TEST REPORT

Tolly.

#211101
2011年2月
Trend Micro社からの委託

McAfeeおよびSymantecと比較したTrend Micro Deep Security 7.5の評価

VMware ESX仮想環境におけるアンチウィルス パフォーマンス

評価結果の概要

設備投資や運用コストの削減を目指すIT戦略において、サーバおよびデスクトップの仮想化は不可欠です。しかし仮想化技術が急速に普及する一方、物理サーバやデスクトップ システム向けのアンチウィルス ソリューションをそのまま仮想環境で使用する組織も少なくありません。これら従来のアンチウィルス ソリューションは必ずしも仮想環境が考慮されていないため、アンチウィルス（以下 AV）ストームやリソースの浪費、管理オーバーヘッドの増加など運用効率に大きな影響を及ぼしたり、仮想マシン（以下 VM）密度を最大限に高めようとする組織の目標を妨げる要因となります。

Tolly は、Trend Micro 社より同社の Trend Micro Deep Security ソリューションと McAfee 社の Total Protection for Endpoint および Symantec 社の Endpoint Protection 11.0 を比較するパフォーマンス評価を委託されました。本テストでは、特に VMware ESX 4.1 環境で一度に稼動するゲスト マシンが最大 100 台まで増えた場合、各ソリューションがホスト システム（物理サーバ）のリソースにどのような影響を与えるかを評価するものです。

テストのハイライト

Trend Micro Deep Security Virtual Applianceの評価

1. 従来のエージェント ベースのソリューションに対し、AV に負荷がかからない設定においても一貫してシステムCPUおよびメモリ、ディスクI/Oの使用率を抑制
2. 定期的なスキャンとパターン更新により、他のソリューションが終了できなかった VM 25 台以上のテスト環境で AV ストーム問題を回避
3. 負荷テストの実行中、McAfee および Symantec に比べて 29%～275% の VM 密度向上を実現

テストの結果、仮想環境向けに最適化された、エージェントレスの仮想アプライアンス ベースでアンチウィルスを提供するTrend Micro Deep Securityは、アンチウィルス エージェントがWindows 7を実行している各仮想マシン上でそれぞれ処理を行う、仮想環境非対応のソリューションに比べてCPUおよびRAM、ディスクのI/Oリソースの使用率が一貫して少ないことがわかりました。

一般負荷テストにおいて、従来の AV ソリューションは Trend Micro の 1.7～8.5 倍のリソース オーバーヘッドを消費するだけでなく、VM 25 台が一度に稼動するとアクティビティのピーク時（オンデマンド スキャンやシグネチャ更新の実行時など）に AV ストームが発生しました。特に従来のソリューションは VM 最終的に、Trend Micro Deep Security はリソース使用量を抑えることで仮想マシン密度 (ホスト 1 台あたりで実行可能な VM 台数を増やすなど) を高め、設備投資費 (CAPEX) と運用費 (OPEX) の削減を実現しました。リソース使用量を低く抑え、独自の負荷テスト環境で AV ストームを回避したTrend Microは、McAfee および Symantec のソリューションに比べて 29%（AV に負荷がかからない程度のタスク実行時）から最高 275%（AV ストームの発生時）まで VM 密度を向上させることに成功しました。Tolly エンジニアが即時に競合システムの修正を試みた場合でも、管理ステーションが 25 台の仮想マシンにオンデマンド スキャンまたはシグネチャ ファイルの更新をリクエストすると、すべてのマシンが一斉に稼動してCPUやメモリなどのホスト リソースに急激な負荷を与える結果となりました。

最終的に、Trend Micro Deep Securityはリソース使用量を抑えることで仮想マシン密度（ホスト1台あたりで実行可能なVM台数を増やすなど）を高め、設備投資費(CAPEX)と運用費(OPEX)の削減を実現しました。リソース使用量を低く抑え、独自の負荷テスト環境でAVストームを回避したTrend Microは、McAfeeおよびSymantecのソリューションに比べて29%（(AVに負荷がかからない程度のタスク実行時）から最高275%（AVストームの発生時）までVM密度を向上させることに成功しました。

今回、Tolly のエンジニアは最大 100 台の仮想マシンを同時稼動させるなど、あらゆる負荷状況においてセキュリティ システム リソースの使用量をテストしました。ベースライン値は、エンドポイントのセキュリティ ソリューションがインストールされていないシステム上でさまざまなエンド ユーザー機能の負荷シミュレーションを行い、計測されたリソース使用量を用いています。

本テストには、特定のアンチウィルス タスク（オンデマンド スキャンおよびシグニチャ更新）実行時のリソース使用量の評価、ならびにそれぞれアンチウィルスがインストールされた仮想マシン上での一般的なユーザー負荷テストが含まれます。

