Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用 Cisco ACE Application Control Engine ACE30 モジュール

製品の概要

Cisco Catalyst® 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用 Cisco® ACE Application Control Engine ACE30 モジュールは、データセンター アプリケーションのアベイラビリティ、アクセラレーション、およびセキュリティを高めるための次世代アプリケーション スイッチです。

Cisco ACE30 モジュールを使用すると、企業はアプリケーションの配信に関する 4 つの主要な IT 目標を達成できます。

- アプリケーションのアベイラビリティの強化
- アプリケーションのパフォーマンスの向上
- データセンターおよび重要なビジネス アプリケーションの保護
- 少数のサーバ、ロード バランサ、およびファイアウォールによるデータセンター統合の促進

Cisco ACE30 モジュール（図 1）は、最先端のアクセラレーションおよびセキュリティ機能を備えたインテリジェントなレイヤ 4 のロード バランシングとレイヤ 7 のコンテンツ スイッチング テクノロジーによって、これらの目標を達成します。Cisco ACE を市場の他のソリューションと比べた場合の差別化要因となる決定的な設計エレメントは、仮想アーキテクチャとロールベースの管理を利用してアプリケーションの展開、拡張、高速化、および保護に関連する運用コストを合理化し削減できるという点です。

Cisco ACE30 モジュールは、アプリケーション トラフィックを管理するために、1 つのモジュールで最大 16 Gbps という業界最高レベルのスケーラビリティとスループットを提供します。1 台の Cisco Catalyst 6500 シリーズ シャーシで最大 4 つのモジュールが稼動可能であり、ソフトウェア ライセンスまたは新しいモジュールを追加してアップグレードできるため、IT への長期的な投資保護とスケーラビリティを実現できます。

また、Cisco ACE 独自の仮想化機能により、単一の Cisco ACE30 モジュールから幅広い種類のアプリケーションをプロビジョニングおよび配信することが可能なため、データセンターにおけるアプリケーション プロビジョニングのスケーラビリティが向上します。

アプリケーションのアベイラビリティを強化するために、Cisco ACE30 モジュールは、ハイ アベイラビリティを提供するシステム ソフトウェアとハードウェアを備えたクラス最高レベルのアプリケーション スイッチング アルゴリズムを採用しています。

Cisco ACE30 モジュールは、非常に柔軟なアプリケーション トラフィック管理のほか、SSL 暗号化/復号化処理や TCP セッション管理など、CPU を集中的に消費するタスクをオフロードすることで、サーバの効率性を大幅に向上させます。

Cisco ACE は、データセンターのサーバとアプリケーションの直前に置かれるセキュリティ保護装置としても機能するように設計されています。Cisco ACE30 モジュールはディープ パケット インスペクションを実行し、悪意のある攻撃をブロックします。非常にスケーラブルな統合型セキュリティに

より、IT 担当者は、データセンター内の重要アプリケーションを包括的に保護できるので、データセンターの統合が容易になります。

高性能アプリケーションの提供と、最新のアプリケーション配信機能の包括的なセットを組み合わせた Cisco ACE30 モジュールは、IT の効率性を高め、総所有コスト（TCO）を削減します。仮想デバイス、ロールベースの管理、アプリケーションの瞬間的な分離、単一のビューによるプロビジョニングなど、革新的な機能によって IT の効率性が高められます。信頼性の高い 1 台の完全なアプリケーション配信プラットフォームに、レイヤ 4 ～ 7 の大部分の要件を統合することで、TCO が削減されます。

