データ シート

Cisco Catalyst 6500 シリーズ SSL 対応 コンテント スイッチング モジュール

Cisco® Content Switching Module with SSL（CSM-S; SSL 対応コンテント スイッチング モジュール）は、レイヤ 4 ～ 7 のコンテント スイッチング機能を Secure Socket Layer（SSL）アクセラレーション機能とともに 1 つのライン カードに集積した、Cisco Catalyst® 6500 シリーズ スイッチ用ソリューションです。これら 2 つのテクノロジーを組み合わせることにより、セキュアなエンドツーエンド接続をアプリケーションに提供し、高度なコンテント スイッチング機能を実現します。このように 2 つの機能が統合されていることで、Cisco CSM-S は、SSL セッションのデータ フィールドまたはヘッダーに含まれる、暗号化された情報を利用したロードバランシングを行います。また、SSL セッション ID 以外の情報も使用できるため、コンテント スイッチはより柔軟性に富んだセッション保持が可能です。これらすべての機能は、ネットワーク上での情報の暗号化を維持したまま、単一モジュール内で実行されます。金融データや医療記録など、機密性の高い顧客情報を扱うビジネスにとって、このようなセキュリティ機能は欠かすことのできない条件です。

SSL 終端処理をバックエンド サーバからなくすことによって、これらのサーバにかかる高いプロセッサ負荷が取り除かれ、増大する SSL 要求に対応するためのサーバを新たに追加する必要がなくなります。Cisco CSM-S のような集中型デバイスで SSL を処理すれば、必要とされるデジタル証明書の数が減り、これらの証明書を管理する手間が最小化されます。

Cisco CSM-S は、ネットワーク セッションとサーバ負荷状況をリアルタイムで追跡しながら、クライアント要求を適切なデバイスに送信することで、高速なコンテンツ配信ネットワークの要件を満たします（図 1）。

図 1　Cisco CSM-S

Cisco CSM-S には、次の利点があります。

- **実証済みのプラットフォームに基づくテクノロジー** — Cisco CSM-S は、Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータ用の CSM と SSL サービス モジュール（SSLSM）の利点と機能を統合した製品です。
- **データ センターのパフォーマンスに最適化** — Cisco CSM-S を採用すると、サーバ ファーム、キャッシュ クラスタ、および一連の VPN およびファイアウォール デバイスのスケーラビリティとパフォーマンスが向上します。

- **安全なエンドツーエンドの暗号化** — Cisco CSM-S は、SSL トラフィックを終端処理して、ロードバランシングをインテリジェントに決定し、トラフィックを再暗号化してから、ネットワークに再送信することができます。これらの機能により、ネットワーク上では情報を暗号化したままで、通常は暗号化されているために利用できない SSL セッションの情報を使って、高度なコンテント スイッチング機能を実行します。
- **優れた価格性能比** — Cisco CSM-S は、コンテント スイッチングと SSL のどちらについても安価な接続コストを実現しています。また、新規または既存の Cisco Catalyst 6500 シリーズ シャーシのスロットに装着されるため、占有面積も少なくて済みます。
- **SSL インフラストラクチャのコストと複雑さの軽減** — Cisco CSM-S では、SSL 終端処理をネットワーク内で一元化するため、この処理要求への対応に必要なサーバ台数を削減できます。また、サイトごとに要求される証明書の数も減るため、コストの節減につながります。さらに、複数の証明書の管理に伴う複雑さも排除します。
- **容易な設定** — Cisco CSM-S は、Cisco Catalyst 6500 シリーズ スイッチの設定にも使用される Cisco IOS® ソフトウェアの CLI（コマンドライン インターフェイス）を使用します。
- **既存のインフラストラクチャの強化** — Cisco CSM-S を新規または既存の Cisco Catalyst 6500 シリーズ スイッチに追加することにより、SSL をオフロードしたうえで、Cisco Catalyst スイッチのすべてのポートでレイヤ 2 ～ 7 のサービスを実行できます。
- **セッション保持** — この機能により、送信元 IP アドレス、クッキー、HTTP リダイレクション、または SSL セッション ID によるセッション保持が可能になります。セッション中に、クライアントが新しいセッション ID を要求した場合でも、Cisco CSM-S はセッション保持を実現します。
- **スケーラビリティの高いパフォーマンス** — 最大 4 枚のモジュールを単一シャーシ内に搭載できる Cisco CSM-S は、増大するコンテント スイッチングと SSL の要件に対応できるソリューションを提供します。

