Cisco ASA 5500 シリーズ CSC-SSM（コンテンツ セキュリティ & コントロール セキュリティ サービス モジュール）

一般情報

Q. Cisco® ASA 5500 シリーズ CSC-SSM（コンテンツ セキュリティ & コントロール セキュリティ サービス モジュール）とは何ですか。

A. Cisco ASA 5500 シリーズ CSC-SSM は、Cisco ASA-5500 シリーズ アプライアンス用のアドオン サービス モジュールです。包括的なアンチウイルス、アンチスパイウェア、ファイル ブロッキング、アンチスパム、アンチフィッシング、URL ブロッキングとフィルタリング、コンテンツ フィルタリングなどの先進的な脅威防御機能およびコンテンツ制御機能をインターネット エッジで提供します。

Q. Cisco ASA 5500 シリーズ CSC-SSM にはどのような利点がありますか。

A. シスコの優れたファイアウォールおよび VPN サービス、トレンドマイクロ社の高性能ゲートウェイ アンチウイルスおよびコンテンツ セキュリティ ソリューションを利用するためには、以前ならシスコとトレンドマイクロ社のそれぞれから、個別の 2 製品を購入する必要がありました。Cisco CSC-SSM を Cisco ASA 5500 シリーズ専用アプライアンスに搭載して使用すると、市場をリードするこれらの製品を組み合わせ、1 つのパッケージで包括的な統合型攻撃防御ソリューションを構成できるため、導入および管理を簡素化できます。

Q. Cisco ASA 5500 シリーズ CSC-SSM の主な機能を教えてください。

A. Cisco ASA 5500 シリーズ CSC-SSM には、次の特徴があります。

- **包括的なマルウェア防御** — トレンドマイクロ社の優れたアンチウイルスおよびアンチスパイウェア テクノロジーが組み込まれています。CSC-SSM により、悪意ある既知のコードがネットワークに侵入したり、ネットワーク内で感染したりすることを阻止できます。これによって、ビジネスクリティカルなアプリケーションおよびサービスの中断を防止し、貴重なキー システムと業務のダウンタイムを回避できるほか、コストのかかる感染後のクリーンアップ プロセスを低減できます。
- **拡張コンテンツ フィルタリング** — URL フィルタリング、コンテンツ フィルタリング、およびアンチフィッシング テクノロジーを統合し、企業と個々の従業員を機密情報の盗難から守るとともに、ネットワーク利用ポリシーの違反によって、コンテンツに関する法的責任が発生する可能性を軽減します。また、企業が Health Insurance Portability and Accountability Act（HIPAA; 医療保険の相互運用性と説明責任に関する法律）、Sarbanes-Oxley（SOX; 米国企業改革法）、個人情報保護法、日本版 SOX 法や内部統制などのネットワーク コンテンツに関する規制に準拠するための手段となります。
- **統合メッセージ セキュリティ** — メール サーバに到達する前に迷惑メールの大部分を削除するアンチスパム テクノロジーを実装しているので、従業員の生産性を向上させ、貴重なネットワーク帯域幅とストレージ リソースの浪費を回避できます。
- **カスタマイズおよびチューニング機能** — 特定の企業ポリシーやネットワーク環境に適合するように、管理者はスパムおよびコンテンツの制御機能をカスタマイズできます。
- **容易な管理と自動アップデート機能** — Adaptive Security Device Manager（ASDM）のインテリジェントなデフォルト設定とわかりやすいインターフェイスにより、初期設定、導入、および継続的な運用が容易になります。スキャニング エンジンやパターン ファイルなど、すべての CSC-SSM コンポーネントが自動アップデートされるため、最小限の管理作業で、ネットワークを常に最新の脅威から保護できます。

Q. どんなモデルがありますか。

A. CSC-SSM-10 と CSC-SSM-20 の 2 つのモデルがあります。どちらのモデルも、Cisco ASA 5510 および 5520 シャーシに対応しています。CSC-SSM-10 では、最大 500 ユーザまでの組

織をサポートします。CSC-SSM-20 では、最大 1,000 ユーザまでの組織をサポートします。両モデルの CSC モジュールは Cisco ASA 5540 プラットフォームにも対応していますが、1,000 ユーザまでしかサポートできないため、併用には適していません。