図 1　Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用 Cisco ACE30 モジュール

機能と利点

表 1 Cisco ACE30 モジュールの機能と利点の要約

表 1　機能と利点

特長	利点
アベイラビリティ	
アプリケーション スイッチング	次世代のアプリケーション スイッチである Cisco ACE30 モジュールは、緊密に統合された重要なアプリケーション サービス機能を 1 つの強力なシステムで提供します（図 2）。カスタマイズ可能なレイヤ 4 ～ 7 ルールに基づく詳細なトラフィック制御を備えた、ロード バランシングおよびコンテンツ スイッチング機能を提供します。 • **インテリジェントなデバイス ロード バランシング**：Cisco ACE は、Domain Name System（DNS; ドメイン ネーム システム）、キャッシュ、透過キャッシュ、ファイアウォール、Intrusion Detection System（IDS; 侵入検知システム）、Intrusion Prevention System（IPS; 侵入防御システム）、VPN、および SSL VPN のサポートを提供します。 • **Generic Protocol Parsing（GPP）**：Cisco ACE は、HTTP、FTP、DNS、Internet Control Message Protocol（ICMP）、Session Initiation Protocol（SIP）、Real-Time Streaming Protocol（RTSP）、Extended RTSP、RADIUS、および Microsoft Remote Desktop Protocol（RDP）の各プロトコルをネイティブで認識します。 ◦ Cisco ACE の GPP 機能により、カスタム アプリケーションやパッケージ アプリケーションのトラフィック ペイロード内の任意の情報に基づいてアプリケーション スイッチングおよび持続性ポリシーを設定することができます。プログラミングの必要はありません。 ◦ Cisco ACE は、他のソフトウェアベースのソリューションとは異なり、強力な正規表現エンジンによってハードウェアでペイロード解析を実行し、パフォーマンスを向上させます。 • **HTTP ヘッダーの処理**：Cisco ACE は、HTTP ヘッダーの変更、挿入、または削除をクライアント要求とサーバ応答の両方でサポートします。 • **部分的なサーバ ファーム フェールオーバー**：Cisco ACE は、使用可能な実サーバ（RServer）の数に基づいて、新しいトラフィックを受信するサーバ ファーム（プライマリまたはバックアップ）を決定する機能を提供します。 • **TCP ダンプ**：Cisco ACE は、Cisco ACE モジュールを通過するネットワーク トラフィックに関するパケット情報をリアルタイムでキャプチャし、トラブルシューティングに役立てることができます。 • **仮想 IP 対応の送信元 Network Address Translation**：仮想 IP 対応の送信元 NAT（ネットワーク アドレス変換）により NAT プールに仮想 IP アドレスを含め、ダイナミック NAT および Port Address Translation（PAT; ポート アドレス変換）を実行することで、クライアント側ネットワークで実 IP アドレスを節約できます。 • **サーバ ファーム対応の送信元 NAT**：プライマリ サーバ ファームに障害が発生した場合、数ホップ先にあるバックアップ サーバ ファームに送信元 NAT を切り替えることで、障害時にも途切れのないアプリケーション アベイラビリティを確保します。