Cisco CSM-S の機能

高性能

Cisco CSM-S は、1 秒あたり最大 165,000 の新規レイヤ 4 TCP 接続と、最大 100 万の同時接続を確立します。SYN Cookie Distributed-Denial-of-Service（DDoS）機能を有効にすれば、毎秒 30 万以上の接続を確立することが可能となります。これらの接続は、使用可能な任意のスイッチ ポートを通じて 4,000 台の仮想サーバに送信され、さらに最大 16,000 台の実サーバまたはデバイスに分散されます。また、20,000 の同時 SSL 接続を維持して、100 Mbps のバルク暗号化処理を行いながら、1 秒あたり最大 1,000 の SSL トランザクションをサポートします。1 台の Cisco Catalyst 6500 シリーズ シャーシには最大 4 枚までの Cisco CSM-S モジュールを搭載できるため、スケーラブルなパフォーマンスが提供されます。さらに、1 つまたは任意のスイッチ ポートを利用できるという点において、最大限のパフォーマンスを発揮するためにすべてのポートを使用する分散アーキテクチャ製品よりも効率的です。

ネットワーク設定

Cisco CSM-S は、さまざまなタイプのネットワーク トポロジーをサポートします。Cisco CSM-S は、ブリッジ構成とルータ構成が混在した環境でも動作可能であり、同じあるいは異なる IP サブネット上でも、クライアント側からサーバ側にトラフィックを送信できます。

URL およびクッキー ベースのロードバランシング

Cisco CSM-S では、URL、クッキー、および HTTP ヘッダー フィールドに基づくポリシーに対して、完全な正規表現によるパターン マッチングを使用できます。また、すべての URL 形式またはクッキー形式をサポートしているため、URL またはクッキーの形式を変更しなくても、既存の Web コンテンツのロードバランシングを実行できます。

ヘッダー インサート

Cisco CSM-S では、SSL セッション ID またはクライアントの送信元 IP アドレスのような情報を HTTP ヘッダーに挿入できます。通常、このような情報は、SSL 終端処理、または送信元の Network Address Translation（NAT; ネットワーク アドレス変換）を実行した時点で失われます。HTTP ヘッダーに挿入されたこの情報は、SSL セッション ID を認識する必要のあるバックエンド アプリケーションで活用されたり、または、送信元 IP アドレスを使用して、課金情報を得るために利用されたりします。

バックエンド暗号化

Cisco CSM-S を SSL クライアントとして設定し、バックエンド サーバから SSL セッションを確立することも可能です。このような設定を行うと、Cisco CSM-S はクライアントからの着信トラフィックを復号化し、通常は暗号化されているために利用できない情報を使ってロードバランシングを決定したり、セッション保持を実現することができます。そのあと、要求を再暗号化し、バックエンド サーバに送信します。このプロセスにより、ネットワーク上では暗号化の状態を保ったまま、コンテントスイッチング処理をする際に、暗号化されたトラフィックの上位レイヤの情報にアクセスすることができます。

クライアント認証

Cisco CSM-S が SSL サーバとして動作する場合、クライアント証明書の要求と認証を行うように設定することができます。このような設定で、CSM-S が SSL クライアントとして動作する場合は、サーバ証明書を自動認証することも可能です。この機能では、信頼されている一連の認証局と、各プロキシ サービスに対応する有効範囲を指定します。

クライアント証明書

クライアント タイプのプロキシ サービスに対応する証明書は、Cisco CSM-S 上で設定することができます。CSM-S が SSL クライアントとして動作する場合、SSL サーバから認証を要求されたときに、サーバ リスト上の許可済み認証局の中に証明書の発行者が載っていれば、要求側 SSL サーバに証明書を送信して、認証を受けることができます。

