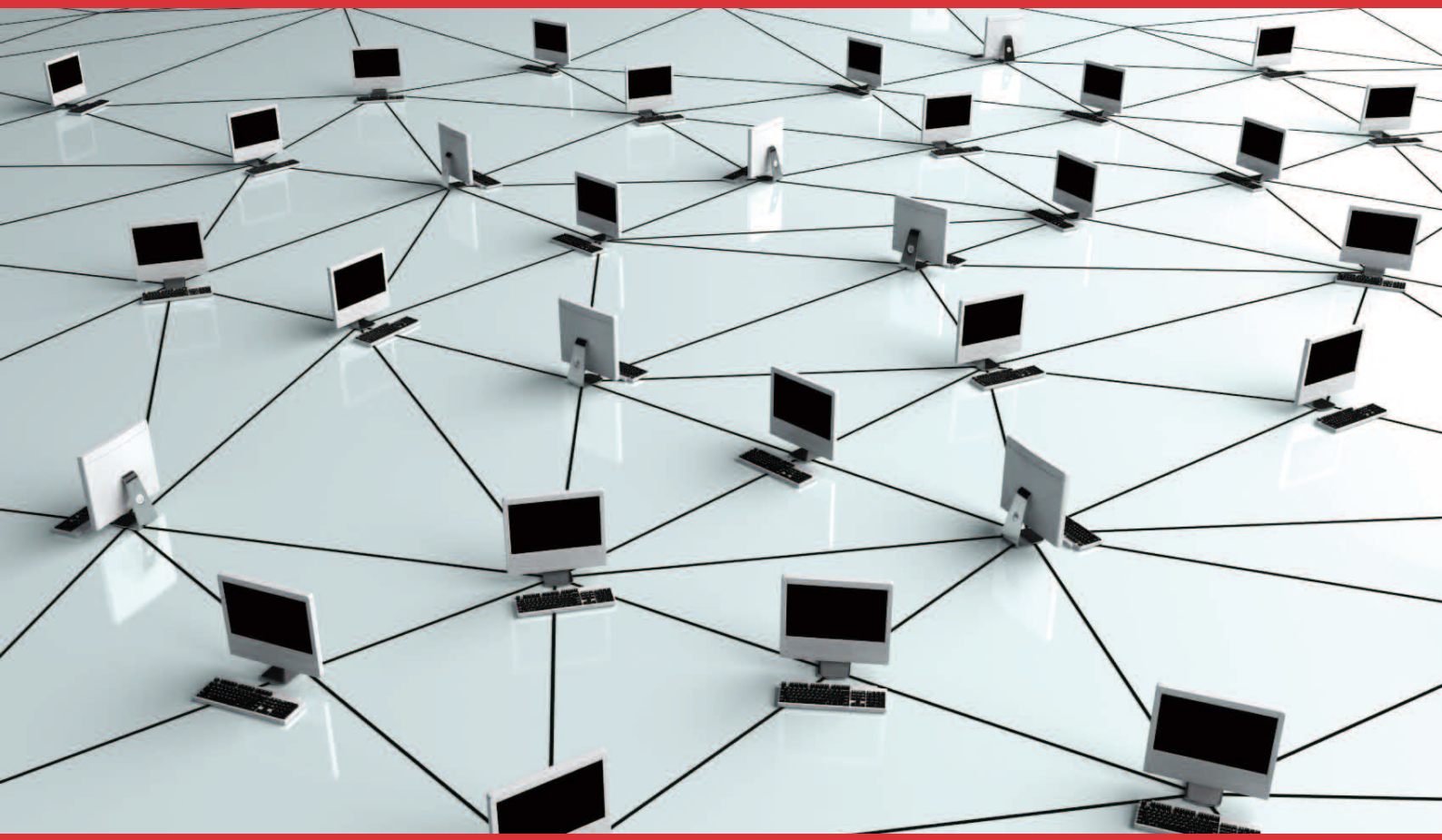
COMPUTERWORLD Deep Dive

コンピュータワールド ディープ・ダイブ



VDI／仮想デスクトップ導入、成否を分けるのはセキュリティ対策

導入前に知っておきたい新しい技術

text by Computerworld.jp

Copyright © 2011 IDG Interactive, Inc. All rights reserved.