特長	利点
	• **柔軟なネットワーク構成**：Cisco ACE モジュールは内部 VLAN インターフェイスを使用します。VLAN はスーパーバイザ エンジンから Cisco ACE に対して割り当て可能です。対応する VLAN インターフェイスを Cisco ACE 上でルーテッド インターフェイスまたはブリッジド インターフェイスとして設定できます。Cisco ACE モジュールは、次のモードで設定できます。 ◦ **ルーテッド モード**：クライアント側 VLAN とサーバ側 VLAN が異なるサブネットに存在する場合、トラフィックをルーティングするように Cisco ACE を設定できます。 ◦ **ブリッジ モード**：クライアント側 VLAN とサーバ側 VLAN が同じサブネットに存在する場合、トラフィックをブリッジするように Cisco ACE を設定できます。 ◦ **Asymmetric Server Normalization（ASN）**：Cisco ACE はクライアントからの初期要求を実サーバにロード バランスできます。ただし、サーバは Cisco ACE をバイパスし、直接クライアントに応答します。
プレディクタ	Cisco ACE は、一連のチェックおよび計算を実行して、ロードバランシング アルゴリズムまたはプレディクタに基づいて、各クライアント要求に最良のサービスを提供できるサーバを判断します。Cisco ACE は、適応応答、最小負荷、最小帯域幅、最小接続、ラウンド ロビン、ハッシュ アドレス、ハッシュ クッキー、ハッシュ ヘッダー、ハッシュ URL、および SSL 暗号の各プレディクタを使用して、クライアント要求を満たすのに最適なサーバを選択します。
サーバのヘルス モニタリング	Cisco ACE でサーバおよびサーバ ファームの状態をチェックするため、ヘルス プローブ（別名キープアライブ）を設定できます。サポートされるプローブは、ICMP、TCP、UDP、ECHO {tcp | udp}、Finger、HTTP、HTTPS、FTP、Telnet、DNS、Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）、Internet Mail Access Protocol（IMAP）、Post Office Protocol（POP）、RADIUS、スクリプト、Keepalive Appliance Protocol（KAL-AP）、RTSP、SIP、HTTP リターンコード解析、および Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）プローブです。また、Cisco ACE はインバンド TCP ヘルス チェックをサポートします。
持続性とスティッキ性	Cisco ACE30 は、クライアントがセッションの持続中に、同じ実サーバとの間で複数の同時または後続 TCP 接続や IP 接続を維持できるスティッキ性を提供します。Cisco ACE は、送信元または宛先 IP アドレス、クッキー、HTTP ヘッダー、および SSL セッション ID の各スティッキ方式をサポートしています。
冗長性	Cisco ACE モジュールは、次の 3 タイプのハイ アベイラビリティを提供します。 • **シャーシ間**：1 台の Cisco Catalyst 6500 または Cisco 7600 シリーズ デバイスに搭載された Cisco ACE モジュールは、ピアの Cisco Catalyst 6500 または Cisco 7600 シリーズ デバイスの Cisco ACE モジュールによって保護されます。 • **シャーシ内**：Cisco Catalyst 6500 または Cisco 7600 シリーズ デバイスに搭載された Cisco ACE モジュールは、同じ Cisco Catalyst 6500 または Cisco 7600 シリーズ デバイスの別の Cisco ACE モジュールによって保護されます。 • **仮想デバイス間**：Cisco ACE モジュールは、2 つのモジュールで構成された仮想デバイス間でのハイ アベイラビリティをサポートします。この機能を使用すると、特定のモジュールの他の仮想デバイスやアプリケーションに影響を与えることなく、特定の仮想デバイスをフェールオーバーすることができます。Cisco ACE を Cisco ACE Global Site Selector（GSS）と統合し、複数のデータセンターのフェールオーバー システムを提供できます。
高速化機能	
圧縮	Cisco ACE30 モジュールは、ハードウェアでアクセラレートされた強力な 6 Gpbs のデータ圧縮を備え、高速なアプリケーション パフォーマンスをアプリケーション ユーザに提供します。GZIP 圧縮と Deflate 圧縮の両方のアルゴリズムがサポートされます。
User Datagram Protocol（UDP）ブースター	Cisco ACE30 モジュールは、DNS ロード バランシングなど、UDP ベース アプリケーションのパフォーマンスを数百万リクエスト/秒までブーストできます。
UDP ファスト エージング	Cisco ACE30 モジュールは、要求ごとに 1 つずつ応答を必要とするアプリケーションのクライアント数に関して、非常に高度なスケーラビリティを提供できます。
SSL アクセラレーション	• Cisco ACE30 モジュールは SSL アクセラレーション テクノロジーを内蔵しています。SSL アクセラレーションは、外部デバイス（サーバやアプライアンスなど）から SSL トラフィックの暗号化/復号化の処理をオフロードします。このため、Cisco ACE30 モジュールで暗号化されたデータを詳細に検査して、セキュリティ ポリシーやアプリケーション スイッチング ポリシーを適用することができます。この機能により、Cisco ACE でインテリジェントなポリシーによる判断が可能になるだけでなく、アプリケーション配信プラットフォームを内外の規定に確実に準拠させることが可能です。 • 再暗号化機能を使用する Cisco ACE の SSL アクセラレーションによって、インテリジェントなポリシーを適用する機能を維持したまま、機密データをエンドツーエンドで確実に暗号化することができます。 ◦ **サポートされる SSL 機能**：SSL 終端および開始、SSL バージョン 3.0、Transport Layer Security（TLS）バージョン 1.0、バックエンド SSL、エクスポート可能な RSA 暗号スイート、セッション ID のスティッキ性、SSL URL の書き換え（HTTP ヘッダーの書き換え）、セッション ID の再利用、クライアント認証、クライアント/サーバ証明書フィールドおよび SSL セッション パラメータの HTTP ヘッダー挿入、クライアント認証失敗時の HTTP リダイレクト、強力な RSA 暗号スイート、および Advanced Encryption Standard（AES; 高度暗号化規格）暗号スイート ◦ **SSL アクセラレーテッド プロトコル**：HTTPS、Secure IMAP（IMAPS）、Secure Lightweight Directory Access Protocol（LDAPS）、Secure Network News Transfer Protocol（NNTPS）、Secure POP バージョン 3（POP3S）、および Secure Telnet（STELNET）

