CISCO SECURE

Cisco Secure Web Appliance

2024 年 3 月

The bridge to possible

目次

仮想アプライアンス	3
機能と利点	4
製品仕様	5
導入	7
ライセンス	7
サービス	9
SMARTnet サポートサービス	10
保証情報	10
Cisco Capital	10
詳細情報	10
謝辞	11

お客様のネットワークを守るために必要なのは、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です。シスコでは、これらの対策や機能をすべて単一のプラットフォームで実現する、Cisco Secure Web Appliance（旧 Web Security Appliance（WSA））を提供しています。

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、Secure Web Appliance 導入のための多様なオプションも提供しています。Cisco Secure Web Appliance 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、Secure Web Appliance 仮想アプライアンス（SWAV）を利用すると、場所や時間を問わず、Secure Web Appliance を必要に応じて迅速にビジネスに導入できます。

Secure Web Appliance は、Web トラフィックのセキュリティや制御などの進化を続ける課題に企業が対処する際に役立つ、先進的な保護機能を組み合わせた初の Secure Web Gateway です。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、遅延や運用コストを削減します。「Set and forget」テクノロジーでは、初期の自動ポリシー設定を行うと、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に自動的にプッシュ配信され、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 SWAV は、管理者が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 Secure Web Appliance を導入する際のコストを大幅に削減します。Cisco SWAV はソフトウェア版の Secure Web Appliance であり、VMware ESXi、KVM ハイパーバイザ、Microsoft Hyper-V および Cisco Unified Computing System™（Cisco UCS®）サーバー上で動作します。いずれかの Cisco Secure Web Appliance ソフトウェアバンドルを購入すると、Cisco SWAV の無制限ライセンスが付いてきます。

さらに、Cisco Secure Web Appliance または Cisco Secure Email ソフトウェアバンドルのいずれかまたは両方を購入すると、Cisco Content Security Management Appliance Virtual（SMAV）の無制限のライセンスに対する権限も付与されます。

注： ただし、SMA ライセンスは別途購入する必要があります。

Cisco SWAV 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が不要になります。アプライアンスを購入して移送する必要もありません。またデータセンターを複雑化したり、人員を増やしたりせずに、新しいビジネスチャンスに対応することが可能になります。

機能と利点

機能	メリット
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 のセキュリティ情報 • ファイアウォール、IPS、Web、E メールアプライアンスを含む 160 万台の導入済みセキュリティデバイス • 1 億 5000 万台のエンドポイント • 1 日あたり 130 億件の Web 要求 • 世界の企業向け 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が 24 時間 365 日体制で表示されるので、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リングが可能です。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 Secure Web Appliance に適用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。
Secure Web Appliance の使用制御	従来の URL フィルタリングを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 5000 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。このほか、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。
Cisco Advanced Malware Protection	Cisco Advanced Malware Protection（AMP）は、すべての Secure Web Appliance ユーザーが使用できる、追加機能ライセンスです。AMP はマルウェア検出およびブロック、継続的な分析、過去にさかのぼるアラートを実現する、包括的なマルウェア対策ソリューションです。シスコと Sourcefire® テクノロジーによる、広範に及ぶクラウド セキュリティ インテリジェンス ネットワークを利用します。AMP は、Secure Web Appliance に搭載済みのマルウェア検出およびブロック機能を、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、レトロスペクティブ判定アラートで強化します。AMP Threat Grid は、マルウェアサンプルのクラウドへの送信に対してコンプライアンスまたはポリシー制限を設けている組織向けに、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ー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ーは、従来の Secure Web Appliance ソリューションの回避を試み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に動的に追加され、ブロックされます。
Cognitive Threat Analytics	Cognitive Threat Analytics は、ネットワーク内部で動作す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。動作分析と異常検出を使用してマルウェア感染の症状またはデータ侵害を識別し、境界ベースの防御に存在するギャップに対処します。Cognitive Threat Analytics は、Secure Web Appliance 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、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。Secure Web Appliance 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、対象ユーザー、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。