TREND MICRO™

VDI／仮想デスクトップ導入、成否を分けるのはセキュリティ対策

BCP（事業継続計画）やワークスタイル変革といった観点から、クライアント環境を仮想化するVDI（Virtual Desktop Infrastructure）を導入する企業が増えている。VDIの導入に当たっては、使い勝手を左右するパフォーマンスや導入コストなどばかりでなく、セキュリティ対策も不可欠である。だが、VDIのセキュリティ対策には特有の課題がある。

デスクトップ仮想化の導入時に見過ごされがちなセキュリティ対策

在宅勤務やテレワークなど、これからのワークスタイルを支えるソリューションとして、ここ数年の間に仮想デスクトップ環境（VDI：Virtual Desktop Infrastructure）への注目が急速に高まっている。IT専門調査会社のIDC Japanが2010年11月に発表した市場予測によると、2010年のクライアント仮想化市場（VDIのほかアプリケーション仮想化、プレゼンテーション仮想化なども含む）の市場規模は1,921億円だったが、これが2014年には5,388億円にまで急拡大する見込みだという。とりわけVDIの成長には目覚ましいものがあり、VDIを構成するクライアント仮想化ソフトウェアの2009～2014年における年間平均成長率は、実に70.6%にも達すると予測されている。

さらに、2011年3月に発生した東日本大震災の影響により、企業のVDI導入ニーズはさらなる高まりを見せている。災害発生時のBCP（事業継続計画）遂行や、懸念されている首都圏の電力事情に対応するため、在宅やサテライト・オフィスでの勤務が真剣に検討されており、それをサポートする手段としてVDIが注目されているのだ。

単に社内のPCを自宅に持ち帰って業務を行うのとは異なり、VDIであればどこからでも社内にいるのと同じように、社内の業務アプリケーションやファイル・サーバを利用することができる。つまり、オフィスを離れた場合の業務生産性への影響をほぼゼロにすることができるわけだ。IT部門にとっても、社員がPCを自宅に持ち帰ることで生じるIT統制上のリスクが軽減されるメリットがある。

このように注目を集めるVDIだが、導入の際にしばしば検討を忘れがちなのが「クライアント・セキュリティ」の問題である。VDIによる仮想デスクトップでも、通常のクライアントPCと同じようにOSやアプリケーションが動作し、インターネットにも接続されている。したがって、OS／アプリケーションのセキュリティ・アップデートやウイルス検知／駆除などのセキュリティ対策も、通常のPCと同じように必要である。

もっとも、VDIによる仮想デスクトップでは、1つのマスター・イメージに対してOS／アプリケーションのセキュリティ・パッチを適用するだけで、すべての仮想デスクトップに対してアップデートを一括展開することができる。そのため、OSやアプリケーションの管理上の負担は軽減される。