特長	利点
	◦ **SSL アクセラレーテッド サイファ**:rsa-with-rc4-128-md5、rsa-with-rc4-128-sha、rsa-with-des-cbc-sha、rsa-with-3des-ede-cbc-sha、rsa-export-with-rc4-40-md5、rsa-export-with-des40-cbc-sha、rsa-export1024-with-rc4-56-md5、sa-export1024-with-des-cbc-sha、rsa-export1024-with-rc4-56-sha、rsa-with-aes-128-cbc-sha、および rsa-with-aes-256-cbc-sha ◦ **Public Key Exchange アルゴリズム**:RSA 512 ビット、768 ビット、1024 ビット、1536 ビット、および 2048 ビット ◦ **デジタル証明書**:VeriSign、Entrust、Netscape iPlanet、Windows 2000 Certificate Server、Thawte、Equifax、および Genuity など、Certificate Authority（CA; 認証局）による主要なすべてのデジタル証明書 ◦ SSL キー/証明書ペアのサンプル
TCP オフロード	TCP オフロードは、着信トラフィックを要求レベルで分析し方向付けることにより、最も効率的な方法でトラフィックを方向付けます。TCP オフロードは、アプリケーション要求とトランスポート レイヤの依存関係を排除し、アプリケーションレベルの要求を、バックエンド サーバへの持続的な接続に多重化/逆多重化します。クライアントとサーバの TCP 接続をそれぞれ無関係に維持し、それらの TCP 接続を再利用することで、詳細なアプリケーション レイヤ ポリシーおよび Web サーバからの TCP 処理のオフロードを可能にし、CPU サイクルを節約します。

図 2　Cisco ACE によるネットワーク統合

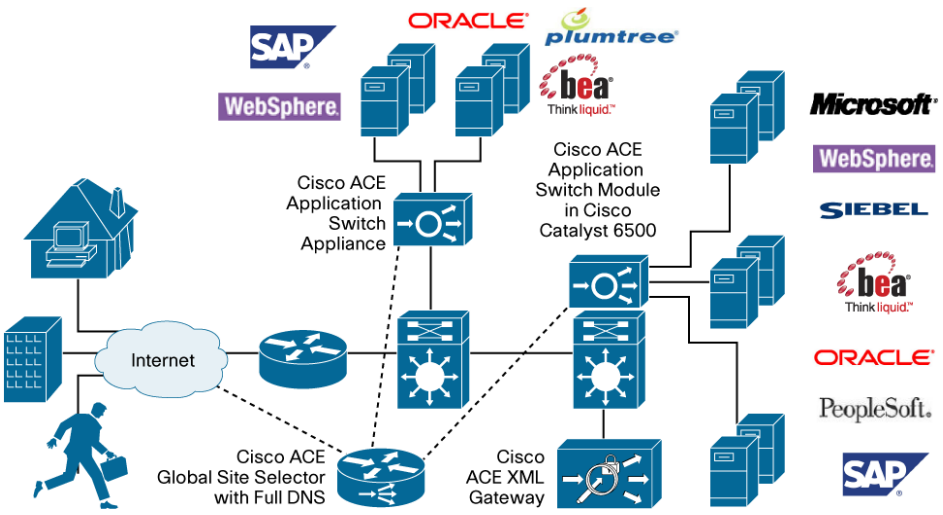

表 2

特長	利点
セキュリティ	
データセンター セキュリティ	Cisco ACE モジュールは、データセンターのサーバとアプリケーションの直前に置かれるセキュリティ保護装置としても機能するように設計されています。データセンター セキュリティは、プロトコル攻撃とサービス拒絶（DoS）攻撃を防ぎ、ミッションクリティカルなコンテンツを暗号化します。Cisco ACE データセンター セキュリティ機能は、以下の機能により、データセンターとクリティカル アプリケーションを悪意のあるトラフィックから保護します。 • **HTTP ディープ パケット インスペクション**:HTTP ヘッダー、URL、およびペイロード • 双方向 NAT および PAT • スタティック、ダイナミック、およびポリシーベースの NAT/PAT のサポート • ポート間のトラフィックを選択的に許可する ACL（アクセス コントロール リスト） • TCP 接続状態トラッキング • UDP の仮想接続状態 • シーケンス番号のランダム化 • TCP ヘッダー検証 • TCP ウィンドウ サイズ チェック • セッション確立時の Unicast Reverse Path Forwarding（URPF）チェック • ACL オブジェクト グループ化 • TCP SYN Cookie による分散型 DoS（DDoS）の防止 • **レート リミット**:Cisco ACE のレート リミット機能は、実サーバ、仮想サーバ、または両方の組み合わせに適用可能です。
アプリケーション セキュリティ	統合型のハードウェア アクセラレーションによるプロトコル制御によって、HTTP、RTSP、DNS、FTP、ICMP、SIP、Skinny Client Control Protocol（SCCP）、LDAP など、一般的なデータセンター プロトコルの効率的なインスペクションとフィルタリングを実行します。