Q. Cisco ASA 5500 シリーズ CSC-SSM の機能とサービスを教えてください。

A. Cisco ASA 5500 シリーズ CSC-SSM は、アンチウイルス、アンチスパイウェア、およびファイル ブロッキング サービスを提供するデフォルトの機能セット付きで出荷されます。プラス ライセンスにより、アンチスパム、アンチフィッシング、URL ブロッキング/フィルタリング、およびコンテンツ制御などの追加機能を利用できます。これらのオプションの機能ライセンスを利用するには、CSC-SSM ごとに別途料金が必要です。さらに、追加のユーザ ライセンスを購入してインストールすれば、CSC-SSM のユーザ キャパシティを拡張できます。出荷時のデフォルトは、CSC-SSM-10 モデルで 50 ユーザ、CSC-SSM-20 モデルで 500 ユーザです。ユーザ ライセンスのアップグレードは段階に応じて利用でき、CSC-SSM-10 には 100、250、および 500 ユーザ パック、CSC-SSM-20 には 750 および 1,000 ユーザ パックが用意されています。表 1 に、CSC-SSM の標準ライセンスおよびオプション ライセンスの詳細を示します。

表 1 標準機能とオプション機能

CSC-SSM ハードウェア	標準ライセンス	オプション ライセンス	
		ユーザ アップグレード（合計ユーザ）	機能アップグレード
CSC-SSM-10	• 50 ユーザ • アンチウイルス、アンチスパイウェア、ファイル ブロッキング	• 100 ユーザ • 250 ユーザ • 500 ユーザ	• プラス ライセンス — アンチスパム、アンチフィッシング、URL ブロッキング/フィルタリング、およびコンテンツ制御
CSC-SSM-20	• 500 ユーザ • アンチウイルス、アンチスパイウェア、ファイル ブロッキング	• 750 ユーザ • 1,000 ユーザ	• プラス ライセンス — アンチスパム、アンチフィッシング、URL ブロッキング/フィルタリング、およびコンテンツ制御

Q. Cisco ASA 5500 シリーズ CSC-SSM はどんな場所に導入できますか。

A. Cisco ASA 5500 シリーズ CSC-SSM およびアプライアンスは、インターネット接続ポイントなど、組織間または外部ネットワーク間の境界に導入する目的で設計されています。これらのアプライアンスをインターネット エッジに導入することで、CSC-SSM がユーザとインターネットの中間に配置され、必要に応じて管理者が選択したトラフィックを CSC-SSM を使ってスキャンすることができます。

Q. 「ユーザ」の定義を教えてください。

A. サイジングの観点から、24 時間を 1 つの単位と考え、セキュリティが最低レベルのインターフェイスを除いた、いずれかのインターフェイスから認識可能な一意の IP アドレスがそれぞれ 1 ユーザとしてカウントされます。一般的に言うと、これは「外部」インターフェイス（インターフェイスのセキュリティ レベルによって決定）以外のインターフェイスで認識可能な、すべての IP アドレスを指します。

Q. Cisco ASA 5500 シリーズ CSC-SSM で提供されるアンチウイルス防御機能には、どんな種類がありますか。

A. Cisco ASA 5500 シリーズ CSC-SSM では、ウイルス、トロイの木馬、悪意あるコード、その他のマルウェアに対する防御機能からなる、ファイルベースのアンチウイルス防御機能を提供します。CSC-SSM は、ファイルやパケットが ASA 5500 アプライアンスを通過する際に、それらを検査する透過プロキシとして動作します。これによって、悪意あるコンテンツを阻止して、攻撃対象のシステムでの被害を未然に防ぐことができます。また、こうした機能の一環として、CSC-SSM では、疑わしいファイルやコンテンツの削除や、実行したアクションとその理由についてのレポート機能も備えています。

Q. アンチウイルス テクノロジーでは圧縮ファイルはスキャンされますか。

A. はい。圧縮ファイルは解凍され、コンテンツをスキャンしたあとに再圧縮されるため、複数の階層を持つ圧縮ファイルをスキャンすることができます。

Q. アンチウイルス シグニチャ リストはどのぐらいの頻度でアップデートされますか。

A. Cisco ASA 5500 シリーズ CSC-SSM 用のパターン ファイルの定期アップデートは、トレンドマイクロ社の TrendLabsSM から、毎週 1 つ以上リリースされます。また、新たに感染力の強い脅威が出現した場合は、より短いサイクルで緊急対策用の公認アップデートを提供します。

