セキュリティソフトがシステムに与える影響の評価

稲置慎也
森俊也

1．はじめに

近年のマルウェアは種類が膨大な数に上ると共に巧妙化したため、その対策のために大きな手間暇が必要とされるようになっている。このため対策に用いられるセキュリティソフト、アンチウィルスソフトも肥大化し、システムに過大な負担を強いるものとなっている。結果として、マルウェアの対策にマシンパワーの多くを占有されるため、コンピュータの動作が遅くなったり、本来の動作に支障をきたす場合があり、本学のように旧式のパソコンを大切に利用しているような環境に与える影響は深刻である。

そこで、各種セキュリティソフトの有無が基本OSであるWindowsの起動時間と終了時間に与える影響を計測し、これをもってシステムに与える負荷を評価した。

2．実験方法

Table. 1 に示すパソコンにマイクロソフトVirtual PC 2007 Service Pack1をインストールし、Virtual PC 2007上にWindows XP Service Pack3をインストールした。

そのWindows XP SP3のイメージを必要台数分コピーし、同じ環境に整えてから各種セキュリティソフトをインストールし最新版にアップデートをおこなった。

すべてのセキュリティソフトを同時期にアップデートし最新版とした後に、ネットワークから切り離した状態で起動時間、ならびに終了時間の測定をおこなった。

［実験に使用したパソコンの仕様］
日本HP ProLiant ML115

CPU　AMD Athlon 3500＋(周波数 2.2GHz)
L2キャッシュ　512KB
CPU数　1個
筐体　タワー型
チップセット　nVidia MCP55S Pro
メインメモリ　2048MB (PC2-5300 SDRAM)
HDD容量(標準)　80.0GB(SATA)
CD　最大48倍速(IDE)CD-ROM
FD　なし
ディスクコントローラ　オンボード 4ポートSATAコントローラ
RAIDアダプタ　内蔵RAID機能付き、RAID 0、1、5
LAN　オンボード NC320i PCI Express Gigabitサーバ アダプタ
その他バス
　フルレングス/ フルハイトPCI Express x16×1、
　ハーフレングス/ ロープロファイルPCI Express x8×1、
　32ビット/ 33MHz PCI×1
インストールOS　Windows XP Service Pack3
本体サイズ(H×W×D)　W175×H367×D426mm
本体重量　10.5kg
電源　100～127V(50～60Hz)/ 200～240V(50～60Hz)
最大消費電力　370.00W

Table.1　ホストパソコンの仕様

Virtual PC 2007 Service Pack1
バージョン：6.0.192.0
公開された日付：2008/05/15
言語：日本語
ダウンロード サイズ：31.7 MB (32ビット版)
ホストOS：Windows XP Service Pack3
ゲストOS：Windows XP Service Pack3
(ゲストの環境はメモリを256MBとした以外はデフォルト)

Table.2　Microsoft Virtual PC 2007 Service Pack1の仕様

3．各種セキュリティソフトの紹介

(1) ノートン インターネットセキュリティ 2009

シマンテック社の主要な製品である。トレンドマイクロ社のウィルスバスター、マカフィーと共に古くから存在する製品であり、三社合わせて御三家とも呼ばれる。

[製品サイト]

http://www.symantec.com/ja/jp/norton/internet-security

（特徴の一覧）

＊ ウイルス対策
＊ スパイウェア対策
＊ パーソナルファイアウォール
＊ 個人情報盗難対策（アドオンパック）
＊ フィッシング対策
＊ ネットワーク監視機能
＊ ボットネット対策
＊ ルートキット削除機能
＊ ブラウザ保護機能
＊ インターネットワーム対策
＊ 侵入検知と防止機能
＊ OSとアプリケーションの保護
＊ Webサイト認証
＊ パルス アップデート
＊ ノートン インサイト
＊ SONAR(TM) ビヘイビア検出技術
＊ スパム対策
＊ 保護者機能（アドオンパック）

的確なノートンソリューション：

・かんたんに利用できる総合的な管理
・自動化されたウイルス対策とスパイウェア対策

主要な保護機能：

・ウイルス、スパイウェア、トロイの木馬、ワーム、ボット、ルートキットからの保護
・作業の邪魔をしないパーソナルファイアウォールが、脅威を水際で防止
・５分から15分間隔のパルス アップデートによる定義ファイルの更新
・インテリジェンス技術による、より高速かつ少ない回数での、短時間のスキャン

高度な保護：

・ブラウザ、OS、アプリケーションに対する脅威を阻止し、感染したWebサイトから保護
・プロアクティブな多層保護による最新の脅威からの保護
・リアルタイムのSONAR技術が、通常の定義ファイルが利用可能になる前に、新たなスパイウェアとウイルスを検出

