

安心を、ひとつ上のステージへ。



報告

[巧妙化する脅威から価値ある情報を守り、
競争力の源泉となる企業価値を向上させるために]

[Trend Micro Direction 2010]開催報告

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/>
- 最新セキュリティツール <http://www.trendmicro.co.jp/freetools/>
- 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/ウイルスバスター相談室モバイル* <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

トレンドマイクロ広報紙 【トレンドパーク】

TREND PARK vol.21

AUGUST

2010

NEWS&TOPICS

トレンドマイクロ、中小規模オフィス向けNAS組込み型
ウイルス対策ソリューション
「Trend Micro NAS Security™」提供開始

TOPICS

セキュリティ無料ツール!

安心を、ひとつ上のステージへ。



トレンドマイクロ株式会社

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	〒460-0002 愛知県名古屋市中区丸の内3-22-24 名古屋桜通ビル7F (8月30日より上記住所にて営業)	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 サンエフビル 7F	TEL:092-471-0562	FAX:092-471-0563

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事の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.21

AUGUST

2010

TOPICS

セキュリティ無料ツール!

最新のセキュリティ技術を体験できる、トレンドマイクロの各種無料ツールを紹介する Web ページを公開。エンドポイント向け無償ウイルス検索ツール「Trend Micro HouseCall (ハウスコール)」や、Apple 社製 iPhone、iPod touch に加え、iPad でも利用可能なセキュアブラウザ「Smart Surfing for iPhone and iPod touch (スマートサーフィン フォー アイフォーン アンド アイポッドタッチ)」を提供しています。

また、47 の質問に回答して自社のセキュリティ対策の状況把握・問題発見を行う企業診断システム「Trend Micro Security Pro (セキュリティプロ)」も本サイトから受診できます。

ぜひ、トレンドマイクロの最新技術を試してください。

検索ツール ~何かおかしい?と思ったらまずこちら~

Trend Micro HouseCall
Trend Micro HouseCall (以下HouseCall) は、製品版ではまだ提供されていない最新技術が実装された、クライアントPC向けのプロトタイプ製品です。お客様は必要と感じた際にHouseCallを利用いただくことで、最新の技術を使用し、最新のウイルス、スパイウェアやその他の「Webからの脅威」を検出することができます。
詳細はこちら

予防ツール ~最新の脅威から事前に防御~

Smart Surfing for the iPhone and iPod
3G iPhone、iPodのための安全なブラウザ
詳細はこちら

Web Protection Add-On
危険なサイトへのアクセスをブロックするブラウザプラグイン
詳細はこちら

Browser Guard 2010
ブラウザの脆弱性をねらった攻撃をブロック
詳細はこちら

感染復旧ツール ~感染したウイルスなどを検出・削除~

HijackThis
レジストリ、ファイルの設定を検索・レポート
詳細はこちら

RUBotted
「ボット」の挙動を監視
詳細はこちら

CWShredder
スパイウェア「CoolWebSearch」を検出・削除
詳細はこちら

RootkitBuster
ルートキットを検出・削除
詳細はこちら

<http://www.trendmicro.co.jp/freetools/>

※1 本サイトの無料ツールは、最新技術をいち早くお試しいただくためのベータ版であり、トレンドマイクロのサポート対象外です。
※2 Smart Surfing for iPhone and iPod touch は、App Store からダウンロードできます。

CONTENTS

3 TOPICS
セキュリティ無料ツール!

4 Direction 2010
[巧妙化する脅威から価値ある情報を守り、競争力の源泉となる企業価値を向上させるために]
報告 「Trend Micro Direction 2010」開催報告

15 News & Topics
トレンドマイクロ、中小規模オフィス向けNAS組込み型ウイルス対策ソリューション「Trend Micro NAS Security™」提供開始
Internet Threat Report
不正プログラム感染被害報告数ランキング

「Trend Micro Direction 2010」開催報告

DATA 開催日：2010年7月7日(水)
場 所：ANAインターコンチネンタルホテル東京



巧妙化する脅威から価値ある情報を守り、競争力の源泉となる企業価値を向上させるために

トレンドマイクロは2010年7月7日(水)、都内ホテルにて「Trend Micro Direction 2010」を開催しました。今回は、広く注目を集めているクラウドをはじめ、企業経営におけるITマネジメント・ガバナンス、企業内外の脅威への対抗策、セキュリティソリューションの評価法など、様々な観点からこれからの時代にITを活用して企業が強く生き残るための実践的な指針となるセッションを展開しました。800名を超える参加者は、基調講演と各セッションを熱心に聴講していました。

Keynotes 基調講演

クラウド時代に求められるセキュリティ

～ブレイン、ハイブリッドクラウドとセキュリティ～

トレンドマイクロ株式会社
代表取締役社長 兼 CEO
エバ・チェン

境界線のない時代へ

基調講演に登壇したエバは、さまざまな環境が混在するハイブリッドなクラウド世界に移行するに伴い、顕在化してきた課題を解説。今後、求められるセキュリティ対策について語った。

講演の冒頭でエバは、「われわれは現在、「プライベートクラウド+パブリッククラウド」、「クラウド+クライアント」、「仮想環境+物理環境」、「オンデマンドアプリケーション+オンプレミスアプリケーション」が共存するハイブリッドクラウドの中で生きている」と説明。人間の右脳と左脳の働きをコンピュータアーキテクチャに見立て、「脳は右脳と左脳の協調動作によって機能する。コンピュータ環境においても、クラウドアーキテクチャと従来のアーキテクチャが協調することが必要だ」と語った。

また、ハイブリッドクラウドでは、ハードウェアやソフトウェアのリソースが共有され、データもあらゆる場所に存在し、境界線のある世界から境界線のない世界へと移行するため、セキュリティというルールが不可欠になる。

インサイド・アウトのアプローチで

クラウド環境では、1台の物理サーバ上で複数の仮想サーバが稼働する。ある仮想サーバがウイルスに感染すれば、ほかのサーバに感染が拡大してしまうリスクが発生する。また、データがあらゆる場所に存在するようになることから、データの所有権や機密性といったデータ保護の観点で対処が求められる。

エバは、「ハイブリッドクラウドのセキュリティでは、従来のセキュリティへの考えを刷新し、新たなアプローチを採用することが重要だ」と指摘。これまでの境界線のある環境では、ファイアーウォールなどによって外部からの脅威を防ぐ「アウトサイド・イン」のアプローチに重点を置いてきたが、今後は外部の共有ストレージに格納するデータを保護するなど「インサイド・アウト」のアプローチを適用することも必要となる。