機能	メリット
データ漏洩防止（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、Secure Web Appliance 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。Secure Web Appliance は、Secure Web Appliance 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。
リモートブラウザ分離（RBI）	Secure Web Appliance RBI は、Web トラフィックをユーザーデバイスと脅威から分離することにより、Secure Web Appliance に追加の保護層を提供し、ユーザーがマルウェア感染のリスクなしに危険な Web サイトに安全にアクセスできるようにします。RBI を使用すると、Secure Web Appliance は、エンドポイントや企業ネットワークから切り離されたクラウド内のリモートサロゲートブラウザで Web コンテンツを分離してエンドユーザーに安全に提供し、シームレスなエンド ユーザー エクスペリエンスを提供します。
ローミングユーザー保護	オンプレミスソリューションへとトラフィックをリダイレクトする VPN トンネルを開始し、リモートクライアントに Secure Web Appliance 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、Secure Web Appliance はローミングユーザーを保護します。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。 また、Secure Web Appliance は、Cisco Identity Services Engine（ISE）とも統合されます。この画期的な機能拡張により、要求に応じて、Cisco ISE の機能を Secure Web Appliance のために活用できるようになりました。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、Secure Web Appliance 上でポリシーを作成できるようになります。
中央管理およびレポート	脅威、データ、アプリケーションに関する実用的な情報を受け取ります。Secure Web Appliance では、使いやすい中央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 Advanced Secure Web Appliance Reporting は、Secure Web Appliance と Cisco Umbrella 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お客様に、スケーラブルなレポート機能を提供します。そのため、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できます。

製品仕様

表 1 および 2 では、それぞれ Secure Web Appliance のパフォーマンスとハードウェアの仕様を示します。

表 1. Secure Web Appliance のパフォーマンス仕様

	モデル	ディスク容量	RAID ミラーリング	メモリ	CPU	
大規模企業	S696	12 TB（10x1.2 TB SAS）	対応（RAID 10）	128 GB、DDR4	2 X 3.1	ギガヘルツ（GHz）、16C
中規模オフィス	S396	4.8 TB（4x1.2 TB SAS）	対応（RAID 10）	64 GB、DDR4	1 X 2.9	ギガヘルツ（GHz）、16C
SMB およびブランチ	S196	2.4 TB（2x1.2 TB SAS）	対応（RAID 1）	16 GB、DDR4	1 X 2.3	ギガヘルツ（GHz）、10C

表 2. Secure Web Appliance のハードウェア仕様

ハードウェア プラットフォーム	Cisco S696	Cisco S396	Cisco S196
フォーム ファクタ	 2 RU	 1 RU	 1 RU
寸法	3.4 インチ X 16.9 インチ X 29.5 インチ	1.7 インチ X 16.89 インチ X 29.8 インチ	1.7 インチ X 16.89 インチ X 29.8 インチ
冗長 P/S	対応	対応	対応（アクセサリオプション）
リモートからの電源の再投入	対応	対応	対応
DC 電源オプション	×	×	×
ホットスワップ対応 HD	対応	対応	対応
消費電力	3,262 BTU/時 3,412 BTU/時（光ファイバ）	2,060 BTU/時	1,765 BTU/時
電源モジュール	1050 W	1050 W	1050 W
イーサネット インターフェイス	6ポート 1G 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 1G 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 1G Base-T 銅線ネットワーク インターフェイス（NIC）、RJ-45
ファイバ オプション	対応。個別の SKU、6 ポート 1G Base-SX 光ファイバまたは 10GBASE-SR 光ファイバを発注時に選択（モジュールを含む）：SWA-S696F	×	×
HD サイズ	SAS ドライブ用にホットスワップ可能なアクセスを提供する前面パネルのドライブベイに、10 台の 1.2 TB ハードディスクドライブ（2.5 インチ 12G SAS 10K RPM）を取り付け	SAS ドライブ用にホットスワップ可能なアクセスを提供する前面パネルのドライブベイに、4 台の 1.2 TB ハードディスクドライブ（2.5 インチ 12G SAS 10K RPM）を取り付け	SAS ドライブ用にホットスワップ可能なアクセスを提供する前面パネルのドライブベイに、2 台の 1.2 TB ハードディスクドライブ（2.5 インチ 12G SAS 10K RPM）を取り付け
CPU	3.1 GHz 16c 3200 MHz プロセッサ X 2	2.9 GHz 16c 3200 MHz プロセッサ X 1	2.3 GHz 10c 2666 MHz プロセッサ X 1
RAM	32 GB DDR4-3200 RDIMM X 4	32 GB DDR4-3200 RDIMM X 2	16 GB DDR4-3200 RDIMM X 1

