ITR White Paper

仮想デスクトップ時代のマルウェア対策

株式会社アイ・ティ・アール

C11070032

本書の目的および趣旨

本ホワイトペーパーは、トレンドマイクロ株式会社からの依頼に基づき、株式会社アイ・ティ・アールが、仮想デスクトップ環境におけるマルウェア対策ツールの特徴、パフォーマンスについて客観的に評価を行ったものである。

目 次

第１章　仮想デスクトップの進展とセキュリティ課題

クライアントPCの管理に頭を悩ませる国内企業は依然として少なくない。特に昨今は、端末そのものの管理はもとより、セキュリティ・リスクの極小化、モバイル端末の台頭への対応など、課題の中身も大きく変質しつつある。そうしたなかで期待を集めている技術が、「デスクトップ仮想化（VDI）」である。しかし、本来、セキュリティ課題を軽減するとされるデスクトップ仮想化を巡っては、新たなセキュリティ上の課題も浮上している。

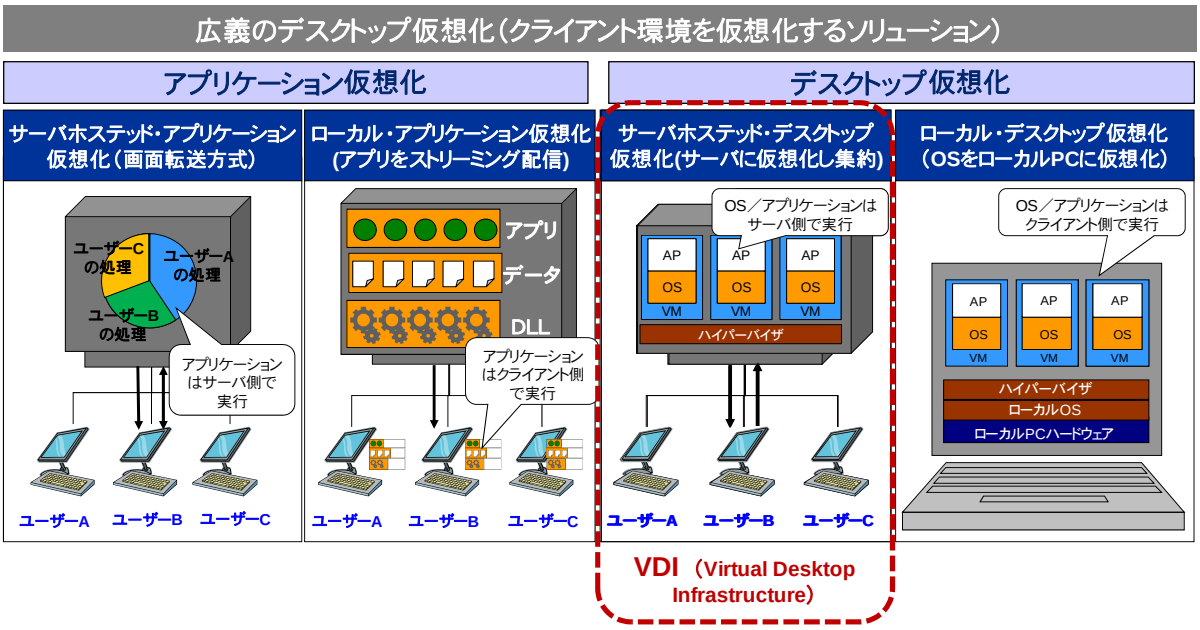
導入期を迎えつつあるVDI

企業のIT部門において「クライアントPCの管理」は、永遠の課題であると言って差し支えないテーマである。相変わらず引きも切らずに登場する新種のマルウェアへの対応、情報漏洩の防止、ソフトウェア・ライセンスの把握、さらにはOSのアップデートやパッチ管理――そうした作業に費やされるITスタッフの労力は増えこそすれ、一向に減る気配が見られない。また、管理を過度に強化すれば、業務の生産性に悪影響を及ぼすことも考えられる。社員の誰もが使うマシンであるがゆえに、その管理には絶えず細心の注意が求められるのである。とりわけ近年は、モバイルワークの普及や在宅勤務の増加などにより、安全性と生産性を両立させることに対するニーズはこれまで以上に高くなっている。

そうしたなかで、そうしたクライアントPCの管理を巡る課題を抜本的に解決するひとつの手段として注目されているのが「デスクトップ仮想化（VDI：Virtual Desktop Infrastructure）」である。これは、クライアント端末から仮想的に作成されたPC環境（Windows、LinuxなどのクライアントOS）にアクセスして、そのデスクトップ環境を利用する技術の総称であり、厳密な定義としては、図１に示すように大きく４つに分類される。ちなみに、今日において、VDIと呼ばれる製品は、概ね、仮想マシンのOSならびにアプリケーションをサーバ上で実行する「サーバホステッド・デスクトップ仮想化」を指すのが一般的である。

かつてはハイエンド・サーバが必須となるがゆえのコスト増やパフォーマンスの低下が指摘され、導入は一部の企業に限られていたが、ここにきてヴイエムウェア、シトリックスといった仮想化ツール・ベンダーが製品開発を強化したこと、ハードウェア価格が低下したこと、クライアント端末の多様化が進んだことなどによって、多くの企業が現実的な選択肢としてとらえるようになってきている。

図１．デスクトップ仮想化技術の分類



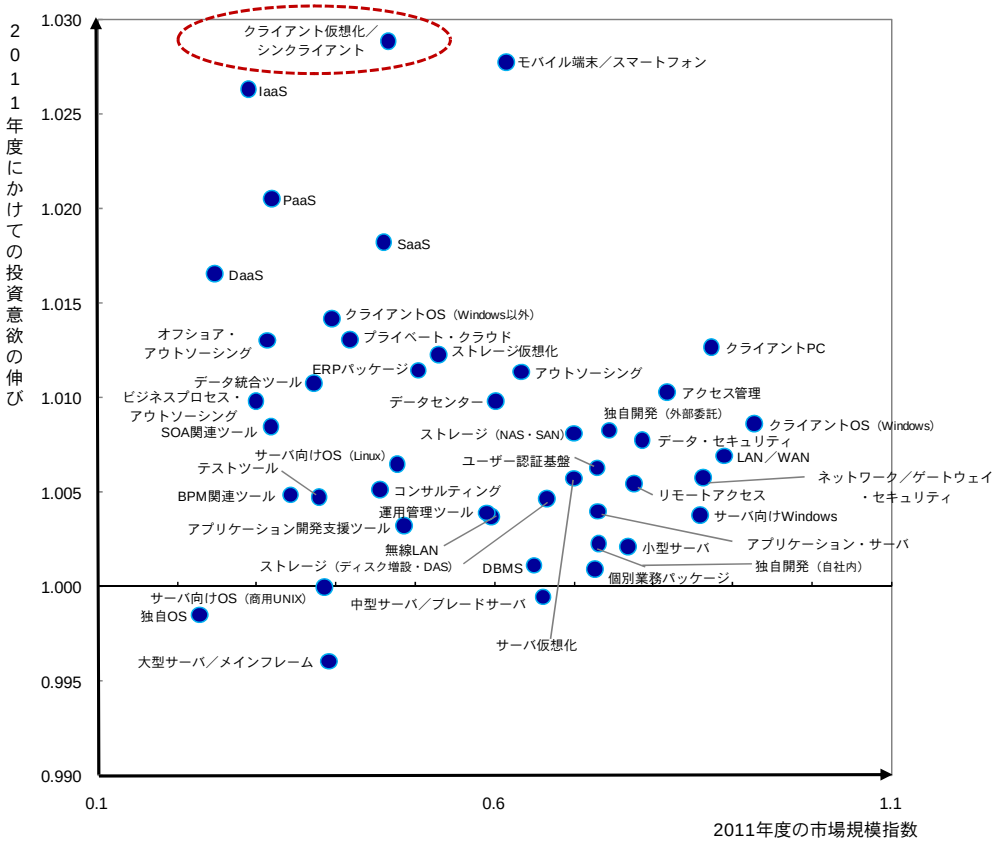
出典：ITR

ITRが2010年９月から10月にかけて実施した「IT投資動向調査2011」では、「クライアント仮想化／シンクライアント」という分類名で国内のユーザー企業に投資意欲を尋ねているが、同項目は、2010年度から2011年度にかけての投資意欲の伸び率が全45項目中トップとなった（図２）。

