

Cisco ACE および Cisco AVS によるアプリケーション インフラストラクチャの制御、パフォーマンス、セキュリティ の向上、およびインフラストラクチャの簡素化

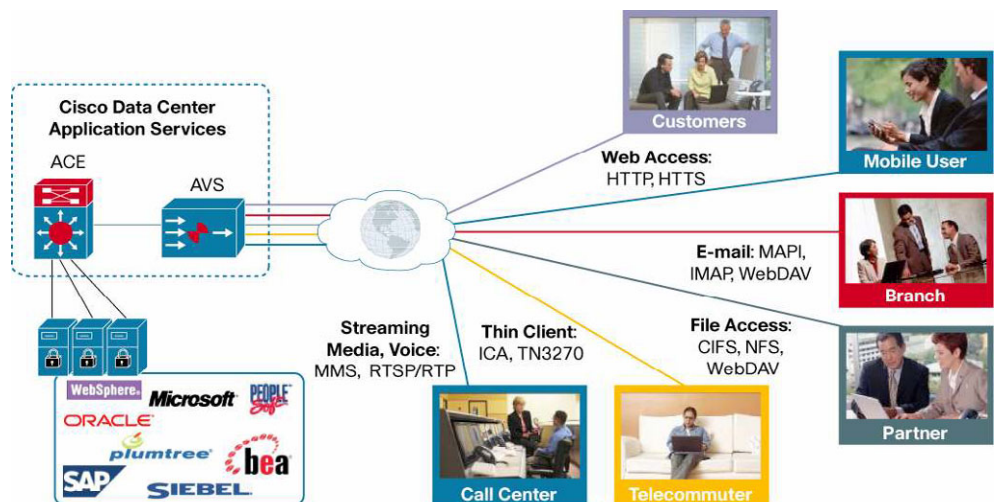
概要

アプリケーション ネットワーキング サービスに対応したシスコのデータセンター ソリューション ポートフォリオに 2 つの重要な機能が追加されました。まず、Cisco Catalyst® 6500 シリーズ スイッチにモジュールとして搭載する Cisco Application Control Engine (ACE) により、これまでにない優れたアプリケーション制御が実現しました。また、Cisco Application Velocity System (AVS) 専用アプライアンスのセキュリティ機能が大幅に強化されました。これらの製品を利用すると、次のような課題を克服するアプリケーション ソリューションを実現できます。

- **アプリケーション制御** — IT 部門によるアプリケーション インフラストラクチャの導入、運用、および管理方法の改善
- **アプリケーション パフォーマンス** — エンド ユーザに対するサービスの向上 (スケーラビリティ、アベイラビリティ、およびフェールオーバー)
- **アプリケーション セキュリティ** — 重要なアプリケーションの保護、インフラストラクチャの保護、およびデータの不正利用の防止
- **インフラストラクチャの簡素化** — インフラストラクチャの複雑さの解消、デバイスおよびベンダー数の削減、ネットワークとアプリケーションの適切な統合、インフラストラクチャ コストの削減

アプリケーション ネットワーキング サービスに対応したシスコのデータセンター ソリューション ポートフォリオを利用すると、アプリケーションのスケーラビリティとアベイラビリティを強化できます (図 1)。これにより、使用するサーバおよびネットワーク リソースの数を削減でき、TCO (総所有コスト) の抑制と IT 業務の柔軟性向上が可能になります。このポートフォリオには、企業の IT チームがアプリケーション制御の最適化、インフラストラクチャの簡素化、およびエンドツーエンドでのビジネス プロセスの提供を実現するのに役立つ各種ソリューションが統合されています。

図 1 データセンターにおける Cisco ACE および Cisco AVS の使用例



課題

企業やサービス プロバイダーのデータセンターは、サービス速度の向上、信頼性と Quality of Service (QoS; サービス品質) の向上、およびコスト削減などを絶えず要求されています。アプリケーションは、ネットワーク内の個別の場所で使用および管理されている場合もあります。このようなネットワークでは、多くの場合、アプリケーション パフォーマンスはさほど重要視されていません。企業では、多種多様な単独の製品を使用して、場所ごとの困難な課題に対処しています。また、セキュリティや法令遵守などによって、IT 部門では対応にさらに制約を受けています。

