

安心を、ひとつ上のステージへ。



報告

不正Webサイトに誘導するガンブラー攻撃が定番化
システム、運用、ユーザの3つのポイントを
軸にしたセキュリティ対策がカギに
2009年度、不正プログラムの動向総括

トレンドマイクロ広報紙 【トレンドパーク】

TREND PARK vol.19

March

2010

セキュリティのことで困ったら、まずはトレンドマイクロへ。

- トレンドマイクロ ホームページ <http://www.trendmicro.co.jp>
- セキュリティ情報 <http://jp.trendmicro.com/jp/threat/>
- ウイルス駆除ツール <http://www.trendmicro.co.jp/tool/>
- トレンドマイクロ モバイルサービス* <http://www.trendmicro.co.jp/mobile/>
- ウイルスバスター相談室 / 教えて!ウイルスバスター* <http://tmqa.jp>
- インターネット・セキュリティ・ナレッジ <http://is702.jp>

*携帯電話向け情報提供サービス

TECHNOLOGY

総合的な防御力を評価したNSS Labsのテスト
トレンドマイクロはあらゆる項目で最高の評価

NEW PRODUCTS

トレンドマイクロ、総合サーバセキュリティソリューション
「Trend Micro Deep Security™」の提供を開始

TOPICS

官民連携で情報セキュリティを啓発

安心を、ひとつ上のステージへ。



東京本社 〒151-0053 東京都渋谷区代々木 2-1-1 新宿メインズタワー TEL:03-5334-3600 FAX:03-5334-4008
 大阪営業所 〒532-0003 大阪府大阪市淀川区宮原3-4-30 ニッセイ新大阪ビル13F TEL:06-6350-0330 FAX:06-6350-0591
 名古屋営業所 〒460-0003 愛知県名古屋市中区錦 3-5-27 錦中央ビル 10F TEL:052-955-1221 FAX:052-963-6332
 福岡営業所 〒812-0011 福岡県福岡市博多区博多駅前 2-3-7 サンエビル 7F TEL:092-471-0562 FAX:092-471-0563

Copyright ©2010 Trend Micro Incorporated. All Rights Reserved. TRENDMICRO, ウイルスバスター, InterScan, INTERSCAN VIRUSWALL, ISVW, InterScanWebManager, ISWM, InterScan Message Security Suite, InterScan Web Security Suite, IWSS, TRENDMICRO SERVERPROTECT, Trend Micro Control Manager, Trend Micro MobileSecurity, VSAPI, トレンドマイクロ・プレミアム・サポートプログラム, Trend Park, Trend Labs, Trend Micro Network VirusWall, Network VirusWall Enforcer, LEAKPROOF, Trendプロテクト, InterScan Messaging Hosted Security, DataDNA, Trend Micro Threat Management Solution, Trend Micro Threat Management Services, Trend Micro Threat Management Agent, Trend Micro Threat Mitigator, Trend Micro Threat Discovery Appliance, Trend Micro USB Security, InterScan Web Security Virtual Appliance, InterScan Messaging Security Virtual Appliance, Trend Micro Reliable Security License, TRSL, Trend Micro Smart Protection Network, Smart Protection Network, SPNおよびSMARTSCANは、トレンドマイクロ株式会社の登録商標です。
 記載の内容は2010年3月現在のものです。内容は予告なく変更される場合があります。

P/N TPK-RS-1003



安心を、ひとつ上のステージへ。

トレンドマイクロは創業以来、
安全なデジタル社会の実現に寄与することを企業理念としてきました。

デジタル情報ネットワークはいまや生活に欠かせないインフラです。
しかし、ネットワークは常に予測不可能な脅威にさらされています。
コンピュータウイルスをはじめフィッシングやスパイウェア、
さらにこれまで誰も知ることもなかった新しい脅威が次々と生まれては、
デジタル社会のセキュリティを脅かし続けているのです。

そのような中で、人々が自由にそして安全に情報の交換を行えるよう、
スピードと品質を両立させた製品・サービスを提供していくことが
トレンドマイクロの使命です。

～安心を、ひとつ上のステージへ。
お客様の安心のため、さらなる前進と向上をめざす私たちの信念と姿勢を、
このメッセージが表現しています。

安心を、ひとつ上のステージへ。



TREND PARK vol.19

March

2010

TOPICS

官民連携で情報セキュリティを啓発

トレンドマイクロ株式会社は、株式会社シマンテック、マカフィー株式会社、独立行政法人情報処理推進機構、および経済産業省とともに、「セキュリティ普及促進委員会」を設立しました。

本委員会では、内閣官房が定める「情報セキュリティ月間」を機に、官民、そして企業の壁を超えて連携し、情報セキュリティの啓発活動を推進します。2月25日から、ご家庭における情報セキュリティ対策を改めて見直していただくため、家電量販店や銀行などにポスター1万枚を配布しています。

また3月9日には、「企業の情報セキュリティの課題と在り方」をテーマとする緊急セミナーを開催。企業が直面する情報セキュリティの課題と対応、米国や中国の最新セキュリティ事情、セキュアなクラウドコンピューティングや仮想環境などのセッションを、約500名の参加者の皆様に熱心に受講していただくことができました。