また、2011年2月にITRとITmediaリサーチインタラクティブが共同で行ったアンケート調査では、174社の有効回答のうち、「デスクトップ仮想化（VDI）を導入・利用している」とした企業の割合は、「アプリケーション仮想化と併用している」とした企業を併せると16％を占めた（図３）。また、「導入検討・評価段階である」とした企業の割合も23％にのぼっている。

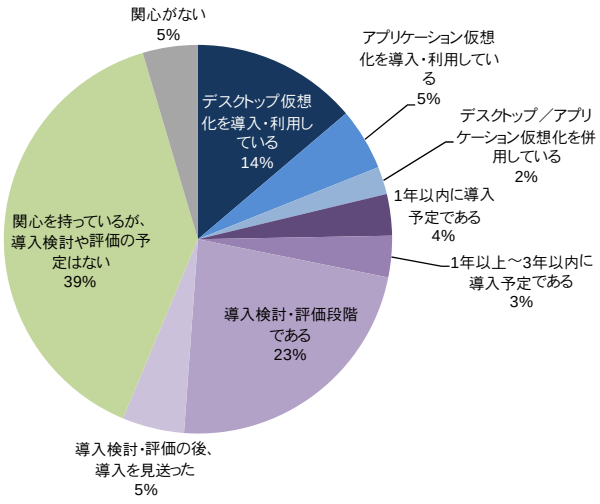
とりわけ、足下の2011年度においては、国内企業の間でWindows７環境への大がかりなアップグレードを検討する向きが多く、そのタイミングに合わせてVDIの導入を選択肢のひとつに加えるといった動きも見られている。

図２．製品／サービスにおける投資意欲



出典：ITR「IT投資動向調査2011」

図３．デスクトップ仮想化の導入状況（有効回答：174件）

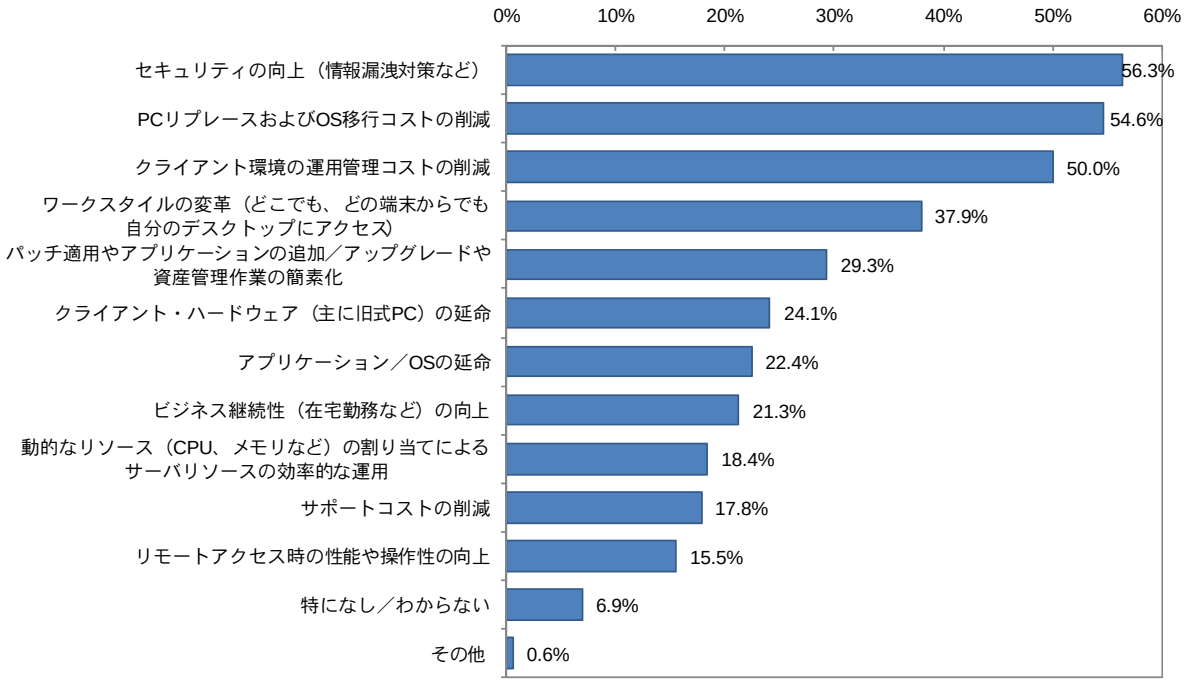


出典：ITR／ITmediaリサーチインタラクティブ（2011年2月調査）

ユーザー企業における VDI の価値

では、VDI環境の導入を検討する企業は、はたしてどのようなメリットを期待しているのであろうか。前節で紹介したユーザー・アンケートにおいて、VDIがもたらすメリットとして特に重視する事柄を尋ねたところ、「セキュリティの向上（情報漏洩対策など）」をあげる企業が56.3％と最も多く、次いで「PCリプレースおよびOS移行コストの削減」（54.6％）、「クライアント環境の運用管理コストの削減」（50.0％）の順で続いた（図４）。

図４．デスクトップ仮想化導入のメリット（最大５つ選択）



出典：ITR／ITmedia

この結果を見る限り、「セキュリティの強化」と「コスト（負荷）の削減」の２つのニーズを同時に満たす可能性があるという点に、VDIの魅力を感じている企業が多いことがわかる。また、上位３項目からはやや水をあけられているが、「ワークスタイルの変革（どこでも、どの端末からでも自分のデスクトップにアクセス）」が約38％で４位につけているのも、スマートフォンやタブレットなどクライアント端末の多様化が進む近年の市場の変化を受けてのニーズであろう。さらに、「ビジネス継続性（在宅勤務など）の向上」も、20％を超える企業が選択している。東日本大震災発生を受けた今日においては、このメリットを重視す

る企業がさらに増加しているものと予想される。

VDI 環境で浮上する新たなセキュリティ課題

前節でも確認したように、ユーザー企業にとって、VDI導入における最大のトリガーとなっているのは「セキュリティの向上」である。確かに、すべての作業をサーバ側で実行し、ローカルのクライアント端末にデータを保有する必要のないVDIは、「重要データの保護」という観点で極めて合理的なシステム環境である。しかし、クライアント環境に求められるセキュリティ対策は、決して情報漏洩対策だけではない。とりわけ、最も基本的なセキュリティ対策のひとつであり、企業ユーザーのほとんどが何らかのかたちですでに対策済みの課題――すなわち、ウイルス／ワーム／スパイウェアなどのマルウェア対策――は、デスクトップ環境がたとえ仮想化されたとしても欠かせないセキュリティ課題となる。そして実は、このマルウェア対策こそが、VDI環境における新たな課題として浮上してきているのである。

PCにおけるマルウェア対策は、マシン内部を常時スキャニングし、不正なプログラムを検知／駆除するというアプローチによって実現されている。インターネットが本格的に利用されるようになって以降、その脅威は減るどころかますます増加しており、手口も巧妙になってきている。