負荷シミュレーションにおけるアンチウィルスのリソース使用率（仮想マシン 25～100 台）

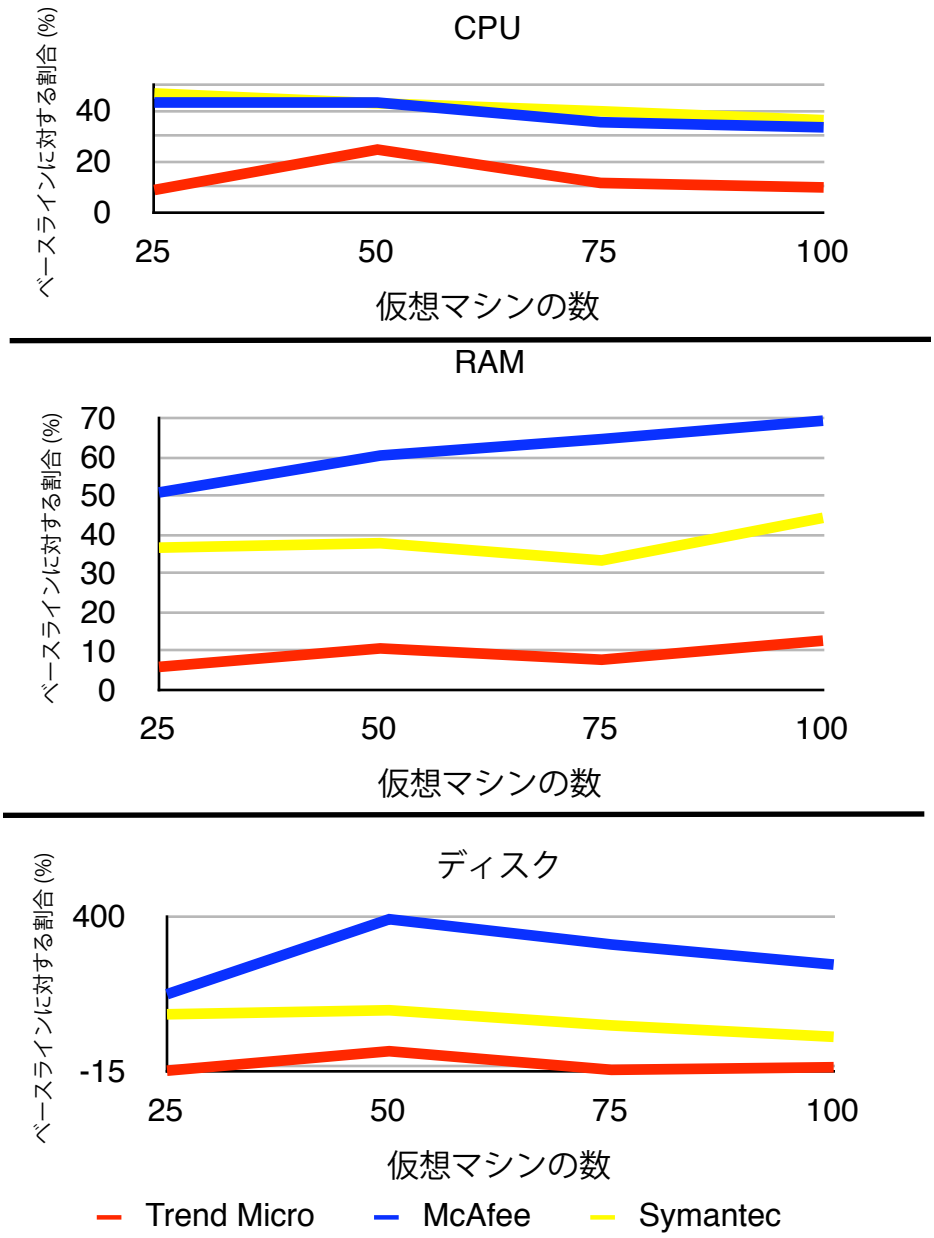
図 1 は、100 台までの仮想マシンを同時稼動したプライマリ テストでの VMware ESX サーバの主要システム リソースの平均使用率を示しています。（個別のデータ ポイントについては 表 4 を参照してください。）

これらの図には仮想マシン（Trend Micro のテストでは Deep Security 仮想アプライアンス）で使用するリソースが含まれます。テストの負荷レベルおよび環境に関する詳細は、「テスト方法とテスト用プラットフォームの設定」セクションを参照してください。

McAfee および Symantec のソリューションは、AV エージェントを実行するのに仮想マシンごとに個別のインスタンスを設定する必要がありますが、Trend Micro Deep Security は、ホスト 1 台につき 1 つの仮想アプライアンスのインスタンスだけで実行が可能です。右図は、すべての VM 密度レベルにおける 3 つのリソース（CPU、メモリ、ディスク）の使用率を示しています。Symantec および McAfee のリソース使用率は Trend Micro の 1.7～8.5 倍に上りました。[1]