私たちは、こうした取り組みを通じて、インターネットを安全・安心に保つ努力を続けていきます。

CONTENTS

- 3 TOPICS
官民連携で情報セキュリティを啓発
- 4 Threat Report
不正Webサイトに誘導するランサム攻撃が定番化
システム、運用、ユーザの3つのポイントを
軸にしたセキュリティ対策がカギに
報告 2009年度、不正プログラムの動向総括
- 6 Technology
総合的な防御力を評価したNSS Labsのテスト
トレンドマイクロはあらゆる項目で最高の評価
- 8 New Products
トレンドマイクロ、総合サーバセキュリティソリューション
「Trend Micro Deep Security™」の提供を開始
- 10 News & Topics
トレンドマイクロ、パッチマネジメントに悩む企業管理者向けセミナーを開催
～Network VirusWall Enforcer™により、
未パッチやサポート切れのシステムを保護～
- 11 News & Topics
USBメモリ型ウイルス検索ツール
Trend Micro Portable Security™を発表

Internet Threat Report

インターネット脅威マンスリーレポート

2009年度、不正プログラムの動向総括

不正Webサイトに誘導するガンブラー攻撃が定番化 システム、運用、ユーザの3つのポイントを 軸にしたセキュリティ対策がカギに

トレンドマイクロは1月7日、都内で報道関係者向けセミナーを開催し、2009年度(2009年1月～12月)のインターネット上の脅威動向を総括しました。USBメモリをはじめとするリムーバブルメディアの自動実行機能を悪用する不正プログラムが、2009年度の不正プログラム感染被害総報告数の約8%を占めました。

また、「ガンブラー」をはじめとした正規Webサイトを改ざんし、サイト訪問者を不正プログラムの埋め込まれたWebサイトに誘導することで、ウイルス感染させる攻撃が増加していることを報告。2010年度の不正プログラムの傾向を予測し、「システム」「運用」「ユーザ」の3つのポイントを軸とした包括的なセキュリティ対策を行う必要性を説きました。



トレンドマイクロ株式会社
Threat Monitoring Center 課長
飯田朝洋

不正Webサイトに誘導する攻撃が急増

トレンドマイクロは2009年度の不正プログラム感染被害の報告数が4万5,310件となり、前年比で約20.3%減少したことを発表しました。その中でもUSBメモリをはじめとするリムーバブルメディアの自動実行機能を悪用する「MAL_OTORUN(オートラン)」の年間感染報告数は、最も多い3,617件。2008年に比べ約750件増加し、総報告数の約8%を占めました。この数字について、トレンドマイクロ株式会社 Threat Monitoring Center 課長 飯田 朝洋は、「USBメモリを媒介として感染を広げるオートランは、たとえゲートウェイやエンドポイントで高度なセキュリティ対策を行っていても防げません。これがUSBメモリを悪用するオートランの増加を後押ししています」と語ります。

また、Windowsの脆弱性などを狙い、複数の侵入経路で感染する2位の「WORM_DOWNAD(ダウンロード)」は、企業ユーザからの報告が99%を占めました。企業ユーザによる感染が相次ぐのは、個人ユーザと比べ、最新パッチファイルのタイムリーな適用が難しいため。2008年10月に確認された当初は単純にOSの脆弱性を狙うワームだったダウンロードの亜種が次々と登場し、USBメモリ経由の感染手法などを新たな機能として実装したことも要因でした。

今回のセミナーで最も大きなトピックが、不正プログラムの中でも2009年春より注目を集めた

「JS_GUMBLAR(ガンブラー)」です。正規Webサイトを改ざんし、サイト訪問者を不正プログラムの埋め込まれたWebサイトに誘導することでウイルス感染させる手口は年間を通じて確認されました。これらの攻撃に関連する不正プログラムでは、感染したPCのユーザ情報をはじめ、FTPサーバのログイン名やパスワードを盗む「TSPY_KATES(カテス)」や「TROJ_SEEKWEL(シークウェル)」、正規のWebサイトを装った不正Webサイトから不正プログラムをダウンロードさせる「JS_IFRAME(アイフレーム)」や「MAL_HIFRAME(ハイフレーム)」の4種が感染報告数の上位10種にランクインしました。

