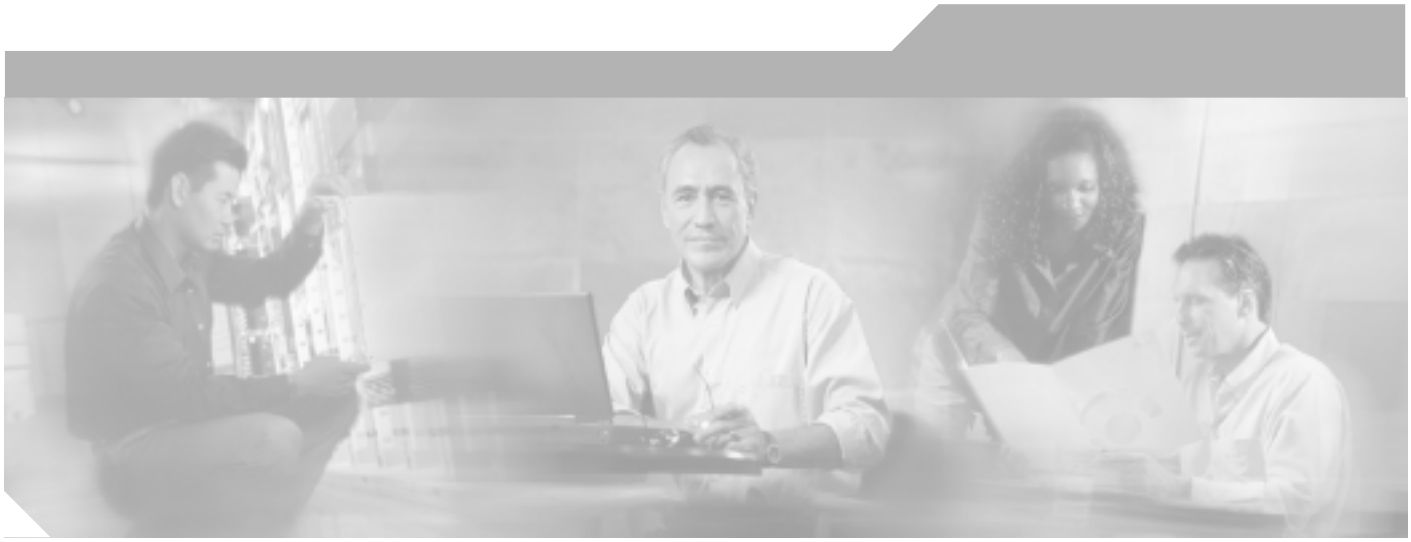


Cisco Content Security and Control SSM アドミニストレータ ガイド

Version 6.0

Text Part Number: OL-8628-01-J

CONTENTS

このマニュアルについて

ここでは、『*Cisco Content Security and Control SSM アドミニストレータ ガイド*』の概要を示します。次の項について説明します。

マニュアルの目的

このマニュアルは、Trend Micro InterScan for Cisco CSC SSM を設定する際に役立ちます。Trend Micro InterScan for Cisco CSC SSM の GUI には、ASDM（Web ベースの GUI アプリケーション）を使用してアクセスします。ASDM には、CSC SSM の初期設定用のコンフィギュレーション ウィザードと、Cisco ASA 5500 シリーズ セキュリティ アプライアンスを調整して CSC SSM を最大限に利用するために役立つオンライン ヘルプが用意されています。詳細については、http://www.cisco.com/univercd/cc/td/doc/product/netsec/secmgmt/asdm/index.htm を参照してください。

このマニュアルは、Trend Micro InterScan for Cisco CSC SSM に使用できます。CSC SSM は Cisco ASA 5500 シリーズ セキュリティ アプライアンス（ASA 5510、ASA 5520、および ASA 5540）に含まれています。このマニュアルを通じて、「セキュリティ アプライアンス」という語は、特に指定がなければ、一般的にサポートされているすべてのモデルに適用されます。

対象読者

このマニュアルは、次のタスクを実行するネットワーク管理者を対象としています。

- コンテンツ セキュリティ ポリシーの管理
- セキュリティ アプライアンスおよびネットワーク セキュリティ アプリケーションのインストールと設定
- コンテンツ セキュリティの実装に伴う問題のトラブルシューティング

関連マニュアル

詳細については、次のマニュアルを参照してください。

- *Cisco ASDM Release Notes*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco Security Appliance Logging Configuration and System Log Messages*

マニュアルの構成

このマニュアルは、表 1 に示す章と付録で構成されています。

表 1　マニュアルの構成

章 / 付録	定義
第 1 章「Content Security and Control SSM の概要」	Trend Micro InterScan for Cisco CSC SSM の概要について
第 2 章「初期セットアップの確認」	Trend Micro InterScan for Cisco CSC SSM が正しく動作していることを確認する方法について
第 3 章「メール トラフィック（SMTP および POP3）の設定」	SMTP および POP3 のメール トラフィックをスキャンするための Trend Micro InterScan for Cisco CSC SSM の設定について
第 4 章「Web（HTTP）トラフィックおよびファイル転送（FTP）トラフィックの設定」	HTTP および FTP のトラフィックをスキャンするための Trend Micro InterScan for Cisco CSC SSM の設定について
第 5 章「アップデートおよびログ クエリーの管理」	アップデートおよびログ クエリーの管理方法について
第 6 章「Trend Micro InterScan for Cisco CSC SSM の管理」	Trend Micro InterScan for Cisco CSC SSM の管理タスクについて
第 7 章「コンテンツ セキュリティのモニタリング」	CSC SSM で利用可能なモニタリング機能について
第 8 章「Trend Micro InterScan for Cisco CSC SSM のトラブルシューティング」	Trend Micro InterScan for Cisco CSC SSM で発生した問題のトラブルシューティングについて
付録 A「コマンドラインを通じたインストールおよび設定」	SSM CLI を使用した Trend Micro InterScan for Cisco CSC SSM のインストールおよび初期設定について

表記法

コマンドの説明では、次の表記法を使用しています。

- 選択する必要があるものは、中カッコ ({ }) で囲んで示しています。
- オプションの要素は、大カッコ ([ ]) で囲んで示しています。
- どちらか選択する必要がある要素は、パイプ（|）で区切って示しています。
- 記載されているとおりに入力するコマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。

例では、次の表記法を使用しています。

- 画面に表示される情報およびコマンドラインは、`screen` フォントで示しています。
- ユーザが入力する情報は、太字の **`screen`** フォントで示しています。
- ユーザが値を指定する変数は、イタリック体の *`screen`* フォントで示しています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参考資料などを紹介しています。

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com/techsupport

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

Product Documentation DVD（英語版）

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Product Documentation DVD パッケージでご利用いただけます。Product Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納した、包括的なライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関する複数のバージョンのマニュアルにアクセスし、技術情報を HTML で参照できます。また、この DVD を使用すると、シスコの Web サイトで参照できるのと同じマニュアルに、インターネットに接続せずにアクセスできます。一部の製品については、PDF 版のマニュアルもご利用いただけます。

Product Documentation DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザ（Cisco Direct Customers）の場合、Ordering ツールまたは Cisco Marketplace から Cisco Documentation DVD（Product Number DOC-DOCDVD=）を発注できます。

http://www.cisco.com/go/marketplace/

マニュアルの発注方法（英語版）

2005 年 6 月 30 日以降、Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store からシスコ製品の英文マニュアルを発注できるようになっています。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/

Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告および注意事項の最新のリストには、次の URL からアクセスできます。

http://www.cisco.com/go/psirt

勧告および注意事項がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードにアクセスしてください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合：security-alert@cisco.com（英語のみ）

  緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと見なされます。
- 緊急でない場合：psirt@cisco.com（英語のみ）

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302（英語のみ）
- 1 408 525-6532（英語のみ）

ヒント シスコに機密情報をお送りいただく際には、PGP（Pretty Good Privacy）または互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.*x* から 8.*x* と互換性のある暗号化情報に対応しています。
無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/techsupport

Cisco Technical Support & Documentation Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） Web または電話でサービス リクエストを発行する前に、Cisco Product Identification（CPI）ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support & Documentation Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果には、シリアル番号のラベルの場所がハイライトされた製品の説明図が表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『Packet』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『Packet』は、米国版『Packet』と日本版のオリジナル記事で構成されています。日本語版『Packet』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet/

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『iQ Magazine』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

  デジタル版には、次の URL からアクセスできます。

  http://ciscoiq.texterity.com/ciscoiq/sample/

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『Internet Protocol Journal』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコシステムズが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共有できます。次の URL にアクセスしてディスカッションに参加してください。

  http://www.cisco.com/discuss/networking

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

Content Security and Control SSM の概要

この章では、Content Security and Control Security Services Module （CSC SSM）の概要について説明します。この章は、次の項で構成されています。

概要

Trend Micro InterScan for Cisco CSC SSM （Content Security and Control Security Services Module）は、ネットワーク用統合アンチウイルスおよびスパイウェア管理ソリューションです。このマニュアルでは、Cisco アプライアンスに常駐して次の機能を実行する CSC SSM を管理する際の考え方について説明します。

- SMTP、POP3、HTTP、FTP を使用するネットワーク トラフィックに対するウイルス、ワーム、トロイの木馬、その他の脅威を検出し、適切な処置を取ります

（注）　HTTPS など他のプロトコルを使用するトラフィックを CSC SSM はスキャンしません。

- 圧縮ファイルまたは指定されたパラメータを超える非常に大きなファイルをブロックします
- スキャンによってスパイウェア、アドウェア、および他のタイプのグレーウェアを見つけ、削除します

CSC SSM ソフトウェアの Base ライセンスを持つユーザはすべて、上記の機能を利用できます。Base ライセンスに加えて CSC SSM ライセンスの Plus レベルを購入した場合は、次の機能も利用できます。

- SMTP および POP3 トラフィックでスパムを減らし、フィッシング詐欺から保護します
- キーワードやフレーズを含む電子メール トラフィックを、許可または禁止するようにできるコンテンツ フィルタをセットアップします
- 社員にアクセスさせたくない URL または隠された目的や悪意の目的がある URL をブロックします
- 成人向けコンテンツ、ゲーム、チャット / インスタント メッセージ、ギャンブルのサイトなどを許可または禁止する定義済みのカテゴリに従って、URL トラフィックをフィルタリングします

Base ライセンスおよび Plus ライセンスの詳細については、P.1-12 の「ライセンス」を参照してください。

トラフィックのスキャンを開始するには、1 つ以上のサービス ポリシー規則を ASDM で作成し、スキャンするトラフィックを CSC SSM に送信する必要があります。詳細については、ASDM のオンライン ヘルプを参照してください。

Trend Micro InterScan for Cisco CSC SSM を使用すると、ウイルスからの保護、スパイウェアのブロック、スパム検出、コンテンツ フィルタリング用のアプリケーションを別々にインストールする必要がありません。これらの機能すべてが 1 つのパッケージで利用できます。Trend Micro InterScan for Cisco CSC SSM では、主要なトラフィック プロトコル、たとえば SMTP、HTTP、FTP、および POP3 トラフィックを保護し、社員が個人の電子メール アカウントから知らないうちにウイルスを取り込むのを防ぐことができます。また、このアプリケーションは保守管理が容易です。インストールし、初期設定を行った後は、このマニュアルを再度参照する必要はありません。

アプライアンスの詳細については、シスコのマニュアルを参照してください。セットアップ ウィザードでは、インストール プロセスを順を追って案内します。

このマニュアルでは、Trend Micro InterScan for Cisco CSC SSM ユーザ インターフェイスについて説明し、インストール後に微調整を行う場合の、コンフィギュレーション設定について説明します。このマニュアルには、ユーザ インターフェイスのウィンドウのフィールドごとの説明は含まれていません。固有のウィンドウのフィールドの説明については、CSC SSM のオンライン ヘルプを参照してください。

機能および利点

Trend Micro InterScan for Cisco CSC SSM は、ネットワークへの脅威に対処するのに役立ちます。表 1-1 に、機能および利点の概要を示します。

表 1-1　機能および利点

機能
スキャンによってウイルスが含まれているトラフィックを見つけ、感染したメッセージやファイルを管理します
スキャンによって下限しきい値レベルから上限しきい値レベルでスパムを見つけ、スパムの処理方法を決めることができます
攻撃的なコンテンツや不適切なコンテンツをフィルタリングします
ネットワークに被害を及ぼす可能性のあるファイル タイプの着信をブロックします
メッセージのサイズに制限を設定して、DoS 攻撃（サービス拒絶攻撃）を防ぎます
ファイルおよび URL のブロッキングについて、承認する送信者およびブロックする送信者を指定する機能を提供します
URL へのアクセスをカテゴリによってフィルタリングします
企業ポリシーによって禁止されている URL サイトや FTP サイトへの接続をブロックします
利点
シスコの強力なファイアウォール保護と組み合せることにより、Trend Micro InterScan for Cisco CSC SSM は、脅威、スパム、および好ましくないコンテンツからネットワークを保護します
ユーザ フレンドリなセットアップ プログラムにより、インストールが容易に行えます
アンチウイルス、スパイウェア / グレーウェア検出、ファイル ブロッキング、およびネットワーク トラフィックのセキュリティ リスクに対するその他の保護が、ASDM と統合されます
インストール後にスキャン、アンチスパム、およびフィルタリングの諸機能のコンフィギュレーションを微調整することができます
Trend Micro から新しいバージョンが入手できるようになったときは、ウイルス パターン ファイル、スキャン エンジン、およびスパム検出の各コンポーネントを自動的にアップデートするように設定できます
電子メール通知および syslog 通知を送信して、ユーザがアクティビティについての情報を常に得られるようにします
30 日後に自動的に消去されるログ ファイルを提供します
タスクの手順を案内するオンライン ヘルプといった、ユーザ フレンドリなコンソールが用意されています
ライセンスの期限満了が近づくと自動的に通知します

利用可能なマニュアル

この製品のマニュアルは、ファイアウォールの管理およびネットワークの管理の基本的な概念を理解しているシステム管理者を対象としています。また、ネットワークのセキュリティ アプライアンスを管理する特権を持っていることを前提としています。

先に進む前に、『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』も読んでおくことをお勧めします。この *Quick Start Guide* には、購入したアプライアンスにまだ SSM がインストールされていない場合に CSC SSM をインストールするためのマニュアルが含まれています。

Trend Micro InterScan for Cisco CSC SSM で利用可能なマニュアルは次のとおりです。

- 本マニュアル：『*Cisco Content Security and Control SSM アドミニストレータ ガイド*』
- オンライン ヘルプ：次の 2 種類のオンライン ヘルプが利用できます。
  - 状況依存スクリーン ヘルプ。1 つのウィンドウでタスクを実行する方法を説明します。
  - 一般ヘルプ。複数のウィンドウでアクションが必要なタスク、またはタスクの実行に必要な周辺知識について説明します。
- Knowledge Base：問題解決およびトラブルシューティングの情報のオンライン データベース。Knowledge Base には、既知の製品問題に関する最新情報があります。Knowledge Base を利用するには、次の URL にアクセスしてください。

  kb.trendmicro.com/solutions/solutionSearch.asp

重要な用語

マニュアルおよびオンライン ヘルプで使用されている専門用語の中には、あまりなじみのないものや、予想とは異なる方法で使用されているものがあります。専門用語の定義は、用語集に説明されています。

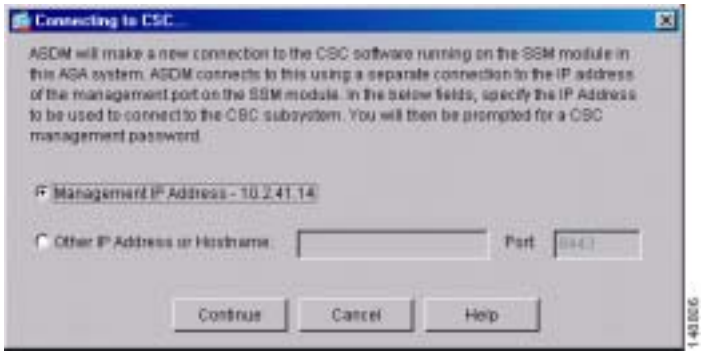
ASDM Content Security タブの概要

ASDM Home ページには、Content Security と呼ばれるタブがあります。メイン ASA システム ホームページはデフォルト表示です。Content Security タブをクリックすると、CSC SSM アクティビティの要約が表示されます。

CSC SSM へ接続するよう求められます。ダイアログボックスが表示され、ASDM に認識されている IP アドレスまたは代替アドレスを選択することができます。代替アドレスは、NAT デバイスを介して ASDM にアクセスする場合に使用される場合があります。NAT デバイスでは、コンピュータに表示される SSM の IP アドレスは、CSC SSM 管理ポートの実際の IP アドレスと異なります。

ダイアログボックスは次のように表示されます。

図 1-1　CSC SSM への接続のプロンプト



ローカル ホストまたは代替ホストを選択した後、**Continue** をクリックします。次に、インストール中に設定した CSC SSM のパスワードを入力するように求められます。パスワードを入力し、**OK** をクリックします。

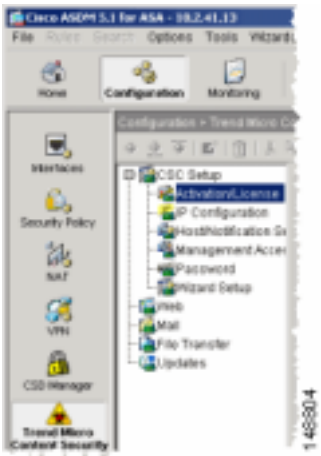
Content Security タブが表示されます。詳細については、P.7-2 の「Content Security タブの機能」を参照してください。

Content Security の設定

ASDM コンソールで、**Configuration > Trend Micro Content Security** をクリックしてコンフィギュレーション オプションを表示します。オプションは次のとおりです。

- CSC Setup：CSC SSM をインストールおよび設定するセットアップ ウィザードを起動します
- Web：Web スキャン、ファイル ブロッキング、URL フィルタリング、および URL ブロッキングを設定します
- Mail：着信および発信する SMTP メールと POP3 メールのスキャン、コンテンツ フィルタリング、およびスパム防御を設定します
- File Transfer：ファイル スキャンおよびファイル ブロッキングを設定します
- Updates：コンテンツ セキュリティ スキャン コンポーネント（ウイルス パターン ファイル、スキャン エンジンなど）のアップデートのスケジュールを設定します

図 1-2　ASDM のコンフィギュレーション オプション



セットアップ オプションは、『*Cisco ASA5500 Adaptive Security Appliance Getting Started Guide*』に説明があります。これらの各オプションの詳細については、オンライン ヘルプも参照してください。

Web、Mail、File Transfer、および Updates のオプションは、この『*アドミニストレータ ガイド*』の別の章でより詳しく説明されています。

- Web コンフィギュレーション：第 4 章「Web（HTTP）トラフィックおよびファイル転送（FTP）トラフィックの設定」を参照してください。
- Mail コンフィギュレーション：第 3 章「メール トラフィック（SMTP および POP3）の設定」を参照してください。
- File Transfer コンフィギュレーション：第 4 章「Web（HTTP）トラフィックおよびファイル転送（FTP）トラフィックの設定」を参照してください。
- Updates：第 5 章「アップデートおよびログ クエリーの管理」を参照してください。

CSC SSM コンソールの概要

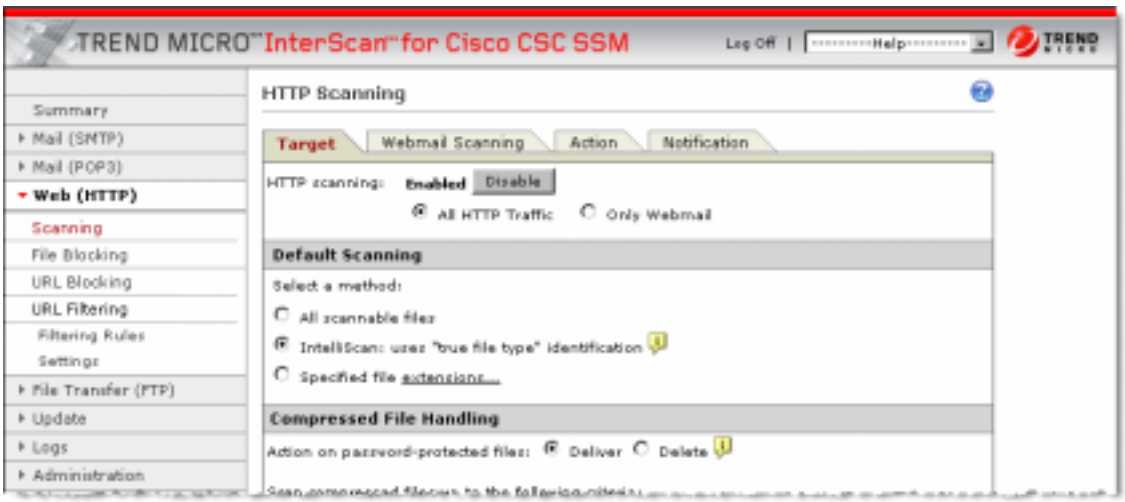
Trend Micro InterScan for Cisco CSC SSM を正常にインストールし、CSC SSM にトラフィックを送信するように ASA を設定すると、ウイルス スキャンおよび検出機能がアクティブになり、ネットワーク トラフィックはデフォルト設定を使用してスキャンされます。スパイウェア / グレーウェア検出などの追加機能は、デフォルトではイネーブルになっていません。CSC SSM インターフェイスで設定できます。

CSC SSM インターフェイスに入るには、**Configuration > Trend Micro Content Security** をクリックします。Configuration メニュー（上記の図 1-2 を参照）で、タスクを選択します。たとえば、Web スキャンを設定するには、**Configuration > Trend Micro Content Security** メニューで **Web** を選択します。Configuration ウィンドウの右側（上には示されていません）には、目的のタスクを実行するためのリンクがあります。たとえば、Configure Web Scanning リンクをクリックすると、CSC SSM インターフェイスの **HTTP Scanning** 画面が表示され、Web スキャン設定を行うことができます。

CSC SSM インターフェイスに初めてログインすると、ASDM によってセキュリティ証明書が表示され、続いて **Connecting to CSC < リンク名 >** 画面が表示されます。CSC SSM インターフェイスを終了した後 ASDM からログアウトしないで戻った場合は、セキュリティ証明書のみが表示されます。

CSC SSM インターフェイスでは、ブラウザ ウィンドウが表示されます。Trend Micro InterScan for Cisco CSC SSM コンソールのデフォルト表示は状況依存で、選択したリンクによって決まります。次に例を示します。

図 1-3　Configure Web Scanning リンクをクリックした場合に表示される HTTP Scanning ウィンドウ



ログオフするには、図 1-3 に示すように画面ヘッダーに表示されている **Log Off** をクリックします。次にブラウザ ウィンドウを閉じます。

ナビゲーション パネル

Trend Micro CSC SSM コンソールの左ペインはメイン メニューで、ナビゲーション ペインの役割も果たします。ナビゲーション ペインの選択項目をクリックすると、対応するウィンドウが開きます。選択項目は、矢印が右を向いているときは縮小されており、矢印が下を向いているときは展開されています。ナビゲーション ペインで選択項目をクリックするまで、対応するペインはリフレッシュされません。

図 1-4　Trend Micro CSC SSM Console のナビゲーション ペイン

パス名 **Mail (SMTP) > Scanning > Incoming > Action** という表現は、次のような意味を表しています。

- ナビゲーション ペインの主選択は Mail （SMTP）です
- 第 2 の選択は Scanning です
- 第 3 の選択は Incoming です
- SMTP Incoming Message Scan 画面の選択されたタブは Action タブです

タブの動作

CSC SSM コンソールの右側に選択を行うための対話型の画面が表示されます。ユーザ インターフェイスの大部分のウィンドウには複数のビューがあります。たとえば、SMTP Incoming Message Scan ウィンドウには、Target、Action、および Notification という 3 つのビューがあります。ビューの切り替えは、表示する情報に該当するタブをクリックして行います。アクティブなタブは、名前が赤で表示され、アクティブでないタブは、黒で表示されます。

通常、これらのタブは関連しており、総合的に動作します。たとえば、次の図では、着信 SMTP トラフィックのウイルス スキャンを設定するために、3 つのタブすべてが必要です。

図 1-5　総合的に動作するタブ

- **Target**：アクティビティの対象となる範囲を定義することができます
- **Action**：トリガー イベントが発生したときに実行するアクション（たとえば無害化または削除）を定義することができます
- **Notification**：通知メッセージを作成し、イベントおよびアクションの通知相手を定義することができます

上記のような関連するタブでは、一度 **Save** をクリックすると、3 つのタブすべてに対して行った作業が保存されます。

Save ボタン

Save ボタンは、見れば保存する必要があるかどうかがわかります。**Save** ボタンはウィンドウが最初に開いたときには使用できません。ウィンドウでタスクを実行すると、**Save** ボタンの文字がグレーから黒に変わります。黒に変化したボタンは、実行した作業を有効にするには **Save** をクリックして保存する必要があることを示します。

デフォルト値

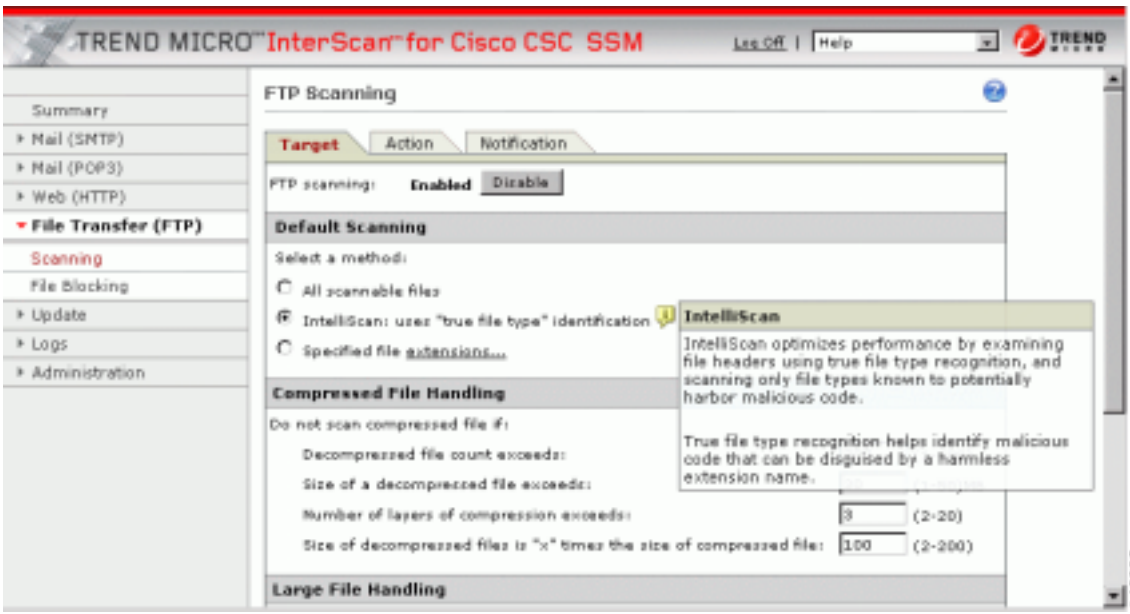
Trend Micro for Cisco CSC SSM ユーザ インターフェイスの多くのウィンドウには、デフォルトの選択値が含まれているフィールドがあります。デフォルトの選択値は大部分のユーザに最適な選択を表わしますが、別の選択が環境に適している場合は自由に変更できます。個々のフィールドのエントリの詳細については、オンライン ヘルプを参照してください。

通知を作成できるフィールドには、デフォルトのメッセージが含まれています。既存のエントリの上に入力して、デフォルトの通知を変更することができます。

ツールチップ アイコン

CSC SSM コンソールの一部のウィンドウには、ツールチップと呼ばれる情報アイコンがあります。マウスをツールチップ アイコンの上に置くと、ポップアップ テキストボックスが開き、決定を行ったりタスクを完了したりするのに役立つ追加情報が表示されます。次の例では、ツールチップ アイコンの上にマウスを置くことにより、ウイルス スキャン オプションの 1 つである IntelliScan に関する詳細が表示されています。

図 1-6　情報アイコン（ツールチップ）



オンライン ヘルプ

Trend Micro InterScan for Cisco CSC SSM では、2 種類のオンライン ヘルプが利用できます。一般ヘルプと状況依存ヘルプがあります。

図 1-7　一般オンライン ヘルプおよび状況依存オンライン ヘルプ

1	Help ドロップダウン メニュー	2	Help アイコン

Trend Micro InterScan for Cisco CSC SSM バナーの Help ドロップダウン メニューから Contents タブおよび Index タブをクリックして、一般ヘルプを起動します。2 番目のブラウザ ウィンドウが開き、ヘルプの内容を表示することができます。プラス記号をクリックして、ヘルプ トピックを展開します。

図 1-8　オンライン ヘルプの内容

概要に続いて、オンライン ヘルプ トピックの構成が、ユーザ インターフェイスの左メニューの構成に似た形で表示されます。オンライン ヘルプの内容の最後にコンピュータ ウイルスに関する有用な情報があります。

Index タブをクリックしてオンライン ヘルプのインデックスを表示するか、**Search** をクリックしてキーワードを使用して情報を検索します。

状況依存ヘルプを起動するには、ウィンドウのヘルプ アイコン（）をクリックします。2 番目のブラウザ ウィンドウが開き、現在ユーザ インターフェイスに表示されているウィンドウについての情報が表示されます。

オンライン ヘルプのリンク

オンライン ヘルプにはリンクがあり、青い下線が引かれた文字列で表示されています。リンクをクリックすると、別のヘルプ ウィンドウが表示されるか、ポップアップ テキストボックスが開き、定義などの追加情報が表示されます。オンライン ヘルプのこの機能を使用するには、ブラウザのポップアップ ブロッキングをディセーブルにしておきます。

オンライン ヘルプの大部分の情報は、この『*アドミニストレータ ガイド*』には記載されていません。Trend Micro InterScan for Cisco CSC SSM の詳細については、必ずオンライン ヘルプを参照してください。

ライセンス

この章の概要で説明したように、Trend Micro InterScan for CSC SSM のライセンスには、Base ライセンスと Plus ライセンスの 2 つのレベルがあります。Base ライセンスでは、アンチウイルス、アンチスパイウェア、およびファイル ブロッキング機能が提供されます。Plus ライセンスでは、アンチスパム、アンチフィッシング、コンテンツ フィルタリング、および URL フィルタリング機能が追加されます。Plus ライセンスを有効にするには、Base ライセンスが必要です。

Base ライセンスのみを購入した場合、ライセンスのない機能が CSC SSM コンソールに表示されることがありますが、それらの機能は動作しません。しかし、オンライン ヘルプでライセンスのない機能を表示することはできます。また、Plus ライセンスで提供される追加機能を後で購入することもできます。

購入したライセンスのレベルがわからない場合は、Content Security タブの CSC SSM Information セクションを調べてください。このセクションにライセンス情報が要約されています。

図 1-9　Content Security タブのライセンス情報の場所

または、CSC SSM コンソールで、**Administration > Product License** をクリックして Product License ウィンドウを表示します。ウィンドウの Plus License セクションまでスクロールして、**Status** フィールドを確認します。このフィールドに「Activated」が表示されている場合は、Plus ライセンスの機能があります。Plus ライセンスの機能がない場合、このフィールドには「Not Activated」が表示されています。

Plus ライセンスが必要なウィンドウ

表 1-2 に、Base ライセンスだけで有効な CSC SSM コンソールのウィンドウと、追加の Plus ライセンスを購入した場合にのみ有効なウィンドウを示します。