IT 部門が必要としているのは、アプリケーション インフラストラクチャの詳細な制御を可能にし、各種機能を集約して管理を簡素化し、さらに企業全体でのアプリケーション サービスのセキュリティ保護と高速化を可能にするソリューションです。このような課題に対応するために、企業やサービス プロバイダーは次のようなデータセンター ソリューションを必要としています。

- アプリケーションの導入や移行を行う際に、アプリケーション インフラストラクチャを追加する必要がない
- アプリケーション インフラストラクチャを拡張できる
- 多層的なデータセンターおよびアプリケーション セキュリティを備えている
- 分散型のワークフローが利用できる
- 機能、装置、および管理を統合できる
- アプリケーション スループットを向上させることができる

ソリューション

アプリケーション フロントエンドのアプライアンスとは異なり、Cisco ACE はシスコ ネットワークに完全に統合できるため、IT チームは、データセンターのリソース、スタッフ、およびインフラストラクチャのシステム全体を効率的に利用できます。シスコのプラットフォームは、必要な場合に必要な場所でアプリケーションの最適化、拡張、保護、および提供を行うという課題に対処しており、これまでにない優れた制御を実現しています。また、このソリューションを使用すると、仮想化されたアプリケーションのハイ アベイラビリティの確保、アプリケーションの最適化、データセンターおよびアプリケーションのセキュリティ要件への対応、およびデータセンターのパフォーマンスとリソース利用の最大化を実現できます。これにより、運用上のオーバーヘッドおよびコストを最小限に抑えるアプリケーションの提供が可能になります。

Cisco ACE および Cisco AVS 製品には、要求の厳しい企業環境でのアプリケーションの提供に必要な、仮想化および Role-Based Access Control (RBAC; ロールベース アクセス コントロール) による高度なアプリケーション制御、優れたパフォーマンス、高度なセキュリティ、およびインフラストラクチャの簡素化などを実現する複数のテクノロジーが搭載されています。Cisco ACE および Cisco AVS ソリューションのその他の主要な機能も合わせて利用すると、卓越したパフォーマンス、運用上の柔軟性、セキュリティ、およびアプリケーションの最適化を総合的に実現できます。

パフォーマンス — 遅延の軽減と帯域幅利用の削減

Cisco ACE および Cisco AVS は、レイヤ 2 ~ 7 のネットワークおよびアプリケーションのパフォーマンスを向上させる機能を搭載しており、アプリケーションの応答時間短縮を実現しています。

データセンターに追加されるアプリケーション数が増加すると、各アプリケーションに割り当てられるサポート コストは減少します。Cisco ACE および Cisco AVS を Cisco Catalyst 6500 シリーズ スイッチに搭載した場合、Cisco ACE モジュールは、スイッチの電源、スペース、冷却装置、および管理インターフェイスを使用するため、IT 予算の半分以上を占める運用コストの削減も可能です。

Cisco AVS アプライアンスは、応答時間を短縮させることにより、WAN 上でのアプリケーションのパフォーマンスを強化します。Cisco AVS ソリューションを使用すると、アプリケーションやクライアント操作に変更を加えることなく、エンドユーザの応答時間を定期的に 50 ~ 80% 短縮できます。シスコのデータセンター ソリューションは、アプリケーションのクライアントおよびサーバ環境に一切変更を加えません。また、要求のコンテキスト認識により、これまでキャッシュできないと考えられてきたデータの変換が可能のため、Web サーバまたはアプリケーション サーバでの確認の必要性が無くなります。さらに、Web 要求を集約し、必要のないネットワーク コールを最小限に抑えることにより、ユーザの場所、接続方法、またはクライアント システムに関係なく、応答時間を短縮します。これらは、Cisco AVS 製品の主要な 4 つの機能によって実現されます。