個人情報保護：

・フィッシング詐欺サイトを遮断し、信頼できるサイトを認証

・ログイン情報および個人情報を安全に保存し管理
・ログイン操作とフォーム入力を自動化してキーロガーから保護
・人気のショッピングサイトやネットバンキングWebサイトを認証する

ネットワーク：
・ホームネットワークの保護と監視を支援
・公衆のワイヤレスホットスポットからの接続時に、自動的にコンピュータを保護

サポート：
・365日受けられる無償のチャットサポート
・自動修復機能が頻繁に起こる問題を診断し、修復

【15日間体験版ダウンロードサイト】
http://www.symantecstore.jp/trial/index.asp

(2) ウィルスバスター2009

トレンドマイクロ社の主要な製品である。シマンテック社のノートン、マカフィーと共に古くから存在する製品であり、三社合わせて御三家とも呼ばれる。

[製品サイト]
http://jp.trendmicro.com/jp/products/personal/vb2009/

製品の特長
【ウイルス/スパイウェア対策】
危険なウイルスやスパイウェアに感染しないよう、常にモニタリング。ウイルスやスパイウェアを発見した場合は自動駆除。

・リアルタイム検索：
・予約検索：
・手動検索：
・メッセンジャー検索：
・圧縮ファイル検索：
・感染ファイルの自動駆除：
・受信メール検索：
・ルートキット対策：
・ウイルス/スパイウェア隔離：
・不正変更（ウイルス/スパイウェア）の監視：
・履歴クリーナー：

・クッキーの例外設定：
・ウイルス緊急警告：

【有害サイト対策】
・Webレピュテーション技術：
・フィッシング詐欺対策：
・改良されたサイトブロック機能：
・メッセンジャー/WebメールのURL評価：
・ローカルWebレピュテーション：
・有害サイト規制：

【迷惑（スパム）メール対策】
・迷惑（スパム）メール/詐欺メールの判定（自動振り分け）：
・リンクフィルタ：

【不正侵入対策/ネットワーク管理】
・パーソナルファイアウォール：
・無線LANパトロール：
・ホームネットワーク管理：
・無線LANアドバイザ：

【個人情報漏えい防止対策】
・個人情報の保護：
・キー入力暗号化：
・リモートファイルロック：

【パソコン最適化】
・システムチューナー：

【30日間体験版ダウンロードサイト】
http://jp.trendmicro.com/jp/products/personal/vb2009/trial/index.html

(3) マカフィー・インターネットセキュリティ2009

マカフィー社の主要な製品である。シマンテック社のノートン、トレンドマイクロ社のウィルスバスターと共に古くから存在する製品であり、三社合わせて御三家とも呼ばれる。

[製品サイト]
http://www.mcafee.com/japan/mcafee/home/2009/security.asp

製品機能一覧
* ウイルス対策：スパイウェア対策およびサイトアドバイザが悪意のあるソフトウェアからパソコンを守る。
* ファイアウォール：外部からのパソコンへの侵入者を防ぎます。
* サイトアドバイザ：ウェブサイトの危険性を「赤」「黄」「緑」のアイコンで知らせてくれるもの。
* Network Manager（ネットワークマネージャー）：家庭内のパソコンにマカフィーのセキュリティ対策が行われているかどうかを確認する。
* 個人情報保護、フィッシング対策：サイトアドバイザが個人情報を守る。
* 保護者機能：子供に不適切なサイトの閲覧を制御する。

【30日間体験版ダウンロードサイト】
https://service.mcafeestore.jp/MCFS-TRL/TL001-01.asp?prod_cd=MIS

(4) Windows LiveOneCare

マイクロソフトが開発しているインターネットセキュリティスイート。2007年1月30日にWindows Vistaと並行して発売された比較的新しいセキュリティソフトである。

[製品サイト]
http://onecare.live.com/standard/ja-jp/default.htm

Microsoftが提供する常時稼働の PC ケア サービス "Windows Live OneCare" であり、コンピュータの保護、メンテナンス、および管理を行うことができる。OneCareはコンピュータのバックグラウンドで目立たずに動作し、ウイルス、スパイウェア、ハッカー、およびその他の迷惑な侵入者からコンピュータを保護する。

製品機能一覧
* 複数のPCおよびホーム ネットワークの管理
* プリンタ共有の対応
* 起動時間の最適化
* 事前対策と推奨作業
* WiFiセキュリティ
* 中央管理バックアップ