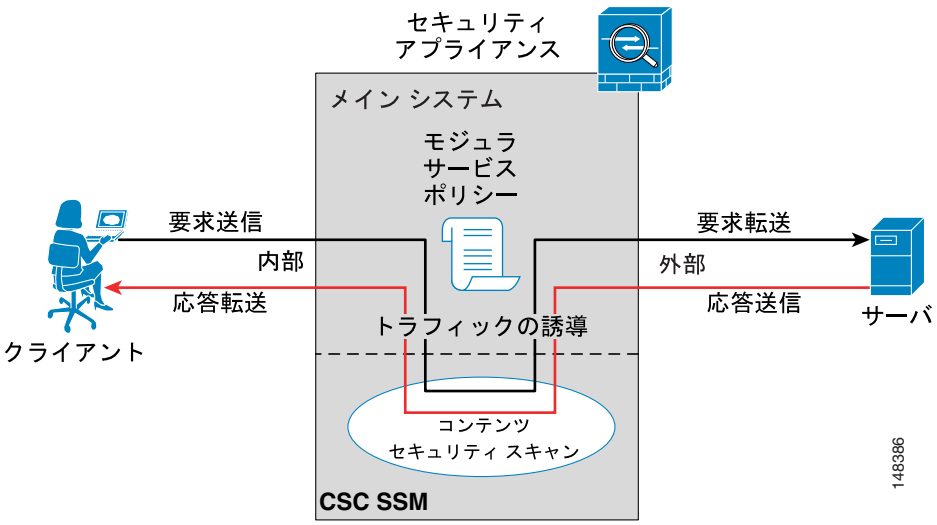
表 1-2　使用可能なウィンドウとライセンス

画面のタイトル	Base ライセンス	Plus ライセンス
Summary > Status/Mail (SMTP)/Mail (POP3)/Web (HTTP)/File Transfer (FTP)	X	
Mail (SMTP) > Scanning > Incoming > Target/Action/Notification	X	
Mail (SMTP) > Scanning > Outgoing > Target/Action/Notification	X	
Mail (SMTP) > Anti-spam > SMTP Incoming Anti-spam Target/Action		X
Mail (SMTP) > Content Filtering > Incoming > SMTP Incoming Content Filtering Target/Action/Notification		X
Mail (SMTP) > Content Filtering > Outgoing > SMTP Incoming Content Filtering Target/Action/Notification		X
Mail (SMTP) > Configuration > Message Filter/Disclaimer/Incoming Mail Domain	X	
Mail (POP3) > Scanning > POP3 Scanning > Target/Action/Notification	X	
Mail (POP3) > Anti-spam > POP3 Anti-spam Target/Action		X
Mail (POP3) > Content Filtering > POP3 Content Filtering Target/Action/Notification		X
Web (HTTP) > Scanning > Target/Webmail Scanning/Action/Notification	X	
Web (HTTP) > File Blocking > Target/Notification	X	
Web (HTTP) > URL Blocking > Via Local List/PhishTrap/Notification		X
Web (HTTP) > URL Filtering > Filtering Rules		X
Web (HTTP) > URL Filtering > Settings > URL Filtering Settings URL Categories/Exceptions/Schedule/Re-classify URL		X
File Transfer (FTP) > Scanning > FTP Scanning Target/Action/Notification	X	
File Transfer (FTP) > File Blocking> Action/Notification	X	
Update > すべての画面	X	
Logs > すべての画面	X	
Administration > すべての画面	X	

プロセス フロー

図 1-10 に、セキュリティ アプライアンスに CSC SSM がインストールされている場合のトラフィックのフローを示します。要求がクライアント ワークステーションからサーバに送信されます。この要求は、セキュリティ アプライアンスによって処理されるとき、コンテンツ セキュリティ スキャンのために CSC SSM に誘導されます。セキュリティ リスクが検出されなければ、この要求はサーバに転送されます。応答の場合も逆順で同じパターンになります。

図 1-10　プロセス フロー



セキュリティ リスクが検出された場合は、CSC SSM の設定状況に従って、無害化または削除されます。

CHAPTER 2

初期セットアップの確認

この章では、Trend Micro InterScan for Cisco CSC SSM が正しく動作していることを確認する方法について説明します。この章は、次の項で構成されています。

ASA クロック セットアップの確認

セットアップの確認を開始するには、まず ASA クロックが正しく設定されていることを確認する必要があります。この設定を確認するには、**Configuration > Properties** をクリックします。Properties メニューで、Device Administration トピックを展開し、**Clock** をクリックします。詳細については、『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』を参照してください。

CSC SSM のアクティベーションの確認

次に、CSC SSM が正しくアクティブになっていることを確認します。実際のデバイスに近づくことができる場合は、デバイスの背部にあるステータス LED を確認してください。ステータス LED は緑色に点灯している必要があります。LED がオレンジで点灯または点滅している場合は、カードがアクティブになっていないか、サービスが開始されていません。詳細については、P.2-6 の「ステータス LED の表示」を参照してください。

実際のデバイスに近づくことができない場合は、ASDM の Content Security タブを確認してください（図 1-9（P.1-12）を参照）。Content Security タブの左上部に表示されているデバイスの型番、管理 IP、バージョンなどを確認する必要があります。確認できない場合は、TAC に問い合せてサポートを受けてください。

スキャンの確認

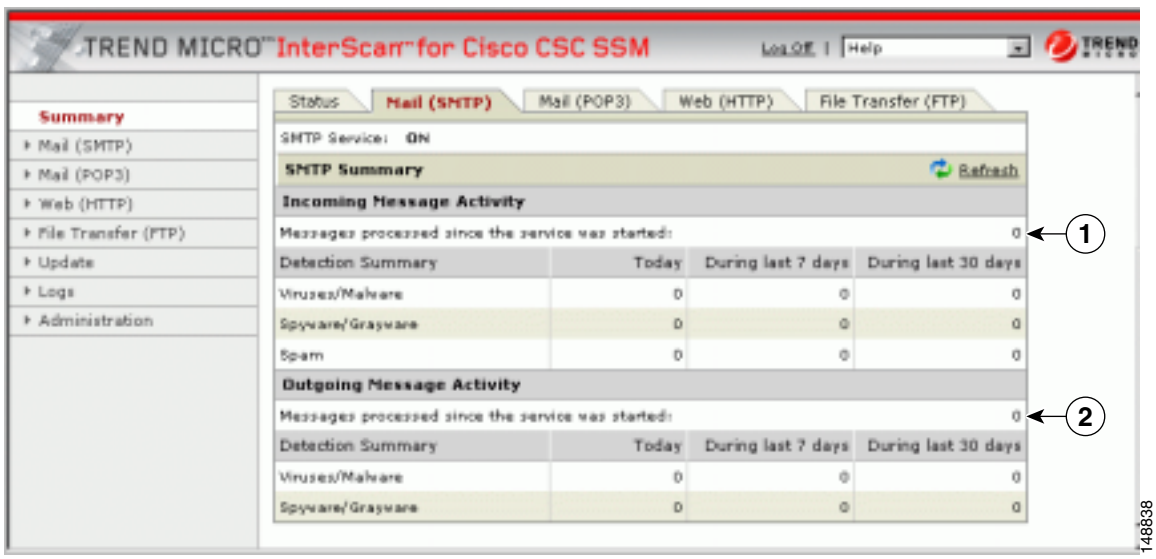
SSM にトラフィックを転送するように ASA を設定すると、CSC SSM コンソールにログオンする前であっても、Trend Micro InterScan for Cisco CSC SSM は、ウイルスやその他のマルウェアがないかどうか、すぐにスキャンを開始します。スキャンは、ログオンしているかどうかにかかわらず実行され、手動でオフにしない限り実行され続けます。

Trend Micro InterScan for Cisco CSC SSM が SMTP ネットワーク トラフィックをスキャンしていることを確認するには、次の手順を実行します。

- ASDM で、Content Security タブの Email Scan ペインを調べます。Email Scanned Count グラフが増加している必要があります。
- CSC SSM コンソールで、Summary ウィンドウの **Mail (SMTP)** タブをクリックします。Summary - Mail (SMTP) ウィンドウの「Incoming Message Activity」および「Outgoing Message Activity」セクションにある **Messages processed since the service was started** フィールドを調べます。図 2-1 に例を示します。

(注)　また、コマンドライン インターフェイスから、パケットが CSC SSM に転送されていることを確認することもできます。**show service-policy csc** コマンドを使用します。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

図 2-1　Summary ウィンドウでのスキャンの確認



1	着信メッセージ アクティビティ カウンタ	2	発信メッセージ アクティビティ カウンタ

メッセージ アクティビティ カウンタは、トラフィックがネットワークを通過するにつれて増加します。カウンタをアップデートするには、Refresh リンクをクリックします。

(注)　サービスが再開始されると、常にカウンタもリセットされます。

POP3 トラフィックについて同様のテストを実行するには、**Mail (POP3)** タブをクリックするか、POP3 トラフィックのカウントが示す ASDM の Email Scanned Count グラフを表示します。

アンチウイルス機能のテスト

European Institute for Computer Antivirus Research （EICAR）は、Trend Micro InterScan for Cisco CSC SSM などのアンチウイルス テクノロジーによって本物のウイルスとして検出される、安全なテスト ウイルスを開発しました。このテスト ウイルスは、.com 拡張子を持つテキスト ファイルで、ウイルス コードは断片であれ、まったく含まれていません。このテスト ウイルスを使用してウイルス事象を発生させ、電子メール通知およびウイルス ログが正しく動作することを確認します。

テストを実行するには、ブラウザ ウィンドウを開いて次の URL にアクセスします。

http://www.eicar.com/anti_virus_test_file.htm

図 2-2 に示す情報ボックスが表示されるまでスクロールします。

図 2-2　EICAR ダウンロード エリア

eicar.com リンクをクリックします。セキュリティ イベントが発生したことを知らせる通知が、すぐにブラウザで受信されます。CSC SSM コンソールで **Logs > Query** に移動して、ウイルス / マルウェア ログ ファイルをクエリーし、ログに記録されたテスト ウイルスの検出を確認することができます。また、インストール時に（**Host Configuration** インストール ウィンドウで）選択した管理者の電子メール アドレスにも通知が送信されます。

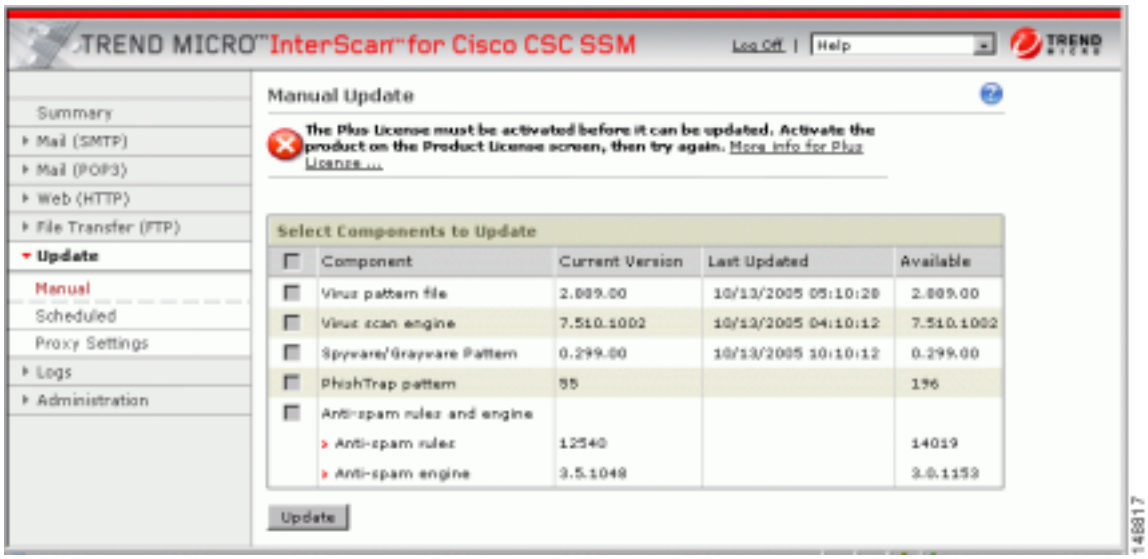
送信されない場合は、次のいずれかが考えられます。

1. CSC SSM がアクティブになっていない可能性があります。P.2-1 の「CSC SSM のアクティベーションの確認」の情報によってデバイスがアクティブになっていることを確認します。
2. ASA の設定が誤っている可能性があります。詳細については、P.8-12 の「不正な ASA ファイアウォール ポリシー設定のためにスキャンが動作しない」を参照してください。
3. CSC SSM が、リブート処理中である、またはソフトウェア障害が発生しているといった、障害状態となっています。実際に障害の場合は、syslog エラー 421007 が生成されています。このエラーがあるかどうか、syslog をチェックしてください。また、TAC に問い合せる前に、P.8-12 の「CSC SSM が失敗ステータスにあるためにスキャンが動作しない」で詳細を確認してください。

コンポーネントのステータスの確認

最新のウイルス パターン ファイル、スキャン エンジン、スパイウェア パターン ファイル、PhishTrap パターン、アンチスパム ルール、およびアンチスパム エンジンが CSC SSM コンソールにあるかどうかを確認するには、**Update > Manual** をクリックして、**Manual Update** ウィンドウを表示します。図 2-3 を参照してください。

図 2-3　Manual Update ウィンドウ



より新しいバージョンが使用できる場合は、アップデート バージョン番号が **Available** カラムに赤で表示されます。アップデートするコンポーネントを選択し、**Update** をクリックして選択したコンポーネントの最新バージョンをダウンロードします。

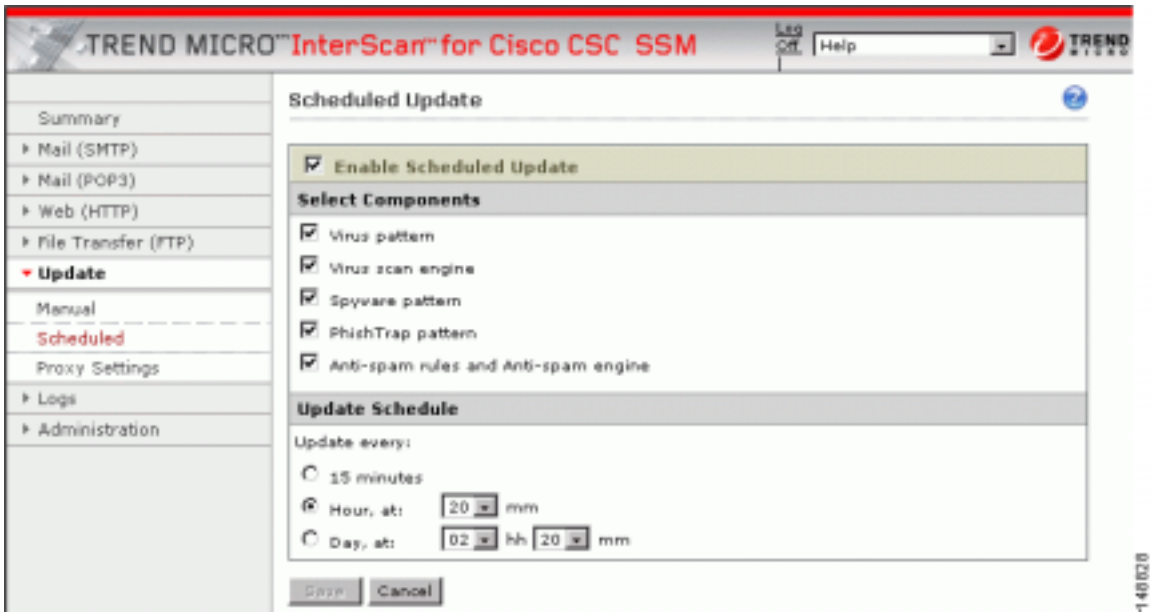
ヒント

現在のバージョンと使用可能なバージョンが同じで、新しいバージョンが入手できると考えられる場合、または **Available** カラムが空白の場合は、次のいずれかの可能性があります。

1. Trend Micro ActiveUpdate サーバがダウンしている。
2. ネットワークに問題がある。
3. 使用可能な新しいコンポーネントは存在せず、すべて実際に最新のものである。
4. Trend Micro InterScan for Cisco CSC SSM が正しく設定されていない。

不確定要素を回避するには、**Update** > **Scheduled** をクリックして、Scheduled Update ウィンドウを表示します。図 2-4 を参照してください。

図 2-4　Scheduled Update ウィンドウ

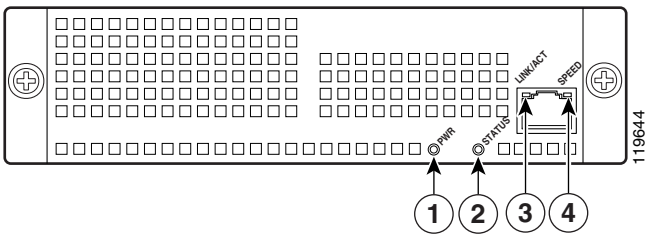


デフォルトでは、Trend Micro InterScan for Cisco CSC SSM は定期的にコンポーネントをアップデートし、スケジュールされたアップデートの実行後に自動的に通知を行います。スケジュールされたアップデートの間隔を変更して、アップデートの頻度を多くしたり少なくしたりすることができます。

ステータス LED の表示

アプライアンスの背面に、ASA SSM インジケータの**ステータス** LED があります。図 2-5 を参照してください。

図 2-5　ASA SSM インジケータ



ステータス LED には **2** のラベルが付いています。**ステータス** LED には、次の表に示す複数の状態があります。

表 2-1　ASA-SSM インジケータ

	LED	色	状態	説明
1	電源	緑	オン	システムは通電状態です。
2	ステータス	緑色およびオレンジ	点滅	SSM は動作中でアクティブですが、スキャン サービスはダウンしています。点滅が 1 分以上続く場合は、CSC SSM が新しいパターン ファイル / スキャン エンジンをロード中であるか、または、問題のトラブルシューティングを行う必要がある場合です。
		緑	点灯	SSM は起動されていますが、アクティブではありません。
		オレンジ	点灯	SSM は電源投入診断に合格しました。これは通常の動作ステータスです。
3	リンク / アクティブ	緑	点灯	イーサネット リンクがあります。
			点滅	イーサネット アクティビティが発生しています。
4	速度	緑	100 MB	ネットワーク アクティビティが発生しています。
		オレンジ	1000 MB（ギガビット イーサネット）	ネットワーク アクティビティが発生しています。

（注） **1**、**3**、および **4** のラベルが付いた LED は CSC SSM ソフトウェアでは使用されません。

SSM 管理ポート トラフィックについて

インストール時に（IP Configuration インストール ウィンドウで）、管理インターフェイスの IP アドレス、ゲートウェイ IP、およびマスク IP を選択します。次に管理ポートを使用するトラフィックのリストを示します。

- **ActiveUpdate**：Trend Micro InterScan for Cisco CSC SSM が新しいパターン ファイルおよびスキャン エンジンのアップデートをダウンロードする Trend Micro アップデート サーバとの通信
- **URL rating lookups**：URL ブロッキングおよびフィルタリングを実行する Plus ライセンスを購入した場合に使用される、URL フィルタリング データベースのダウンロード
- **Syslog**：このポートは Trend Micro InterScan for Cisco CSC SSM から syslog サーバへのデータのアップロードに使用されます
- **Email notifications**：ウイルス検出などのトリガー イベントの通知が SSM 管理ポート経由で送信されます
- **DNS lookup**：管理ポートは、Trend Micro サーバ IP を検索するために、パターン ファイルのアップデートに使用されるホスト名の解決にも使用されます
- **Cisco ASDM/Trend Micro GUI access**：管理ポートは Cisco ASDM インターフェイスと Trend Micro InterScan for Cisco CSC SSM インターフェイスの間の通信を可能にします

CHAPTER 3

メール トラフィック（SMTP および POP3）の設定

インストール後に ASA が SSM にトラフィックを送信するよう設定した場合、SMTP トラフィックおよび POP3 トラフィックに、ウイルスや、ワームやトロイの木馬といったその他のマルウェアがないかどうか、スキャンが行われます。この章では、スパイウェアなどのセキュリティ リスクの検出に必要な追加設定、および着信メッセージと発信メッセージへの組織としての免責条項の追加に必要な追加設定について説明します。この章は次の項で構成されています。

デフォルトのメール スキャン設定

表 3-1 に、メール コンフィギュレーション設定、およびインストール後に動作するデフォルト値の要約を示します。

表 3-1　デフォルトのメール スキャン設定

機能	デフォルト設定
着信メールおよび発信メールのメール（SMTP）スキャン	デフォルトのスキャン方式として All Scannable Files の使用がイネーブルになっています
メール（POP3）スキャン	デフォルトのスキャン方式として All Scannable Files の使用がイネーブルになっています
メール（SMTP）およびメール（POP3）のスキャン メッセージ フィルタ（指定したサイズより大きいメッセージを拒否します）	20 MB より大きいメッセージを拒否するようにイネーブルになっています
メール（SMTP）メッセージ拒否（指定した数よりも多くの受信者があるメッセージを拒否します）	100 人以上の受信者宛のメッセージを拒否するようにイネーブルになっています
着信メールおよび発信メールに対するメール（SMTP）圧縮ファイル処理、および メール（POP3）圧縮ファイル処理	次の場合は圧縮ファイルのスキャンを省略するように設定されています • 圧縮解除されるファイル数が 200 よりも多い場合 • 圧縮解除されるファイル サイズが 20 MB を超える場合 • 圧縮レイヤ数が 3 を超える場合 • 圧縮解除/圧縮ファイルのサイズ比率が 100/1 を超える場合
メール（SMTP）の着信と発信、およびマルウェアが検出されたメッセージのメール（POP3）アクション	マルウェアが検出されたメッセージまたは添付ファイル（あるいはその両方）を修復します メッセージまたは添付ファイル（あるいはその両方）を修復できない場合は、削除します
メール（SMTP）の着信と発信、およびスパイウェア / グレーウェアが検出されたメッセージのメール（POP3）アクション	ファイルの配信を許可します
メール（SMTP）の着信と発信、およびマルウェアが検出された場合のメール（POP3）通知	マルウェアが検出されたメッセージには、%VIRUSNAME% was detected in the file (%FILENAME%). The following action has been taken: %ACTION% というインライン通知が挿入されます。
パスワードで保護された電子メール メッセージ（SMTP および POP3）	スキャンを行わずにファイルの配信を許可します
指定したスキャンの基準を超えるためスキャンされない、SMTP および POP3 経由で送信された圧縮ファイル	ファイルの配信を許可します

これらのデフォルト設定では、Trend Micro InterScan for Cisco CSC SSM をインストールした後に、電子メール トラフィックにある程度の保護が適用されます。これらの設定は変更できます。変更する前に、これらの選択の詳細についてオンライン ヘルプで慎重に検討してください。

インストール後にアップデートすることで、電子メール トラフィックを最大限に保護する追加のコンフィギュレーション設定があります。これらの追加設定については、この章の残りのページで説明します。

アンチスパムおよびコンテンツ フィルタリング機能を使用できる Plus ライセンスを購入した場合は、これらの機能を設定する必要があります。デフォルトでは動作しません。

着信 / 発信 SMTP メールの定義

1 つの電子メール メッセージが複数の受信者宛で、受信者の 1 人または複数人へは着信メッセージ（同じドメイン名を持つ同じ組織内のだれか宛）で、受信者の 1 人へは発信メッセージ（異なるドメイン名を持つ異なる組織のだれか宛）である場合、着信規則が適用されます。たとえば、psmith@example.com からのメッセージが jdoe@example.com および gwood@example.net 宛になっています。

着信 SMTP メッセージが「scan all」オプションでスキャンされるのに対し、発信 SMTP メッセージは IntelliScan でスキャンされるとします。また、スパイウェア / グレーウェア検出が着信メッセージに対してのみイネーブルになっているとします。

たとえ gwood が「発信」受信者であっても、psmith から jdoe および gwood へのメッセージは両方の受信者宛の着信メッセージとして扱われます。

SMTP および POP3 スパイウェア / グレーウェア検出のイネーブル化

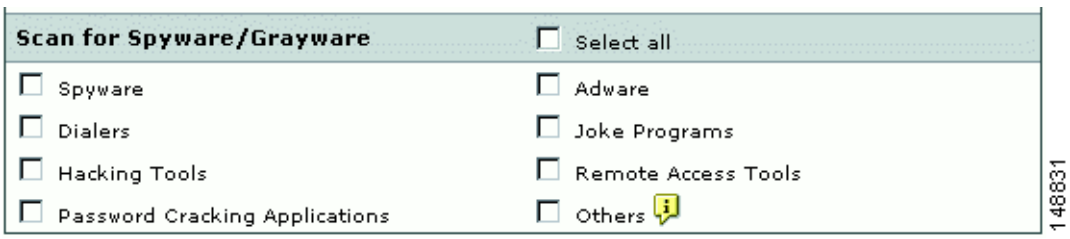
グレーウェアは、正当か、好ましくないか、または悪意があるかが不明確なソフトウェアのカテゴリです。ウイルス、ワーム、トロイの木馬などの脅威とは異なり、グレーウェアは、データが感染したり、データの複製または破壊を行ったりすることはありませんが、プライバシーが侵害される可能性があります。グレーウェアの例としては、スパイウェア、アドウェア、リモート アクセス ツールがあります。

スパイウェア / グレーウェア検出は、デフォルトではイネーブルになっ*ていません*。電子メール トラフィックでスパイウェアおよびその他の形態のグレーウェアの検出を開始するには、次のウィンドウでこの機能を設定します。

- ASDM の **Configuration > Trend Micro Content Security > Mail** で Configure Incoming Scan リンクをクリックすると、**SMTP Incoming Message Scan/Target** ウィンドウが表示されます
- ASDM の **Configuration > Trend Micro Content Security > Mail** で Configure Outgoing Scan リンクをクリックすると、**SMTP Outgoing Message Scan/Target** ウィンドウが表示されます
- CSC SSM コンソールで **Mail (POP3) > Scanning > POP3 Scanning/Target** をクリックすると、**POP3 Scanning/Target** ウィンドウが表示されます

これらのウィンドウの **Scan for Spyware/Grayware** セクションで（図 3-1 を参照）、Trend Micro InterScan for Cisco CSC SSM で検出するグレーウェアのタイプを選択します（チェックボックスをオンにします）。

図 3-1　スパイウェア / グレーウェアのスキャンの設定



これらのタイプのグレーウェアの説明については、上記のウィンドウの固有のオンライン ヘルプを参照してください。検出するグレーウェアのタイプを指定した後、必ず **Save** をクリックして新しい設定をイネーブルにしてください。

SMTP 通知および POP3 通知の検討

デフォルトの通知設定で十分な場合、それ以上の設定は必要ありません。しかし、通知オプションを検討して、デフォルトを変更するかどうかを決定することができます。次の例を参考にしてください。

- 電子メール メッセージにセキュリティ リスクが検出された場合、管理者に通知を送信することができます（SMTP では、送信者と受信者の両方、またはいずれか一方に通知することもできます）
- 所属組織により適するように、通知メッセージのデフォルトのテキストを変更することができます

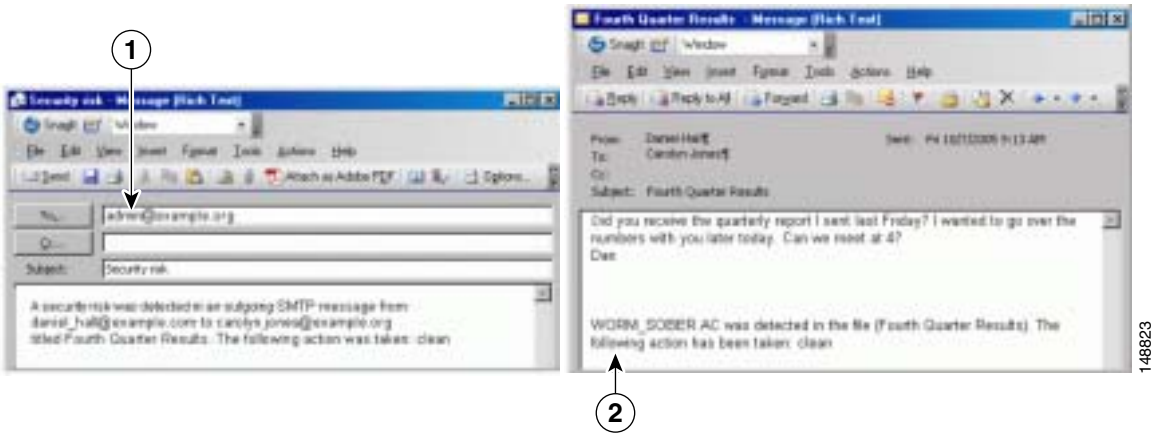
電子メール メッセージを検討し、場合によって書き換えるには、CSC SSM コンソールで次のウィンドウに進みます。

- **Mail (SMTP) > Scanning > Incoming > SMTP Incoming Message Scan/Notification**
- **Mail (SMTP) > Scanning > Outgoing > SMTP Outgoing Message Scan/Notification**
- **Mail (POP3) > Scanning > POP3 Scanning/Notification**

通知のタイプ

図 3-2 に示すように、電子メール トラフィックでは、電子メール通知とインライン通知の 2 つのタイプの通知を使用することができます。

図 3-2　通知の例



1	電子メール通知	2	インライン通知

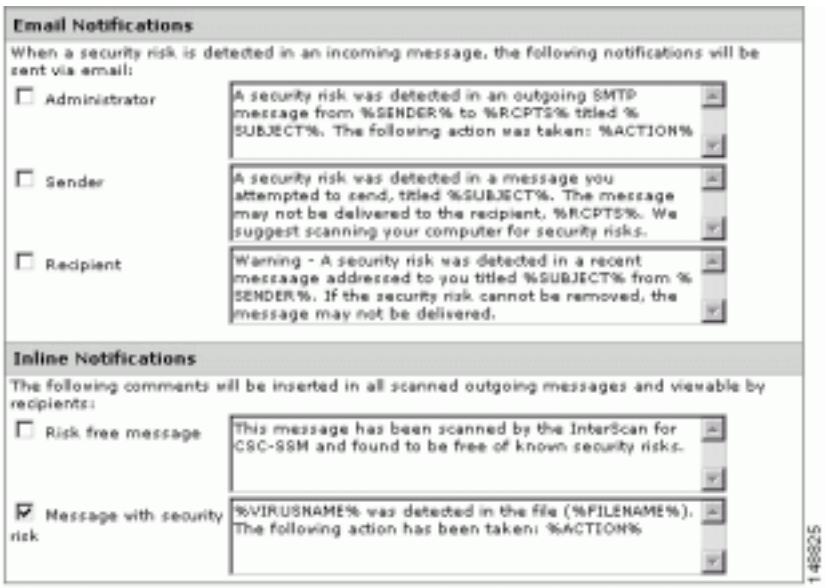
トークンと呼ばれる変数を使用して、通知をさらに有益なものとする情報を提供します。たとえば、%VIRUSNAME% と呼ばれるトークンは、右側のインライン通知の例のテキストでは WORM_SOBER.AC に置き換えられています。

トークンの詳細については、オンライン ヘルプのトピック「Using Tokens in Notifications」を参照してください。

通知の変更

追加の受信者に通知を送信する場合、またはトリガー イベントの発生時に送信される通知メッセージのデフォルトのテキストを変更する場合は、アップデートするメッセージ スキャン通知ウィンドウに進みます。例として、図 3-3 に、**Mail (SMTP) > Scanning > Outgoing > SMTP Outgoing Message Scan/Notification** ウィンドウの通知フィールドを示します。

図 3-3　発信 SMTP の通知の設定



デフォルトでは、通知は、メッセージ受信者に送られるインライン通知のみです。これは、送信者も発信元組織の管理者もセキュリティ上の脅威が検出され、無害化されたことを認識していないことを意味します。変更するには、次の手順を実行します。

- ウィンドウの **Email Notifications** セクションで、電子メールによる通知を受けとる追加の受信者をクリックします。
- ウィンドウの **Inline Notifications** セクションで、「risk-free」インライン通知のみ、デフォルトの「risk detected and action taken」メッセージのみ、どちらも指定しない、または両方とも指定する、のいずれかを選択します。
- いずれかの通知のテキストを変更するには、既存のテキストを強調表示し、独自のメッセージをテキストボックスに入力します。入力が終了したら必ず **Save** をクリックしてください。

SMTP メッセージ フィルタ、免責条項、および着信メール ドメインの設定

(注)　これらの設定は、SMTP プロトコルだけに適用されます。

Mail (SMTP) > Configuration > SMTP Configuration から可能なコンフィギュレーション設定を検討します。**SMTP Configuration** ウィンドウには次の 4 つのタブがあります。

- Message Filter
- Disclaimer
- Incoming Mail Domain
- Advanced Settings

これらを設定するには、次の手順を実行します。

ステップ 1　**SMTP Configuration** ウィンドウの **Message Filter** タブで、Trend Micro InterScan for Cisco CSC SSM は、20 MB より大きいメッセージ、および 100 人を超える受信者宛のメッセージを拒否するように、すでに設定されています。これらの設定は、電子メール サーバが数百人の受信者宛の膨大な偽のメッセージを処理しようとして CPU 時間を消費するネットワーク上の攻撃からの保護に役立ちます。デフォルト設定を推奨します。デフォルト設定を使用し続ける場合、このウィンドウでの処置は不要です。