- **FlashForward オブジェクト アクセラレーション** — Cisco AVS 3120 Application Velocity System は、必要のないブラウザ キャッシュの確認要求を省略します。この新しいテクノロジーを使用すると、イメージ、スタイルシート、および JavaScript ファイルなどのキャッシュ可能な組み込み Web オブジェクトに伴って発生するネットワーク遅延を解消できます。Web 環境で組み込みオブジェクトを使用する場合、組み込みオブジェクトごとにユーザが適切なブラウザ バージョンを使用していることを確認する必要があります。そのため、確認を行うたびにクライアントからオリジン サーバに個別の HTTP 要求が発生します。多くのオブジェクトが組み込まれたページは、クライアントとサーバ間のラウンドトリップが完了するまで表示されません。シスコの FlashForward テクノロジーは、サーバ側でこのプロセスを自動的に処理します。オブジェクトの有効性を示す情報は、親 HTML ドキュメントをダウンロードする際にすべて一緒にダウンロードされます。この際、Cisco AVS 3120 は、有効性および有効期限の管理を透過的に行います。オブジェクトの有効性をクライアント側ではなくサーバ側で検証するこの自動集約により、トラフィックの量を削減できます。この機能は、すべてのアプリケーションで使用可能です。
- **Smart Redirect** — この機能を使用すると、Cisco AVS 3120 がリダイレクト方式を HTML のメタタグベースから効率の高い HTTP ヘッダーベースに変換できるようになり、Web ページのリダイレクトを高速化できます。これにより、メタタグベースのリダイレクトの柔軟性や生産性を犠牲にすることなく、ページの応答時間を大幅に短縮できます。
- **Fast Redirect** — HTTP ヘッダーベースの 301/302 リダイレクトを高速化し、ラウンドトリップの回数を 2 回から 1 回に削減します。Cisco AVS 3120 は 301/302 HTTP ステータス コード応答を処理して、データセンターの LAN 上にあるリダイレクト先のリソースを取得します。
- **FlashConnect** — 応答を、順次処理ではなく並列処理することにより、ブラウザのパフォーマンスを向上させます。Microsoft Internet Explorer は、デフォルトでは、HTML コンテナ ページに記載されたドメイン名ごとに確立される TCP 接続を 2 つだけ使用してオブジェクトを取得します。このような制約があると、要求の待ち行列が不必要に発生し、初めてアクセスする際のパフォーマンスが悪化する原因になります。Cisco AVS 3120 は、これらの接続を多重化することでパフォーマンスを改善します。

アプリケーション展開時の時間、コスト、および複雑性の削減

企業およびサービス プロバイダーは、柔軟性、スケーラビリティ、および信頼性の高いアプリケーションを配信できるプラットフォームを必要としています。仮想パーティショニング、RBAC、および階層型管理ドメインによる非集中型管理および集中制御機能を使用すれば、アプリケーションの展開に必要な時間を大幅に短縮できます。仮想パーティショニングを使用すると、最大 250 の論理グループに同レベルのサービスを提供できます。また、RBAC を活用することで、集中制御と非集中型管理が可能になります。これらの機能に加えて階層型管理ドメインを使用すると、特定の物理プラットフォーム上で複数の論理グループ(ビジネス、アプリケーション、またはカスタマーなど)にリソースを分散して、論理グループごとに管理を行うことが可能になります。また、構成の柔軟性が最大限に高まるため、ACE の最もスケーラブルで効率的な利用も実現できます。

セキュリティ

自己防衛型ネットワークは、データセンターのさまざまなレベルに防御機能を組み込むことにより、確実なセキュリティ保護を実現します。アプリケーション ネットワーキング サービスに対応したシスコのデータセンター ソリューションとシスコの自己防衛型ネットワークを組み合わせると、多層的なセキュリティの構築とアプリケーション トラフィックの効率的な処理を同時に実現できます。このようなソリューションを利用すると、すべてのビジネス ポリシーやセキュリティ ポリシーを集中的に制御し、次のような機能を備えた強力なアプリケーション セキュリティを実現できるようになります。

- SSL の暗号化および復号化
- 双方向のディープ インスペクション
- ハードウェア アクセラレートされた統合型のプロトコル制御
- ポジティブおよびネガティブ(ホワイトリストおよびブラックリスト)セキュリティ
- プロトコル適合
- 異常検出
- アプリケーション セキュリティ フォレンジクスに対応したトランザクション ロギングおよびレポート

Intrusion Prevention System (IPS; 侵入防御システム) や Intrusion Detection System (IDS; 侵入検知システム) が Web サーバを保護するのに対し、Cisco ACE および Cisco AVS ソリューションは Web ベース アプリケーションの脆弱性に対する保護を提供します。ファイアウォールはネットワーク レベルの保護(明示的に許可されたものを除くすべてのアクティビティの拒否)を提供しますが、Cisco ACE および AVS ソリューションはアプリケーション レベルでの保護を提供します。ルールベースのポリシーに基づいた方式を使用することによって、アプリケーションに対する要求やアプリケーションからの要求をポリシーに適合させ、アプリケーションを停止させる要求などが含まれないようにします。