トレンドマイクロはこのコンセプトを踏襲するソリューションとして、物理、仮想、クラウドコンピューティング環境のサーバに対してセキュリティを実装する「Trend Micro Deep Security™」を提供している。エバは、「今後もコンピュータアーキテクチャ全体を見渡し、多様なコンピュータ環境に最適なセキュリティを提供していく」と講演を締めくくった。

Keynotes 基調講演

セキュリティと企業ブランド

～ブランド価値向上意識が情報セキュリティを守る～

株式会社 堀場製作所
業務改革推進センター 情報技術担当 センター長
新井 修氏

オープン&フェアのIT戦略

講演の冒頭で新井氏は、人生で最も大事な時期を費やす会社(仕事)に「誇り」を持ち、おもしろおかしく仕事をしようという社は「おもしろおかしく(JOY and FUN)」と「オープン&フェア」の精神に基づいて推進する同社のIT戦略を紹介。セキュリティ体制を盤石にし、HORIBAブランドを守るための4つのセキュリティ戦略について解説した。

創業以来、研究開発に対する経営資源の集中、海外進出、デファクトスタンダード化、M&Aによる技術の獲得など、精力的なチャレンジを通じてビジネスを拡大してきた同社は、常に最先端のITを経営に組み入れてきた企業でもある。その中で、同社のシステムの管理・運用を行う業務改革推進センターは、情報を従業員に開示し、チャレンジを促す「オープン&フェア」の精神に基づいたIT戦略を推進。いつでも、どこでも仕事のできる環境を目指し、グループが一体となって強固なセキュリティの構築に注力してきた。具体的には、セキュリティ啓蒙などの「人的セキュリティ」、組織管理などの「管理的セキュリティ」、ファイアーウォールや認証などの「システムセキュリティ」、および建物・設備などの「物理的セキュリティ」の4つの側面からセキュリティを強化している。

4つのセキュリティアプローチを展開

管理的セキュリティやシステムセキュリティは、従業員が社外に持ち出すことを許容しているモバイルPCに対して徹底している。たとえば、モバイルPCの盗難や紛失に備え、ハードディスクの暗号化や、USBキーおよび指紋認証によるログオンを強制。不正アクセス対策として固定IP/モバイルMACアドレス認証を採用している。物理的セキュリティでは、ERPおよびグループ共有サーバの外部データセンターへの移設などでシステム障害に備える体制を整えている。

新井氏は、「人的セキュリティでは、WinnyやSkypeの危険性やUSBメモリなどの使用にあたってウイルス感染リスクを内包していることなどについての教育や啓蒙が中心だ。セキュリティポリシー違反には、イエローカードやレッドカードを提示することで対処し、コンプライアンスを強化している」と語った。

また、人的セキュリティにおいて、50%を超えた外国人を含むグループ従業員が社外をはじめとする企業文化を正しく理解するために「ブランドブック」を共有したり、人材教育に力を入れている。

「長年にわたって培ってきたHORIBAブランドを守る意識とトレンドマイクロのセキュリティソリューションは、われわれが情報セキュリティを維持・強化する両輪になっている」と新井氏は講演を締めくくった。

株式会社 堀場製作所
業務改革推進センター 情報技術担当 センター長
新井 修氏



トレンドマイクロ株式会社
代表取締役社長 兼 CEO
エバ・チェン

Room A

Session セッション

クラウドで大きく変わるICT

～NTTコミュニケーションズが実現するセキュアでユビキタスなクラウド環境～

NTTコミュニケーションズ株式会社
ビジネスネットワークサービス事業部 担当部長
中山 幹公氏

「BizCITY」がセキュアなクラウドを支える

本セッションでは、NTTコミュニケーションズが提供するセキュアなクラウドコンピューティング基盤「BizCITY」を紹介。高い競争力を獲得するために企業が実践したいクラウド戦略について解説した。

クラウド市場は急速に拡大している。多くの国内企業は、すぐに利用可能、使用リソースの増減が容易、環境構築が簡便、保守・運用が不要など、クラウドを活用することで得られるメリットを認めつつも、ネットワークやセキュリティに関連する不安を抱えているのが現状だ。その中で、クラウドを活用するにあたっては、社内システムとの連携やクラウドの特性をフル活用するためのユビキタスな接続環境の構築を担うネットワークが生命線になる。

中山氏は、「米国にサーバを置くクラウドサービスを日本で利用し、米国の法制度に基づいて運用されるリスクや、ネットワークの遅延およびカスタマーサポートの不備などのリスクに晒さ

れたケースは少なからず存在する。われわれは、さまざまなITアウトソーシング事業でネットワークインフラを提供してきたノウハウを生かし、高い品質と安全性を誇るクラウドコンピューティング基盤「BizCITY」を展開。この基盤は、モバイルやVPNを含めた多様かつセキュアなネットワークを使って、必要なときに必要なだけICTを利用できることが特長」と語る。

コアコンピタンスに注力できる体制を

「BizCITY」は、長年にわたって培ったノウハウを集積した独自のネットワーク技術とバンドルしたさまざまなサービスをワンストップで提供している。たとえば、企業VPNに直結できるセキュアなクラウド型ファイルサーバサービスとして「Bizストレージ」を展開。同サービスは、拠点ごとに運用するファイルサーバを統合し、リスクマネジメントを強化したり、回線利用料やシステム管理者の運用負荷を含めたコストを削減したい企業に有効だ。ユーザー端末からBizストレージヘッダー

タを読み書きする際にウイルスを検索する機能は、トレンドマイクロの技術に支えられている。

中山氏は、「競争を勝ち抜くため、企業にはハードウェアを調達したり、システムを構築したりするコモディティ化した作業をクラウドにアウトソースし、顧客に付加価値を提供するコアコンピタンスにリソースを集中させることが求められる」と講演を締めくくった。



Session セッション

情報インフラにおける安全と軽快の両立

～クライアントセキュリティを刷新した大手食品会社の導入事例～

株式会社日立フーズ&ロジスティクスシステムズ
システム基盤事業部 副事業部長
高山 哲郎氏

トレンドマイクロ株式会社
エンタープライズマーケティング部
プロダクトマネージャー
染谷 征良

必要最小限のパターンファイルを適用

本セッションでは、先ず染谷氏が従来の対策手法であるパターンファイルに依存しない最新のセキュリティ技術を紹介。

不正プログラムが急速に増加し、感染経路も複雑化する中で、クライアントPC上で行うパターンマッチング処理により、脅威に対抗する従来の方法には限界が見えてきた。というのも、各クライアントPCに最新のセキュリティを実装

