ウイルス対策の比較

パフォーマンス・テスト

セキュリティ・ソフトウェアがシステム・パフォーマンスに及ぼす影響

言語：日本語

2016 年 10 月

最終更新日：2016 年 11 月 1 日

www.av-comparatives.org

目次

はじめに

このレポートに記載された結果は、当該テストでのセキュリティ製品のシステム・パフォーマンス（主としてリアルタイム／オンアクセス・コンポーネントによる）への影響だけを示すものです。ユーザーはご自身のPCでソフトウェアを使用し、各自システムでパフォーマンスを確認することをお勧めします。

現在、SSD を搭載しているコンピュータが多いので、このパフォーマンス・テストでは、テスト対象マシン上の SSD を使用しました。この変更に合わせて、アワード・レベルを調整いたしました。

テスト対象品

このテストでは、64 ビット・システムの以下の製品を評価しました（デフォルト設定で）。

- Avast Free Antivirus 12.3
- AVG Internet Security 16.121
- AVIRA Antivirus Pro 15.0
- Bitdefender Internet Security 2017
- BullGuard Internet Security 16.0
- Emsisoft Anti-Malware 12.0
- eScan Internet Security Suite 14.0
- ESET Smart Security 9.0
- Fortinet FortiClient 5.4（FortiGate使用）
- F-Secure Safe 2017
- Kaspersky Internet Security 2017
- Lavasoft Ad-Aware Pro Security 11.12
- McAfee Internet Security 2017
- Microsoft Windows Defender 4.10
- Quick Heal Total Security 17.0
- Sophos Endpoint Protection 10.6
- Tencent PC Manager 11.6（英語）
- ThreatTrack Vipre Internet Security Pro 9.3
- Trend Micro Internet Security 2017

過去数年の間に実施されたパフォーマンス・テスト結果を読まれたことがある読者に対しては、このテストには「Antivirus」と「Internet Security」製品が両方含まれており、両方を「セキュリティ製品」と呼んでいることをあらかじめお伝えしておきます。各メーカーから Main Test Series での保護テスト用に提供された製品をテストしました。本レポートに記載された結果は、上記の製品バージョンにのみ適用される点に注意してください（すなわち、当該バージョンで 64 ビット・システムに対して）。また、ベンダーによって製品で提供している機能が異なる（また機能数も異なる）点にも注意してください。

以下のアクティビティ／テストを、最新の**Windows 10 64ビット・システム**で実行しました。

- ファイルのコピー
- アーカイブ／アンアーカイブ
- アプリケーションのインストール／アンインストール
- アプリケーションの起動
- ファイルのダウンロード
- PC Mark 8 Professional Testing Suite

テスト方法

このテストは Intel Core i5-6200 CPU、8GB の RAM と SSD ハード・ディスクを搭載した Lenovo ThinkPad E560 マシンで実施しました。パフォーマンス・テストは、まずクリーンな Windows 10 64 ビット・システム（英語版）で実行し、次にセキュリティ・ソフトウェアをインストールして（デフォルト設定を使用）実行しました。このテストはインターネット接続がアクティブな状況で実行し、実際の環境におけるクラウド・サービス／機能の影響を確認できるようにしました。

測定やシステムの比較に影響を及ぼす可能性があるその他の要素をできるだけ最小化するように配慮いたしました。各製品で使用している最適化プロセス／指紋認証についても検討しました。したがって、本書に記載の結果は、ユーザーがある一定期間運用していたシステムへの影響を示しています。平均値を得て、測定エラーを除外するために、テストは複数回実行しました（指紋認証機能を使用する場合と使用しない場合の両方で）。テスト終了後、毎回ワークステーションの断片化を行い、6 回リブートしました。コンピュータのユーザーが実行する可能性がある、次のような各種ファイル操作のシミュレーションを行いました。1 か所から別な場所に各種クリーン・ファイルをコピー[1]、ファイルのアーカイブとアンアーカイブ、インターネットからのファイルのダウンロードとアプリケーションの起動（文書を開く）。サブテストでは、Windows Assessment と Deployment Toolkit（Windows ADK）を Windows Performance Toolkit（WPT）と併用しています。このツールキットは、コンピュータ・システムのパフォーマンス測定用に、業界内で広く利用されています。このツールを使用することで、ベンダーは簡単に結果を復元し、製品のどの部分がパフォーマンスに影響を及ぼしているのかを特定することができます。ベンダーが今回のテスト用に製品を最適化しないようにするため、独自の ADK 用テスト・ドライバーを実装しました。これにより、相互の影響なく、各サブテストのパフォーマンス上の影響を測定することができます。

