トレンドマイクロ「読むセミナー」No.3
脅威の入り口は、インターネットだけ？
～脅威が狙う、新たな「バックドア」とは？～

■ 最近の脅威はインターネットを迂回してやってくる・・・

「インターネットは危険」。
これは言うまでもない常識だ。しかし、最近の脅威傾向を見ると、意外な侵入手段が使われているのがわかってくる。これらの手段を用いる「脅威の作者」たちは、われわれの企業活動において、どうしても欠かせない行動を予測し、巧みにその穴を狙っている・・・
本ドキュメント、「トレンドマイクロ『読むセミナー』No. 3」では、最新の脅威傾向について述べながら、感染から拡散までの 3 つのポイントにおいて取ることができる一般的な対策と、トレンドマイクロのそれぞれのソリューションについて紹介するものである。

■「読むセミナー」の使い方

本ドキュメントは、短時間で知りたい情報だけをピックアップして読むことも、全体を通じて問題と解決策を把握することもできる。ニーズに応じて、使い分けていただきたい。

1. **最近の脅威傾向について知りたい！**
→ 1. はじめに(p. 3)へ
2. **それぞれの脅威と、それらに対する一般的な対策について知りたい！**
→ 2. ウイルス被害へのステップ(p. 6) へ
3. **トレンドマイクロから提供される具体的ソリューションを知りたい！**
→ 3. トレンドマイクロのソリューション(p. 7) へ

目次

1. はじめに

「インターネットは危険」という意識を持っていない人はさすがにいないだろう。便利な反面、危険が多くひそむインターネット。トレンドマイクロも大きく 5 つの危険に分けた啓発を行っている。

- Web からの脅威
- 差出人を偽るウイルス
- ネットワークウイルス
- スパイウェア
- ウイルスデマ情報

※トレンドマイクロ「セキュリティ情報」ページより「インターネットに潜む危険性･脅威を知る」ページから(http://jp.trendmicro.com/jp/threat/threats-knowledge/)。

本ホワイトペーパをご覧の方なら、これらの危険についてはよくご存知だろう。インターネットからやってくる脅威に関しては、1990 年代後半よりファイアウォール、IDS/IPS, ウイルス対策ソフトなどによる対策が謳われ、ほとんどの企業がインターネットとの接続ポイント(ウイルス対策はエンドポイント)にて何らかの対策を取っているはずだ。
しかし、この脅威の経路が、実はインターネットだけではなくなってきていることをご存知だろうか？
そう、USB メモリの登場だ。

1.1. 新たな媒介の登場

近年低価格化と大容量化が加速している USB メモリは、その可搬性の良さからも爆発的に普及した。その USB メモリは今、脅威をも「可搬」な媒体となっているのである。

表 1 は、トレンドマイクロが発表した、本年 2 月のインターネット脅威マンスリーレポートだ。1 位に輝く WORM_DOWNAD は 2008 年に発見された Windows OS の脆弱性を攻撃する脅威だが、いまだにランキングの 1 位を取り続けている。昨年のランキングでも 1 位になっており、息の長い攻撃と化している。WORM_DOWNAD は、MS08-067 と呼ばれるセキュリティパッチによって修正される Windows OS の脆弱性を利用して攻撃を行うワームだが、ネットワーク越し以外に、USB メモリを経由して感染する能力を持つ。WORM_DOWNAD が一度内部に入り込むと、インターネットに接続されているか否かに関わらず、感染可能な Windows OS を搭載した他のシステムに徹底した自己感染を試みる。その結果、脆弱性対策がなされていないシステムは全感染を引き起こしてしまう。その影響で、業務停止に陥ったケースも少なくなく、トレンドマイクロも実際に何件も現地対応を行っている。

表 1 ：2011 年 2 月　トレンドマイクロインターネット脅威マンスリーレポート

	検出名	通称	種別	検出件数	先月順位
1 位	WORM_DOWNAD.AD	ダウンアド	ワーム	4,570 台	2 位
2 位	CRCK_KEYGEN	キーゲン	クラッキングツール	3,273 台	3 位
3 位	MAL_DLDER	ディローダー	その他	1,478 台	-
4 位	HKTL_KEYGEN	キーゲン	クラッキングツール	1,450 台	6 位
5 位	WORM_ANTINNY.AI	アンティニー	ワーム	1,377 台	4 位
6 位	PE_PARITE.A	パリット	ファイル感染型	1,347 台	8 位
7 位	TROJ_SPYEYE.SMEP	スパイアイ	トロイの木馬	1,269 台	NEW
8 位	WORM_ANTINNY.JB	アンティニー	ワーム	1,149 台	7 位
9 位	MAL_OLGM-41	オーエルジーエム	その他	1,142 台	-
10 位	TROJ_DLOADR.KDS	ディローダー	トロイの木馬	1,076 台	NEW