アンチウィルス VMware ESX 4.1 のホスト リソース消費とベースラインの比較

独自設定の負荷を使用し、最大 100 台の VM を Microsoft Windows 7 で起動 vCenter によるレポート（数値が低いほうが良好）

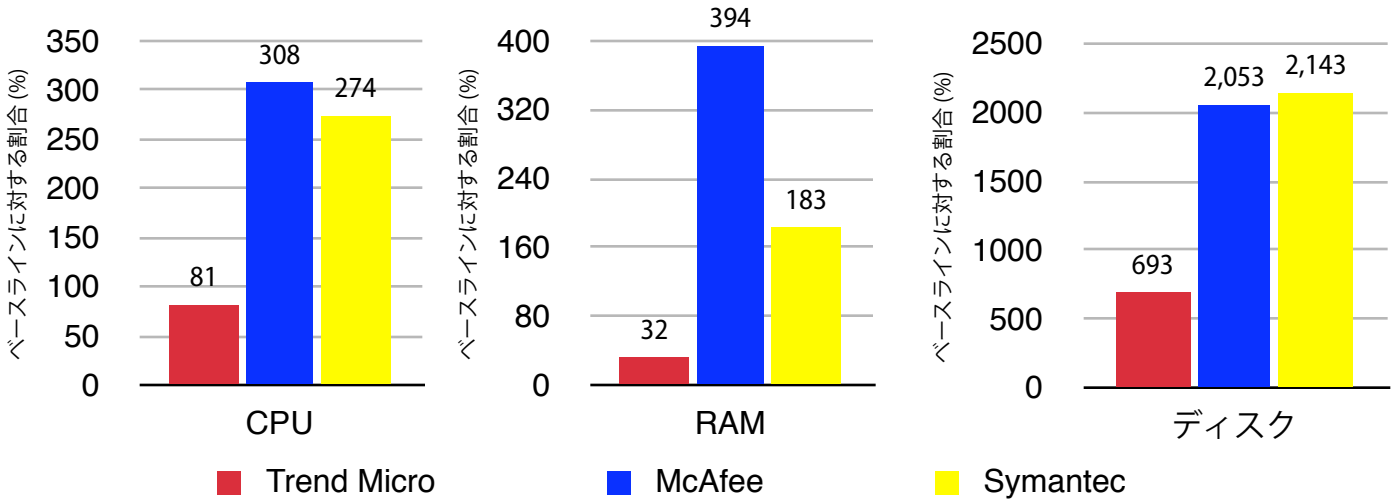


注意：すべてのシステムでスキャンに加え、独自設定の負荷テストを実行しています。ベースライン値は、インストール済みのエンドポイント セキュリティ ソリューションを実行せずに独自に設定した負荷テストを実施した結果です。ベースライン値および詳細な結果については、レポート本文を参照してください。ベースラインと比較した使用率は、結果からベースラインの値を引いた後、さらに同値で割った数字に 100 を掛けて算出されます。McAfee ソリューションは VM 100 台のテストを完了できなかったため、結果は 25、50、75 台のテストから推定した値を示しています。テストの実施時間は平均 30 分です。ディスク使用量の結果は、最大 30% の誤差があり、これは参照目的でのみご利用ください。

出典：Tolly、2010 年 10 月 図 1

[1] McAfee ソリューションは、複数回の試行および再テストの実施を試みましたが、VM 100 台のテストを完了できませんでした。よって McAfee の VM 100 台についての結果は、Tolly のエンジニアが VM 25 台、50 台、75 台の試験結果をもとに予想しました。

アンチウィルス 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
Microsoft Windows 7 を実行する 25 台の仮想マシンでのオンデマンド スキャン リクエスト
vCenter によるレポート（数値が低いほうが良好）



注意：すべてのシステムでスキャンに加え、独自設定の負荷テストを実行しています。ベースライン値は、インストール済みのエンドポイント セキュリティ ソリューションを実行せずに独自に設定した負荷テストを実施した結果です。ベースライン値は、それぞれ平均 CPU 使用率 ー 4,109.76 MHz、平均 RAM 使用率 ー 7,893.28 MB、平均ディスク使用率 ー 1,741.23 KBps とします。Trend は自動で 1 度に 1 つのスキャン タスクを実行しているのに対し、他のベンダーは 25 台すべてにおいて同時にスキャンを開始しています。各ベンダーはオンデマンド スキャンの負荷平準化にランダム化などの方法を推奨しています。詳細はレポート本文を参照してください。ベースラインと比較した使用率は、結果からベースラインの値を引いた後、さらに同値で割った数字に 100 を掛けて算出されます。テストの実施時間は平均 30 分です。

出典：Tolly、2010 年 10 月

図 2

アンチウィルス オンデマンド スキャン テスト（仮想マシン 25 台）

当社エンジニアは、セキュリティ管理システムから仮想マシン 25 台でのフルスキャンを実行するリクエスト受けた場合、各ソリューションがどのように反応するかを評価しました。複数台での同時スキャンは大量のリソースを消費することから、全体的なユーザー エクスペリエンスの質が低下する恐れがあります。

しかし Trend Micro Deep Security はリソースがすべてのマシンで共有されることを考慮しているため、スキャンを逐次処理（1 度に 1 台のみの実行）するよう自動的にスケジュールを行っています。その結果、Deep Security は 25 および 50 台でのテストも終了することができました。Tolly では、本テストのリソース使用率から、Trend Micro のソリューションは VM 100 台以上のシナリオにも対応可能であると予想しています。

デフォルト設定では、他のソリューション（共有された仮想環境に非対応）は、25 台すべてのマシンで同時スキャンを試行しました。図 2 では、McAfee ソリューションが Trend Micro に対し、CPU は 2.8 倍、RAM は 11 倍のリソースを使用していることを示しています。Symantec では CPU は Trend Micro の 2.4 倍、RAM では 4.7 倍のリソースを使用しています。