＊ オンライン写真バックアップ

【90日間体験版ダウンロードサイト】
http://onecare.live.com/standard/ja-jp/install/install.htm

(5) ウィルスセキュリティZERO

ソースネクスト社が販売するセキュリティ対策ソフトである。発売当初、1,980円と価格が低く抑えられたことで反響を呼んだ。現在では年間更新料無料となったウイルスセキュリティZEROが発売されている。

[製品サイト]
http://sec.sourcenext.info/products/zero/

製品の特長

「ウイルスセキュリティZERO」は、期限設定のない業界初の無期限セキュリティソフトである。Windowsの公式サポート期間中、毎年の費用負担と更新の手間がいらず、期限切れのまま使う危険がないのが特徴。

この製品の対応OSとサポート期間は以下のようにアナウンスされている。
マイクロソフト社の公式サポート期間に準ず（2008年10月現在）
Windows Vista（Business/Enterprise） 2017年４月11日まで
Windows Vista（Home Basic/Home Premium/Ultimate） 2015年４月11日まで
Windows XP 2014年４月８日まで
Windows 2000 2010年７月13日まで

製品機能一覧

ウイルス、スパイウェア、ネット詐欺対策
・ウイルス、スパイウェアの自動処理
・ヒューリスティック機能
・ポリモーフィック型ウイルス検出
・ワームの無断送信防止
・設定の無断変更を監視
・ネットワーク内ウイルス検知
・その場でウイルス検査
・検査しないファイル、フォルダの設定
・自動定期ウイルス検査

・検査後パソコン自動終了

不正アクセス対策
・ファイアウォール
・ネットワーク自動検知
・ポートの設定
・アプリケーションごとの設定

個人情報対策
・個人情報の送信防止
・個人情報を送信するサイトの設定
・広告ブロック
・閲覧制限
・迷惑メール・フィッシング対策
・メール自動監視
・許可リスト・ブロックリスト作成
・特定の言葉を含むメールを分類
・指定した外国語のメールを分類
・自動迷惑メール振り分け

【7日間体験版ダウンロードサイト】
http://sec.sourcenext.info/corporate/

4．各種セキュリティソフトの仕様

(1) ノートン インターネットセキュリティ 2009
対応OS
Microsoft Windows Vista Home Basic/Home Premium/Business/Ultimate
Microsoft Windows XP (SP2) Home/Professional/Media Center Edition
必要なシステム
＊ 300 MHz 以上のプロセッサ
＊ 256 MB の RAM (*リカバリツールを使用する場合は 512 MB の RAM)
＊ 200 MB 以上のハードディスク空き容量
＊ 標準の Web ブラウザ
＊ Windows Vista Service Pack 1 対応
＊ Windows XP Service Pack 3 対応

(2) ウイルスバスター2009

対応OS

* Microsoft Windows Vista Home Basic/Home Premium/Business/Ultimate (Service Packなし、およびService Pack 1に対応)
* Microsoft Windows XP Home Edition/Professional Service Pack 2、3
* Microsoft Windows XP Media Center Edition 2005 Service Pack 2、3
* Microsoft Windows XP Tablet PC Edition 2005 Service Pack 2、3

必要なシステム

Windows XPの場合:Intel Pentium 450MHz以上 または同等の互換プロセッサ

Windows Vistaの場合:800MHz以上の32ビット (x86) または64ビット (x64) プロセッサ (1GHz以上を推奨)

Windows XPの場合:256MB以上 (512MB以上推奨)

Windows Vistaの場合:512MB以上 (1GB以上推奨)

500MB以上のハードディスク空き容量(RAID-0/RAID-1に対応)

ディスプレイ:解像度1024×768以上、High Color (65536色) 以上

(3) マカフィー・インターネットセキュリティ2009

対応OS

Microsoft Windows 2000 SP 4 以降、Windows XP SP1 以降、Windows Vista

必要なシステム

500 MHz 以上の Pentium 互換プロセッサ

メモリ (RAM) :256MB 以上

ハードディスク:150 MB以上の空き容量

画面解像度:800x600 ピクセル以上

(4) Windows Live OneCare

対応OS

Service Pack 2 (SP2) 以降を適用済みの Microsoft Windows XP (Home Edition、Professional、Media Center Edition、または Tablet PC Edition)

Windows Vista 32 ビット版および 64 ビット版 (Home Basic、Home Premium、Business、または Ultimate)

