

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

Q. 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 ソリューションとは何ですか。

A. 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 ソリューションとは、企業によるビジネス アプリケーションおよびインフラストラクチャの拡張、展開、および最適化を容易にする集中管理型のソリューション セットです。このソリューションを利用すれば、お客様はアプリケーション パフォーマンスの大幅な向上、展開や運用に必要な時間の短縮、ビジネス上の要求を満たすのに必要なリソース数の削減を実現できます。また、これらの利点を実現するために、開発、サーバ リソース、または帯域幅への追加費用を負担する必要はありません。主な製品は次のとおりです。

- Cisco Catalyst® 6500 向けアプリケーション インフラストラクチャ制御モジュール: Cisco Application Control Engine (ACE)
- Cisco AVS 3120 Application Velocity System 向けアプリケーション セキュリティ ソフトウェア モジュール
- アプリケーション ロード バランシング アプライアンス: Cisco CSS 11500 シリーズ コンテント サービス スイッチ (CSS)
- Cisco Catalyst 6500 向けアプリケーション ロード バランシング: [Cisco Catalyst 6500 シリーズ コンテント スイッチング モジュール \(CSM\)](#)
- アプリケーション ロード バランシングおよび SSL アクセラレーション: [Cisco Catalyst 6500 シリーズ向け CSM-S モジュール](#)
- グローバル ロード バランシング: [Cisco GSS 4400 Global Site Selector スイッチ](#)
- アプリケーション アクセラレーションおよびアプリケーション セキュリティ: [Cisco AVS 3120 Application Velocity System](#)
- アプリケーション アクセラレーションおよびアプリケーション セキュリティ管理: [Cisco AVS 3180 Application Velocity System](#)

Q. これらのソリューションは、シスコのアドバンスト テクノロジーであるシスコのアプリケーション ネットワーキング サービスとどのような関係があるのですか。

A. シスコは、アプリケーション ネットワーキング サービスの分野で初の製品および機能拡張として、これらのソリューションを発表しました。シスコが提供する WAN およびブランチ向けソリューションと Application-Oriented Networking (AON; アプリケーション指向ネットワーク) ソリューションを組み合わせると、お客様はネットワークを通じた包括的なビジネス機能の提供を行えるようになります。アプリケーション配信ソリューションを利用すると、任意のクライアントとアプリケーションまたはビジネス機能間でのスケーラビリティの確保、高速化、および最適化が可能になります。






Q. 今回の発表の新しい内容について教えてください。

A. 今回の発表では、Cisco Catalyst 6500 向けの高性能アプリケーション サービス モジュールである Cisco ACE とアプリケーション セキュリティの機能を大幅に強化した Cisco AVS 3100 Application Velocity System 向けのソフトウェア モジュールが新しく追加されます。

Cisco Catalyst 6500 の新しいサービス モジュールである Cisco ACE を利用すると、アプリケーションやビジネス サービスの導入、運用、配信、保護、および管理を企業全体で詳細かつ容易に制御することができます。また、アプリケーション インフラストラクチャのより詳細な制御が可能になり、企業はアプリケーションの迅速な展開と移行、エンド ユーザへのハイレベルなサービスの提供、およびデータセンターの全体的な管理と運用の簡素化を実現できます。このデバイスには、ロールベースのアクセス コントロール、強力なワークフロー エンジン、および各種管理ツールと API が搭載されています。最大 16 Gbps のスループットと将来の機能拡張に対応できる柔軟なアーキテクチャを備えた Cisco ACE は、データセンターでアプリケーション支援サービスを提供する際の新たなパフォーマンス標準になります。Cisco AVS ソフトウェア モジュールは、Cisco AVS 3100 ファミリーに高度かつ双方向のアプリケーション セキュリティ機能を新たに提供しています。Cisco ACE を Cisco AVS の新しいアプリケーション セキュリティ モジュールと組み合わせて使用すると、アプリケーション インフラストラクチャの制御、パフォーマンスの向上、セキュリティの確保、およびインフラストラクチャの簡素化が可能になります。これにより、ますます高度化するビジネス上の課題への柔軟な IT 対応を実現できます。