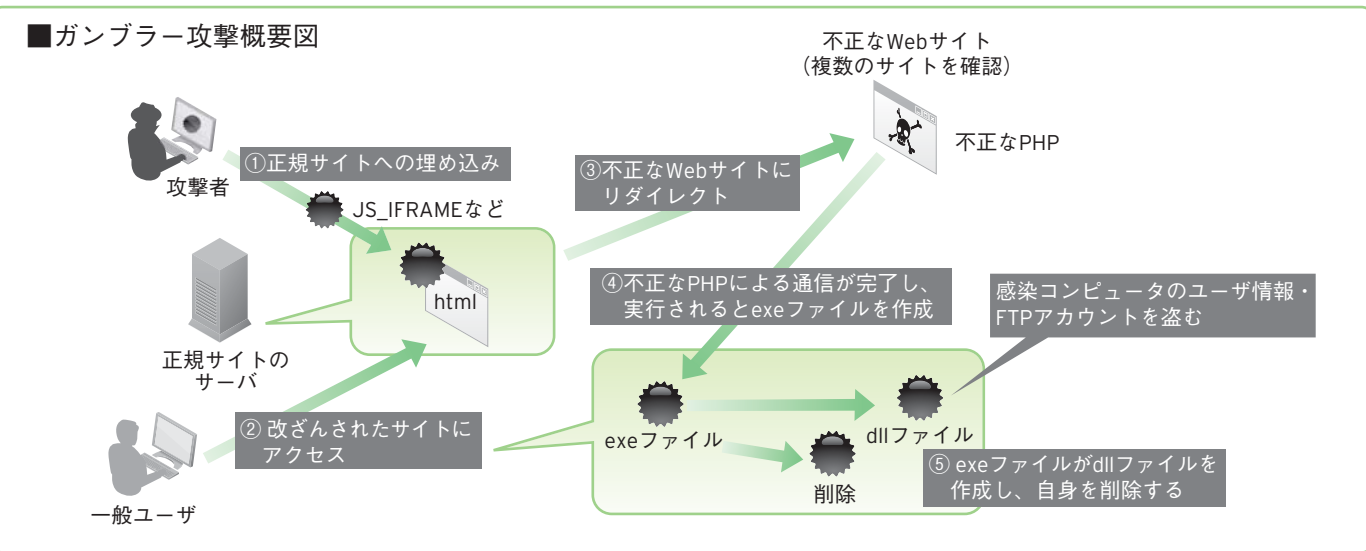
正規Webサイトを改ざんし、FTPサーバのアカウント情報を詐取

2009年12月の感染報告数で1位になったカテスは、ガンブラーやアイフレームなどが埋め込まれたWebサイトからリダイレクトされる不正なWebサイトより感染するケースが確認されています。Webサーバを構成するアプリケーションなどの脆弱性を利用し、企業のWebサイト管理者のPCからFTPサーバのログイン名やパスワードを詐取するのが特徴です。飯田は、「ユーザ企業には、FTPサーバへのアクセスに際してログイン名とパスワードを用いたベーシック認証だけでなく、暗号化やアクセス制御などの技術を利用する仕掛けも必要です」と話しました。

続いて登壇したトレンドマイクロ株式会社 Threat Monitoring Center セキュリティコンサ

トレンドマイクロ株式会社
Threat Monitoring Center
セキュリティコンサルタント
松川博英

DATA 開催日：2010年1月7日(木)



ルタント 松川 博英は、ガンブラー攻撃の一連の動きを仮想マシン上でデモンストレーションしました。「TROJ_DROPR.GB」は、Adobe ReaderやAcrobat、Flash Playerなどの脆弱性を利用して感染する不正プログラム。コンピュータの背後で作成したカテスがOS起動時に自動実行されるようレジストリを改ざんし、正常なシステムファイルのWINMM.dllが読み込まれたタイミングでカテスを実行します。以降、カテスはネットワークトラフィックを監視し、搾取したIDやパスワードなどの情報を攻撃者のサーバに送信します。

松川は、「カテスが収集したFTPサーバのアカウント情報は、感染したコンピュータがWebサーバに接続されたタイミングで外部に送信されます。攻撃者はこうして詐取したアカウント情報を利用してFTPサーバにアクセスし、正規Webサイトを改ざんすることでサイト訪問者を不正Webサイトに誘導します。これにより、複数の正規Webサイ



トに不正プログラムが埋め込まれ、被害の拡大につながってしまったのです」と解説しました。

セキュリティレベルの底上げが急務

2010年も引き続き、正規Webサイトの改ざんをはじめとするWebからの脅威が猛威を振るうと予想されます。その中で、「システム」「運用」「ユーザ」の3つのポイントを軸に包括的なセキュリティ対策を実施することが重要です。

「システム」では、パターンマッチング処理による対策に加え、振る舞い検知や不正Webサイトへのアクセスを遮断するWebレピュテーションなどの最新技術を複合的に組み合わせた対策が求められます。というのも、未知の不正プログラムが生み出されるスピードが加速する中、従来のパターンマッチング処理によってあらゆる脅威に対抗するには限界があるためです。

「運用」では、セキュリティ製品、パターンファイル、およびウイルス検索エンジンを常に最新の状態に保つことがカギになります。脅威の動向に合わせてUSBメモリの運用ポリシーやパスワードの設定ルールなどといった基本的な対策を見直し、柔軟に変更できる体制の構築もポイントです。飯田は、「企業では収益を上げる部門の都合が優先される傾向にあります。高度なセキュリティを実装するには、軽視されてしまいがちなIT部門がセキュリティツールの導入を主導できる環境作りが不可欠です」と語ります。

「ユーザ」では、セキュリティセミナーなどを通じて

ユーザが脅威の傾向を理解し、セキュリティ意識を高めることがポイント。2010年はソーシャルエンジニアリングを駆使し、オリンピックやワールドカップの情報を利用したスパムメールが横行すると予想されます。ユーザへのセキュリティ啓発を促し、こうした攻撃に対処するための施策の実行が必要です。

飯田は、「セキュリティレベルは、システム、運用、ユーザのかけ算によって算出されるため、ある要素がゼロならセキュリティレベルもゼロになってしまいます。特定のポイントだけを強化するのではなく、すべてのレベルの底上げが求められます」と話しました。

TP

インターネットの脅威に対抗できる最も安全・安心なソリューション

総合的な防御力を評価したNSS Labsのテスト トレンドマイクロはあらゆる項目で最高の評価

セキュリティ製品の性能を評価するテスト手法のあり方が問われています。従来のテスト手法は、不正プログラムの“検出率”にフォーカスしたもので、パターンファイルを用いて、ローカルの不正プログラムを検出する機能のみを評価しています。このテスト手法は、一日、あるいは一週間に数十から数百種程度しか不正プログラムが登場しない時代に考案されました。しかし、インターネット上の脅威は劇的に変化を続けています。