考慮しなければならないのは、ウイルス対策ソフトが消費するリソースの部分なのである。

ウイルス対策ソフトが引き起こすVDI特有の問題とは

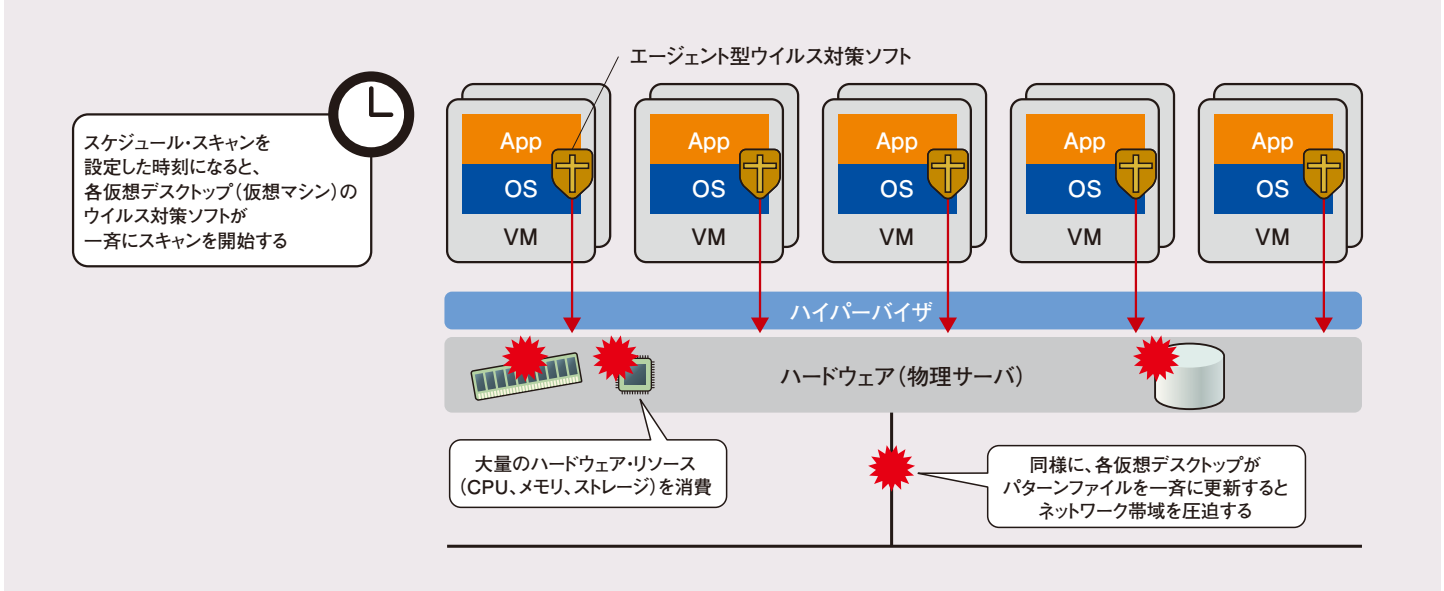
なぜ、VDIにおいてはウイルス対策が問題となるのだろうか。

基本的にはVDIによる仮想デスクトップにも、通常のクライアントPCと同じようにエージェント型のウイルス対策ソフトをインストールすることができる。先ほども触れたとおり、VDIではマスター・イメージにウイルス対策ソフトをインストールすれば一斉に展開できるので、導入作業は容易だ。

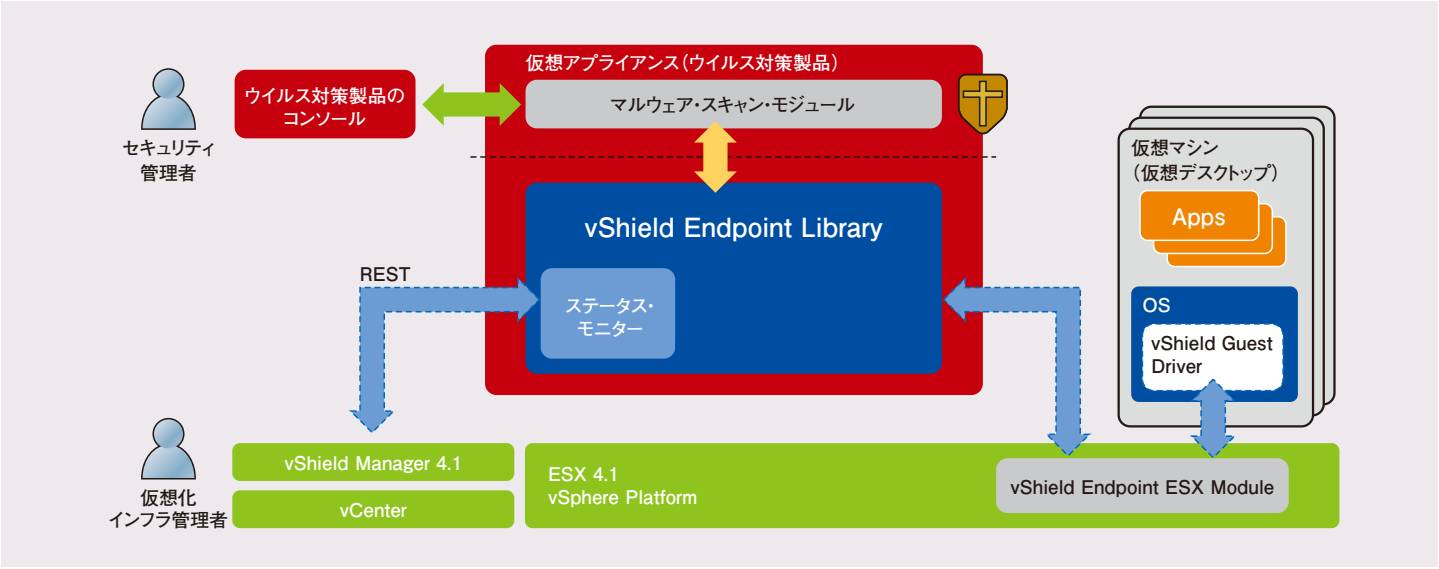
だがここに、VDIならではの“見えない問題”が潜んでいる。それは、個々の仮想デスクトップ上で動作するウイルス対策ソフトが消費するリソースの問題だ。