- Q. Cisco ACE は、アプリケーション ネットワーキングに対応したシスコのデータセンター ソリューションにおいてどのような位置付けにありますか。**
- A. Cisco ACE は、アプリケーション ネットワーキング ソリューション ファミリーにおける次世代型のアプリケーション サービス モジュールです。当面、Cisco ACE は、ACE レベルのパフォーマンスと機能が要求される大規模かつ最も要件の厳しいデータセンター環境向けに提供されます。小規模な環境を利用しているお客様や個別の問題を重視しているお客様は、Cisco CSM を引き続き利用することで、高い効果を上げることができます。アプライアンス製品をご希望のお客様は、Cisco CSS 製品と Cisco AVS アプライアンスを組み合わせてご利用いただくのが最適です。**

表 1 CSS、CSM、および ACE 製品の比較

	Cisco CSS 11501	Cisco CSS 11503	Cisco CSS 11506	Catalyst® 6500 向け Cisco CSM	Catalyst® 6500 向け Cisco ACE
					
フォームファクタ	スタンドアロン 固定型	スタンドアロン モジュール型	スタンドアロン モジュール型	統合型モジュール	統合型モジュール
ポート密度	8 FE 標準 1 GE オプション	2 GE 標準 最大 32 FE/6 GE	2 GE 標準 最大 80 FE/12 G	46-528 FE 8-178 GE	46-528 FE 8-178 GE
サイト アクティビティ	低	中	高	高	最高
ハードウェアの 拡張性	★	★★	★★★	★★★★	★★★★★
ハードウェアの 冗長性	×	×	○	○	○
セッションの 冗長性	○	○	○	○	○
レイヤ 2 ~ 3 ネットワーキング	○	○	○	○	○
管理/制御	○	○	○	○	○
SSL アクセラ レーション	外部	内部	内部	Catalyst 6500 の SSL モジュール	内部
コンテンツ スイッチング	サーバ、キャッシュ、ファイアウォール、VPN				

位置付け

Q. Cisco ACE とは何ですか。

- A.** Cisco ACE は、Cisco Catalyst 6500 に搭載する多機能モジュールです。Cisco ACE を使用すると、企業はアプリケーションの導入、プロビジョニング、高速化、および、管理を迅速に行うことができます。また、インフラストラクチャの論理的なパーティション分割を使用して物理的なアプリケーション サイロを最小限に抑え、新たな基準となる優れたパフォーマンスとセキュリティを提供し、多数の機能を統合することができます。これにより、これまでにない優れた IT 制御が可能になり、ビジネスにおけるサービスの迅速な展開と優れたパフォーマンスを提供できるようになります。

Cisco ACE ソリューションは、次の特長を備えています。

- **アプリケーション インフラストラクチャの制御** — 仮想パーティショニングやロールベースのアクセス制御を使用して、アプリケーション インフラストラクチャの導入、運用、および管理を制御できる次世代型の IT ソリューションを提供します。
- **アプリケーション パフォーマンス** — データセンターのアプリケーション配信に必要な卓越したパフォーマンス、優れたスケーラビリティ、および高度なアベイラビリティを提供します。
- **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やインフラストラクチャの保護、およびデータの不正利用防止を保証します。
- **インフラストラクチャの簡素化** — 業界をリードするエンタープライズクラスのスイッチである Cisco Catalyst 6500 との統合により、インフラストラクチャのコストと複雑性を最小限に抑え、デバイスおよびベンダー数を減少させます。

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 はネットワークに完全に統合された唯一の製品であり、完全に仮想化されたパーティションを作成する機能を持っています。この機能を使用すると、非集中型管理による集中展開が可能になり、個々のアプリケーション チームが完全な管理制御を実行できるようになります。Cisco ACE はレイヤ 2 ~ 7 のすべてのサービスを提供します。これらのサービスは、リソースの保証と Role-Based Access Control (RBAC; ロールベース アクセス コントロール) によって、単一モジュール内でパーティション分割されます。