一体、どのようなテスト手法が、現在のセキュリティ製品の真の有効性を評価できるのでしょうか。



トレンドマイクロ株式会社
データセンター／コアテクノロジー マーケティンググループ
プロダクトマネージャー

染谷征良

総合的な防御力を 評価する必要性

不正プログラムの発生スピードは加速化し、現在では2.2秒に1つの新しい不正プログラムが登場しています。また、不正プログラムの約92%がWebサイトの閲覧やメールなど、インターネットを経由して侵入してきます。不正プログラムは従来の愉快犯によるものとは異なり、組織犯罪グループによって金銭や情報を不正に詐取するために使われています。そのため、不正プログラムが、セキュリティ製品に検出されないような仕組みを持ったりと巧妙化が進んでいるのです。

現在の主な侵入経路はWebサイトであり、何らかの方法で侵入した不正プログラムは、悪意のWebサイトに接続し、他の不正プログラムを呼び込む連鎖的な攻撃が主流です。また、悪意のWebサイトでは不正プログラムやURLが短時間で次々と入れ替えられ、対策を困難にさせています。そのため、最近のセキュリティ製品には、従来のパターンファイルによるウイルス検出機能だけでなく、スパムメール対策、ファイアウォール、システムへの不正な改ざんを検知する挙動監視、URLフィルタリングではないWebサーバの評価を用いて不審度を判断するレピュテーションといったさまざまな機能が搭載されています。

トレンドマイクロ株式会社 データセンター／コアテクノロジーマーケティンググループ プロダクトマネージャー 染谷征良は、「従来の製品テスト手法は、数週間から数ヶ月にわたって収集した既知の不正プログラムをオフラインのPCのハードディスクにコピーし、手動によるウイルス検索を一回限り実施するもの。ファイル検索技術の優位性のみを評価するテスト、つまり不正プログラムの“検出率”のみを評価するものでした。しかしながら、このテスト手法では巧妙化し、増加し続ける脅威に対するセキュリティ製品の実際の有効性を正しく評価することができません」と語ります。

製品の有効性を正当に評価するためには、単一の機能にフォーカスするのではなく、コンピュータを不正プログラムから守るさまざまな機能の集合体として、総合的な“防御力”を評価する必要があります。「総合的な防御力は、大きく2つのレイヤーがポイントになります。不正プログラムの発生源やネットワークレベルで不正プログラムがコンピュータに侵入してくるのを防ぐ“侵入レイヤー”と、コンピュータに侵入してしまった不正プログラムの実行をブロックする“感染レイヤー”です。正当に製品を評価するテスト手法は、インターネットから収集したリアルな不正プログラムを使用し、オンライン環境においてテストを実施するもの。繰り返しテストを行うことにより長期間にわたって脅威に対抗できる能力を見極めること、つまり“点”ではない“線”での評価も重要です」(染谷)

■総合的な防御力

・法人向け製品

ベンダー	総合
Trend Micro	93.6%
A社	89.0%
B社	86.3%
C社	82.2%
D社	81.6%
E社	80.7%
F社	75.2%
G社	67.5%
H社	67.1%
I社	62.5%

・個人向け製品

ベンダー	総合
Trend Micro	96.4%
A社	87.8%
J社	81.8%
C社	81.6%
D社	81.2%
E社	80.0%
H社	73.3%
F社	72.0%
G社	67.9%

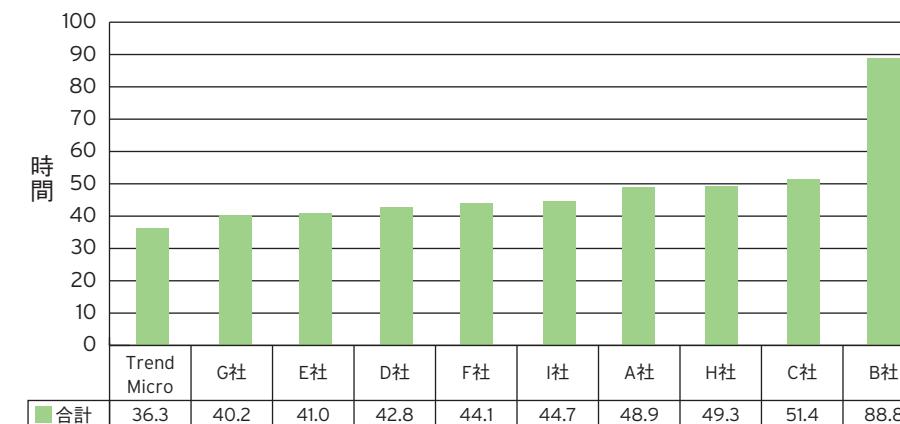
NSS Labsのテストで 最高の評価

米国に拠点を置く第三者テスト機関である「NSS Labs」が2009年7月から8月にかけて現在の脅威動向、製品動向や利用環境に即したテストを実施しました。具体的なテスト内容は、リアルタイムに収集した不正プログラムを使用し、オンライン環境において8時間ごとのテストを17日間にわたって実施。総合的な防御力だけでなく、デイゼロにおける防御力や時間軸による防御力の変遷、未対応の不正プログラムへの対応速度など、長期的な防御力を測るものです。

NSS Labsが実施した製品テストにおいて、トレンドマイクロは、コンシューマおよびコーポレート製品ともに最も高い数値を示しました。コーポレート製品では、感染レイヤーおよび侵入レイヤーにおける総合的な防御力が93.6%と、対象製品中最も高い割合で不正プログラムをブロックしました。また、8時間ごとにブロック率を測るテストでも、トレンドマイクロは継続して安定した防御力を発揮しています。最近の不正Webサイトは数十分や数時間のうちに新たな不正Webサイトに作り替えられるといった動きをするため、安定した防御力を示すこの指標は重要です。