一般的な攻撃では、攻撃者は正規のユーザのデスクトップ上にある Web プロキシを使用します。攻撃者は、アプリケーションのさまざまな部分に悪意のあるコードを書き込んで、メッセージ ヘッダー、プロトコル、またはペイロードを改ざんする場合があります。多くの場合、開発者はこのような攻撃からコードを保護する対策を取っていません。

Cisco AVS ソリューションは、次の手法を使って悪意のあるコードを排除します。

- **正規化** — Cisco AVS 3120 は、TCP ヘッダーだけでなくペイロードも検査できるように暗号化されたトラフィックを復号化し、HTTP および HTTPS トラフィックを正規化します。

- **双方向のディープパケット インスペクション** — Cisco AVS 3120 は、プロトコルおよびメッセージのペイロード レベルで、双方向のメッセージを検査します。また、ホワイトリストやブラックリストなどのポリシーを適用して、悪意のあるトラフィックを識別します。
- **ブロッキング** — Cisco AVS 3120 は、ホワイトリスト（許可）とブラックリスト（禁止）を組み合わせて使用し、ポリシーに適合しないプロトコルやメッセージ ペイロードをブロックします。また、アプリケーションの動作分析により、主要なアプリケーション プロトコルの動作やペイロードの特性がポリシーに適合していることを確認します。

Cisco AVS ソリューションは、このような機能を組み合わせることによって、あらゆる種類の攻撃を防御します。既知の脅威のみに対処するシグニチャベースの保護や、膨大なトレーニングを要する学習ルールベースの保護とは異なり、Cisco AVS セキュリティ ソリューションは、既知および未知の脅威からアプリケーションを保護します。Cisco AVS 3180 でグラフィカルな AppScope ツールを使用すると、データセンターと任意のリモート拠点間のアクティビティを表示できるため、問題の特定と解決が容易になります。

最適化

Cisco ACE および Cisco AVS は、次の機能を組み合わせることにより、アプリケーションの応答時間の短縮やビジネス トランザクションのスループット向上を実現します。

- 帯域幅の削減およびアプリケーション遅延の最小化
- サーバ処理サイクルの軽減によるアプリケーションの最適化
- コンテント スwitチング機能によるリソース利用の最適化とアプリケーションの可用性の保証

このような包括的なソリューションを利用すると、これまで LAN 環境でしか実現できなかった応答時間を、WAN 経由のアプリケーションでも実現できるようになります。また、Cisco AVS を利用すると、エンド ユーザの応答時間などのアプリケーション パフォーマンス メトリックをグラフィカルに表示できるため、アプリケーションのボトルネックを迅速に発見して修復できます。

多くの場合、アプリケーション配信における課題はネットワーク遅延の克服だけではありません。企業は、コスト、可用性、またはパフォーマンスなどの理由で、帯域幅の利用を最小限に抑えたいと考えています。Cisco AVS ソリューションでは、次の技術を利用することによって、高いパフォーマンスを維持したまま、帯域幅の利用を 70 ~ 90% 削減します。

- **差分エンコーディング** — Web ページのキャッシングが有効なのは、多くのページが静的であり、後続の要求をサーバではなくキャッシュから取得できる場合です。動的なリソースやコンテンツの場合は、元のページがキャッシュされた後もサーバへの要求が必要になります。しかし、キャッシュされている元のページと更新後のページの差分だけをエンコードしてクライアントに配信できれば、多くの場合、数バイトを送信するだけで済みます。これは差分エンコーディングという手法で、Cisco AVS 3120 のコア テクノロジーです。この手法を使用すると、クライアント システムは小さな差分を追加するだけで、キャッシュされたページから最新のページを動的に作成できます。このプロセスは自動的かつ透過的に実行され、ブラウザ クライアント、アプリケーション サーバ、またはコンテンツに変更を加える必要はありません。
- **ダイナミック ブラウザ キャッシング** — 通常、Customer Relationship Management (CRM) やポータルで使用される多くの企業アプリケーションでは、画像、JavaScript ファイル、ActiveX コントロール ファイル、またはバイナリ ファイルなどのオブジェクトがキャッシュ不可に設定されています。このような設定では、特に、帯域幅に制約のあるリモート ユーザの場合、ダウンロードのパフォーマンスが低下する場合があります。Cisco AVS 3120 に搭載されている Cisco Just-

in-Time Object Evaluation テクノロジーを使用すると、個々のオブジェクトの有効性をリアルタイムで自動的にトラッキングできます。要求されたオブジェクトが変更されていない場合、クライアントはキャッシュされているオブジェクトを使用します。特定のコンテキストでのみオブジェクトが変更されている場合には、Cisco AVS 3120 からオブジェクトが配信されます。