するためには、不正プログラムの特徴を格納した大量のパターンファイルをダウンロードする必要があるためだ。また、大量のパターンファイルをダウンロードすることにより、ネットワークやシステムリソースへの負荷の増大は否めない。

こうした企業の課題を解決するソリューションの1つが、スマートスキャン機能を搭載したウイルスバスター™ コーポレートエディション10.0だ。染谷氏は、「スマートスキャンは、疑わしいファイルを検索した場合、必要に応じてクラウド上のパターンファイルを参照する機能。これにより、パターンファイルのサイズや更新時のトラフィックを抑えながら、常に最新のセキュリティを実装できる」と語った。

システムおよび人的リソースを大幅に低減

続いて登壇した高山氏は、自身がリードした大手食品会社がウイルスバスター コーポレートエディション 10.0を社内セキュリティの標準として導入したポイントを解説。高山氏は、「社内の一部PCでは、パターンファイルをアップデートする際の高負荷が原因で更新に失敗するケースが散見された。人やシステムにかかるセキュリティソフトの運用負荷を軽減することが最大の目的だった」と語った。

セキュリティソフトの選定では、従来ソフトとウイルスバスター コーポレートエディション 10.0の

パフォーマンスを比較する複数のテストを実施。たとえば、低スペックPCと高スペックPCのそれぞれにかかるアップデート時のメモリ使用量とCPU使用率を計測し、ウイルスバスター コーポレートエディション 10.0が消費するリソースは従来ソフトの約半分に抑えられることを確認。また、フルスキャンに要する時間も従来ソフトに比べ、圧倒的に短いことが明らかになった。

高山氏は、「約5,000台のPCに対して常に最新のセキュリティを実装できたことはもちろん、セキュリティ運用におけるメモリ使用量やCPU使用率、および人的リソースを抑えられるようになったことは最大の成果」と講演を締めくくった。



Session セッション

計画的なセキュリティパッチ運用とDeep Securityを用いた脆弱性の可視化

～企業が抱えるセキュリティパッチマネジメントの課題～

大和ライフネクスト株式会社
システムセンター センター長
大西 雄三氏

トレンドマイクロ株式会社
セキュリティエキスパート本部
コンサルティングSE部
ソリューションSE3課 担当課長代理
三枝 大高

セキュリティパッチを迅速に適用する必要性

本セッションでは、システムの脆弱性が企業に与えるリスクや、パッチマネジメントにおける課題について三枝氏が解説。大西氏は、トレンドマイクロの「Trend Micro Deep Security™ (以下、Deep Security)」を活用した自社の事例を紹介した。

三枝氏は、「公開された脆弱性情報に基づいてセキュリティパッチを即時に適用するのが理想的なパッチマネジメント。とはいえ、ミッションクリティカルなサーバへのパッチ適用後に、システム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がある」と語った。

OSやアプリケーションなどの脆弱性は、攻撃者がリモートで任意のコードを実行して機密情報を散布したり、プログラムやデータなどのファイルを変更・破壊したりすることに悪用されるケースが目立つ。このため企業には、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タイムラグを短縮する施策が求められる。

仮想パッチ機能を提供するDeep Security

大西氏は、2010年4月にサービスインした外部向けWebサイトのリリースと同時に、トレンドマイクロのDeep Securityを稼働させ、セキュリティパッチ運用における課題を解決した事例を紹介した。大西氏は、「最大の課題は、パッチ適用の動作検証を含め、脆弱性情報の公開から正式なパッチ適用までに1日から3日を要していたこと。脆弱性が発見されればシステムやサービスを停止しなければいけないケースもあり、ユーザーが求めるサービス稼働率を維持することが難しくなっていた」と語った。

また、脆弱性への対応が属人化し、発生した脅威や対応履歴を管理できないこと、プライオリティの高いパッチ適用が他システムの計画的な運用を妨げていたことも悩みだった。これらの課題を解決するため、同社はDeep Securityを導入。ネットワークを流れるパケットを精査し、サーバの脆弱性を狙う攻撃をブロックする“仮想パッチ”として機能させた。結果、正式なパッチを適用する間も、脅威に対抗できるようになったので安心感は大い。

また、脅威の発生やパッチの適用状況などを履歴として一元管理できるため、コンプライアンスの強化にも役立っている。計画に沿ってパッチを適用できるため、業務へのさまざまな影響を制御することも大きな成果だ。大西氏は、「外部向けWebサイトの運用基盤として導入を検討中の仮想サーバでもDeep Security適用を計画している」と講演を締めくくった。



Room B

Panel discussion パネルディスカッション

クラウドで変化する情報セキュリティ

～エンタープライズリスクマネジメント～

「セキュリティ普及促進委員会」協力パネルディスカッション

【モデレータ】
トレンドマイクロ株式会社
斧江 章一
【パネリスト】
経済産業省
情報セキュリティ政策室 課長補佐
佐藤 明男氏

【パネリスト】
独立行政法人情報処理推進機構
セキュリティセンター
石井 茂氏
【パネリスト】
株式会社シマンテック
村上 智氏

【パネリスト】
マカフィー株式会社
本橋 裕次氏
【パネリスト】
トレンドマイクロ株式会社
小屋 晋吾

クラウドセキュリティ監査を利用者視点で

2010年2月、内閣官房が定める「情報セキュリティ月間」を機に、官民の壁、企業の壁を超えて5つの組織が「セキュリティ普及促進委員会」を設立。同委員会の協力によるパネルディスカッションを展開し、クラウド時代における情報セキュリティ政策や情報セキュリティのあり方について討議した。

最も活発に意見が交わされたのは、クラウドセキュリティ監査について。ISO/IEC 27001

Annex/27002でもクラウドセキュリティについての監査が十分に達成されないとする佐藤氏が「項目ごとに利用者視点で整理し、既存の監査基準と現実との差分を監査する仕組みが必要。クラウドセキュリティ管理基準のドラフト版を早期に策定したい」と語った。