さらに、Symantec および McAfee のソリューションは VM 25 台のテストにおいて、信頼性とユーザー エクスペリエンスの全容を把握することができませんでした。McAfee および Symantec ソリューションのリソース浪費はユーザー エクスペリエンスの質の低下につながります。また Symantec および McAfee では、25 台以上のテストを終了することができませんでした。Symantec のテストでは、2 つのエージェントと管理サーバとの接続が切断され、ディスクの待ち時間（図には表示されていません）は平均 31 ミリ秒に上っています。McAfee でのオンデマンド スキャン シナリオでは、ディスクの待ち時間は平均 80 ミリ秒を超え、25 台中 14 台がデスクトップにアクセスできませんでした。詳細なコメントについては、表 2 を参照してください。

従来のソリューションは通常、仮想環境のリソース競合を防ぐためにランダム化やグループ化といった 2 つのアプローチを推奨していますが、このどちらの方法も仮想環境は考慮されていないないため、本テストの判定外としています。

ランダム化を選択すると、管理者は独自に定める期間中、エンドポイントでのタスクをランダムで実行できます。フルスキャンのような時間のかかるタスクでは、クライアント タスクが互いに重複する可能性を回避するため、期間設定を長く（ホストの VM 密度により 1

日または 1 週間など）設定する必要があります。しかしこの場合、結果として重大なセキュリティ脅威に直面した際に企業の管理者がシステムを即時に修正できない可能性が発生します。また、不定期にタスクを実行することで、既にシステムを多く使用している場合、ユーザーエクスペリエンスの質が下がる可能性があります。

VMware ESX 4.1 環境でのアンチウィルス ソリューションの拡張性
Microsoft Windows 7 を実行する仮想マシンでのオンデマンド スキャン

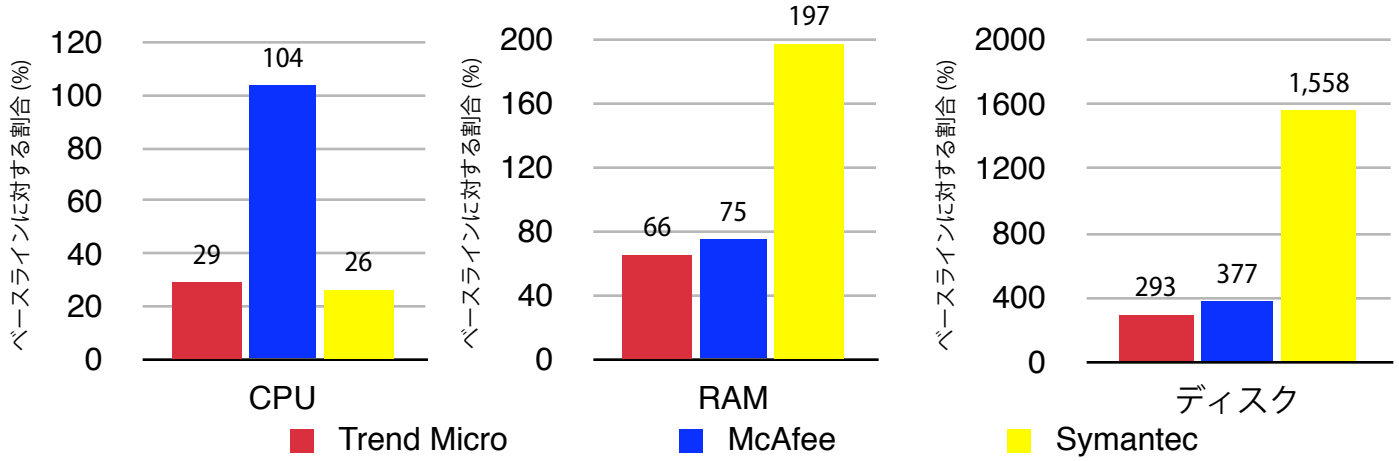
ベンダー	製品	オンデマンド スキャンの対象となる仮想マシンの数			
		25	50	75	100
Trend Micro	Deep Security 7.5	実行可（安定性にも優れる）	実行可（安定性にも優れる）	実行可（テストなしの推定値）	実行可（テストなしの推定値）
McAfee	Total Protection for Endpoint	実行可（安定性に問題）	25 台での同時スキャンにおいて安定性の問題が発生したため、台数を増やしてのテストは実施しませんでした。McAfee のソリューションにはクライアント タスクのランダム化オプションがあり、定期的に実行するタスクと手動で実行するタスクの配分を決定することができます。		
Symantec	Endpoint Protection 11.0	実行可（安定性に問題）	25 台での同時スキャンにおいて安定性の問題が発生したため、台数を増やしてのテストは実施しませんでした。Symantec ではランダム化を行うためのタスクのスケジュール設定を推奨しています。この場合、デフォルト設定では仮想マシン 100 台のオンデマンド スキャンに約 160 時間かかることになります。手動で実行するタスクにおいては、ランダムな開始時間を設定することはできません。		

注意：Trend Micro はテストで使用したソリューションのうち仮想環境に対応した唯一のソリューションで、オンデマンド スキャンを逐次処理するため自動的に調整を行っています。

出典：Tolly、2010 年 10 月

表 1

アンチウィルス ソリューション VMware ESX 4.1 のホスト リソース消費とベースラインの比較
Microsoft Windows 7 を実行する仮想マシン 50 台でのシグネチャ更新リクエスト
vCenter によるレポート（数値が低いほうが良好）