Q. アプリケーション インフラストラクチャの制御とは、何を意味しているのですか。

- A.** IT 企業に対する要求が厳しさを増し、組織のサイロ間でのより迅速な対応と協力の必要性が高まる中で、お客様はアプリケーション インフラストラクチャの強力な制御を可能にするソリューションを必要としています。Cisco ACE では、仮想パーティションという概念が採用されています。仮想パーティションでは、単一の物理デバイスを個別に管理および運用することが可能な最大 250 の論理デバイスとして機能させることができます。また、GUI ベースのデバイス マネージャ、強力な CLI (コマンドライン インターフェイス)、および Extensible Markup Language (XML) ベースの API のいずれかを使用して、単一の物理デバイスを論理的にパーティション分割することで、完全に分離された管理コンテキストをサポートできます。リソースは、ビジネス、アプリケーション、顧客区分などの要件に基づいて配分および管理できます。変更管理 (追加、削除、変更) は論理/仮想インスタンスごとに実施できます。また、より詳細な制御を可能にする RBAC により、単一の ACE モジュールの各種サービスを同時に使用する複数のチームに管理責任を完全に委任できます。仮想パーティションと RBAC を組み合わせると、業務の委任によりワークフローを簡素化できます。Cisco ACE は、論理的な抽

象レイヤを提供することにより、スイッチング/ルーティング (VLAN および Virtual Route Forwarding [VRF] を使用)、ストレージ (Virtual Storage-Area Network [VSAN] を使用)、およびアプリケーション/セキュリティ サービスなどの他の仮想化および管理方式を補完しています。Cisco ACE は、このような優れた運用上の柔軟性を備えているため、ビジネス ニーズやお客様の要求への迅速な対応を低コストかつ複雑性を伴わずに実現できます。柔軟性の高い展開および制御が可能な Cisco ACE を利用すると、アプリケーション インフラストラクチャ全体をよりスケーラブルかつ効率的に利用することで卓越したパフォーマンスを実現できます。

Q. 企業に Cisco ACE が必要となる理由を教えてください。

A. Cisco ACE は、企業やサービス プロバイダーのお客様が必要とする卓越したネットワーク/アプリケーション パフォーマンス、運用の柔軟性、セキュリティ、およびアプリケーションの高速化を提供します。Cisco ACE を使用すると、お客様はセキュリティの強化とエンドユーザのアプリケーションの操作性向上を同時に実現しながら、運用コストを削減できます。Cisco ACE は、このような機能の利用を検討しているすべてのお客様にとって有益ですが、大規模なスケーラビリティを必要とし、アプリケーション展開の合理化ニーズを持つ大企業のお客様に最も適しています。

Q. Cisco ACE サービス モジュールと Cisco AON には、どのような関係があるのですか。

A. Cisco ACE モジュールは、拡張性、信頼性、セキュリティ、およびパフォーマンスに優れたアプリケーション インフラストラクチャを実現することを目的としています。Cisco AVS と組み合わせて使用する場合、Cisco ACE は、主に使用するリソースを最小限に抑えてエンドユーザ応答時間を向上させる役割を果たします。Cisco AON テクノロジーはビジネス アプリケーション間のコミュニケーションをサポートすることを主な目的として設計されており、分散したアプリケーション間のメッセージ変換や切り替えを可能にします。ACE と AON はそれぞれ企業内の異なる問題を解決するように設計されています。

Q. Cisco Catalyst 6500 のサービス モジュール製品は、Cisco ACE サービス モジュールによってどのように強化されるのですか。

A. Cisco ACE は、現在 Cisco CSM や Cisco SSL Module (SSLM) で提供されている次世代型のテクノロジーを搭載しています。従来のサービス モジュールは、特定のデータセンター タスクに特化し、一般的なお客様に適したスピードでこれらのタスクを実行しています。Cisco ACE モジュールでは、仮想パーティションを採用し、1 枚の拡張可能なラインカードに複数のサービスを統合できるため、卓越したスループット、スケーラビリティ、およびセキュリティでこれらのサービスを提供できます。これらのサービスは、データセンター内のすべての IP ベース アプリケーションで使用できます。

Q. Cisco ACE サービス モジュールはどのような市場を対象としていますか。

A. Cisco ACE サービス モジュールは、一般的にアプリケーション配信と呼ばれる市場を対象としています。現在、アプリケーション配信の機能には、Server Load Balancing (SLB; サーバロードバランシング) やレイヤ 4 ~ 7 スwitching、高度なアプリケーション最適化サービス、および SSL アクセラレーションや TCP 再利用などのサーバ オフロード機能などがあります。Cisco ACE と Cisco AVS などの関連ソリューションは、これらの機能に加えてさらに多くの機能をサポートしています。