ステップ 2　SMTP Configuration ウィンドウの **Message Filter** タブで、SMTP メッセージの最初または最後に表示される組織としての免責条項を追加できます。**Add this disclaimer...** チェックボックスをオンにすると、この機能がイネーブルになります。または、この機能を使用しない場合は、現状のままでこのページを終了します。免責条項のテキストをカスタマイズするには、デフォルトのメッセージを強調表示しておいて、上書きします。

ステップ 3　SMTP Configuration ウィンドウの **Incoming Mail** タブでは、次の目的で追加の着信メール ドメインを定義することができます。

- ウイルスおよびその他の脅威のスキャン
- アンチスパム
- コンテンツ フィルタリング

Incoming mail domains フィールドには、インストール時に（Host Configuration インストール ウィンドウで）入力した着信電子メール ドメイン名がすでに表示されています。ドメインを追加する場合は、トップ レベル ドメイン（tld）名のみを入力します。たとえば、example1.com や example2.com などの下位ドメインは入力せずに、example.com のみを入力します。他の着信ドメインがない場合は、このウィンドウでの処置は不要です。

ステップ 4　SMTP Configuration ウィンドウの **Advanced Settings** タブには次の設定ができるフィールドがあります。

- 攻撃者からのものと思われるメッセージに対してより積極的な（または緩やかな）タイムアウトを設定する
- メッセージが攻撃という形の動作をした場合、SMTP トラフィックの移動をより困難にする設定をイネーブルにする

詳細については、オンライン ヘルプを参照してください。

ステップ 5　変更を加えた場合は、**Save** をクリックして、アップデートした SMTP 設定をアクティブにします。

SMTP および POP3 スパム フィルタリングのイネーブル化

（注） この機能には Plus ライセンスが必要です。

SMTP および POP3 アンチスパム機能はデフォルトではディセーブルになっており、設定する必要があります。

ヒント Base ライセンスと Plus ライセンスを同時に購入した場合も、後で Plus ライセンスを追加した場合も、アンチスパムはデフォルトでディセーブルになっています。使用を開始するには、アンチスパム機能をイネーブルにして設定する必要があります。

アンチスパム機能を設定するには、次の手順を実行します。

- **ASDM の Configuration > Trend Micro Content Security > Mail** で Configure Anti-spam リンクをクリックすると、**SMTP Incoming Anti-spam** ウィンドウが表示されます
- CSC SSM コンソールで **Mail (POP3) > Anti-spam > POP3 Anti-spam** をクリックすると、**POP3 Anti-spam** ウィンドウが表示されます

アンチスパムをイネーブルにするには、次の手順を実行します。

ステップ 1　上記のウィンドウの **Target** ビューで **Enable** をクリックします。

ステップ 2　デフォルト値の **Low** を使用しない場合は、アンチスパムしきい値を **Medium** または **High** に再設定します。

ヒント 組織でスパムをブロックする経験を積んでから、後でこの設定を調整することもできます。しきい値が低すぎる場合は、スパムの発生率が高くなります。しきい値が高すぎる場合は、誤検出（スパムと識別された正当なメッセージ）の発生率が高くなります。

ステップ 3　**SMTP Incoming Anti-spam** ウィンドウおよび **POP3 Anti-spam/Target** ウィンドウの **Approved Senders** セクションで、承認された送信者を追加します。承認された送信者からのメールは、スパムと判断されることなく常に受信されます。

（注） 承認された送信者は、一方のウィンドウで追加および保存されると、もう一方のウィンドウにも表示されます。たとえば、**POP3 Anti-spam** ウィンドウの **Approved Senders** リストに robert_li@example.com を追加したとします。ここで、**SMTP Incoming Anti-spam** ウィンドウを開きます。robert_li@example.com のアドレスは、**SMTP Incoming Anti-spam** ウィンドウの **Approved Senders** のリストにもすでに追加されています。

Blocked Senders リストも同様に、一方のウィンドウで作成されたブロックされる送信者は、両方のウィンドウに表示されます。

ステップ 4　**SMTP Incoming Anti-spam** ウィンドウおよび **POP3 Anti-spam/Target** ウィンドウの **Blocked Senders** セクションで、ブロックされる送信者を追加します。ブロックされる送信者からのメールは常に拒否されます。ブロックされる送信者は、一方のウィンドウで追加および保存されると、もう一方のウィンドウにも表示されます。

ステップ 5　**SMTP Incoming Anti-spam** ウィンドウおよび **POP3 Anti-spam/Action** ウィンドウで、スパムと識別されたメッセージに対する処置を設定します。選択できる処置は、次のとおりです。

- メッセージに「Spam:」などのスパム識別子のマークを付けて送信します（スパム識別子は、たとえば、「Spam:Designer luggage at a fraction of the cost!」などメッセージ件名のプレフィックスの役割を果たします）
- メッセージを削除する

ステップ 6　**Save** をクリックして、設定ごとにアンチスパムをアクティブにします。

SMTP および POP3 コンテンツ フィルタリングのイネーブル化

（注） この機能には Plus ライセンスが必要です。

SMTP および POP3 コンテンツ フィルタリング機能はデフォルトではディセーブルになっており、設定する必要があります。コンテンツ フィルタリング機能を設定するには、次のウィンドウに進みます。

- ASDM の **Configuration > Trend Micro Content Security > Mail** で Configure Incoming Filtering リンクをクリックすると、SMTP Incoming Content Filtering/Target ウィンドウが表示されます
- ASDM の **Configuration > Trend Micro Content Security > Mail** で Configure Outgoing Filtering リンクをクリックすると、SMTP Outgoing Content Filtering/Target ウィンドウが表示されます
- CSC SSM コンソールで **Mail (POP3) > Content Filtering > POP3 Content Filtering/Target** をクリックすると、POP3 Content Filtering/Target ウィンドウが表示されます。

コンテンツ フィルタリングをイネーブルにするには、次の手順を実行します。

ステップ 1　上記のウィンドウの **Target** ビューで **Enable** をクリックします。

ステップ 2　メッセージ サイズ フィルタリング基準を使用するかどうかを決定し、使用する場合は、**Message size is** フィールドにパラメータを設定します。たとえば、5 MB を超えるメッセージおよび添付ファイルのメッセージ フィルタリングを指定した場合、5 MB より小さい添付ファイルがあるメッセージはフィルタリングされません。メッセージのサイズを指定しない場合、サイズにかかわらずすべてのメッセージがフィルタリングされます。

ステップ 3　ウィンドウの **Message Subject and Body** セクションで、メッセージの件名または本文（あるいは両方）に存在した場合に、コンテンツ フィルタリング アクションをトリガーする言葉を指定します。

ステップ 4　ウィンドウの **Message Attachment** セクションで、添付ファイル名の中に存在した場合に、コンテンツ フィルタリング アクションをトリガーする文字または言葉を指定します。ウィンドウのこのセクションで、ファイル タイプによってコンテンツ フィルタリングを選択することもできます。たとえば、フィルタリングに Microsoft Office のファイル タイプを選択した場合、Microsoft Office ツールを使用して作成された添付ファイルは、コンテンツのためにフィルタリングされます。

ステップ 5　上記のウィンドウの **Action** タブをクリックして、コンテンツ フィルタリングがトリガーされたときのアクションを指定します。電子メール メッセージでは、選択できるアクションは次のとおりです。

- コンテンツ フィルタリング ポリシーのいずれかに違反するメッセージを削除する
- メッセージを送信する

添付ファイルでは、選択できるアクションは次のとおりです。

- 違反する添付ファイルの通過を許可する（この場合、ウィンドウの **For messages that match the attachment criteria** セクションで変更を加えないでください）
- 添付ファイルを削除し、メッセージ本文にインライン通知を挿入する

ステップ 6　上記のウィンドウの **Notification** タブをクリックして、コンテンツ フィルタリング違反の通知を管理者に送信するかどうかを指定します（SMTP では、送信者または受信者（あるいは両方）に通知することもできます）。デフォルトのメッセージを強調表示して上書きすることで、通知メッセージボックスのデフォルトのテキストを変更します。

ステップ 7　**Save** をクリックして、設定ごとにコンテンツ フィルタリングをアクティブにします。

CHAPTER 4

Web（HTTP）トラフィックおよびファイル転送（FTP）トラフィックの設定

インストール後、デフォルトで、HTTP トラフィックおよび FTP トラフィックは、ウイルス、ワーム、およびトロイの木馬がないかどうかスキャンされます。スパイウェアなどのマルウェアやその他のグレーウェアを検出するには、コンフィギュレーションを変更する必要があります。この章では、これらのコンフィギュレーションのアップデートの方法について説明します。この章は、次の項で構成されています。

デフォルトの Web および FTP のスキャン設定

表 4-1 に、Web およびファイル転送のコンフィギュレーション設定、およびインストール後に動作するデフォルト値の要約を示します。

表 4-1　デフォルトの Web および FTP のスキャン設定

機能	デフォルト設定
ファイル ダウンロードの Web（HTTP）スキャン	デフォルトのスキャン方式として All Scannable Files の使用がイネーブルになっています
Web メール スキャン	デフォルトで、Yahoo™、AOL™、MSN™、および Google™ の Web メール サイトをスキャンするように設定されています
ファイル転送に対するファイル転送（FTP）スキャン	デフォルトのスキャン方式として All Scannable Files の使用がイネーブルになっています
Web からのダウンロードに対する Web（HTTP）圧縮ファイル処理、および FTP サーバからのファイル転送に対するファイル転送（FTP）圧縮ファイル処理	次の場合は圧縮ファイルのスキャンを省略するように設定されています • 圧縮解除されるファイル数が 200 よりも多い場合 • 圧縮解除されるファイル サイズが 30 MB を超える場合 • 圧縮レイヤ数が 3 を超える場合 • 圧縮解除 / 圧縮ファイルのサイズ比率が 100/1 を超える場合
Web（HTTP）およびファイル転送（FTP）の大容量ファイル処理（指定サイズより大きいファイルをスキャンしません - 指定サイズより大きいファイルの据え置きスキャンのイネーブル化）	50 MB より大きいファイルのスキャンを省略し、2 MB より大きいファイルの据え置きスキャンをイネーブルにするように設定されています
Web（HTTP）ダウンロード、およびマルウェアが検出されたファイルのファイル転送（FTP）アクション	マルウェアが検出されたダウンロードまたはファイル（あるいはその両方）を修復します 修復できない場合は、削除します
Web（HTTP）ダウンロード、およびスパイウェア / グレーウェアが検出されたファイルのファイル転送（FTP）アクション	ファイルは削除されます
Web（HTTP）ダウンロード、およびマルウェアが検出された場合のファイル転送（FTP）通知	InterScan for CSC SSM によってユーザが転送しようとしているファイルがスキャンされ、セキュリティ リスクが検出されたことを示すインライン通知がユーザのブラウザに掲載されます

これらのデフォルト設定では、Trend Micro InterScan for Cisco CSC SSM をインストールした後に Web および FTP のトラフィックに多少の保護が適用されます。これらの設定は変更できます。たとえば、マルウェアの検出に **All Scannable Files** ではなく、**Scan by specified file extensions...** オプションを使用できます。変更する前に、これらの選択の詳細についてオンライン ヘルプで慎重に検討してください。

インストール後にアップデートすることで、Web および FTP のトラフィックを最大限に保護する追加のコンフィギュレーション設定があります。これらの追加設定については、この章の残りのページで説明します。

URL ブロッキング、アンチフィッシング、および URL フィルタリング機能を使用できる Plus ライセンスを購入した場合は、これらの機能を設定する必要があります。デフォルトでは動作しません。

大容量ファイルのダウンロード

HTTP Scanning ウィンドウおよび FTP Scanning ウィンドウの Target タブを使用すると、スキャンする最大ダウンロードのサイズを定義することができます。たとえば、20 MB 未満のダウンロードはスキャンするが、20 MB より大きいダウンロードはスキャンしないように指定することができます。

さらに、次の指定ができます。

- これらのスキャンされない大容量のダウンロードの送信を、スキャンなしで許可するかどうかを指定します。スキャンなしの場合、セキュリティ リスクが発生する可能性があります。または、
- 指定した制限を越えるダウンロードを削除することを指定します

デフォルトでは、CSC SSM ソフトウェアは 50 MB 未満のファイルはスキャンし、50 MB 以上のファイルはスキャンせずに要求クライアントに送信するように指定されています。

据え置きスキャン

据え置きスキャン機能はデフォルトではイネーブルになっていません。この機能をイネーブルにした場合、ユーザはダウンロード全体をスキャンせずにデータのダウンロードを開始することができます。そのため、据え置きスキャンでは、ユーザは情報の本体すべてがスキャンされるのを長時間待つことなく、データの表示を開始することができます。

注意　据え置きスキャンがイネーブルの場合、情報のスキャンされない部分ではセキュリティ リスクが発生する可能性があります。

据え置きスキャンがイネーブルでない場合は、ユーザに示される前にダウンロードの内容全体がスキャンされる必要があります。しかし、クライアント ソフトウェアの中には、スキャンするファイル全体を構成するのに十分なネットワーク パケットの収集に要する時間が長いために、タイムアウトするものがあります。

次に要約を示します。

方式	利点	欠点
据え置きスキャンがイネーブルの場合	クライアントのタイムアウトを防ぎます	セキュリティ リスクが発生する可能性があります
据え置きスキャンがディセーブルの場合	より安全です。ユーザに提示される前にファイル全体がセキュリティ リスクがないかどうかスキャンされます	ダウンロードが完了する前にクライアントのタイムアウトが発生する可能性があります

HTTPS トラフィックのスキャン

CSC SSM ソフトウェアは、HTTPS プロトコル経由で移動するトラフィックについては、ウイルスおよびその他の脅威がないかどうか、スキャンを行うことはできません。

スパイウェア / グレーウェアの検出

グレーウェアは、正当か、好ましくないか、または悪意があるかが不明確なソフトウェアのカテゴリです。ウイルス、ワーム、トロイの木馬などの脅威とは異なり、グレーウェアは、データが感染したり、データの複製やデータの破壊を行ったりすることはありませんが、プライバシーが侵害される可能性があります。グレーウェアの例としては、スパイウェア、アドウェア、リモート アクセス ツールなどがあります。

スパイウェア / グレーウェア検出は、デフォルトではイネーブルになっ*ていません*。Web トラフィックおよびファイル転送トラフィックで、スパイウェアとスパイウェアの変形、およびその他のグレーウェアの検出を開始するには、次のウィンドウでこの機能を設定します。

- **Web (HTTP) > Scanning > HTTP Scanning/Target**
- **File Transfer (FTP) > Scanning > FTP Scanning/Target**

ASDM の **Configuration > Trend Micro Content Security > Web** で Configure Web Scanning リンクをクリックして、HTTP Scanning ウィンドウの Target タブに直接進むことができます。ASDM の **Configuration > Trend Micro Content Security > File Transfer** で Configure File Scanning リンクをクリックして、FTP Scanning ウィンドウの Target タブに直接進むことができます。

詳細については、P.3-4 の「SMTP および POP3 スパイウェア / グレーウェア検出のイネーブル化」を参照してください。上記のウィンドウについては、オンライン ヘルプも参照してください。

Web メールのスキャン

注意　Web メールだけをスキャンするように選択した場合、HTTP スキャンは **Web (HTTP) > Scanning > HTTP Scanning** ウィンドウの Webmail Scanning タブで指定したサイトに限定されます。その他の HTTP トラフィックはスキャン*されません*。

表 4-1 に示したように、Yahoo、AOL、MSN、および Google の Web メール スキャンはデフォルトですでに設定されています。サイトを追加するには、ASDM の **Configuration > Trend Micro Content Security > Web** で Configure Web Scanning リンクをクリックします。**HTTP Scanning** ウィンドウの Target タブが表示されます。**Webmail Scanning** タブをクリックします。

次の情報を使用して **Name** フィールドに Web メール サイトを入力します。

- 正確な Web サイト名
- URL キーワード
- 文字列

（注）　Web メールを介して管理されるメッセージの添付ファイルはスキャンされます。

スキャンする追加の Web メール サイトを設定する方法の詳細については、オンライン ヘルプを参照してください。設定されたサイトは、ごみ箱アイコンをクリックしてウィンドウの **Scan Webmail at following sites** セクションから削除しないかぎりスキャンされます。**Save** をクリックして設定をアップデートします。

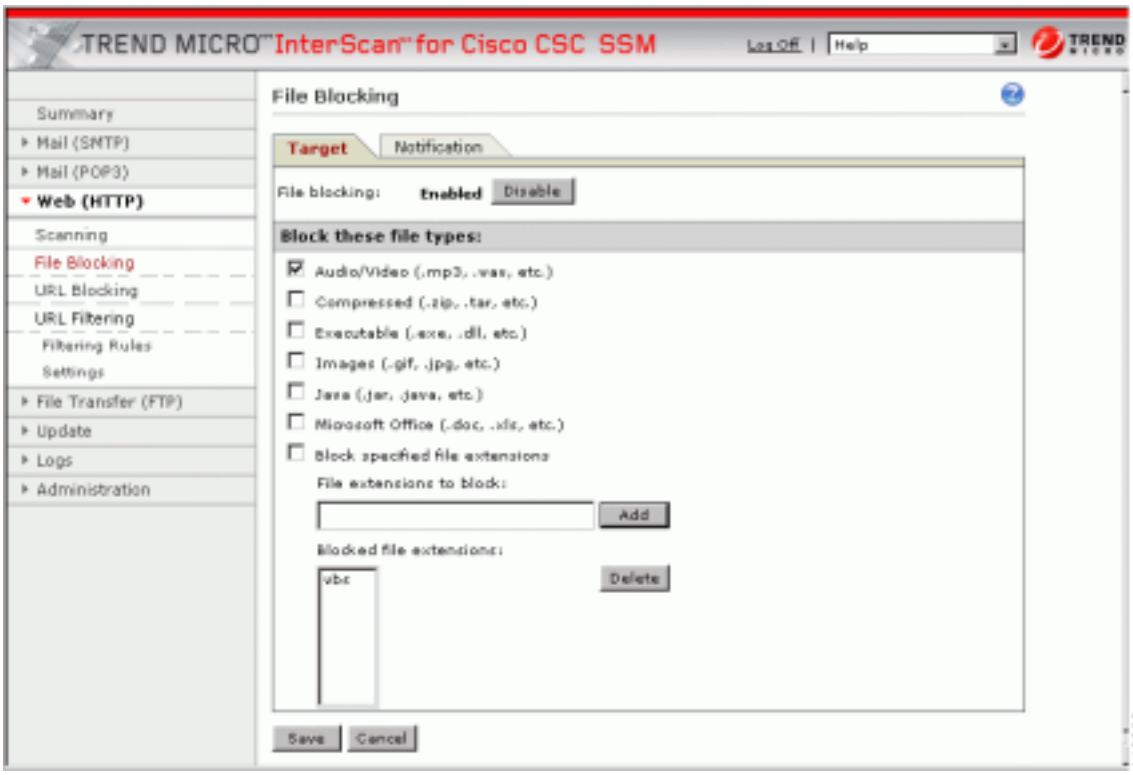
ファイル ブロッキング

この機能はデフォルトでイネーブルになっていますが、ブロックするファイルのタイプを指定するまで、いずれのファイルもブロックされません。ファイル ブロッキングは、勤務時間中のインターネットおよびその他のコンピューティング リソースの使用に関する組織のポリシーを適用するのに役立ちます。たとえば、従業員の生産性のためだけでなく、法律上の問題のために、会社で音楽のダウンロードを禁止しているとします。

HTTP プロトコルを介したダウンロードをブロックするには、ASDM の **Configuration > Trend Micro Content Security > Web** で Configure File Blocking リンクをクリックして、**File Blocking** ウィンドウを表示します。FTP プロトコルを介したダウンロードをブロックするには、ASDM の **Configuration > Trend Micro Content Security > File Transfer** で Configure File Blocking リンクをクリックします。**File Blocking** ウィンドウはどちらのプロトコルの場合も同じです。

File Blocking ウィンドウの **Target** タブで Audio/Video をオンにして音楽ファイルの転送をブロックします。図 4-1 を参照してください。

図 4-1　ファイル ブロッキングのイネーブル化



ファイル名拡張子によって追加のファイル タイプを指定できます。**Block specified file extensions** をオンにして、この機能をイネーブルにします。次に、**File extensions to block** フィールドにファイル タイプを追加し、**Add** をクリックします。例では、.vbs ファイルもブロックされます。

ファイル ブロッキングの詳細、およびブロッキングを停止するファイル拡張子の削除に関する情報については、オンライン ヘルプを参照してください。

File Blocking ウィンドウの **Notifications** タブをクリックすると、ファイル ブロッキング イベントがトリガーされた場合にユーザのブラウザ /FTP クライアントに表示されるデフォルトの通知が表示されます。デフォルトのメッセージを強調表示して上書きすることで、これらのメッセージのテキストをカスタマイズすることができます。管理者に対するオプションの通知を HTTP ファイル ブロッキングで使用できますが、デフォルトではオフになっています。**Send the following message...** チェックボックスをオンにして、通知をアクティブにします。

終了したら、**Save** をクリックして設定をアップデートします。

URL ブロッキング

（注）　この機能には Plus ライセンスが必要です。

URL ブロッキング機能では、社員が禁止されている Web サイトにアクセスするのを防ぐことができます。たとえば、組織のポリシーでデート サービスやオンライン ショッピング サービスの使用、および攻撃的なサイトの閲覧を禁止するために、一部のサイトをブロックすることを想定します。

また、フィッシングなどの詐欺行為を行うことが知られているサイトもブロックします。フィッシングは、犯罪者が使用する手法で、合法的な組織から来たように*見える*電子メール メッセージを送信して、銀行口座番号などの個人情報を提供するようにユーザを誘導します。図 4-2 に、フィッシングに使用される電子メール メッセージの一般的な例を示します。

図 4-2　フィッシングの例

デフォルトでは URL ブロッキングはイネーブルですが、ブロックする追加のサイトを指定するまで、TrendMicro PhishTrap パターン ファイルのサイトのみがブロックされます。

ローカル リストによるブロック

URL ブロッキングを設定するには、次の手順を実行します。

ステップ 1　ASDM の **Configuration > Trend Micro Content Security > Web** で **Configure URL Blocking** をクリックして、**URL Blocking** ウィンドウを表示します。

ステップ 2　**URL Blocking** ウィンドウの **Via Local List** タブで、**Match** フィールドにブロックする URL を入力します。次の項目で指定できます。

- 正確な Web サイト名
- URL キーワード
- 文字列

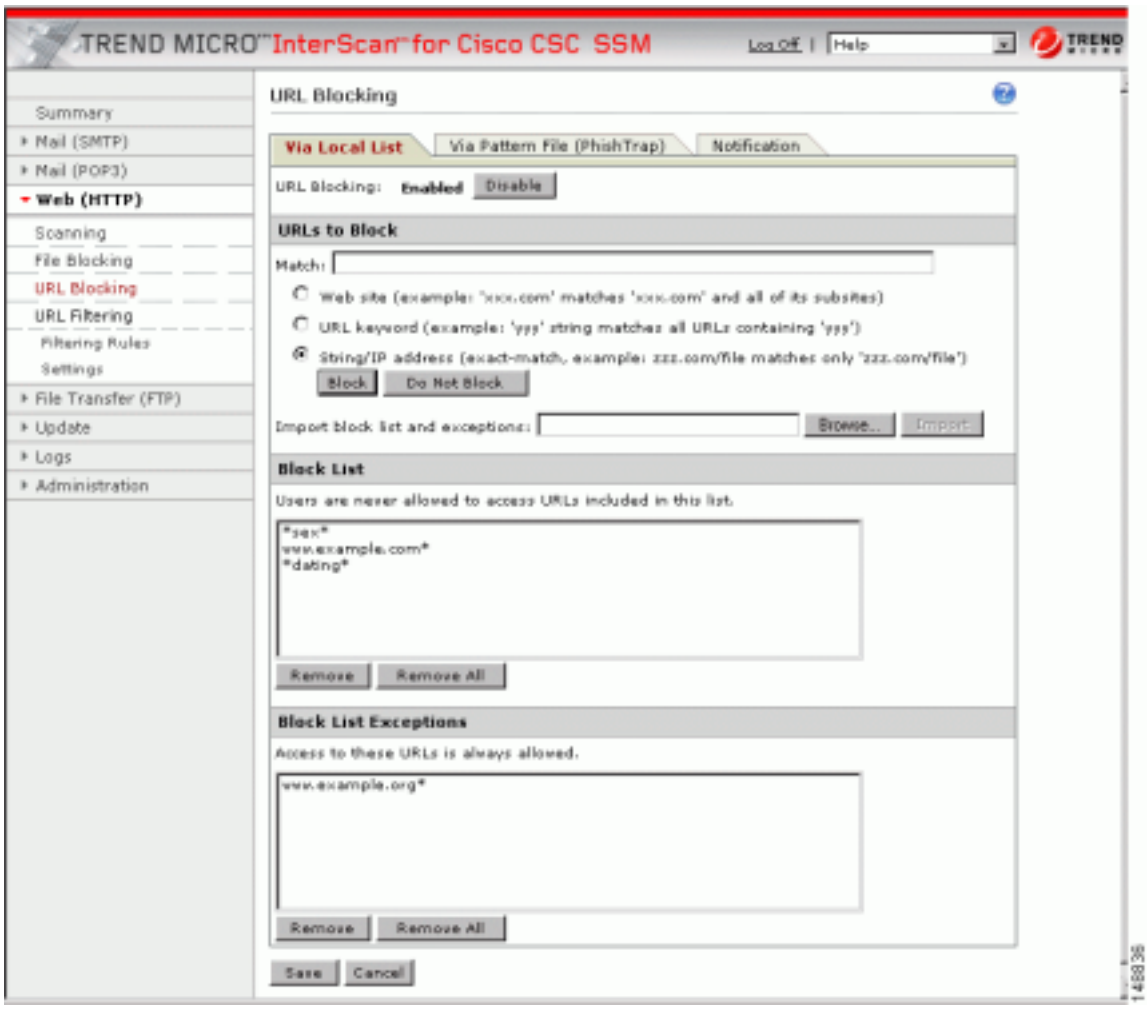
Match フィールドのエントリのフォーマッティングの詳細については、オンライン ヘルプを参照してください。

ステップ 3　エントリを 1 つ入力するたびに **Block** をクリックして、**Block List** に URL を移動します。エントリを例外に指定するには、**Do Not Block** をクリックしてエントリを **Block List Exceptions** に追加します。エントリは削除するまでブロック対象または例外のままです。

（注）　ブロックまたは例外のリストをインポートすることもできます。インポートするファイルは特定のフォーマットである必要があります。方法については、オンライン ヘルプを参照してください。

図 4-3 に、エントリがある **URL Blocking** ウィンドウ（**Via Local List** タブ）の例を示します。

図 4-3　URL ブロッキング ウィンドウ



パターン ファイル（PhishTrap）によるブロッキング

ASDM の **Configuration > Trend Micro Content Security > Web** で Configure URL Blocking リンクをクリックして、**URL Blocking** ウィンドウを表示します。次に、**Via Pattern File (PhishTrap)** タブをクリックします。

デフォルトでは、Trend Micro PhishTrap パターン ファイルは既知のフィッシング サイト、スパイウェア サイト、ウイルス加担サイト（既知の不正利用に関連付けられたサイト）、およびウイルス媒介サイト（悪意の目的のためのみに存在する Web サイト）を検出し、ブロックします。**Submit the Potential Phishing URL to TrendLabs** フィールドを使用して、PhishTrap パターン ファイルに追加する必要があると思われるサイトを送付してください。TrendLabs ではサイトを評価して、そのようなアクションが適切である場合はサイトを追加することがあります。

Notification タブをクリックして、ブロックされているサイトにアクセスしようとした場合にユーザのブラウザに表示される、デフォルトのメッセージのテキストを検討します。オンライン ヘルプに例が示されています。デフォルトのメッセージを強調表示して上書きすることで、テキストをカスタマイズします。

終了したら、**Save** をクリックして設定をアップデートします。

URL フィルタリング

（注）　この機能には Plus ライセンスが必要です。

前述の **URL Blocking** ウィンドウで定義した URL は、常に許可されるか、常に禁止されるかのいずれかです。しかし、URL フィルタリング機能を使用すると、URL をカテゴリで設定し、特定の時間（休憩時間として定義）には許可し、勤務時間中には禁止するようにスケジュールすることができます。

次の 6 つの URL カテゴリがあります。

- Company-prohibited
- Not work related
- Research topics
- Business function
- Customer defined
- Others

デフォルトでは、会社で禁止したサイトは勤務時間と休憩時間の両方でブロックされます。

フィルタリング設定

URL フィルタリング機能を設定するには、次の手順を実行します。

ステップ 1　ASDM の **Configuration > Trend Micro Content Security > Web** で **Configure URL Filtering Settings** をクリックして、**URL Filtering Settings** ウィンドウを表示します。URL Categories タブで、表示されているサブカテゴリおよび各カテゴリに割り当てられたデフォルトの分類を検討して、割り当てが組織に適切かどうかを判断します。たとえば、「Illegal Drugs」は、「Company-prohibited」カテゴリのサブカテゴリです。投資情報サービス会社の場合は、このカテゴリを Company-prohibited に分類したままにすることができます。**Illegal Drugs** チェックボックスをクリックして、違法薬物に関連するサイトのフィルタリングをイネーブルにします。ただし、法執行機関の場合は、「Illegal Drugs」サブカテゴリを「Business function」カテゴリに再分類する必要がある可能性があります。再分類の詳細については、オンライン ヘルプを参照してください。

ステップ 2　サブカテゴリの分類を検討し、調整した後、サブカテゴリのチェックボックスをオンにして、フィルタリングを実行するすべてのサブカテゴリをイネーブルにします。

ステップ 3　イネーブルにしたサブカテゴリの中にフィルタリングを行わないサイトがある場合は、**URL Filtering Exceptions** タブをクリックします。フィルタリングから除外する URL を **Match** フィールドに入力します。次の項目で指定できます。

- 正確な Web サイト名
- URL キーワード
- 文字列

Match フィールドのエントリのフォーマッティングの詳細については、オンライン ヘルプを参照してください。

ステップ 4　エントリを 1 つ入力するたびに **Add** をクリックして、**Do Not Filter the Following Sites** リストに URL を移動します。エントリは削除するまで例外のままです。

（注）　例外のリストをインポートすることもできます。インポートするファイルは特定のフォーマットである必要があります。方法については、オンライン ヘルプを参照してください。

ステップ 5　**Schedule** タブをクリックして、勤務時間と見なす曜日および 1 日の時間を定義します。勤務時間として指定しなかった時間は、自動的に休憩時間として指定されます。

ステップ 6　**Save** をクリックして、URL フィルタリング設定をアップデートします。

Reclassify URL タブをクリックして、不確かな URL を評価するために TrendLabs に送付します。

フィルタリング規則

URL サブカテゴリを、組織に適切なカテゴリ、定義された例外（存在する場合）、および作成された勤務時間 / 休憩時間スケジュールに割り当てた後、カテゴリでフィルタリングを行うタイミングを決定するフィルタリング規則を割り当てます。ASDM の **Configuration > Trend Micro Content Security > Web** で Configure URL Filtering Rules リンクをクリックして、**URL Filtering Rules** ウィンドウを表示します。図 4-4 を参照してください。

図 4-4　URL Filtering Rules ウィンドウ

6 つの主要カテゴリについて、そのカテゴリの URL をブロックするかどうかをそれぞれ指定します。ブロックする場合は、勤務時間、休憩時間、またはその両方を指定します。詳細については、オンライン ヘルプを参照してください。**Save** をクリックして設定をアップデートします。

CHAPTER 5

アップデートおよびログ クエリーの管理

この章では、アップデート、プロキシ設定、syslog 設定、およびログ クエリーについて説明します。この章は、次の項で構成されています。

コンポーネントのアップデート

今や、新しいウイルスやその他のセキュリティ リスクは、インターネットまたは他の配布方法を介して毎日絶え間なく「未開の地」（世界的なコンピューティング コミュニティで悪事をはたらくことを意味します）に送り出されています。TrendLabs はただちに新しい脅威を分析し、ウイルス パターン ファイルなどの新しい脅威の検出に必要なコンポーネントをアップデートする適切な手順を実行します。この迅速な対応によって、たとえば、今日の午前 3 時にアムステルダムで悪意のあるハッカーのコンピュータから新しいワームが送り出されたとしても、Trend Micro InterScan for Cisco CSC SSM は、これを検出することができます。

