Cisco Web セキュリティ アプライアンス

セキュリティを確保するために、ネットワークには、マルウェア対策、アプリケーションの可視化と制御、アクセプタブル ユース ポリシーによる制御、洞察力に富んだレポート機能、セキュアなモビリティが必要です。シスコではこのすべての保護を 1 つのプラットフォーム、Cisco® Web セキュリティ アプライアンス（WSA）で提供しています。

ネットワーク化とモバイル化の進んだ現代では、より複雑で高度な脅威に対抗するために、さまざまなセキュリティ ソリューションを適切に組み合わせることが求められています。シスコは、ネットワーク インフラストラクチャのあらゆる階層に、強力な保護、きめ細かい制御、投資に見合う価値、ビジネス ニーズといった要件を満たすセキュリティを導入します。また、最先端のグローバル脅威インテリジェンスと、Web セキュリティ導入のための多様なオプションも提供しています。Cisco WSA は、セキュリティをシンプルにする高性能な専用アプライアンスです。また、Cisco Web セキュリティ仮想アプライアンス（WSAV）を利用すれば、場所や時間を問わず、Web セキュリティを必要に応じて迅速に導入できます。

Cisco WSA は、Web トラフィックのセキュリティや制御において増加し続ける課題に、先進的な保護機能を組み合わせて取り組む最初のセキュアな Web ゲートウェイの 1 つでした。Cisco WSA は、より少ないメンテナンス要件で簡単かつ迅速に導入でき、遅延を抑え、運用コストを削減します。「Set and forget」テクノロジーのおかげで、最初の自動ポリシー設定を行えば、3 ～ 5 分おきにセキュリティ アップデートがネットワーク デバイスへ自動的にプッシュ配信されるので、管理者の手を煩わせることがありません。柔軟な導入オプションに加えて、既存のセキュリティ インフラストラクチャとの統合が可能であるため、進化していくセキュリティ要件にも迅速に対応できます。

仮想アプライアンス

現代では、ビデオなどのリッチ メディアの利用が広まったことでトラフィックの予測が困難になり、過負荷やパフォーマンス低下の問題が生じています。こうした問題を解決しようとする企業（特に多国籍企業）の管理者は、ハードウェアを購入して設置するまでの準備時間の長さ、リモート インストールの難しさ、関税といったロジスティクス面での課題に直面することになります。

Cisco Web WSAV は、いつでも、どこにでも必要に応じてセキュリティ インスタンスを作成でき、特に大規模な分散ネットワーク環境に Web セキュリティを導入する際のコストを大幅に削減します。Cisco WSAV はソフトウェア版の Cisco WSA であり、VMware ESXi 上または KVM ハイパーバイザおよび Cisco Unified Computing System™（Cisco UCS®）サーバ上で動作します。Cisco E メール セキュリティまたは Cisco Web セキュリティのいずれかのソフトウェア バンドルを購入すれば、Cisco SMAV の無制限のライセンスと、対応する SMA ソフトウェア ライセンスを入手できます。

Cisco WSAV を使用すると、管理者はトラフィックの急増にすばやく対応できるため、キャパシティ プランニングが不要になります。アプライアンスの購入や出荷は必要ありません。データセンターをさらに複雑化したり、人員を追加したりしなくても、新たなビジネス チャンスに対応することが可能です。