染谷は、「ブロックできなかった不正プログラムへの対応を完了させるまでに要した時間でも、トレンドマイクロは、唯一40時間を切っています。

■不正プログラムをブロックするまでの平均対応時間(法人向け製品)



これらのテスト結果によって分かることは、クラウドの概念を採用したトレンドマイクロのレピュテーション技術が、ユーザのセキュリティ強化に大きく寄与していることです」と語ります。

このテスト結果の裏付けとなるトレンドマイクロの技術が、クラウドセキュリティ基盤の「Trend Micro Smart Protection Network™(以下、SPN™)」です。SPNでは、Webレピュテーション、E-mailレピュテーション、およびファイルレピュテーションの3つのレピュテーションデータベースを協調動作させ、あらゆる脅威情報を評価データベースに登録。評価データベースを参照し、不正Webサイトやスパムメール、危険なファイルを

ブロックすることで強固なセキュリティを実現します。染谷は、「新たな脅威の発生スピードが加速し、Webからの脅威が増加の一途をたどる中、クライアント環境で行うパターンマッチング処理では対応できません。現在の脅威に対抗する新しい技術としてSPNを開発しました。さまざまな技術やノウハウを組み合わせることで、総合的な防御力の高いセキュリティ基盤を備えていることがトレンドマイクロの最大の強みです」と話しました。 **IP**

出典: NSS Labs「エンドポイントセキュリティ ソーシャルエンジニアリングを悪用したマルウェア対策 比較テストの結果」2009年9月
<http://nsslabs.com/reprints/9b/EndpointProtection-3Q2009>

物理、仮想、クラウドコンピューティング環境のサーバセキュリティを確保

物理、仮想、およびクラウドコンピューティングのマルチプラットフォームに対応 トレンドマイクロ、総合サーバセキュリティソリューション 「Trend Micro Deep Security™」の提供を開始

トレンドマイクロは、企業向けの総合サーバセキュリティソリューション「Trend Micro Deep Security (以下、TMDS)」を発表しました。同製品は、「Deep Security エージェント」、「Deep Security Virtual Appliance」、「Deep Security マネージャ」から構成され、物理、仮想、およびクラウドコンピューティング環境のサーバに対して最適なセキュリティ機能を提供し、単一の管理ツールで集中管理できることが特長です。

激変するIT環境にフィットする セキュリティソリューションを展開

トレンドマイクロは2010年1月21日(木)、都内ホテルで行われた報道関係者向け発表会で、企業向け総合サーバセキュリティソリューションのTMDSを発表しました。同製品は3月15日(月)より出荷を開始しています。

発表会の冒頭、トレンドマイクロ株式会社 取締役 日本地域担当 大三川 彰彦は、「トレンドマイクロの2010年のキーワードは、『Security That Fits』です。IT分野のトレンドであるクラウドコンピューティングによって企業のIT環境が急速に変化する中、多様な市場ニーズにフィットすることが求められています」と語りました。

世界各国の大手130社のネットワーク環境を、2008年10月から2009年8月までトレンドマイクロが診断した結果、ポットウイルスが72%、情報漏えい関連不正プログラムが56%検出され、100%の企業で活動している不正プログラムを検出しました。企業を取り巻くさまざまな脅威が

増加している中で、トレンドマイクロは、「クラウドからセキュリティを確保する」クラウド型セキュリティ基盤「Trend Micro Smart Protection Network™」を軸に、広範なセキュリティソリューションを展開してきました。

大三川は、「セキュリティのリーディングベンダーであるトレンドマイクロは、強みであるエンドポイントセキュリティやサーバセキュリティ事業で培ってきた技術力を生かし、脅威の増加とともに多様化する顧客ニーズに対応していきます。今回のTMDSは、クラウド技術を取り入れながら進化する企業の多様なIT環境に対応し、「クラウドそのものを脅威から守る」総合サーバセキュリティソリューションです」と語りました。

OSやアプリケーションなどの脆弱性を狙った攻撃に対抗

続いて登壇したトレンドマイクロ株式会社マーケティング本部 本部長 九里 禎久は、TMDSについて説明しました。同製品はサーバにエージェントをインストールし、OSやアプリケーションなどの脆弱性を狙った攻撃を阻止するセキュリティソリューションです。1つのアーキテクチャで、物理、仮想、およびクラウドコンピューティング環境のすべてのサーバにセキュリティを提供し、単一の管理ツールで集中管理できることが特長です。

「仮想マシンの移動に伴う脅威、仮想マシンの増加によるセキュリティギャップ、クラウド上にあるサーバ間での攻撃など、従来からあるセキュリ

ティ問題に上乗せして、仮想化、クラウドコンピューティング特有の新しい問題が出てきています。IT環境の規模や形態に依存しないTMDSは、企業やデータセンターなど、物理サーバと仮想サーバが混在する環境のセキュリティとして有効です。」(九里)

セキュリティ状況を可視化し、 適切なサーバ保護を提供

Deep Security エージェントは、サーバ保護に必要なIDS/IPS、Webアプリケーション プロテクション、ファイアウォール、改ざん検知、セキュリティログ監視の5つの機能を実装。SQLインジェクションやクロスサイトスクリプティングなど、Webアプリケーションの脆弱性を狙った攻撃を防御したり、ファイルやレジストリの監視によってシステムへの不正な変更や改ざんを検知したりする複数の機能を組み合わせた多層防御を実現します。