Q. Cisco ASA 5500 シリーズ CSC-SSM は、ICSA やその他の認定を受けていますか。

A. はい。Cisco ASA 5500 シリーズ CSC-SSM は、高い評価を得ているトレンドマイクロ社のインターネット ゲートウェイ テクノロジーに基づいています。このテクノロジーは、ICSA の Gateway Antivirus 認定、West Coast Lab のアンチスパイウェアを対象とした Checkmark 認定、Veritest のアンチスパム認定をはじめ、多くの業界認定を取得しています。CSC-SSM 自体は現在、ICSA の評価中です。

Q. Cisco ASA 5500 シリーズ CSC-SSM の管理方法を教えてください。

A. Cisco ASA 5500 シリーズ CSC-SSM はデフォルト設定済みの状態で出荷され、ほとんどの構成に対応しています。セットアップ、管理、モニタリングは Cisco ASDM から実行します。 Cisco ASDM のセットアップ ウィザードを使って CSC-SSM およびセキュリティ ポリシー ルール テーブルを起動し、管理者はこのテーブルから CSC-SSM でスキャンすべき対象トラフィックを指定することができます。

Q. Cisco ASA 5500 シリーズ CSC-SSM を複数利用する場合の管理方法を教えてください。

A. 近々リリース予定のトレンドマイクロ社の Control Manager（TMCM）を使用すると、複数の CSC-SSM ユニットを一元管理できます。TMCM は、トレンドマイクロ社から提供される有料オプションです。TMCM では、組織内の複数の CSC-SSM モジュール、およびその他のトレンドマイクロ社製品を一元管理できます。これによって、複数の CSC-SSM およびトレンドマイクロ社製品で構成される大規模組織で、あらゆるアンチウイルスおよびその他の関連機能とテクノロジーを管理するための、統合されたワンストップ管理機能が実現されます。

Q. Cisco ASA 5500 シリーズ CSC-SSM でブロックできる攻撃には、どんな種類がありますか。

A. Cisco ASA 5500 シリーズ CSC-SSM では HTTP、FTP（ファイル転送プロトコル）、SMTP（シンプル メール転送プロトコル）、および POP3 プロトコルを使用して、不正なコンテンツやマルウェアを含むファイルベースのウイルス、スパイウェア、Directory Harvest Attack（DHA）、スパム、およびフィッシングを検出し、ネットワークへの侵入をブロックします。マルウェアがデスクトップやサーバ システムに到達するのを阻止することで、攻撃の開始は未然に食い止められます。

Q. Cisco ASA 5500 シリーズ CSC-SSM では、インターネット ワームを阻止できますか。

A. いいえ。Cisco ASA 5500 シリーズを使用してインターネット ワームの被害を軽減するには、サーバなどのクリティカルな資産を保護するために設計された Advanced Inspection and Prevention Security Services Module（AIP-SSM）と、新しく発生したワームの脅威に迅速に防御策を講じるためのオプションである Cisco ICS（Incident Control Server）製品を購入する必要があります。

Q. Cisco ASA 5500 シリーズ CSC-SSM では、新しい脆弱性にすばやく対処するため、どのような対策がとられていますか。

A. Cisco ASA 5500 シリーズ CSC-SSM では、トレンドマイクロ社の TrendLabs による支援を受けて、24 時間体制でモジュールに対する最新の防御機能を維持しています。TrendLabs は、ウイルス、スパイウェア、およびスパムの専門家で構成された、業界最大級のチームです。CSC-SSM では、パターン ファイルの自動アップデートが定期的に実行されます。

Q. Cisco ASA 5500 シリーズ CSC-SSM によって、正規のトラフィックがブロックされることはありませんか。

A. 設定が適切であれば、Cisco ASA 5500 シリーズ CSC-SSM によって正規のインターネット トラフィックが阻止されることはほとんどありません。シスコでは、各環境でのニーズに応じてモジュールをセットアップできるよう、ユーザによる詳細な設定オプションを用意しています。