1.2. USB メモリを悪用する脅威 - OTORUN と STUXNET について

WORM_DOWNAD 以外にも、USB メモリを悪用する攻撃は存在する。例えば、MAL_OTORUN だ。これは USB メモリを接続した

ときに、USB メモリの内容を自動的に読み込む機能、オートラン(autorun.inf)を悪用したものとして 2008 年に大騒動を巻き起こしたウイルスだ。MAL_OTORUN は、autorun.inf を無効にすることで、自動的な USB メモリの読み出しを禁止することが有効手段として、多くの企業などで対策がなされたが、現在も、報告数ベースのランキングでは 2 位にとどまる、これも息の長い攻撃だ。ちなみに報告数 1 位は、WORM_DOWNAD.AD である。
しかし、この防御手段が効かない新たな攻撃が観測されている。LNK_STUXNET(スタクスネット) と呼ばれる攻撃だ。昨年、イランのプラントが攻撃を受け、爆発の危機にさらされたことは記憶に新しいだろう。サイバー犯罪が、物理犯罪にまで展開するという、全く新しい攻撃として世界に衝撃を与えた。
STUXNET は、感染ファイルを開かなくても、エクスプローラなどで USB メモリを開き、アイコンを表示させた時点で感染行為を行うのだ。もともと、STUXNET は MS10-046 と呼ばれる、Windows ショートカットの脆弱性を悪用するもの。表示されるアイコンは実はこの脆弱性を悪用した LNK_STUNXET であり、そこから PC に WORM_STUXNET をコピーすることで感染する。
STUXNET のほかにも、autorun.inf を利用しなくても感染する USB メモリを媒介としたウイルスは、今後も登場し続ける可能性は大きい。
このように、ウイルスの作者は、Windows の脆弱性はもちろんのこと、標的が USB メモリを利用することを想定している。そして、autorun.inf を無効化していることもあらかじめ想定している。ウイルスの作者は、新たに見つかる脆弱性と、セキュリティ対策の裏をかき、よく考えられた攻撃を仕掛けてきている。従来の対策だけでは不十分となりうる可能性は十分にある。

1.3. 最も狙われるポイント - 閉鎖ネットワーク(Closed Network)

「危険はインターネットから」という常識に基づけば、「インターネットに接続していなければ安全性が高い」という結論に至るのは当然だ。その結果、インターネットに接続されていない閉じたネットワーク、Closed Network (閉鎖ネットワーク)のセキュリティ対策は、おのずと手薄になる傾向がある。攻撃者は、この事情もよく理解した上で脅威の開発を行っていると思われる。

1.4. 利用者の行動学に基づいた「攻撃手法」

システムがインターネットにつながっていない場合、インターネットからの情報や、メールに添付されているような情報を取り込みたい時どうすればよいのだろう？ここで再度登場するのが USB メモリだ。必要なデータを、インターネット接続端末や自宅の PC から USB メモリにコピーし、それを閉鎖ネットワークの端末に指して、コピーすることで、インターネットにつながっていなくても、インターネット上の情報を「ダウンロード」することができるようになる。そして、一緒にウイルスもネットワークに入り込んでしまうという具合だ （図 1)。
攻撃者は、このような行動パターンを熟知した上で、あえて USB メモリをウイルスや攻撃の媒体としていると考えられている。インターネットからの攻撃は、すでに普及しているさまざまなセキュリティシステムから攻略困難だ。そうなれば、必然的にセキュリティ強度の低い環境や、インターネット境界線上のセキュリティシステムをかいくぐる、「人の手で運ばれる」ことができる媒体を選ぶようになるだろう。