Deep Security Virtual ApplianceはVMwareのセキュリティ技術「VMsafe API」を利用し、VMware vSphere 4で構築された仮想プラットフォーム上にインストールすることで、各ゲストOSを攻撃から守ります。Deep Security エージェントがインストールされていない仮想サーバを検知し、IDS/IPS、Webアプリケーションプロテクション、ファイアウォールの3つの機能を動的に提供します。

九里は、「仮想環境における大きなセキュリティ課題は、OSやアプリケーションに対する攻

撃が、物理環境と同等のダメージを仮想システムに与える可能性があることです。こうした課題を解決するソリューションとして提供を開始したDeep Security Virtual Applianceは、ハイパーバイザー層に実装することで仮想サーバ間の攻撃をブロックすることが可能です」と説明しました。

Deep Security マネージャは、物理、仮想、およびクラウドコンピューティング環境のサーバにインストールするDeep Security エージェントやDeep Security Virtual Applianceを集中管理するツール。Webベースの管理コンソールにより、セキュリティポリシー管理、レポート表示、タスクスケジュール設定、既存のログ統合システムや監視システムとの連携に関連する管理機能を提供し、サーバOSのセキュリティ状況を可視化します。

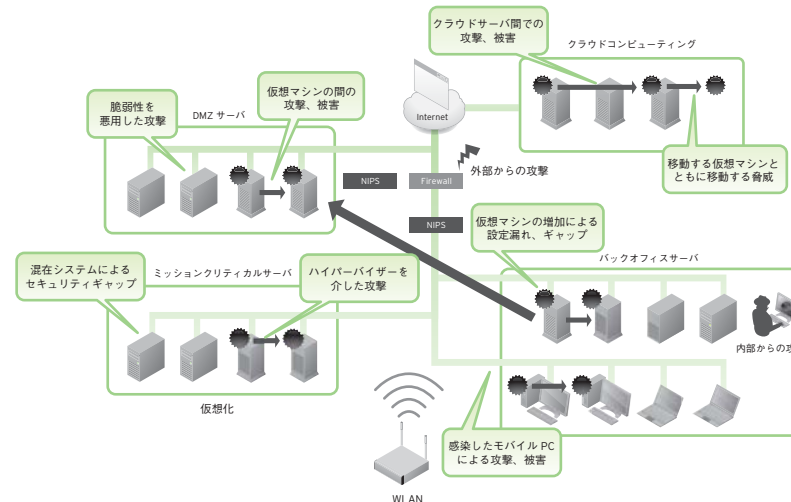
価格は、Deep Security エージェントが物理、仮想サーバを問わず、1エージェント 8万4,000円(税別)、Deep Security Virtual Appliance 23万円(税別)、管理ツールのDeep Security マネージャ 1管理サーバあたり23万5000円(税別)。本ソリューションはパートナー経由で販売します。



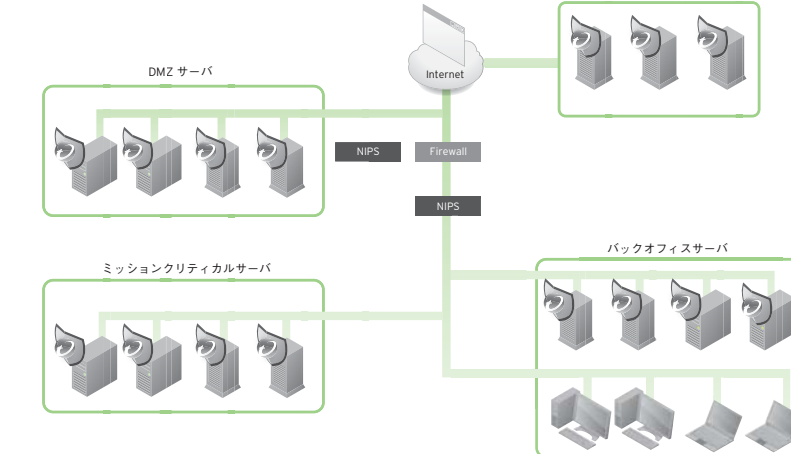
トレンドマイクロ株式会社
マーケティング本部 本部長
九里 禎久

製品名	システム要件
Deep Security エージェント	Microsoft ・ Windows 2000, Windows 7 ・ Windows XP, 2003 (32/64ビット) ・ Vista (32/64ビット) ・ Windows Server 2008 (32/64ビット)
	Solaris ・ 8, 9, 10 on SPARC ・ 10 on x86 (64ビット)
	Linux ・ Red Hat 4, 5 (32/64ビット) ・ SuSE 9, 10
	UNIX系 ・ HP-UX 11i (11.23, 11.31) ・ AIX 5.3 ※ HP-UX, AIX 用エージェントでは、改ざん検知及びログ分析機能のみが提供されます。
Deep Security マネージャ	Microsoft ・ Windows 2003/2008 (32/64ビット)
Deep Security Virtual Appliance	VMware ・ VMware vSphere 4

■境界線の無いサーバセキュリティ



■クラウド環境のサーバを守る新しいアーキテクチャ



トレンドマイクロ、パッチマネジメントに悩む企業管理者向けセミナーを開催
～Network VirusWall Enforcer™により、未パッチやサポート切れのシステムを保護～