また、業界で認められたサードパーティのパフォーマンス・テスト用スイート（PC Mark 8 Professional）を使用して、実際の製品利用がシステムに及ぼす影響を測定しました。読者が各種製品をご自身で評価されることをお勧めします。それによって、システムへの影響（たとえばソフトウェアの競合、ユーザー・プリファレンス、様々な結果を招く可能性がある各種設定による影響）を確認することができます。

セキュリティ製品は早い段階でシステムにロードし、当初からセキュリティを確保する必要があります。これにより、システムのスタートアップに要する時間に一定の影響を及ぼします。ブート時間の正確な測定は困難です。最大の問題はシステムがいつ起動したのかを正確に定義することです。多くの運用環境では、システムがユーザーに応答した後も、しばらくの間はスタートアップ・アクティビティを実行することがあるためです。テスト対象のセキュリティ・ソリューションが提供している保護機がいつ完全にアクティブな状態になるのかを考慮することも重要です。セキュリティ・ソリューションに関しては、これをブート完了の判断材料に使用することができます。一部のセキュリティ製品は、ブート時のロードに非常に時間がかかります（数分かかることも）。システムのロード後、しばらくの間、システム速度が非常に遅くなります。したがってシステムのロードは非常に高速に行われたように見えても、実際にはセキュリティ製品によるサービスの読み込みが後からなので、システムの脆弱性が高くなってしまいます。このような点が判明したため、レポートでは現在もブート時間を公表していません。

[1] 種類もサイズも異なる各種ファイル（写真、動画、音声ファイル、MS Office 文書、PDF 文書、アプリケーション／実行可能ファイル、オペレーティング・システム・ファイル、アーカイブなど）から成る約 3GB のデータを使用しました。

注記とコメント

ウイルス対策ソフトウェアのオンアクセス／リアルタイム・スキャナー・コンポーネントは、バックグラウンド・プロセスとして実行されます。これにより、アクセスされたすべてのファイルをチェックして、マルウェアの脅威からシステムを継続的に保護します。たとえば、オンアクセス・スキャナーはアクセスがあればすぐにファイルをスキャンします。一方、たとえば挙動ブロッカーでは、異なる保護レイヤーを追加し、実行中のファイルを監視します。この種のタスクのためにバックグラウンドで実行するサービスとプロセスも、システム・リソースを必要としており、システム・リソースを使用します。一般に、スイート製品のほうが含まれているサービス／機能が多く、それらがバックグラウンドで実行するため、ウイルス対策製品よりもシステム・パフォーマンスへの影響が大きいのです。

セキュリティ製品でシステムを保護するには、はシステムの深い部分で機能する必要があります。たとえば、システム起動中にアクティブになったプロセスなどのスキャンを行い、ルートキットやその他のマルウェアを識別します。この種のプロシージャには追加の時間がかかるので、システムのブート／起動が遅れます。

製品によるシステム・リソースの消費量が多すぎる場合、ユーザーは不満を感じ、基本的な保護機能を無効化、またはアンインストールする（したがってシステムのセキュリティを大幅に危険にさらします）、またはリソース消費量が少ないセキュリティ・ソフトウェアに切り替えます。したがって、ウイルス対策ソフトウェアは検出率が高く、マルウェアに対する保護機能も優れているだけではなく、システム・パフォーマンスを低下させない、またはユーザー側で問題が発生しないことも重要です。