必要なシステム

300 MHz 以上の処理速度の CPU を搭載した PC

256 MB の RAM および 600 MB のハード ディスクの空き領域

(5) ウイルスセキュリティ

対応OS

Windows Vista

Windows XP(SP2)以降/2000(SP4)以降

必要なシステム

インストール容量：約20MB

5．実験結果

得られた実験結果をTable.3に示す。略称は以下のとおり。

Security無： 一切のセキュリティソフトのインストールがない状態

NIS2009： ノートン インターネットセキュリティ 2009

VB2009： トレンドマイクロ ウィルスバスター2009

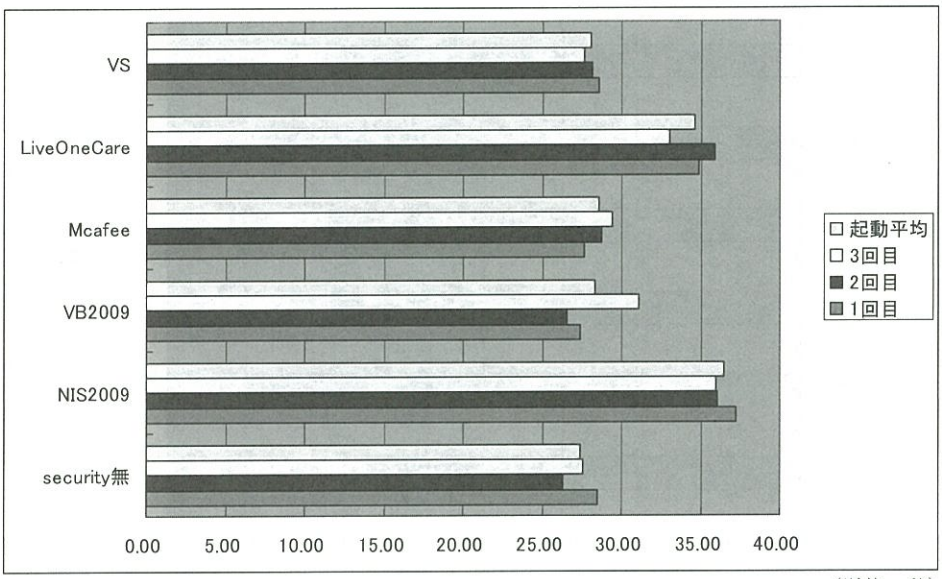
Mcafee： マカフィー・インターネットセキュリティ2009

LiveOneCare： マイクロソフトWindows LiveOneCare

VS： ソースネクスト ウィルスセキュリティZERO

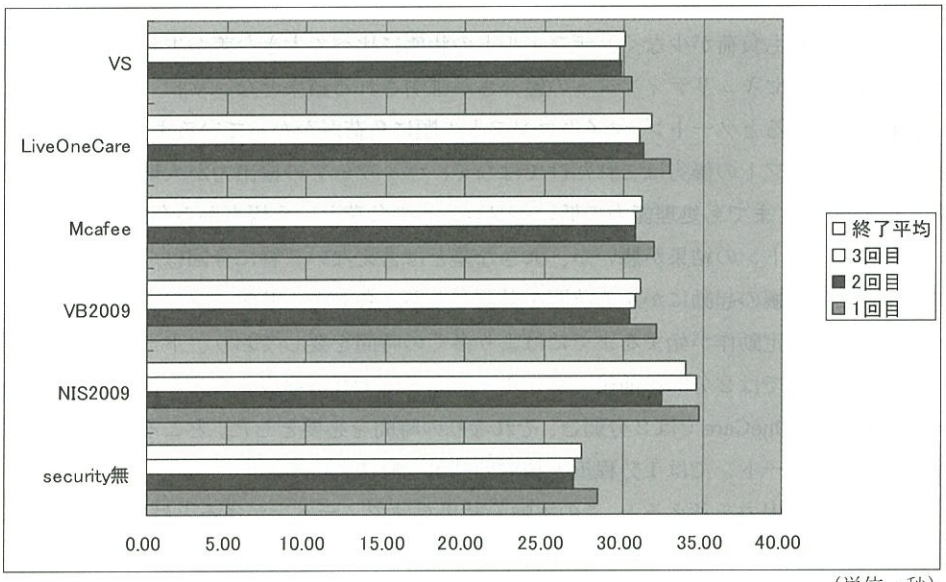
	security無	NIS2009	VB2009	Mcafee	LiveOneCare	VS
1回目	28.47	37.25	27.37	27.62	34.90	28.54
2回目	26.28	36.09	26.53	28.75	35.88	28.16
3回目	27.53	36.00	31.06	29.37	33.03	27.62
起動平均	27.43	36.45	28.32	28.58	34.60	28.11
1回目	28.44	34.81	32.13	31.90	32.97	30.53
2回目	26.87	32.40	30.40	30.75	31.22	29.85
3回目	27.00	34.59	30.72	30.79	31.00	29.75
終了平均	27.44	33.93	31.08	31.15	31.73	30.04