機能と利点

Talos セキュリティ インテリジェンス	世界最大級の脅威検知ネットワークをベースとした迅速かつ包括的な Web への保護を受けられます。可視性と規模も最大級で、詳細は次のとおりです。 • 毎日 100 TB のセキュリティ インテリジェンス • 160 万台の導入済みセキュリティ デバイス（ファイアウォール、IPS、Web、E メール アプライアンス） • 1 億 5,000 万台のエンドポイント • 1 日あたり 130 億件の Web 要求 • 世界のエンタープライズ E メール トラフィックの 35 % グローバルなトラフィック アクティビティを 24 時間体制で提供し、問題点の分析、新しい脅威の検出、トラフィック トレンドのモニタが可能です。Talos は、新しいルールを継続的に生成し、そのアップデートを 3 ～ 5 分おきに Cisco WSA に供給することでゼロアワー攻撃を防止し、競合他社よりも数時間または数日早く、最先端の脅威防御を実現することができます。
Cisco Web 使用コントロール	従来の URL フィルタリングに動的コンテンツ分析と組み合わせることで、コンプライアンス、法的責任、生産性のリスクを軽減します。これまで継続的に更新されてきた URL フィルタリング データベースには 5,000 万のブロック済みサイトが登録されており、既知の Web サイトでは群を抜いたカバー率を誇ります。動的コンテンツ分析（DCA）エンジンは、未知の URL の 90 % をリアルタイムで正確に認識し、テキストをスキャンして関連性のスコアを決定し、モデル ドキュメントの近似値を求めて、一致したカテゴリの中で最も近いものを返します。管理者はインテリジェントな HTTPS インスペクションで特定のカテゴリを選択することもできます。
高度なマルウェア防御	高度なマルウェア防御（AMP）は、すべての Cisco WSA ユーザが使用できる、追加ライセンス機能です。AMP は包括的なマルウェア回避ソリューションで、マルウェアの検出とブロック、継続的な分析、および遡及的なアラートが可能です。シスコと Sourcefire® のテクノロジーによる広範なクラウド セキュリティ インテリジェンス ネットワークを活用します。AMP は、拡張ファイル レピュテーション機能、ファイル動作の詳細レポート、連続的なファイル分析、および遡及的な判定アラートを使用して、Cisco WSA にすでに搭載されているマルウェア検出およびブロック機能をさらに強化します。Cisco AMP Threat Grid は、クラウドへのマルウェア サンプルの送信にコンプライアンスやポリシー規制を敷いている組織のために、オンプレミス アプライアンスによるマルウェア防御を提供しています。レイヤ 4 トラフィック モニタはアクティビティを連続的にスキャンし、スパイウェアによる「コール ホーム」コミュニケーションを検知してブロックします。すべてのネットワーク アプリケーションをトラッキングすることで、レイヤ 4 トラフィック モニタは、従来の Web セキュリティ ソリューションをくぐりぬけようとするマルウェアを効果的に阻止することができます。既知のマルウェア ドメインの IP アドレスは、悪意あるプログラムのリストへ動的に追加され、ブロックされます。
Cognitive Threat Analytics	シスコの認識脅威分析は、ネットワーク内部で動作している脅威の検出時間を短縮する、クラウド ベースのソリューションです。このソリューションは、動作分析と異常検出を使用してマルウェアへの感染やデータ漏洩の症状を識別することにより、境界ベースの防御におけるギャップを解消します。Cisco Cognitive Threat Analytics は、ご使用の Web セキュリティ ソリューションにライセンスを追加するだけで利用できます。複雑性を軽減しながらも、変化する脅威の状況に応じて進化する優れた防御機能を手に入れることができます。
Application Visibility and Control（AVC）	何百もの Web 2.0 アプリケーションや 150,000 以上の小規模なアプリケーションの使用を簡単に制御できます。きめ細かい制御で、Dropbox や Facebook などのアプリケーションの使用を許可しながら、ドキュメントのアップロードや「いいね」ボタンのクリックといったアクティビティを阻止することができます。Cisco WSA は、ネットワーク全体のアクティビティを可視化できます。新機能：お客様は、ユーザ、グループ、およびポリシーごとに帯域幅および時間クォータをカスタマイズできます。
データ損失の防止（DLP）	基本の DLP でコンテキスト ベースのルールを作成し、機密データがネットワーク外に流出するのを防ぎます。また、Cisco WSA は Internet Content Adaptation Protocol（ICAP）でサードパーティの DLP ソリューションを統合し、より詳細なコンテンツ インスペクションと DLP ポリシーの強化を実現します。Cisco WSA は、WSA とサードパーティ DLP のソリューション間でやり取りされるトラフィックを暗号化する、安全な ICAP をサポートしています。