では、VDI環境に一般的なマルウェア対策製品を適用すると、はたしてどのようなことが起こるのであろうか。仮想マシン１台ごとにエージェントが常駐し、ファイルやデータのスキャニング、パターンファイルの更新といった動作が行われるために、ホストマシン（すなわち物理サーバ）のシステム・リソースが一時的に枯渇したり、ハイパーバイザ経由のネットワーク負荷が増大したりといった事態が生じやすい。これは一般に「AV（アンチウイルス）ストーム」と呼ばれる現象であり、VDI環境全体のパフォーマンスを低下させるだけでなく、場合によっては予期せぬシステムダウンを招くことにもつながる。今日では、仮想化技術の進展によって、１台の物理サーバ上に50台ないしはそれ以上の数の仮想マシンの統合が可能になってきているが、この統合率が向上すればするほど、AVストームの問題は深刻化する。企業によっては、実装段階になって初めてこの問題に直面し、結果的に仮想マシンの統合率を当初の計画よりもかなり低く設定せざるをえなくなるようなケースさえ見受けられる。

仮想マシンの統合率を落とせば、当然ながらその影響はコストに響くこととなる。つまり、セキュリティ・レベルを高めるために導入を決めたVDIが、セキュリティ製品の影響を受けて、そのコスト・メリットを大きく損なうという皮肉な結果が生じることにもなりかねないわけである。

したがって、VDI環境の導入を本格的に検討するうえでは、セキュリティ対策の基本とも言うべきマルウェア対策のアプローチをあらためて根本から見直すことが求められる。

第２章　VDI におけるマルウェア対策のアプローチ

今日、VDI環境を企業が採用するにあたって、マルウェア対策を実現する手段としては、大きく分けて3つのアプローチが考えられる。本章では、それぞれの手法の特徴について見ていくこととする。

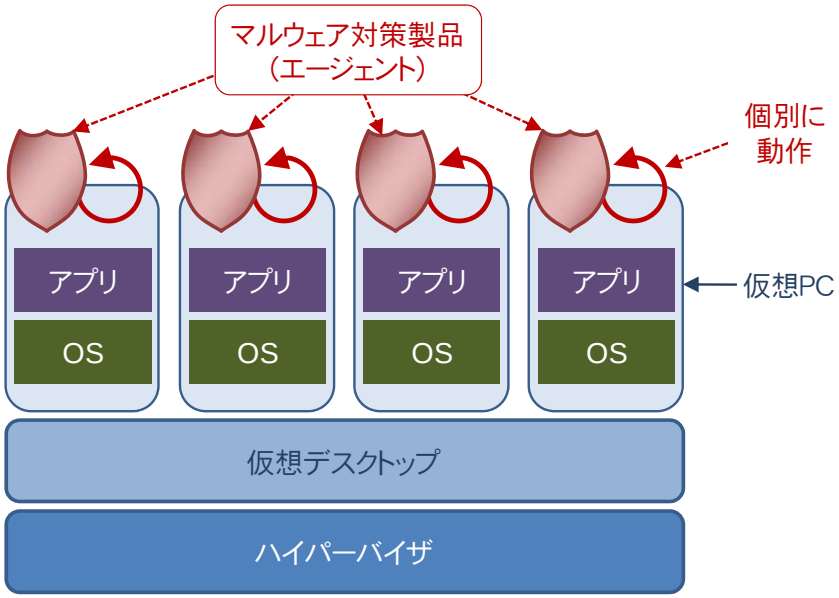
アプローチ①：従来型デスクトップ用製品の流用

VDIといえども、個々の仮想マシンの中身を見れば、OSとアプリケーションの組み合わせによって機能が提供されているという点では、通常のデスクトップPCと大きく変わるものではない。したがって、現在市販されているデスクトップ用のマルウェア対策製品の多くは、仮想マシン上のゲストOSにもインストールして動作させることが可能である。VDI環境の導入を検討するような規模の企業においては、すでに何らかのマルウェア対策製品が導入済みであると想定されるため、過去の投資の保護という観点からも本アプローチはおそらく最初に検討される選択肢となるであろう。

また、通常のデスクトップPC環境とVDI環境を併存させるような組織においては、同一のマルウェア対策製品を用いることによって、物理マシン、仮想マシンを問わずにマルウェア対策の一元管理が可能であるというメリットも享受できる。

しかしながら、このタイプの製品は、個々の仮想マシン上に物理マシンと同一のエージェントを導入することになるため、消費するリソースが大きいのが難点である。また、仮想マシンの台数が増えれば、前章で述べたAVストームの影響も受けやすい。したがって、導入に際しては、マルウェア対策製品自体の基本性能がシビアに問われることになろう。エージェントやパターンファイルのサイズやCPU、メモリ、ディスクに対する負荷の度合い、さらにはスキャン性能といった総合的な見地から製品評価を行うことが大前提となる。

図５．従来型マルウェア対策製品の利用イメージ



出典：ITR

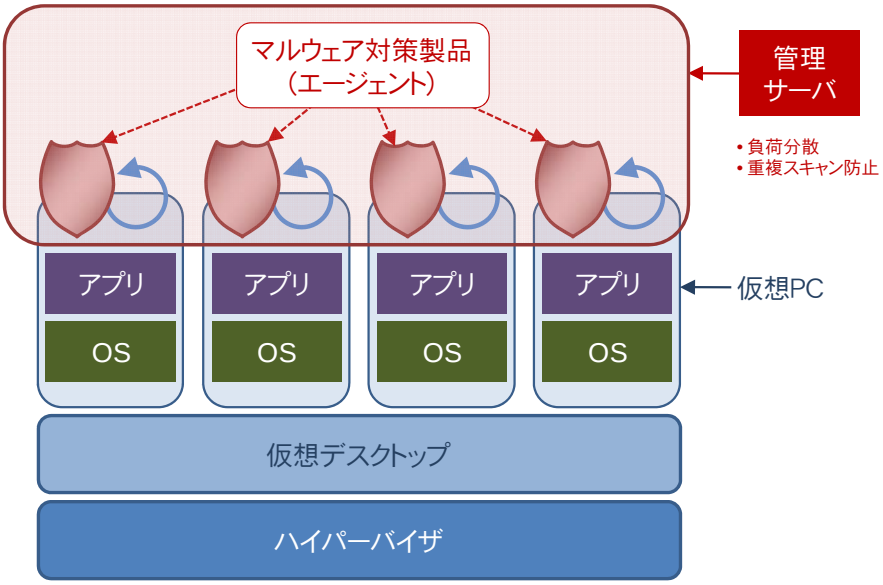
アプローチ②：VDI 最適化機能を備えるハイブリッド型製品の導入

２つ目のアプローチとしてあげられるのが、通常のデスクトップPC向けでありながら、VDI環境に最適化された管理機能やプラグインをもつハイブリッド型のマルウェア対策製品の導入である。各仮想マシンにエージェントが必要であることは①のアプローチと同様だが、管理機能によって個々のエージェントにかかる負荷を分散させたり、異なる仮想マシン間の重複スキャンを抑制したりといった最適化機能を提供する。

具体的な最適化機能としては、定期的に実行されるフルスキャンを時間差で実行することによって同時間帯に負荷が集中するのを防止するほか、仮想マシン間で共通に保有するデータやファイルを検索対象から除外することによってスキャン作業自体の処理を軽くするといったものがあげられる。

最新版のPC用マルウェア対策製品の一部では、このような最適化機能が標準で盛り込まれるようになっており、今後、VDI環境の普及が進むにつれて、この種の機能がより一般化することが予想される。