Table.3 各セキュリティソフトの起動時間と終了時間 (単位：秒)



（単位：秒）

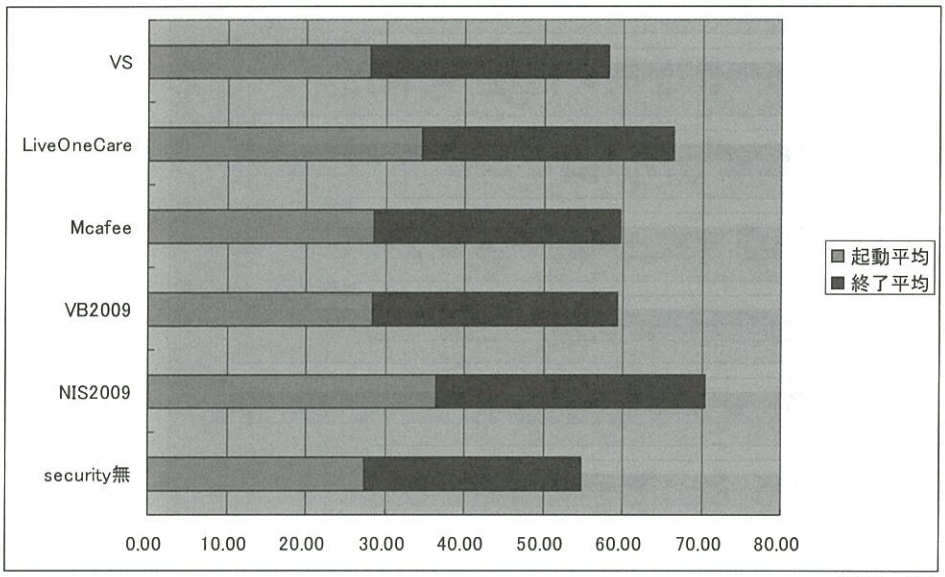
Fig. 1　起動時間



（単位：秒）

Fig. 2　終了時間

ここで起動時間とは、起動（電源オン）してからスタートアップに登録したメモ帳が起動するまでの時間、終了時間とは終了ボタンをクリックしてから画面が消える（電源オフ）までの時間を意味している。



(単位：秒)

Fig.3 起動時間と終了時間の和

6．考察とまとめ

予想したよりも負荷が少なく、デフォルトの状態に比べて大きな差が生じなかった。各社の2009年度版セキュリティソフトの優秀さが証明される結果となった。

結果だけを見るとノートン、マイクロソフトの順に負荷がかかっているように見えるが、セキュリティソフトの優劣はこれだけではなく、マルウェアの検出力が大切なことは言うまでもない。あくまでも処理能力の低いパソコンへの負荷という観点から今回は評価した。

総合的にノートンの結果が悪いが、大きな差とは言えない。特に今回はスタートアップに登録したメモ帳の起動にかかる時間を計測したが、各セキュリティソフトがタスクトレイに登録され安定動作が始まるまでにはより多くの時間を要しており、トータルで成績のよいマカフィーでは２分30秒前後、ウィルスバスターで２分程度、ウィルスセキュリティとWindows LiveOneCareでは２分弱と、それなりの時間を必要とした。ところが総合成績ではふるわないノートンでは１分程度と抜群の結果を収めている。

定評のある検出力を考えると、この実験の結果だけでノートンが劣るとは断定できない。むしろ第一に考えておかしくない製品であると考える。

今後もより対象を広げて追試を続けていきたい。

参考文献

(1) 相戸浩志，よくわかる最新情報セキュリティの基本と仕組み 増補改訂版，秀和システム(2007)
(2) 谷口　功，図解 ネットワークセキュリティ―攻撃と防御のメカニズム，オーム社(2005)

(3) SoftwareDesign編集部，ネットワークセキュリティExpert8，技術評論社(2008)
(4) 財団法人インターネット協会，インターネット白書2008，インプレスR&D(2008)
(5) 情報通信総合研究所，情報通信データブック 2008，エヌティティ出版(2008)
(6) 総務省，情報通信白書 平成20年版，ぎょうせい(2008)
(7) 情報処理推進機構，情報セキュリティ白書(2008)，実教出版(2008)
(8) 情報処理推進機構，情報セキュリティ教本―組織の情報セキュリティ対策実践の手引き，実教出版(2007)
(9) 情報処理推進機構，情報セキュリティ読本―IT時代の危機管理入門，実教出版(2006)