新しい脅威がネットワークに侵入しないように、コンポーネントを最新の状態に保つことがきわめて重要です。コンポーネントを最新の状態に保つには、次の作業を実行します。

- いつでもオンデマンドでコンポーネントの手動アップデートを実行します
- コンポーネントを定期的に自動でアップデートするアップデート スケジュールを設定します

手動またはスケジュールによって管理されるコンポーネントは次のとおりです。

- ウイルス パターン ファイル
- ウイルス スキャン エンジン
- スパイウェア パターン ファイル（他のタイプのグレーウェアのパターンも含む）
- PhishTrap パターン ファイル
- アンチスパム規則
- アンチスパム エンジン

PhishTrap パターン ファイル、アンチスパム規則、およびアンチスパム エンジンというコンポーネントは、Plus ライセンスを購入されている場合にのみアクティブでアップデートされます。

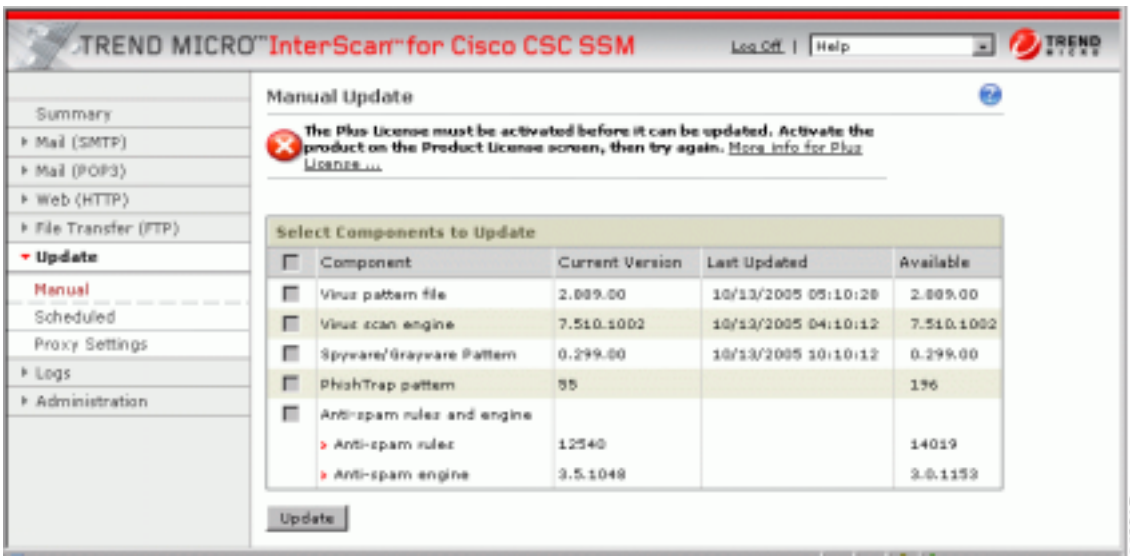
最新のコンポーネントがインストールされているかどうかを確認するには、**Manual Update** ウィンドウに進んでコンポーネントのステータスをチェックします。

（注） CSC SSM ソフトウェアは、スキャン エンジンおよびパターン ファイルのこれらのアップデートのロールバックはサポート*していません*。

手動アップデート

コンポーネントのステータスを表示するには、またはコンポーネントを手動でアップデートするには、**Updates** > **Manual** に進みます。**Manual Update** ウィンドウが表示されます（図 5-1 を参照）。

図 5-1　Manual Update ウィンドウ



ウィンドウの右側にある **Available** カラムをスキャンして、コンポーネントが古くなっているかどうかを即座に確認できます。より新しいコンポーネントを使用できる場合は、コンポーネントのバージョンが赤で表示されます。

たとえば、**Update** をクリックして最新のパターン ファイルのバージョンをダウンロードします。新しいパターン ファイルのダウンロード中は、進捗メッセージが表示されます。アップデートが完了すると、**Manual Update** ウィンドウがリフレッシュされ、最新のアップデートが適用されたことが表示されます。

この機能の詳細については、オンライン ヘルプを参照してください。

スケジュール アップデート

Scheduled Update ウィンドウでは、コンポーネントの更新を 15 分ごとに行うように設定できます。**Updates** > **Scheduled** と進んで、**Scheduled Update** ウィンドウを表示します。アップデート スケジュールごとにアップデートするコンポーネントを選択します。

スケジュールをそのままにするか、頻度を変更します。詳細については、オンライン ヘルプを参照してください。**Save** をクリックして、設定をアップデートします。

プロキシ設定

Trend Micro ActiveUpdate サーバとの通信にプロキシ サーバを使用している場合は、インストール時にプロキシ サーバの IP とポートを指定しています。**Update** > **Proxy Settings** をクリックすると、**Proxy Settings** ウィンドウにこれらの設定が表示されます。図 5-2 を参照してください。

図 5-2　プロキシ設定ウィンドウ

インストール時にプロキシを設定する場合、デフォルトで HTTP プロキシ プロトコルが設定されます。SOCKS4 に変更するには、**SOCKS4** オプション ボタンをクリックします。詳細については、オンライン ヘルプを参照してください。

このウィンドウで可能なその他の変更としては、オプションのプロキシ認証ユーザ名とパスワードを **User ID** および **Password** フィールドに追加することに限られます。終了したら、**Save** をクリックして設定をアップデートします。

Syslog 設定

インストール後に、ウイルスまたはスパイウェア / グレーウェアの検出などのログ データが一時的に保存されます。ログ データを格納するには、少なくとも 1 台（最大 3 台）の syslog サーバを設定します。**Logs** > **Settings** と進んで、**Log Settings** ウィンドウを表示します。

少なくとも 1 台の syslog サーバを設定します。**Enable** チェックボックスをオンにし、次に syslog サーバの IP、ポート、および優先プロトコル（UDP または TCP）を入力します。詳細については、オンライン ヘルプを参照してください。

デフォルトでは、検出されたセキュリティ リスクがロギングされます。使用していない機能のロギングをオフにすることができます。たとえば、Plus ライセンスを購入していない場合は、URL ブロッキング / アンチフィッシングおよび URL フィルタリングをオフにすることができます。

ログ データの選択と表示の詳細については、P.5-5 の「ログ データの表示」を参照してください。syslogs は ASDM から表示することもできます。詳細については、ASDM のオンライン ヘルプを参照してください。

ログ データの表示

Trend Micro InterScan for Cisco CSC SSM をインストールして設定した後、セキュリティ リスクが検出され、それぞれのリスクのタイプに対して選択したアクションに従って処理されます。これらのイベントはログに記録されます。システム リソースを節約するため、これらのログは定期的に消去される場合があります。

ログを表示するには、**Logs** > **Query** と進んで **Log Query** ウィンドウを表示します。問い合せパラメータを指定し、**Display Log** をクリックしてログを表示します。詳細については、オンライン ヘルプを参照してください。

図 5-3 に、スパイウェア / グレーウェアのログの例を示します。

図 5-3　スパイウェア / グレーウェアのログ

スキャン パラメータの例外のロギング

Target タブで指定する次のスキャン パラメータの例外がウイルス / マルウェア ログに表示されます。

SMTP、POP3、HTTP および FTP の場合は、次のとおりです。

- 圧縮解除時に、指定したファイル数制限を越える圧縮ファイル
- 圧縮解除時に、指定したファイル サイズ制限を越える圧縮ファイル
- 圧縮レイヤ数が制限を越える圧縮ファイル
- 圧縮比率の制限を超える圧縮ファイル（圧縮解除されたファイルのサイズは圧縮ファイルのサイズの「x」倍）
- パスワード保護されたファイル（削除に対して設定されている場合）

HTTP および FTP のみの場合は、次のとおりです。

- スキャンを行うには大きすぎるファイルまたはダウンロード

これらのファイルは、ウイルス / マルウェア名の代わりに次のようなメッセージで示されます。

- Decompressed_File_Size_Exceeded
- Large_File_Scanning_Limit_Exceeded

CHAPTER 6

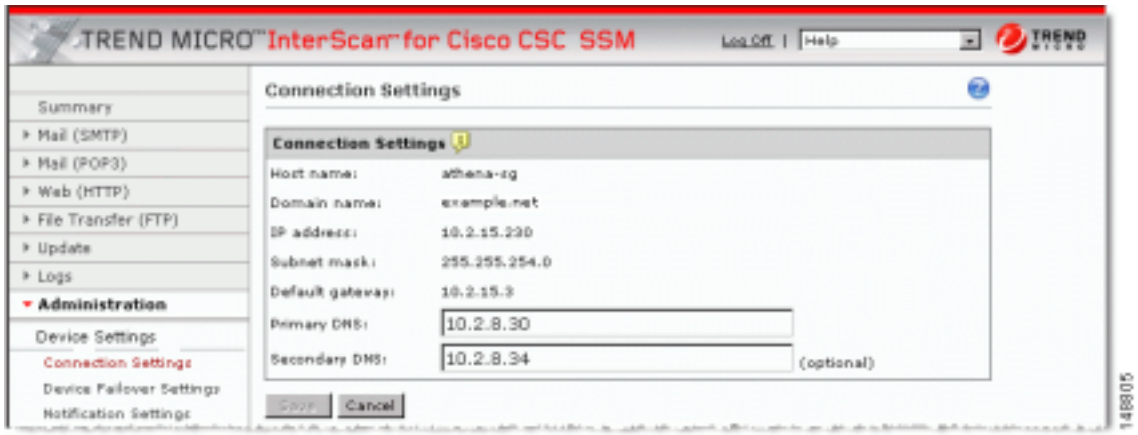
Trend Micro InterScan for Cisco CSC SSM の管理

この章では、パッチのインストールなど実行頻度が少ないタスクについて説明します。この章は、次の項で構成されています。

接続設定

ネットワークの接続設定を表示するには、**Administration > Device Settings > Connection Settings** を選択します。**Connection Settings** ウィンドウ（図 6-1 を参照）に、インストール時に行った選択が表示されます。

図 6-1　Connection Settings ウィンドウ



この画面では、**Primary DNS** および **Secondary DNS** の IP アドレス フィールドを変更することができます。ホスト名、ドメイン名、または IP アドレスなど、その他の接続設定を変更するには、**Configuration > Trend Micro Content Security** と進み、メニューから **CSC Setup** を選択します。

これらの設定は、コマンドライン インターフェイス（CLI）を使用して変更することもできます。CLI にログインし、**session 1** コマンドを発行します。CLI に初めてログインする場合は、デフォルトのユーザ名（cisco）とパスワード（cisco）を使用します。パスワードを変更するよう求められます。

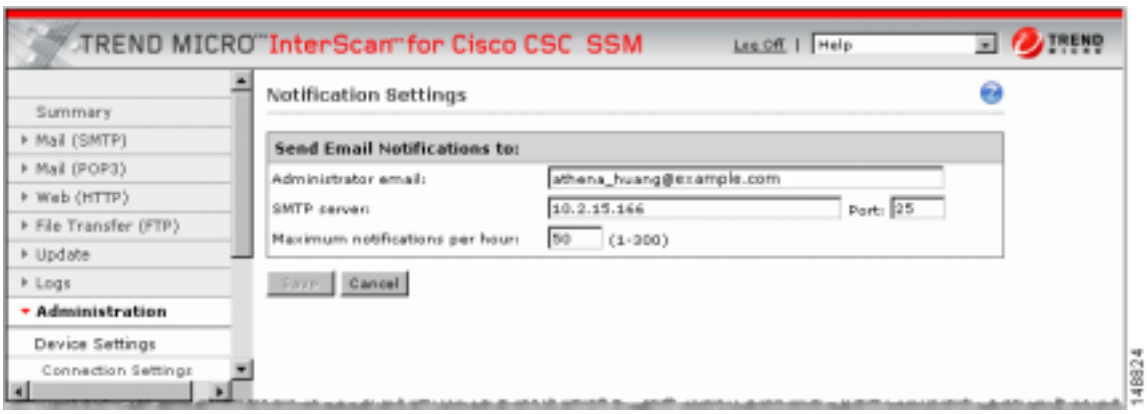
ログインした後、Trend Micro InterScan for Cisco CSC SSM Setup Wizard メニューからオプション **1** の Network Settings を選択します。プロンプトに従って設定を変更します。詳細については、P.A-6 の「インストールの手順」を参照してください。

管理電子メールおよび通知の設定の管理

Notification Settings ウィンドウ（図 6-2 を参照）では、次の作業を行うことができます。

- インストール時に（**Host Configuration** ウィンドウで）選択した管理者電子メール アドレスの表示または変更（あるいはその両方）
- インストール時に（**Host Configuration** ウィンドウで）選択した SMTP サーバの IP およびポートの表示
- 1 時間あたりの管理者通知の最大数の設定

図 6-2　Notification Settings ウィンドウ



このウィンドウで変更を行うには、新しい情報を入力し、**Save** をクリックします。

これらの変更は、ASDM で **Configuration > Trend Micro Content Security** を選択した後、メニューから **CSC Setup** を選択して行うこともできます。

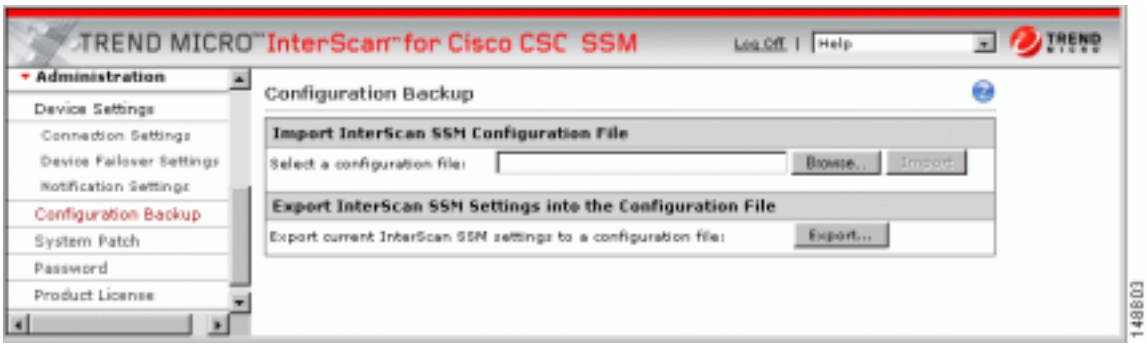
コンフィギュレーションのバックアップの実行

Trend Micro InterScan for Cisco CSC SSM には、デバイスのコンフィギュレーションをバックアップして圧縮ファイルに保存する機能があります。保存したコンフィギュレーションをインポートし、システムを保存時の設定に復元することができます。

(注)　ASDM/Web GUI パスワードを忘れた場合、コンフィギュレーションのバックアップはリカバリにきわめて重要です。詳細については、P.8-7 の「失ったパスワードの回復」を参照してください。

前の章の手順に従って Trend Micro InterScan for Cisco CSC SSM の設定が終了したら、すぐにコンフィギュレーションのバックアップを実行してください。**Administration > Configuration Backup** と進んで、**Configuration Backup** ウィンドウを表示します。図 6-3 を参照してください。

図 6-3　Configuration Backup ウィンドウ



コンフィギュレーションのエクスポート（保存）

Export をクリックして、コンフィギュレーション設定を保存します。**File Download** ダイアログボックスが表示されます。デフォルトで config.tgz という名前のファイルを開くか、ファイルをコンピュータに保存することができます。

コンフィギュレーションのインポート

保存したコンフィギュレーション ファイルを復元するには、**Configuration Backup** ウィンドウで、**Browse** をクリックします。config.tgz ファイルを見つけて、**Import** をクリックします。ファイル名が **Select a configuration file** フィールドに表示されます。保存されていたコンフィギュレーション設定がアプライアンスに復元されます。

保存されていたコンフィギュレーション ファイルをインポートすると、スキャン サービスが再開されます。たとえば、**Summary** ウィンドウのカウンタがリセットされることに注意する必要があります。

フェールオーバーの設定

Trend Micro InterScan for Cisco CSC SSM には、ASA のデバイス フェールオーバー機能をサポートして、コンフィギュレーションをピア装置に複製する機能があります。ピア装置または CSC SSM をフェールオーバー デバイスに設定する前に、まずプライマリ デバイスの設定を終了します。つまり、スパイウェア / グレーウェア スキャンをイネーブルにし、通知をカスタマイズする予定がある場合は、カスタマイズするなどです。

プライマリ デバイスが必要な動作を行うように設定したら、次のチェックリストの手順を実行して、フェールオーバー ピアを設定します。チェックリストを印刷して、進捗に応じて手順を記録するのに使用します。

手順	フェールオーバー設定のチェックリスト	確認チェック
1	プライマリ デバイスとして動作するアプライアンス、およびセカンダリ デバイスとして動作させるアプライアンスを決定します。ここにそれぞれの IP アドレスを記録します。 **メモ：** _____ _____	❑ ❑
2	ブラウザのウィンドウを開き、次の URL を **Address** フィールドに入力します。http://<primary device IP address>:8443。**Logon** ウィンドウが表示されます。ログインして、**Administration > Device Settings > Device Failover Settings** と移動します。	❑
3	2 番目のブラウザのウィンドウを開き、次の URL を **Address** フィールドに入力します。http://<secondary device IP address>:8443。ステップ 2 では、ログインして **Device Failover Settings** ウィンドウに移動します。	❑
4	プライマリ デバイスの **Device Failover Settings** ウィンドウで、セカンダリ デバイスの IP アドレスを **Peer IP address** フィールドに入力します。1 ～ 8 文字の英数字の暗号キーを **Encryption key** フィールドに入力します。**Save** をクリックし、次に **Enable** をクリックします。ウィンドウ タイトルの下に次のメッセージが表示されます。 **`InterScan for CSC SSM could not establish a connection because the failover peer device is not yet configured. Please configure the failover peer device, then try again.`** このメッセージは正常で、ピアがまだ設定されていないために表示されます。この時点ではこのメッセージに注意する必要はありません。	❑
5	セカンダリ デバイスの **Device Failover Settings** ウィンドウで、プライマリ デバイスの IP アドレスを **Peer IP address** フィールドに入力します。1 ～ 8 文字の英数字の暗号キーを **Encryption key** フィールドに入力します。暗号キーは、プライマリ デバイスに入力したキーと同じにする必要があります。**Save** をクリックし、次に **Enable** をクリックします。ウィンドウ タイトルの下に次のメッセージが表示されます。 **`InterScan for CSC SSM has successfully connected with the failover peer device.`** *この時点ではセカンダリ デバイスで他の操作をしないでください。*	❑

手順	フェールオーバー設定のチェックリスト	確認チェック
6	プライマリ デバイスの **Device Failover Settings** ウィンドウに戻り、**Synchronize with peer** をクリックします。	❑
7	ウィンドウの下部にある **Status** フィールドのメッセージは、次のように同期化の日時を表示するはずです。 `Status: Last synchronized with peer on: 09/29/2005 15:20:11`	❑

注意　ステップ 5 の最後で、セカンダリ デバイスの **Device Failover Settings** ウィンドウがまだ表示されている間は、絶対に **Synchronize with peer** をクリックしないでください。クリックした場合、プライマリ デバイスですでに設定したコンフィギュレーションが消去されます。ステップ 6 の手順に従って、プライマリ デバイスから手動で同期化を実行する必要があります。

チェックリストの手順を完了すると、フェールオーバー関係が正常に設定されています。

将来コンフィギュレーションを変更する場合、たとえば、スパム フィルタリングしきい値を Low から Medium に変更する場合は、プライマリ デバイスのみでコンフィギュレーションを変更する必要があります。Trend Micro InterScan for Cisco CSC SSM はコンフィギュレーションのミスマッチを検出し、最初のデバイスで行ったコンフィギュレーションの変更でピアをアップデートします。

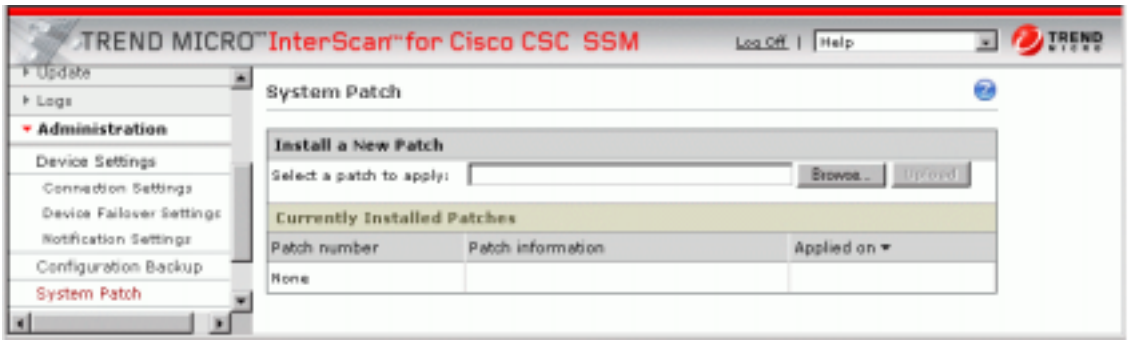
自動同期化機能の例外は、システム パッチのアップロードです。パッチは、プライマリ デバイスとセカンダリ デバイスの両方に適用する必要があります。詳細については、P.6-7 の「システム パッチのインストール」を参照してください。

何らかの理由でピア デバイスを使用できない場合は、電子メール通知が管理者に送信されます。ピアの問題が解決されるまでメッセージは定期的に送信され続けます。

システム パッチのインストール

既知の問題を修正するシステム パッチ、または新しい機能を提供するシステム パッチが、必要に応じ利用可能になります。まず Web サイトまたは提供された CD からシステム パッチをダウンロードしてから、**Administration > System Patch** と進んで **System Patch** ウィンドウを表示します。図 6-4 を参照してください。

図 6-4　System Patch ウィンドウ



注意　パッチ アプリケーションはシステム サービスを再開始し、システムの運用を中断する場合があります。デバイスの動作中にシステムにパッチを適用すると、ウイルスやマルウェアが含まれているトラフィックにネットワークの通過を許可することがあります。

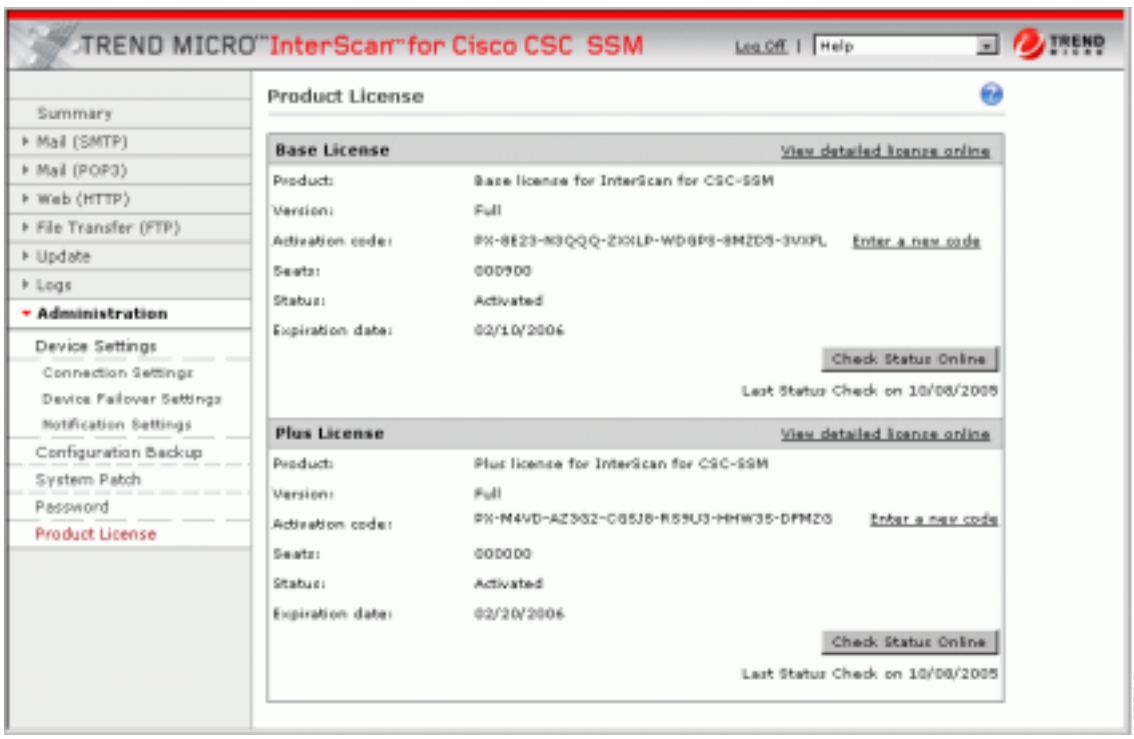
システム パッチの適用と削除の詳細については、このウィンドウのオンライン ヘルプを参照してください。

製品ライセンスの表示

Product License ウィンドウ（図 6-5 を参照）では、製品ライセンスの次の項目のステータスを確認することができます。

- 有効なライセンス（Base ライセンスのみ、または Base ライセンスと Plus ライセンス）
- ライセンスのバージョン（一時的に「Evaluation」コピーを使用している場合を除き、「Full」を示している必要があります）
- ライセンスのアクティベーション コード
- ライセンス許諾数（ユーザ）：この情報は、Plus ライセンスを購入した場合にも、Base ライセンスに対してのみ表示されます。
- ステータス。「Activated」である必要があります。
- ライセンスの有効期限：Base ライセンスと Plus ライセンスの両方がある場合、有効期限が異なる場合があります。

図 6-5　Product License ウィンドウ



ライセンスが更新されなかった場合、アンチウイルス スキャンは、期限切れに短い猶予期間を加えた時点で有効だったパターン ファイルのバージョン、およびスキャン エンジンで続行されます。しかし、その他の機能は使用できなくなる場合があります。詳細については、ライセンスの有効期限の項を参照してください。

ライセンスの有効期限

有効期限に近づいたとき、および有効期限を過ぎたとき、ウィンドウ ヘッダーの下の **Summary** ウィンドウに、図 6-6 の例に示すようなメッセージが表示されます。

図 6-6　ライセンスの有効期限のメッセージ

製品ライセンスの期限が切れた場合、Trend Micro InterScan for Cisco CSC SSM を継続して使用できますが、（ウイルス パターン ファイル、スキャン エンジンなどの）アップデートを受け取ることはできません。ネットワークは新しいセキュリティ上の脅威に対して保護されなくなる場合があります。

Plus ライセンスの期限が切れた場合、コンテンツ フィルタリングおよび URL フィルタリングは使用できなくなります。その場合、トラフィックはコンテンツまたは URL のフィルタリングなしで通過します。

Base ライセンスを購入してインストールした後に Plus ライセンスを購入した場合は、期限の期日が異なります。更新日が近づいたときに各ライセンスを別々に更新することができます。

ライセンス情報リンク

Product License ウィンドウには複数の役立つリンクがあります。リンクは次のとおりです。

- View detailed license online
- Check Status Online

View detailed license online リンクでは、Trend Micro オンライン登録 Web サイトにアクセスしてライセンスに関する情報を表示し、更新の方法を知ることができます。**Check Status Online** では、**Product License** ウィンドウのタイトルの下に、前の図の例と同様のライセンスのステータスを示すメッセージが表示されます。

詳細については、**Product License** ウィンドウのオンライン ヘルプを参照してください。

■　製品ライセンスの表示

CHAPTER 7

コンテンツ セキュリティのモニタリング

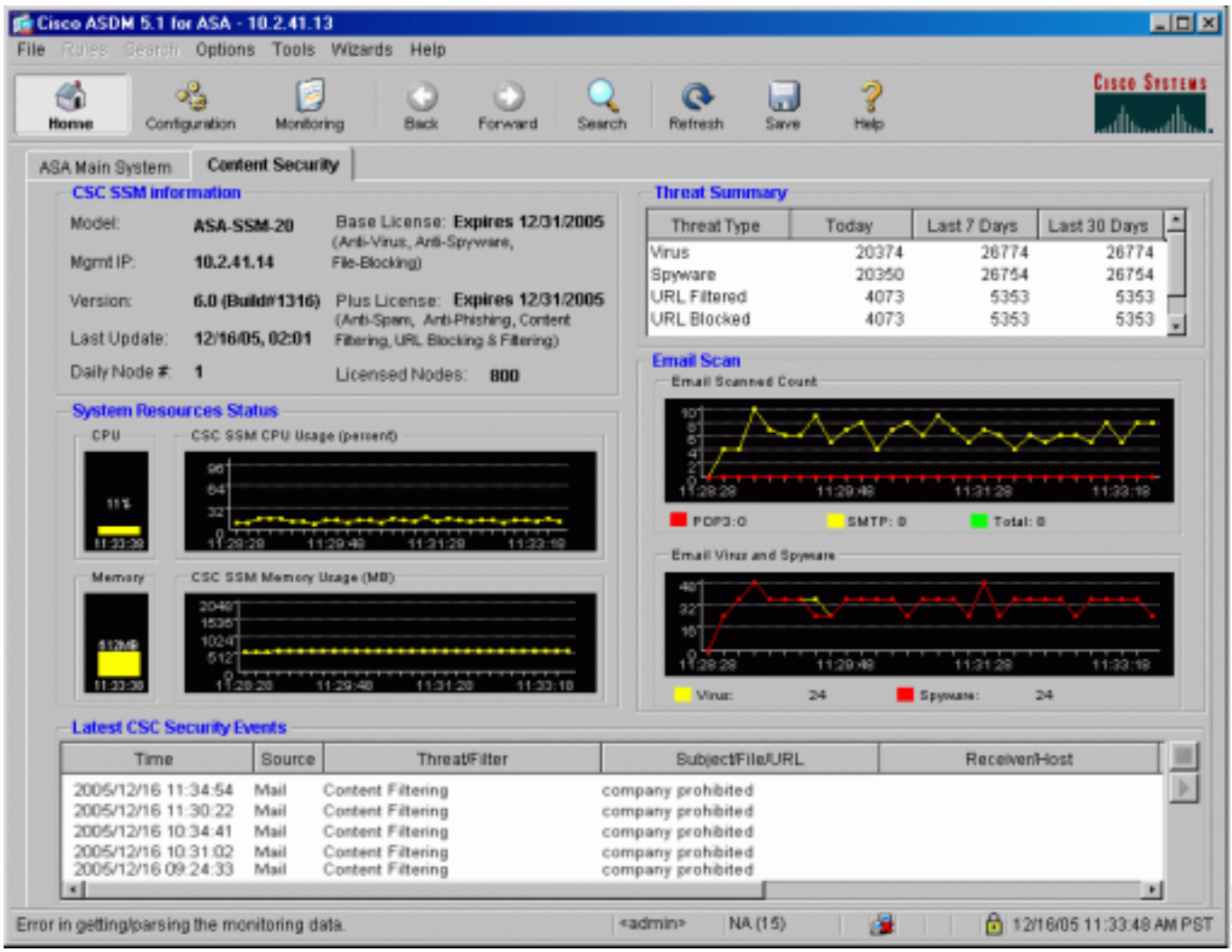
この章では、ASDM のコンテンツ セキュリティについて説明します。次の項で構成されています。

Content Security タブの機能

CSC SSM に接続すると、図 7-1 に示すように、Content Security タブが表示されます。Content Security タブでは、次のコンテンツ セキュリティ ステータスを一目で確認することができます。

- CSC SSM Information：製品モデル番号、デバイスの IP アドレス、CSC SSM ソフトウェアのバージョンおよびビルド番号、重要な通知情報
- Threat Summary：検出された脅威の当日、7 日、30 日ごとの検出数を表形式で表示
- System Resources Status：SSM の CPU およびメモリの使用状況の確認が可能
- Email Scan：スキャンされた電子メールの数およびスキャンした電子メールで検出された脅威の数をグラフィックで表示
- Latest CSC Security Events：最近ログに記録されたセキュリティ イベント 25 個をリスト表示

図 7-1　Content Security タブ



Help アイコンをクリックすると、このウィンドウに表示された情報の詳細が表示されます。

コンテンツ セキュリティのモニタリング

Monitoring > Trend Micro Content Security の順にクリックして、モニタリングのオプションを表示します。次のオプションがあります。