一般的なウイルス対策ソフトは、ダウンロードなどで新たなファイルが追加されたときにファイルを検査する「リアルタイム・スキャン」と、ディスク内に保存されているファイルを定期的に検査する「スケジュール・スキャン」の両方の機能を備えている。だが、1台の物理サーバ上で数十台もの仮想デスクトップが稼働するVDIの場合、ウイルス対策ソフトが一斉にスケジュール・スキャンを開始すると、仮想ホスト・サーバのリソース（CPUやメモリ、ディスクI/O）を一気に消費してしまう。パターン・ファ

従来のクライアント環境をそのまま移行できるのがVDIのメリットだ。しかし、従来型のウイルス対策ソフトとその運用方法をそのままVDIに適用すると、パフォーマンス問題が生じやすい



VMware vShield Endpointのアーキテクチャ



イルの更新にも同様の問題があり、ダウンロードが一斉に始まることで、物理サーバのリソースやネットワーク帯域を大量に消費してしまうのである。

大量のリソース消費によって、ふだんは問題なく動作している仮想デスクトップのパフォーマンスも著しく低下してしまう。例えば、急ぎの書類を作成している最中や客先でのプレゼンテーションの最中にウイルス・スキャンが始まり、仮想デスクトップがほとんど動かなくなってしまっては、ビジネス上の大きな損失にもつながりかねない。何よりも“快適な使い勝手”が重視される仮想デスクトップにとって、これは大きな課題なのである。

VMwareの新しい技術「vShield Endpoint」

VDIにおけるこうした課題を解消するために、仮想化ソフトウェアを提供するヴイエムウェアは昨年8月、「VMware vShield Endpoint（以下、vShield Endpoint）」という新たな製品を投入した。vShield Endpointは、仮想化プラットフォーム「VMware vSphere 4.1」とVDIプラットフォーム「VMware View 4.6」に対応しており、仮想化システムをトータルに保護するソリューション群「VMware vShield」ファミリーの1つとして、VDIのウイルス対策を中心に、仮想化されたインフラを常にセキュアに保つ機能を提供する。

vShield Endpointは、ハイパーバイザ上に展開されたウイルス対策専用の仮想アプライアンスを用いて、他のすべての仮想デスクトップ（仮想マシン）を保護する仕組みを提供する。アンチウイルスの機能をオフロードし、保護対象とする個々の仮想デスクトップにエージェントをインストールする必要がないのが特徴だ。

ウイルス検知／駆除を実行する仮想アプライアンスは、ヴイエムウェアのパートナーであるセキュリティ・ベンダーが提供する。この仮想アプライアンスと仮想マシンにインストールされているシン・エージェント（Thin-Agent、仮想ディスクのI/Oをスキャンするドライバ）を、ハイパーバイザ・レイヤにあるカーネル・モジュールが仲介することでウイルススキャンを実行する。

ちなみにvSphereプラットフォームでは、vShield Endpointの登場以前から、仮想アプライアンスを利用したセキュリティ技術として「VMsafe」が存在していた。VMsafeは、サードパーティーのソフトウェアがAPIを通じてメモリやCPU、ネットワーク・パケット、ストレージなどを監視することができる仕組みである。ただし、ウイルス対策に特化したvShield Endpointがリリースされたため、現在では、VMsafeは侵入防御／検知やファイアウォールの機能に、vShield Endpointはアンチウイルスに、と目的によって使い分けられるようになっている。