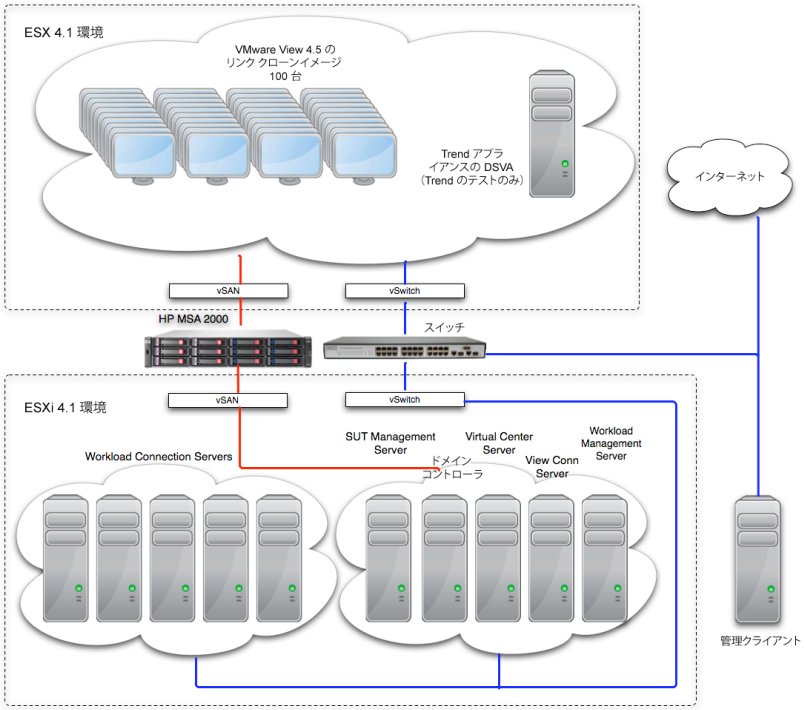
注意：すべてのシステムでテスト タスクに加え、独自設定の負荷テストを実行しています。ベースライン値は、エンドポイント セキュリティ ソリューションをインストールずに独自に設定した負荷テストを実施した結果です。ベースライン値は、それぞれ平均 CPU 使用率 ー 8,434.91 MHz、平均 RAM 使用率 ー 14,119.62 MB、平均ディスク使用率 ー 2,341.41 KBps とします。Trend ソリューションではシグネチャ ファイルを単一の仮想セキュリティ アプライアンスにダウンロードするだけで終了しますが、他のベンダーでは 25 台がそれぞれ同時に更新を行いました。各ベンダーは更新の負荷を平準化するためのさまざまな方法を提案しています。詳細はレポート本文を参照してください。ベースラインと比較した使用率は、結果からベースラインの値を引いた後、さらに同値で割った数字に 100 を掛けて算出されます。テストの実施時間は平均 15 分です。

出典：Tolly、2010 年 10 月

図 3

グループ化を選択すると、管理者は異なるグループに VM を割り当てられるようになり、グループ別にクライアントタスクをスケジュールできます。しかしこれは管理作業を要するため、企業の IT 管理が複雑化する恐れがあります。また新しい VM は手動でグループに割り当てる必要があり、負荷分散や他の理由で VM を別のホストに移動させる場合、管理者はグループの割り当てを更新しなければなりません。

仮想化アンチウィルス ソリューションのテスト環境



出典：Tolly、2010 年 10 月

図 4

テストを実施したシステム

ベンダー	製品	コンポーネント	仮想マシン対応	実装
Trend Micro	Deep Security 7.5	Trend Micro Deep Security Manager バージョン 7.5.1378、Trend Micro Deep Security Virtual Appliance 7.5.0.1600、Filter Driver 7.0.0.894、デフォルト設定。事前設定の Windows 向け Anti-Malware Protection セキュリティ プロファイルを割り当てています。	対応	自動、単一の仮想アプライアンス。エージェントレスのクライアントは VMware vShield API を介して通信
McAfee	Total Protection for Endpoint	McAfee ePolicy Orchestrator 4.5、McAfee Agent for Windows 4.5.0 Minor Version 1270、McAfee VirusScan(R) Enterprise 8.7.0 Minor version 570 with Hot Fix 2、McAfee AntiSpyware Enterprise 8.7 Minor version 129、McAfee SiteAdvisor(R) Enterprise Plus 3.0.0 Minor version 476、すべてデフォルトのポリシー。事前設定のフルスキャンおよびクライアントの更新 タスクは含まれません。	非対応	従来のエンドポイント クライアント
Symantec	Endpoint Protection 11.0	バージョン 11.0.6100.645	非対応	従来のエンドポイント クライアント

出典：Tolly、2010 年 10 月

表 2

アンチウィルス シグネチャ（パターン）の更新テスト（仮想マシン 50 台）

システム全体に対するアンチウィルス パターンの更新が必要な場合、各ソリューションがどのようにそれを実施しているかを評価しました。パターンの更新はフルスキャンよりもリソースを使用しないとはいえ、特に通常の営業時間中に実行する場合は、パフォーマンス劣化や操作上の問題を引き起こすことが分かっています。