図６．VDI最適化機能をもつマルウェア対策製品の利用イメージ



出典：ITR

アプローチ③：オフロード型対策製品の導入

VDI環境の本格導入を検討しており、さらに最適化レベルが進んだマルウェア対策製品を望む企業にとって、今後重要な選択肢になると考えられるのが、仮想化環境専用に開発されたオフロード型のマルウェア対策製品の導入である。これは、仮想マシンのうちの１台をマルウェア対策専用のバーチャル・アプライアンスとして稼働させ、マルウェアの検出、パターンファイルの更新といった作業を集約して実行することを可能にするタイプの製品である。バーチャル・アプライアンスと他の仮想マシンとの間の通信は、仮想デスクトップ・プラットフォームが提供するAPI、もしくはTCP/IP経由で行うことになる。

セキュリティ・スキャン機能をバーチャル・アプライアンスに負わせることで、負荷を軽減（オフロード化）できることから、個々の仮想マシンのCPUやメモリの消費量を抑えることが可能になる。つまり、エージェント型製品で起こりがちなデスクトップ環境のパフォーマンス低下という問題を抑制することが可能になるわけである。

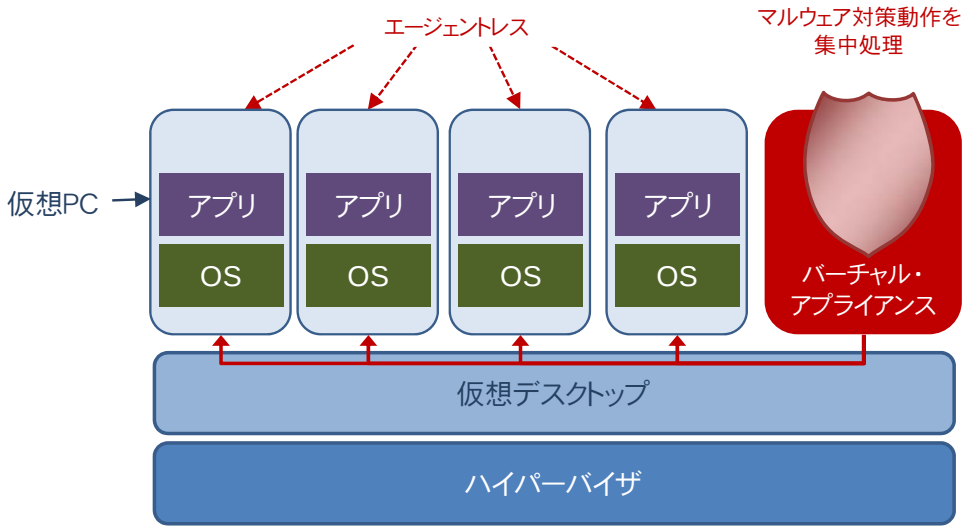
また、製品によっては個々の仮想マシンにエージェントを導入する必要がない（あるいは必要な場合でも軽量化が図られている）ことから、システム・リソー

スの節減にも貢献する。

そもそも仮想サーバ環境用に開発された製品をVDI環境に対応させている製品が多いため、最新のデスクトップPC向けマルウェア対策製品に搭載されるような、振る舞い検知、検出後のマルウェア駆除、感染後の自動復旧、Webセキュリティ、デバイス制御、といった高度な機能は備えていないという制限がある。しかし、VDIにおいては、障害発生後のロールバックが容易であったり、エンドユーザーの用途がそもそも限定されていたりというように、物理PC環境とは異なる運用モデルも想定される。そのため、VDIの導入目的や業務内容によってはこうした制限がさほど問題にならないケースも考えられる。

技術的には成熟途上ではあるが、VDI環境を効率的に保護するための技術として、今後はますます注目を集めることになると考えられる。

図７．オフロード型マルウェア対策製品の利用イメージ



出典：ITR

第 3 章　主要 VDI 対応製品の紹介

種類はまだ限られているが、ここ1年ほどの間に、国内市場でもVDI対応のマルウェア対策製品が相次いでリリースされている。本章では、その中で代表的な製品をいくつかピックアップして、その特徴を概説する。

エージェント・スキャン型

通常のデスクトップPC向けとして利用可能であり、かつVDI環境向けの最適化が図られたエージェント型の代表的な製品としては、以下の 2 製品があげられる。

トレンドマイクロ社「ウイルスバスター コーポレート・エディション 10.5」

トレンドマイクロ社の企業向けマルウェア対策製品のフラッグシップである同製品には、2010年8月に登場したバージョン10.5において、VDIプラグインが搭載され、VDI環境向けの最適化機能が他製品に先駆けて盛り込まれた。現在、搭載されている機能は以下の 2 つである。

- 負荷分散機能

予約スキャンやパターンファイルの更新などの動作において、同時に実行する仮想マシンの数を制限することによって、ホスト・マシン（物理マシン）全体の負荷を軽減する。

- 重複スキャン防止機能

すべての仮想マシンで共通するOSやアプリケーションのテンプレートを最初に検索し、正常と判断されたファイル／データについてはホワイトリストによって個々の仮想マシンの検索対象から除外する。トレンドマイクロ社では、同機能を実装していないバージョン10.0 SP1に比べ、ウイルス検索時間を約70%以上短縮することができるとしている。

シマンテック社「Symantec Endpoint Protection 12」

シマンテック社も、2011年7月に国内リリースとなった企業向けマルウェア対

策製品において初めてVDI最適化機能を搭載し、トレンドマイクロ社を追撃する構えを見せている。同製品に搭載されている機能は以下のとおりである。

- 負荷分散機能

予約スキャン時において、各仮想マシンのスキャン開始時刻をランダムにずらすことにより、負荷がホスト・サーバに集中することを防止する機能を搭載している。

- 重複スキャン防止機能

トレンドマイクロ社と同様、仮想マシンの複製元マスタ・イメージからスキャン済みファイルのホワイトリストを作成し、複製後の仮想マシンではこれらを検索対象から除外することで負荷を軽減する。また、Shared Insight Cache機能により、特定の仮想マシン上にあるファイルがクリーンだと判定された場合、他の仮想マシン上の同一ファイルを検索対象から除外することも可能である。

- オフラインの仮想マシン・イメージの検索機能

VMwareのディスクイメージであるvmdkファイルについては、オフライン時でもスキャンを行うことが可能であるとしている。

オフロード・スキャン型

仮想環境に特化して開発され、VDI環境においてオフロード型のマルウェア対策を行える製品としては、以下の２製品があげられる。

トレンドマイクロ社「Trend Micro Deep Security 7.5」

IDS／IPS、ファイアウォール、ログ監視、ファイル・レジストリ変更監視、マルウェア対策という業務サーバに必要な保護機能を盛り込んだホスト型のセキュリティ製品。物理サーバの保護も可能であるが、昨今は主に仮想サーバ向けのセキュリティ製品として注目度が高まっている。

当然ながらVDI環境にも対応しており、ホスト・サーバ内のバーチャル・アプライアンスから、各仮想マシンのマルウェア検索をオフロードで実行することが

できる。また、ヴイエムウェア社が開発した仮想マシン用のエンドポイント保護ツールである「vShield Endpoint」にいち早く対応しているのが大きな特徴で、VMware View環境（あるいは、ホスト側のハイパーバイザがVMware ESX 4.1以降）であれば、独自のエージェントを利用することなくマルウェア対策機能を実行することが可能である。同じくヴイエムウェア社から提供されている仮想マシン管理ツール「vSphere Server」ないし「vSphere Client」による統合管理もサポートしている。

マカフィー社「McAfee MOVE for Anti-Virus for Virtual Desktops」

2010年10月にリリースされた、仮想化環境専用のマルウェア対策製品。VDI用の「for Virtual Desktops」と、仮想サーバ用の「for Virtual Servers」の２つの製品ラインをもつ。

VDI環境では、前述のDeep Security同様、バーチャル・アプライアンスによるオフロード型のマルウェア検索に対応しており、ホスト・サーバの負荷を抑えることができる。ただし、IDS／IPSやファイアウォールなどのコンポーネントはもっておらず、マルウェア対策により特化した構成となっている。