SSL 2.0 の転送

SSLv2 サーバの IP アドレスが設定されている場合、SSLv2 接続を他のサーバにトランスペアレントに転送するように Cisco CSM-S を設定できます。

証明書失効リスト

Certificate Revocation List（CRL; 証明書失効リスト）は、失効した証明書を識別するタイムスタンプ付きのリストを Cisco CSM-S に提供します。通信先のピア デバイスが証明書を使用する際、そのデバイスは証明書のシグニチャと有効性を確認するだけでなく、証明書のシリアル番号が CRL に存在しないこともチェックします。

ハイ アベイラビリティ

Cisco CSM-S は、さまざまなプローブ、インバンド ヘルス モニタリング、カスタム スクリプト、リターン コード チェック、Dynamic Feedback Protocol（DFP）、および Server Application State Protocol（SASP）を使用して、サーバとアプリケーションのアベイラビリティを継続的にモニタします。デバイスに障害が発生すると、Cisco CSM-S はトラフィックを別の場所にリダイレクトします。サーバが追加あるいは削除されたとしても、エンド ユーザに影響することなく、サービスを中断することもありません。

ユーザ セッションの保持

多くの場合、エンド ユーザは、セッション中に常に同じエンド デバイスに接続する必要があります。Cisco CSM-S は次のソリューションを提供することにより、クライアント要求が適切なエンド デバイスに送信されるようにセッションを保持します。

- SSL セッション ID、送信元 IP アドレス、クッキー、または HTTP リダイレクションに基づくスティッキー機能
- バックエンド アプリケーションがクッキーを設定できない場合でも、クッキーをスティッキー機能として使用できるようにするためのクッキー インサート
- セッション保持に使用される動的クッキーの静的な部分を管理者が定義できるようにする、クッキー オフセットおよびクッキー レングス

Cisco CSM-S は、アクティブな Cisco CSM からバックアップ用の Cisco CSM に対して保持情報を同期させることで、ユーザにとってトランスペアレントなフェールオーバーを実現します。

高性能な DDoS 保護機能

Cisco CSM-S は、明らかに SYN 攻撃とわかるトラフィックなど、不正トラフィックを回避する付加機能をバックエンド デバイスに提供します。バックエンド デバイスを不正トラフィックから保護するだけでなく、サービスが中断されないように、有効なクライアント要求の実行と送信を続行します。

ファイアウォール ロードバランシング

Cisco CSM-S では、複数のファイアウォール デバイスにトラフィックを分散することにより、ファイアウォールの保護を拡張できます。また、特定の接続に属するすべてのパケットが、同じファイアウォールを経由するようにします。ステルス型と通常タイプのファイアウォールの両方がサポートされています。

Quality of Service（QoS; サービス品質）

Cisco Catalyst 6500 シリーズの堅牢な QoS 機能を利用することにより、Cisco CSM-S は、適切なレベルのサービスを実現するとともに、次のような機能を提供します。

- レイヤ 7 のルールに基づいてミッションクリティカルなパケットの優先順位を適切に設定
- 優先順位の高いユーザ トラフィックを高速のサーバまたは負荷に余裕のあるサーバに転送

グローバル サーバ ロードバランシング

Cisco CSM-S には、グローバル ロードバランシング環境を構築するための複数のオプションがあります。Cisco CSM-S は、Authoritative Domain Name System（DNS; ドメイン ネーム システム）として機能し、地理的に分散された Cisco CSM-S の間で Global Server Load Balancing（GSLB）を実行します。この方法は、2 ～ 4 のロケーションで構成される小規模な GSLB 環境における障害回復に使用されます。また、Cisco CSM-S の仮想 IP に関する負荷情報を Global Site Selector（GSS）に通知することもできます。GSS は、最大 128 サイトまでサポートできる高度な GSLB サービス用に設計された装置です。さまざまな GSLB オプションを使用することにより、Cisco CSM-S は、要件に合わせて GSLB 機能を―拡張できます。