ローミング ユーザ保護	トラフィックをオンプレミス ソリューションにリダイレクトする VPN トンネルを開始してリモート クライアントに Web セキュリティを提供する Cisco AnyConnect® セキュア モビリティ クライアントと統合することで、Cisco WSA はローミング ユーザを保護します。Cisco AnyConnect テクノロジーは、アクセスを許可する前にリアルタイムでトラフィック分析を行います。 Cisco WSA は、Cisco Identity Services Engine（ISE）とも統合されています。この画期的な機能拡張により、要求に応じて、Cisco WSA で Cisco ISE の機能を利用できます。Cisco ISE の統合により、管理者は Cisco ISE がシングル サインオン プロセスで収集したプロファイルまたはメンバーシップ情報に基づいて Cisco WSA 上でポリシーを作成できるようになります。
一元化された管理およびレポート	脅威、データ、アプリケーションにわたって実行可能な見識を受け取ります。Cisco WSA では、使い勝手のよい集中管理ツールから、運用の制御、ポリシー管理、レポートの表示ができます。 Cisco M シリーズ コンテンツ セキュリティ管理アプライアンスは、仮想インスタンスを含む複数のアプライアンスや複数の場所を一元管理し、レポートを提供します。 Cisco® Web セキュリティ レポート アプリケーションは、Cisco Web Security Appliance（WSA）と Cisco Cloud Web Security（CWS）が生成したログをすばやくインデックス化して分析する、レポート ソリューションです。このツールは、トラフィックとストレージのニーズが大きい顧客にスケーラブルなレポート機能を提供します。レポート管理者は、Web の使用とマルウェア脅威に関する詳細な考察を収集することができます。
柔軟な導入	Cisco WSAV は、Cisco WSA の機能をすべて備えながら、インスタント セルフサービス プロビジョニングを含む仮想導入モデルの利便性とコスト節約のメリットも提供します。Cisco WSAV ライセンスがあれば、インターネットに接続することなく、ローカルに保存された新しい Cisco WSAV 仮想イメージ ファイルにライセンスを適用することで、Web セキュリティ仮想ゲートウェイを導入できます。元の仮想イメージ ファイルは、複数の Web セキュリティ ゲートウェイをすばやく導入するために、必要に応じてクローン作成できます。 ハードウェアと仮想マシンを同じ導入環境で実行できます。小規模なブランチ オフィスや離れた場所にも、Cisco WSA と同じ保護を適用できます。現地でハードウェアを設置したり、サポートする必要はありません。Cisco M シリーズ コンテンツ セキュリティ管理アプライアンスを使用すると、カスタム導入を簡単に管理できます。

製品仕様

表 1 と 2 は、それぞれ Cisco WSA のパフォーマンスとハードウェア仕様を示しています。

表 1. Cisco WSA のパフォーマンス仕様

	モデル	ディスク領域	RAID のミラーリング	メモリ	CPU
大規模企業	S690	4.8 TB （600 GB SAS X 8）	対応（RAID 10）	64 GB、DDR4	2 X 2.5 Ghz、24C
大規模企業	S690X	9.6TB （600 GB SAS X 16）	対応（RAID 10）	64 GB、DDR4	2 X 2.5 Ghz、24C
大規模企業	S680	2.4 TB （300 GB SAS X 8）	対応（RAID 10）	32 GB、DDR3	2 X 2.7 Ghz、16C
中規模オフィス	S390	2.4 TB （600 GB SAS X 4）	対応（RAID 10）	32 GB、DDR4	1 X 2.4 Ghz、8C
中規模オフィス	S380	2.4 TB （600 GB SAS X 4）	対応（RAID 10）	16 GB、DDR3	1 X 2.0 Ghz、6C
SMB およびブランチ	S190	1.2TB （600 GB SAS X 2）	対応（RAID 1）	8 GB、DDR4	1 X 1.9 Ghz、6C
SMB およびブランチ	S170	500 GB （500 GB SATA X 2）	対応（RAID 1）	4 GB、DDR3	1 X 2.8 Ghz、2C