Q. Cisco ACE サービス モジュールは、シスコ エンタープライズ データセンター ソリューションでどのように位置付けられるのですか。

A. Cisco ACE サービス モジュールは標準的な Cisco Catalyst 6500 シャーシに搭載できるため、優れたアプリケーション インフラストラクチャ制御、高速化、アプリケーション 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の各種サービスを搭載した多機能デバイスとして Cisco Business Ready Data Center ソリューションに組み込むことができます。Cisco ACE と新しい Cisco AVS 製品を組み合わせると、Web アプリケーションのさらなる高速化やアプリケーション プロトコル/ペイロードの強固なセキュリティを実現できます。

- Q. 既存のサービス モジュールを Cisco ACE サービス モジュールにアップグレードすることは可能ですか。**
- A.** いいえ。Cisco ACE サービス モジュールは、新しく導入されたハードウェア/ソフトウェア ソリューションです。ただし、Cisco CSM などの既存のサービス モジュールと同じシャーシに搭載することは可能です。

機能

Q. Cisco ACE の主な展開シナリオについて教えてください。

- A.** 通常、Cisco ACE サービス モジュールは、複数のサーバ ファームのフロントエンドにあるデータセンターで、多数のアプリケーション タイプをサポートするために使用します。Cisco ACE サービス モジュールは通常、内部および外部のユーザ アプリケーション要求を処理するクライアント VLAN およびサーバ リソースの分離と保護を可能にするサーバ VLAN を使用して構成されます。

Q. Cisco ACE サービス モジュールのコア機能は何ですか。

- A.** Cisco ACE サービス モジュールのコア機能は、アプリケーション インフラストラクチャ制御、アプリケーション パフォーマンス、アプリケーション セキュリティ、およびインフラストラクチャの簡素化に分類されます。以下に簡単な説明を示します。

- **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、サービス展開の大幅な迅速化、管理上のオーバーヘッドの削減、およびワークフローの簡素化を実現します。このようなデバイスには、XML、API、管理 GUI、および強力な CLI などの複数の管理インターフェイスが含まれます。
- **業界最高レベルのパフォーマンスとスケーラビリティ** — 最大 16 Gbps のスループットとモジュールあたり毎秒 345,000 のレイヤ 4 接続の確立が可能であり、大容量のデータ ファイル、リッチメディア、および大規模なユーザ ベースにも対応できます。
- **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 ログイングなどの機能が利用できます。
- **Cisco Catalyst 6500 スイッチのシャーシに搭載されたコントローラや入出力ポートと連携したレイヤ 2 ~ 7 機能の統合、および単一のデータ処理パスでの複数サービスの集約** — トラフィック効率の向上、高密度なネットワーク設計、デバイス数の削減、アベイラビリティの向上、および管理の簡素化を実現します。

コア機能には、次の詳細な機能が実装されています。

SLB

- **プレディクタ** — ラウンド ロビン、重み付きラウンド ロビン、最小接続、IP ハッシュ、接続ウォーターマーク、およびコンテンツ認識
- **ヘルス プローブ** — レイヤ 3 ping、レイヤ 4 UDP データ、HTTP GET、HTTP HEAD、Domain Name System (DNS; ドメイン ネーム システム)、Point of Presence (POP)、Internet Mail

Access Protocol(IMAP)、Telnet、Internet Control Message Protocol(ICMP)、TCP、UDP、Echo、Finger、Simple Mail Transfer Protocol(SMTP)、RADIUS、Lightweight Directory Access Protocol(LDAP)、および HTTP GET over SSL

- TCP 接続管理(複数のクライアント TCP 接続で単一のサーバ TCP 接続を横断)
- HTTP リダイレクション
- 保持 — クッキー、クッキー挿入(オフセットおよび長さ)、およびヘッダー挿入
- 冗長性 — アクティブ-アクティブ、ステートフル、およびアクティブ-バックアップ

SSL オフロード

- SSL 復号化
- SSL 暗号化
- 証明書の集中管理
- バックエンド SSL
- エクスポート暗号スイート
- SSL v2、v3 および Transparent LAN Services(TLS; 透過型 LAN サービス)v1.0
- セットアップ証明書

データセンター セキュリティ

- プロトコル検査および一般的なデータセンター プロトコルのフィックスアップ
- ポート間のトラフィックを選択的に許可する最大 256,000 のアクセス制御要素を持つ Access Control List(ACL; アクセス コントロール リスト)
- SYN クッキー
- 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