- **インテリジェントな画像の最適化** — Cisco AVS 3120 デバイスは画像ファイルをインテリジェントに圧縮して画質を最適化します。これにより、画像のダウンロード時間の短縮、ページ表示の迅速化、および帯域幅利用の効率化が可能になります。他の方式では画像が均一に圧縮されるため、一部の画像の品質が極端に悪化したり、さらに圧縮可能な画像を十分に圧縮できないというが発生します。画像には、大幅に圧縮できる画像と、細部をそのまま維持しなければならない画像があります。Cisco AVS 3120 を使用すれば、たとえば、事故の請求に使用される JPG 形式の写真は高い解像度のまま維持し、保険証券のコピーの場合は高い圧縮率を使用しながら判読性を犠牲にしないようにといった制御ができます。
- **圧縮** — シスコは標準的な圧縮にとどまらず、適応型ダイナミック キャッシュ(この資料の後半で説明)、差分エンコーディング、および FlashForward テクノロジーなどの高度な最適化技法を提供しています。シンプルなバイト圧縮を組み込むデバイスや手法では、ページに反復コンテンツがどの程度含まれるかによって圧縮率が変わります。この場合、一般的な HTML ページではページ サイズを 1/2 ~ 1/5 に圧縮できます。一方、差分エンコーディングを使用すると、多くの場合、ページ サイズを 1/10 ~ 1/50 に圧縮できます。これは、ページが実際にどの程度変更されるかによって異なります。Cisco AVS 3120 はバイト圧縮を使用して、差分エンコーディングにより最適化されたページのサイズをさらに圧縮します。既存の GZIP や DEFLATE 実装とは異なり、最適化されたシスコの GZIP 圧縮技法は Mozilla Firefox などのすべてのブラウザ タイプと完全な互換性を持っています。この圧縮は Cisco Content Services Switch(CSS)バージョン 8.10 でも利用できます。

多くの企業は、Web 機能や Web アプリケーションをサポートするのに必要なサーバ処理能力の膨大さに困惑しています。シスコは各企業の IT 展開に適したさまざまなサーバ オフロード機能を提供しています。次の機能を組み合わせると、サーバ サイクルを最大 80% 削減できます。

- **TCP 接続の多重化による接続管理のオフロード** — Cisco ACE および Cisco AVS 3120 は、TCP 接続機能を使用して Web サーバやアプリケーション サーバとの持続的な TCP 接続を維持することにより、ネットワーク接続の管理に伴うオーバーヘッドに対処します。また、バックエンドサーバに対する持続的な TCP 接続の数を負荷状態に合わせて調整することにより、トラフィックレベル変動時のパフォーマンスを全体的に最適化します。これにより、Web サーバやアプリケーション サーバをコンテンツ生成に特化させることができ、Web サーバの容量を倍増させることができます。
- **キャッシング** — 差分エンコーディングや FlashForward オブジェクト アクセラレーションといった Cisco AVS 3120 の複数の先進的な最適化技法は、高性能なキャッシング アーキテクチャによって実現されています。スタティック キャッシングを使用すると、画像やアプレットなどの要求頻度の高いスタティック オブジェクトに対する要求をサーバから直接オフロードできます。この柔軟な設定が可能な機能を使用すると、全体的なアプリケーション パフォーマンスやトランザクションスループットを強化できます。
- **適応型かつ設定可能なダイナミック キャッシング** — これは、Cisco AVS 3120 でダイナミック コンテンツに対する要求を実行するための機能です。この機能を使用すると、アプリケーション サーバやコア データベースのオフロードが可能になります。設定可能なダイナミック キャッシングを使用すると、Cisco AVS 3120 は指定されたキャッシュ パラメータ(URL クエリー スtring、HTTP ヘッダー、およびクッキーの値など)に基づいて、特定の URL に対する複数の応答をキャッシュし

ます。つまり、ダイナミック コンテンツをスタティック コンテンツとして処理することでパフォーマンスを向上させることができます。また、シンプルなスクリプトの利用により、個別化されたデータでもダイナミックにキャッシュできるようになるため、より多くのリソースをコア トランザクション用に確保できます。