エンジニアは、50 台の仮想マシン（以下 VM）でシグネチャ更新シナリオを実行しました。従来のソリューションでは、各 VM でシグネチャ ファイルを更新する必要がありましたが、Trend Micro ソリューションの場合、Trend Micro Deep Security アプライアンス上にシグネチャ ファイルのコピーが 1 ファイルだけあればよく、このファイルを Trend Micro の管理化にあるすべての VM が使用します。よって、CPU や RAM のリソースを大量に消費していた従来のソリューションに比べ、Trend Micro の場合はリソース消費量が確実に低く抑えられています（表 3 を参照）。

また、Trend Micro ソリューションを実装する利点として、ネットワーク セキュリティ管理者がシグネチャの更新処理を実施する際に、「オフライン」になっている VM がないかどうかを心配する必要がないことも挙げられます。従来のソリューションでは、更新を実行するには、VM は必ずオンラインでなければなりません。

同時に実施したオンデマンドのスキャン テストと同様に、McAfee および Symantec のソリューションは、一度に 50 台すべての VM で更新を行う必要があり、システムのすべてのレベルにおいて、リソースおよびパフォーマンスに影響がでました。

Symantec の場合、各マシンに割り当てられた 1GB RAM を Symantec のシグネチャ更新タスクがすべて使用したため、ほとんどの仮想マシンが VMware の vCenter 管理ステーションにメモリアラームを発行しました。また、50 台中 10 台の VMware View デスクトップが、このテスト中に切断されました。

本テストでは使用していませんが、McAfee ソリューションにはアイドル状態の VM でシグネチャ ファイルを 1 日 1 回更新するタスクが含まれてることをエンジニアが指摘しています。このタスクは、手動でキャンセルしても自動的に開始されました。

Symantec ソリューションのように、50 台の VM を同時に更新すると、大量のリソースを消費する可能性があり、テスト実行時に VMware ESX システムの CPU 使用量が 10 分以上常に 100% になること、もありました。また、仮想化システム全体に深刻なパフォーマンス劣化が見られました。

仮想マシンの密度（集約度）比較

仮想化を実施する場合、たいていはプライマリ VM の負荷を基準にサイズを算出し、パフォーマンスに影響を及ぼすような従来型のアンチウィルス（以下 AV）負荷は考慮されていません。Tolly では、本テストの一環として AV 効率性が VM 密度に与える影響の評価を試みました。VM 密度の向上は、(a) AV がアイドル状態の場合、(b) AV ソリューションがオンデマンド スキャンやシグネチャ更新といったクライアント タスクを即座に実行している場合など、さまざまな方法で測定可能です。

Trend Micro 社

Deep Security 7.5

VMware アンチウィルス パフォーマンス

Tolly. Certified

2010 年 10 月 テスト実施

VMware パフォーマンス テストを実施したホスト プラットフォーム コンポーネント

コンポーネント	バージョン/ビルド
VMware ESX	4.1.0
VMware vCenter Server	4.1.0 ビルド 258902
VMware View Composer Server	2.1 ビルド 277387
VMware View Connection Server	4.5.0
VMware vShield Manager	4.1 ビルド 310451
サーバー ハードウェア	2x Xeon x5680 (Hexacore)、3.33GHz、192 GB の DDR 3 RAM（論理コア数 24）で起動
ストレージ エリア ネットワーク	HP StorageWorks MSA（4GB FibreChannel 経由で接続）
ゲスト VM リソース	1GB RAM および 1 vCPU
ゲスト オペレーティング システム	Microsoft Windows 7 Enterprise

出典：Tolly、2010 年 10 月 表 3

公称 VM 密度（AV アイドル状態）

ここでは、プライマリ負荷はかかっているが特定の AV タスクは実施されていない、アイドル状態の AV ソリューションのリソース使用量に注目しました。Trend Micro ソリューションを採用した場合の VM 密度は、CPU とメモリを基準にそれぞれ Symantec と比較すると 34.5% および 29% 向上しました。同様に McAfee と比較すると、CPU とメモリを基準にそれぞれ 31.4% および 42.4% の向上でした（表 5 を参照）。

実際の VM 密度（フル スキャン）

アイドル状態の AV 公称密度は、ピーク時の AV アクティビティを考慮していません。そのため「AVストーム」といった集中的なアクティビティは ESX ホストに負担をかけ、VM 負荷に大きな影響を与えます。テスト結果から見ると、AV スキャンと更新は、CPU とメモリ、デスク使用量という 3 つのエリアすべてにおいてリソースを多量に使用しています。そしてリソースがボトルネックとなるかは、システムや負荷によって異なります。

Trend Micro ソリューションを採用した場合の VM 密度は、CPU とメモリを基準に

Trend Micro Deep Security

Trend Micro から「VM 対応」機能を提供する Deep Security 7.5 が登場しました。従来のエージェントベースのソリューションとは違い、Deep Security はアンチウィルスの一括パターン更新やリソース消費、管理コストといったオペレーションにかかわるセキュリティ問題を低減します。Deep Security は別途エージェントをインストールすることなく、VM 上でアンチウィルス保護を実行し、パフォーマンス速度の向上、より高度な VM 集約化、管理の容易化、仮想化された資産のより「迅速な」保護を可能にします。