- Threats：最近検出された脅威をもたらすアクティビティを、後述のカテゴリ別にグラフで表示します。
- Live Security Events：モニタリング対象プロトコルで最近検出された、セキュリティ イベント（コンテンツフィルタリング違反、スパム、ウィルス検出、スパイウェア検出など）のレポートを表示します。
- Software Updates：コンテンツのセキュリティをスキャンする各種コンポーネント（ウィルス パターン ファイル、スキャン エンジン、スパイウェア / グレイウェア パターンなど）の、バージョンおよび最近のアップデート日時 / 時刻を表示します。
- Resource Graphs：SSM の CPU 使用状況とメモリの使用状況をグラフで表示します。

図 7-2 に、ASDM の Monitoring オプションの表示画面を示します。

図 7-2　ASDM のコンテンツ セキュリティの Monitoring オプション

脅威のモニタリング

Monitoring ペインで Threats をクリックすると、図 7-2 に示すように、最大 4 種類のグラフ表示用のカテゴリから選択できます。次のカテゴリ別に、最新アクティビティの件数を表示することができます。

- 検出されたウィルスおよび他の脅威
- ブロックされたスパイウェア
- 検出されたスパム（この機能を使用するには Plus ライセンスが必要です）
- URL フィルタリング アクティビティ、および URL ブロッキング アクティビティ（この機能を使用するには Plus ライセンスが必要です）

たとえば、Base と Plus の両方のライセンスがある場合は、上記の 4 種類すべての脅威タイプのモニタリングを選択できます。図 7-3 に、グラフの表示例を示します。

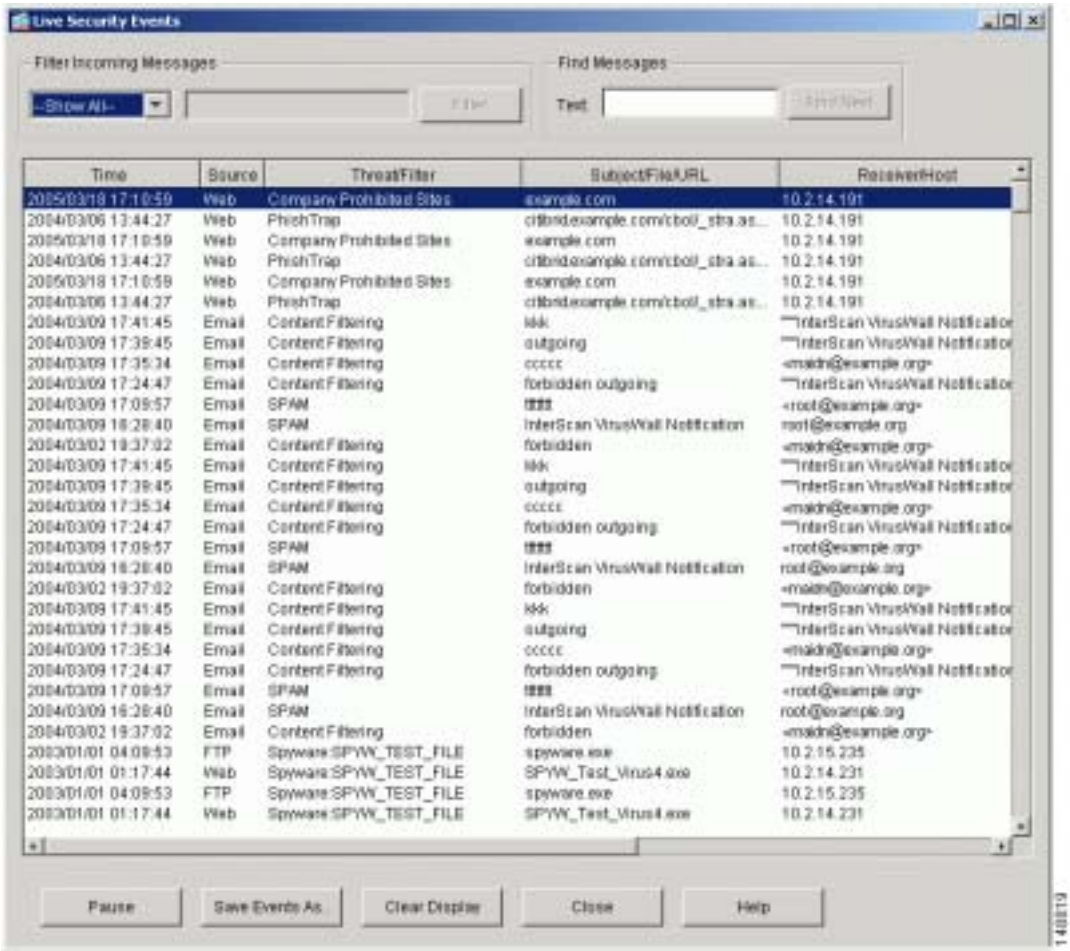
図 7-3　脅威のモニタリング グラフ

グラフは一定の時間間隔（通常は 10 秒）でリフレッシュされるため、最新のアクティビティが一目で分かります。詳細については、オンライン ヘルプを参照してください。

セキュリティ イベントのライブによるモニタリング

Monitoring ペインで Live Security Events をクリックして、**View** をクリックすると、図 7-4 のようなレポートが作成されます。

図 7-4　Live Security Events モニタリング レポート

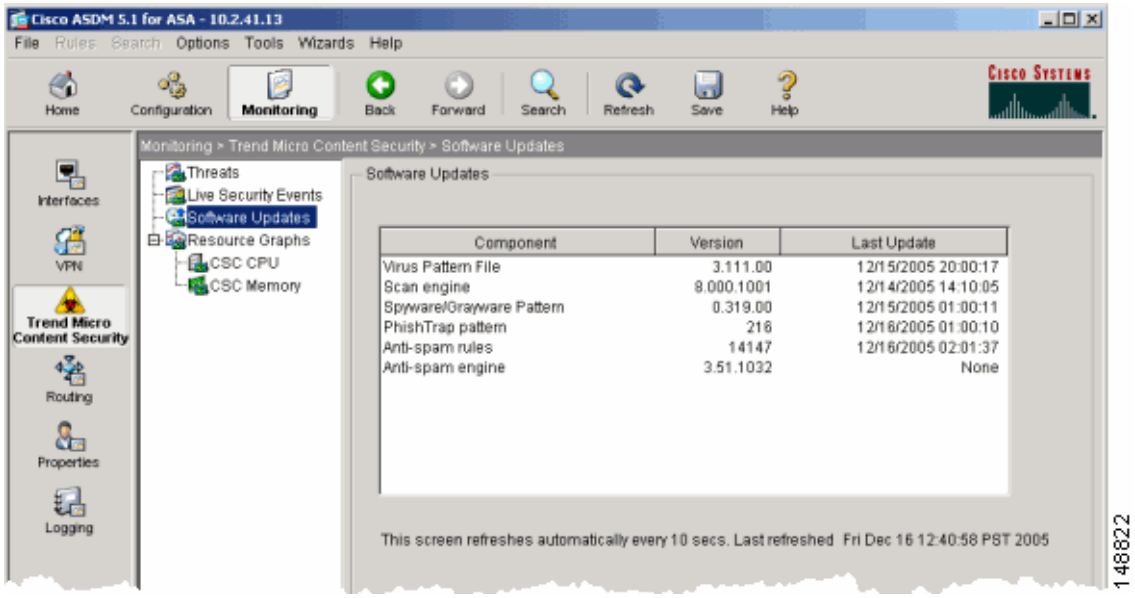


このレポートには、CSC SSM で検出されたすべてのイベントがリスト表示されます。**Source** カラムでは、検出ソースが SMTP と POP3 の両プロトコルの場合は「Email」と表示されます。縦横のスクロール バーで、画面に表示されなかった追加部分のレポート内容が確認できます。画面上部でフィルタリングを行うと、特定のイベントが検索されるように調整できます。詳細については、オンライン ヘルプを参照してください。

ソフトウェアのアップデートのモニタリング

図 7-5 のように、Monitoring ペインで Software Updates をクリックすると、CSC SSM のコンポーネントに関する情報が次のように表示されます。

図 7-5　Software Updates モニタリング ウィンドウ



ASDM で **Monitoring** > **Trend Micro Content Security** > **Software Updates** の順にクリックすると表示される、**Configure Updates** リンクをクリックすると、Scheduled Update ウィンドウが CSC SSM コンソールに表示されます。図 2-4（P.2-5）を参照してください。

Scheduled Update ウィンドウでは、CSC SSM が Trend Micro ActiveUpdate サーバからコンポーネントのアップデートを受信する間隔を、1 日、1 時間、または 15 分から選択して指定できます。

SCS SSM コンソールの Manual Update ウィンドウでは、オンデマンドでコンポーネントを手動アップデートすることもできます。図 5-1（P.5-3）を参照。いずれのアップデートについても、詳細はオンラインヘルプを参照してください。

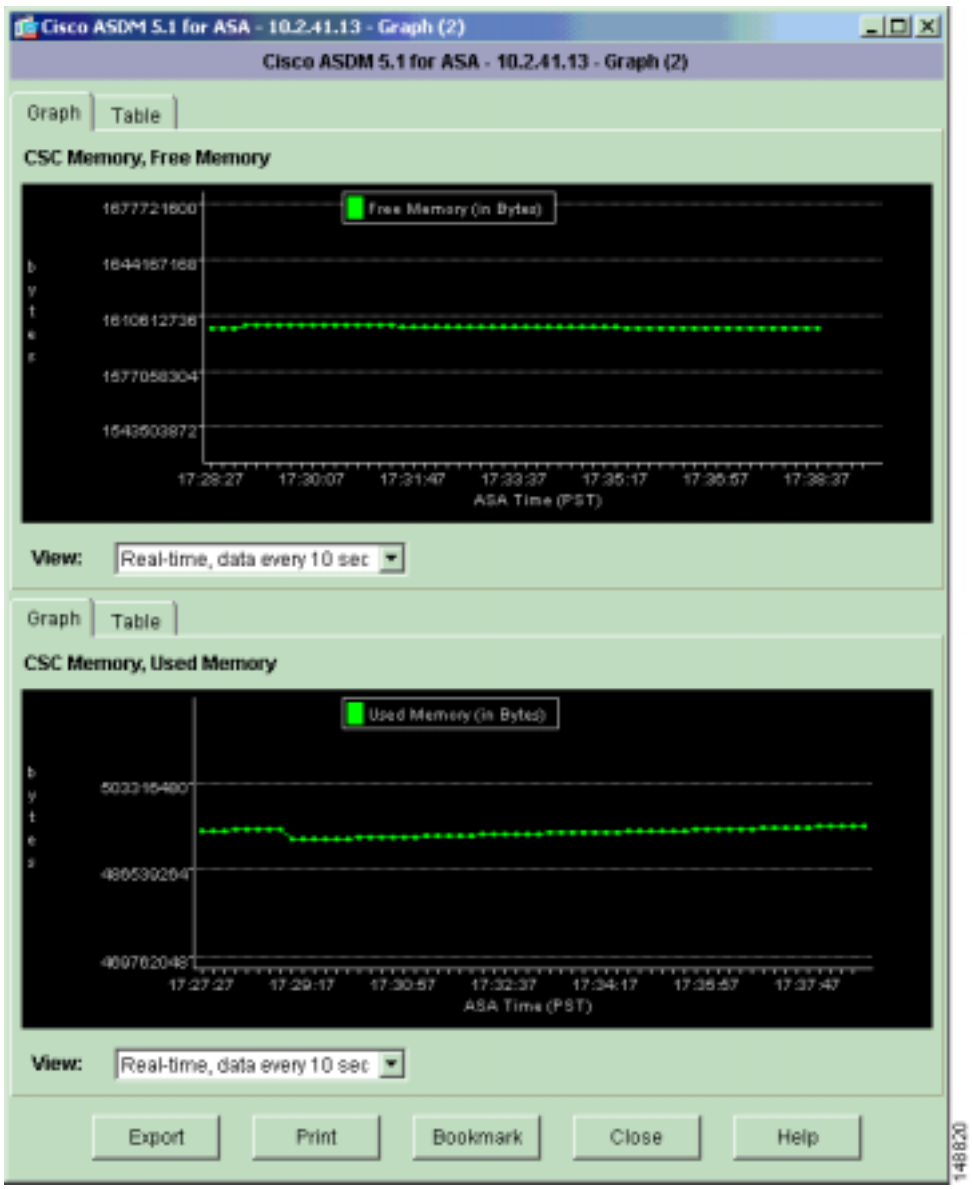
リソースのモニタリング

Monitoring ペインで Resource Graphs をクリックすると、モニタリング可能な 2 種類のリソースである、CPU 使用状況とメモリが表示されます。これらのリソースの使用状況が 100% に近いと表示された場合は、次のいずれかを推奨します。

- ASA-SSM-20 にアップグレードする（現在 ASA-SSM-10 を使用している場合）、または
- 他の ASA アプライアンスを購入する

CPU またはメモリの使用状況を表示するには、表示する情報の種類を選択してから **Show Graphs** をクリックします。次に例を示します。

図 7-6　メモリ モニタリング グラフ



CHAPTER 8

Trend Micro InterScan for Cisco CSC SSM のトラブルシューティング

この章では、サポートについて TAC にお問い合わせになる前に、潜在的な問題を解決するための有益な情報を提供します。次の項で構成されています。

インストール時のトラブルシューティング

次に、インストールを正しく実行するためのコマンドライン バージョンについて説明します。インストール中に問題が発生した場合は、P.8-6 の「インストールに失敗した場合の対処法」を参照してください。

コマンドライン インターフェイスを通じて CSC SSM をインストールするには、次の手順を実行します。

ステップ 1　コマンドライン プロンプトから次のように入力してインストールを開始します。

```
hostname# hw-module module 1 recover configure
```

次のような出力が表示されます。

```
Image URL [tftp://171.69.1.129/dqu/sg-6.0-1345-tftp.img]:
Port IP Address [30.0.0.3]:
VLAN ID [0]:
Gateway IP Address [30.0.0.254]:
hostname# hw-module module 1 recover boot

The module in slot 1 will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
Recover issued for module in slot 1
hostname#
hostname# debug module-boot
debug module-boot  enabled at level 1
```

ステップ 2　約 1 分後に、CSC-SSM の ROMMON が実行され、次のようなメッセージが出力されます。

```
hostname# Slot-1 206> Cisco Systems ROMMON Version (1.0(10)0) #0: Sat Mar 26 00:13:50
PST 2005
Slot-1 207>     morlee@bowmore:/pixab/biosbuild/1.0.10.0/boot/rommon
Slot-1 208> Platform ASA-SSM-AIP-10-K9
Slot-1 209> GigabitEthernet0/0
Slot-1 210> Link is UP
Slot-1 211> MAC Address: 000b.fcf8.01b3
Slot-1 212> ROMMON Variable Settings:
Slot-1 213>   ADDRESS=30.0.0.3
Slot-1 214>   SERVER=171.69.1.129
Slot-1 215>   GATEWAY=30.0.0.254
Slot-1 216>   PORT=GigabitEthernet0/0
Slot-1 217>   VLAN=untagged
Slot-1 218>   IMAGE=dqu/sg-6.0-1345-tftp.img
Slot-1 219>   CONFIG=
Slot-1 220>   LINKTIMEOUT=20
Slot-1 221>   PKTTIMEOUT=2
Slot-1 222>   RETRY=20
Slot-1 223> tftp dqu/sg-6.0-1345-tftp.img@171.69.1.129 via 30.0.0.254
```

ステップ 3　SSM は、イメージをダウンロードするために TFTP サーバに接続を試みます。数分後に、次のような出力が表示されます。

```
Slot-1 224>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 225>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 226>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 227>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 228>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
. . . [ output omitted ]. . .
Slot-1 400>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 401>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 402>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 403>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 404>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 405> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 406> Received 59501255 bytes
```

ステップ 4　TFTP のダウンロードが終了します。受信したバイト数に注意してください。このバイト数はユーザの CSC SSM イメージと同じサイズになるはずです。次に、ROMMON がこのイメージを起動します。

```
Slot-1 407> Launching TFTP Image...
```

ステップ 5　イメージが解凍され、インストールされます。数分すると、CSC SSM がリブートします。次のようなメッセージが表示されます。

```
Slot-1 408> Cisco Systems ROMMON Version (1.0(10)0) #0: Sat Mar 26 00:13:50 PST 2005
Slot-1 409>     morlee@bowmore:/pixab/biosbuild/1.0.10.0/boot/rommon
Slot-1 410> Platform ASA-SSM-AIP-10-K9
Slot-1 411> Launching BootLoader...
```

ステップ 6　1、2 分後に、CSC SSM がブートします。システムのブート時に次のように表示されることを確認してください。

```
hostname# show module 1
```

次のような出力が表示されます。

```
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  1 ASA 5520/5530 AIP Security Service Module-10 ASA-SSM-AIP-10-K9  P00000000TT

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  1 000b.fcf8.01b3 to 000b.fcf8.01b3  1.0          1.0(10)0     CSC SSM 6.0
(Build#1345)

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 CSC SSM                        Down             6.0 (Build#1345)

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  1 Up                 Up
```

Mod Status テーブル（出力の最終行）に「Up」というインスタンスが 2 つ表示されているかどうか検索してください。SSM Application Name テーブルの Status フィールドに「Down」と表示されている場合は、カードがまだアクティブ化されていないことを示しています。

インストールに失敗した場合の対処法

表 8-1 に、P.8-3 の「インストール時のトラブルシューティング」で説明したインストールに失敗した場合の対処法を手順別に示します。

表 8-1　インストールに失敗した場合の対処法

インストールの失敗が発生した手順	処置
ステップ 2	Cisco TAC にお問い合せください。
ステップ 3	1. ユーザの TFTP サーバが CSC SSM と同じ IP サブネットにある場合は、ゲートウェイの IP アドレスを 0.0.0 に設定したことを確認してください。 2. ルータまたはファイアウォールが CSC SSM とユーザの TFTP サーバとの間に存在する場合は、これらのゲートウェイで UDP ポート 69 を介して TFTP トラフィックが通過できることを確認してください。また、該当するルータがこれらのゲートウェイに正しく設定されていることも確認します。 3. イメージ パスが TFTP サーバ上に存在し、ディレクトリとファイルがすべてのユーザから読み取り可能であることを確認します。
ステップ 4	ダウンロードされた合計バイト数を確認します。このバイト数が CSC SSM イメージのサイズと異なる場合は、ユーザの TFTP サーバがイメージのサイズをサポートしていない可能性があります。この場合は、別の TFTP サーバを使用してください。
ステップ 5	イメージを再びダウンロードし、再度インストールします。2 度目もインストールできなかった場合は、Cisco TAC にお問い合わせください。
ステップ 6	イメージを再びダウンロードし、再度インストールします。2 度目もインストールできなかった場合は、Cisco TAC にお問い合わせください。

アクティベーションのトラブルシューティング

すべての処置を講じる前に、ASA にクロックが正しく設定されていることを確認してください。詳細については、『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および ASDM のオンライン ヘルプを参照してください。

次に、**show module**、**show module 1**、および **show module 1 details** コマンドを使用して CSC SSM のアクティブ化が正しく実行されていることを確認してください。これらのコマンドの出力を使用しても問題を解決できない場合は、Cisco TAC にお問い合わせください。

基本機能のトラブルシューティング

次の項では、ログオンまたはパスワードの回復といった、基本機能で発生する可能性のある問題の対処法について説明します。

ログオンできない

セットアップ ウィザードを使用して Trend Micro InterScan for Cisco CSC SSM をインストールしたときに、管理者パスワードを指定しています。ログインするには、インストレーション時に作成したこのパスワードを使用する必要があります。このパスワードは、ASDM にアクセスするのに使用するパスワードとは異なります。パスワードは大文字と小文字を区別するため、文字を正確に入力する必要があります。

パスワードを忘れた場合は、回復することができます。詳細については、P.8-16 の「Knowledge Base の使用」を参照してください。

失ったパスワードの回復

ASDM/CSC SSM を管理するには、次の 3 種類のパスワードを使用します。

- ASDM/Web インターフェイスのパスワード
- CLI パスワード
- ルート アカウント パスワード

この 3 種類のパスワードとも、デフォルトのエントリは「cisco」です。3 種類のパスワードすべてをなくした場合に、次の回復手順を実行します。

ステップ 1　CSC SSM を再イメージして、工場出荷時のデフォルト設定に戻します。再イメージすると、工場出荷時のデフォルトのソフトウェア イメージが SSM に転送されます。イメージを転送する場合の手順については、『*Cisco Security Appliance Command Line Configuration Guide*』の、「Managing AIP SSM and CSC SSM」の章の説明を参照してください。

ステップ 2　再イメージ後は、すべてのパスワードがデフォルト値に復元されます。これで、デフォルトのパスワード「cisco」を使用してログインし、ASDM/Web インターフェイス パスワードを新たに作成できるようになります。

ステップ 3　作成した新規 ASDM/Web インターフェイス パスワードを使用して、CSC SSM インターフェイスにアクセスします。**Administration > Configuration Backup** の順にクリックします。

ステップ 4　最新のコンフィギュレーションのバックアップをインポートして、コンフィギュレーション設定を復元します。

ステップ 5　デフォルトのパスワード「cisco」を使用して、コマンドライン インターフェイスおよびルート アカウントにアクセスし、デフォルトの CLI およびルート アカウント パスワードをアップデートします。

パスワードを、全部ではなく 1 つか 2 つだけなくす場合があります。次に、このような場合の対処法について説明します。

- ASDM/Web インターフェイス パスワードはあるが、シスコおよびルート アカウントのパスワードをなくした場合は、Web インターフェイスを通じて CSC SSM の管理を継続できますが、将来の必要時にコマンドライン インターフェイスまたはルート アカウントを使用できません。この 2 種類のパスワードを回復するには、前述の手順で再イメージと復元を行ってください。
- CLI パスワードしかない場合は、CSC SSM にログインして Restore Factory Defaults オプションに移動し、SSM をリセットしてください。これで再イメージと同じ効果があります。その後、保存済みのコンフィギュレーションをインポートします。Restore Factory Defaults オプションについては、P.A-12 の「工場出荷時のデフォルトの復元」を参照してください。
- ルート アカウント パスワードしかない場合は、ログインして **password** コマンドを使用して CLI パスワードを設定します。その後、前述と同様の手順を続行します。

要約ステータスとログ エントリが同期していない

場合によっては、Summary ウィンドウの Mail（SMTP）、Mail（POP3）、Web（HTTP）、および File Transfer（FTP）の各種タブに表示されるカウンタが、ログ レポートに表示される統計情報と同期していない場合があります。（CSC SSM コンソールで **Logs** > **Query** をクリックしてログにアクセスします）。この「不整合」は次の理由によるものです。

- デバイス　エラーまたはパッチ　インストール後のリブートのいずれかで発生したリブートによって、ログがリセットされている。
- SSM のメモリ ストレージの容量が足りないために、頻繁にログがパージされる。

HTTP 接続の遅延

CSC SSM で URL のフィルタリングをイネーブルにしている場合は、30 秒程度の遅延が発生することがありますが、CSC SSM はインターネットに接続するのに HTTP を使用しません。Trend Micro では、異なるカテゴリの URL を保管するオンライン データベースを維持しています。CSC SSM は、クライアントからの HTTP 要求を代行受信する場合に、URL データベースへのアクセスを試みます。インターネットへのアクセスが実行できない場合は（直接またはプロキシ経由で）、URL フィルタリングをディセーブルにしてください。

一部の Web サイトへのアクセス速度が遅い、またはアクセスできない

銀行やオンライン ショッピング サイトなどの Web サイトや、他の特定の用途のサーバでは、クライアントの要求に応答する前に、追加のバックエンド処理を必要とする場合があります。CSC SSM では、クライアント要求とサーバ応答の間に 90 秒のタイムアウトがハードコードされており、これによってトランザクションが CSC SSM のリソースを長時間占有することを防止します。これは、トランザクションの処理が長時間に及ぶと失敗することを意味しています。

これを回避するには、サイトをスキャンの対象から外します。コマンドライン インターフェイスでこれを行う場合は、たとえば、IP アドレスが 192.168.10.10 の外部ネットワークに対して、次のように実行します。

```
! exempt http traffic to 192.168.10.10
    access-list 101 deny tcp any host 192.168.1.1 eq http
    ! catch everything else
    access-list 101 permit tcp any any eq http
    class-map my_csc_class
          match access-list 101
    policy-map my_csc_policy
         class my_csc_class
             csc fail-close
    service-policy my_csc_policy interface inside
```

このように設定すると、192.168.10.10 までの HTTP トラフィックは CSC SSM からスキャンされなくなります。

パケット キャプチャの実施

CSC SSM を経由せずにアクセス可能なサイトはあるが、トラフィックがスキャンされているためにアクセスできない場合は、Cisco TAC にこの URL を報告してください。可能な場合は、パケット キャプチャを実施し、結果を TAC にも送信してください。たとえば、クライアントの IP が 10.1.1.1 だとすると、外部 Web サイトの IP は、次のように 10.2.2.2 になります。

```
access-list cap_acl permit tcp host 1.1.1.1 host 2.2.2.2
access-list cap_acl permit tcp host 2.2.2.2 host 1.1.1.1
capture cap access-list cap_acl interface inside
capture cap access-list cap_acl interface outside
```

FTP ダウンロードが実行できない

FTP にログインはできるが FTP 経由のダウンロードが実行できない場合は、**inspect ftp** 設定が ASA でイネーブルになっているか確認してください。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

スキャン機能のトラブルシューティング

次の項では、ウィルスまたはスパムのスキャンで発生する可能性のある問題の対処法について説明します。

パターン ファイルをアップデートできない

パターン ファイルが期限切れでアップデートできない場合は、ご使用の Maintenance Agreement が失効している可能性が高いです。**Administration** > **Product License** ウィンドウの **Expiration Date** フィールドを確認してください。過去の日付が表示されている場合は、Maintenance Agreement を更新するまではパターン ファイルをアップデートできません。

これ以外に考えられる原因は、Trend Micro ActiveUpdate サーバが一時的にダウンしていることです。数分後に、再度アップデートを試みてください。

スパムが検出されない

アンチスパム機能が動作していないように見える場合は、次の点を確認してください。

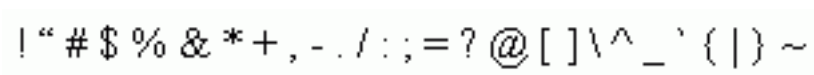
- この機能をイネーブルにしていても、アンチスパムのオプションはデフォルトではイネーブルになっていません（詳細については、P.3-9 の「SMTP および POP3 スパム フィルタリングのイネーブル化」を参照してください）。
- 着信メール ドメインを設定している（詳細については、P.3-7 の「SMTP メッセージ フィルタ、免責条項、および着信メール ドメインの設定」を参照してください）。

スパム スタンプ識別情報が作成できない

スパム スタンプ識別情報とは、電子メール メッセージの件名に表示されるメッセージです。たとえば、「Q3 Report」という見出しのメッセージに対して、スパム スタンプ識別情報で「スパム」と定義された場合、メッセージの件名には「Spam:Q3 Report」と表示されます。

スパム識別情報の作成で問題が発生している場合は、英字の大文字と小文字、数字の 0 ～ 9、図 8-1 に示す特殊文字の組み合わせのみを使用していることを確認してください。

図 8-1　スパム スタンプ識別情報で使用可能な特殊文字



指定以外の文字を使用しようとすると、SMTP および POP3 メッセージでスパム識別情報を使用できません。

許容できない数のスパムの false positive が検出される

スパム フィルタリングしきい値を、過度にアグレッシブな（高すぎる）レベルに設定している場合があります。しきい値を Medium または High に合わせている場合、**Mail (SMTP) > Anti-spam > SMTP Incoming Anti-spam** ウィンドウと **Mail (POP3) > Anti-spam > POP3 Anti-spam** ウィンドウで、しきい値のフィールドを低くしてみてください。また、**SMTP Incoming Anti-spam** ウィンドウと **POP3 Anti-spam** ウィンドウで、アンチスパムの「stamp message」機能をイネーブルにします。この 2 種類のウィンドウの詳細については、オンライン ヘルプを参照してください。

さらに、ネットワーク上のユーザがニュースレターを受信している場合は、この種のメッセージによって多数の false positive がトリガーされる傾向があります。承認済みの送信者リストにこのニュースレターの電子メール アドレスまたはドメイン名を追加して、これらのメッセージに対するスパム フィルタリングを省略してください。

スパムの false positive を許容できない

銀行や保険会社などの企業では、メッセージが false positive と識別されるようなリスクを負うことはできません。このような場合は、SMTP および POP3 に対するアンチスパム機能をディセーブルにしてください。

許容できない大量のスパムが検出される

スパム フィルタリングのしきい値を、低すぎるレベルに設定している場合があります。この場合は、**Mail (SMTP) > Anti-spam > SMTP Incoming Anti-spam** ウィンドウと **Mail (POP3) > Anti-spam > POP3 Anti-spam** ウィンドウのしきい値のフィールドで、設定を高くしてください。

ウィルスは検出されるがクリーニングされない

ウィルスに感染したすべてのファイルをクリーニングできるわけではありません。たとえば、パスワードで保護されたファイルは、スキャンもクリーニングもできません。

クリーニングに反応しないウィルスに感染したと思われる場合は、次の URL にアクセスしてください。

http://subwiz.trendmicro.com/SubWiz/Default.asp

このリンクからアクセスする Trend Micro Submission Wizard には、ウィルス感染が疑わしいファイルについて TrendLabs に評価を依頼する際の提出方法など、対処法に関する情報が含まれています。

ウィルスのスキャンが動作しない

SMTP Incoming、SMTP Outgoing、POP3、HTTP、および FTP Scanning の各ウィンドウで、ウィルスのスキャン機能をディセーブルにしているユーザがいないことを確認します。スキャンがイネーブルにも関わらずウィルスが検出されない場合は、カスタマー サポートにお問い合わせください。

また、P.2-3 の「アンチウイルス機能のテスト」の手順に従ってウィルスのスキャン機能をテストしてください。

不正な ASA ファイアウォール ポリシー設定のためにスキャンが動作しない

スキャンが動作しない原因として考えられるもう一つの原因は、ASA ファイアウォール ポリシー設定が正しくないために、ファイルがスキャンされていないことがあります。CLI で ASA **show service-policy csc** コマンドを使用して、SSM でトラフィックを処理するように設定します。次に例を示します。

```
show service-policy flow tcp host [clientIP] host [server IP] eq [proto]
```

次に例を示します。

```
hostname(config)# show service-policy flow tcp host 192.168.10.10 host 10.69.1.129 eq
http
Global policy:
Service-policy: global_policy
    Class-map: trend
        Match: access-lit trend
            Access rule: permit tcp any any eq www
        Action:
            Output flow: csc fail-close
            Input flow set connection timeout tcp 0:05:00
    Class-map: perclient
        Match: access-lit perclient
            Access rule: permit IP any any
            Action:
            Input flow: set connection per-client-max 5 per-client-embryonic-max 2
```

CSC SSM が失敗ステータスにあるためにスキャンが動作しない

CSC SSM がリブートのプロセス中か、ソフトウェアに障害が発生していると、syslog エラーの 421007 が生成されます。CLI で次のコマンドを入力して SSM カードのステータスを表示します。

```
hostname# show module 1
```

次の例に示すように、出力にはいくつかのテーブルが表示されます。3 番目のテーブル（SSM Application Name）にステータスが表示されます。この例では、SSM のステータスは「Down」です。

```
Mod Card Type                                    Model  Serial No.
--- -------------------------------------------- ------------------------------
1 ASA 5500 Series Security Services Module-10  ASA-SSM-10 JAB092400TX

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ---------------------------
  1 0013.c480.ae4c to 0013.c480.ae4c  1.0          1.0(10)0     CSC SSM 6.0
(Build#1345)

Mod SSM Application Name           Status            SSM Application Version
--- ------------------------------ ----------------------------------------
  1 CSC SSM                        Down              6.0 (Build#1345)

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  1 Up                 Up
```

3 番目のテーブルの **Status** フィールドに表示可能なステータスは、次の 3 種類です。

- **Down**：無効なアクティベーション コードが使用された、ライセンスが失効している、ファイルが壊れている、などの永続的なエラーの場合に表示されます。
- **Reload**：パターン ファイルのアップデート中など、スキャンが再起動中の場合に表示されます。
- **Up**：通常の操作時を表すステータスです。