また、VMware環境に傾注しているDeep Securityとは異なり、ホスト側のハイパーバイザに関わらず同等の機能を提供できるが、その反面、独自のエージェントを各仮想マシンに導入すること、仮想マシンとバーチャル・アプライアンスとの通信にTCP/IP接続が必要といった制限も存在する。

第４章　パフォーマンス・テスト結果

では、ここまで述べてきたような、マルウェア対策ソフトウェアのアーキテクチャの違いが、VDI環境のパフォーマンスにどのような影響を及ぼすのであろうか。そこで、仮想マシン数50～100台のVDI環境を構築し、マルウェア対策ソフトウェアをインストールして、パフォーマンスの計測を行った。本章はその結果についてまとめる。

テスト環境

テストで利用したマルウェア対策ソフトウェア

今回のパフォーマンス・テストで利用したマルウェア対策ソフトウェアは、トレンドマイクロ社から提供されている以下の３製品である。

- ウイルスバスター コーポレートエディション 10.0（以下、VB Corp 10.0）
  - VDI最適化機能をもたない一般的なPC用マルウェア対策製品のサンプルとして採用
- ウイルスバスター コーポレートエディション 10.5（以下、VB Corp 10.5）
  - PC用マルウェア対策製品でありながら、VDI環境向けの最適化機能を有する製品のサンプルとして採用
- Trend Micro Deep Security 7.5（以下、DS 7.5）
  - オフロード型のマルウェア検索に対応したVDI専用のマルウェア対策製品のサンプルとして採用

仮想環境全体の構成

仮想デスクトップ環境については、ヴイエムウェア社の製品群を利用することとし、仮想化プラットフォームとして「VMware vSphere 4.1（ESX 4.1、vCenter Server 4.1）」、VDIツールとして「VMware View 4.5」を採用した。

なお、VDI環境の構築のために使用した各ソフトウェアの名称と役割は次のとおりである。

- View Connection Server
  - VMware Viewのクライアントと仮想デスクトップ間の接続を管理するソフトウェア
- View Administrator
  - VMware Viewの管理コンソール
- View Manager
  - VMware Viewの中核的な管理ソフトウェア
- View Composer
  - VMware Viewにおいて、１つの仮想デスクトップをマスタ・イメージとして、複数の仮想デスクトップを複製して展開するためのソフトウェア
- vCenter Server
  - VMware vSphereの仮想環境を管理するためのプラットフォーム・ソフトウェア。本テストのパフォーマンス計測にも利用
- ESX 4.1
  - VMware vSphereのハイパーバイザ
- Viewエージェント
  - VMware View管理下のデスクトップにインストールされるエージェント・プログラム
- vSphere Client
  - VMware vSphereの管理コンソール
- View Client
  - VMware View管理下のデスクトップを利用するためのクライアント・マシン
- ADドメイン・コントローラ
  - ユーザー／コンピュータの認証や名前解決などに利用

マルウェア対策製品を導入する前の段階のシステム構成ならびに使用ハードウェアについては、図８に示したシステム構成図、ならびに図９に示したハードウェア構成情報を参照されたい。

図８．テスト環境のシステム構成図

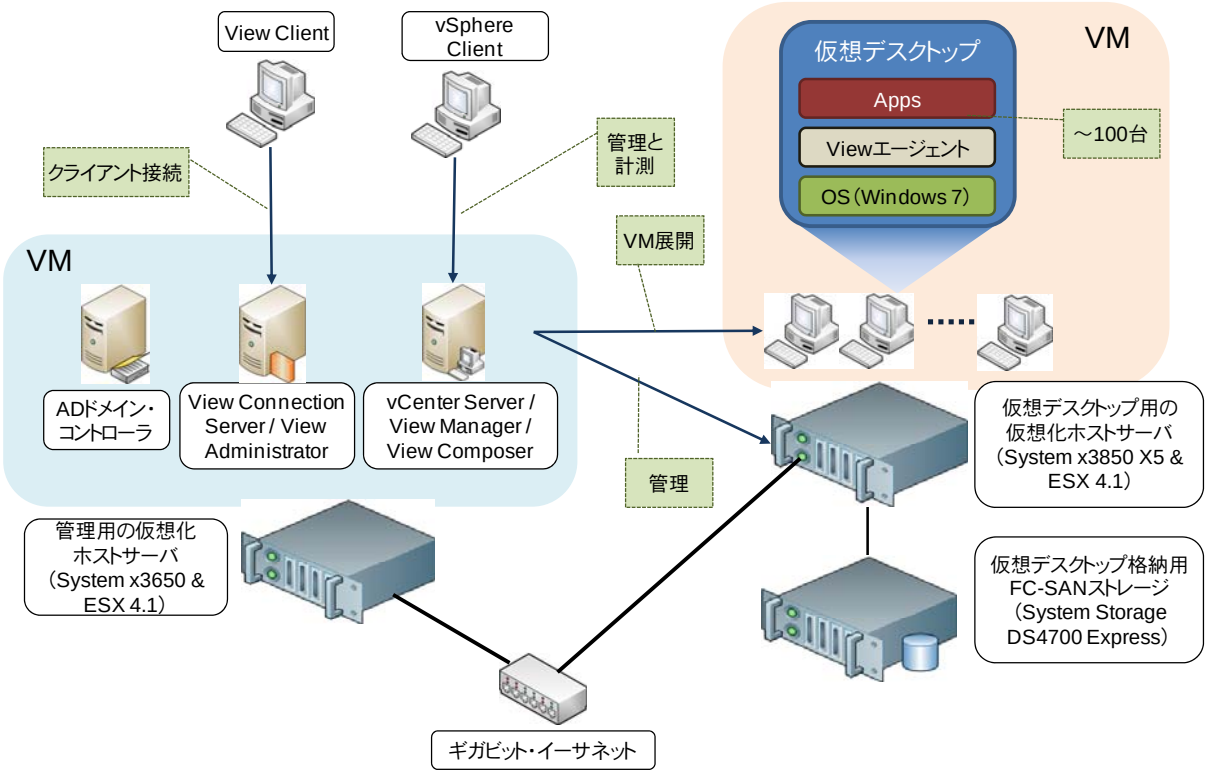


図９．ハードウェア構成

● VDI用ホスト・サーバ

製品名	System x3850 X5
プロセッサ	Xeon X7560（8コア／2.66GHz）×4基
メインメモリ	256GB
ストレージ	FC-SANストレージ（System Storage DS4700 Express） ［SAS HDD 300GB×4台／RAID10］×4セット
ネットワーク	ギガビット・イーサネット
仮想化ソフトウェア	VMware ESX 4.1

● 管理用ホスト・サーバ

製品名	日本IBM System x3650
プロセッサ	Xeon E5430（4コア／2.66GHz）×2基
メインメモリ	16GB
ストレージ	内蔵SAS HDD 146GB×6台／RAID-5
ネットワーク	ギガビット・イーサネット
仮想化ソフトウェア	VMware ESX 4.1

● Active Directoryホスト・サーバ（仮想マシン）

役割	ドメインコントローラ、DNSサーバ
仮想プロセッサ数	1基
メインメモリ	1GB
仮想ハードディスク	20GB
OS	Windows Server 2008

● VMware管理サーバ（仮想マシン）

製品名	VMware vCenter Server 4.1
	VMware View Manager 4.5
	VMware View Composer 4.5
仮想プロセッサ数	1基
メインメモリ	2GB
仮想ハードディスク	20GB
OS	Windows Server 2008

● VMware View Connection Server（仮想マシン）

製品名	VMware View Connection Server 4.5
	VMware View Administrator 4.5
仮想プロセッサ数	1基
メインメモリ	1GB
仮想ハードディスク	10GB
OS	Windows Server 2003