これに対して小屋は、「利用者視点は良いが、監査が煩雑になるとコストがかかる。小さなソフトウェアベンダーやリスクを許容できる環境では厳しすぎない制度を期待する」と意見した。

早期にガイドラインを整備

石井氏は、クラウドコンピューティングのセキュリティ保証のためのベストプラクティス普及にあたるCSA (Cloud Security Alliance) の最新スタディについて紹介した。CSAには全世界で約50社が加入しており、提携団体は約10団体。IPAもその一員だ。ここでは、CSAが2009年

12月に発表したクラウドコンピューティングのセキュリティに関するベストプラクティスであるガイドラインV2.1について語った。

村上氏は、リスクマネジメントと絡めたクラウド利用を提唱。的確なビジネスリスク評価を実施してリスクを見える化することが必要になるとし、「クラウドに移行しても良いデータとだめなデータを仕分けすることが必要になる。クラウドになるとユーザの利用形態は多種多様になるため、ベンダーとして新しいニーズに応えられるソリューションを提供しなければならない」と語った。

本橋氏は、システムを守るのではなく、情報資産を守ることへと意識変革することが必要と指摘した上で、クラウド側とエンドユーザ側で対策を複合的に組み合わせることがクラウド有効活用のカギになるとし、「新しくクラウド端末として注目を浴びている、iPhoneやiPadなどの端末へのセキュリティ対策も重要。このような端末向けのソリューションも必要になってくるのではないか」と語った。



解説した。複数台のサーバ上で複数の仮想マシンを動かす場合、オフピーク時に仮想マシンを他のサーバにオンラインのまま移動させ、空いたサーバを停止することができる。これにより電力を削減できるだけでなく、サービスを停止することなくサーバのメンテナンスを実施することも可能になる。

また、VMware vSphere 環境上に展開するシステムは、容易に切り出して社外のクラウド環境に移行できるようになる。このため、VMware vSphere のインストールベースが、事業者にとってビジネスチャンスになるという。そのクラウドインフラとサービスのモデルは、IaaS (インフラストラクチャ・アズ・ア・サービス)、PaaS (プラットフォーム・

アズ・ア・サービス)、SaaS (ソフトウェア・アズ・ア・サービス) を包括した幅広い概念となる。

森田氏は、「VMware vSphere によってポリシーベースで管理されたプライベートクラウドの構築が可能になり、VMware vCloud によってサービスプロバイダの提供するパブリッククラウドとシームレスに連携できます。その結果既存のITインフラストラクチャを変更することなく、柔軟なITサービスを実現できるようになります」と語った。

仮想化とセキュリティ

森田氏は、VMware のセキュリティ機能についても触れた。vSphere のセキュリティは、VMkernel

によってロードされるモジュール、ドライバ、アプリケーションのデジタル証明での整合性や信憑性の保証、クライアントからの通信のSSLによる保護などがあり、仮想環境での安全な運用を実現する。さらに仮想マシン間のCPUやメモリへのアクセス制限をはじめ、ネットワークも含めた「隔離」により、複数の仮想マシンが安全に実行できる。

また、仮想化基盤のファイアウォールのVMware vShield Zones を利用すれば、ゾーンベースでポリシー設定などが可能。森田氏はさらに、「VMsafe が備えるAPIを利用すれば、セキュリティベンダが仮想環境を保護する優れたセキュリティソフトを提供できるようになる。トレンドマイクロとの提携もその一環」と語った。



Session セッション

クラウド時代のセキュリティガバナンス

工学院大学
情報学部 教授
大木 栄二郎氏

リスク移転に意味がなくなる

本セッションでは、情報社会について、農業革命で生まれた農業社会、産業革命による工業社会の次に、情報革命によって誕生した社会という切り口から、新時代のリスク対応とクラウドコンピューティングのセキュリティについて語られた。

講演の冒頭で大木氏は、『原典 情報社会』(増田米二著)をとりあげ、技術が社会を変革させてきた流れについて解説。有限の資源を配分し、リスクを分担してきた工業社会においてはリ



スク移転が重要であったのに対し、情報社会は無限の情報共有することが大切になるためアトムリスクとビットリスク*の構成割合が大きく変化することとなり、リスクを共有する必要が出てくると指摘した。

「情報社会では、無限にコピーできる情報を扱うため、リスクを移転しようとする発想に意味がなくなります。替わって、リスクコミュニケーションの重要性が増大することになります」(大木氏)

この情報社会が本格化する中で、企業が取り組むべきリスクは、技術の的確なマネジメントにかかわるITリスクと、情報活用にかかわる情報リスクに分けて考えることが必要になる。大木氏は、技術が人間労働にとってかわる段階を経て、人間ではできないことを可能にする段階、そしてクラウドや仮想化に代表される根本的に変革する段階を経るとし、クラウド時代のリスクコミュニケーションの重要性について、次のように語った。

クラウド時代のリスクコミュニケーション

「情報セキュリティリスクの定量化は困難だが、リスク情報を正確に把握し、リスク評価の枠組みを共有することが不可欠。ガバナンスや内部

監査による対内コミュニケーションと共に、外部監査など対外コミュニケーションも活用し、リスクコミュニケーションの効果を高める必要が出てくる」(大木氏)

クラウドの利用には、効率性の向上とITコストの削減という大きなメリットがある反面、セキュリティにかかわる課題が数多く指摘されている。グローバルな機関で検討されているこれらの課題は、1. 所有から利用への変化がもたらす課題、2. クラウド技術がもたらす課題、3. クラウドの本質的な特徴がもたらす課題、の3つに大別できる。

大木氏は、「課題を解決するためには、ベンダーとユーザだけでなく、信頼できる第三者がリスクコミュニケーションの間に立って、ミスコミュニケーションを防ぐ仕組みが必要。それによってクラウドが発展し、企業の情報セキュリティ意識も高まるはず」と講演を締めくくった。

*「アトムリスク」→物理的、局所的、隔離対応、被害激烈
経験豊富
「ビットリスク」→グローバル、多面的対応、被害認識
遅延、未経験

Session セッション

VMware vSphereで実現するITインフラの進化と、仮想化におけるセキュリティ対策

VEIウェア株式会社
テクノロジーアライアンス部長
森田 徹治氏

VMwareの目指すクラウドとは

システムの効率性追求と共に、仮想化技術がクローズアップされ、いまではミッションクリティカ

ルな分野でもごく当たり前に仮想化技術が採用されるようになっていく。サーバ数千台を仮想化するプロジェクトが実行され、仮想化管理ソフトウェア市場と仮想サーバ市場のどちらも右肩上がりの成長を見せている。