各プロセスのステータスを個別に表示するには、CLI で次のコマンドを実行してください。

```
hostname# show module 1 detail
```

次のような出力が表示されます。

```
Getting details from the Service Module, please wait...
    ASA 5500 Series Security Services Module-10
    Model:              ASA-SSM-10
    Hardware version:   1.0
    Serial Number:      JAB092400TX
    Firmware version:   1.0(10)0
    Software version:   CSC SSM 6.0 (Build#1345)
    MAC Address Range:  0013.c480.ae4c to 0013.c480.ae4c
    App. name:          CSC SSM
    App. Status:        Down
    App. Status Desc:   CSC SSM scan services are not available
    App. version:       6.0 (Build#1345)
    Data plane Status:  Up
    Status:             Up
    HTTP Service:       Down

    Mail Service:       Down

    FTP  Service:       Down

    Activated:          No

    Mgmt IP addr:       <not available>

    Mgmt web port:      8443

    Peer IP addr:       <not enabled>
```

CSC SSM のステータスは、**App.Status** フィールドに表示されます。前述の例ではステータスは「Down」です。このフィールドで可能なステータスは次のとおりです。

- **Not Present**：SSM カードは未検出
- **Init**：SSM カードはブート中
- **Up**：SSM カードは稼動中
- **Unresponsive**：SSM カードは応答していない
- **Reload**：SSM カードはリロード中
- **Shutting Down**：SSM カードはシャットダウンしている
- **Down**：SSM カードはダウン状態にあり、スロットから安全に取り外しが可能
- **Recover**：SSM カードは再イメージ中

大容量ファイルのダウンロード

非常に大きいサイズのファイルを扱うと、HTTP プロトコル、または FTP プロトコル上の問題が発生しやすくなります。HTTP Scanning ウィンドウ、および FTP Scanning ウィンドウの Target タブで設定した大容量ファイルの処理フィールドに、スキャンを遅らせるオプションが含まれています。

スキャンの遅延をイネーブルにしなかった場合は、InterScan for Cisco CSC SSM は、ファイル全体を受信およびスキャンしてから、要求しているユーザにファイル内容を渡す必要があります。ファイル サイズによっては、次のようになることもあります。

- 結局、ファイルはダウンロードされるが、最初は非常に低速でダウンロードが進むにつれて高速になる

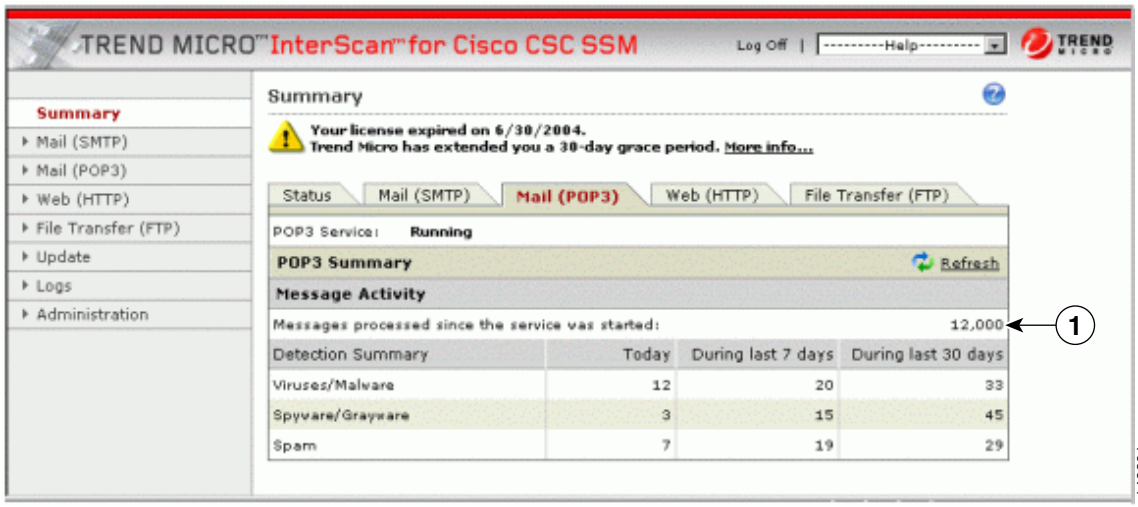
- ブラウザの自動タイムアウト時間が超過して、ユーザは結局ファイルの内容をまったく受信できない（ダウンロードが完了する前にブラウザがタイムアウトしたため）

スキャンの遅延をイネーブルにした場合は、タイムアウトになるのを防ぐため、大規模ファイルの一部の内容はスキャンされずに配信されます。それ以降の部分はバックグラウンドでスキャンされ、その後、脅威が検出されなければダウンロードされます。脅威が*検出された*場合は、残りのファイルはダウンロードされませんが、大規模ファイルのスキャンしていない部分はすでにユーザのマシンに保存されているため、セキュリティ リスクとなる可能性があります。

スキャン サービスの再起動

Summary ウィンドウの Mail （SMTP および POP3）タブでは、ウィンドウの Message Activity 領域に、**Messages processed since the service was started** のカウント数が表示されます。図 8-2 に、表示例を示します。

図 8-2　Summary ウィンドウの Mail（POP3）タブに表示されたメッセージ処理カウンタ



1	メッセージ アクティビティ カウンタ

イベントによってはこのカウンタをゼロにリセットするものがあります。次のようなイベントです。

- パターン ファイルまたはスキャン エンジンのアップデート
- コンフィギュレーションの変更
- パッチの適用

Detection Summary 領域はリセットされません。これらの統計情報は、上記のイベントに関わらず、トリガー イベントが発生するたびにアップデートし続けます。

カウンタがリセットされても問題はありません。カウンタがリセットされる理由を理解しておく必要があるだけです。ただし、**Messages processed...** フィールドでゼロの状態が続いた場合は、電子メール トラフィックがスキャンされていないことを示しているため、状況を調査する必要があります。

パフォーマンスのトラブルシューティング

次の項では、パフォーマンスについて発生する可能性のある問題について説明します。

CSC SSM コンソールがタイムアウトした

CSC SSM コンソールをアクティブにしてから約 10 分間、アクティビティが 1 つも検出されない状態のままにしておくと、セッションはタイムアウトします。処理を続行するには再びログインしてください。保存していない作業上の変更は失われます。席を離れる場合は、作業内容を保存して戻るまでログオフすることを推奨します。

ステータス LED が 1 分以上点滅する

ステータス LED が 1 分以上点滅を繰り返している場合は、スキャン サービスが利用できない状態になっています。この問題を解決するには、システムを ASDM からリブートするか、カスタマー サポートにお問い合わせください。

注意　ダウンロードするファイルが **Do not scan files larger than...** フィールドの指定よりも大きいと、ファイルはスキャンされずに配信され、セキュリティ リスクとなる場合があります。

SSM が ASDM と通信できない

ポート アクセス制御をリセットすることで、この問題を解決できる可能性があります。手順については、P.A-16 の「管理ポートのアクセス コントロールのリセット」を参照してください。

ASDM を使用しないログイン

何らかの理由で ASDM が利用できない場合は、Web サーバから直接 CSC SSM にログインすることができます。ログインするには、次の手順を実行します。

ステップ 1　ブラウザのウィンドウに、次の URL を入力します。

```
https://{SSM IP addresss}:8443
```

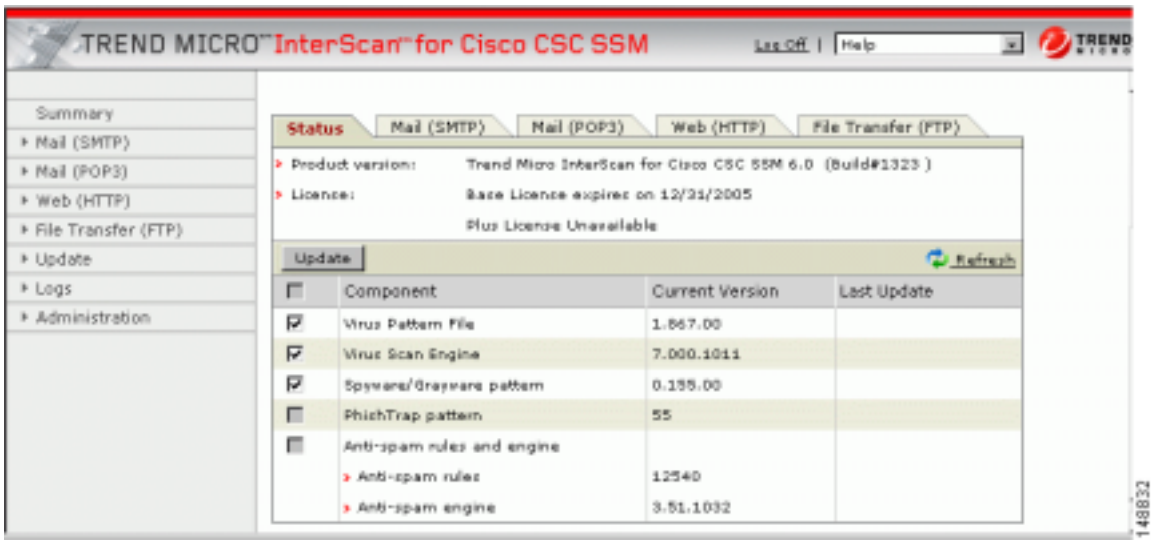
次に例を示します。

```
https://10.123.123.123:8443/
```

ステップ 2　**Logon** ウィンドウが表示されます。セットアップ ウィザードで **Password Configuration** インストール ウィンドウで作成したパスワードを入力し、**Log On** をクリックします。

ステップ 3　CSC SSM コンソールのデフォルト ビューは、次に示すように、**Summary** ウィンドウの Status タブです。

図 8-3　CSC SSM コンソールの Summary 画面に表示された Status タブ



CSC SSM のスループットが ASA よりはるかに低い

TCP 接続からファイルを復元してスキャンする処理は負荷が大きいため、ファイアウォールで通常実行されるプロトコル準拠チェックに比べ、はるかにオーバーヘッドが必要となります。対応策としては、スキャンが必要な接続だけを CSC SSM に誘導して、パフォーマンスのミスマッチを軽減する方法があります。

たとえば、HTTP トラフィックは、発信トラフィック（内部ユーザから外部 Web サイトへのアクセス）、着信トラフィック（外部ユーザから内部サーバへのアクセス）、イントラネット トラフィック（内部サイトと信頼済みパートナー間でのトラフィック）に分割することができます。発信トラフィックのみウィルスをスキャンして、着信トラフィックはスキャンしないように CSC SSM を設定することができます。

詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の「Managing AIP SSM and CSC SSM」の章を参照してください。

Knowledge Base の使用

Trend Micro のオンライン Knowledge Base を使用すると、より詳細な情報を検索することができます。Knowledge Base の URL は、次のとおりです。

http://esupport.trendmicro.com

Knowledge Base の検索エンジンでは、製品名、問題カテゴリ、キーワードを入力して検索を絞り込むことができます。Knowledge Base には、数千種類のソリューションが用意されており、毎週追加されます。

Security Information Center の使用

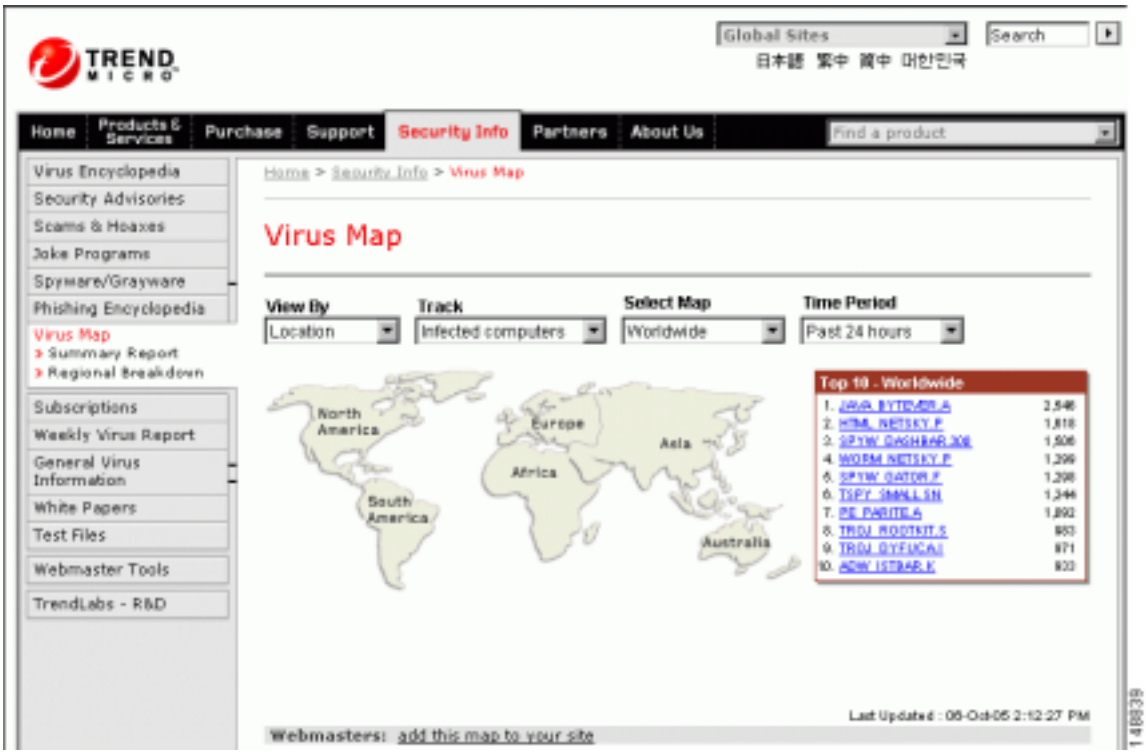
Trend Micro では、無料のオンライン リソースである Security Information Center から、包括的なセキュリティ情報が 24 時間週 7 日利用できます。Security Information Center の URL は次のとおりです。

http://trendmicro.com/vinfo/

Security Information Center では、次の情報を提供しています。

- **Virus Encyclopedia**：ウィルス、ワーム、トロイの木馬、その他すべての既知の脅威に関する知識をまとめたもの
- **Security Advisories**：マルウェアのアラート、最も顕著なリスクの危険度レーティング、最新のパターン ファイルとスキャン エンジンのバージョン、その他の有益な情報の表示
- **Scams and Hoaxes**：マルウェアによるデマ情報、チェーン メールまたは金銭的損失を与えるような詐欺情報、都市伝説などの情報
- **Joke Programs**：Trend Micro のスキャン エンジンで検出された、既知のジョーク プログラムに関する情報のリポジトリ
- **Spyware/Grayware**：検出されたスパイウェア / グレイウェア プログラムのトップ 10 情報、スパイウェア / グレイウェア プログラムの検索可能なデータベース
- **Phishing Encyclopedia**：既知のフィッシング詐欺のリストおよび犯行の手口の説明
- **Virus Map**：世界の地域別に脅威を表示

図 8-4　Virus Map



- **Weekly Virus Report**：その週に検出された脅威についての最新ニュース（Weekly Virus Report を購読すると、週に 1 度レポートが電子メールで自動配信されます）。
- General virus information に含まれる情報は次のとおりです。
  - **Virus Primer**：ウィルスの用語解説とウィルスのライフサイクルに関する説明
  - **Safe Computing Guide**：感染のリスクを減らすための安全基準
  - **Risk ratings**：マルウェアおよびスパイウェア / グレイウェアによる脅威を、グローバル IT コミュニティに対する危険度から Very Low、Low、Medium、または High とレーティング
- **White papers**：「*The Real Cost of a Virus Outbreak*」または「*The Spyware Battle—Privacy vs. Profits*」という見出しのセキュリティ概念を説明したドキュメントへのリンク
- **Test files**：Trend Micro InterScan for Cisco CSC SSM をテストするためのテスト ファイル、およびテストの実施手順
- **Webmaster tools**：Webmasters に関する無料の情報およびツール
- **TrendLabs**：ISO 9002 認定の、ウィルス調査および製品サポート センターである TrendLab に関する情報

CSC SSM Syslog の概要

CSC SSM 関連の syslog メッセージには 13 種類あります。この項では、メッセージごとに解説します。

SSM アプリケーションのミスマッチ [1-105048]

エラーメッセージ　`%ASA-1-105048: (unit) Mate's service module (application) is different from mine (application)`

説明　フェールオーバー プロセスで、アクティブ ユニットとスタンバイ ユニットのサービス モジュール間で、異なるアプリケーションが動作していることが検出されました。複数のサービス モジュールが使用されている場合、2 種類のフェールオーバー ユニットの間に互換性はありません。

unit：プライマリまたはセカンダリ。

application：InterScan Security Card などのアプリケーションの名前。

推奨処置　フェールオーバーを再度イネーブルにする前に、両ユニットに同一のサービス モジュールがインストールされていることを確認してください。

CSC カードの障害のためにトラフィックが破棄された [3-421001]

エラーメッセージ　`%ASA-3-421001: TCP|UDP flow from interface_name:ip/port to interface_name:ip/port is dropped because application has failed.`

説明　CSC SSM アプリケーションの障害のためにパケットが破棄されました。デフォルトでは、このメッセージは、10 秒に 1 回しか表示されないように制限されています。

interface_name：インターフェイス名。

IP_address：IP アドレス。

port：ポート番号。

application：CSC SSM が現在のリリースでサポートされている唯一のアプリケーションです。

推奨処置　すぐにサービス モジュールの問題を調査してください。

適用外のトラフィックをスキップする [6-421002]

エラーメッセージ　`%ASA-6-421002: TCP|UDP flow from` *interface_name*`:`*IP_address*`/`*port* `to` *interface_nam*`:`*IP_address*`/`*port* `bypassed` *application* `checking because the protocol is not supported.`

説明　サービス モジュールで使用するプロトコルがスキャンされないために、サービス モジュールのセキュリティ チェックの接続がバイパスされました。たとえば、CSC SSM は TELNET トラフィックのスキャンには適用されません。ユーザが TELNET トラフィックをスキャンするように設定している場合は、トラフィックがスキャン サービスをバイパスします。デフォルトでは、このメッセージは、10 秒に 1 回しか表示されないように制限されています。

IP_address：IP アドレス。

port：ポート番号。

interface_name：ポリシーが適用されているインターフェイス名。

application：CSC SSM が現在のリリースでサポートされている唯一のアプリケーションです。

推奨処置　サービス モジュールでサポートされているプロトコルのみを含めるように、設定を変更する必要があります。

無効なカプセル化によって ASDP パケットが破棄された [3-421003]

エラーメッセージ　`%ASA-3-421003: Invalid data plane encapsulation.`

説明　サービス モジュールで挿入されたパケットには、正しいデータ プレーン ヘッダーがありませんでした。シスコ専用プロトコルに準拠するデータ バックプレーンで交換されるパケットは、ASDP と呼ばれます。適切な ASDP ヘッダーのないパケットは破棄されます。

推奨処置　**capture** *name* **type asp-drop** [**ssm-asdp-invalid-encap**] コマンドを実行して有害なパケットをキャプチャし、Cisco TAC にお問い合わせください。

パケットを挿入できない [7-421004]

エラーメッセージ　`%ASA-7-421004: Failed to inject {TCP|UDP} packet from` *IP_address*`/`*port* `to` *IP_address*`/`*port*

説明　セキュリティ アプライアンスは、サービス モジュールで指示されたパケットを挿入できませんでした。これは、セキュリティ アプライアンスがすでに解放されたフローにパケットを挿入しようとして発生した可能性があります。

IP_address：IP アドレス。

port：ポート番号。

推奨処置　この状態は、セキュリティ アプライアンス がその接続テーブルをサービス モジュールに依存せず、独自に維持しているために発生した可能性があります。通常は、これによって問題は発生しません。セキュリティ アプライアンス のパフォーマンスに影響が生じた場合は、Cisco TAC にお問い合わせください。

アカウント ホスト数がライセンスの上限に近づいている [6-421005]

エラーメッセージ　`%ASA-6-421005: interface_name:IP_address is counted as a user of application`

説明　ホストがライセンスの上限に近づいているとカウントされました。指定されたホストは *application* のユーザであるとカウントされました。午前 0 時に、ライセンス検証のために、過去 24 時間分のユーザの合計数が計算されます。

interface_name：インターフェイス名。

IP_address：IP アドレス。

application：CSC SSM が現在のリリースでサポートされている唯一のアプリケーションです。

推奨処置　処置は不要です。ただし、全体のカウント数が購入したユーザ ライセンス数を上回る場合は、ライセンスのアップグレードについてシスコにお問い合わせください。

日単位のノード カウント [5-421006]

エラーメッセージ　`%ASA-6-421006: There are number users of application accounted during the past 24 hours.`

説明　過去 24 時間に *application* を使用したユーザの合計数を特定します。このメッセージは、サービス モジュールが提供するサービスを使用したホストの合計数を算出するために、24 時間ごとに生成されます。

推奨処置　処置は不要です。ただし、全体のカウント数が購入したユーザ ライセンス数を上回る場合は、ライセンスのアップグレードについてシスコにお問い合わせください。

CSC カードの障害のためにトラフィックが破棄された [6-421007]

エラーメッセージ　`%ASA-3-421007: TCP|UDP flow from interface_name:IP_address/port to interface_name:IP_address/port is skipped because application has failed.`

説明　このメッセージは、サービス モジュール アプリケーションに障害が発生し、フローがスキップされた場合に生成されます。デフォルトでは、このメッセージは、10 秒に 1 回しか表示されないように制限されています。

IP_address：IP アドレス。

port：ポート番号。

interface_name：ポリシーが適用されているインターフェイス名。

application：CSC SSM が現在のリリースでサポートされている唯一のアプリケーションです。

推奨処置　すぐにサービス モジュールの問題を調査してください。

新しいアプリケーションが検出された [5-505011]

エラーメッセージ　%ASA-5-505011: Module in slot *slot*, application detected *application*, version *version*.

説明　新しいアプリケーションが 4GE SSM 上に検出されました。このメッセージは、システムのブート時、4GE SSM のブート時、または 4GE SSM の新規アプリケーションの起動時に生成される可能性があります。

slot：アプリケーションが検出されたスロット。

application：検出されたアプリケーションの名前。

version：検出されたアプリケーションのバージョン。

推奨処置　記述されたアクティビティが正常または正常と予期される場合は、処置は不要です。

アプリケーションが停止した [5-505012]

エラーメッセージ　%ASA-5-505012: Module in slot *slot*, application stopped *application*, version *version*

説明　このメッセージは、アプリケーションが停止したか、4GE SSM から削除されるたびに生成されます。4GE SSM がアプリケーションをアップグレードしたか、4GE SSM 上のアプリケーションが停止またはアンインストールされた場合に発生する場合があります。

slot：アプリケーションが停止したスロット。

application：停止したアプリケーションの名前。

version：停止したアプリケーションのバージョン。

推奨処置　アップグレードが 4GE SSM で実行されなかったか、アプリケーションが予期せずに停止またはアンインストールされた場合は、4GE SSM のログを確認して、アプリケーションが停止した原因を特定してください。

アプリケーションのバージョンが変更されている [5-505013]

エラーメッセージ　%ASA-5-505013: Module in slot *slot* application changed from: *application* version *version* to: *newapplication* version *newversion*.

説明　このメッセージは、アップグレード後など、アプリケーションのバージョンが変更されるたびに生成されます。これはアプリケーションのソフトウェア アップグレードがモジュールで完了すると発生します。

slot：アプリケーションがアップグレードしたスロット。

application：アップグレードしたアプリケーションの名前。

version：アップグレードしたアプリケーションのバージョン。

slot：アプリケーションがアップグレードしたスロット。

application：アップグレードしたアプリケーションの名前。

version：アップグレードしたアプリケーションのバージョン。

newapplication：新規アプリケーションの名前。

newversion：新規アプリケーションのバージョン。

推奨処置　アップグレードが予期されていることと、新規バージョンが正しいことを確認します。

データ チャネルの通信障害 [3-323006]

エラーメッセージ　`%ASA-3-323006: Module in slot slot experienced a data channel communication failure, data channel is DOWN.`

説明　このメッセージは、データ チャネル通信に障害が発生して、システムが 4GE SSM にトラフィックを転送できなかったことを示します。この障害がフェールオーバー ペアのアクティブなアプライアンスで発生すると、フェールオーバーがトリガーされます。また、通常は 4GE SSM に送信される、設定済みのフェール オープンまたはフェール クローズのポリシーが強制的に実行されます。このメッセージは、システム モジュールと 4GE SSM との間で、セキュリティ アプライアンスのデータプレーンを介した通信上の問題が発生するたびに生成されます。これは 4GE SSM が停止、リセット、または削除されると発生します。

slot：障害が発生したスロット。

推奨処置　このメッセージが 4GE SSM のリロードまたはリセットの結果ではなく、また、4GE SSM のステータスが UP に戻った後に、対応するメッセージ 5-505010 が表示されない場合、**hw-module module 1 reset** コマンドでモジュールのリセットが必要な場合があります。

データ チャネルの通信は正常 [5-505010]

エラーメッセージ　`%ASA-5-505010: Module in slot slot data channel communication is UP.`

説明　このメッセージは、データ チャネルの通信が DOWN 状態から回復するたびに生成されます。このメッセージは、チャネル通信が正常に動作していることを示します。データ チャネル通信の失敗後、回復するとこのメッセージが表示されます。

slot：データ チャネル通信が確立されたスロット。

推奨処置　直前にデータ チャネル通信障害（メッセージ 3-323006）が発生した結果を受けこのメッセージが生成されたのでなければ、処置は不要です。通信障害の場合は、4GE SSM のメッセージを確認して、通信障害の原因を判定してください。

Cisco TAC にお問い合わせになる前に

Technical Assistance Center (TAC) にお問い合わせになる前に、マニュアルやオンライン ヘルプに必要な回答が記載されていないか確認してください。マニュアルや Knowledge Base を調べても回答が見つからない場合は、問題を効率良く解決するために、次の情報をお手元に用意してください。

- 製品のアクティベーション コード（複数の場合もあります）
- 製品のバージョン番号
- パターン ファイルおよびスキャン エンジンのバージョン番号
- ユーザ数
- エラー メッセージを受信した場合はその正確な文面
- 問題の発生手順

詳細については、P.-xv の「テクニカル サポート」を参照してください。

コマンドラインを通じたインストールおよび設定

この付録では、コマンドライン インターフェイス（CLI）を通じて Trend Micro InterScan for Cisco CSC SSM をインストール、または設定する必要があるユーザに、情報を提供します。コマンドラインでインストールを行う必要はまずありませんが、何らかの理由で必要が生じた場合に備え、以下に説明します。

(注) インストールが必要な場合は、ASDM　で起動されるセットアップ　ウィザードを使用してインストールする方法を推奨します。詳細については、『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』を参照してください。

CSC SSM は、ほとんどのユーザのアプライアンスにあらかじめインストールされているため、セットアップ ウィザードや CLI でインストールを行う必要はありません。

この付録では、次の項目について説明します。

インストール時のチェックリスト

インストールを開始する前に、次の情報を用意してください。必要に応じてこのページを印刷し、インストール中に入力を求められる値を記録するためのチェックリストとして活用できます。

入力を求められる事項	ユーザ入力	チェックマーク
管理者のパスワード（CLI 用）	パスワードは入力しないでください	
SSM カードの IP アドレス		❑
Subnet mask		❑
ホスト名（cisco1-ssm-csc など、冒頭以外のハイフンを含む 1 ～ 63 字の英数字）		❑
ドメイン名		❑
プライマリ DNS IP アドレス		❑
セカンダリ DNS IP アドレス（オプション）		❑
ゲートウェイの IP アドレス		❑
プロキシ サーバ（オプション）を使用する場合 プロキシ サーバの IP アドレス プロキシ サーバのポート		 ❑ ❑
着信メール用のドメイン名		❑
CSC SSM コンソールの管理者パスワード	パスワードは入力しないでください	
管理者の電子メール アドレス		❑
通知電子メール サーバの IP アドレス		❑
通知電子メール サーバのポート		❑
Base ライセンスのアクティベーション コード		❑
Plus ライセンスのアクティベーション コード（オプション）		❑

インストールの準備

インストール中に、SSM とセキュリティ アプライアンスとの日付と時刻を同期化するように求められます。開始する前に、アプライアンスの日付と時刻の設定が正確であることを確認してください。

コマンドライン インターフェイスを使用してインストールするには、次の手順を実行します。

ステップ 1　Trend Micro InterScan for Cisco CSC SSM ソフトウェアを、TFTP サーバにダウンロードします。

ステップ 2　Windows HyperTerminal などの端末アプリケーションを使用してログインし、ASA コンソールへのターミナル セッションを開きます。プロンプトで、次のように入力します。

```
hostname# hw module 1 recover config
```

システムの応答例は、次のとおりです。

```
Image URL [tftp://insidehost/sg-6.0-1177-tftp.img]:
tftp://insidehost/sg-6.0-1177-tftp.img
Port IP Address [192.168.7.20]:
VLAN ID [0]:
Gateway IP Address [0.0.0.0]:
hostname# hw module 1 recover boot
The module in slot 1 will be recovered. This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

ステップ 3　**y** を入力して確認します。

```
Recover issued for module in slot 1
```

ステップ 4　次のように、debug-module boot コマンドをイネーブルにします。

```
hostname# debug module-boot
debug module-boot enabled at level 1
hostname# Slot-1 199> Cisco Systems ROMMON Version (1.0(8)1) #0: Thu Jan 20 20:28:49
PST 2005
Slot-1 200> Platform SSM-IDS20
Slot-1 201> GigabitEthernet0/0
Slot-1 202> Link is UP
Slot-1 203> MAC Address: 000b.fcf8.0134
Slot-1 204> ROMMON Variable Settings:
Slot-1 205>   ADDRESS=192.168.7.20
Slot-1 206>   SERVER=192.168.7.100
Slot-1 207>   GATEWAY=0.0.0.0
Slot-1 208>   PORT=GigabitEthernet0/0
Slot-1 209>   VLAN=untagged
Slot-1 210>   IMAGE=sg-6.0-1177-tftp.img
Slot-1 211>   CONFIG=
Slot-1 212> tftp sg-6.0-1177-tftp.img@192.168.7.100
Slot-1 213> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 214> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
.
.
.
```

(注)　このプロセスが終了するまでには、約 10 分かかります。

```
.
.
.
Slot-1 389>!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 390> Received 57985402 bytes
Slot-1 391> Launching TFTP Image...
Slot-1 392> Cisco Systems ROMMON Version (1.0(8)1) #0: Thu Jan 20 20:28:49 PST 2005
Slot-1 393> Platform SSM-IDS20
Slot-1 394> GigabitEthernet0/0
Slot-1 395> Link is UP
Slot-1 396> MAC Address: 000b.fcf8.0134
Slot-1 397> Launching BootLoader...
```

ステップ 5　次のように、debug-module boot コマンドをディセーブルにします。

```
hostname# no debug module-boot
```

ステップ 6　module 1 の詳細が表示されます。次のサンプル コードが表示されます。

```
JDPIX# show module 1 d
Getting details from the Service Module, please wait...
SSM-IDS/10-K9
Model:              SSM-IDS10
Hardware version:   1.0
Serial Number:      0
Firmware version:   1.0(8)1
Software version:   CSC SSM 6.0 (Build#1345)
MAC Address Range:  000b.fcf8.0159 to 000b.fcf8.0159
App. name:          CSC SSM
App. Status:        Down
App. Status Desc:   CSC SSM scan services are not available
App. version:       6.0 (Build#1345)
Data plane Status:  Up
Status:             Up
HTTP Service:       Down
Mail Service:       Down
FTP  Service:       Down
Activated:          No
Mgmt IP addr:       <not available>
Mgmt web port:      8443
Peer IP addr:       <not enabled>
```

ステップ 7　次のようにコマンド セッションを開きます。

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

ステップ 8　デフォルトのログイン名「cisco」とパスワードを入力して、Trend Micro InterScan for Cisco CSC SSM にログインします。

```
login: cisco
Password:
```

ステップ 9　パスワードをすぐに変更するように求められます。ASDM にアクセスする際に、同じパスワードを使用しないようにしてください。

```
You are required to change your password immediately (password aged)
Changing password for cisco
(current) UNIX password:
New password:
Retype new password:
```

インストールの手順

コマンドラインの Setup Wizard でインストールするには、次の手順を実行します。

ステップ 1　管理者の CLI パスワードを確認すると、Trend Micro InterScan for Cisco CSC SSM Setup Wizard が表示されます。

```
Trend Micro InterScan for Cisco CSC SSM Setup Wizard
------------------------------------------------------------------------------
To set up the SSM, the wizard prompts for the following information:
    1. Network settings
    2. Date/time settings verification
    3. Incoming email domain name
    4. Web console administrator password
    5. Notification settings
    6. Activation Codes
The Base License is required to activate the SSM.
Press Control-C to abort the wizard.