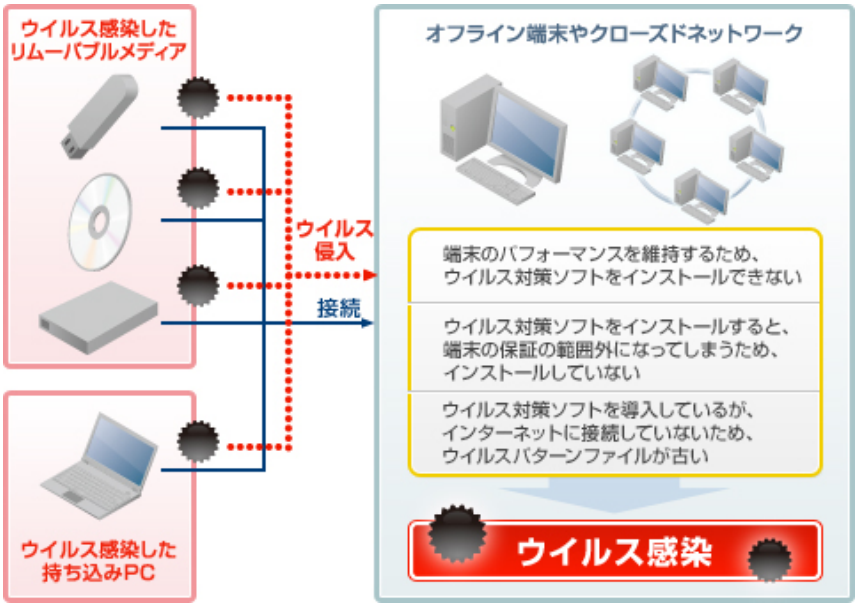


図 1：USB メモリ や持ち込み PC を介した感染の拡大

「外出先でインフルエンザなどの病原菌がついてしまったかもしれない手を洗わず、生まれたての子供に触る」人はさすがにいないだろう。しかし、情報の世界になるとあまり問題ではないように思えるから危険だ。ファイアウォールやIDS/IDF などの「消毒」を経ずにウイルス対策そのものがされていないシステムから構築される「無菌室」に入り込んだUSB メモリ経由のウイルスは、その後猛威を振るうことになる。

2. ウイルス被害へのステップ

USB メモリなどの可搬型メモリを媒介とした脅威のもたらす被害には段階がある。

1. (USB メモリなどを媒介とした)PC への感染
2. (感染した PC から)他のシステムへの拡散

それぞれの段階で取れる手段はある。具体的な方法について考えてみよう。

2.1. 「PC への感染」への対策

USB メモリの利用を制限するために、利用ルールを設けたり、PC の USB ポートを物理的につぶす、あるいはドライバで利用できなくするなど、いくつかの方法が考えられる。
しかし、手のひらに隠れるサイズの USB メモリの持ち込みを厳密に制限することは困難であるし、また、USB ポートやドライバなどにより、USB メモリの利用を完全に不可能にしてしまうことで、生産性を向上させる目的で利用されている USB メモリの利用まで制限することとなり、結果、業務効率の低下を招きかねない。

そこで、USB メモリなどから、PC への感染を防止することで、一つの技術的対策とすることができる。その方法について考えてみよう。

この問題に対する対策は、ひとつしかない。ウイルス対策の導入だ。少なくとも USB メモリを介して入ってこようとしている脅威が「既知」のものである限り、ウイルス対策ソフトウェアが検出し、ブロックすることができる。
しかし、環境によってはウイルス対策ソフトウェアがインストールできない場合もある。例えば医療機器や工場のライン監視システムなどの特殊システムだ。こういった特殊端末に対しては、定期検索を実行するための他の方法が必要になる。例えば、最近は USB メモリがそのままウイルス検索を実行してくれるようなウイルス対策製品も登場している。USB メモリを対象システムに挿すだけで、ウイルス検索や駆除を行ってくれるというものだ。また、ウイルスが発する通信を分析し、ウイルス感染端末を検出する新たなアプローチもある。この方法は、通信のみを見張るため、システムにはソフトウェアのインストールは不要だ。パターンベースでの検出ではないことから、未知の脅威の検出も期待できる。

ホワイトリスト方式の新たなウイルス対策アプローチも登場しているが、こういった対策には必ずソフトウェアのインストールを伴う。ソフトウェアのインストールを一切行わず、業務に差し支えのない時間を選んで実行することができるオンデマンドの USB メモリ型ウイルス検索は、今後特殊端末向けのウイルス対策の主流になるかもしれない。