セキュリティ対策におけるVDI特有の問題を解消する新たな技術「vShield Endpoint」。VDI／仮想デスクトップにそれを適用する具体的メリットとは何か。また、具体的ソリューションにはどのようなものがあるのか。ヴイエムウェア、トレンドマイクロの両エキスパートに話を聞いた。

物理クライアントPCよりも高度なセキュリティを実現

仮想マシンのウイルス対策をオフロードするvShield Endpointには、物理マシンよりも優れたセキュリティ特性が数多く備わっている。ヴイエムウェアのスペシャリスト システムズエンジニアの各務茂雄氏は、そのメリットを次のように紹介する。

「まずは、仮想化の基盤であるハイパーバイザのレイヤでセキュリティを担保しているため、仮想マシンを新たに作成した時点ですでに『セキュアな状態』になるという点が挙げられる。また、仮想デスクトップを使用することにより、社外からアクセスする場合でも、社内で使用するのと同様のセキュリティ・レベルが保てる。クライアント・セキュリティ全体に穴が生じにくくなるという事実は、IT管理者にとっても大きな利点だろう」

また「耐タンパ性」の高さもvShield Endpointの特徴だと各務氏は述べる。ここでいう耐タンパ性とは、セキュリティ製品そのものへの攻撃が論理的に困難であるということを指す。

ヴイエムウェア
スペシャリスト
システムズエンジニア
各務茂雄氏

トレンドマイクロ
エンタープライズマーケティング部
プロダクトマーケティングマネージャ
福井順一氏

「ウイルス検知／駆除機能を提供する仮想アプライアンスは、各仮想デスクトップが属するネットワークからは完全に切り離されている。仮想マシンと仮想アプライアンスはネットワークを経由せず、直接物理サーバのメモリ上でデータをやり取りするのだ。そのため、仮想アプライアンスのウイルス対策機能を外部から攻撃することは、論理的に困難だ」

加えて、仮想化技術の大きな利点の１つでもある物理サーバ間のライブ・マイグレーション時にも、vShield Endpointを始めとしたセキュリティ機能は透過的に継承される。

「仮想デスクトップが別の物理サーバに移動しても、そこのハイパーバイザ上で動いている仮想アプライアンスがセキュリティをカバーする。それぞれの仮想デスクトップ（仮想マシン）から見れば、セキュリティ機能は何も変わることなくそのまま維持されるということだ」

ほかにも、仮想マシンの停止時にも仮想アプライアンスは動作を続けているため、長期間停止していた仮想デスクトップを起動した際に、即時に最新のセキュリティが適用されるというのも優位点だ。実際に、物理マシンの場合は、古いパターン・ファイルをしばらく使用していたためにマルウェアに感染する例が多いのだという。

ハードウェア・リソースの有効活用でROIの最適化

各務氏は、運用管理面でのメリットも強調する。

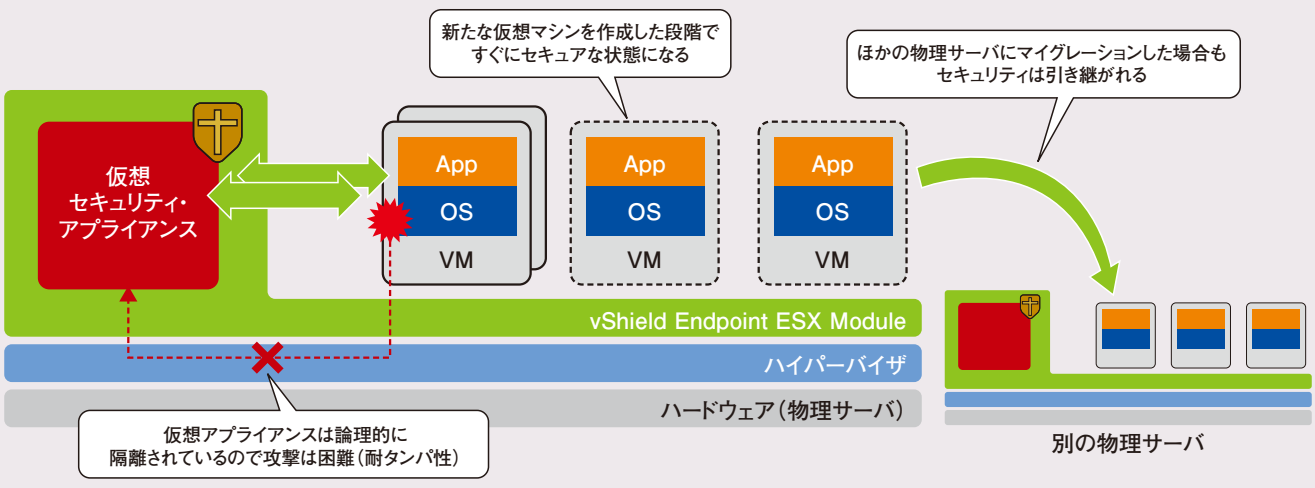
「vShield Endpointの導入により、IT管理者はVDIの運用をきわめて効率的に行うことができるようになる」（各務氏）