Press Enter to continue ...
```

ネットワーク設定を設定するために **1** を選択して、**Enter** を押します。

ステップ 2　次のように Network Settings プロンプトが表示されます。

```
Network Settings
------------------------------------------------------------------------------
Enter the SSM card IP address:
Enter subnet mask:
Enter host name:
Enter domain name:
Enter primary DNS IP address:
Enter optional secondary DNS IP address:
Enter gateway IP address:
Do you use a proxy server? [y|n]
```

ネットワーク設定のプロンプトに応じて、インストール チェックリストの各値を入力します。最後のネットワーク設定用プロンプトで入力が終了すると、入力したすべての値が確認のために表示されます。次に例を示します。

```
Network Settings
------------------------------------------------------------------------------
IP              192.168.7.20
Netmask         255.255.255.0
Hostname        CSCSSM
Domain name     example.com

Primary DNS     10.2.200.2
Secondary DNS   10.2.203.1

Gateway         192.168.7.1
No Proxy

Are these settings correct? [y|n] y
```

ステップ 3　設定が正しい場合は、**y** を入力して確定します。（**n** を入力すると、Network Settings プロンプトが再び表示されるので、ステップ 2 を繰り返します）。

ステップ 4　ネットワーク設定の確認が終了すると、システムは次のメッセージで応答します。

```
Applying network settings ...
```

オプションで、ゲートウェイの IP アドレスに対して ping を実行してネットワーク設定を確認します。ping をスキップする場合は、**n** を入力します。

```
Do you want to confirm the network settings using ping? [y|n] y
Enter an IP address to ping: 192.168.7.1
PING 192.168.7.1 (192.168.7.1): 56 data bytes
64 bytes from 192.168.7.1: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 192.168.7.1: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 192.168.7.1: icmp_seq=3 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=4 ttl=255 time=0.1 ms

--- 192.168.7.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.2 ms
Press Enter to continue ...
```

ステップ 5　次のように Date/Time Settings プロンプトが表示されます。

```
                        Date/Time Settings
------------------------------------------------------------------------

SSM card date and time: 10/06/2005 18:14:14

The SSM card periodically synchronizes with the chassis.
Is the time correct? [y|n] y
```

シャーシとの日付と時刻の同期設定に応答する **y** を入力します。日付と時刻をアップデートするには **n** を入力してインストール ウィザードを終了し、ASA シャーシで日付 / 時刻または NTP 設定をアップデートしてから、SSM のインストールを再開してください。

ステップ 6　次のように Incoming Domain Name プロンプトが表示されます。

```
Incoming Domain Name
------------------------------------------------------------------------

Enter the domain name that identifies incoming email messages: (default:example.com)
Domain name of incoming email: example.com
Is the incoming domain correct? [y|n] y
```

所属の組織で最上位レベルのドメイン名を入力し、**y** を入力して手順を続行します。

ステップ 7　次のように Administrator/Notification Settings プロンプトが表示されます。

```
Administrator/Notification Settings
------------------------------------------------------------------------

The password will be hidden while you type.
Web console administrator password:
Retype Web console administrator password:
Administrator email address:
Notification email server IP:
Notification email server port: (default:25)
```

エントリを作成すると、次のような確認メッセージが表示されます。

```
Administrator/Notification Settings
------------------------------------------------------------------------

Administrator email address: tester@example.com
Notification email server IP: 10.2.202.28
Notification email server port: 25
Are the notification settings correct? [y|n] y
```

y を入力して手順を続行します。

ステップ 8　次のように Activation プロンプトが表示されます。

```
                            Activation
------------------------------------------------------------------------

You must activate your Base License, which enables you to update
your virus pattern file. You may also activate your Plus License.

Activation Code example: BV-43CZ-8TYY9-D4VNM-82We9-L7722-WPX41
Enter your Base License Activation Code: PX-ABTD-L58LB-XYZ9K-JYEUY-H5AEE-LK44N
Base License activation is successful.

(Press Enter to skip activating your Plus License.)
Enter your Plus License Activation Code: PX-6WGD-PSUNB-9XBA8-FKW5L-XXSHZ-2G9MN
Plus License activation is successful.
```

ステップ 9　次のように Activation Status が表示されます。

```
Activation Status
------------------------------------------------------------------------

Your Base License is activated.
Your Plus License is activated.

Stopping services: OK
Starting services: OK

The Setup Wizard is finished.
Please use your Web browser to connect to the management console at:
https://192.168.7.20:8443
Press Enter to exit ...

Remote card closed command session. Press any key to continue.
Command session with slot 1 terminated.
hostname#
```

サービス開始メッセージが表示されると、インストールが完了したことが分かります。Setup Wizard の最後のプロンプトで提示されたように、ユーザのブラウザから CSC SSM コンソールにログオンしてください。次のフォーマットで URL を入力します。

```
https://<SSM IP address>:8443/
```

インストールの確認

インストールが完了したら、次の手順を実行します。

ステップ 1　次のコマンドを入力して、インストール時に設定した SSM およびサービスに関する情報を表示します。

```
hostname# show module 1 details
```

次のシンタックスで応答が表示されます。

```
Getting details from the Service Module, please wait...
SSM-IDS/20-K9
Model: SSM-IDS20
Hardware version:   1.0
Serial Number:      0
Firmware version:   1.0(8)1
Software version:   CSC SSM 6.0 (Build#1177)
MAC Address Range:  000b.fcf8.0134 to 000b.fcf8.0134
App. name:          CSC SSM proxy services are not available
App. version:
App. name:          CSC SSM
App. version:       6.0 (Build#1177)
Data plane Status:  Up
Status:             Up
HTTP Service:       Up
Mail Service:       Up
FTP  Service:       Up
Activated:          Yes
Mgmt IP addr:       192.168.7.20
Mgmt web port:      8443
Peer IP addr:       <not enabled>
hostname#
```

ステップ 2　次のようにコマンド セッションを開きます。

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

ステップ 3　デフォルトのログイン名「Cisco」と、インストール時に Administrator/Notification Settings ウィンドウで設定したパスワードを使用して、ログインします。

```
login: cisco
Password:
Last login: Mon Oct 10 13:24:07 from 127.0.1.1
```

次のように、Trend Micro InterScan for Cisco CSC SSM Setup Main が表示されます。

```
     Trend Micro InterScan for Cisco CSC SSM Setup Main Menu
------------------------------------------------------------------------

1. Network Settings
2. Date/Time Settings
3. Product Information
4. Service Status
5. Change Password for Command Line Interface
6. Restore Factory Default Settings
7. Troubleshooting Tools
8. Reset Management Port Access Control List
9. Ping
10. Exit ...

Enter a number from [1-10]:
```

ネットワーク設定の表示および変更

オプションの **1** を選択してユーザのネットワーク設定のコンフィギュレーションを表示します。次のように表示されます。

```
Network Settings
------------------------------------------------------------------------

IP              192.168.7.20
Netmask         255.255.255.0
Hostname        CSCSSM
Domain name     tester@example.com
MAC address     00:0B:FC:F8:01:34

Primary DNS     10.2.200.2
Secondary DNS   10.2.203.1

Gateway         192.168.7.1
No Proxy

Do you want to modify the network settings? [y|n] n
```

いずれの設定もコマンドライン インターフェイスで変更することができます。

日付および時刻の設定の表示

オプションの **2** を選択して、SSM の日付と時刻の設定を表示します。次のように Date/Time Settings プロンプトが表示されます。

```
Date/Time Settings
------------------------------------------------------------------------

SSM card date and time: 10/10/2005 13:27:09 PDT

Press Enter to continue ...
```

この設定は変更できません。表示される情報は参照専用です。

製品情報の表示

オプションの **3** を選択して、コンポーネント（バージョンおよびビルド）の設定を表示します。次のように Product Information プロンプトが表示されます。

```
Product Information
----------------------------------------------------------------------

Main           version 6.0 build 1177
Mail component version 5.5 build 1064
Web component  version 2.1 build 1103

Press Enter to continue ...
```

この設定は変更できません。表示される情報は参照専用です。

サービス ステータスの表示

オプションの **4** を選択してコンポーネント（バージョンおよびビルド）の設定を表示します。次のように表示されます。

```
Service Status
----------------------------------------------------------------------

The CSC SSM RegServer service is running
The CSC SSM HTTP service is running
The CSC SSM FTP service is running
The CSC SSM Notification service is running
The CSC SSM Mail service is running
The CSC SSM GUI service is running
The CSC SSM SysMonitor service is running
The CSC SSM Failoverd service is running
The CSC SSM LogServer service is running
The CSC SSM SyslogAdaptor service is running
The CSC SSM Syslog-ng service is running

Do you want to restart all services? [y|n] n
```

Do you want to restart all services プロンプトで、スキャン サービスを再起動することができます。すべての手順が正常に実行されている場合は、再起動は必要ありません。トラブルシューティングを実行しようとしている場合は、再起動すると適切な動作ステータスに戻ることができる場合があります。サービスの再起動の影響に関する詳細は、P.8-14 の「スキャン サービスの再起動」を参照してください。

コマンドライン インターフェイスのパスワードの変更

オプションの **5** を選択すると、Set Password for Command Line Interface プロンプトが表示されます。次のように表示されます。

```
Set Password for Command Line Interface
----------------------------------------------------------------------
This option allows you to change the password for the Command Line Interface
that you are currently using.
Do you want to continue? [y|n]

The password will be hidden while you type.
Changing password for cisco
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Re-enter new password:
Password changed.
```

プロンプトに従ってパスワードをアップデートしてください。

工場出荷時のデフォルトの復元

オプションの **6** を選択して、インストール前のコンフィギュレーション設定に復元します。次のように Restore Factory Default Settings プロンプトが表示されます。

```
Restore Factory Default Settings
----------------------------------------------------------------------

Are you sure you want to restore the factory default settings? [y|n] n
```

注意　**y** を選択すると、すべてのコンフィギュレーション設定がインストール前のデフォルト設定に戻ります。デフォルト設定の詳細については、P.3-2 の「デフォルトのメール スキャン設定」およびP.4-2 の「デフォルトの Web および FTP のスキャン設定」を参照してください。インストール後に登録やアクティベーション、ライセンス設定、スパイウェア / グレイウェア検出機能のイネーブル化、ファイル ブロッキング、ファイル ブロッキングの例外指定などの追加設定を行っていると、これらの設定は失われます。

このオプションはコマンドラインからも利用できますが、コンフィギュレーション設定を復元するためのもっと良い方法が、CSC SSM コンソールから利用できます。**Administration > Configuration Backup** の順にクリックして Configuration Backup ウィンドウを表示します。Configuration Backup ウィンドウを使用すると、コンフィギュレーション設定をコンフィギュレーション ファイルに保存（エクスポート）して、後でインポート（復元）することができます。

CSC SSM を起動して再インストールする必要がある場合のみ、Restore Factory Default Settings オプションを選択してください。

トラブルシューティング ツール

オプションの **7** を選択して、トラブルシューティング ツールを表示することができます。

```
Troubleshooting Tools
------------------------------------------------------------------------

1. Enable Root Account
2. Show System Information
3. Gather Logs
4. Gather Packet Trace
5. Modify Upload Settings
6. Return to Main Menu

Enter a number from [1-6]:
```

これらのツールは、ユーザまたは TAC がシステム情報を活用して問題を解決するのに役立ちます。

ルート アカウントのイネーブル化

オプション **1** は、ルート アカウントをイネーブル化します。次の警告メッセージが表示されます。

```
************************ WARNING ************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and
troubleshooting purposes only. Unauthorized modifications
are not supported and will require this device to be
re-imaged to guarantee proper operation.
*********************************************************
Do you want to accept the warning and enable the root account? [y|n]
```

この警告は、ルート アカウントを最初にイネーブル化した場合にのみ、表示されます。ルート アカウントは、一度イネーブル化されるとディセーブル化できません。

注意　このオプションは、システム管理者が使用することを前提としていません。シスコのサービス担当者専用です。Cisco TAC から指示された場合を除き、このオプションを選択しないでください。

システム情報の表示

オプション **2** を使用すると、役に立つシステム情報を表示することができます。情報は画面に直接表示したり、データをファイルに保存して FTP または TFTP で転送することもできます。オプション **2** を選択すると、次のように Show System Information メニューが表示されます。

```
Troubleshooting Tools - Show System Information
------------------------------------------------------------------------

1. Show System Information on Screen
2. Upload System Information
3. Return to Troubleshooting Tools Menu
```

Show System Information の画面表示

次に、Show System Information メニューからオプション **1** を選択した場合に画面表示される、システム情報の例を示します。この情報は、ASDM および CSC SSM インターフェイスのさまざまな場所で表示できますが、次のように CLI バージョンを使用すると、すべての情報を一度にすばやく表示できます。

```
++++++++++++++++++++++
Mon Jan 9 18:38:01 PST 2006 (-8)

System is : Up

# Product Information
Trend Micro InterScan for Cisco CSC SSM
Version: 6.0 (Build#1340 )
SSM Model: SSM-10

# Scan Engine and Pattern Information
Virus Scan Engine: 8.100.1002 (Updated: 2006-01-09 14:10:07)
Virus Pattern: 3.149.00 (Updated: 2006-01-09 14:10:39)
Garyware Pattern: 0.327.00 (Updated: 2006-01-09 14:13:11)
PhishTrap Pattern: 223 (Updated: 2006-01-09 14:13:28)
AntiSpam Engine: 14196 (Updated: 2006-01-09 14:11:04)
AntiSpam Rule: 3.51.1033 (Updated: 2006-01-09 14:12:53)

# License Information
Product:Base License
Version:Full
Activation Code:BX-9YWQ-3685S-X39PZ-H96NW-MAJR7-CWBXR
Seats:000250
Status:Expired within grace period
Expiration date:12/31/2005
Product:Plus License
Version:Full
Activation Code:PX-P67G-WCJ6G-M6XJS-2U77W-NM37Y-EZVKJ
Seats:000250
Status:Expired within grace period
Expiration date:12/31/2005

Daily Node Count: 0
Current Node Count: 0

# Kernel Information
Linux csc 2.4.26-cscssm #2 SMP Mon Dec 19 11:53:05 PST 2005 (1.0.6) i686
unknn

ASDP Driver 1.0(0) is UP:
    Total Connection Records: 169600
    Connection Records in Use: 0
    Free Connection Records: 169600
```

スクロールするとさらに情報を確認できます。終了するには、**q** を入力します。

システム情報のアップロード

Show System Information メニューからオプション **2** を選択すると、次のプロンプトが表示されます。

```
Gathering System Information ...
Creating temporary file CSCSSM-SYSINFO-20060109-184511.txt
Uploading temporary file CSCSSM-SYSINFO-20060109-184511.txt
Uploading file ...
Deleting temporary file CSCSSM-SYSINFO-20060109-184511.txt
Press Enter to continue ...
```

プロンプトに従って入力すると、システム情報がアップロードされます。システム情報は、オプション **5** の Modify Upload Settings を使用して作成したアップロード設定を使用すると送信されます。詳細については、P.A-16 の「アップロード設定の修正」を参照してください。アップロード設定を行なっていない場合は、次の表示の後にプロンプトが表示されます。

```
Choose a protocol [1=FTP 2=TFTP]: 1
Enter FTP server IP: 10.2.15.235
Enter FTP server port: (default:21)
Enter FTP user name: ftp
The password will be hidden while you type.
Enter FTP password:
Retype FTP server password:
Saving Upload Settings: OK
```

Show System Information メニューが終了したら、オプション **3** の Return to Troubleshooting Tools メニューを選択します。

ログの収集

オプション **3** では、CSC SSM に関するすべてのログを収集し、FTP または TFTP を介して Cisco TAC などに送信することができます。ログは、オプション **5** の Modify Upload Settings で作成したアップロード設定を使用して送信されます。詳細については、P.A-16 の「アップロード設定の修正」を参照してください。

```
Troubleshooting Tools - Gather Logs
-------------------------------------------------------------------------

Gather logs now? [y|n] y
Gathering logs ...
Creating temporary file CSCSSM-LOG-20060109-184525.tar.gz
Uploading temporary file CSCSSM-LOG-20060109-184525.tar.gz
Uploading file ...
Deleting temporary file CSCSSM-LOG-20060109-184525.tar.gz
```

(注) ログは、CSCSSM-LOG-<date-time>.tar.gz の表記法で自動的に命名されます。パケット（後述）も同様に、CSCSSM-PACKET-<date-time>.gz の表記法で命名されます。

パケット トレースの収集

オプション **4** では、CSC SSM と ASA 間を通過するパケットをキャプチャできます。通常、この情報は Cisco TAC で使用します。

次のプロンプトが表示されます。

```
Troubleshooting Tools - Gather Packet Trace
-------------------------------------------------------------------------

Gather packet trace now? [y|n] y
Press Control-C to stop.
Gathering packet trace ...
Creating temporary file CSCSSM-PACKET-20060109-184529.gz
Upload the packet trace now? [y|n] y
Uploading temporary file CSCSSM-PACKET-20060109-184529.gz
Uploading file ...
```

パケット トレースをイネーブル化するには、次の手順を実行します。

ステップ 1　パケット トレースを収集するプロンプトが表示されたら、**y** を選択します。

ステップ 2　停止する場合は Control + C キーを押します。

ステップ 3　パケット トレースをアップロードするプロンプトが表示されたら、**y** を選択します。

パケットは、オプション **5** の Modify Upload Settings で定義したプロトコルを使用してアップロードされます。詳細については、P.A-16 の「アップロード設定の修正」を参照してください。

アップロード設定の修正

オプション **5** では、この章で前述した機能で使用したように、FTP または TFTP のいずれかによるアップロード方法を設定できます。

（注）　FTP サーバまたは TFTP サーバは、アップロードを有効にする設定がされている必要があります。

オプション **5** を選択すると、次のプロンプトが表示されます。

```
Troubleshooting Tools - Upload Settings
-----------------------------------------------------------------------

Choose a protocol [1=FTP 2=TFTP]: (default:1) 2
Enter TFTP server IP: (default:10.2.42.134)
Enter TFTP server port: (default:69)
Saving Upload Settings: OK
Press Enter to continue ...
```

プロンプトに従って入力すると、アップロード設定がコンフィギュレーションされます。設定は、後で使用できるように保存されます。

Troubleshooting Tools メニューが終了したら、オプション **6** の Return to Main メニューを選択します。

管理ポートのアクセス コントロールのリセット

オプションの **8** を選択して管理ポートのアクセス コントロール リストをリセットします。次のように表示されます。

```
Resetting management port access control list: OK
Press Enter to continue ...
```

ASDM が SSM と通信できない場合は、このオプションでポートのアクセスをリセットしてください。

Ping IP

診断の目的で ping オプションが使用できます。オプションの **9** を選択すると IP アドレスを ping します。次のように表示されます。

```
Enter an IP address to ping:
```

IP アドレスが入力されると、システムは次のように応答します。

```
PING 192.168.7.1 (192.168.7.1): 56 data bytes
64 bytes from 192.168.7.1: icmp_seq=0 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=2 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 192.168.7.1: icmp_seq=4 ttl=255 time=0.1 ms

--- 192.168.7.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.2 ms
Press Enter to continue ...
```

終了オプション

オプション **10** の Exit を選択すると、セットアップ オプションが終了します。次のように Exit Options メニューが表示されます。

```
Exit Options
----------------------------------------------------------------------

1. Logout
2. Reboot
3. Return to Main Menu

Enter a number from [1-3]: 1
Remote card closed command session. Press any key to continue.
Command session with slot 1 terminated.
hostname#
```

この Exit Options メニューからログアウトできます。あるいは、システムをリブートするか、Setup メニューに戻ることもできます。

コマンドラインを通じた設定

この項では、CSC SSM コンソールを通じてコマンドラインを実行するユーザが利用可能な、コマンドラインの代替となる手順について説明します。すべての機能に代替の手順が利用できるわけではありません。

設定のリセット

Trend Micro InterScan for Cisco CSC SSM のインストール後、SSM の再イメージに TFTP を使用した場合、CLI にアクセスしたときに次のプロンプトが初めて表示される可能性があります。

“Do you want to restore the previous configuration?[y/n]”

Setup Wizard メニューの質問が次のように表示されます。

```
Trend Micro InterScan for Cisco CSC SSM Setup Wizard
------------------------------------------------------------------------

Do you want to restore the previous configuration? [y|n] n
To set up the SSM, the wizard prompts for the following information:
1. Network settings
2. Date/time settings verification
3. Incoming email domain name
4. Web console administrator password
5. Notification settings
6. Activation Codes
The Base License is required to activate the SSM.
Press Control-C to abort the wizard.