出典：Trend Micro、2010 年 10 月

アンチウィルス VMware ESX 4.1 のホスト リソース消費とベースラインの比較
独自設定の負荷を使用し、最大 100 台の VM を Microsoft Windows 7 で実行
vCenter によるレポート（数値が低いほうが良好）

仮想マシンの数	AV ソリューション		ESX ホスト ベースライン リソース使用/% ベースライン比の増加		
			CPU (GHz)/%	RAM (GB)/%	ディスク (KBps)/%
25	ベースライン		4.113 GHz	6.306 GB	1.705 KBps
	Trend Micro	ベースライン比の増加%	8.86%	5.94%	-13.26%
	McAfee		43.04%	50.83%	191.82%
	Symantec		46.58%	36.63%	138.05%
50	Baseline		8.467 GHz	11.908 GB	2.592 KBps
	Trend Micro	ベースライン比の増加%	24.65%	10.7%	38.98%
	McAfee		43.02%	60.34%	393.09%
	Symantec		42.73%	37.78%	148.91%
75	Baseline		12.645 GHz	17.325 GB	3.381 KBps
	Trend Micro	ベースライン比の増加%	11.61%	7.79%	-11.03%
	McAfee		35.33%	64.57%	325.32%
	Symantec		39.61%	33.33%	108.22%
100	Baseline		17.197 GHz	22.468 GB	5.417 KBps
	Trend Micro	ベースライン比の増加%	9.86%	12.7%	-4%
	McAfee		33.33%	69.31%	271.43%
	Symantec		36.14%	44.31%	77.61%

注意：ベースライン値は、アンチウィルスやエンドポイント セキュリティ ソリューションをインストールせずに独自に設定した負荷で 30 分間のテストを実施した結果です。リソース消費量については、パーセンテージの値が低いほうが良好です。多くの場合、テストは時間内に終了しませんでした。McAfee ソリューションは、複数回の試行および再テストの実施を試みましたが、VM 100 台のテストを完了できませんでした。よって McAfee の VM 100 台についての結果は、Tolly のエンジニアが VM 25 台、50 台、75 台 の試験結果をもとに予想しました。ディスク使用量の結果は、最大 30% の誤差があり、これは参照目的でのみご利用ください。

出典：Tolly、2010 年 10 月 表 4

それぞれ Symantec と比較すると 106% および 114% 向上しました。同様に McAfee と比較すると、CPU とメモリを基準にそれぞれ 124.9% および 273.5% の向上でした（表 5 を参照）。

テスト方法とテスト用プラットフォームの設定

すべてのテストは同一のハードウェアインフラを使用して実施されたため、連続的に行われました。表 2 にはテストを実施したソリューションと仮想マシンのゲスト システムの詳細が表示されており、表 3 はパフォーマンステストを実施したプラットフォームの仮想マシンホスト環境の詳細です。

物理サーバの CPU は 24 の論理コアで構成されており、100 台の VM に対し物理 CPU リソースがおよそ 4:1 の割合で過負荷状態であることを意味します。しかしテスト担当者によると、テスト全般を通して CPU リソースはボトルネックとはなり得なかったと報告されています。

テスト用のその他のインフラを実行するために VMware ESXi ホストが使用されており、これにはロード ジェネレータ システムをはじめ、テスト対象のシステムが必要とする多様な管理サーバが含まれています。

Trend Micro ソリューションは、仮想アプライアンスとして実装されており、VMware API を使ってゲスト マシンと通信しています。この API は仮想ネットワーク インターフェイスを経由して通信を実行します。

他のソリューションは「仮想マシンに対応」していないため、100 台の物理 Windows マシンに実装する方法と同様のやり方で行われています。

テスト環境が最終的に決定された時点で、仮想化環境のエンドポイント セキュリティ用の McAfee ソリューションである、McAfee Management for Optimized Virtual Environments (MOVE) は、Vmware ホスト環境では使用できませんでした。

テスト対象となったすべての製品は、それぞれデフォルトでアンチウィルス ポリシーを有しており、事前にスケジュールが設定されたフル スキャンと更新タスクはキャンセルされました。

プライマリ負荷

プライマリ テストには、順番に次の 3 つのレベルのアクティビティに分類された、当社が独自に設定した負荷を使用しました。

高：ゲスト マシンの 55% が Microsoft Outlook や Word、Excel、Powerpoint、Internet Explorer、Adobe Reader のアプリケーション使ったスクリプトを実行している。
低：ゲスト マシンの 35% が Microsoft Outlook や Word、Internet Explorer、Adobe Reader のアプリケーション使ったスクリプトを実行している。アイドル：ゲストマシンの 10% が Windows を起動しており、アイドル状態に保たれている。

すべてのテストにこの負荷を使用し、オンデマンド スキャンやシグネチャ更新テストではバックグラウンド負荷として使用しました。Windows ファイヤウォールや Windows Defender はすべてのゲスト仮想マシンではオフにしていました。

プライマリ負荷テストでは、Tolly のエンジニアがすべてのユーザーが自動的に VMware View クライアントにログインし、アプリケーション スクリプトを実行するような負荷を設定しました。

スクリプト アクティビティには、電子メールや Microsoft Office 文書の編集、Adobe PDF ファイルのページ表示、ウェブ閲覧が含まれています。負荷には I/O 負荷の高いものあるいはファイルのコピーといったタスクは含まれておらず、実施時間は 30 分でした。

