効果的な Antivirus の設定と運用
(第二部　性能比較評価)

--ダイジェスト版--

AntiVirus Configuration

目次

はじめに 3
I. AntiVirus ソフトウェアがシステムに及ぼす性能劣化に関して 4
II. 性能試験について ..... エラー! ブックマークが定義されていません。
II – 1 性能試験項目 ..... エラー! ブックマークが定義されていません。
II – 2 対象 AntiVirus ソフトウェア 6
II – 3 テスト環境 7
III. 性能試験結果 7
III – 1 オンアクセススキャン 7
III – 1 - 1 vmstat 結果 7
III – 1 - 2 UnixBench 結果 9
III – 1 - 3 SysBench 結果 ..... エラー! ブックマークが定義されていません。
III – 2 オンデマンドスキャン ..... エラー! ブックマークが定義されていません。
III – 2 - 1 vmstat 結果 ..... エラー! ブックマークが定義されていません。
III – 2 - 2 UnixBench 結果 ..... エラー! ブックマークが定義されていません。

はじめに

2015 年から、マルウェアの一種であるランサムウェアが脅威として注目されています。これは、悪意のある攻撃者が、ユーザのデータを勝手に暗号化や改変を行い、復旧するために身代金を要求してくるというものです。特に昨今、ビットコインなど犯罪者にとっても足のつきにくい仮想通貨が実用化されたため、この仮想通貨を利用した身代金要求ということで被害件数が増加しています。

このようなランサムウェアを含むマルウェアに対応するには、やはり昔からある「AntiVirus ソフト」を利用することが最も効果的です。サイオステクノロジーでは、この AntiVirus の効果的な設定方法に関して、特に実際の日々の運用を行う上で、いわゆるウィルススキャンの種類や効果的な設計・設定方法、スキャン対象などの点について記載していきたいと思います。

第二弾の本書では、代表的な Linux 用の AntiVirus ソフトウェアがシステムに及ぼす性能劣化に関して比較していきたいと思います。特に通常の AntiVirus ソフトウェアではウィルスの検知率や更新頻度などに目が行きがちですが、通常の運用環境にどの程度の影響を与えるのかを見ていくことで、お客様に、より安定したシステムを設計・運用していいただく手助けになるのではないかと考えています。

〈　サイオステクノロジーについて 〉
1997 年創業(旧社名:株式会社テンアートニー)で Java の開発、オープンソース分野で強みを持つ会社であり、サイオス（SIOS）という名前は、「SIOS is Innovative Open Solutions」の頭文字を取ったもので、″革新的な技術を活用して、オープンソリューションを提供していく″という思いが込められています。

I. AntiVirus ソフトウェアがシステムに及ぼす性能劣化に関して

通常、各社製品の違いを見る場合には主に検知率などを中心に議論されますが、”AV-Compatitor”が提供している AntiVirus の現実に即した検知率の比較グラフ（毎月更新）
http://chart.av-comparatives.org/chart1.php
を見てもわかる通り、現在はほぼ全ての製品が 95%以上の検知率を誇っており、ある意味ではどの製品を使用しても（ほぼ）検知率には大差がないと言えます。
そのため、本ホワイトペーパーでは、AntiVirus ソフトウェアがシステムに及ぼす「性能の劣化」に着目したいと思います。

理論上も経験的にも広く知られていることですが、AntiVirus ソフトウェアをインストールすることで、インストール前に比べてシステムの性能が劣化することがあります。

このシステムの性能劣化ですが、理論上は

1. オンアクセススキャン時：
    1. プロセスがファイルにアクセスするたびに、ファイルに対して AntiVirus ソフトウェアが（プロセスには wait()を掛けて）割り込みを行い、ウィルスの有無をスキャンする事による処理時間的な劣化
    2. 常駐プロセス（スキャンエンジンや管理エージェント）が CPU を使用することによる処理能力劣化
    3. 常駐プロセス（スキャンエンジンや管理エージェント）が予めメモリを確保／使用することによる空きメモリサイズの減少
    4. 圧縮ファイルや、PDF など内部リンクを多用するファイルをスキャンする際にメモリ上でのファイルの展開が発生することによるメモリ逼迫と SWAP アクセス増加による遅延