このレポートは各種のインターネット・セキュリティ製品がシステム・パフォーマンスに及ぼす影響について記載していますが、システムのスピードが低下する原因は必ずしもセキュリティ・ソフトウェアだけではありません。その他の要因に影響されることもあり、ユーザーが簡単なルールに従って対処することで、システム・パフォーマンスが大幅に向上する可能性があります。以降のセクションでは、影響を及ぼす可能性があるその他の要因について説明します。

一部のユーザーの PC で見られる一般的な問題：

- **古いハードウェア**：10 年も前のハードウェアを使用しているため、PC が非常に遅い場合、最新の（セキュリティ）ソフトウェアを使用すると機能しない状態になります。
  - o 可能であれば、使用するソフトウェアの最低推奨要件を満たす新しい PC を購入してください。Multi-Core プロセッサの使用をお勧めします。
  - o RAM を追加するのも効果的です。Windows 7 を使用する場合、4GB 以上の RAM を使用する必要があります。Windows XP、Vista、8、または 8.1 を使用している場合は、Windows 10 64-Bit に切り替えます。
  - o リアルタイム保護機能のあるセキュリティ・プログラムは、1 本だけインストールしていることを確認してください。新しい PC にトライアル版のセキュリティ・スイートが同梱されている場合、別な保護プログラムをインストールする前にこれをアンインストールしてください。

- **すべてのソフトウェアを最新の状態に維持すること：**たとえば 2014 年のものなど、古いバージョンのウイルス対策ソフトウェアでも、シグネチャは更新できるかもしれませんが、新しいバージョンほどシステムを十分保護できません。推奨されているパッチをインストールして、オペレーティング・システムを最新の状態に維持してください。どのソフトウェアにも脆弱性やバグがあるので、PC にインストールされたすべてのソフトウェア

を常に最新の状態に維持してください。これによって多くのエクスプロイトや脆弱性から保護されるだけでなく、その他のアプリケーションの改善点も反映することができます。

- **ハード・ディスクのコンテンツのクリーンアップ：**
  - o ハード・ディスクがほぼ一杯の場合、システム・パフォーマンスも影響されます。ディスク容量を少なくとも20%以上空けておき、動画やその他、頻繁に使用しないファイルは別な（外付け）ディスクに移動します。コスト面で問題がなければ、ソリッドステート・ドライブ（SSD）の購入を検討してください。
  - o 不要なソフトウェアはアンインストールしてください。ウイルス対策製品をインストール後にユーザーが感じる速度低下は、PC 上でバックグラウンドで実行中の他のソフトウェアに起因している可能性があります（すなわち、ソフトウェアの競合や別なプログラムが重いファイルにアクセスすることで、アクセスのたびにウイルス対策のスキャニングが必要になっている）。
  - o 不要なエントリー／ショートカットを［すべてのプログラム］メニューの［スタートアップ］フォルダーから削除します。
  - o 試用した数百のアプリケーションのインストール／アンインストール後に残ったファイルやレジストリ・エントリーがまだ PC 上に多数ある場合、クリーンなオペレーティング・システムを再インストールして、本当に必要なソフトウェアだけをインストールしてください（インストールしているソフトウェアの数が少ないほど脆弱性や競合の可能性も低くなる）。その上で、すべてを再インストールしなくても、たとえばイメージ／バックアップ・ツールを使用してクリーンなシステム状態に戻します。

- **ハード・ディスクのデフラグを定期的に実施すること：**断片化したハード・ディスクはシステム・パフォーマンスに非常に大きな影響を及ぼし、システムのブートアップに必要な時間が非常に長くなります。デフラグを効果的に行うためには、ハード・ディスク上に 15%以上の空き領域が必要です。ソリッドステート・ドライブ（SSD）ではデフラグは不要で、デフラグによってドライブ寿命が短くなる点に注意してください。