2.2. 「他のシステムへの拡散」への対策

WORM_DOWNAD などの攻撃は、OS の脆弱性を悪用してその感染を広げる。つまり、ウイルス対策を行うと同時に、脆弱性対策も正しく迅速に行っていれば、こういった脅威にさらされる危険は低くなる。脆弱性対策とはすなわち、セキュリティ修正パッチの適応だ。しかし、さまざまな事情があって迅速なパッチ展開が困難な場合がある。ソフトウェアベンダのサポート対象環境から外れるために、システム稼働環境を変更できない場合。冗長構成がされておらず、リブートできない場合。さらに、インターネットにつながっていないために、そもそも脆弱性攻撃を受けないと判断している場合などだ。
しかし実は、脆弱性を悪用する攻撃は、社内ネットワークを通じて行われるケースがほとんどだ。この場合、社内ネットワークは、インターネットにつながっている/いないを問わない。IP 接続されていればすべてが拡散の可能性を秘めているといってよい。
ネットワークを介した拡散防止に最も効果的なのは、上記のとおり「脆弱性をなくす」、つまり、セキュリティパッチの迅速な適応だ。しかし、さまざまな事情で、適応が遅れることがあるのは前述のとおりだ。
そのため、他の方法で「パッチのような振る舞い」を代わりに果たさせる方法が必要になる。OS やアプリケーションにパッチを当てなくても、当てたときと同じ効果が得られるものである。こういった「脆弱性保護」を目的としたソリューションには、専用機によって提供されるものと、エンドポイントにインストールして用いるエージェント型がある。

3. トレンドマイクロのソリューション

2 章で、USB メモリなどのデバイスを媒介とした感染、拡散の各ポイントで、どのような対策が必要とされるかを述べた。本章では、トレンドマイクロが具体的にどのようなソリューションで各対策を提供しているかについて説明する。

3.1. トレンドマイクロの「PC などへの感染」対策

ウイルス対策のみが唯一の有効策である本課題に対して、トレンドマイクロは 3 つの製品を提供する。
1 つ目は、言うまでもなくウイルス対策ソフトウェア、ウイルスバスター コーポレートエディションの導入だ。企業向けウイルス対策製品として不正なプログラムの侵入を防止する同製品により、脆弱性を利用して侵入してくるウイルスの検出、防御が可能になる。

製品ページ：http://jp.trendmicro.com/jp/products/enterprise/corp10_5/index.html

3.1.1. Trend Micro Portable Security (TMPS)

しかし、ここでは「ウイルス対策ソフトがインストールできない」、「運用上最新パターンファイルの維持が非常に困難」、といった特殊環境を考えてみたい。
こういった環境に対して、トレンドマイクロは USB メモリ 型ウイルス対策ソリューション、Trend Micro Portable Security(TMPS) を提供している。検索の対象となる端末の USB インタフェースに TMPS を差し込めば、ウイルス検索を実行する。 事前にソフトウェアをインストールしておく必要もない。
TMPS 内のパターンファイルを最新に保つため、管理用のコンピュータを一台用意し、そこへ接続することで TMPS のパターンのアップデートを行う(図 2)。こうすることで、検索対象端末がインターネットにつながっていなくても、間接的に最新パターンでの検索が実現するのだ。また、管理用コンピュータでは、TMPS 内に維持されている検索時のログファイルの管理も行えるため、万が一ウイルスの検出や駆除を行った場合、どの端末で問題が発生したかを管理者は集中的に管理することができる。