Press Enter to continue ...
```

y を選択すると、前回コンフィギュレーションを保存したときの状態に、SSM のコンフィギュレーション設定が復元されます。これが CSC SSM の **Administration > Configuration Backup** ウィンドウ機能の代わりとなるコマンドラインを使用した手順です。

A

ActiveUpdate

Trend Micro ユーティリティの一種で、ウィルス パターン ファイル、スキャン エンジン、スパイウェア / グレイウェア パターン ファイル、PhishTrap パターン ファイル、スパム防止ルール、スパム防止エンジンなどを、オンデマンドまたはバックグラウンドでアップデートできるようにします。

ActiveX

オブジェクトのリンクと埋め込みを実装するオープン ソフトウェア アーキテクチャのタイプ。Web ページのダウンロードなど、一部の標準インターフェイスをイネーブルにします。

ActiveX 不正コード

ActiveX コントロールは、Web ページに埋め込まれたコンポーネント オブジェクトで、ページが表示されると自動的に実行されます。ActiveX コントロールを使用すると、Web 開発者は、Trend Micro の無料オンライン スキャナである HouseCall など、幅広い機能を使用して対話型でダイナミックな Web ページを作成できます。

ハッカー、ウィルス作成者、迷惑行為を働いたりそれ以上の危害をもたらす目的の人物は、システムを破壊するための手段として ActiveX 不正コードを使う可能性があります。多くの場合、Web ブラウザは設定が可能なため、セキュリティ設定を「high」に変更すれば、このような ActiveX コントロールが実行されないようにできます。

C

CLI

Command Line Interface（コマンドライン インターフェイス）。詳細については、P.A-1 の「コマンドラインを通じたインストールおよび設定」を参照。

CSC SSM コンソール

Trend Micro InterScan for Cisco CSC SSM のユーザ インターフェイス。

D

DNS

Domain Name System（ドメイン ネーム システム）。ホスト名を IP アドレスに変換するために主にインターネットで使用されている汎用的なデータ クエリー サービスです。

DNS 名前解決

DNS クライアントが DNS サーバにホスト名とアドレスのデータを要求するときのプロセスを、名前解決と呼びます。基本的な DNS では、サーバはデフォルトの名前解決を実行します。たとえば、リモート サーバは、現在のゾーンにあるコンピュータ上のデータについて、別のサーバにクエリーを送信します。リモート サーバ上のクライアント ソフトウェアがリゾルバにクエリーを出すと、リゾルバは自身のデータベース ファイルからこの要求に応答します。

DoS 攻撃（サービス拒絶攻撃） 大量のデータが添付されているグループアドレスの電子メール メッセージ。メッセージング サービスの明らかな低速化や停止も引き起こすほど、ユーザのネットワーク リソースの障害になります。

DOS ウィルス 「COM」および「EXE」ファイル型感染ウィルスとも呼ばれます。DOS ウィルスは、*.COM または *.EXE という拡張子の付いた DOS 実行可能プログラム ファイルに感染します。ほとんどの DOS ウィルスは、オリジナルのプログラム コードが上書きされるか不測の事態で破棄されない限り、増殖を繰り返して他のホスト プログラムに感染を広げます。

E

ELF Executable and Linkable Format。Unix および Linux プラットフォームの実行可能ファイル形式。

EULA（エンド ユーザ使用許諾契約書） End User License Agreement（EULA; エンドユーザ使用許諾契約書）は、ソフトウェアの発行元とソフトウェア ユーザとの間で交わされる法的契約書です。この契約では、ユーザ側の制約に関する概要が記されているのが普通です。ユーザは、インストール時に「I accept」をクリックしないことで、この契約を拒否できます。「I do not accept」をクリックすると、ソフトウェア製品のインストールが終了します。

多くのユーザは、ある種の無料ソフトウェアのインストール中に表示される EULA プロンプトで「I accept」を不注意にクリックすることによって、スパイウェアや広告プログラムが自分のコンピュータにインストールされることを知らずに合意しています。

EXE ファイル感染プログラム ファイル拡張子 .exe が付いた実行可能プログラム。「DOS ウィルス」も参照。

F

false positive スパム フィルタで「検知され」、スパムと識別されたが、実際にはスパムでない電子メール メッセージ。

FAQ Frequently Asked Questions（よくある質問）。特定のトピックに関する質問と回答を一覧にしたものです。

FTP TCP/IP ネットワークを介して、あるコンピュータから別のコンピュータにファイルを転送できるクライアントサーバ プロトコル。また、ファイルを転送するためにユーザが実行するクライアント プログラムを指すこともあります。

G

GUI グラフィカル ユーザ インターフェイス。プログラムとの入力や出力を表すのに、言葉ではなくグラフィックを使用したインターフェイス。このインターフェイスとは対照的に、コマンドライン インターフェイスでは、テキスト文字列を使用してプログラムと対話します。

H

HTML ウィルス Web ページの情報制作に使用するオーサリング言語である、HTML（Hyper Text Markup Language）をターゲットに攻撃するウィルス。このウィルスは Web ページに常駐して、ユーザのブラウザを介してダウンロードされます。

HTTP Hypertext Transfer Protocol（ハイパーテキスト転送プロトコル）。ワールド ワイド ウェブ で HTML 文書を送受信するために、クライアントサーバ型 TCP/IP プロトコルで使用します。従来から、HTTP では 80 番のポートを使用しています。

HTTPS HTTP over SSL。セキュア トランザクションの処理で使用される HTTP のバリエーションです。

I

ICSA

ICSA ラボは TruSecure Corporation の独立部門です。過去 10 年以上、ICSA は、調査、情報分析、製品の認定検査の分野において、セキュリティ業界の中心的存在であり続けています。ICSA ラボは、情報セキュリティ製品の規格を策定し、アンチウィルス、ファイアウォール、IPSec、暗号化、PC ファイアウォールなどの製品について、今日の世界規模のインストール ベースで 90 % 以上を認定しています。

IntelliScan

IntelliScan は、Trend Micro のスキャニング技術の一種で、実際のファイル タイプの認識機能によってファイルのヘッダーを検証し、不正コードに隠れ場所を提供する潜在性がある既知のファイル タイプだけをスキャンします。実際のファイル タイプを認識する機能は、無害な拡張子名を隠れ蓑にした不正コードを特定するのに有効です。

in the wild

現在アンチウィルス製品で制御されている既知のウィルスを指します。「in the zoo」も参照。

in the zoo

活発に活動する既知のウィルスを指します。「in the wild」も参照。

IP

Internet Protocol（インターネット プロトコル）。「IP アドレス」を参照。

IP アドレス

ネットワーク上のデバイスのインターネット アドレス。一般に、10.123.123.123 など、ドットで区切る表記法によってアドレスを指定します。

IT

Information technology（情報テクノロジー）。ハードウェア、ソフトウェア、ネットワーキング、通信、およびユーザ サポートなどが含まれます。

J

JavaScript ウィルス

JavaScript は、Netscape が開発した簡易プログラミング言語で、このスクリプトを使用した Web 開発者は、ブラウザに表示する HTML ページにダイナミックなコンテンツを追加できます。Javascript には Sun Microsystems の Java プログラミング言語と共通する機能がいくつかありますが、開発は独自に行われています。

JavaScript ウィルスは、HTML コードで書かれたこれらのスクリプトをターゲットに攻撃するウィルスです。Web ページにウィルスを常駐させることができ、ユーザのブラウザを通じてデスクトップにウィルスをダウンロードします。

「VBscript ウィルス」も参照。

Java アプレット

Java アプレットは、小さな移植可能 Java プログラムで HTML ページに埋め込まれており、Web ページを表示すると自動的に実行することができます。Java アプレットを使用すると、Web 開発者は、対話的でダイナミックな、幅広い機能を持つ Web ページを作成することができます。

不正コードの作成者も攻撃の手段として Java アプレットを利用してきました。しかし、ほとんどの Web ブラウザではこのような不正なアプレットが起動されないように設定することができます。セキュリティ設定を「高」に変更するだけで、被害を防止できる場合もあります。

Java ファイル

Java は、Sun Microsystems が開発した汎用プログラミング言語です。Java ファイルには Java コードが含まれています。Java は、プラットフォームに依存しない Java 「アプレット」の形式で、インターネットのプログラミングをサポートしています。（アプレットは、HTML ページに埋め込みが可能な Java プログラミング言語で記述されたプログラムです。Java 技術を有効にしているブラウザを使用してアプレットが含まれたページを表示すると、このアプレットのコードがユーザのシステムに転送されて、ブラウザの Java Virtual Machine で実行されます）。

Java 不正コード

Java で作成または埋め込まれたウィルス コード。「Java ファイル」も参照。

K

KB キロバイト。1024 バイトのメモリを表します。

M

MacroTrap Trend Micro のユーティリティで、文書に関連して保存されたすべてのマクロ コードをルール ベース検証します。通常、マクロ ウィルス コードは、多くの文書とともに移動する不可視のテンプレート（Microsoft Word の .dot など）の一部に含まれています。MacroTrap は、ウィルスのような行為を指示するキー手順をテンプレートで検索して、マクロ ウィルスの兆候がないか調べます。この手順には、テンプレートの一部を別のテンプレートにコピー（複製）したり、潜在的に有害なコマンド（破壊行為）を実行するなどがあります。

MB メガバイト。1024 キロバイトのデータが 1 MB です。

Mbps 1 秒間の伝送速度が 100 万ビットであることを意味します。データ通信での帯域幅の測定基準です。

Microsoft Office ファイル Excel または Microsoft Word などの Microsoft Office ツールで作成されたファイル。

N

NAT デバイス ネットワークアドレス変換デバイス。未登録の IP ネットワーク番号を使用して社内通信に利用され、その一方でインターネットとも良好な通信が可能なデバイス。プライベート アドレッシングと呼ばれる 1 つのパブリック IP アドレスを使用して、プライベート ネットワーク上の複数のホストがインターネットにアクセスできるようにすることが主な目的です。

NTP Network Time Protocol（ネットワーク タイム プロトコル）。データ ネットワーク上のコンピュータ システムのクロックを同期化するために使用する、時刻合わせ用プロトコル。

P

ping ping とは、TCP/IP ネットワークで使用される診断ツールを実行することで、あるホストから別のホストへの接続が正常に動作しているかを確認することができます。コマンドライン インターフェイスによる ping の実行例については、P.A-17 の「Ping IP」を参照してください。

POP3 Post Office Protocol のバージョン 3。クライアント コンピュータが常時接続ではないモバイル コンピュータなどの一時接続を介して、サーバから電子メールを受信するためのメッセージング プロトコル。

POP3 サーバ POP3 電子メールのホスティング サーバで、ユーザのネットワークのクライアントはこのサーバを介して POP3 メッセージを受信します。

R

ROMMON ROM 監視プログラム。ROMMON は ROM で実行されるシングルスレッド プログラムで、ボードを初期化し、より高度なオペレーティング システムをロードします。ROMMON はデバッグやシステムを手動でブートする目的で使用します。

S

SMTP Simple Mail Transfer Protocol（シンプル メール転送プロトコル）。電子メールの転送で使用するプロトコルで、通常はイーサネットを介してコンピュータ間を転送する際に使用します。これはサーバ間通信で使用するプロトコルのため、メッセージにアクセスする場合は別のプロトコルを使用します。

SOCKS4 ファイアウォール ホストで TCP（トランスミッション コントロール プロトコル）セッションの中継となるプロトコルで、アプリケーション ユーザがファイアウォールに対して透過的にアクセス制御できるようにします。

SSL Secure Sockets Layer。インターネットのセキュア通信プロトコル。

T

TAC TAC（Technical Assistance Center）。

TCP/IP Transmission Control Protocol/Internet Protocol。TCP はネットワーキング プロトコルの一種で、IP（インターネット プロトコル）と組み合わせてコンピュータ システムからインターネットへの通信を管理する方法が最も一般的です。

TELNET TCP/IP（Transmission Control Protocol/Internet Protocol）の最上位で実行されるリモート ログイン用のインターネットの標準プロトコル。この用語は、リモート ログイン セッションのターミナル エミュレータとして動作するネットワーキング ソフトウェアのことを指す場合もあります。

TFTP Trivial File Transfer Protocol。リモート サーバとのファイルの読み書きで使用される簡潔なファイル転送プロトコル。

U

UDP User Datagram Protocol（UDP）は、TCP/IP プロトコル スイートのプロトコルの 1 つで、アプリケーション プログラムからリモート マシン上の他のアプリケーション プログラムにデータグラムを送信できるようにします。基本的に、UDP は信頼性の低いコネクションレス型のデータグラム サービスを提供するプロトコルで、データが配信される保証はなく、重複検出もされません。確認応答は実行せず、到着順序の前後も制御しません。

URL Uniform Resource Locator。オブジェクトの位置を指定する標準的な方法。一般に、インターネット上の Web ページを *www.cisco.com* のように指定します。URL は、DNS によって IP アドレスにマッピングされます。

V

VBscript ウィルス VBscript（Microsoft Visual Basic スクリプト記述言語）は、簡易プログラミング言語の一種で、Web 開発者は、ブラウザで表示する HTML ページに対話的な機能性を追加できます。たとえば、開発者は VBscript を使用して Web ページに「Click Here for More Information」（詳しくはここをクリック）ボタンを追加することがあります。

VBscript ウィルスは、HTML コードに書かれたこれらのスクリプトをターゲットにしたウィルスです。Web ページにウィルスを常駐させることができ、ユーザのブラウザを通じてデスクトップにウィルスをダウンロードします。

「JavaScript ウィルス」も参照。

W

Web ワールド ワイド ウェブ。ウェブまたはインターネットとも呼ばれます。

Web サーバ Web サイトで実行中のサーバ プロセスを指し、リモート ブラウザからの HTTP 要求に応答して Web ページを送信します。

Z

Zip of Death 解凍時、著しく大きく（たとえば 1000 %）展開する zip （またはアーカイブ）ファイル、または数千の添付ファイルを含む zip ファイル。圧縮ファイルは、スキャン時に解凍する必要があります。巨大なファイルは、ネットワークを低速化または停止させる場合があります。

zip ファイル WinZip などのファイル保管プログラムを使用して、1 つまたは複数のファイルを圧縮アーカイブ（別名「zip ファイル」）にしたもの。

あ

アーカイブ 1 つまたは複数の（通常は 2 つ以上）個別ファイルと情報を含む単一のファイルで、.zip ファイルなどがあります。適切なプログラムを使用して解凍（分離）できます。

アクション（「ターゲット」および「通知」も参照） 次の場合に実行される操作です。
— ウィルスまたは他の脅威が検出された
— ファイル ブロッキングがトリガーされた
主なアクションには、クリーニング、削除、または通過（何もせずに配信 / 転送すること）があります。何もせずに配信または転送することは推奨しません。感染のリスクを伴うメッセージによって、ユーザのネットワークが汚染される可能性があります。

アクセス（動詞） データを読み書きするための権限です。ほとんどのオペレーティング システムでは、業務の責任に応じて、複数のレベルのアクセス権を定義できます。

アクセス（名詞） コンピュータやサーバなどのストレージ デバイスとの間でデータの読み取りまたは書き込みを行うことを指します。

アクティベーション インストール プロセス中に、Activation Codes Configuration ウィンドウにアクティベーション コードを入力して、ユーザの Trend Micro InterScan for Cisco CSC SSM ソフトウェアをイネーブルにすることを指します。製品がインストールされてアクティベーションされるまで、SSM は動作可能になりません。

アクティベーション コード ハイフンを含む 37 文字のコードで、Trend Micro InterScan for Cisco CSC SSM のアクティベーションに使用します。SM-9UE2-HD4B3-8577B-TB5P4-Q2XT5-48PY4 などのアクティベーション コードがあります。

圧縮ファイル 1 つまたは複数の個別のファイルが含まれている単一のファイルのことで、WinZip などの適切なプログラムで解凍することができます。

アドレス ネットワーキング アドレス（「IP アドレス」を参照）または電子メールアドレスを指します。電子メール メッセージの発信元または宛先を指定する文字列です。

暗号化 暗号化は、意図された受信者のみ読み取り可能な形式にデータを変換するプロセスを指します。メッセージを解読するには、暗号化されたデータの受信者は適切な復号化鍵が必要です。従来の暗号化スキームでは、送信者と受信者はデータの暗号化と復号化を同じ鍵を使用して行います。公開鍵暗号化スキームでは、誰でも使用できる公開鍵と、作成者本人だけが所有する、公開鍵に対応した秘密鍵の 2 種類を使用します。この方法では、所有者の公開鍵を使用して暗号化したメッセージを送信するのは誰でもできますが、これを解読するのに必要な秘密鍵は所有者だけが持っています。PGP（Pretty Good Privacy）および Data Encryption Standard（DES; データ暗号規格）の 2 種類は、最も一般的な公開鍵暗号化スキームです。

アンチウィルス　コンピュータ ウィルスを検出してクリーニングする設計のコンピュータ プログラム。

アンチスパム　広告、わいせつ文書、その他の「迷惑」メールを識別してこれらが配信されないようにする目的で設計されている、フィルタリング メカニズム。

アンチスパム ルールおよびアンチスパム エンジン　スパムを検出およびフィルタリングする Trend Micro 社のツール。

い

イメージ ファイル　2 次元のシーンを表すデータ、つまり画像が含まれているファイル。イメージは、デジタル カメラなどを通じて現実世界から取り出したり、グラフィック ソフトウェアを使用したコンピュータで生成することができます。

インターネット　クライアントサーバ型のハイパーテキスト情報取得システム。ルータに接続した一連のネットワークを基盤としています。インターネットは最新の情報システムで、広告、オンライン販売、サービスの分野で広く受け入れられているメディアであり、大学やその他の研究機関のネットワークとしても利用されています。インターネットで最もよく知られているのがワールド ワイド ウェブです。

イントラネット　外部のインターネットが提供するサービスと同様のサービスを企業内部に提供する、すべてのネットワーク。必ずしもインターネットに接続するわけではありません。

う

ウィルス　コンピュータ ウィルスは、一種のプログラムで、小さな実行可能コードです。感染、増殖するという固有の特性を持っています。生物学上のウィルス同様、コンピュータ ウィルスも急速に増殖が拡大するために根絶が難しい場合がよくあります。

増殖することに加え、一部のコンピュータ ウィルスは、ウィルスのペイロードを伝達するダメージ ルーチンという別の共通性を持つものがあります。ペイロードはメッセージまたはイメージの表示だけを実行する一方で、ウィルスはファイルの破壊、ハード ドライブの再フォーマット、その他の破壊行為を働く場合があります。ウィルスにダメージ ルーチンが含まれていなくても、ストレージ内で多くのスペースやメモリを占有したり、コンピュータの全体的なパフォーマンスを低下させたりします。

ウィルス キット　ウィルスを作成、実行するためのソース コードのテンプレート。インターネットから入手可能。

ウィルス作成者　悪質なコンピュータ ハッカーの別名。ウィルス コードを作成する人物を指します。

ウィルス署名　ウィルス署名は、特定のウィルスを識別する固有のビット文字列です。Trend Micro のウィルス パターン ファイルに保存されています。Trend Micro のスキャン エンジンでは、ファイル同士でコードを比較します。たとえば、電子メールのメッセージ本文や HTTP ダウンロードの内容をパターン ファイルの署名と比較します。一致が見つかってウィルスが検出されると、適切な処置が取られます（クリーニング、削除、検閲など）。

ウィルス トラップ　分析を目的としてウィルス コードのサンプルのキャプチャするためのソフトウェア。

え

エクスプロイト　ソフトウェアの脆弱性またはセキュリティ ホールを狙ったウィルス コードです。エクスプロイトは脆弱性のあるコンピュータに広がり、複雑なルーチンを実行することができます。

お

大文字と小文字が一致 「大文字と小文字の照合」を参照。

大文字と小文字の照合 単語と大文字小文字の区別が一致しているテキストをスキャンすること。たとえば、コンテンツ フィルタに「dog」と追加すると、大文字と小文字の照合機能をイネーブルにしている場合は、「Dog」が含まれるメッセージはこのフィルタを通過する一方、「dog」は検知されます。

音声ファイルまたはビデオファイル 音楽などの音声やビデオ映像が含まれているファイル。

オンライン ヘルプ GUI とともにバンドルされている文書。

か

管理者 「システム管理者」を参照。新規ハードウェアやソフトウェアのセットアップ、ユーザ名やパスワードの割り当て、ディスク スペースやその他の IT リソースの監視、バックアップの実施、ネットワーク セキュリティの管理などを企業内で行うときの責任者を指します。

管理者アカウント 管理者レベルの特権を持つユーザ名およびパスワード。

管理者用電子メール アドレス Trend Micro InterScan for Cisco CSC SSM の管理者が使用する、通知やアラートを管理するためのアドレス。

き

キーロガー キーロガーは、キーボードから実行されるすべてのアクティビティを検知して保存するプログラムです。企業が従業員の業務を監視したり、保護者が子供の行動を把握する目的で使用する場合は、キーロギング プログラムは正当な利用法です。しかし、犯罪者も、他人のログオン資格情報やクレジット カード番号などの貴重な情報をソートする目的で、キーストロークの記録を利用します。

キャッシュ 小さな高速メモリで、最近アクセスされたデータを保持することにより、同じデータへの次回のアクセスを高速化する目的で設計されています。この用語は、主にプロセッサからメモリへのアクセスで使用されますが、ネットワークなどを介してアクセスされるローカルのデータ コピーに対しても使うことができます。

キュー メールを処理速度より高速で受信した場合に複数のリソース要求に順序付けするためのデータ構造。メッセージは、FIFO（ファーストイン ファーストアウト）手法により、先にキューの最後に追加されたものから順にキューから取り出されます。

く

クライアント 他のコンピュータ システムまたはプロセス（サーバ）に対し、特定のプロトコルを使用してサービスを要求し、このサーバの応答を受け入れるコンピュータ システムまたはプロセス。クライアントは、クライアント / サーバ ソフトウェア アーキテクチャの一部です。

クライアント / サーバ環境 サーバ タスクとクライアント タスクにソフトウェアを分散させる、分散型システムの代表的な形態です。クライアントは、プロトコルに準拠した要求をサーバに送信し、情報またはアクションに関する問い合わせを行い、サーバはこれに応答します。

クリーニング ファイルまたはメッセージからウィルス コードを取り除くこと。

グループ ファイル タイプ 共通のテーマを持つファイル タイプ。Trend Micro InterScan for Cisco CSS SSM のインターフェイスには、次の 5 種類のグループ ファイル タイプがあります。
— 音声 / ビデオ
— 圧縮
— 実行可能プログラム
— イメージ
—Microsoft Office

グレイウェア ソフトウェアのカテゴリの 1 つで、違法ではないが迷惑または嫌がらせとなるソフトウェア。ウィルス、ワーム、トロイの木馬型プログラムとは異なり、グレイウェアは感染、増殖、またはデータの破壊はしないものの、プライバシーが侵害される場合があります。グレイウェアの例には、スパイウェア、広告プログラム、リモート アクセス ツールがあります。

け

ゲートウェイ 情報の発信元と Web サーバとの間のインターフェイス。

原因 URL ブロッキングやファイルブロッキングなどの防御的措置がトリガーされた理由。この情報はログファイルに表示されます。

こ

公開鍵暗号化 送受信を行う双方が、公開鍵と秘密鍵と呼ばれるペアになった「鍵」を使用する暗号化スキーム。両者の持つ公開鍵は公開されていますが、一方の秘密鍵は公開せずに秘密にします。メッセージの暗号化は目的の受信者の公開鍵を使用して行いますが、復号化には受信者自身の秘密鍵を使う必要があります。「認証」*および*「デジタル署名」も参照。

広告プログラム 広告を目的としたソフトウェアで、プログラムの実行中に広告バナーを表示します。広告プログラムには「バックドア」をインストールし、ユーザが知らない間にコンピュータを追跡するものがあり、これらは「スパイウェア」と呼ばれています。

混合型脅威による攻撃 複数のエントリ ポイントや企業ネットワークの脆弱性を悪用する複雑な攻撃。「Nimda」または「Code Red」などがこのタイプの脅威です。

コンテンツ違反 コンテンツ フィルタリング ポリシーをトリガーしているイベント。

コンテンツ フィルタリング 電子メールの中に、嫌がらせメール、冒涜的な言葉や表現、わいせつな内容など、組織の人事部ポリシーまたは IT メッセージング ポリシーで禁止されている単語、または語句が含まれていないかスキャンします。

コンフィギュレーション ウィルスに感染した電子メール メッセージを通過させるか削除するかなど、Trend Micro InterScan for Cisco CSC SSM の機能に関するオプションを選択します。

さ

サーバ
他の（クライアント）プログラムに一定のサービスを提供するプログラム。クライアントとサーバの間の接続は、通常、ネットワークを通じたメッセージ伝達で確立される場合がよくあります。この場合は、いくつかのプロトコルを使用して、クライアントの要求とサーバの応答を符号化します。サーバは、要求が到着するのを待機しながら、継続的に稼動することができます（デーモンとして）。また、特定のサーバ数を制御するより高度なレベルのデーモンから呼び出される場合もあります。

セットアップ ウィザード
Trend Micro InterScan for Cisco CSC SSM のインストールで使用する、セットアップ プログラム。インストールに使用するセットアップ ウィザードには、次の種類があります。
—GUI セットアップ ウィザード。ASDM から起動します（ASDM オンライン ヘルプを参照してください）。
— コマンドライン インターフェイス（詳細は P.A-1 の「コマンドラインを通じたインストールおよび設定」を参照してください）。

し

シート
Trend Micro InterScan for Cisco CSC SSM を使用するための 1 人用ライセンスの呼び名です。

実行可能ファイル
機械語で書かれたすぐに実行できるプログラムを含んでいるバイナリ ファイル。

実際のファイル タイプ
IntelliScan で使用するウィルス スキャン技術で、ファイルの拡張子に関わらず（拡張子では識別を誤る可能性がある）ファイルのヘッダーを検証してファイルの情報タイプを識別します。

受信者
電子メール メッセージの宛先となる人物または組織。

承認済み送信者
ユーザのネットワークで常に許容されるメッセージの送信者。

署名ベースのスパム検出
電子メール メッセージにスパムが含まれていないかを判別する方法。メッセージの内容をスパム データベースのエントリと比較して行います。メッセージをスパムと特定するには、完全一致を検索する必要があります。署名ベースのスパム検出で誤検知が検出されることはほぼゼロですが、スパム署名ファイルのテイストに一部だけ一致するような新種のスパムは検出しません。
「ルールベースのスパム検出」も参照。
「false positive」も参照。

信頼できるドメイン
メッセージがスパムかどうかを検討せず、Trend Micro InterScan for Cisco CSC SSM が常時メッセージを受信するドメイン。たとえば、Example, Inc. という企業に子会社 Example-Japan, Inc. があるとします。子会社の example-japan.com からのメッセージは、親会社の example.com ネットワークでスパムかどうかをチェックせずに常に受け入れられます。これは、メッセージの送信元が、既知でかつ信頼できることが明らかなためです。

信頼できるホスト
常に適正に動作し、ユーザのネットワークを介してスパムなどをリレーしないため、ユーザのネットワークを通じてメールをリレーすることが許可されているサーバ。

す

スキャン
ファイルを順番に検証して特定の条件を満たしているか調べることを指します。

スキャン エンジン
アンチウィルス スキャンと統合しているホスト製品での検出を実行するモジュール。

スクリプト
プログラミング コマンドのセットで、呼び出されると、同時に実行されます。「スクリプト」と同義の用語には、「マクロ」または「バッチ ファイル」があります。

スタンプ
識別用の ID を配置すること。電子メール メッセージの件名フィールドに「スパム」などと印を付けることを指します。

ステータスバー ユーザ インターフェイスの機能の 1 つで、特定のアクティビティに関するステータスまたは進捗状況を「ユーザのマシンにファイルのロード中」などと表示します。

スパイウェア 広告目的でサポートされているソフトウェアで、ユーザの情報を他人に送信することができる、追跡用のソフトウェアをユーザのシステムにインストールします。どのデータが収集され、これがどのように使用されるか、ユーザ側で制御できないことが脅威です。

スパム 製品またはサービスを宣伝販売することを目的に送りつけられる電子メール メッセージ。

せ

セキュア パスワード認証 暗号化やチャレンジ / レスポンス方式などを使用して通信を保護する認証プロセス。

セキュリティ セキュリティとは、コンピュータを介して保存または転送されたデータが正当な権限を持たない個人からアクセスできないようにする技術を指します。システム セキュリティを確立する手法としては、データの暗号化やパスワードの適用が代表的です。

そ

増殖 自分自身を複製すること。このマニュアルでは、自己増殖が可能なウィルスやワームを指す場合に使用します。

送信者 電子メール メッセージを他の人物または組織に送信する送り主。

た

ターゲット（「アクション」および「通知」も参照） 電子メール メッセージで検出されるウィルスなど、違反的なイベントを監視するためのアクティビティの範囲。たとえば、ウィルス スキャンするターゲットを、ネットワークを通過するすべてのファイルをターゲットにしたり、特定の拡張子の付いたファイルのみにしたりできます。

ダイヤラ トロイの木馬型のプログラムで、実行されるとユーザのシステムから有料サイトに接続します。無防備なユーザが知らぬ間に課金される仕組みになっています。

ダウンロード（動詞） あるコンピュータから別のコンピュータにデータを転送すること。ダウンロードとは、主に、サイズの大きい方の「ホスト」システム（特にサーバまたはメインフレーム）から小さい方の「クライアント」システムへの転送を意味します。

ダウンロード（名詞） たとえば、Web サイトから HTTP を介してダウンロードされたデータ。

ダメージ ルーチン 破壊行為を実際に行うウィルス コードの部分を指し、ペイロードとも呼ばれます。

ち

着信 ユーザのネットワークに、電子メール メッセージまたは他のデータが入ってくることです。

つ

通知（「アクション」および「ターゲット」も参照）

次のいずれか、または複数の宛先に転送されるメッセージです。
— システム管理者
— メッセージの送信者
— メッセージの受信者、ファイルのダウンロード、ファイルの転送
通知の目的は、HTTP ファイルのダウンロードでウィルスが検出されたなどの、禁止されたアクションが取られた、または試行されたことを知らせることです。

て

デーモン

明示的には呼び出されないが、一定の条件になるまで休止状態で待機するプログラム。この条件の主体である人物は、デーモンが潜んでいることに気づいている必要はありません。

デジタル署名

送信者とメッセージ データを識別、および認証するメッセージに添付される付属データで、公開鍵暗号化と呼ばれる手法を採用しています。「公開鍵暗号化」*および*「認証」も参照。

デフォルト

CSC SSM コンソールのインターフェイスのフィールドに、事前に入力されている値。デフォルト値は、論理的な選択肢を表示し、効率化を目的として提供されます。デフォルト値はそのままの状態で使用したり、変更することができます。

添付ファイル

電子メールのメッセージに付属し、共に送信されるファイル。

と

トップレベル ドメイン（tld）

インターネットの完全修飾ドメイン名で最も重要なコンポーネントで、「.」より後ろの部分です。たとえば、host *wombat.doc.ic.ac.uk* のトップレベル ドメインは「uk」（英国のドメインを表す）です。

ドメイン名

システムの完全名で example.com など、自身のローカル ホスト名とそのドメイン名で構成されています。ドメイン名は、インターネット上のすべてのホストに固有のインターネット アドレスが割り当てられるようにする必要があります。このプロセスは「名前解決」と呼ばれ、ドメイン ネーム システム（DNS）を使用します。

トラフィック

インターネットとユーザ ネットワークとの間で送受信されるデータの流れ。

トリガー

アクションを引き起こす原因となるイベント。たとえば、Trend Micro InterScan for Cisco CSC SSM は、電子メール メッセージのウィルスを検出します。このウィルス検出によってメッセージが*トリガー*され、システム管理者、メッセーの送信者、およびメッセージの受信者に通知が送信されます。

トロイの木馬

無害を装った悪意のあるプログラム。トロイの木馬型ウィルスは増殖しない実行プログラムですが、外部から侵入しやすいようにポートをオープンにするなど、システムに常駐して悪質な行為を働きます。

ドロッパー

ドロッパーは、ウィルス、トロイの木馬型ウィルス、またはワームなどをシステムに運んで投下するメカニズムを持つプログラムです。

に

認証

人物またはプロセスの ID を検証すること。認証によってデジタル データが目的の受信者に確実に伝送されるようになります。認証によって、メッセージの正当な受信者とその発信元（メッセージがどこからまたは誰によって送信されたか）も明らかになります。

最も簡単な認証は、特定のアカウントにアクセスする際にユーザ名とパスワードを求める方法です。認証プロトコルは、Data Encryption Standard（DES; データ暗号規格）などの秘密鍵暗号化や、デジタル署名を使用した公開鍵システムに準拠したものにすることも可能です。

「公開鍵暗号化」*および*「デジタル署名」も参照。

ね

ネットワーク ウィルス

TCP、FTP、UDP、HTTP などのネットワーク プロトコル、および電子メール プロトコルを使用して増殖するタイプのウィルス。ネットワーク ウィルスには、システム ファイルを改変したり、ハード ディスクのブート セクタを変更しないものもよくあります。その代わりに、クライアント マシンのメモリに感染し、トラフィックを通じてネットワーク中に広がることによって、処理の低速化や完全なネットワーク障害を引き起こす場合があります。

は

バイナリ

ゼロと 1 による数字の表現。デジタル エレクトロニクスとブール代数で容易に実装可能なため、ほぼすべてのコンピュータで使用されています。

パスワード クラッカー

パスワードをなくしたり忘れたときに復元するために使用するアプリケーション プログラム。これらのアプリケーションは、コンピュータまたはネットワーク リソースへの不正アクセス権を手にするために侵入者が使用する場合があります。

パターン ファイル (オフィシャル パターン リリースとも呼びます)

オフィシャル パターン リリース（OPR）としても知られるパターン ファイルで、報告されたウィルスの最新のパターンを集めたものです。パターン ファイルは、最新のウィルスの脅威から最大限に身を守ることができるように、複数の重要なテストをパスしたことが保証されています。このパターン ファイルは、最新のスキャン エンジンと共に使用すると最も効果を発揮できます。

ハッカー

「ウィルス作成者」を参照。

ハッキング ツール

攻撃されやすいセキュリティ上の脆弱性を検索するために、コンピュータ システムやネットワークのペネトレーション テスト機能を持つ、ハードウェアやソフトウェアのツール。

発信

電子メールまたは他のデータが、ユーザのネットワークを*離れて*インターネットに送出されること。

パラメータ

値の範囲（1 から 10 までの数など）を表す変数。

ひ

ヒューリスティック ルールベース スキャン

ネットワーク トラフィックのスキャン方法の 1 つで、プロパティの論理分析を使用することにより、解決法を検索する際の制約を少なくする手法。

ふ

ファイアウォール

特定のセキュリティ対策を備えているゲートウェイ マシン。外部のネットワーク（特にインターネット）との接続およびダイヤルイン回線で使用されます。

ファイル 電子メール メッセージまたは HTTP ダウンロードなどのデータ要素。

ファイル感染ウィルス ファイル感染ウィルスは、実行可能プログラム（一般に、拡張子が .com または .exe のファイル）に感染します。このようなウィルスの大部分は、自身を他のホスト プログラムに複製しようとしますが、感染先のプログラムのオリジナル コードの一部を上書きすることで、結果的にプログラムを破壊するものもあります。これらのプログラムの一部は非常に破壊力が強く、事前に定義された時刻にハード ドライブを初期化しようとしたり、その他の悪質な被害をもたらす場合があります。

ファイル感染ウィルスは、ほとんどの場合で感染したファイルから正常に削除できます。ただし、ウィルスがプログラム コードの一部を上書きした場合は、オリジナルのファイルを復元することはできません。

ファイル タイプ ファイルに保存されているデータの種類。ほとんどのオペレーティング システムは、ファイル名の拡張子でファイル タイプを判別します。ファイル タイプは、ファイルをユーザ インターフェイスで表示するための適切なアイコンを選択したり、ファイルの表示、編集、または印刷を実行するための正しいアプリケーションを選択する場合に使用します。

ファイル名の拡張子 主に、ファイルに保存されているデータの種類を示す、ファイル名の一部分（.txt または .xml など）。ファイルが保持する内容の種類をユーザに示すだけでなく、ファイル名の拡張子は、一般に、ファイルが実行される際にどのプログラムを使用するかを決定します。

フィッシング フィッシングは、急速に被害が広がっている詐欺行為の一種で、正規の Web サイトを模倣することで Web ユーザから個人情報を不正に入手しようとします。

フィルタリング基準 メッセージや添付がある場合に、これらを送信するかどうかを決定するために、ユーザが指定するガイドライン。次のようなものがあります。
— メッセージ本文と添付のサイズ
— メッセージの件名に単語またはテキスト文字列があるかどうか
— メッセージの本文に単語またはテキスト文字列があるかどうか
— 添付データの件名に単語またはテキスト文字列があるかどうか
— 添付データのファイル タイプ

ブート セクタ ウィルス ブート セクタ ウィルスは、コンピュータのブート セクタ（オペレーティング システム）をターゲットとして攻撃するウィルスです。コンピュータ システムがブート セクタ ウィルスによる攻撃を最も受けやすいのは、フロッピー ドライブを介して感染したディスクでシステムを起動したときです。ウィルスにとっては、ハード ディスクを感染させることが目的のため、ブート自体を成功させる必要はありません。

また、外部プログラムを通じてブート セクタを感染させるウィルスもいくつか存在します。マルチパータイト型ウィルスと呼ばれる、比較的まれな種類があります。システムが一度感染すると、ブート セクタ ウィルスは、このコンピュータがアクセスしたすべてのディスクに感染を試みます。一般に、ブート セクタ ウィルスは正常に削除できます。

不快なコンテンツ 冒涜、セクシャル ハラスメント、人種差別、嫌がらせメールなど、他人に対する侮辱や攻撃と見なされる言葉や表現が含まれるメッセージ、または添付ファイル。

ブラウザ Internet Explorer や Mozilla など、ハイパーテキストの読み取りを可能にするプログラム。ブラウザには、ノード（「ページ」）のコンテンツを表示したり、1 つのノードから別のノードに移動する機能があります。ブラウザは、リモートの Web サーバのクライアントとして動作します。

プロキシ 他のサーバから利用可能な項目のキャッシュを提供するプロセス。アクセスは低速で高価になることが予想されます。

プロキシ サーバ ワールド ワイド ウェブのサーバ。特殊なプレフィックスが付いた URL を受け入れて、ローカル キャッシュまたはリモート サーバから文書を取り出す際にこれを使用し、要求側にこの URL を戻します。

ブロック ユーザのネットワークに侵入されないように防止することを指します。

ブロックされた送信者 送信するメッセージがユーザのネットワークに届かないように拒否されている送信。

へ

ペイロード ペイロードとは、感染したコンピュータでウィルスが実行する処理を指します。メッセージを表示したり CD ドライブをイジェクトするなど、比較的被害が少ない場合もありますが、ハード ドライブ全体を削除するなどの破壊行為が行われる場合もあります。

ヘッダー ファイルまたは送信に関する透過的な情報を含む、データ パケットの一部。

ほ

ポート 通信システムにおける論理チャネルまたはチャネルのエンドポイントで、同一コンピュータの同一ネットワーク インターフェイスに存在する複数の論理チャネル間を区別するために使用します。アプリケーション プログラムにはそれぞれ固有のポート番号が割り当てられています。

ホスト ネットワークに接続するコンピュータ。

ポリモーフィック型ウィルス 複数の形式を取ることができるウィルス。

ま

マクロ アプリケーション内の特定の機能を自動的に実行するコマンド。

マクロ ウィルス 他のウィルス タイプとは異なり、マクロ ウィルスはオペレーティング システムでのみ脅威となるわけではなく、電子メールの添付ファイル、Web のダウンロード、ファイル転送、または共有アプリケーションといった様々なメディアを通じて、感染が広がる可能性があります。

マスメーラ（またはワーム） 大量のネットワーク トラフィックを発生させるため、潜在的に有害な悪意のあるプログラム。

マルウェア（悪意のあるソフトウェア） ウィルス、ワーム、およびトロイの木馬など、有害な活動を目的として開発されるプログラミングまたはファイル。

マルチパータイト型ウィルス ブート セクタ型ウィルスとファイル感染ウィルスの両方の特徴を持つウィルス。

め

メッセージ メッセージ ヘッダーの件名とメッセージの本文が含まれている電子メール メッセージのことです。

メッセージ サイズ メッセージと添付ファイルのサイズを KB または MB で表したものです。

メッセージの件名 電子メールの見出しまたはトピックのことで、「第 3 四半期の結果」または「金曜日のランチ」などと記されます。

免責条項 電子メール メッセージの冒頭または末尾に追加されている文で、メッセージに関する法的および機密上の条件について説明したものです。オンライン ヘルプの **SMTP Configuration - Disclaimer** ウィンドウで例文を確認することができます。

ら

ライセンス Trend Micro InterScan for Cisco CSC SSM を合法的に使用するための認可。

ロード バランシング ロード バランシングは、並列処理の効率を向上させる目的で、作業をプロセッサにマッピング（または再マッピング）することです。

ロジック ボム アプリケーションまたはオペレーティング システムにひそかに挿入されるコードで、指定された条件が満たされた場合に、ある種の破壊行為やセキュリティ上の脅威となる行動を起こします。

り

リスニング ポート データ交換のためのクライアント接続要求で使用するポート。

リモート アクセス ツール システム管理者が合法的にネットワークをリモート管理できるようにするハードウェアおよびソフトウェア。一方、このようなツールはネットワーク システムの安全性を脅かそうとする侵入者も使用できる場合があります。

リンク（またはハイパーリンク） 1 つのハイパーテキスト文書のある地点から、別の文書または同じ文書内の別の場所を指し示す参照。リンクには、下線付き青色テキストなど、異なる色やテキストを使用するのが普通です。クリックなどを行ってリンクをアクティブにすると、ブラウザによってリンク先の情報が表示されます。

る

ルールベースのスパム検出 メッセージの特徴を分析して電子メール メールがスパムかどうかを判別する、ヒューリスティック評価に基づいたスパム検出手法の一種。スパム防止エンジンで電子メール メッセージを検証するときは、電子メールの内容とエントリについてルール ファイルに一致するものがあるかどうか検索します。ルールバースのスパム検出では、署名ベースのスパム検出より高い確率でスパムを検出できますが、同時に誤検知の可能性も高くなります。
「署名ベースのスパム検出」も参照。
「false positive」も参照。

わ

ワークステーション（またはクライアント） 一度に 1 人のユーザが使用することを目的に設計されている汎用コンピュータで、特にグラフィック、処理速度、同時タスク実行能力などの点で、通常、パーソナル コンピュータより高いパフォーマンスが装備されています。

ワーム 内蔵型の 1 つのプログラム（またはプログラム セット）で、自身の機能を複製したり、自身の一部を他のコンピュータ システムに感染させることができます。

ワイルドカード Trend Micro InterScan for Cisco CSC SSM では、コンテンツ フィルタリングを指す用語で、アスタリスク (*) を使用して任意の文字を表します。たとえば、*ber とした場合、barber、number、plumber、timber などの単語を表すことができます。トランプの 1 セットの中で、どの数または組のカードとしても使えるように特定のカードを「ワイルドカード」と呼んだトランプのゲームを語源としています。

割り込み 通常の処理を中断して、一時的に「割り込みハンドラ」ルーチンを通過するようにフロー制御を誘導する非同期イベント。

A

B

C

D

E

F

H

K

P

S

T

U

V

W

あ

い

お

か

き

く

こ

さ

し

す

せ

た

ち

つ

て

と

な

ね

は

ひ

ふ

ほ

ま

め

よ

ら

る

ろ