- **指紋認証／最適化：**ほとんどのウイルス対策製品は、各種技術を使用してシステム・パフォーマンスへの影響を軽減しています。指紋認証はスキャン済みのファイルを再スキャンしたり、ホワイトリストに入れたり（このほうがまれ）しない技術です。これによって大幅なスピードアップが可能になりますが（特に PC を長時間使用した後は）、一部のファイルはスキャンされなくなるため、潜在的なリスクが高まります。ユーザー自身で対処方法を判断する必要があります。定期的にシステム全体のスキャンを行うことをお勧めします（すべてのファイルが少なくともクリーンな状態であることを確認し、指紋認証機能をさらに最適化するため）。

- **辛抱強くなること：**セキュリティ・ソフトウェアによって数秒間遅れることは、実際にはそれほど深刻な問題ではありません。ただし、上記の推奨内容に従った場合でも PC の状態に不満がある場合は、別なウイルス対策製品を試してみる必要があります。長期間ウイルス対策ソフトウェアの使用後にのみ速度が低下する場合は、速度低下の原因が他にある可能性があります。ほんの少し PC を高速にしたいからといって、基本的な保護機能を無効化してセキュリティを下げることはしないでください。

テスト・ケース

ファイルのコピー：ウイルス対策製品によっては、設計上／デフォルト設定により、特定の種類のファイルを無視することがあります（たとえばファイル拡張子など）。また、スピードアップのために、指紋認証技術を使用して、スキャン済みのファイルをスキップする場合もあります（6 ページのコメントを参照）。一般的な各種ファイルを、物理ハード・ディスクから別な物理ハード・ディスクにコピーしました。

アーカイブとアンアーカイブ 一般的にファイル・ストレージ用にアーカイブを使用します。新しいアーカイブの作成や、既存のアーカイブからのファイルのアンアーカイブに要する時間に、ウイルス対策ソフトウェアが及ぼす影響については多くの人の関心事になっています。自宅やオフィスのワークステーションで一般的な各種ファイルのアーカイブを行いました。ほとんどのユーザーは、ディスク上の既存のファイルのアーカイブを行うことが一般的なため、ウイルス対策製品の指紋認証／最適化技術も考慮した結果になっています。

アプリケーションのインストール／アンインストール：サイレント・インストール・モードで、一般的な複数のアプリケーションをインストールし、次にそれらをアンインストールして、所要時間を測定しました。アプリケーションは通常複数回インストールされるため、指紋認証は考慮していません。

アプリケーションの起動：Microsoft Office（Word、Excel、PowerPoint）およびPDF文書は非常に一般的です。Microsoft OfficeとAdobe Acrobat Readerで各種文書を開いて、その後閉じました。ビューワやエディター・アプリケーションの起動と、それを閉じるまでに要した時間を測定しました。最初に開いたときと、その後開いたときの結果を記載していますが、通常はユーザーがこの種の操作を複数回行い、ウイルス対策製品の最適化が行われ、システムへの影響が最小化されるため、後から開いたときの結果のほうが重要だと考えています。

ファイルのダウンロード：GUIのないブラウザーでローカル・サーバーから大きなファイルをダウンロードします。このブラウザーにより、バックグラウンドでHTTPリクエストを送信することができます。さらに、ローカル・サーバーから、複数の一般的なWebサイトのコンテンツを*wget*でフェッチします。

テスト結果

記載したテスト結果は、あるセキュリティ製品がシステム・パフォーマンスに及ぼす影響を、テスト対象になった他のセキュリティ製品と比較したものです。レポートに記載されたデータは単なる指標で、非常に多くの要因に影響を受けるので、すべての状況に該当するわけではありません。テスト担当者は統計技法を検討し、ユーザーの立場になって気付いた点を考慮し、あるいは他のセキュリティ製品と比較することで、中、高速、超高速というカテゴリー分けをしました。一部の製品が 1 回のサブテストで他の製品よりも高速／低速だった場合、結果に反映されます。