OSやアプリケーションの脆弱性を狙う不正プログラムの出現は、後を絶ちません。また、複雑化するシステム環境において更新プログラムの適用にかかる負荷は大きく、事業継続性の観点からミッションクリティカルなサーバに最新のパッチを適用することが困難です。昨今の脅威動向として、一度、感染してしまうと連鎖的に不正プログラムが侵入してきてしまうことから、時として、完全復旧までに多大な時間と労力を要することがあります。トレンドマイクロはこうした課題を解決するツールとしてサーバやクライアントPCにインストールすることなく、脆弱性を狙う攻撃からシステムを保護するNetwork VirusWall Enforcerを提供しています。OSのサポート終了に伴って脆弱性の修正に必要なセキュリティパッチが提供されなくなったレガシーシステムの対策としても有効です。

企業を取り巻く脅威の現状

トレンドマイクロは2月25日(木)、都内において、近年の脅威動向やサポート切れOSに潜む危険性、企業に求められるセキュリティ対策などをテーマにしたセミナーを開催しました。

Web、メール、USBメモリなどを媒介して侵入・感染し、さまざまな機能をもった複数の不正プログラムを連鎖的にダウンロードさせるWebからの脅威は、2005年から2008年の4年間で約23倍に増加しています。これは不正プログラムの作成者が、自己顕示欲を満たすことを目的とする愉快犯から、詐取した機密情報を不当に換金するために組織された地下犯罪グループへとシフトしてきたことが背景にあります。ビジネスにとってインターネットが不可欠になった現在、こうしたさまざまな脅威からコンピュータを保護することは事業継続性の観点で強く求められています。

サポートサービス本部 Threat Monitoring Center 課長 飯田 朝洋は、「ウイルス被害に遭遇してしまった企業のシステム担当者には、迅速なシステム復旧が求められます。そのため、感染したシステムやネットワーク環境の緻密な解析に基づく不正プログラムの種類や侵入経路などを特定しないまま、駆除を最優先にしてしまうケースが多く見受けられます」と語ります。

しかしながら、これでは被害の実態をつかめません。このため、将来のセキュリティ施策に生かせず、復旧後も依然として大きなセキュリティリスクが残ってしまいます。サポートサービス本部 プレミアムサポートセンター シニアテクニカルアカウントマネージャ 戸村 泰則は、「ウイルス被害に遭った企業は復旧過程において、感染したウイルスの出所や挙動を確認する作業が不可欠です。なぜなら、異なる不正プログラムの種類や特性を見極め、最適な対策をとる必要があるためです。ミッションクリティカルなサーバ群を中心に対策を行った後、各クライアントPCに対策範囲を広げていくなど、脆弱性対策の優先順位を設定することも重要です」と語りました。

近年、企業ユーザからの報告が圧倒的に多い不正プログラムとして注目されているのが、「MS08-067」と呼ばれるWindowsの脆弱性を狙い、複数の経路から侵入する「WORM_DOWNAD(以下、ダウンアド)」です。2008年11月に確認された当初は単純にOSの脆弱性を狙うものだったのに対し、USBメモリ経由の感染手法などを新たな機能として取り入れた亜種が次々と登場。ウイルス被害件数を押し上げました。実際、2008年11月の問い合わせ件数は87件。ピークは過ぎたものの2010年1月は52件で、脆弱性を埋めるセキュリティパッチが公開されているにもかかわらず、問い合わせ件数は40%しか減少していません。この数字について飯田は、「企業ユーザによる感染が相次ぐのは、複雑化の一途をたどるシステム環境において更新プログラムの適用にかかる負荷が大きく、ミッションクリティカルなサーバに最新のパッチを適用することが難しいためです」と説明します。

企業においてパッチの適用をユーザに委ねているケースでは、全クライアントPCへの最新パッチの適用を徹底することは困難です。また、サーバへのパッチ適用後にシステム全体が正常に機能することや、業務を停止させてしまうリスクの有無を検証するテストに多大な時間を費やし、最新パッチの適用が遅れてしまうケースも存在します。サイバー犯罪者によって作成される不正プログラムの発生頻度は年々加速化し、ユーザ側の対応が十分に追いついていません。企業には、脆弱性を修正する最新のセキュリティパッチが公



開されてから適用するまでの「空白の時間」を可能な限り短縮する施策が求められています。

レガシーシステムへの対応

トレンドマイクロは、こうした課題を解決するツールとしてTrend Micro Network VirusWall Enforcer(以下、NVWE)を提供しています。アプライアンス製品として展開するNVWEは、サーバやクライアントPCにソフトウェアをインストールすることなく、脆弱性を狙う攻撃からシステムを保護することが可能です。ソリューションビジネス推進部 市場開発課 横川 典子は、「NVWEは、万一、社内システムがウイルスに感染しても被害を外部に拡散させない仕組みや、セキュリティポリシーに違反するPCなどを社内ネットワークに接続させない機能などを備えています。潜在的な脅威を可視化する「Trend Micro Threat Management Solution™」との連携により、未知の脅威[※]に対応できることも特長です」と話します。

2010年7月には、マイクロソフトのWindows 2000 ファミリのサポートが終了します。NVWEは、サポート終了に伴って脆弱性の修正に必要なセキュリティパッチが提供されなくなったレガシーシステムや、ウイルス対策ソフトの導入が困難な環境におけるセキュリティ対策としても有効です。

戸村は、「凶悪さを増すさまざまな脅威に対抗するために、組織として取り組んでいただきたいことが3つあります。1つは、オンライン環境だけでなくオフライン環境においてもセキュリティパッチのマネジメントを徹底すること。2つ目は、管理コンピュータのウイルス対策状況を把握すること。最後に、セキュリティインシデントの発生を想定した組織内の連携を確認し、柔軟なインシデントオペレーションを実行できる組織体制を構築することです」と話しました。 TP