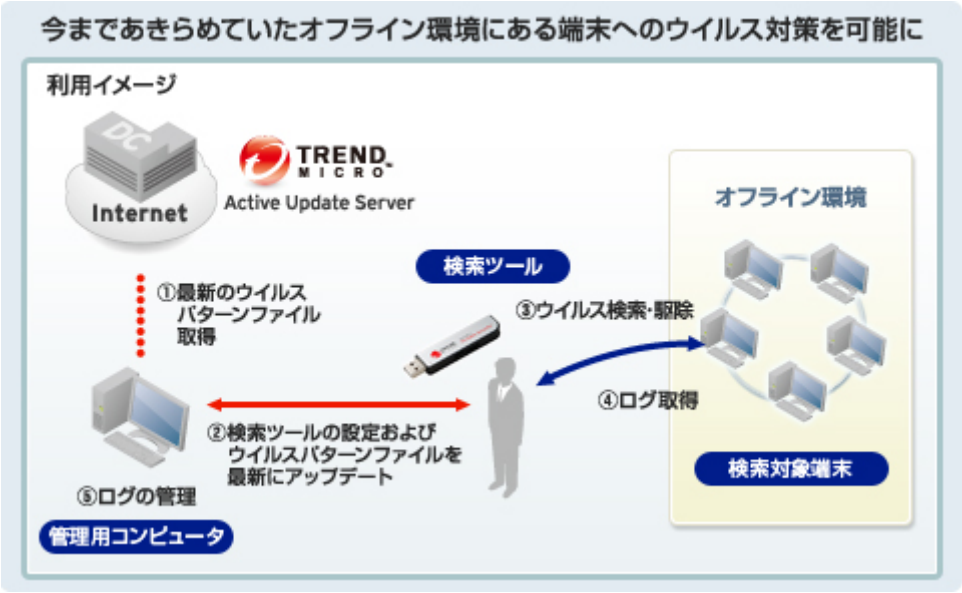


図 2: TMPS による特殊環境のウイルス検索の実現[2]

3.1.2. Trend Micro Threat Management Solution (TMS)

トレンドマイクロには、もうひとつ非常にユニークなウイルス検出ソリューションがある。Trend Micro Threat Management Solution (TMS) と呼ばれるこの製品は、ウイルスが発する通信をもとに、感染端末の検出、特定を行う。昨

[2] ウイルス検索時に、一時的に検索対象端末にドライバおよびローカル HDD にファイルを作成しますが、検索終了後、検索対象端末にドライバおよびファイルは残りません。TMPS は、管理用コンピュータのウイルス検出は行いません。

今のウイルスは、インターネット上のシステムをはじめとする、他のシステムと通信を頻繁に行う傾向がある。つまり、感染した後も「おとなしくはしていない」のだ。したがって、その動きを観察することで、感染がばれてしまうのだ。TMS は、通信の監視を行うシステムである Threat Discovery Appliance(TDA) と、TDA が検出した情報をもとに作成されるレポートなどからなる、総合ウイルス対策ソリューションである(図 3)。