Q. 何らかの理由でモジュールに障害が発生した場合はどうなりますか。

A. CSC-SSM に障害が発生した場合、Cisco ASA 5500 シリーズ アプライアンスでは、トラフィックを拒否するか、または未検査のトラフィックを許可するように設定できます。Cisco ASA では、CSC-SSM のフェールオーバーもサポートされます。アプライアンスがフェールオーバー グループに属している場合は、CSC-SSM に障害が発生すると、ペアのスタンバイ ユニットへフェールオーバーが開始されます。フェールオーバーが実行された場合、CSC-SSM を経由する確立済みのアクティブなフローは、再度確立する必要があります。

サポートおよびその他の情報

Q. テクニカル サポート、アップデート、および返品方法について教えてください。

A. テクニカル サポートは、Cisco Technical Assistance Center（TAC）またはシスコの認定パートナーから提供されます。CSC-SSM のアプリケーション ソフトウェアに関する問題については、トレンドマイクロ社が TAC を通じてサポートします。パターン ファイルとスキャン エンジンのアップデートは、トレンドマイクロ社のアップデート サーバから直接、透過的に提供されます。返品は、その他すべてのシスコ製品の場合と同様に、モジュールを購入した代理店で取り扱います。

Q. Cisco ASA 5500 シリーズ CSC-SSM の購入方法を教えてください。

A. シスコ製品の購入方法の詳細は「購入案内」を参照するか、シスコ認定の販売代理店またはシスコの販売担当者にお問合せください。

Q. サポート契約の方法を教えてください。また、Cisco ASA 5500 シリーズ CSC-SSM にはどのようなサポート オプションがありますか。

A. サービス プログラムは、ハードウェア サポート、ソフトウェア サポート、およびコンテンツ登録状況から構成されます。表 2 に、Cisco ASA 5500 シリーズ CSC-SSM 製品に提供されているサービスおよびサポート契約を示します。モジュールの購入価格には、トレンドマイクロ社による最初の 1 年分のアップデート サービスが含まれています。ライセンス登録後 2 年目以降は、トレンドマイクロ社と直接、年間料金を支払い、ソフトウェアとアップデート サービスの契約更新手続きを行ってください。シスコは、CSC-SSM のテクニカル サポートとハードウェアのメンテナンスをカバーする SMARTnet メンテナンス プログラムを提供しています（別途年間料金が必要です）。Cisco ASA 5500 シリーズ CSC-SSM ソリューションの保護機能を最大限に活用し、最適なパフォーマンスを得るには、トレンドマイクロ社のソフトウェアおよびアップデート サービスと Cisco SMARTnet サービスの両方が必要です。

表 2 利用可能なサポート サービス

提供可能なサポート	Cisco SMARTnet® (SNT) サービス	トレンドマイクロ アップデート サービス
Cisco ASA 5500 シリーズ アプライアンス シャーシ サポート		
Cisco.com への登録	○	—
TAC テクニカル サポート（年中無休）	○	—
オペレーティング システム ソフトウェア リリース（メンテナンス、メジャー、マイナー）	○	—
ハードウェア交換オプション	○	—
Cisco ASA 5500 シリーズ CSC-SSM サポート		
Cisco.com への登録	○	—
TAC テクニカル サポート（年中無休）	○	—
オペレーティング システム ソフトウェア リリース（メンテナンス、メジャー、マイナー）	○	—
パターン ファイル、スキャン エンジン、シグニチャ アップデート	—	○
ハードウェア交換オプション	○	—

Q. Cisco SMARTnet とトレンドマイクロアップデート サービスは両方とも購入する必要がありますか。

A. はい。Cisco ASA 5500 シリーズ CSC-SSM を常に最新の状態に保ち、最適なパフォーマンスで動作させるには、両方のサービスが必要です。トレンドマイクロ社のソフトウェアおよび最初の 1 年分のアップデート サービスは、製品の購入価格に含まれています。

Q. Cisco ASA 5500 シリーズ CSC-SSM では検出できないマルウェア（または疑わしいプログラム）がある場合、疑わしいデータの分析を依頼する方法を教えてください。また、分析の依頼から回答までの進捗状況を（TAC ケースの処理段階に応じて）追跡する追跡メカニズムはありますか。

A. 次の URL から専用ページにアクセスし、マルウェアと思われるプログラムの分析を依頼してください。分析の進捗状況は、随時電子メールで通知されます。
http://subwiz.trendmicro.com/SubWiz/Default.asp

