効果的な Antivirus の設定と運用
(第二部　性能比較評価)

--ドラフト版--

AntiVirus Configuration
第 0.1 版

SIOS

サイオステクノロジー株式会社

目次

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. 性能試験について

II – 1 性能試験項目

今回の性能試験は大きく分けて

1. オンアクセススキャン
2. オンデマンドスキャン

を実施している際の性能劣化について計測していきます。

1. vmstat を用いて、システム全体のパフォーマンスを測定します。
2. UnixBench を用いて、システム全体のパフォーマンステストの劣化度を測定します。
3. SysBench を用いて、システムのアプリ(今回は MariaDB)が AntiVirus ソフトウェアによってどの程度性能が劣化するのかを見てみます。

オンアクセススキャンの性能試験では、ファイルにアクセスした際にスキャンがかかる状態にしておき、特にスキャンを行った状態での負荷は測定しません。何らかのファイルにスキャンを行っている状態での性能劣化度合は、オンデマンドスキャンを実施時の性能劣化と同列になるためです。

また、オンデマンドスキャンのテストを実施する際には、オンアクセススキャンを無効にした状態でテストを行っています。これは、オンアクセススキャンのプロセスがシステムに及ぼすパフォーマンスの影響を除外し、純粋にオンデマンドスキャンの影響を測定するためです。

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)
- ESET NoD32 (※)
  - ESET NOD32 Antivirus 4 for Linux 評価版

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。

(※) ESET NOD32 Antivirus 4 for Linux は、オンアクセススキャン・オンデマンドスキャンともに UnixBench 実施時にベンチマークプロセスがハングしてしまうため、今回は性能試験の対象外にしています。