2. オンデマンドスキャン実施時
    1. オンデマンドスキャン対象のファイルをプロセスに使用する必要がある際に、スキャン終了までプロセスがファイルアクセス待ちになることによる処理時間的な劣化
    2. スキャンエンジンが CPU を使用することによる処理能力劣化
    3. スキャンエンジンが予めメモリを確保／使用することによる空きメモリサイズの減少

4. 圧縮ファイルや、PDF など内部リンクを多用するファイルをスキャンする際にメモリ上でのファイルの展開が発生することによるメモリ逼迫と SWAP アクセス増加による遅延

などが考えられます。

今回は、これらのパフォーマンス劣化を

- UnixBench(*)
- SysBench(**)

を用いて計測し、各社製品により違いがどの程度あるか、またその中で OSS の AntiVirus 製品である ClamAV は商用製品と比べてどの程度の性能が出るのかを見ていきます。

(*)UnixBench は、1983 年に開発された、Unix システムのパフォーマンス（性能）を測定するためのソフトウェアです。“George”と呼ばれるメモリ 128MB のシステム「SPARCstation 20-61」のスコアを 10.0 とし、システムのパフォーマンススコアを算出します。

(**)SysBench は、CPU やメモリ、ディスク I/O など、さまざまなシステム性能を測定することができる、ベンチマークツールです。 また、MySQL などのデータベースのトランザクション処理の測定も出来るのが大きな特徴となっています。

II－2　対象 AntiVirus ソフトウェア

AntiVirus ソフトウェアは、Linux 製品対象のものに限らせていただき、

- Mcafee(Intel Security)
  - VirusScan Enterprise for Linux 2.0 (VSEForLinux-2.0.2.29099) 評価版
- TrendMicro
  - ServerProtect™ for Linux 3.0 (SProtectLinux-3.0) 評価版
- Sophos
  - Sophos Anti-Virus for Linux 9 (sav-linux-free-9) 無償版
- ClamAV
  - ClamAV 0.99.2 (CentOS の yum で提供されているバージョン)

を対象としてシステムに及ぼす影響の計測を行います。

インストールはそれぞれのソフトウェアでデフォルトを使用し、可能な限り製品バージョンはインストール後に更新しています。

II－3　テスト環境

本テストは、各社の AntiVirus での性能劣化が大きく出てくるように、古いノート PC をテスト環境として用いています。

PC: Thinkpad X61

CPU: Intel(R) Core(TM)2 Duo CPU　　T7100　@ 1.80GHz

Memory: 4GB

HDD: ADATA SP900 (SSD) 128GB

OS: CentOS 7.2(最新)

インストールソフトウェア：GUI(GNOME) + MariaDB (CentOS 標準版)