表 1　Cisco Catalyst 6500 シリーズ CSM-S の機能概要

機能	説明
モジュールごとの接続数	• 最大 100 万の TCP 同時接続 • 1 秒あたり最大 165,000 の接続確立 • 最大 20,000 の SSL 同時接続 • 1 秒あたり最大 1,000 の SSL トランザクション
モジュールごとのスループット	• モジュールあたり最大 4 Gbps の合計スループット（クライアント / サーバ間） • 1 秒あたり最大 125 万パケット • 最大 100 Mbps のバルク暗号化
モジュールごとの設定容量	• 合計 VLAN 数（クライアントおよびサーバ）：512 • 仮想サーバ：4,000 • サーバ ファーム：4,000 • 実サーバ：16,000 • プローブ：4,000 • Access Control List（ACL; アクセス制御リスト）項目数：16,000 • 256 個のキー ペア • 256 の証明書 • 512、768、1,024、1,536、および 2,048 の各ビット長に対応 • 256 台のプロキシ サーバ

機能	説明
ロードバランシング プロトコル	• TCP ロードバランシング • UDP の汎用 IP ロードバランシング • FTP および Real Time Streaming Protocol（RTSP）用の特別なアプリケーション レイヤ サポート
サポート対象のロードバランシング	• SLB（TCP、UDP、または汎用の 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 • ステルス型のファイアウォール ロードバランシング（FWLB） • トランスペアレント キャッシュ リダイレクション • リバース プロキシ キャッシュ • SSL オフロード • VPN IP Security（IPSec）ロードバランシング • 汎用 IP を使用するデバイスおよびプロトコル
ロードバランシング アルゴリズム	• ラウンドロビン • 重み付きラウンドロビン • 最小接続数 • 重み付き最小接続数 • URL ハッシング • 送信元 IP ハッシング（マスク設定可能） • 宛先 IP ハッシング（マスク設定可能） • 送信元と宛先 IP ハッシング（マスク設定可能）
レイヤ 7 の機能	• 完全な正規表現によるマッチング • URL、クッキーに基づくスイッチング、HTTP ヘッダー解析、HTTP メソッド解析
スティッキー機能および保持	• 設定可能なオフセットとレングスによるクッキーのスティッキー機能 • SSL ID • 送信元 IP（設定可能なマスク） • HTTP リダイレクション
冗長性	• スティッキーの状態 • 接続の冗長性
ヘルス チェック	• HTTP • Internet Control Message Protocol（ICMP） • Telnet • TCP • FTP • SMTP • DNS • リターン エラー コードのチェック • インバンド ヘルス チェック • ユーザ定義の Tool Command Language（TCL）スクリプト

機能	説明
その他のロードバランシング機能	• VIP 接続ウォーターマーク • バックアップ（非常用サーバ）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 • GSLB — ライセンスが必要 • 設定可能なアイドル タイムアウトおよび保留接続タイムアウト • 単一方向トラフィックのアイドル タイムアウト • 外部 SSLSM との統合による SSL ロードバランシング • 実サーバの名前 • すべてのタイプのフロー（TCP、UDP、および IP）に適用される TCP 接続の冗長性 • フォールト トレラントな show コマンドの拡張 • Cisco IOS ソフトウェアの SLB FWLB の相互運用（IP のリバース スティッキー） • Cisco CSM-S と Cisco IOS ソフトウェアの SLB が単一のシャーシ内で同時に機能 • 設定可能な HTTP 1.1 の保持（すべての GET を同じサーバで実行するか、複数のサーバに対してロードバランシングするかのいずれかを選択 • 完全に設定可能な NAT • サーバによる接続の確立 • ルート ヘルス インジェクション
SSL の機能	• SSL の確立 • SSL Version 2.0 の転送 • URL のリライト • HTTP ヘッダー インサート • ワイルドカード プロキシ
ハッシュ アルゴリズム	• Message Digest Algorithm 5（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
ハンドシェイク プロトコル	• SSL 3.0 • SSL 3.1 および Transport Layer Security（TLS）1.0 • SSL 2.0（Client Hello） • セッションの再使用 • セッションの再ネゴシエーション • セッション タイムアウト
アルゴリズム	• Alleged RC4（ARC4） • Data Encryption Standard（DES） • Triple DES（3DES） • RSA