Q. Cisco ASA 5500 シリーズ CSC-SSM を導入すれば、デスクトップ パソコンやノート パソコンでウイルス対策を行ったり、Cisco Security Agent を使ったりする必要はありませんか。

A. いいえ。Cisco ASA 5500 シリーズ CSC-SSM は、侵入防御やデスクトップ セキュリティを含むマルチレイヤ セキュリティ ストラテジで重要な役割を果たします。さらにトレンドマイクロ社の OfficeScan や Cisco Security Agent といったデスクトップ パソコンおよびラップトップ パソコン用のセキュリティ製品を使用することで、脅威に対して多重的な防御を行うことができます。これによって、リムーバブル メディア（フラッシュ メモリ、光ディスク ドライブなど）から直接コンピュータに脅威が侵入するのを防ぎ、企業ネットワーク外の安全性の低い環境で使用する場合もコンピュータが保護されます。また、OfficeScan と Cisco Security Agent では、シスコの Network Admission Control（NAC）プログラムがサポートされます。NAC は、エンドポイントから脅威がネットワークに侵入するのを阻止するために不可欠な要素です。

Q. 以前に購入した Cisco ASA 5500 シリーズ AIP-SSM カードを使用して、CSC ソフトウェア アプリケーションを稼働することはできますか。

A. いいえ。SSM ハードウェアには互換性がなく、シスコはハードウェアの交換をサポートしていません。SSM ハードウェアでは、AIP アプリケーションと CSC アプリケーションの両方を同時に実行できません。

Q. ファイアウォールや VPN など、Cisco ASA シリーズ アプライアンスのその他の機能を CSC-SSM 機能と同時に使用することはできますか。

A. はい。Cisco ASA 5500 シリーズ CSC-SSM は、Cisco ASA プラットフォームに統合可能なサービスの 1 つです。その他のすべての機能を CSC-SSM と並行して利用できるため、防御機能と制御機能を最大化し、セキュアな通信を実現できます。

Q. ユーザ ライセンスのアップグレード方法を教えてください。

A. 適切なユーザ アップグレード ライセンス（50 ユーザから 100 ユーザへのアップグレードなど）を購入してから、http://www.cisco.com/go/license にアクセスしてください。このページでは、ユーザの連絡先情報および PAK 番号（発注の完了後に発送）と、SSM のシリアル番号を入力する必要があります。次回アップデート時に、トレンドマイクロ社のサーバからアップデート通知を受信すると、CSC-SSM 上のソフトウェアでは自動的かつ透過的に新しいユーザ数が有効となります。

Q. Cisco ASA 5500 シリーズ CSC-SSM と、Websense 社製品の機能にはどのような違いがありますか。

A. CSC-SSM と Websense 社の URL およびコンテンツ フィルタリング製品の機能は似ていますが、中堅・中小企業での使用には CSC-SSM ソリューションの方が適しています。Websense 社は、エンタープライズ マーケット向けウェブ フィルタリングおよびセキュリティ ソフトウェアの世界的なトップ企業で、IDC の調査によると、市場シェアの 30% 近くを占有しています。CSC-SSM URL フィルタリング ソリューションは、オールインワン型のコンテンツ セキュリティ ソリューションの一部として、中堅・中小企業向けに基本的なポリシー管理機能およびコンテンツ フィルタリング機能を提供します。Websense 社製品はエンタープライズ クラスのお客様を対象に、ウェブ フィルタリングとセキュリティを実現する、より堅牢で精巧なアプローチを提供するスタンドアロン ソリューションです。Websense 社とシスコとの強固なパートナーシップによって、Websense 社のウェブ フィルタリングおよびセキュリティ ソリューションと、すべての Cisco ASA 5500 シリーズ アプライアンスはシームレスにオフボックス統合できます。このオフボックス統合では、共同開発による専用インターフェイスを活用することで、優れた性能と最大限の機能のサポートを実現します。

Websense 社製品が提供する完成された堅牢なウェブ フィルタリングおよびセキュリティ ソリューションによって、Cisco ASA アプライアンスおよび CSC-SSM ソリューションをさらに強化することができます。

お問い合わせ先

シスコシステムズ株式会社
〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館
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

07.04