中	高速	超高速
このクラスター内の製品の平均値によって、特定のサブカテゴリーの第 3 のクラスターが確立する	このグループの製品の平均値が、特定のサブカテゴリーの全スコア平均値よりも高くなっている	このグループの製品の平均値が、特定のサブカテゴリーの全スコア平均値よりも低くなっている

単一の AV-C パフォーマンス・スコアの概要

ベンダー	ファイルのコピー		アーカイブ／アンアーカイブ	アプリケーションのインストール／アンインストール	アプリケーションの起動（文書と PDF ファイルを開く）		ファイルのダウンロード
	初回実行時	以降の実行時			初回実行時	以降の実行時	
Avast							
AVG							
Avira							
Bitdefender							
BullGuard							
Emsisoft							
eScan							
ESET							
Fortinet							
F-Secure							
Kaspersky Lab							
Lavasoft							
McAfee							
Microsoft							
Quick Heal							
Sophos							
Tencent							
ThreatTrack							
Trend Micro							

キー： 中 高速 超高速

PC Mark テスト

業界で認められたパフォーマンス・テストを実施するために、PC Mark 8 Professional Edition[2]テスト・スイートを使用しました。PC Mark 8 ベンチマーク[3]を使用する際は、テスト・スイートに影響を及ぼす可能性があるすべての外部要因を最小化する必要があります。また、少なくとも PC Mark マニュアルに記載された推奨内容に厳格に従って、一貫性のある、有効／有益な結果を得る必要があります。さらに、複数回テストを繰り返して、内容を確認する必要があります。PC Mark に含まれている各種消費者シナリオに関する詳細は、Web サイトに掲載されたホワイトペーパーを参照してください[4]。

「セキュリティ・ソフトウェアがない状態」は、ベースライン[5]・システム上で、まったくセキュリティ・ソフトウェアをインストールしていない状態でテストしました。PC Mark 8 Home ベンチマークでは、100 ポイントのスコアになります。

	PC Mark 8 ポイント
セキュリティ・ソフトウェアなし	100
Avira	99.7
ESET	
F-Secure	
Avast	99.6
Bitdefender	
Kaspersky Lab	
AVG	99.5
BullGuard	
Emsisoft	
McAfee	
Quick Heal	
ThreatTrack	
Sophos	99.4
Microsoft	99.3
Fortinet	99.0
Trend Micro	98.6
Tencent	98.3
Lavasoft	97.9
eScan	

[2] 詳細は http://www.futuremark.com/benchmarks/pcmark8 を参照してください。

[3] PCMark®は Futuremark Corporation の登録商標です。

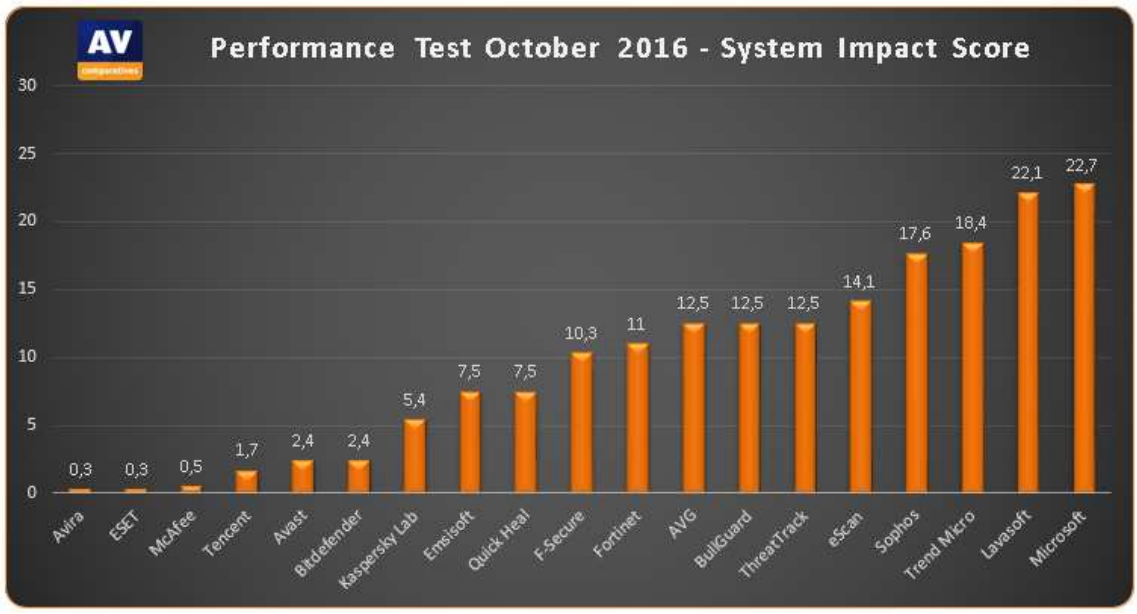
[4] http://www.futuremark.com/downloads/pcmark8-technical-guide.pdf（PDF）

