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。