デスクトップ環境の構成

各仮想マシンによって実行されるデスクトップ環境の構築にあたっては、VMware Viewのリンク・クローン機能を利用して、ベースのOSと主要アプリケーションをインストールしたマスタ・イメージから、複数の仮想デスクトップを複製・展開する手法をとった。またユーザー・プロファイルは、ユーザーごとに固有のものを保持できるようにし、ユーザーが変更したデスクトップの設定をログオフ後も維持するような設定を施した。デスクトップ環境の構成は、図10のとおりである。

図10. 想定したデスクトップ環境

OS	Windows 7 Professional
テストに利用したアプリケーション	Office 2010
	Adobe Reader X
仮想デスクトップの複製方式	リンク・クローン（単一のマスタ・イメージから複数の仮想デスクトップを複製）
ユーザー・プロファイル	ユーザーごとに保持可能
仮想プロセッサ数	1基
メインメモリ	2GB
仮想ハードディスク	40GB

マルウェア対策ソフトウェアの稼働／管理のために使用したシステム環境

なお、テスト対象としたマルウェア対策ソフトウェアを動作させるうえでは、上記の共通環境に加えて、管理サーバやバーチャル・アプライアンスの構築が必要となる。それら、マルウェア対策ソフトウェアに固有で必要となったシステム環境の概要は、以下のとおりである。

VB 10.0／10.5については、基本的に管理サーバを１台追加するだけであるが、DS 7.5については、DSそのものの管理サーバに加えて、ヴイエムウェア社のvShield Endpoint用管理サーバが必要となる。さらに、VDIのホスト・サーバ上

に、マルウェア・スキャンを実行する仮想アプライアンスを構築する必要がある。この仮想アプライアンスには、仮想PC50台の環境では２基の仮想CPU、同75台／100台の環境では４基の仮想CPUをそれぞれ割り当てた。

図11. ウイルスバスター コーポレートエディション（10.0／10.5）管理サーバの概要

仮想プロセッサ数	１基
メインメモリ	2GB
仮想ハードディスク	20GB
OS	Windows Server 2008

図12. Deep Security 7.5で使用したシステム環境

● Deep Security Manager 7.5 (DS 用の管理ソフト)

仮想プロセッサ数	１基
メインメモリ	2GB
仮想ハードディスク	20GB
OS	Windows Server 2008

● vShield Manager (vShield Endpoint の管理ソフト)

仮想プロセッサ数	１基
メインメモリ	1GB
仮想ハードディスク	20GB
OS	—

● Deep Security Virtual Appliance（仮想アプライアンス）

仮想プロセッサ数	仮想PC 50台時＝２基 仮想PC 75台／100台時＝４基
メインメモリ	2GB
仮想ハードディスク	20GB
OS	Ubuntu Linux

デスクトップ利用時の負荷の想定

本テストでは、実際の稼働環境に近い状態でのパフォーマンスを測定するために、人為的にアプリケーション実行による負荷を与えることとした。エンドユーザーが実際にデスクトップ環境でアプリケーションを操作しているかのように、一定の手順で複数のアプリケーションを自動実行させ、マルウェア対策が導入されていない状態でも、仮想CPUやメモリ、ディスクといったリソースが一定量消費されるようにした。

負荷をかけるうえで、利用したアプリケーションは次のとおりである。

- Microsoft Word 2010
- Microsoft Excel 2010
- Adobe Reader X

各アプリケーションは上記の順番で１つずつ起動して自動実行させることとし、これを１ループとしてパフォーマンス・テストの最中に繰り返し実行した。自動実行の内容の詳細について以下に記す。

- Word 2010による負荷
  - VBAを利用してWord文書に対する操作を自動実行した。具体的には、複数の画像を含むWord文書を開き、文字列の置換やテキストのコピー＆ペースト、画像のコピーと挿入、編集した文書の保存などを行っている。各操作の合間には数秒のウェイトを設けることで、人間と同程度の速さで操作されるように仕向けた。Word文書のサイズは、最初は1MBだが、編集中には15MBまで増加することとした。
- Excel 2010による負荷
  - Word 2010の場合と同様に、VBAを利用してExcelブックに対する操作を自動実行した。具体的には、複数のシートを含むExcelブックを開き、表全体を見渡すためのスクロールや表のコピー＆ペーストを複数のシートに対して実行しつつ、編集したExcelブックを保存している。各操作の合間には数秒のウェイトを設けることで、人間と同程度の速さで操作されるように仕向けた。
- Adobe Reader Xによる負荷
  - UWSCという自動化ツールを利用して、Adobe Reader XによるPDF文書の各種閲覧操作を自動実行した。具体的には、画像を含む17MB程度のPDF文書を開き、いくつかのページへのジャンプや文字列の検索、ズームイン／ズームアウトなどを実行している。各操作の合間には数秒のウェイトを設けることで、人間と同程度の速さで操作されるように仕向けた。

パフォーマンス・テストの手順と測定項目

本テストでは、仮想デスクトップにインストールされたマルウェア対策ソフト

ウェアの常駐監視（リアルタイム・スキャン）機能によって、仮想化ホスト・サーバにどの程度の負荷がかかるかを、CPU使用率を指標に確認することとした。仮想マシンの台数は50台、75台、100台の３パターンを設定した。具体的な測定手順は以下のとおりである。

1. テスト対象のマルウェア対策ソフトウェアを組み込んだ仮想マシンを、VMware Viewのリンク・クローン機能を使用して100台複製する。
2. あらかじめ各仮想マシンを起動した後に、自動でログオンして負荷プログラムが起動するように設定する。
3. 各仮想マシンを約20秒間隔で１台ずつ起動する。間隔を空けている理由は、仮想マシン起動時の高い負荷がVMware ESXiホスト・サーバに集中するのを防ぐためである。
4. 50台の仮想マシンを起動したら、負荷プログラムのループが３周するのを待つ（約30分～40分）。
5. VMware vCenter Serverのパフォーマンス・チャートにて、VMware ESXiホスト・サーバにおけるCPU占有率データをそれぞれ保存する。
6. 各仮想マシンを終了させる。
7. 全仮想マシンの起動完了直後から負荷ループ２周分の測定値の平均を算出してグラフ化する。
8. 仮想マシンの起動台数を75台、100台と順次増やして、3～7を繰り返す。
9. 別のウイルス対策ソフトウェアを組み込んだ仮想マシンを新たに用意し、1～8を繰り返す。

テスト結果

CPU 使用率の遷移

今回のテストでは、リアルタイム・スキャン（常駐スキャン）中のCPU使用率に焦点を当てて、３つのマルウェア対策ソフトウェアのパフォーマンス比較を行った。リアルタイム・スキャンとは、ファイルを開くたびにその安全性のチェックを行う仕組みであるため、日常業務の生産性に影響を及ぼしやすく、エンドユーザーがパフォーマンス・レベルを体感しやすい。当然ながら、マルウェア対策ソフトウェアのCPU使用率はできる限り低くとどめることが望ましいということになる。

