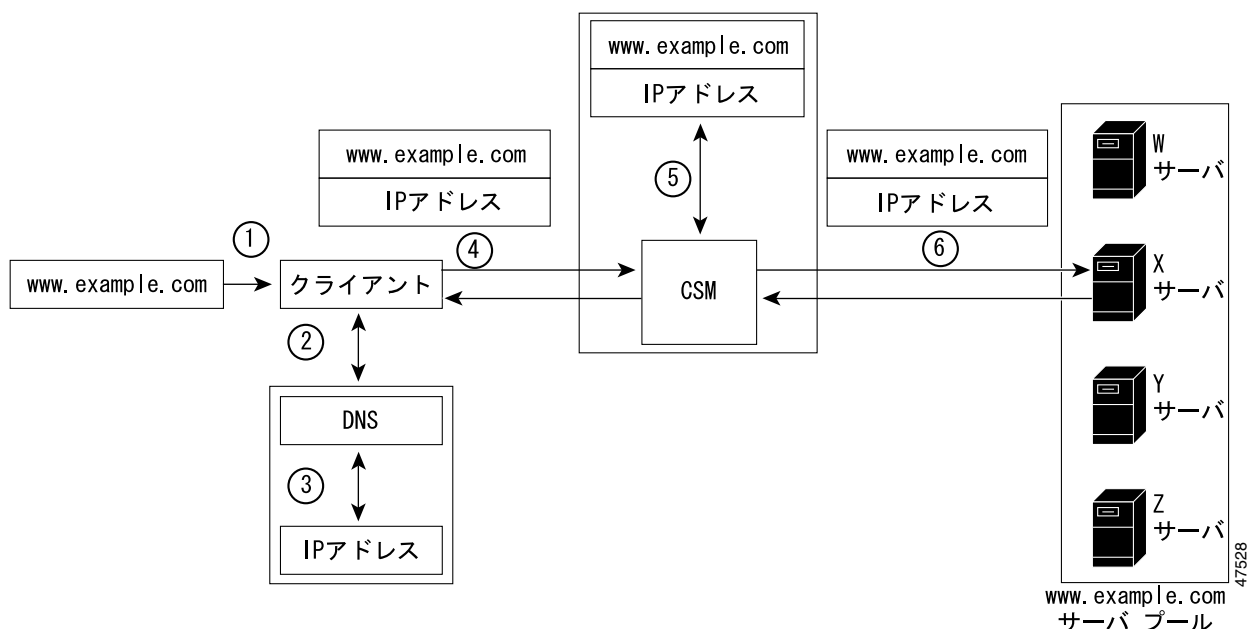


105790

CSM のトラフィック フロー

ここでは、CSM 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 1-3 を参照)。

図 1-3 クライアントとサーバ間のトラフィック フロー



(注)

図 1-3 の番号は、次の手順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 1-3 では、例として `www.example.com` と示されています)。
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 VIP) を使用して、HTTP 要求を CSM 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 1-3 では、CSM 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 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。