* 現在のニーズと将来のニーズを満たすソリューションを選択するために、サイジングについてシスコのコンテンツ セキュリティ スペシャリストに確認してください。

表 2. Cisco WSA のハードウェア仕様

	Cisco S690	Cisco S690X	Cisco S680	Cisco S390	Cisco S380	Cisco S190	Cisco S170
ハードウェア プラットフォーム							
フォーム ファクタ	2 RU	2 RU	2 RU	1 RU	2 RU	1 RU	1 RU
寸法	8.6 X 48.3 X 73.7 cm（3.4 X 19 X 29 インチ）	8.6 X 48.3 X 73.7 cm（3.4 X 19 X 29 インチ）	8.9 X 48.3 X 73.7 cm（3.5 X 19 X 29 インチ）	8.6 X 48.3 X 73.7 cm（1.7 X 19 X 31 インチ）	8.9 X 48.3 X 73.7 cm（3.5 X 19 X 29 インチ）	8.6 X 48.3 X 73.7 cm（1.7 X 19 X 31 インチ）	8.9 X 48.3 X 73.7 cm（1.64 X 19 X 15.25 インチ）
冗長 P/S	対応	対応	対応	対応	対応	対応（アクセサリオプション）	非対応
リモートによる電源の再投入	対応	対応	対応	対応	対応	非対応	非対応
DC 電源オプション	対応	対応	対応	非対応	対応	非対応	非対応
ホットスワップ可能ハードディスク	対応	対応	対応	対応	対応	対応	対応
イーサネットインターフェイス	6 ポート 1 G Base-T 銅線 ネットワーク インターフェイス（NIC）、RJ - 45	6 ポート 1 G Base-T 銅線 ネットワーク インターフェイス（NIC）、RJ - 45	6 ポート 1 G Base-T 銅線 ネットワーク インターフェイス（NIC）、RJ - 45	6 ポート 1 G Base-T 銅線 ネットワーク インターフェイス（NIC）、RJ - 45	6 ポート 1 G Base-T 銅線 ネットワーク インターフェイス（NIC）、RJ - 45	2 ポート 1 G Base-T 銅線 ネットワーク インターフェイス（NIC）、RJ - 45	2 ポート 1 G Base-T 銅線 ネットワーク インターフェイス（NIC）、RJ - 45
速度（Mbps）	10/100/1000、オートネゴシエーション	10/100/1000、オートネゴシエーション	10/100/1000、オートネゴシエーション	10/100/1000、オートネゴシエーション	10/100/1000、オートネゴシエーション	10/100/1000、オートネゴシエーション	10/100/1000、オートネゴシエーション
ファイバ オプション	あり（別個の SKU） 6 ポート 1 G Base-SX ファイバ: WSA- S690-1G 6 ポート 10 G Base-SR ファイバ WSA- S690-10 G	あり（別個の SKU） 6 ポート 1 G Base-SX ファイバ: WSA- S690-1G 6 ポート 10 G Base-SR ファイバ WSA- S690-10 G	あり（別個の SKU） 6 ポート 1 G Base-SX ファイバ: WSA- S680-1G 6 ポート 10 G Base-SR ファイバ WSA- S680-10G	なし	なし	なし	なし

表 3 に Cisco WSAV の仕様、表 4 に Cisco M シリーズ コンテンツ セキュリティ管理アプライアンスの仕様を示します。

表 3. Cisco WSAV

Web ユーザ数				
Web ユーザ数	**モデル**	**ディスク**	**メモリ**	**コア**
～ 1000	S000v	250 GB	4 GB	1
1000 ～ 2999	S100v	250 GB	6 GB	2
3000 ～ 6000	S300v	1,024 GB	8 GB	4
サーバ		**ハイパーバイザ**		
Cisco UCS **Red Hat Enterprise Linux 7.0** **Ubuntu 14.04.1 LTS**		**ESXi 5.0、5.1、および 5.5** **KVM：QEMU 1.5.3** **KVM：QEMU 2.0.0**	vmware KVM	