[5] ベースライン・システム：8GB RAM および SSD ドライブを搭載した Intel Core i5-6200 マシン

結果概要

ユーザーはニーズに応じて、各種サブテストに加重を適用する必要があります。各種結果を要約するために、スコアリング・システムを適用しました。ファイルのコピーとアプリケーションの起動サブテストについては、最初と以降の実行結果を別途記載しています。AV-C スコアについては、初回と以降のファイルのコピー操作に関しては、概算平均値を計測しました。一方、アプリケーションの起動に関しては初回ではなく、それ以降の実行についてのみ計測しました。「超高速」は 15 ポイント、「高速」は 10 ポイント、「中」は 5 ポイントになります。これによって次のような結果になりました。

	AV-C スコア	PC Mark スコア	合計	インパクト・スコア
Avira, ESET	75	99.7	**174.7**	0.3
McAfee	75	99.5	**174,5**	0.5
Tencent	75	98.3	**173,3**	1.7
Avast、Bitdefender	73	99.6	**172,6**	2.4
Kaspersky Lab	70	99.6	**169,6**	5.4
Emsisoft、Quick Heal	68	99.5	**167,5**	7.5
F-Secure	65	99.7	**164,7**	10.3
Fortinet	65	99.0	**164,0**	11.0
AVG、BullGuard、Threat-Track	63	99.5	**162,5**	12.5
eScan	63	97.9	**160,9**	14.1
Sophos	58	99.4	**157,4**	17.6
Trend Micro	58	98.6	**156,6**	18.4
Lavasoft	55	97.9	**152,9**	22.1
Microsoft	53	99.3	**152,3**	22.7



このテストにおけるアワード・レベル

以下のアワード・レベルは、このパフォーマンス・テスト・レポートに記載された結果に対するものです。パフォーマンス・テストは、他のセキュリティ製品と比較して、そのセキュリティ製品がシステムに及ぼす影響を示したものに過ぎません（8 ページの注記を参照）。製品の保護機能の効果を示すものではないため、弊社 Web サイトに掲載された『Real-World Protection』および『File Detection』テストを参照してください。

アワード	製品[6]
AV comparatives ADVANCED+ ★★★ PERFORMANCE TEST OCT 2016	✓ Avira ✓ ESET ✓ McAfee ✓ Tencent ✓ Avast ✓ Bitdefender ✓ Kaspersky Lab ✓ Emsisoft ✓ Quick Heal
AV comparatives ADVANCED ★★ PERFORMANCE TEST OCT 2016	✓ F-Secure ✓ Fortinet ✓ AVG ✓ BullGuard ✓ ThreatTrack ✓ eScan
AV comparatives STANDARD ★ PERFORMANCE TEST OCT 2016	✓ Sophos ✓ Trend Micro ✓ Lavasoft ✓ Microsoft
AV comparatives TESTED PERFORMANCE TEST OCT 2016	-

[6] 同じアワードの製品は、同じアワードの他の製品と同程度軽量とみなすことをお勧めします。

著作権と免責事項