本セッションでは、VMware による仮想化の価値について語られた。森田氏はまず、仮想化を省電力化とメンテナンス性の向上という観点から

Room C

Session セッション

企業の実例に見る最新の脅威

～セキュリティの抜け穴を狙う不正プログラム～

トレンドマイクロ株式会社

セキュリティエキスパート本部 セキュリティエンハンスメントグループ 課長 CISSP

平原 伸昭氏

驚異的なスピードで発生し続ける脅威の連鎖

本セッションで平原は、不正プログラムによる脅威について、最新の企業の実例をデモを交えて報告した。

平原は、最新の不正プログラムによる攻撃の特徴は、その感染経路と発生スピードだという。「AV-test.org 提供のデータをもとに算出した脅威の発生速度において、昨年は、2.5 秒に1つだったのに対し、今年は1.5 秒に1つ新しい不正プログラムが登場している」とし、これら不正プログラムの主な侵入経路は、Web へのアクセスであると語った。

また、国内企業における「不正プログラム脅威トップ4」として、偽セキュリティソフト、USB ウィルス、ダウンロードファミリ、ランサムウェア攻撃を挙げた。平原は、「特に、偽セキュリティソフトは、偽のセキュリティソフトをインストールさせて、個人情報盗むソフトウェアの総称で、すでに第9世代に達している。また、正規の

Web サイトを改ざんし、不正プログラムに感染させる攻撃の総称であるランサム攻撃は、驚異的に変化し、拡大し続けている」と、従来の対策であるパターンファイルによる検出だけでは、これら爆発的に増え続ける最新の脅威に対抗するのは限界と指摘した。

レピュテーションなど、異なるテクノロジーを併用した新たな対策が必要

最新の脅威に対抗するための対策として、平原はレピュテーション技術の採用を提案。「Web レピュテーションとは、クラウドコンピューティングを利用した Web サイトの評価技術で、信頼性やリンク状況から Web サイトを分析し、疑わしいサイトへのアクセスをブロックする。これにより、不正ファイルのダウンロードや不正な情報送信を遮断し、高いセキュリティを提供する」という。

また、従来の対策に頼るのではなく、異なるテクノロジーを用いた複数のアプローチの併用に

よって、攻撃の連鎖を断ち切ることが重要だとしている。実際にパターンマッチングとレピュテーションを合わせた複合対策によって、従来のパターンファイルのみの対策に比べて、ブロックできる脅威が約4倍向上したケースもあるという。

さらに、刻一刻と変化する脅威と自社のセキュリティ対策を照らし合わせ、ギャップの有無を継続して確認するPDCA サイクルも必要とし、「そのためには、ネットワーク上の挙動を監視して、未確認の不正プログラムの活動を可視化するための新しいテクノロジーを組み合わせる必要がある」と説明した。



が主流となっていると説明。また、「攻撃は、巧妙かつ増加の一途をたどり、セキュリティソフトのテスト手法は、従来のウィルス検出率のみでは通用しなくなった」と語った。

ゲネスからの「テスト実施の難易度」についての質問に対して、AV-Comparatives.org のシュテルツハマー氏は、「製品ごとに複雑なテスト環境に対応しなければならないため、我々テスト機関は、多くの人手とハードウェアに加え、仮想環境までも想定する必要がある。一方、ベンダーの不正プログラム対策製品は、Webのブロック機能、ヒューリスティック検出、シグネチャによる検出、挙動監視などさまざまな機能を組み

合わせている。したがって、これら機能を包括した、より現実に即したテストは今後、ますます重要となる」と語った。

現状を踏まえたテスト手法のあるべき姿

また、AV-Test.org のモルゲンスタン氏は今後の方向性について、「製品の検証に当たっては、その全体像を把握することが重要。我々は、すべてのステップごとにシステムをチェックして、何が検出され、検出されなかったのかを調査する。これが、より現実に即した方法だ」と語った。しかし、テスト機関のすべてが、同様の認識や技術力を備えているわけではなく、それが、テ

ト結果の信頼性の面での課題でもあるという。

一方、NSS Labs のモイ氏は、「我々は、製品分析ラボであると自負しており、そのビジネスモデルはガートナーやフォレスター、IDC に似ている」と語った。同社はテストを実施するに当たりベンダーから報酬を受け取っていない。同社では、1. 脅威の侵入をどれだけブロックできるかの検証、2. 不正プログラムが実行された場合にソフトウェアの全機能で守れる範囲の検証、の2つを8時間おきを実施していると解説。同社の考え方では、セキュリティを強化するためには、恣意的でない正直なテストが必要であり、防御が、どこまで有効であるかを正確に把握することだと語った。



Panel discussion パネルディスカッション

皆様の疑問にお答えする来場者参加型パネルディスカッション

～従来の検出率テストの有効性やセキュリティ製品の選定ポイントとは～

【モデレータ】
Trend Micro Chief Technology Officer (CTO)
レイモンド・ゲネス

【パネリスト】
AV-Comparatives.org Vice Chairman
ペーター・シュテルツハマー氏

【パネリスト】
AV-Test.org Chief Technology Officer
マイク・モルゲンスタン氏

【パネリスト】
NSS Labs President
リック・モイ氏

企業は何をもって自社のセキュリティレベルを判断すべきか

本セッションでは、参加者からの投票で選ばれたテーマを取り上げ、討議を展開。最初のテーマには、「企業がとるべきセキュリティ対策のレベル」が選ばれた。

モルゲンスタン氏は、「セキュリティに万能薬はない」とした上で、「セキュリティはプロセスであり、継続して更新しなければならない。また、ソフトウェア以外にもユーザのトレーニングなど投資が必要な分野も多い。適切な投資のためにも、明確なセキュリティの保護対象と効果測定基準が必要となる」と述べた。

シュテルツハマー氏は、「ベンダーの選択においては、従来のような検出率だけでなく、ユーザビリティや性能、管理性、またサポートも重要。企業が最も適している製品を判断するためにテストは不可欠。だから我々が存在する」との意見を述べた。

これを受け、モイ氏は、「我々がラボで行うテストは、いい指標になっていると思う。しかし、それが個々の企業の特有の条件に適しているかどうかは、また別の問題となる。大規模なセキュリティ製品の導入予定があるのであれば、その投資の一部をテストにあて、自社の固有条件にあった製品を模索することも重要だ」と語った。