特長	利点
仮想化サービス	
仮想デバイス	仮想デバイスは、リソースを分割および分離する手段を提供し、Cisco ACE モジュールが 1 つの物理モジュール内で複数の仮想モジュールとして動作できるようにします。仮想デバイスを使用すると、1 つの Cisco ACE モジュールから最大 250 の異なるビジネス組織、アプリケーション、または顧客/パートナー向けに指定されたレベルのサービスを提供できます。 • 仮想デバイスを使用する場合、次のものが完全に分離されます。 ◦ コンフィギュレーション ファイル ◦ 管理インターフェイス ◦ アプリケーション ルール セット • 仮想デバイスは、次の点においてアプリケーションごとにカスタマイズされ、特別に割り当てられたリソースを提供します。 ◦ スループット ◦ 1 秒あたりの接続数 Cisco ACE リソースである ACL メモリ、Syslog メッセージおよび TCP Out-Of-Order（OOO）セグメント用のバッファ、同時接続（Cisco ACE 経由のトラフィック）、管理接続（Cisco ACE 向けのトラフィック）、プロキシ接続、リソース制限（秒速で設定）、正規表現メモリ、SSL 接続、Sticky エントリ、およびスタティックまたはダイナミック NAT（Xlate）の割り当てを制限および管理することが可能です。
ロールベース アドミニストレーション（RBA）	RBA 機能を使用すると、企業は管理ロールを指定して、それぞれの管理者の権限をモジュールまたは仮想デバイス内の特定の機能に限定することができます（図 3）。企業内の管理者は Cisco ACE モジュールをさまざまなレベル（アプリケーション管理、サーバ管理、ネットワーク管理、およびセキュリティ管理など）で操作する必要があります。そのため、特定の管理者グループが他の管理者グループに影響を与えることなく自由に作業できるように、管理者ロールを定義できる機能は重要です。この機能により、タスクを各グループに安全に委任することができます。Cisco ACE は次の定義済みロールを提供します。これらのロールは削除または変更できません。 • **Admin**：このロールでは、仮想デバイス内のすべてのオブジェクトに対する完全なアクセスおよび制御が提供されます。コンテキストの管理者は、そのコンテキスト内のすべてのオブジェクト（ポリシー、ロール、ドメイン、サーバ ファーム、および実サーバ）の作成、設定、および変更が可能です。 • **Network Admin**：このロールでは、インターフェイス、ルーティング、接続パラメータ、NAT、仮想 IP コピー設定、および **change to** コマンド の機能に対する完全なアクセスおよび制御が提供されます。 • **Network-Monitor**：このロールでは、すべての **show** コマンドおよび、**change to** コマンドに対するアクセスのみが提供されます。**username** コマンドを使用してユーザにロールを明示的に割り当てない場合は、このロールがデフォルトで使用されます。 • **Security-Admin**：このロールでは、コンテキスト内でセキュリティ関連機能である ACL、アプリケーション インスペクション、接続パラメータ、インターフェイス、authentication, authorization, and accounting（AAA; 認証、認可、アカウンティング）、NAT、コピー設定、および **change to** コマンドに対する完全なアクセスおよび制御が提供されます。 • **Server-AppIn-Maintenance**：このロールでは、実サーバ、サーバ ファーム、ロード バランシング、コピー設定、および **change to** コマンドの機能に対する完全なアクセスおよび制御が提供されます。 • **Server-Maintenance**：このロールでは、実サーバのメンテナンス、モニタリング、およびデバッグに対するアクセスが提供されます。 ◦ **実サーバ**：変更権限 ◦ **サーバ ファーム**：デバッグ権限 ◦ **仮想 IP**：デバッグ権限 ◦ **プローブ**：デバッグ権限 ◦ **ロード バランシング**：デバッグ権限 ◦ **change to コマンド**：作成権限 • **SLB-Admin**：このロールでは、コンテキスト内で Cisco ACE 機能である実サーバ、サーバ ファーム、仮想 IP、プローブ、ロード バランシング（レイヤ 3、4、および 7）、NAT、インターフェイス、コピー設定、および **change to** コマンドに対する完全なアクセスおよび制御が提供されます。 • **SSL-Admin**：このロールは、すべての SSL 機能の管理者です。 ◦ **SSL**：作成権限 ◦ **PKI（Public Key Infrastructure; 公開鍵インフラストラクチャ）**：作成権限 ◦ **インターフェイス**：変更権限 ◦ **コピー設定**：作成権限 ◦ **change to コマンド**：作成権限 ◦ **secure backup** および **restore** コマンド（admin および user の両方のコンテキスト） ◦ SNMP MIB をサポートするサードパーティ製の管理ツール 上記のデフォルト ロールに加えて、さまざまな組織構造に適応するために新しいロールを作成できます。