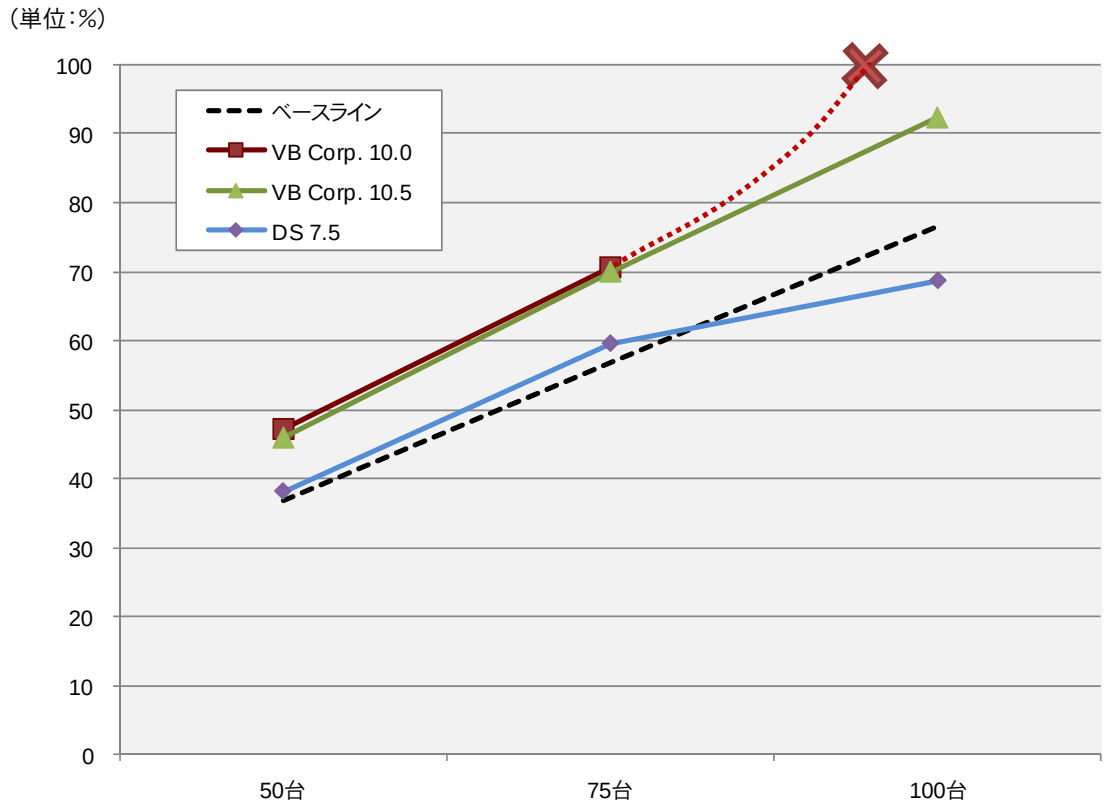
測定結果によると、エージェント型であるVB Corpについては、10.0、10.5とも、マルウェア対策ソフトウェアを導入していないベースラインよりも、CPUの負荷が常時20～25％程度上回るとの傾向が示された。とりわけ、仮想PC100台の環境では、CPUの使用率が極限に達しており、VB Corp 10.5では92.3％で辛うじて稼働を継続できたものの、同10.0では、一部の仮想PCがダウンしたり、負荷プログラムがエラーで実行不能となったりといった明らかな限界が示された。ちなみにこの数値は、メモリ容量、ディスク転送量については、それぞれ十分な余裕が残されていた状態で計測したものである。

一方、DS 7.5では、スキャニング作業を仮想PCとは別の仮想アプライアンスによってオフロード処理していることから、ホスト・マシンへの影響が最小限に抑えられていることがわかる。仮想PC50台、同75台の環境ではベースラインに対するCPU使用率の上昇は５％程度にとどまっており、同100台では、ベースラインをむしろ下回る使用率となった（図13、図14）。

図13.　マルウェア対策ソフトウェアごとのCPU使用率

	仮想PC 50台	仮想PC 75台	仮想PC 100台
マルウェア対策ソフトなし（ベースライン）	36.9%	56.7%	76.5%
VB Corp. 10.0	47.1%	70.5%	計測不能
VB Corp. 10.5	45.8%	69.9%	92.3%
DS 7.5	38.2%	59.6%	68.8%

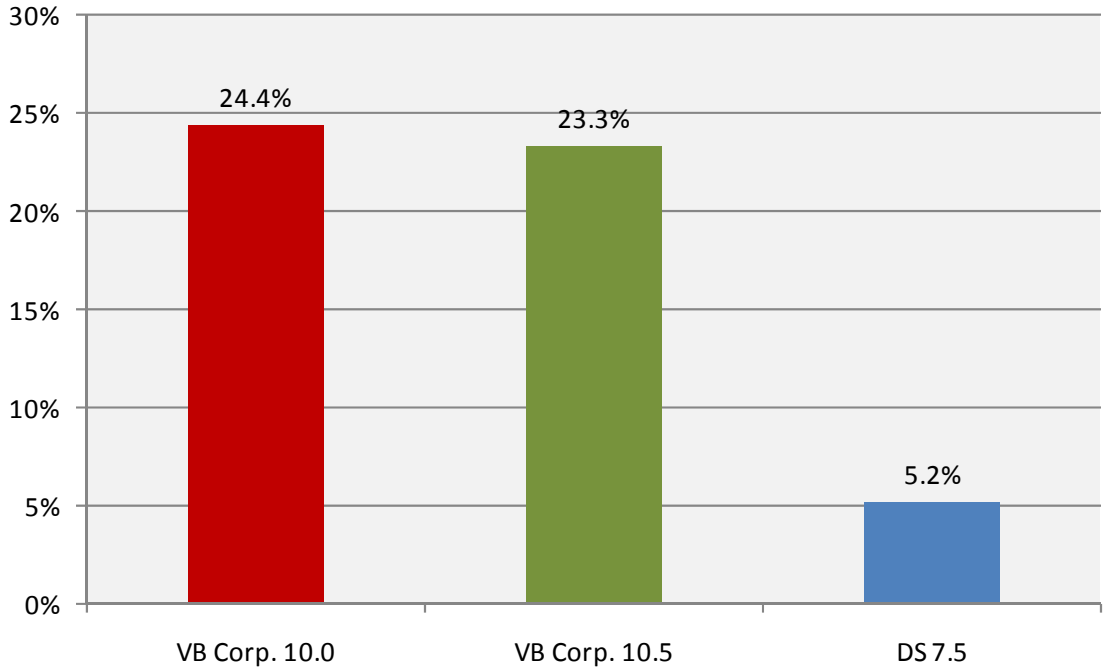
図14.　マルウェア対策ソフトウェアごとのCPU使用率



なお、仮想PC100台環境において、DS 7.5のCPU使用率がベースラインを下回っているが、これは、DSが使用する仮想アプライアンス側の性能のボトルネックによるものと考えられる。今回のテストでは、仮想アプライアンスの構築段階において、仮想PC50台環境では２基、同75台／100台環境では４基の仮想CPUを割り当てたが、仮想PC100台という超高密度環境になると、上記の割り当てでは不十分である可能性が高い。すべての仮想PCのマルウェア対策を一手に担うDSの仮想アプライアンスのリソース割り当てには、事前の入念なテストと検証が不可欠であるといえる。

ちなみに、すべてのマルウェア対策ソフトウェアが問題なく動作した仮想PC75台の環境において、各ソフトウェアによるホスト・マシンへの負荷増大分を表したのが図15である。このグラフからも、リアルタイム・スキャン時におけるDS 7.5のCPU負荷の小ささがはっきりとうかがえる。