不正プログラムの侵入口と対策のポイント

2つ目のテーマとして、「攻撃の侵入口」について討議が行われた。モイ氏は、「脆弱性は、大きな問題だ」とした上で、「昨年、Google が中国からのサイバー攻撃の被害に遭った。このInternet Explorer の脆弱性を狙ったゼロデイ攻撃で最大の警鐘となったのは、高度なセキュリティ対策を施している組織でも被害に遭うことがあるという点だ。今年に入り、すでに3,000～4,000の脆弱性が発生している」と語った。

一方、シュテルツハマー氏は、仮想化の普及にともなう新たな課題として「ハードウェアとVMware の間で問題が生じた場合、大きな脆弱性に発展する可能性がある」と指摘。モルゲンスタン氏もこれに同意し、「仮想化がもたらす新たな脆弱性として、懸念している」と語った。

また、ゲネスの「攻撃者にとって、魅力的なターゲットとは何か？」との問いに対して、モイ氏は、「彼らは常に重要な情報が集積される場所を目指すものだ。その意味でいえば、データセンターは魅力的に映るだろう。一方、データセンターの仮想化インフラは導入が進み始めてまだ3年程度と歴史が浅く、十分なセキュリティのノウハウが蓄積されていない」と指摘した。



Panel discussion パネルディスカッション

セキュリティ製品に求められる真の実力とは?

～セキュリティ製品のテスト手法はどうあるべきか～

【モデレータ】
Trend Micro Chief Technology Officer (CTO)
レイモンド・ゲネス

【パネリスト】
AV-Comparatives.org Vice Chairman
ペーター・シュテルツハマー氏

【パネリスト】
AV-Test.org Chief Technology Officer
マイク・モルゲンスタン氏

【パネリスト】
NSS Labs President
リック・モイ氏

効力を失う従来のテスト手法

本セッションでは、トレンドマイクロのCTOであるレイモンド・ゲネスをモデレータとして、世界的な主要第三者テスト機関の専門家によるパネルディスカッションが行われた。

冒頭、ゲネスは脅威の状況が劇的に変化し、いまや不正プログラムは、「アンチ・ディテクションベンダー」あるいは「ツールキット・ベンダー」と呼ばれる組織により、組織的に生産されること

Exhibition 展示コーナー

トレンドマイクロと技術アライアンスを組む、業界をリードする各社が最新のソリューションを展示

「Trend Micro Direction 2010」では、トレンドマイクロと技術的なアライアンスを組む企業による展示が設けられました。各社が提供する先進的な技術とトレンドマイクロとの連携によるソリューションが紹介され、数多くの来場者でにぎわいました。

クラウドゾーン

日本ヒューレット・パッカード株式会社

- Q1. 大きく2つあり、セキュア仮想化ソリューションと、クラウド実現のためのソリューションです。
- Q2. クラウド実現のためのソリューションとして、その方向性とステップの具体化の手段として「クラウドディスクカバレッジワークショップ」と、セキュアな仮想インフラ実現手段としてDeep Security導入サービスを柱にしています。
- Q3. トレンドマイクロのセキュリティ技術とHPのノウハウを連携し、セキュアなインフラ環境の提供を行っています。

株式会社日立製作所

- Q1. 統合サービスプラットフォーム「BladeSymphony BS2000」、BladeSymphony BS320」、及び日立サーバ仮想化機構「Virtage」です。
- Q2. 出展しているVirtageは、BS2000、及びBS320でご使用可能な日立独自の高性能、高信頼のサーバ仮想化機構です。
- Q3. 日立はVirtageによる仮想化環境で、トレンドマイクロの2つのVirtual Appliance製品をサポートしており、これらの製品の動作環境を構築するサービスも提供しています。また、「ウイルスバスター™ コーポレートエディション」といったスタンダードなセキュリティ製品についてもトレンドマイクロと共同で動作検証を行っており、お客様に安心してお使いいただけるようサポート体制を整えています。

伊藤忠テクノソリューションズ株式会社

- Q1. 仮想化統合インフラソリューション「Vblock」「Trend Micro Deep Security™」「Splunk」です。
- Q2. 仮想化統合インフラソリューション、統合セキュリティソリューション、統合ログ管理ソリューションです。
- Q3. 次世代IT基盤のセキュリティ対策ソリューションに、仮想サーバと物理サーバの双方を守る「Trend Micro Deep Security」を活用しています。

ネットワークゾーン

株式会社大塚商会

- Q1. 「インターネットおまかせバック」と「マネージドネットワークサービス」です。
- Q2. 小規模から大企業まで、規模やお客様の要望に合わせたインターネット環境の構築を、オールインワンで提供。社内のIT機器のマネージメントやワンストップサービスを提供します。
- Q3. 長年のパートナーシップにより、トレンドマイクロのセキュリティサービスのノウハウを提供しています。また、イベントの共催などで、セキュリティの啓蒙や製品PR活動を行っています。

ヤマハ株式会社

- Q1. 「QAC/TM」と「Trend Micro Web Security for Yamaha Router」です。
- Q2. ガンブラー攻撃などによる危険な不正サイトや改ざんサイトへアクセスしないよう未然にWebサイトの危険性をチェック、不審なものがWebから侵入しないように防御を固めます。
- Q3. ヤマハルーター「SRT100」との連携機能により、セキュリティ対策が簡単にそして安価に導入、運用が可能です。

日本電気株式会社

- Q1. 未知のウイルスにも対応するウイルス感染の監視/隔離ソリューションです。
- Q2. 未知の脅威をはじめとする不正プログラムの早期発見と隔離による早急な対処でウイルスの感染拡大、被害を最小限にとどめ、ネットワークの継続的な安全性を確保します。
- Q3. NECの「Plug & Secure テクノロジー」と「Trend Micro Threat Management Solution™」の連携をはじめとしたソリューションの共同開発や、お客様のニーズに合ったソリューション提案など、技術的な部分から提案まで幅広い範囲で強力なパートナーシップを築いています。



インタビュー項目

- Q1. 今回出展されているのは、どのような製品/ソリューションですか？
- Q2. 出展されている製品/ソリューションのアピールポイントについて教えてください。
- Q3. トレンドマイクロとは、どのような協力体制をとっていますか？