図 3　Cisco ACE 仮想デバイスとロールベースの管理

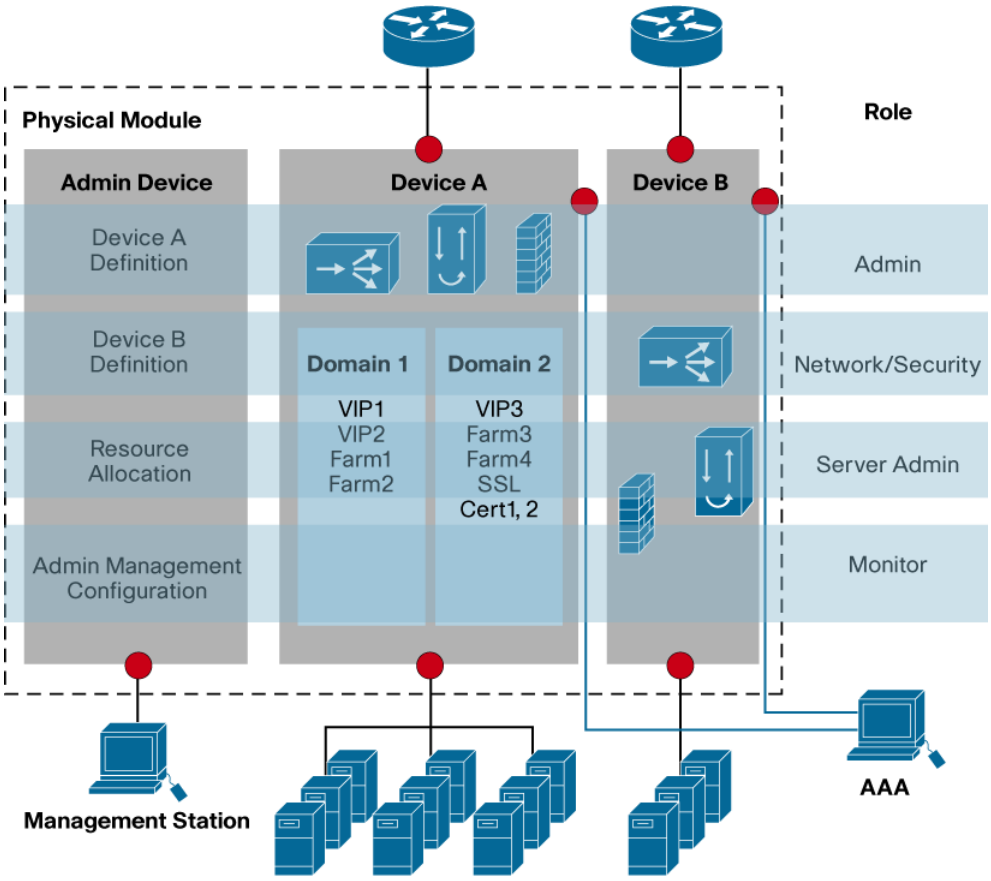

表 3

特長	利点
構成と管理	
レイヤ 2 ～ 7 ネットワークの統合	Cisco Catalyst 6500 シリーズおよび Cisco 7600 シリーズ シャーシのモジュールである Cisco ACE30 は、新規または既存のネットワークに容易に統合することができ、レイヤ 2 ～ 7 のすべてに対応した完全なソリューションを提供します。 • このソリューションは最大 1,152 個のポートと最大 720 Gbps のシャーシ スループットをサポートしているため、大規模なネットワークの要件にも容易に対応できます。また、統合型のソリューションを利用することによって、設置面積を大幅に削減することが可能になります。アプリケーションおよびデータセンターのハイ アベイラビリティは、Route Health Injection（RHI）および自動ステート機能によってサポートされます。これらの機能を使用すると、ネットワーク内でサービスを出入りする物理インターフェイスによって、Cisco ACE 仮想デバイス フェールオーバーを強制的に実行できます。 • ダイナミック レイヤ 3 ルーティングの仮想化は、Cisco Catalyst 6500 シリーズおよび Cisco 7600 シリーズに搭載された Multi-Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）上の Virtual Routing and Forwarding（VRF）インスタンスとの統合によってサポートされます。 • VLAN インターフェイス上では、セカンダリ IP アドレスがサポートされます。
機能の統合	• アプリケーション スイッチング、SSL アクセラレーション、データセンター セキュリティなどの機能を 1 つのデバイスに統合することにより、Cisco ACE はビット/秒（bps）単位からパケット/秒（pps）単位への大幅な処理速度の向上を実現し、アプリケーション遅延を短縮します。機能を統合することによって、ネットワークの 4 箇所以上で終端していた TCP フローは 1 箇所だけで終端するようになります。これは、応答時間の短縮や処理能力とメモリの節約につながります。 • 暗号化/復号化、ロード バランシングの決定、セキュリティ チェック、およびビジネス ポリシーの割り当てと検証をネットワーク内の 1 箇所ですべて実施することによって、デバイス数の削減、ネットワーク構成の簡素化、管理の簡素化、および優れたアプリケーション パフォーマンスを実現します。

特長	利点