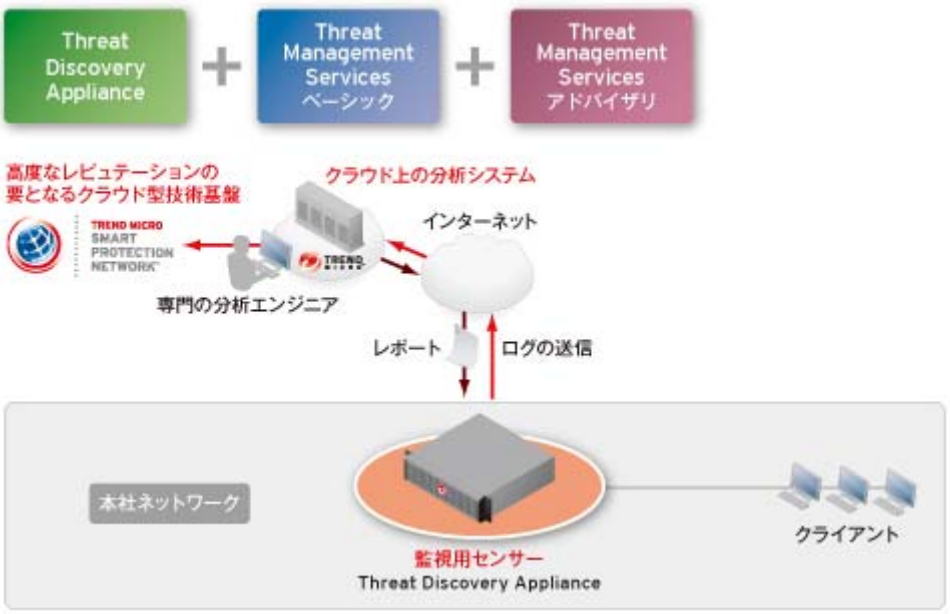


図 3 Trend Micro Threat Management Solution の概要

通常のウイルス対策は、パターンファイルにマッチする脅威を検出する方法で行われるが、TMS のアプローチは通信を監視する、新しいものだ。したがって、異常通信として検出された活動のもととなるウイルスが、パターンファイルの用意がない、未知の脅威である可能性もある。そういう意味から、TMS は、未知脅威検出の可能性も持っていると言える。さらに、Threat Management Services アドバイザリにより、検出された脅威への迅速な対応が可能になる。定期的なレポートにより、セキュリティの可視化や、必要とされるセキュリティ対策などの情報が得られるほか、緊急度の高い感染が発生した場合には、トレンドマイクロからお客様へ緊急連絡がいく仕組みになっている。技術と、トレンドマイクロの専門分析エンジニアの知識により感染時の迅速復旧を実現する、新しい形のウイルス対策ということができる。

製品ページ：http://jp.trendmicro.com/jp/products/enterprise/tms/index.html

3.2. トレンドマイクロの「他のシステムへの拡散」対策

拡散を防止するためには、二次被害を受ける可能性のある端末への脆弱性対策が必須だ。ここでは、セキュリティパッチが公開されても、すぐにパッチを当てることが困難なシステムなどに対するソリューションとして、セキュリティパッチと同等の役割を果たす 2 製品を紹介する。

3.2.1. Trend Micro Deep Security

特に業務上重要なサービスや web サービスを提供しているサーバに対しては、脆弱性対策のほか、サーバに特化したセキュリティ対策を総合的に行うことが理想的だ。Trend Micro Deep Security は、脆弱性対策を含むサーバに必要となる 5 つの機能を持つ統合サーバセキュリティ対策ソリューションだ(図 4)。

図 4：Trend Micro Deep Security のもつ 5 つのサーバ保護機能

仮想パッチに関する考え方は、侵入防止ファイアウォールと同じだ。エージェントと呼ばれるソフトウェアをインストールし、パッチの代わりに脆弱性を保護させる。自動設定により保護が必要とされる脆弱性を自動的に検知し、それに対する仮想パッチを展開。パッチ適応などによって脆弱性対策がなされれば、仮想パッチを解除し、システムに必要以上の負荷をかけない工夫がされている。
Trend Micro Deep Security は、仮想環境にも対応している。仮想マシン上で動作する複数の仮想マシンに対し、VMsafe API 上で動作する仮想アプライアンスとして各インスタンスを保護することが可能だ(図 5)。複数の業務サーバを統合し、仮想化した場合などに最適なソリューションとなる。仮想化向けソリューションの利用により、Windows2000 などのサポート切れ OS の延命利用も可能となる。