機能	説明
Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）	• 最大 2048 ビットの証明書に対応する RSA キーペアの生成 • Cisco CSM-S のフラッシュ メモリ デバイスへの安全なキーの保存 • クライアント タイプおよびサーバタイプのプロキシ サービス用のサーバ証明書の登録 • サーバ キーと証明書のインポートおよびエクスポート（Public-Key Cryptography Standards 12 [PKCS12] および PEM • キーと証明書のインポートおよびエクスポート機能を使用した、スタンバイ Cisco CSM-S でのキーと証明書の複製 • 手動によるキーのアーカイブ、回復、およびバックアップ • CLI を使用したキーと証明書の更新 • 期限切れのキーと証明書に対するグレースフル ロールオーバー • 証明書の自動登録と自動更新 • 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 CA 証明書のインポート • 証明書チェーン内で最大 8 レベルの CA をサポート • 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、証明書の手動登録 • 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 • 証明書のセキュリティ属性に基づく ACL • CRL • 証明書期限切れの警告
NATおよびPort Address Translation（PAT; ポート アドレス変換）	• クライアントの NAT および PAT • サーバの NAT および PAT
その他の機能	• IP リアセンブリ • TCL スクリプティング • Extensible Markup Language（XML）設定インターフェイス • SNMP（簡易ネットワーク管理プロトコル） • リソース使用状況の表示 • バックエンド暗号化
管理	• SNMP トラップ • SNMP および MIB（管理情報ベース）の完全サポート • リモート CSM 設定用の XML インターフェイス
ワークグループ管理のサポート	• SASP
Cisco Catalyst 6500 シリーズ スイッチ プラットフォームの要件	• Cisco IOS ソフトウェアを実行するスイッチ • バス対応のライン カード機能 • Supervisor Engine 720 または Multilayer Switch Feature Card 2（MSFC2; マルチレイヤ スイッチ フィーチャ カード 2）を搭載した Supervisor Engine 2
物理仕様	• Cisco Catalyst 6500 シリーズ シャーシの 1 スロットを占有 • 寸法（高さ×幅×奥行）: 3.0 × 35.6 × 40.6 cm（1.2 × 14.4 × 16 インチ） • 重量：2.27 kg（5 ポンド）

機能	説明
動作環境	• 動作温度：0 ～ 40°C（32 ～ 104.5°F） • 保管温度：–40 ～ 70°C（–40 ～ 158°F） • 相対動作湿度：10 ～ 90%（結露しないこと） • 相対保管湿度：5 ～ 95%（結露しないこと） • 動作高度および保管高度：海面レベルから 3,050 m（10,000 フィート）
適合規格	• 放射：FCC Part 15 (CFR47) クラス A、ICES-003 クラス A、EN55022 クラス A、CISPR22 クラス A、および AS NZS3548 クラス A • 安全基準：UL1950、CSA22.2 No. 950、EN60950、IEC60950、TS001、および AS/NZS3260 に基づく CE マーク

発注情報

表 2 に、Cisco Catalyst 6500 シリーズ CSM-S の発注情報を示します。

表 2　Cisco Catalyst 6500 シリーズ CSM-S の発注情報

製品番号	製品説明
WS-X6066-SLB-S-K9	Cisco Catalyst 6500 シリーズ SSL 対応コンテント スイッチング モジュール
WS-X6066-SLB-S-K9=	Cisco Catalyst 6500 シリーズ SSL 対応コンテント スイッチング モジュール、スペア モジュール

CISCO SYSTEMS

シスコシステムズ株式会社

URL: http://www.cisco.com/jp/

問合せ URL: http://www.cisco.com/jp/go/contactcenter/

〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
TEL: 03-6670-2992

電話でのお問合せは、 以下の時間帯で受付けております。
平日 10:00 ～ 12:00 および 13:00 ～ 17:00

お問合せ先

05.05