投資の保護	• Cisco ACE30 はデフォルトで、1 つの管理デバイスおよび 5 つのユーザ デバイスによる仮想化、4 Gbps のモジュール帯域幅、1000 SSL トランザクション/秒（TPS）、および無料の販促用セキュリティ ライセンスをサポートしています。 • ソフトウェア ライセンスのアップグレードにより、新しい機器への大幅な再投資なしでネットワークを拡張できます。 ◦ **スループット**：デフォルトのモジュール帯域幅 4 Gbps を、同じモジュールで 8 Gbps または 16 Gbps に増加させることができます。1 台の Cisco Catalyst 6500 シリーズまたは Cisco 7600 シリーズ シャーシに 最大 4 つの Cisco ACE モジュールを搭載して、帯域幅を拡張可能です。 ◦ **仮想デバイス**：ソフトウェア ライセンスのアップグレードにより、デフォルトのユーザ デバイス数 5 から 20、50、100、または 250 の仮想デバイスに増やすことができます。 ◦ **SSL TPS**：ソフトウェア ライセンスのアップグレードにより、デフォルトの 1000 SSL TPS から 5000、10,000、または 15,000 TPS に増やすことができます。
Cisco Application Networking Manager（ANM）	Cisco ANM は、複数の Cisco ACE30 モジュールにまたがる仮想デバイスと階層型管理ドメインの管理をサポートします。 • Cisco ANM はサーバベースの管理スイートで、複数の Cisco ACE30 モジュール上ですべての仮想デバイスの検出、プロビジョニング、およびモニタリングを行う機能を備えています。Cisco ANM を使用すると、複数の Cisco ACE モジュールを意識することなく、透過的な管理が可能になります。 • サービスの開始や停止を補完するフォームベースのコンフィギュレーションを備えているため、アプリケーションを迅速に導入できます。 • Role-Based Access Control（RBAC; ロールベース アクセス コントロール）によるタスクの委任設定を行えるため、多数の Cisco ACE30 モジュールおよび仮想デバイスの運用を、複数の管理者グループで並行して実施できます。

IT の効率向上と TCO の削減

Cisco ACE30 は、サーバ ロード バランシング、データセンター セキュリティ、および SSL アクセラレーションなどのアプリケーション サービスを 1 つのデバイスに統合することで、IT の効率を高め、TCO を削減します。重要なアプリケーション サービスを統合することによって、ネットワークの 4 箇所以上で終端していた TCP フローは 1 箇所だけで終端するようになります。これは、応答時間の短縮や処理能力とメモリの節約につながります。