図15. CPU使用率（仮想マシン75台における各製品の対ベースライン比率）



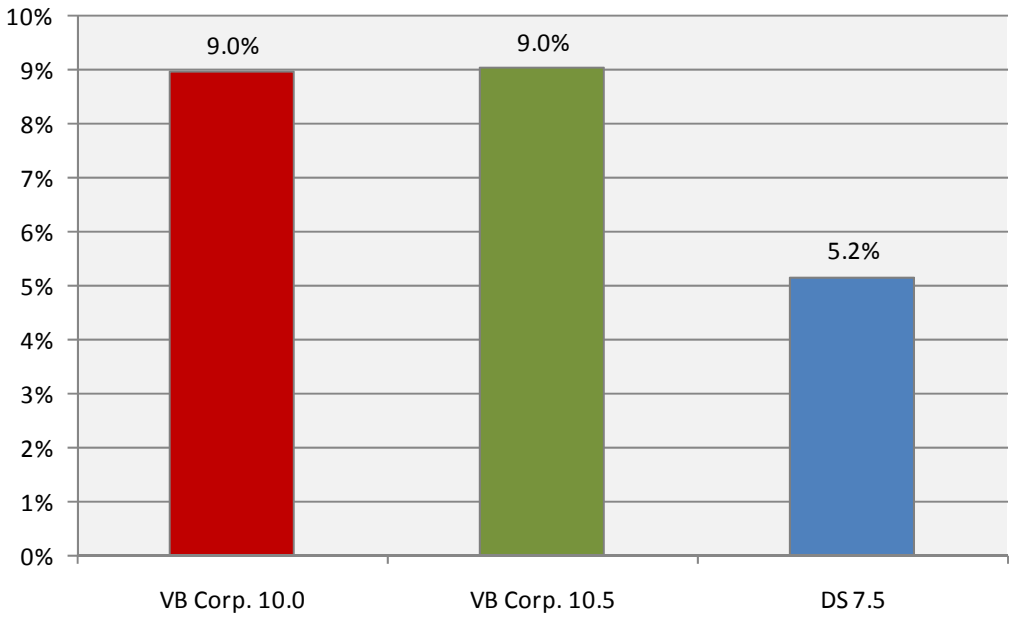
仮想 PC の作業速度

では、各仮想PC上で実際に行われる作業速度への影響はどうであろうか。本テストでは、前述のとおり、Word、Excel、PDFファイルを用いた操作をあらかじめ自動化して負荷として設定している。その一連の作業が完了するまでに要した時間についても、併せて測定した。

こちらについても、すべてのマルウェア対策ソフトウェアが問題なく動作した仮想PC75台の環境において、各ソフトウェアによるホスト・マシンへの負荷増大分を見てみたところ、エージェント型のVB 10.0／10.5はいずれも9.0%、オフロード型のDS 7.5は5.2%、それぞれベースラインよりも余分に時間を費やしていることが確認できた（図16）。ファイル操作に伴って動作するリアルタイム・スキャ

ンの場合、その仕組み上、作業速度が犠牲になることは避けられないが、ここでも、オフロード型スキャンを実行するDS 7.5の優位性が確認できる。

図16. 負荷ループ所要時間（仮想マシン75台における各製品の対ベースライン比率）



第５章　所見とまとめ

●実証されたオフロード型マルウェア対策ソフトウェアの優位性

企業ユーザーにおけるクライアントPC戦略のなかで、VDI環境が現実的な選択肢として浮上しつつあることは、本レポートの冒頭で述べたとおりである。しかしながら、今日のクライアントPCには、リスクを回避するためのさまざまなツールが組み込まれており、なかでも、当たり前のようにインストールされているマルウェア対策ソフトウェアの存在は無視できるものではない。

本レポートでは、企業における今後のマルウェア対策ソフトウェアの選定の一助とすべく、主要製品の仮想化対応の実情やアーキテクチャ上の特徴をまとめるとともに、VDI環境を実際に構築し、異なるタイプのマルウェア対策ソフトウェアがパフォーマンスにどのような影響を与えるかについてテストを試みた。テスト自体は、リアルタイム・スキャン時のCPU使用率という限定的な内容にとどまったものの、その結果だけを見ても、仮想化環境用に特化して開発されたオフロード型のマルウェア対策ソフトウェアの明らかな優位性が確認できた。CPUの使用率、作業時間のいずれにおいてもベースラインからの上昇率が１ケタ台にとどまったことは、ピーク・サイジングを見極めるうえで重要な指針となるであろう。仮想PCの統合率を追い求めつつ、かつ生産性の犠牲を最小限に抑えたかたちでVDI環境の構築を目指す企業においては、オフロード型のマルウェア対策ソフトウェアを最優先で評価すべきであると考える。

ただし、このタイプの製品において注意が必要なのは、マルウェア対策のオフロード処理を担う仮想アプライアンスに対するリソース配分である。特に、仮想PCの台数が大規模な環境においては、処理が集中する仮想アプライアンスに十分なリソースを割り当てることが求められる。

●エージェント型マルウェア対策ソフトウェアの利用に際しては、余裕をもったサイジングが不可欠

一方、今日、一般的に導入されているエージェント型のマルウェア対策ソフトウェアは、VDI環境上で稼働させた場合、CPU使用率の上昇分が20％を超えるとの結果が示された。また、統合率を高めた環境においては、CPUリソースの不足

によって一部の仮想PCが予期せずダウンしたり、エラーによって作業継続が不可能になったりと、深刻な問題が引き起こされることも確認された。以上のことから、このタイプのマルウェア対策ソフトウェアをVDI環境に導入する際には、ホスト・サーバ全体のCPU使用率のピークに余裕をもたせることが大前提となろう。個々の企業で想定される仮想PCの負荷にも依存するため一概に断言はできないが、今回のテスト結果に基づけば、ベースラインのCPU使用率を少なくとも70%以下に抑えたサイジングを行うことが、現実的なラインになると考えられる。

とはいえ、エージェント型のマルウェア対策ソフトウェアが、すべてのVDI環境に適さないかといえば、決してそうではない。今回実施したテストでも、VB Corp. 10.5については、仮想PC100台の環境での動作が確認されており、作業速度の低下も許容範囲にとどまることが示された。エージェント型製品では、ファイル以外のレジストリやメモリの防御が可能であるなど、オフロード型製品にはない機能面での優位性がある。また、物理PCの置き換えとしてVDI環境を導入するようなケースでは、過去に行った投資を保護しやすいという観点から、エージェント型製品を採用したほうがコスト面で有利となるケースも考えられよう。したがって、CPU使用率に余裕のあるサイジングが可能であるならば、エージェント型のマルウェア対策ソフトウェアも、評価の候補に加えることが推奨される。

その際に問われるのは、今回のテスト項目には含まれていないが、AVストームがより深刻にパフォーマンスに影響すると想定されるフルスキャン時のパフォーマンスである。したがって、そうしたフルスキャン時の問題を回避することを目的としたVDI最適化機能の有無は、今後欠かせない評価ポイントのひとつになると考える。

●クライアント環境の転換期にあらためて問われる、セキュリティ製品の柔軟性

本レポートではマルウェア対策に絞って調査と検証を行ったが、クライアントPCに求められるセキュリティ要件はそれだけではない。各端末にデータを保有しないVDIは、確かに情報の保全性やPC環境の管理性を向上させるといった効果をもたらすが、それでも従業員個人に利用させるデスクトップ環境である以上、OS／アプリケーションの脆弱性対策やネットワークを介した情報漏洩の防止など、対応すべき課題はいくつも存在する。今後は、マルウェア対策以外の分野でも“VDI対応”が重要なキーワードになっていくであろう。その際に、物理マシンの世界ではあまり問題にならなかったパフォーマンス上の課題が大きくクローズアップされる可能性も否定できない。

ユーザー企業の情報セキュリティ責任者は、保護すべき対象であるクライアントPCの環境が大きな転換期を迎えていることを理解したうえで、今後のセキュリティ製品の選定に臨むべきであろう。特に、将来的にVDI環境の導入を検討する可能性がある企業においては、仮想化技術への現在の対応状況、ならびにベンダー各社のロードマップを入念に評価することが不可欠であると考える。

執筆・分析: 舘野 真人
text by Masato Tateno

ITR White Paper

仮想化デスクトップ時代のマルウェア対策

C11070032

発行　2011年7月20日

発行者 株式会社アイ・ティ・アール

〒160-0023
東京都新宿区西新宿3-8-3
新都心丸善ビル ３Ｆ
TEL：03-5304-1301（代）
FAX：03-5304-1320