Q. Cisco ACE サービス モジュールのパフォーマンス特性について教えてください。

A. Cisco ACE サービス モジュールを使用すると、アプリケーション配信市場で最高レベルのパフォーマンスを実現できます。Cisco ACE サービス モジュールは、最大 16 Gbps のスループットを持ち、モジュールあたり毎秒 345,000 の持続的なレイヤ 4 接続の確立が可能です。Cisco ACE モジュールは、単一の Cisco Catalyst 6500 シャーシに最大 4 つ搭載できるため、卓越したスケーラビリティを実現できます。パフォーマンス メトリックについては、データシートまたは <http://www.cisco.com/jp/go/ace> を参照してください。

Q. Cisco ACE サービス モジュールと互換性のあるスーパーバイザ エンジンは何ですか。

A. Cisco ACE サービス モジュールは、当面、Cisco Catalyst 6500 シリーズ Supervisor Engine 720(Policy Feature Card 3A [PFC3A; ポリシー フィーチャ カード 3A]、PFC3B、または PFC3b-XL を搭載)でサポートされます。

- Q.** Cisco ACE サービス モジュールで、Cisco IOS[®] ソフトウェアを使用することはできますか。
- A.** いいえ。Cisco ACE サービス モジュールは、独自のオペレーティング システムを使用します。ACE は Cisco Catalyst 6500 ファブリック対応モジュールです。
- Q.** Cisco Catalyst 6500 シリーズ ファイアウォール サービス モジュール、Cisco CSM、Cisco SSLM、および Cisco ACE サービス モジュールを同じシャーシに搭載することはできますか。
- A.** はい。
- Q.** Cisco ACE サービス モジュールに外部インターフェイスはありますか。
- A.** はい。Cisco ACE サービス モジュールには、外部制御用の複数の管理インターフェイスが用意されています。まず、Cisco ACE には管理アクセスに使用する標準の外部コンソールポートがあり、標準の CLI を使用することができます。また、各種管理ツールとの統合用に XML API が用意されています。これは、特定のアプリケーションで制御できます。さらに、すべての機能と RBAC をフルサポートするフル GUI ベースのマネージャも提供される予定です。Cisco ACE は、稼働中に Cisco Catalyst 6500 のスーパーバイザ エンジンとセッションを確立できます。Cisco ACE には、データの入出力ポートはありません。
- Q.** Cisco ACE サービス モジュールは、1 台の Cisco Catalyst 6500 シャーシにいくつ搭載できますか。
- A.** Cisco ACE サービス モジュールは、シャーシごとに最大 4 つサポートされます。
- Q.** Cisco ACE サービス モジュールはフェールオーバーをサポートしていますか。
- A.** はい。フェールオーバーは、冗長 Cisco ACE サービス モジュールを使用するアプリケーション インスタンス間において仮想パーティション単位でサポートされます。ステートフルな冗長性は、従来のアクティブ-スタンバイおよびアクティブ-アクティブ構成で利用できます。ステートフル フェールオーバーは、同一の ACE モジュール間のシャーシ内外でともにサポートされます。Cisco ACE モジュールは、Cisco GSS 4400 Global Site Selector と組み合わせた場合、リモート データ センターを含むフェールオーバー シナリオでも使用できます。
- Q.** Cisco ACE サービス モジュールでサポートされる仮想パーティションはいくつですか。
- A.** Cisco ACE サービス モジュールは、最大 250 の仮想パーティションをサポートします。
- Q.** Cisco ACE サービス モジュールは、すべての Cisco Catalyst 6500 または Catalyst 7600 シリーズ シャーシで使用できますか。
- A.** はい。Cisco ACE サービス モジュールはファブリック対応であるため、すべての Cisco Catalyst 6500 または Catalyst 7600 シリーズ シャーシのフォーム ファクタで使用できます。
- Q.** 搭載できるフラッシュ メモリや DRAM メモリの容量について教えてください。また、DRAM のアップグレードは可能ですか。
- A.** Cisco ACE サービス モジュールには、256 MB の交換可能なフラッシュ メモリと 3 GB の DRAM が付属しています。DRAM のアップグレードはできません。
- Q.** Cisco ACE サービス モジュールは、ネイティブの Cisco IOS ソフトウェアおよびハイブリッドシステムの両方で使用できますか。
- A.** はい。