- **負荷ベースのダイナミック キャッシング** — 洗練されたコンテンツ有効期限ポリシーを使用することにより、ダイナミック コンテンツの有効性を保証します。これにより、Cisco AVS 3120 はサーバの負荷をリアルタイムで監視し、コンテンツの有効期限をインテリジェントなクローズド ループで判断できるため、ピーク トラフィック時のサイト パフォーマンスの最適化とハードウェア リソースの効率的な利用が実現されます。この機能は、負荷、タイミング、および URL ごとに設定できます。
- **遅延した要求の評価** — 多くのシステムはグローバルにアップデートを行うため、一定期間アクセスがブロックされてしまいます。たとえば、ユーザ要求によって再コンパイルが開始されると、その間に受け取る他の要求はすべてキューに入れられます。これは、すべてのユーザを待機させる原因になります。遅延した要求を評価する機能を使用すると、要求を受けた際に常にキャッシュされたコピーを提供するようにデバイスを設定できます。バックエンドの処理が完了すると、キャッシュがオリジン サーバのコピーによって自動的にリフレッシュされます。この機能を使用した場合、デバイスは常にダイナミック キャッシュからコンテンツを提供することになります。つまり、クライアントの要求とオリジン サーバの応答を分離できます。
- **SSL アクセラレーション** — SSL は、企業のビジネス トランザクションに必要なセキュリティ、プライバシー、および機密性を実現する業界標準のプロトコルとなっています。シスコ デバイスは、クライアントとの SSL ハンドシェイクの処理、クライアントからの Web 要求の復号化、バックエンドの Web サーバまたはアプリケーション サーバへの Web 要求のプロキシ化、サーバ応答の圧縮（差分エンコーディングや FlashForward 機能を使用）、サーバ応答の暗号化、およびセキュア SSL 接続経由でのクライアントへのサーバ応答の送付を行うことにより、SSL トランザクションを高速化します。これにより、SSL ベースの トランザクション数を大幅に削減し、SSL のスケーラビリティを 4 倍に増やすことができます。SSL の処理は、Cisco ACE、Cisco Content Switching Module (CSM)、Cisco CSS、および Cisco AVS で利用できます。
- **URL マッピング** — シスコの URL マッピング機能を使用すると、HTML ソース内の URL を任意の URL 文字列に置き換えて表示しないようにできます。この機能により、エンド ユーザは、オリジン サーバが使用する実際の URL 構造を表示できなくなるため、バックエンドのインフラストラクチャの隔離が可能になります。
- **Single Sign-On (SSO; シングル サインオン) の最適化** — 多くの企業は、Microsoft NT LAN Manager などの SSO メカニズムを使用して、ユーザが企業のアプリケーションにログインする際の認証を行っています。認証は、ユーザのスプーフィングを防止する手段の 1 つです。シスコは、オブジェクトの検証要求に伴う冗長な認証トラフィックを排除することにより、SSO 対応環境でのアプリケーション パフォーマンス全体を向上させます。
- **XML 変換** — XML を出力するアプリケーションは、柔軟性に優れた接続性と再利用性を備えています。ただし、アプリケーション サーバ上での XML 変換は効率的ではなく、バックエンドのパフォーマンスに大きな問題が生じる可能性があります。シスコでは、通常のスタンドアロンの XML 変換アプライアンスではなく、Cisco AVS 3120 に搭載された XML モジュールを使用した統合型の XML 変換機能を提供します。このソリューションを使用すると、XML オブジェクトのキャッシュによりパフォーマンスとスループットが向上するとともに、バックエンドおよびクライアントからの XML 変換をオフロードすることで、クライアントに完全に最適化された XML 変換を提供できるようになります。

Cisco ACE サービス モジュールでは、次のようなポリシー ベースのアプローチを使用して、企業ネットワークの内外で使用されるアプリケーション サービスの可用性と信頼性を保証します。