先に述べたとおり、個別にウイルス対策ソフトをインストールしたり、ウイルスのパターン・ファイルをダウンロードしたりする必要がなく、ライブ・マイグレーション時にもセキュリティの再設定が必要ないことなどがその根拠だ。また、アーキテクチャ的に、仮想化インフラの管理とセキュリティ管理とが分離されているため、それぞれの管理者が管理作業を分担することもできる。

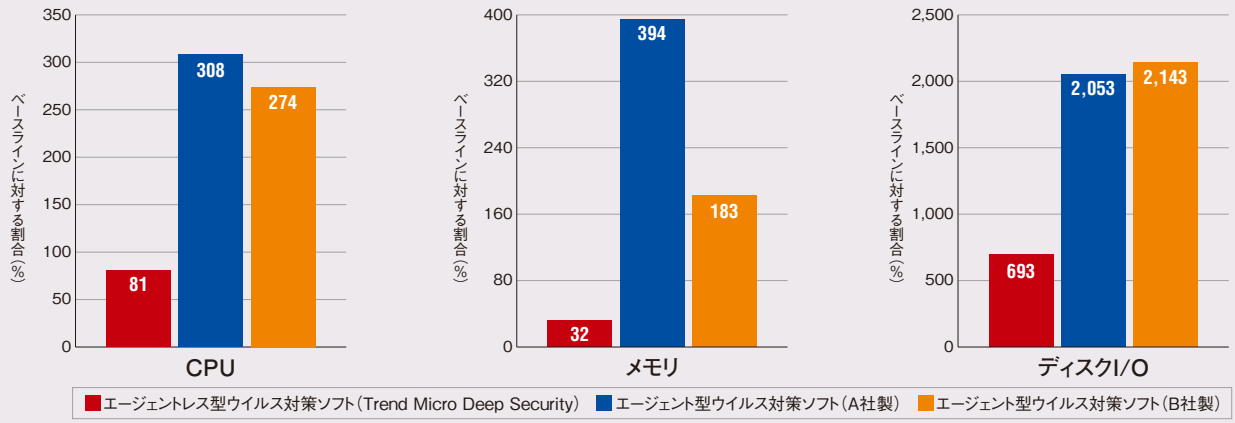
さらに各務氏は、購入するハードウェア・リソースを有効に使えるようになると説明する。

「それぞれの仮想デスクトップからアンチウイルス処理を切り離し、消費リソースを削減すること

vShield Endpointを適用することで、仮想デスクトップは物理クライアントPCよりも強固なセキュリティを手に入れることができる



vShield Endpointに対応したエージェントレス型ウイルス対策ソフトと、従来型のエージェント型ウイルス対策ソフトとの実行負荷の比較（資料提供：トレンドマイクロ）



このテストは、「Micrsoft Windows 7」が稼働する25台の仮想クライアント上でウイルススキャンを実行し、管理ツールの「vCenter」でCPU、メモリ、ディスクI/Oの負荷を計測したもの。数値の小さいほうがより負荷が少ないことを示す

※ このテストでは、ウイルススキャンと同時に独自設定の負荷テストを実行している。また、「ベースライン値」は、ウイルススキャンを実行しない状態で負荷テストを実施した際の結果（平均CPU使用率：4,109.76MHz、平均メモリ使用率：7,893.28MHz、平均ディスクI/O：1,741.23KBps）を指す。グラフ中のそれぞれの負荷の数値は、ベースライン値に対する割合（パーセンテージ）を示す。
※ A社、B社のエージェント型ウイルス対策ソフトは、25台の仮想クライアントで同時にウイルススキャンを開始している。TMDSでは、自動で一度に1台のスキャンだけが行われている。