Q. ハイ アベイラビリティ データセンター向けの Cisco ACE サービス モジュールでは、地理的分散へのサポートはどのようになっていますか。

A. Cisco GSS 4400 Global Site Selector でグローバル SLB が提供されています。これにより、地理的に離れた場所に展開される Cisco ACE サービス モジュールでのハイ アベイラビリティがサポートされます。

コンポーネント

Q. Cisco ACE モジュールのコンポーネントについて教えてください。

A. Cisco ACE は Cisco Catalyst 6500 スイッチまたは Cisco 7600 ルータ向けのサービス モジュールとして提供されます。Cisco ACE は Supervisor Engine 720 と Cisco IOS ソフトウェアが稼働する Cisco Catalyst 6500 または Cisco 7600 シャーシで使用できます。Cisco ACE モジュールには入出力ポートがなく、Cisco Catalyst スイッチを経由してネットワーク接続を行います。

Cisco AVS に関する Q&A

Q. 新しい Cisco AVS 6.0 Web Application Firewall フィーチャ セットとは何ですか。また、これにより、どのような問題が解決されますか。

A. Web アプリケーションは企業のセキュリティ網の大きな弱点となる可能性があるため、Web アプリケーションに対するセキュリティは非常に重要です。従来のファイアウォールは、ポートレベルや送信元/宛先レベルでの保護を提供しますが、危険なトラフィック タイプやコンテンツの識別および防御を行うことはほとんどありません。そのため、ハッカーがビジネス アプリケーションを攻撃して情報を奪ったり、サービスを停止させたりする可能性があります。

新しい Cisco AVS 3120 Web Application Firewall モジュールを使用すると、Web アプリケーションに対する最高レベルの攻撃防御を実現できます。Cisco AVS は、すべてのアプリケーション プロトコルとコンテンツをスキャンして、ビジネス固有のポリシーを適用することにより、Structured Query Language (SQL) インジェクション、データ盗難、パラメータ改ざん、クッキー ポイズニングなどのアプリケーション レイヤ攻撃からインフラストラクチャと企業を防御します。Cisco AVS 3120 は、ネットワーク セキュリティの専門家による迅速かつ容易な導入が可能のため、すべてのエンタープライズ アプリケーションのリスクを速やかに修復するのに最適なソリューションです。アプリケーション レイヤの精査が可能な Cisco AVS 3120 を使用すると、ネットワーク構成に影響を与えることなく、リアルタイムでの脅威の防御と分析を行うことができます。

Q. Cisco AVS 6.0 の新機能について教えてください。

A. Cisco AVS 6.0 ソフトウェアの新機能は、Web アプリケーション セキュリティ機能の向上に重点を置いています(表 2)。

表 2 Cisco AVS 6.0 の新機能

	新機能	利点
攻撃の防止および入力検証に対する改善	<ul style="list-style-type: none"> 事前定義されたアプリケーション レイヤ攻撃ルールの数を増強 ルール作成用のカスタマイズ可能な正規表現 (regex) を GUI で表示 ルールの作成や優先順位の設定における操作性を向上 ユーザは、アクティブ モードまたはパッシブ モードでルール設定が可能 	<ul style="list-style-type: none"> 業界最高レベルの攻撃防御を実現 次の攻撃から Web アプリケーションを保護 <ul style="list-style-type: none"> SQL インジェクション クロスサイト スクリプティング LDAP インジェクション コマンド インジェクション バッファ オーバーフロー 悪意のあるコードの挿入