表 4. Cisco M シリーズ コンテンツ セキュリティ管理アプライアンス

モデル	Cisco M680	Cisco M380	Cisco M170
ユーザ数（概数）	10,000 人以上	最大 10,000	最大 1,000

導入

Cisco WSA はフォワード プロキシで、明示的モード（プロキシ自動構成（PAC）ファイル、Web プロキシ自動発見（WPAD）、ブラウザ設定）、またはトランスペアレント モード（Web Cache Communication Protocol（WCCP）、ポリシーベース ルーティング（PBR）、ロード バランサ）のいずれかで導入できます。Cisco Catalyst® 6000 シリーズ スイッチ、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ、Cisco サービス統合型ルータ、Cisco ASA 5500-X シリーズ次世代ファイアウォール製品群などの Cisco WCCP 対応デバイスは、Cisco WSA に Web トラフィックを再ルーティングします。

Cisco WSA は、HTTP、HTTPS、SOCKS、ネイティブ FTP、FTP over HTTP トラフィックをプロキシし、データ損失防止、モバイル ユーザ セキュリティ、高度な可視性と制御など追加の機能を提供できます。

ライセンス

Cisco WSAV のライセンスは、すべての Cisco Web セキュリティ ソフトウェア バンドル（Cisco Web Security Essentials、Cisco Web Security Antimalware、および Cisco Web Security Premium）に含まれています。このライセンスの期間は、バンドル内のその他ソフトウェアと同様で、必要な数の仮想マシンで使用できます。

期間ベースのサブスクリプション ライセンス

ライセンスは、1 年間、3 年間、または 5 年間の期間ベースのサブスクリプションです。

人数ベースのサブスクリプション ライセンス

Cisco Web セキュリティ ポートフォリオでは、デバイスではなくユーザ数に基づき段階的価格を設定しています。それぞれのお客様の導入に適したサイジングの決定は、販売代理店およびパートナーの代理店がお手伝いします。

Web セキュリティのソフトウェア ライセンス

Web セキュリティのソフトウェア ライセンスには、4 種類あります。Cisco Web Security Essentials、Cisco アンチマルウェア、Cisco Web Security Premium、McAfee アンチマルウェアです。各ソフトウェアの主要なコンポーネントは、次のとおりです。

Cisco Web Security Essentials

- Cisco Talos による脅威インテリジェンス
- レイヤ 4 トラフィック モニタリング
- Application Visibility and Control（AVC）
- ポリシー管理
- 実行可能なレポート
- URL フィルタリング
- ICAP 経由によるサードパーティの DLP 統合

Cisco アンチマルウェア

- リアルタイムのマルウェア スキャン

Cisco Web Security Premium

- Web Security Essentials
- リアルタイムのマルウェア スキャン

高度なマルウェア防御

- 高度なマルウェア防御（AMP）は、アンチマルウェアの検出とブロッキング機能を強化します。ファイル レピュテーション スコアおよびブロック、ファイル サンドボックス機能、およびファイル レトロスペクション機能を備え、脅威を継続的に分析します。

Cognitive Threat Analytics

- CTA は高度な統計モデリングと機械学習を活用して、新たな脅威を独立的に特定し、検出内容から学習して、長期的に適応します。

Cloud Access Security

- シスコと Elastica は、SaaS の可視性、拡張されたきめ細かい制御、およびインテリジェント保護によりセキュリティポリシーを維持しながら、クラウド アプリケーションの利点を活用できるように組織を助けます。

McAfee アンチマルウェア

- McAfee リアルタイム マルウェア スキャンは単一の、アラカルトのライセンスで利用できます。

ソフトウェア ライセンス契約

ソフトウェア ライセンスを購入すると、それぞれについて Cisco エンドユーザ ライセンス契約（EULA）および Cisco E メール & Web セキュリティの補足エンド ユーザ ライセンス契約（SEULA）が提供されます。