- **ロード バランシング ポリシー** — 分散すべき要求を識別する基準、要求を処理する機能を持った適格なデバイスを識別する基準、および要求を分散するアルゴリズムを識別する基準に基づいたポリシーを使用して、サーバの過負荷を分散します。負荷分散アルゴリズムには、ラウンドロビン、重み付きラウンド ロビン、最小接続、重み付き最小接続、最小負荷、および予測ハッシュなどがあります。
- **サーバ障害ポリシー** — サーバに障害が発生した場合の対処方法をオペレータ指定のポリシーによって制御します。たとえば、クライアントが持続的な接続をマッピングしているサーバがトランザクション中にダウンした場合の対処方法などです。こういった場合には、接続のリセット、(エラー メッセージを表示するサーバなどへの)HTTP リダイレクトの発行、ロード バランシング ポリシーによる別サーバへの接続の再構成、(このポリシーに該当する他のサーバが存在しない場合にアクティブになる)特殊な「Sorry サーバ」へのリダイレクトなどが対処として考えられます。
- **コンテンツ固有のポリシー** — コンテンツのタイプごとに、異なる種類の処理を指定できます。これには、キャッシュ可能なコンテンツに対するすべての要求をリバース プロキシのキャッシュにリダイレクトして、アプリケーション サーバからのスタティックな画像の処理をオフロードするポリシーなどがあります。また、Web サーバ ファームをスタティック セクションとダイナミック セクションに分割することもできます。
- **デバイス固有のポリシー** — デバイスのタイプごとに、異なる種類の処理を指定できます。たとえば、ワイヤレス デバイスを使用するクライアントを、デバイスの形式に合わせて、コンテンツをカスタマイズするサーバにリダイレクトすることができます。

まとめ

シスコシステムズは、アプリケーション ネットワーキング サービスに対応したデータセンター ソリューションに最新の機能を追加しました。これらのソリューションを利用すると、企業はアプリケーション展開に最適なネットワークを構築して、広範囲に分散した組織のビジネス上の価値を向上させることができます。また、次のような利点を得ることができます。

- **アプリケーション サービスの導入と管理における優れた IT 制御** — 仮想パーティションの作成や RBAC の使用により、サービスの大幅な向上と管理上のオーバーヘッドの削減を実現できます。
- **アプリケーションおよびデバイスのパフォーマンス向上** — 大規模な運用を可能にする 16 GB のスループットと 4 M の双方向接続、および WAN 遅延の短縮と帯域幅の削減を実現する独自の機能により、ネットワークを介したエンド ユーザの応答時間を短縮します。
- **多様なアプリケーションおよびネットワーク セキュリティ** — 双方向のコンテンツ検査、SSL 暗号化/復号化、およびアプリケーション セキュリティ フォレンジクスに対応したトランザクション ロギングなどの機能が利用できます。
- **単一のデータ処理パスにおける複数のフロントエンド サービスの統合**

アプリケーション ネットワーキング サービスに対応したシスコのデータセンター ソリューションを利用すると、企業は、変化を続ける困難なビジネス環境に迅速かつ予算内で対応することが可能な強固な IT 基盤を新たに構築できます。これには、次のようなソリューションが含まれます。

- [Cisco ACE モジュール](#)
- アプリケーション ロード バランシングおよびアクセラレーション — [Cisco CSS 11500 コンテント サービス スイッチ](#)

- アプリケーション ロード バランシング — [Cisco Catalyst 6500 シリーズ スイッチ向けコンテンツ スイッチング モジュール](#)
- アプリケーション ロード バランシングおよび SSL オフロード — [Cisco Catalyst 6500 シリーズ 向けの SSL に対応したコンテンツ スイッチング モジュール](#)
- [Cisco GSS 4400 Global Site Selector プラットフォーム](#)
- HTTP および HTTPS の最適化 — [Cisco AVS 3120 Application Velocity System](#)
- HTTP および HTTPS の最適化管理デバイス — [Cisco AVS 3180 Application Velocity System](#)

また、シスコのアプリケーション ネットワーキング サービス製品には、Wide Area Application Services (WAAS) も用意されています。WAAS を使用すると、中央でホスティングおよび管理されているアプリケーションに対し、リモート オフィスから LAN と同様にアクセスできます。

- Web およびビデオ サービス — [Cisco Application Content Networking System \(ACNS\) ソフトウェア](#)
- WAN 最適化、アプリケーション高速化 — [Cisco Wide Area Application Services \(WAAS\) ソフトウェア](#)

Cisco Application-Oriented Networking (AON; アプリケーション指向ネットワーク) を活用すれば、シスコのアプリケーション ネットワーキング サービス製品を使用して、アプリケーション インフラストラクチャ機能をネットワークベース サービスとして提供することが可能になります。

©2007 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)

この資料に記載された仕様は予告なく変更する場合があります。



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)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日10:00～12:00、13:00～17:00

お問い合わせ先