エンドポイントゾーン

イーディーコントライブ株式会社

- Q1. 高度なセキュリティ機能を備えた次世代型セキュリティUSBメモリ「TRAVENTYシリーズ」です。
- Q2. インストールレス、制限付きユーザでも可能なSDシリーズの最新版。被害が拡大しているUSBウイルス感染も3つのステップで強固に防御します。運用をサポートするマネージメントツールは、ポリシー、使用許可PC、資産管理など多彩な設定機能を持っています。
- Q3. 「Trend Micro USB Security™ for Biz」を搭載。不正プログラムを検出すると警告表示し、感染ファイルを隔離します。

NRIセキュアテクノロジーズ株式会社

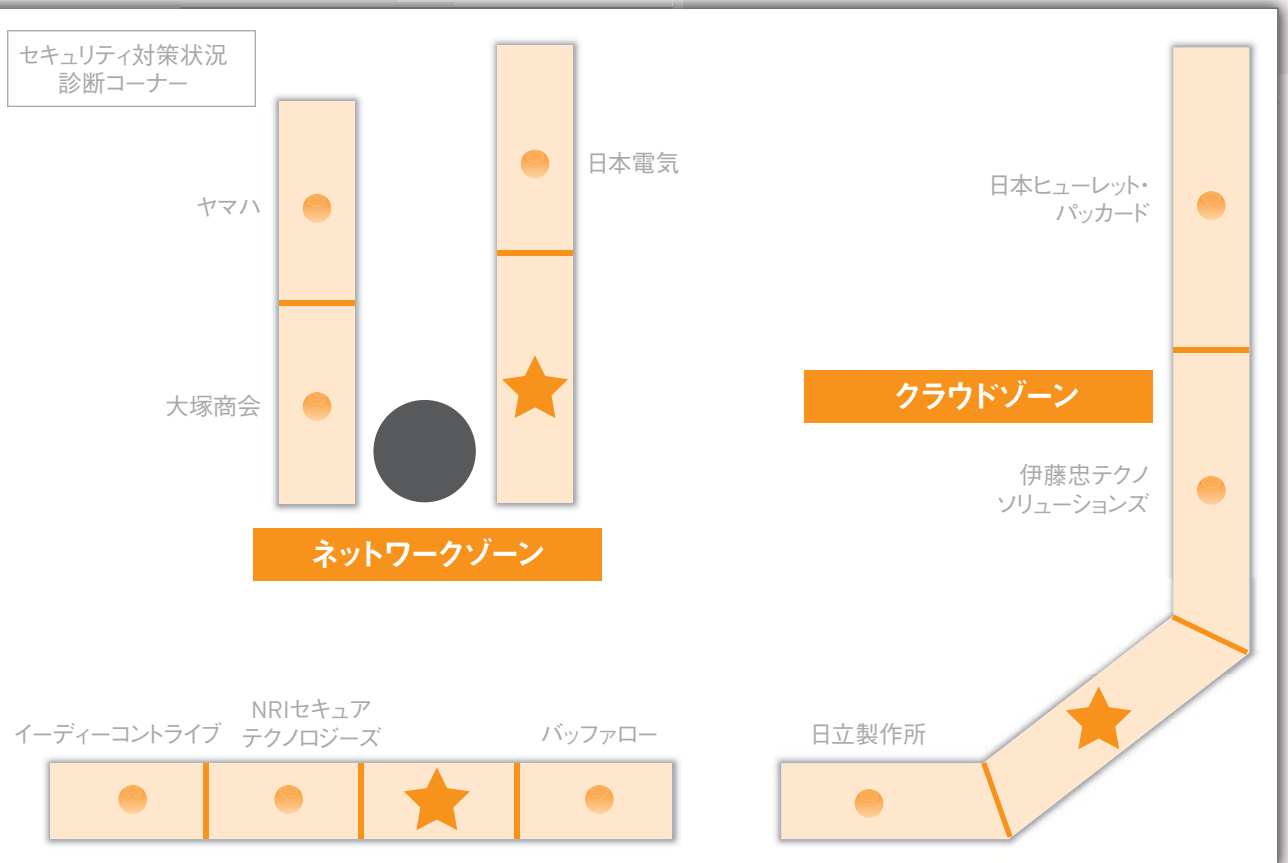
- Q1. 情報資産の機密性の識別や整理のための製品「SecureCube / Labeling」です。
- Q2. ISMS/ISO27001などの対応に向け、社内の電子情報資産の機密性を識別・整理するためのソリューションです。
- Q3. トレンドマイクロの「ServerProtect™」と共に、ストレージ内の効果的情報資産管理手法を提供しています。

株式会社バッファロー

- Q1. 「セキュリティUSBメモリ」、「セキュリティポータブルHDD(参考出展)」と「セキュリティNAS(Network Attached Storage)」です。
- Q2. トレンドマイクロの検索エンジンを使用したウイルスチェック機能を搭載しています。さらにUSBメモリとポータブルHDDでは、データの全自動暗号化や管理ソフトウェアによる一元管理などが可能です。NASはファイルサーバとしての十分な機能を低価格で実現します。
- Q3. 各デバイスのセキュリティ機能として、USBストレージには「Trend Micro USB Security for Biz」、NASには「Trend Micro NAS Security™」を組み込み、製品の差別化を図っています。

出展社によるプレゼンテーション

- 12:00-12:15
日立サーバ仮想化機構「Virtage」のご案内
株式会社日立製作所
- 12:30-12:45
SecureCube/Labelingによる情報資産の識別・整理の必要性
～不正競争防止法の観点から考える～
NRIセキュアテクノロジーズ株式会社
- 14:10-14:25
未知のウイルスにも対応するウイルス感染の監視/隔離ソリューション
～NECとトレンドマイクロの共同開発による
Threat Management Solutionの強化～
日本電気株式会社
- 15:40-15:55
次世代IT基盤とそのセキュリティ対策について
伊藤忠テクノソリューションズ株式会社



★ は、トレンドマイクロのブース
出展内容は次のページへ

Exhibition 展示コーナー

展示コーナーで紹介したトレンドマイクロの最新ソリューション

クラウドゾーン

最新ソリューション

- ・Trend Micro Deep Security™
- ・Trend Micro InterScan WebManager™ SCC
- ・Trend Micro Hosted Email Security™