一つのテストが終わるたびに、マシンを停止->再起動しています。

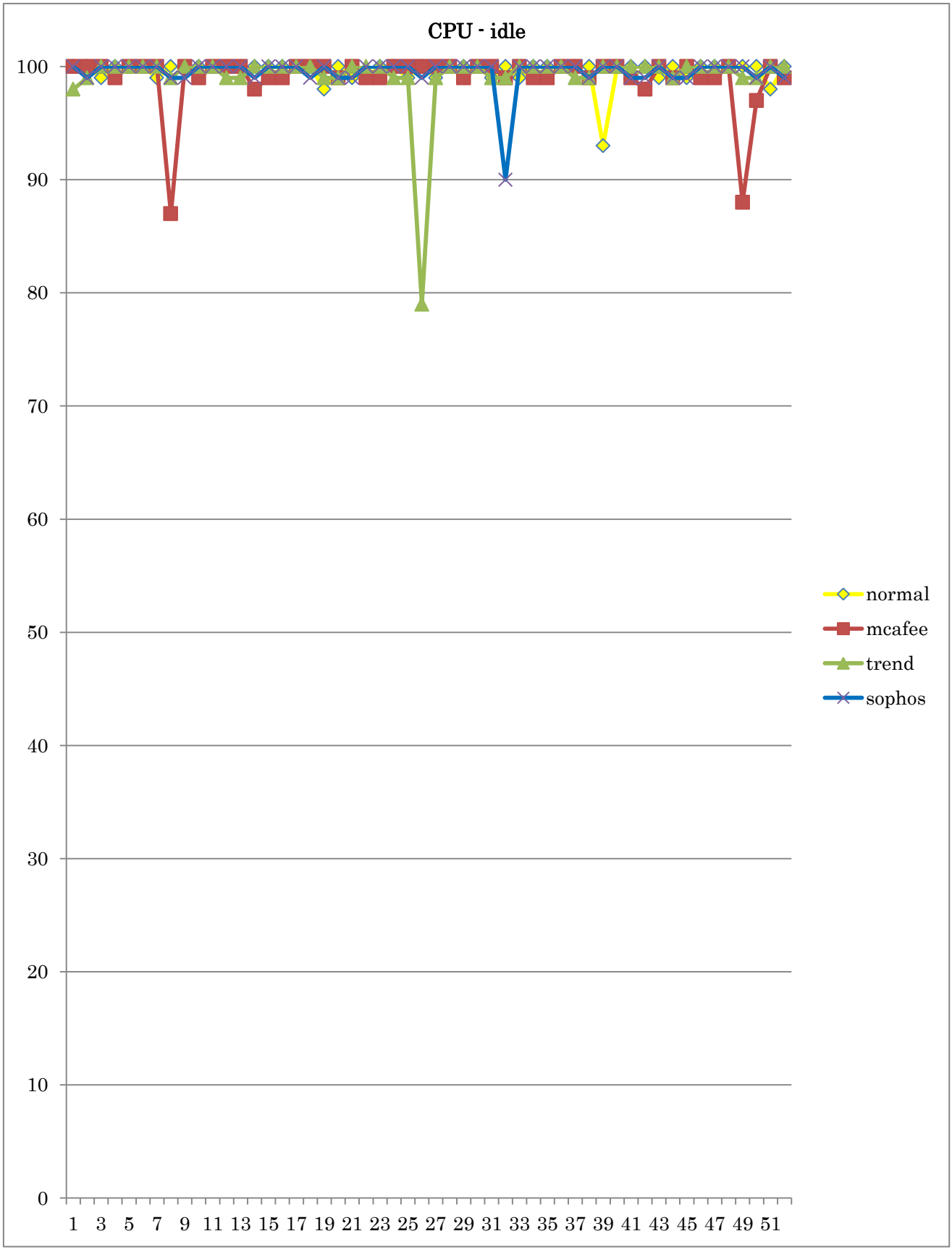
II.　性能試験結果

III－1　オンアクセススキャン

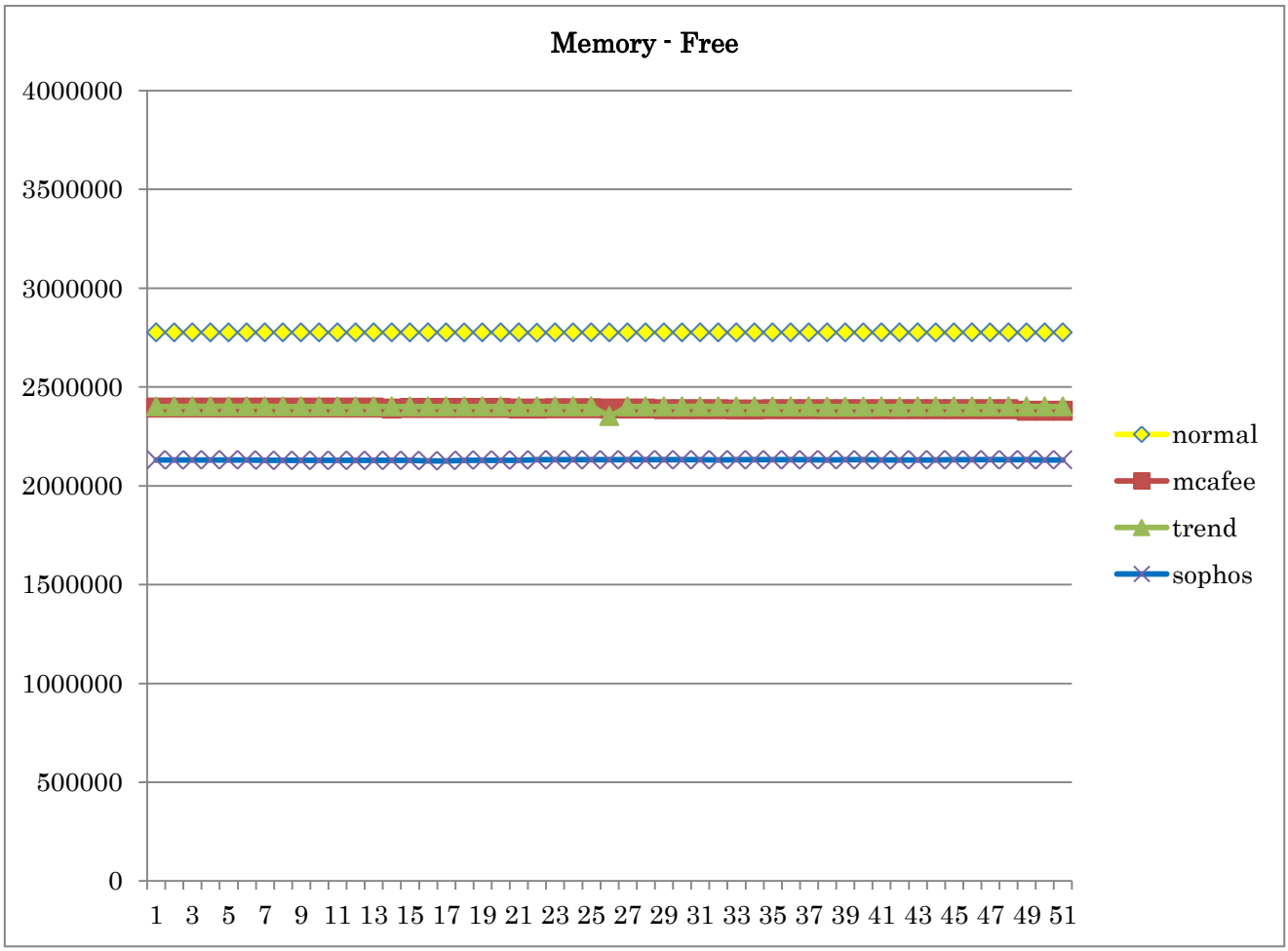
III－1 - 1　vmstat 結果

AntiVirus ソフトウェアをインストールしていない状態(normal)での vmstat 結果を基準とし、どのくらい normal からずれているかをグラフとして表示しています。

III – 1– 1– 1　CPU



III – 1– 1– 2　Memory



III – 1 - 2　UnixBench 結果

AntiVirus ソフトウェアをインストールしていない状態(normal)での UnixBench 結果を基準とし、どのくらい normal からずれているかをグラフとして表示しています。
グラフとしてあらわした時に直感的にするため、スコアは負の数となり、負の数が大きくなる（グラフ内で下に行く）ほど性能が劣化していることになります。

(以降はホワイトペーパーをダウンロードしてご確認ください)。

著作権

本書に記載されているコンテンツ（情報・資料・画像等種類を問わず）に関する知的財産権は、サイオステクノロジー株式会社に帰属します。その全部、一部を問わず、サイオステクノロジー株式会社の許可なく本書を複製、転用、転載、公衆への送信、販売、翻案その他の二次利用をすることはいずれも禁止されます。またコンテンツの改変、削除についても一切認められません。本書では、製品名、ロゴなど、他社が保有する商標もしくは登録商標を使用しています。

サイオステクノロジー株式会社 OSS 事業企画部
〒106-0047 東京都港区南麻布 2-12-3　サイオスビル
電話: 03-6401-5111
FAX:　03-6401-5112
URL: http://www.sios.com