※ すべての未知の脅威に対応するわけではありません。

USBメモリ型ウイルス検索ツール
Trend Micro Portable Security™を発表

トレンドマイクロは2010年3月31日(水)より、製造機器などの専用端末向けUSBメモリ型ウイルス検索ツール「Trend Micro Portable Security」の受注を開始します。オフラインの検索対象端末にセキュリティソフトをインストールすることなく、最新のパターンファイルでウイルスチェックできるのが特長です。

USBメモリをはじめとするリムーバブルメディアの自動実行機能を悪用する「MAL_OTORUN(以下、オートラン)」の感染被害の増加に伴い、インターネットから切り離されているオフライン端末へのウイルス感染被害が拡大しています。これにより、半導体製造装置やFA制御機器などの製造メーカーが生産する製品にウイルスが混入してしまうなどのリスクが高まってきました。製品の開発から生産、出荷までのプロセスで不

可欠な出荷前検査において、検査用端末から製品に検査プログラムを移行する際に、ウイルスに感染してしまうケースなどが考えられます。このため、検査用端末などのオフラインで利用されている端末に対して、定期的なウイルスチェックを行うことで、適切なセキュリティ対策を施し、製品の開発、製造などをより安全な環境下で行うことが求められています。

そこでトレンドマイクロは、検索対象端末にセキュリティソフトをインストール^{※1}することなく、最新のパターンファイル^{※2}を適用し、脅威に対抗するUSBメモリ型ウイルス検索ツール「Trend Micro Portable Security(以下、TMPS)」を発表しました。TMPSでは、管理プログラムをインストールしたオンラインの管理PCを経由してパターンファイルの更新や設定を行い、

USBメモリ型の検索ツールに最新のパターンファイルを適用。各検索対象端末に検索ツールを接続することでウイルス検索を行い、駆除・隔離といったウイルスの種類に合わせて最適な処理を実行します。検索ツールは、ウイルス検索結果や処理結果、検索日時、検索対象端末名などの詳細なログ情報を管理PCに保存することが可能です。

TMPSは独立したネットワークを形成する一般企業、官公庁や学校などにおいても活用できます。標準価格は、1年間のスタンダードサポートサービス料金と、ハードウェア保証を含み、検索ツール1本あたりの使用許諾料金が2万4,800円(税別)。2年目以降も継続的なソフトウェアサポートを希望する場合、1本につき1年間1万9,800円(税別)です。 TP

※1 ウイルス検索時に、一時的に検索対象端末のローカルHDDにドライバおよびファイルを作成しますが、検索終了後、検索対象端末に当該ドライバおよびファイルは残りません。
※2 管理PCにてパターンファイルをアップデートした時点での最新のパターンファイルにてウイルスチェックを行います。

Internet Threat Report

不正プログラム感染被害報告数ランキング【2009年度】

2009年1月1日～12月31日 | トレンドマイクロ調べ

順位	検出名(通称)	種別	被害件数	前年順位
1位	MAL_OTORUN(オートラン)	その他	3617件	(1位)
2位	WORM_DOWNAD(ダウンアド)	ワーム	1538件	(圏外)
3位	BKDR_AGENT(エージェント)	バックドア	784件	(2位)
4位	TSPY_KATES(カテス)	トロイの木馬型	470件	(NEW)
5位	TSPY_ONLINEG(オンラインゲーム)	トロイの木馬型	467件	(6位)
6位	JS_IFRAME(アイフレーム)	Java Script	405件	(3位)
7位	TROJ_VUNDO(ヴァンドー)	トロイの木馬型	347件	(7位)
8位	TROJ_SEEKWEL(シークウェル)	トロイの木馬型	342件	(NEW)
9位	MAL_HIFRM(ハイフレーム)	その他	326件	(4位)
10位	TROJ_FAKEAV(フェイクエイブイ)	トロイの木馬型	240件	(圏外)

2009年の不正プログラム感染被害の総報告数は4万5,310件。最も報告数が多かったのは、USBメモリを悪用する不正な設定ファイル「MAL_OTORUN(オートラン)」でした。全体的には、Webサイトを経由して不正プログラムを連鎖的にダウンロードさせる「Webからの脅威」が定番化しました。「Webからの脅威」のきっかけとして、正規Webサイトの改ざんも頻発しました。日本においても、改ざんされたWebサイトをきっかけにした感染被害が確認されました。

「TSPY_ONLINEG(オンラインゲーム)」など、情報搾取を狙ったと見られる不正プログラム3種が上位10種にランクインしていることから、攻撃者の多くが、機密情報や金銭の詐取を目的にしていることがうかがえます。また、システムや運用における基本的な対策の抜け穴から大きな被害につながりました。

今後の傾向としては、人間の心理的な隙を突くなどのソーシャルエンジニアリングがより一層巧妙化することが予想されます。脅威の動向に合わせ、基本的なシステム運用ポリシーを見直すなどの対策が必要です。 TP

※ このランキングは、2009年1月1日から12月31日までに、日本のトレンドマイクロのサポートセンターに寄せられたウイルス被害件数をもとにランク付けを行ったものです。本数値は、2010年1月5日現在の情報に基づき作成されたものです。今後、サポート調査により、件数に変更が生じる可能性があります。被害件数はウイルス発見のみの数字も含みます。
※ 個々の検出名に関しては、亜種も含んでカウントしています。