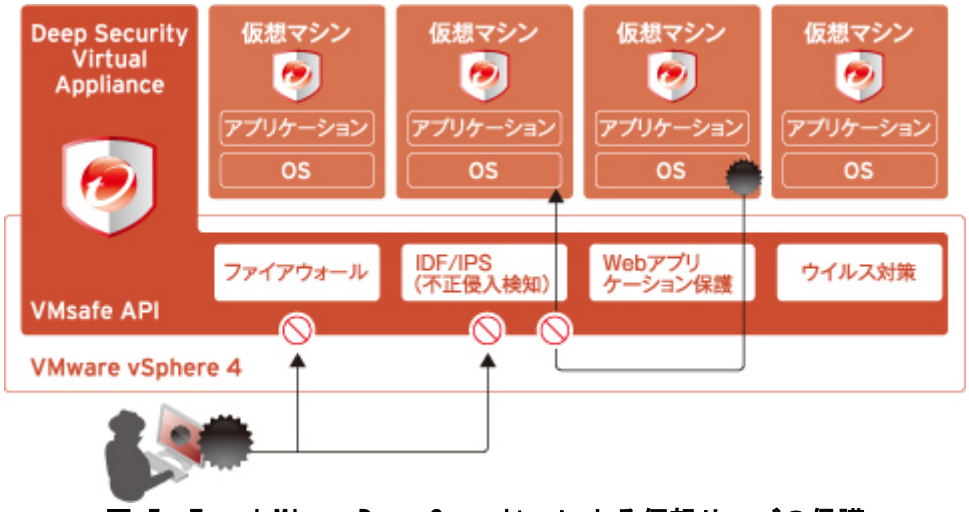


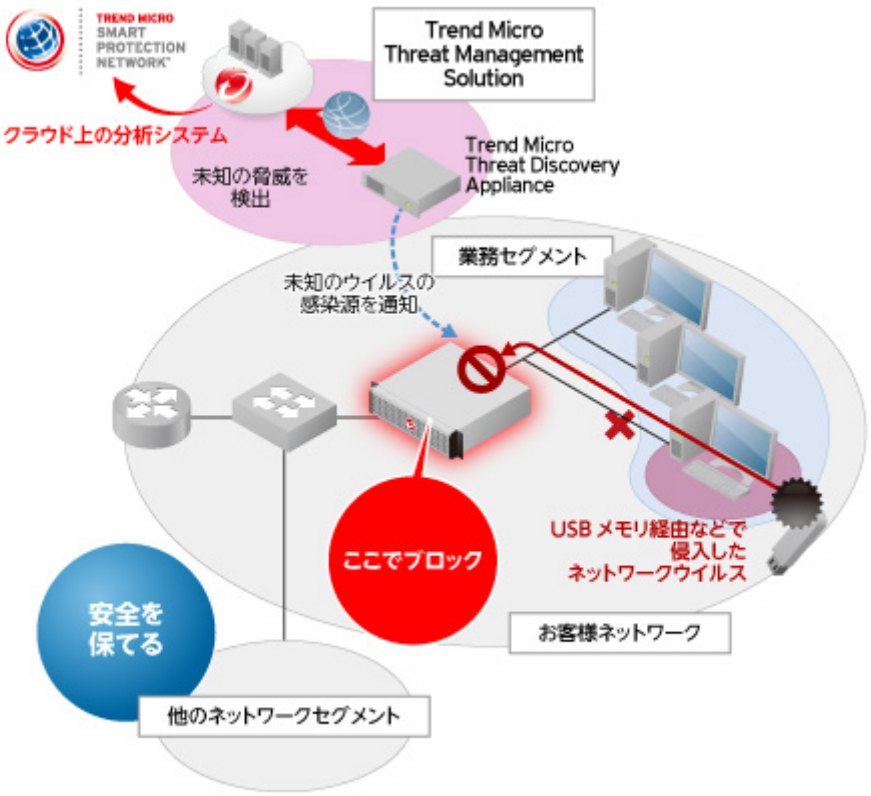
図 5: Trend Micro Deep Security による仮想サーバの保護

製品 URL: http://jp.trendmicro.com/jp/products/enterprise/tmds/index.html

3.2.2. Trend Micro Network VirusWall Enforcer(NVWE)

侵入防止ファイアウォールや Trend Micro Deep Security のように、エージェントソフトウェアのインストールがどうしてもできないというシステムが存在する。この場合、システムには何もソフトウェアをインストールせず、別途専用機に脆弱性を見張らせるソリューションが好ましい。NVWE は、持ち込み端末の制限機能のほか、クライアントやサーバとは独立したひとつの専用機(アプライアンス)として、脆弱性を攻撃する通信を遮断する仕組みを持つ。重要なサーバセグメントや、特殊機器によって構成されるセグメントの前に同機を置いて、脆弱性攻撃を防ぐ壁として利用するイメージだ。

さらに、NVWE は、TMS と組み合わせることで、TDA の検出した感染端末をネットワークから切り離すことができる(図 6)。



※すべての未知の脅威を検出できるものではありません

図 6: NVWE を用いた脆弱性の保護

製品 URL: http://www.trendmicro.co.jp/NVWE

4. まとめ

インターネットが危険であることに関しては、利用者のほとんどが認識していることだろう。しかし、脅威は必ずしもインターネットだけから入ってくるわけではない世の中になっている。USB メモリなどの可搬型デバイスを媒介として感染を広めてくる脅威が目立ち始めている。特に、インターネットとの接続を行わないからこそ、情報をインポートすることが困難な端末などに対し、USB メモリなどを利用するケースが多いと思われるが、そういった端末に限ってウイルス対策や脆弱性対策がなされていないことが多く、狙われやすい傾向にある。
本ドキュメントでは、そういった新たな脅威の傾向について述べ、感染から拡散に至るまでの 3 つの段階において、取ることができるソリューションについて説明した。
ご自身の環境が今、どういった状況にあるかを踏まえ、最適な対策を選択していただき、最新の脅威に備えていただきたい。