ソフトウェア サブスクリプションのサポート

すべての Cisco Web セキュリティのライセンスには、ビジネスに不可欠なアプリケーションを入手可能にして、安全かつ最高のパフォーマンスで運用するために必要なソフトウェア サブスクリプション サポートが含まれています。このサポートでは、購入したソフトウェア サブスクリプションの全期間にわたって以下のサービスを受けることができます。

- ソフトウェア更新およびメジャー アップグレードによって、アプリケーションに最新の機能セットを適用し、最適なパフォーマンスを得る
- Cisco Technical Assistance Center（TAC）にアクセスして、すばやい専門サポートを得る
- 社内の専門知識を構築して拡張し、ビジネスの俊敏性を高めるオンライン ツールを利用する
- 追加的な知識習得とトレーニングの機会を提供するコラボレーション性の高い学習

サービス

表 5 に Cisco Web セキュリティ サービスを示します。

表 5. Cisco Web セキュリティ サービス

シスコ ブランド サービス	Cisco Security Planning and Design：堅牢なセキュリティ ソリューションをすばやく低コストで導入できるようにします。 Cisco Web セキュリティの設定とインストール：アプライアンスのインストール、設定、テストで Web セキュリティのリスクを軽減するために、次を実装します。 • アクセプタブル ユース ポリシーによる制御 • レピュテーションとマルウェア フィルタリング • データ セキュリティ • アプリケーションの可視性と制御 Cisco Security Optimization サービス：セキュリティの脅威、設計の改修、パフォーマンスのチューニング、システム変更など、進化するセキュリティ システムをサポートします。
コラボレーション型のパートナー サービス	Network Device Security Assessment：ネットワーク インフラストラクチャのセキュリティのギャップを特定し、強化したネットワーク環境を維持します。 Smart Care：ネットワークのパフォーマンスを安全に可視化し、そこで得られた情報から実行可能なインテリジェンスを提供します。 その他サービス：シスコ パートナーが計画、設計、導入、最適化のライフサイクルを通じて、幅広い有益なサービスを提供します。
シスコのファイナンス	Cisco Capital® では、ビジネスのニーズに合わせてファイナンス ソリューションをカスタマイズできます。シスコのテクノロジーをすぐに利用し、ビジネス上のメリットをすぐに得ることができます。

SMARTnet サポート サービス

Cisco SMARTnet® サポートを購入して、Cisco WSA で利用することができます。Cisco SMARTnet サポートは、シスコの専門家やセルフサービスのサポート ツールにいつでも直接アクセスしてネットワークの問題をすばやく解決できるほか、ハードウェアの迅速な交換に対応します。詳細については、http://www.cisco.com/jp/go/smartnet/ をご覧ください。

Cisco WSAV の注文:

Cisco WSAV を注文するには、以下を行います。

1. http://www.cisco.com/jp/go/wsa にアクセスします。右にある [Support] の [Software Downloads, Release, and General Information] をクリックします。[Download Software] をクリックし、任意のモデルをクリックして、ダウンロード可能な仮想マシン イメージを確認します。このほか、ダウンロード可能な XML 評価ライセンスもあります。いずれかのイメージと XML 評価ライセンスをダウンロードする必要があります。
2. Cisco.com から、次のドキュメントをダウンロードします。
   a. Sisco セキュリティ仮想アプライアンスのインストール ガイド
   b. AsyncOS® 9.0 のマニュアル
3. Cisco セキュリティ仮想アプライアンスのインストール ガイドの指示に従い、インストールを開始します。コンテンツ セキュリティ仮想アプライアンスの評価は SMARTnet のサポート対象外です。ご注意ください。

保証に関する情報

保証については、Cisco.com の製品保証のページを参照してください。

関連情報

詳細については、http://www.cisco.com/jp/go/wsa/ をご覧ください。シスコのセールス担当者、チャネル パートナー、またはシステム エンジニアとともに、Cisco WSA の動作を評価してください。

お問い合せ先

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

C78-729630-09JA 16.02