表 3 に Cisco SWAV の仕様を示します。

表 3. Cisco SWAV

モデル	ディスク	メモリ	コア
S100v	250 GB	8 GB	3
S300v	1024 GB	12 GB	5
S600v	2.4 TB	24 GB	12
S1000v	2.4 TB	48 GB	24
サーバー		ハイパーバイザ	
Cisco UCS **Red Hat Enterprise Linux 7.0 Ubuntu 14.04.1 LTS**		ESXi 6.5、6.7、および 7.0 KVM：QEMU 1.5.3 KVM：QEMU 2.0.0 Microsoft Hyper-V	

導入

Cisco Secure Web Appliance 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などの Cisco WCCP 対応デバイスは、Cisco SWA に Web トラフィックを再ルーティングします。

Cisco SWA 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 ユーザー 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 SWAV ライセンスは、すべての Cisco Secure Web Appliance ソフトウェアバンドル（Secure Web Appliance Essentials、Secure Web Appliance Antimalware、および Secure Web Appliance 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の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、期間ベースのサブスクリプション（1 年、3 年、5 年）です。

数量ベースのサブスクリプション ライセンス

Secure Web Appliance のポートフォリオでは、デバイスではなくユーザー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。

Secure Web Appliance ソフトウェアライセンス

Secure Web Appliance のソフトウェアライセンスには、Cisco Secure Web Appliance Essentials、Cisco Secure Web Appliance Advantage、および Cisco Secure Web Appliance Premier の 3 種類があります。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。

Secure Web Appliance 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
- 実用的なレポート
- URL フィルタリング
- ICA 経由によるサードパーティの DLP 統合

Secure Web Appliance Advantage

- Secure Web Appliance Essentials
- リアルタイムのマルウェアスキャニング

Secure Web Appliance Premier

- Secure Web Appliance Advantage
- Cisco Advanced Malware Protection
- Cognitive Threat Analytics
- Threat Grid ファイル分析

Cisco Advanced Malware Protection

高度なマルウェア防御（AMP）は、アンチマルウェアの検出および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 は高度な統計モデルと機械学習を利用して、新たな脅威を個別に特定し、観測結果から学習し、最新の状況に適応します。

McAfee Anti-Malware

McAfee によるリアルタイム マルウェア スキャンは、単一の個別ライセンスとして利用可能です。

ソフトウェアライセンス契約

Cisco 一般条件および Cisco Secure Web Appliance 補足一般条件は、ソフトウェアライセンスを購入するたびに提供されます。

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 Secure Web Appliance 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利用可能にして、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。このサポートを通じて、お客様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、次に示すサービスを利用できます。

- 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 4 に、Cisco Secure Web Appliance サービスの内容を示します。

表 4. Cisco Secure Web 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 Secure Web Appliance 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 Secure Web Appliance 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 • データセキュリティ • レピュテーションとマルウェアフィルタリング • アプリケーションの可視化と制御 Cisco Security Optimization Service：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	ネットワーク デバイス セキュリティ アセスメント：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。 その他のサービス：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今すぐ導入して、ビジネス上のメリットを実感してください。

SMARTnet サポートサービス

Cisco SMARTnet® サポートを購入して、Cisco Secure Web Appliance で利用できます。

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、https://www.cisco.com/go/smartnet [英語] を参照してください。

Cisco SWAV の発注

Cisco SWAV を発注するには、次の手順を実行します。

1. https://www.cisco.com/go/swa [英語] にアクセスします。右側の [サポート（Support）] の下にある [ソフトウェアのダウンロード、リリース、および一般的情報（Software Downloads, Release, and General Information）] をクリックします。[ソフトウェアのダウンロード（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表示します。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.『Cisco Security Virtual Appliance Installation Guide』
   b. AsyncOS® 14.5 のマニュアル
3. シスコ 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 サポートの対象外です。ご注意ください。

保証情報

保証については、Cisco.com の「製品保証」ページ [英語] を参照してください。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 か国あまりの国々では、ハードウェア、ソフトウェア、サービス、およびサードパーティの補助機器を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

詳細情報

詳細については、https://www.cisco.com/jp/go/wsa を参照してください。シスコの販売代理店、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、Secure Web Appliance の動作を評価してください。

謝辞

本製品には、OpenSSL Toolkit（http://www.openssl.org）で使用するために OpenSSL プロジェクトによって開発されたソフトウェアが含まれています。本製品には、Eric Young 氏（eay@cryptsoft.com）によって作成された暗号化ソフトウェアが含まれています。本製品には、Tim Hudson 氏（tjh@cryptsoft.com）によって作成されたソフトウェアが含まれています。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA C78-729630-27 03/24