	新機能	利点
アプリケーション ラーニング	<ul style="list-style-type: none"> アプリケーションによるパラメータのリアルタイム学習 アプリケーション情報に基づいたアプリケーションによるルールの迅速な作成 ログ情報に基づいたアプリケーションによるセキュリティルールのダイナミックな作成 	<ul style="list-style-type: none"> 精度の高いセキュリティポリシーの提供 パラメータ改ざんの防止 導入コストの削減
HTTP の正規化	<ul style="list-style-type: none"> HTTP プロトコルによるすべてのアプリケーショントラフィックの正規化 	<ul style="list-style-type: none"> エンコードされた攻撃や偽装された攻撃を防御 ディレクトリ トラバーサルやその他のエンコード関連攻撃を阻止
HTTP プロトコル適合	<ul style="list-style-type: none"> HTTP プロトコル適合の実施 	<ul style="list-style-type: none"> 多様な URL ベースの攻撃を防御
クッキーの保護	<ul style="list-style-type: none"> ユーザによるクッキーのリアルタイムでの暗号化または改ざん防止が可能 	<ul style="list-style-type: none"> クッキーの偽装や改ざんなどのクッキーベースの攻撃を阻止
アプリケーション クローキング	<ul style="list-style-type: none"> アプリケーション クローキングによるサーバヘッダーのマスキング アプリケーション クローキングによるエラーリターンコードのブロックおよびカスタマイズ 	<ul style="list-style-type: none"> アプリケーション偵察の阻止
リクエスト制限	<ul style="list-style-type: none"> リクエスト制限による URL およびヘッダー制限の実施 	<ul style="list-style-type: none"> バッファ オーバーフロー攻撃の防止
モニタリングおよびロギング	<ul style="list-style-type: none"> Syslog によるすべての Web 攻撃の記録 ロギングによる攻撃のグラフィカル表示 	<ul style="list-style-type: none"> 精度の高いモニタリングとフォレンジクス
データ盗難の防止	<ul style="list-style-type: none"> クレジットカード番号や社会保障番号などの機密データの盗難に対する完全な防御を提供 データ構造のカスタマイズが可能 	<ul style="list-style-type: none"> 1996 年の Health Insurance Portability and Accountability Act (HIPAA; 医療保険の携行性と責任に関する法律)、Gramm Leach Bliley Act (GLBA; 米国金融制度改革法)、および CA SB-1386 などの規制による厳しいプライバシー要件に準拠
アウトオブバンド モニタリング	<ul style="list-style-type: none"> アウトオブバンド構成のアーキテクチャにより、ネットワークへのトラフィック送信やハッカーが狙う攻撃ポイントの作成を防止し、ネットワーク上のトラフィック遅延の発生を阻止 	<ul style="list-style-type: none"> リスクを伴わない低コストな展開を実現 最小限の管理要件でアプリケーション レイヤ攻撃の詳細な把握が可能

Q. Cisco AVS Web Application Firewall と Intrusion Prevention System (IPS; 侵入防御システム)の違いは何ですか。

A. IPS は Windows、Solaris、Apache、または Microsoft Internet Information Services (IIS) といった主要なプラットフォームの既知の脆弱性に対する攻撃を防御する優れたソリューションです。Cisco AVS は、ビジネス アプリケーションや Web サイトに対する攻撃の防御に適しています。これらのアプリケーションには、ソフトウェア ベンダーが構築したアプリケーションや社内でカスタマイズされた独自アプリケーションなどがあります。通常、このようなタイプのアプリケーションにはセキュリティ パッチやシグニチャは利用できません。また、それぞれのアプリケーションにこのようなレベルのセキュリティを組み込むことは、ほぼ不可能です。

Q. Cisco AVS Web Application Firewall とネットワーク ファイアウォールの違いについて教えてください。

A. Cisco AVS 3120 は、Cisco PIX[®] Firewall や Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンスなどのネットワーク ファイアウォールと相互に補完しあう製品です。Cisco AVS Web Application Firewall は Web ベースのアプリケーションを保護し、ネットワーク ファイアウォールはネットワークを保護します。そのため、Cisco AVS を使用すると、Web アプリケーションの確実な防御を実現できます。

ネットワーク ファイアウォールは、ネットワーク、IP アドレス、およびポートに対してポリシーを適用します。また、さまざまなプロトコルに対応した幅広いアプリケーション レイヤ機能を持っています。ファイアウォールは、ブランチ、ネットワーク エッジ、およびエンタープライズ エッジなどのさまざまな場所で使用できます。Cisco AVS は URL、ヘッダー、およびパラメータなど

の HTTP データに対してポリシーを適用します。Cisco AVS は、Web アプリケーションのフロントエンドのデータセンターでのみ使用します。

Q. Cisco AVS 3100 シリーズ Application Velocity System アプライアンスの各種製品について教えてください。

A. Cisco AVS 3110 アプライアンス製品は、シスコが Fineground Networks 社を買収したことによって追加されました。このアプライアンスをサポートするソフトウェアの最新バージョンは、Fineground Version 5.0 ソフトウェアです。このアプライアンス ベースの製品には、「Fineground Networks 社」のロゴ、ドキュメント スプラッシュ画面、カラーなどが使用されています。

Cisco AVS 3120 および AVS 3180 は、シスコが開発したアプライアンスで、シスコのロゴ、ドキュメント スプラッシュ画面、およびカラーなどが使用されています。これらのアプライアンスは、Cisco AVS 3110 アプライアンスの後継機種です。