オンデマンド スキャンとシグネチャ更新テスト

Tolly のエンジニアがバックグラウンド負荷としてのプライマリ負荷を設定し、テスト対象であるすべてのゲスト VM に対し管理サーバからフル スキャンあるいは更新タスクを 1 回割り当てるテストを実施し、そのテストの実施に掛かった時間は 15 分でした。

すべてのパーフォマンスの結果は VMware vCenter で 20 秒毎にキャプチャしました。

VM 密度の向上 ー 独自設定の負荷：Trend Micro と競合他社の比較
（公称密度）

	CPU	RAM	ディスク
McAfee	31.4%	42.4%	236%
Symantec	34.6%	29%	174%

VM 密度の向上 ー オンデマンド スキャン：Trend Micro と競合他社の比較
（実際の密度）

	CPU	RAM	ディスク
McAfee	124.9%	273.5%	171.6%
Symantec	106.0%	114.1%	183%

注意：表内の数値はリソース消費量に基づいた Trend Micro と競合他社を比較したスケール/密度の向上見込みを表しています。
公称密度とは、AV ソリューションがアイドル状態でのシステムの負荷で。
実際の密度とは、AV ソリューションを稼動させている負荷です。

出典：Tolly、2010 年 10 月 表 5

Tolly について

Tolly Group の企業は、世界的な IT サービスを 20 年間にわたり提供し続けています。Tolly は IT 製品、コンポーネント、サービスに関する第三者評価の提供で業界をリードするグローバル企業です。
当社には、電子メール *(sales@tolly.com)* または電話 (1 561.391.5610) にてご連絡いただけます。

Tolly のウェブサイトは下記のとおりです。*http://www.tolly.com*

競合他社とのかかわり

Tolly Group は、比較テストを実施する際の Tolly Group のプロセスに従って、公表に先立ち、競合ベンダにテスト方法および結果の確認を依頼しました。McAfee からの返答はなく、Symantec からは Tolly のエンジニアとの協働の申し出がありました。また Symantec からは、長期間に渡るテストにおいて、リソースを多量に消費する負荷を配分するために、同社のランダム化機能を使用するよう推奨されました。

当社の公正テスト憲章に関する詳細については、下記サイトをご覧ください。
http://www.tolly.com/FTC.aspx

利用条件

本書は、特定の製品、技術、サービスがユーザーの要件に合っているかどうかを判断する一助として、無償で提供されています。購入の判断は、自身の適合性調査に基づいて行ってください。本書は、IT や業務の有識者からの提言に相当するものではありません。この評価は、製品の特定の機能または性能に焦点を当てており、管理された検証環境下で実施されています。試験によっては、理想的な条件下での性能を反映するように調整されていることもあります。そのため、実環境の条件下では性能が本書と異なる場合があります。実際のシナリオに基づいて試験を実施し、各自のネットワークでの性能を確認することをお勧めします。

本書に記載されるデータの精度を高めるため、妥当な範囲での努力は行っていますが、誤りや過失がある可能性もあります。本書に記載される試験や監査では、さまざまなテスト ツールを使用していますが、その精度は弊社が管理できる範囲を超えています。さらに、本書ではスポンサーから提供された特定の表現を使用していますが、これも弊社が検証できる範囲を超えています。試験対象のソフトウェアおよびハードウェアには、製品化済みのものと製品化中のものがあり、一般の顧客が現時点で同等製品を入手できる場合と、同等またはよりよい形の製品が将来入手可能になる場合があります。本書は「現状のまま」で提供されるものであり、Tolly Enterprises, LLC（以下「Tolly」）は明示的もしくは黙示的の一切の保証を行いません。また、本書に記載されるいかなる情報の正確性、完全性、有用性、適合性についても、直接的もしくは間接的な一切の法的責任を負いません。本書に記載されるいかなる情報も、利用者の責任において使用されるものとし、得られた情報および資料に起因する直接的もしくは間接的な損失、損害、費用、その他の結果について一切の責任は利用者が負うものとします。Tolly は、本書に記載されるいかなる情報の使用または信用に起因する損失、損害、損傷についても一切の責任を負わないものとし、利用者は Tolly およびその関連会社を無害に保つものとします。

Tolly は、本書に記載されるいかなる製品または企業についてもそれらが投資に適していると主張しているわけではありません。本書に記載される情報、製品または企業に関する投資やプロジェクトについては、それらを開始する前に、法律、会計またはその他について独自に専門家の助言を求めることをお勧めします。翻訳版が存在する場合でも、英語版の文書を正式版とします。正確性を確保するために、Tolly.com から直接ダウンロードした文書のみを使用してください。本書のいかなる部分も、一部または全体にかかわらず、Tolly から文書による許諾を得ることなく複写することはできません。本書で使用されている商標はすべてそれぞれの所有者に帰属します。利用者は、いかなる商標も、弊社以外の活動、製品またはサービスとの関連で利用者の商標の全体または一部で使用しないものとします。また利用者は、混同や誤認を招くような方法、あるいは弊社や弊社の情報、プロジェクトまたは開発を誹謗中傷するような方法でいかなる商標も使用しないものとします。

211101-uv-3-kt - 04Feb2011VerP