出典：「VMware ESX 4.1のホスト・リソース消費オーバーヘッドとベースラインの比較」米国Tolly、2010年10月

ができるため、1台の物理サーバ上でより多くの仮想デスクトップを稼働させることができるようになる。物理サーバ1台当たりの仮想マシン数が多く、ストレージのI/Oへの影響が大きいVDIの場合、サーバやストレージの使用効率を高める事で、最適なROI（投資対効果）を実現することができる」

現在のところ、vShield Endpointに対応したウイルス対策ソリューションとしてはトレンドマイクロの「Trend Micro Deep Security AV for VDI（以下、Deep Security）」がある。

トレンドマイクロのエンタープライズマーケティング部でプロダクトマーケティングマネージャを務める福井順一氏は、「Deep Securityは、仮想アプライアンスを用いて個々の仮想デスクトップにウイルス対策ソフトをインストールする必要がない『エージェントレス型』の仕様であるため、パターンファイルの配信やウイルス・スキャンによってVDIのパフォーマンスを落とすことがない。VDI導入によるユーザーの満足度をより一層高めることにつながるはずだ」と、VDIにおけるメリットを強調する。

福井氏は、vShield EndpointとDeep Securityの組み合わせによって、VDI環境に最適なウイルス対策が実現することを強調する。現在流布しているマルウェアは、万が一感染してしまった場合にはOSのレジストリを変更してしまうものが多く、PCのシステムを感染以前の状態に復元する必要がある。通常のクライアントPCではシステムの復元には失敗のリスクも伴うが、VDIならばマスターイメージを使って簡単にクリーンなシステム環境を復元することができる。もうひとつのメリットは、仮想デスクトップへのウイルス対策ソフトのインストール漏れのリスクが少なくなることだ。vShield EndpointとDeep Securityの場合、エージェントレスなので、新しいゲストOSが稼働を始めた場合も、仮想アプライアンスによって即座に最新のパターン・ファイルが適用されたセキュリティ環境を提供できる。

また、Deep Securityが仮想デスクトップの異変を検知した場合、セキュリティ管理者へのアラートとともに、vShield Endpointを通じて仮想化インフラへのアラートも発するため、インシデント発生時の組織的な対応も可能である。

100ユーザーを超える場合は要検討

国内企業におけるVDIの普及は、これからが本番となる。各務氏は、「VDI導入の際に最も注意すべきはウイルス対策をどのように設計するかにある」と訴える。

「ユーザー数がさほど多くない小規模のVDIであれば、各仮想デスクトップにエージェント型ウイルス対策ソフトをインストールして使用しても大きな問題はない。だが、仮想デスクトップの数が増えていくにつれ、ウイルス対策ソフトの負荷も正比例して増える。ユーザー数が数千人規模になれば、パターン・ファイルの更新やスケジュール・スキャンが深刻なリソース不足を引き起こす」（各務氏）

残念ながら、VDIのウイルス対策にまつわるこうした問題は、ユーザー企業はもちろんSIベンダーにおいても十分な理解を得られてない部分があるようだ。パフォーマンスの問題は本格的に導入してからでないと発覚しにくく、導入後にあわてて追加対策を考えるようなケースも少なくないという。

これからVDIを導入する場合でも、導入済みのVDIの規模を拡張する場合でも、仮想デスクトップが100台以上の規模になるのであれば、vShield Endpointを活用したエージェントレス型の対策は、エンド・ユーザーへのサービス・レベルを保証するうえで重要な選択肢となる。

VDIの導入において、社内のエンド・ユーザーが最も気にかけるのが必要なときに使えるサービスであるということだ。アンチウイルス処理による仮想デスクトップのパフォーマンス劣化は、業務生産性に直接影響を及ぼす。ユーザーも管理者もVDIの恩恵を最大限に享受できるような環境を作るために、ウイルス対策のアーキテクチャの選定と運用の設計については、必ずチェックしたいポイントである。