トレンドマイクロは、「クラウドに対する脅威」と「クラウドからの脅威」という内外両面から複合的に対応する最新ソリューションを提供しています。Deep Securityは、サーバセキュリティに求められる5つの機能(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)を実装しており、不正侵入や脆弱性に対する攻撃をブロックします。InterScan WebManager SCCは、システムの運用負荷と管理コストの大幅削減を可能にするSaaS型URLフィルタリングサービスです。Trend Micro Hosted Email Securityは、クラウド型のメッセージングセキュリティサービス。ウイルスが添付されたメールや迷惑メールが社内に到達する前にトレンドマイクロ側でフィルタリングを行い、必要なメールだけを届けることができます。

ネットワークゾーン

最新ソリューション

- ・Trend Micro Network VirusWall Enforcer™ (以下、NVWE)
- ・Trend Micro Threat Management Solution™ (以下、TMS)

NVWEは、セキュリティパッチの迅速な適用が困難なOSやサポートが終了したレガシーOSなど、脆弱性があるOSによって構築されたシステムに導入することで、脆弱性を標的とした攻撃をネットワークレベルでブロックし、システムの継続的な安全性を確保する製品です。

TMSは、ネットワークを監視し、ネットワーク上の疑わしい挙動を検知することにより、パターンファイルだけでは対処できない未知の脅威*に対応します。危険度の高い挙動を検知すると、NVWEと連携して感染の疑いがある端末を隔離し、拡散を防止すると共に通知機能でトレンドマイクロに潜在的な脆弱性を迅速に報告します。また、復旧機能により自動的にクリーンアップを実行することも可能なため、安全なネットワーク環境を実現します。

※すべての未知の脅威に対応するわけではありません。

エンドポイントゾーン

最新ソリューション

- ・Trend Micro Portable Security™

従来、ウイルス検索を実施することが難しかったオフライン端末や、ウイルス対策ソフトをインストールできない端末に対し、ウイルス検索・駆除を可能にするUSBメモリ型検索ツールです。製造業の工場にあるオフライン端末や、高いパフォーマンスが要求されるために常駐ソフトを導入できない設計ソフト稼働端末などに対してウイルスチェックを行う際に有効です。管理プログラムをインストールした管理PCで最新パターンファイルをダウンロードして利用するため、最新の脅威にも対応できます。また、ログの一元管理が可能であることも大きな特長です。



トレンドマイクロ、中小規模オフィス向けNAS組込み型ウイルス対策ソリューション「Trend Micro NAS Security™」提供開始

トレンドマイクロは8月4日(水)より、中小規模オフィス向けNAS組込み型ウイルス対策ソリューション「Trend Micro NAS Security」の提供を開始しました。

ネットワーク経由でファイルサーバ機能を提供するLinuxベースのNASは、一般的なサーバに比べると管理や運用が容易なため、主に個人ユーザや中小規模のオフィスで利用されています。ところが、通常、ユーザではNASに任意のソフトを追加できないため、セキュリティを実装できないケースが多く見受けられます。

ウイルス対策ソフトを適用していないNASをファイルサーバとして利用する環境では、ウイルスがNASを媒介としてネットワーク上のすべてのPCに感染を拡大してしまう可能

性があります。このため、すべての社内PCにウイルス対策ソフトを導入していなかったり、個人が所有するPCの社内ネットワークへの持ち込みに関するセキュリティポリシーを設定していなかったりする傾向が高い中小規模のオフィスは、NASに対応するウイルス対策ソリューションを求めてきました。

そこでトレンドマイクロは、NASに組込んで使用するウイルス対策ソリューションTrend Micro NAS Securityの提供を開始しました。これまでNASのウイルス対策には検索用に別途サーバを設置することが求められましたが、同ソリューションはNASベンダーの製品にバンドルして出荷されます。このため、導入や運用における専門的な知識に依存することなく、手間をかけずにNASを媒介とするウイルスの感染拡大を予防できます。主な

機能は、自動および手動でのパターンファイルアップデート、リアルタイム・手動・予約によるウイルス/スパイウェア検索。検索結果などをログ情報として管理することもできます。

同ソリューションを搭載したNAS製品の第一弾は、2010年8月中旬に株式会社パッファローより出荷を予定しています。また、今後、各NASベンダーより、同ソリューションを組み込んだ製品が順次提供される予定です。TP

Internet Threat Report

不正プログラム感染被害報告数ランキング【2010年7月度】

2010年7月1日～7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	先月順位
1位	WORM_DOWNAD(ダウンロード)	ワーム	47件	(1位)
2位	MAL_OTORUN(オートラン)	その他	25件	(3位)
3位	TROJ_DLOADR(ディローダー)	トロイの木馬	19件	(圏外)
4位	TROJ_FAKEAV(フェイクエイビ)	トロイの木馬	17件	(4位)
5位	BKDR_AGENT(エージェント)	バックドア	15件	(6位)
6位	WORM_AUTORUN(オートラン)	ワーム	14件	(10位)
7位	JS_IFRAME(アイフレーム)	Java Script	10件	(圏外)
7位	TSPY_ONLINEG(オンラインゲーム)	トロイの木馬	10件	(圏外)
7位	TSPY_ZBOT(ゼットボット)	トロイの木馬	10件	(圏外)
10位	RTKT_BUBNIX(バブニクス)	ルートキット	9件	(圏外)

7月の不正プログラム感染被害の総報告数は1,618件。最も報告件数が多かったのは、「WORM_DOWNAD(ダウンロード)」の47件で、3ヶ月連続で1位になっています。

注目すべきは偽のウイルス感染警告を表示してユーザの不安をあおり、偽セキュリティソフトの購入を促す「TROJ_FAKEAV(フェイクエイビ)」です。メイン画面やWindowsのバルーンチップのメッセージをコンピュータの言語環境に合わせて、日本語のほか25種類の言語で表示するなど、ユーザを欺く手口がより巧妙化。この偽セキュリティソフトは正規Webサイトを改ざんし、サイト訪問者を不正なWebサイトに誘導した上で、不正プログラムをダウンロードさせることが確認されています。

また、正規サイト改ざんの代表例であるランブラー攻撃の手法が、迷惑メールにも応用されました。6月中旬より、迷惑メールに添付されたHTMLファイルを実行すると不正なWebサイトに接続し、不正プログラムをダウンロードしてしまう被害が報告されています。発信元の不明な電子メールは開封しないなどの注意が必要です。TP

※このランキングは、2010年7月1日から7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8月4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まれます。※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。