暗号化/復号化、ロード バランシングの決定、データセンター セキュリティ、およびビジネス ポリシーの割り当てと検証をネットワーク内の 1 箇所ですべて実施することによって、デバイス数の削減、少ないエレメントによる強力なセキュリティ、ネットワーク設計の簡素化、管理の簡易化を実現し、優れたアプリケーション パフォーマンスを達成します。Cisco ACE30 モジュールは、従来のデータセンター向け個別ソリューションの後継として理想的です。マルチベンダー製品で必要となる電力、スペース、トレーニング、管理、トラブルシューティング、およびサポート契約をなくすことで、IT の効率向上と TCO の削減に貢献します。

仕様

表 4 に、Cisco ACE30 モジュールのパフォーマンスと構成を要約します。表 5 に、Cisco ACE30 モジュールの仕様を示します。

表 4　Cisco ACE30 モジュールのパフォーマンスと構成

機能	最大パフォーマンスおよび最大構成
スループット	16 Gbps
圧縮スループット	最大 6 Gbps
仮想コンテキスト	最大 250
SSL スループット	6 Gbps
SSL TPS	最大 30,000 TPS
1 秒あたりの L4 最大接続数	500,000 のトランザクション（平均レート）
1 秒あたりの L7 最大接続数	200,000 のトランザクション（平均レート）
同時接続数	400 万接続

表 5　Cisco ACE30 モジュールの仕様

機能	説明
物理的仕様	
必要なシャーシ スロット数	シャーシ内の 1 スロットを使用
寸法（高さ×幅×奥行）	44.45 X 394 X 415 mm（1.75 X 15.51 X 16.34 インチ）
Weight	4.98 kg（11 ポンド）
動作仕様	
動作温度	0 ～ 40 °C（32 ～ 104 °F）
保管温度	-40 ～ 70 °C（-40 ～ 158 °F）
動作相対湿度	10 ～ 85%
相対湿度（非動作時）	5 ～ 95%
動作高度	
動作認定済み	0 ～ 2,000 m（0 ～ 6,500 フィート）
設計および動作試験済み	-60 ～3,000 m（-200 ～ 10,000 フィート）
NEBS	SR-3580-NEBS：基準レベル（Level 3 準拠） GR-63-CORE-NEBS：物理保護 GR-1089-CORE-NEBS：EMC および安全性
エミッション	FCC Part 15（CFR 47）クラス A または B ICES-003 クラス A または B EN55022 クラス A または B CISPR22 クラス A または B AS/NZS CISPR22 クラス A または B VCCI クラス A または B CISPR24 EN55024 EN50082-1 EN61000-3-2 EN61000-3-3 EN61000-6-1
安全性	UL 60950 Can/CSA-C22.2 No. 60950 EN 60950 IEC 60950 AS/NZS 60950 TS001

システム要件

表 6 に、Cisco ACE30 モジュールに関する Cisco Catalyst 6500 シリーズのシステム要件を要約します。また表 7 に、Cisco ACE30 モジュールに関する Cisco 7600 シリーズのシステム要件を要約します。

表 6　Cisco ACE30 モジュールに関する Cisco Catalyst 6500 シリーズのシステム要件

要件	詳細
シャーシ	Cisco Catalyst 6503E、6504E、6506E、6509E、6509-V-E、または 6513 スイッチ
スーパーバイザ エンジン	WS-SUP720-3B、WS-SUP720-3BXL、VS-S720-10G-3C、VS-S720-10G-3CXL
シャーシ OS	Cisco IOS® ソフトウェア リリース 12.2(33)SXI4 以降を実行する Cisco Catalyst 6500 シリーズ
シャーシ接続	ファブリック対応のライン カード機能
必要なシャーシ スロット数	シャーシ内の 1 スロットを使用

表 7　Cisco ACE30 モジュールに関する Cisco 7600 シリーズのシステム要件

要件	詳細
シャーシ	Cisco 7603、7604、7609、7613、7603-S、7604-S、7606-S、または 7609-S ルータ
スーパーバイザ エンジン	WS-SUP720-3B 、 WS-SUP720-3BXL 、 RSP720-3C-GE 、 RSP720-3CXL-GE 、 RSP720-3C-10GE、RSP720-3CXL-10GE
シャーシ OS	Cisco IOS ソフトウェア リリース 15.0(1)S 以降を実行する Cisco 7600 シリーズ
シャーシ接続	ファブリック対応のライン カード機能
必要なシャーシ スロット数	シャーシ内の 1 スロットを使用

関連情報

Cisco ACE の詳細については、http://www.cisco.com/jp/go/ace/ を参照するか、最寄りのシスコ代理店までお問い合わせください。

お問い合わせ先

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間:平日10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/