Cisco AVS 3120 はインライン型のアプライアンスで、Web アプリケーションのパフォーマンス向上とセキュリティ機能の追加が行われています。Cisco AVS 3180 Management Station は、オプションのアプライアンスベースの管理コンソールであり、Cisco AVS 3120 アプライアンスの設定と管理を行います。また、Cisco AVS AppScope Monitor のパフォーマンス モニタリング機能を使用する場合には、Cisco AVS 3180 も必要になります。Cisco AVS 3120 には組み込み型のデバイス マネージャが用意されているため、Cisco AVS 3180 を使用して設定を行う必要はありません。

Q. Cisco AVS 6.0 ソフトウェアは、どのアプライアンスでサポートされていますか。

A. Cisco AVS 6.0 ソフトウェアは、Cisco AVS 3110 ハードウェアではサポートされていません。Cisco AVS 6.0 ソフトウェアを稼働するには、Cisco AVS 3120 ハードウェアへのアップグレードが必要です。

Cisco AVS 6.0 ソフトウェアで Cisco AVS 3120 アプライアンスを管理する場合は、オプションの Cisco AVS 3180 Management Station を Cisco AVS 6.0 Management Station ソフトウェアにアップグレードする必要があります。Cisco AVS 6.0 Management Station ソフトウェアを搭載した Cisco AVS 3180 Management Station の場合、すべての Cisco AVS 3120 ハードウェアで Cisco AVS 6.0 ソフトウェアが稼働している必要があります。Cisco AVS 5.0 ソフトウェアと AVS 6.0 ソフトウェアが混在した環境を Cisco AVS 3180 で管理することはできません。Cisco AVS 6.0 ソフトウェアを搭載した Cisco AVS 3180 Management Station で Cisco AVS 3110 を管理することは、Cisco AVS 3110 に搭載されたソフトウェアのバージョンを問わずできません。

Q. 現在の Cisco AVS 5.0 AppScreen Web Application Firewall の機能は、Cisco AVS Version 6.0 ソフトウェアでも利用できますか。

A. はい。AppScreen フィーチャ セットは Cisco AVS 6.0 ソフトウェアでも利用できます。AppScreen と新しい Web アプリケーション セキュリティ機能は異なるソフトウェア モジュールですが、類似したフィーチャ セットを備えています。AppScreen 機能は、AVS ソフトウェアの次期メジャー リリースではソフトウェアから削除される予定です。これは、新しい Web アプリケーション セキュリティ モジュールでは AppScreen に代わる設定可能なパラメータが用意されていることへの理解が浸透しつつあるためです。

Q. Cisco AVS 6.0 の構成モードについて教えてください。

A. Cisco AVS 6.0 には、アウトオブバンド モニタリング、インライン透過モード、およびゲートウェイ モードの 3 つの構成モードがあります。ゲートウェイ モードでは Cisco AVS 5.0 ソフトウェアと同じネットワーク構成が必要となります。このモードは原則として、アプリケーションのフロントエンドに配置するリバース プロキシとして展開します。このモードでは、アクセラレーション フィーチャ セットと Web アプリケーション セキュリティ フィーチャ セットの両方を同時に実行できます。インライン透過モードとアウトオブバンド モニタリングは、新しい Web アプリケーション ファイアウォール機能でのみ利用できます。インライン透過モードを使用すると、Cisco AVS をインラインで展開できるため、デフォルト ゲートウェイなどの他のネットワーク構成を変更する必要がありません。インライン透過モードやゲートウェイ モードは、Cisco CSS または Cisco CSM のロード バランシングを使用して、アベイラビリティやスケーラビリティを向上させる場合にも使用できます。アウトオブバンド モニタリング モードは、スイッチ上の SPAN ポートから離れた場所に展開します。SPAN ポートはアプリケーションで送受信されるすべての Web トラフィックを複製して、Cisco AVS に転送します。この展開オプションはリスクを伴いません。ただし、このモードでは、潜在的な攻撃に対するログの取得と警告のみを行い、攻撃検出時のトラフィック ブロックは行いません。

©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>

0120-933-122(通話料無料)、03-6670-2992(携帯電話、PHS)

電話受付時間：平日10:00～12:00、13:00～17:00

お問い合わせ先