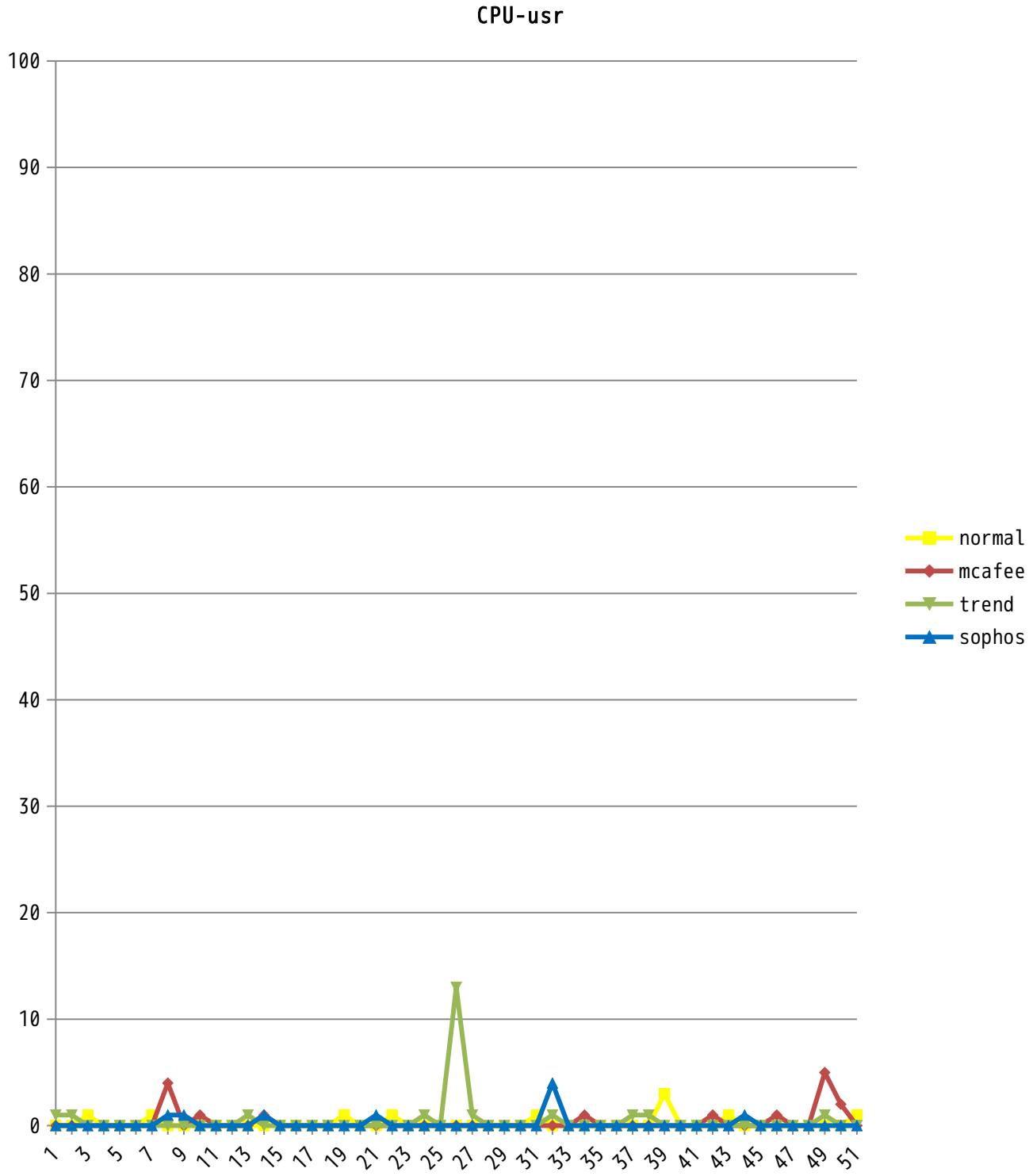
III. 性能試験結果

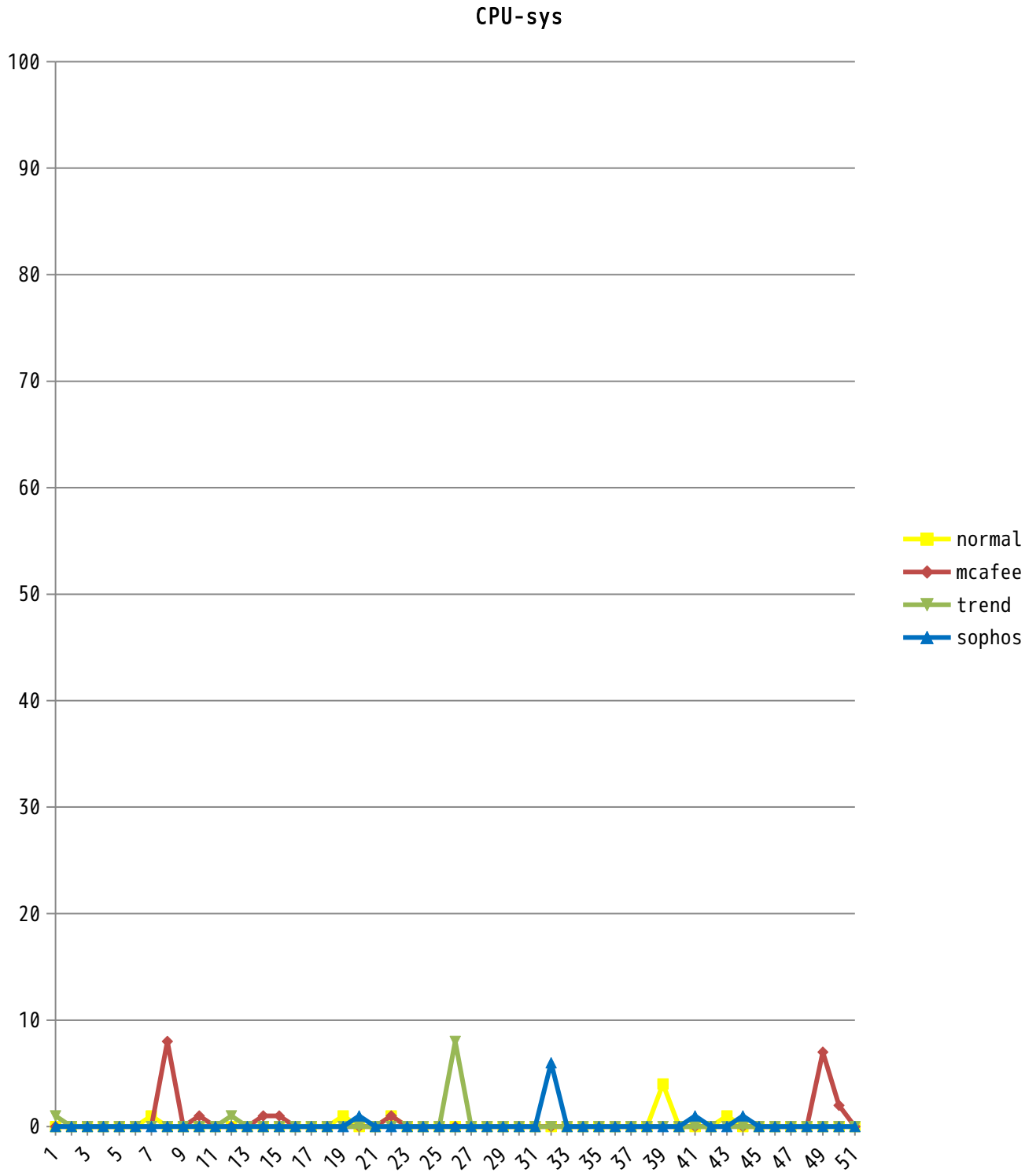
III – 1 オンアクセススキャン

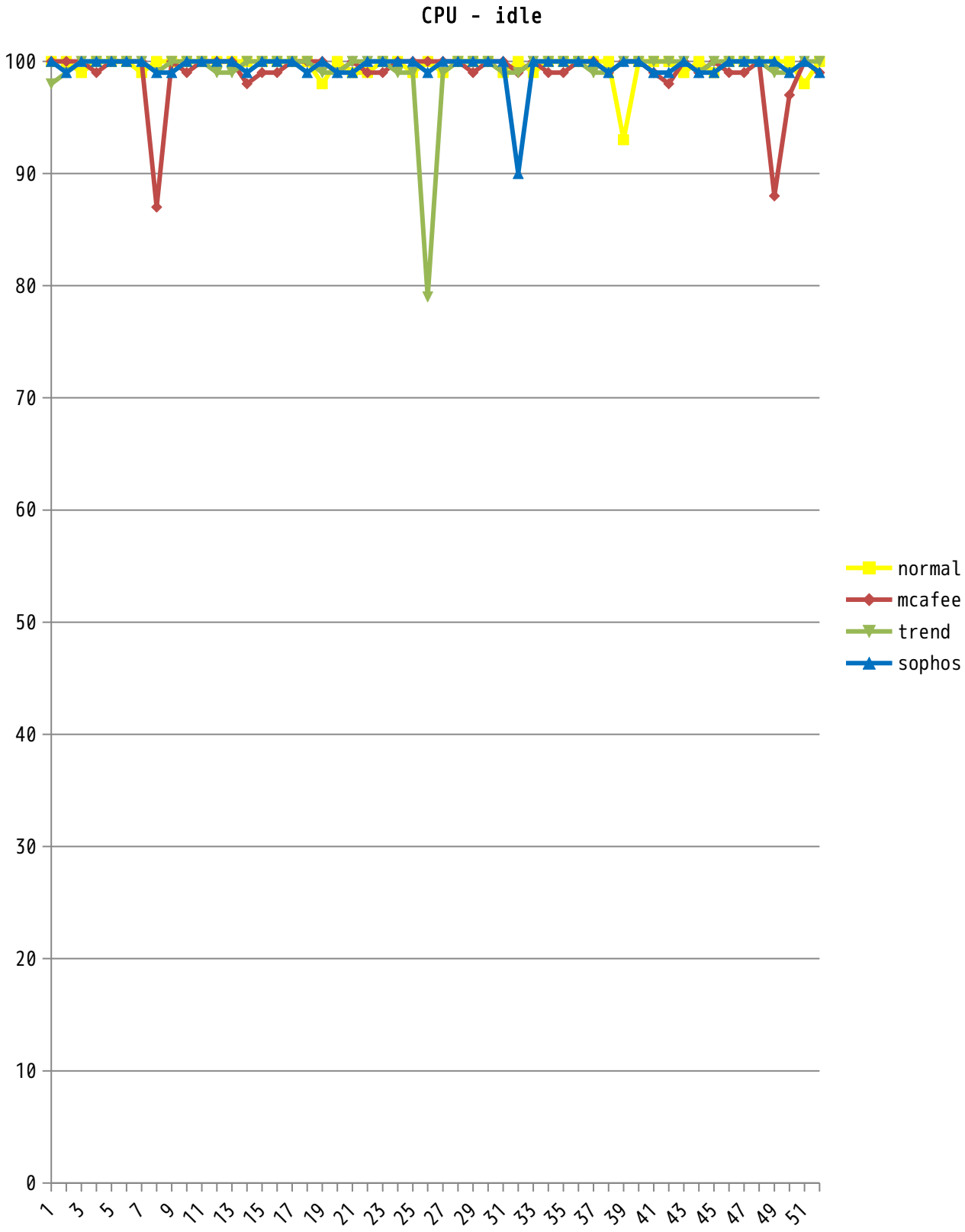
III – 1 - 1 vmstat 結果

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。

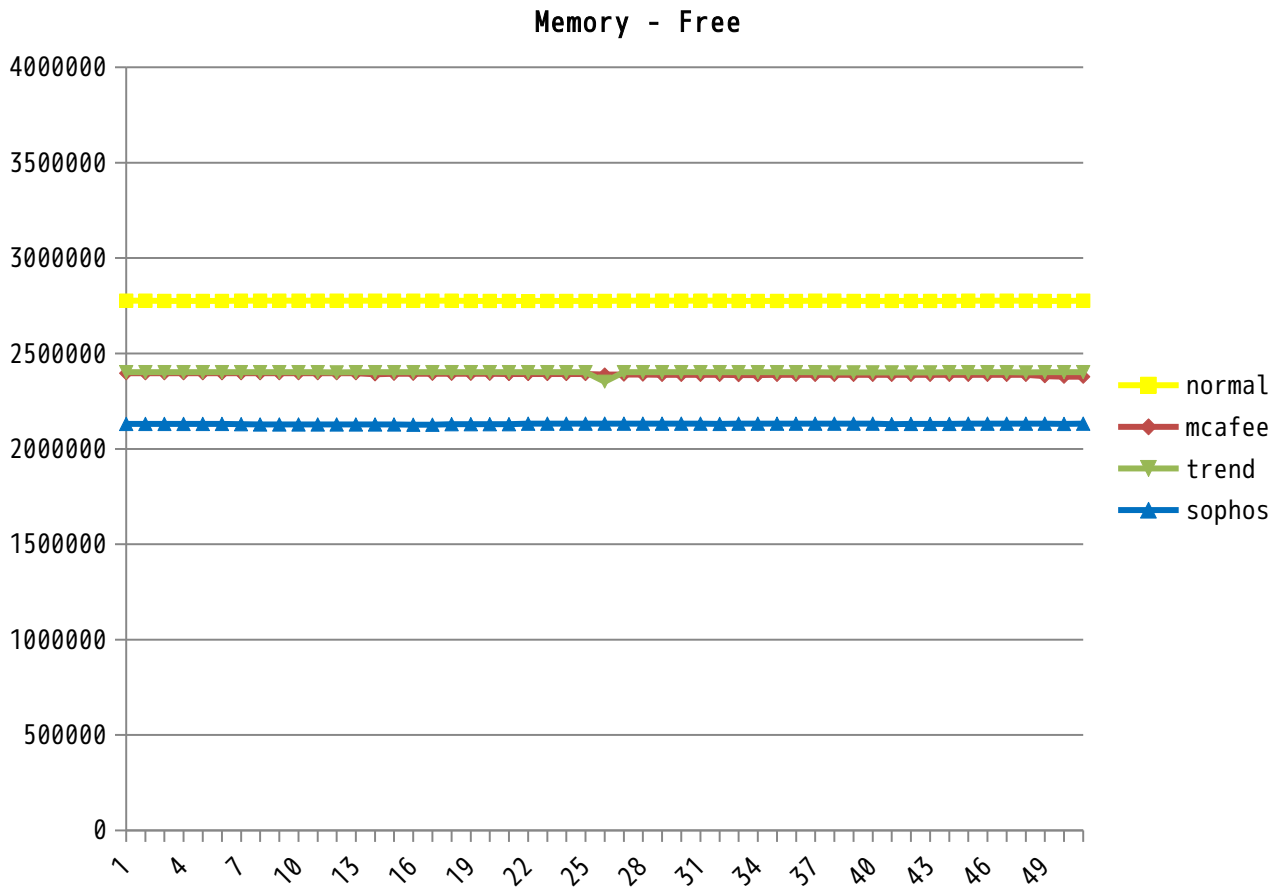
III - 1- 1- 1 CPU







III – 1– 1– 2 Memory



代表値

Free			
normal	mcafee	trend	sophos
2776284	2395752	2401400	2130800
2776316	2395836	2401136	2130464
2775852	2395876	2401696	2130636
2775788	2396056	2401600	2130668
2775852	2396024	2401664	2130604
2775788	2396024	2401600	2130668

III – 1– 1– 3 考察

vmstat による計測を見る限り、定常状態（スキャンジョブが走っていない状態）では Antivirus を入れる前と入れた後では CPU に関しては、殆ど差がないことがわかります。また、AntiVirus を入れた場合には、どの製品でも CPU 使用率の小さい山が一定間隔で並んでいます。これは、定期的にインターネットにパターンファイル等を確認に行っているためです。

メモリに関しては、各 AntiVirus ベンダのスキャンエンジンなどで使用（通常は、アーカイブの展開が発生する可能性を考えて、エンジン部分である程度のメモリ量を確保しています）が発生するため、メモリの Free サイズなどは減少しています。
そのため、メモリの Free サイズは
Normal > Mcafee, Trend (380MB 程減少) > Sophos (640MB 程減少)
となっています。
そのため、AntiVirus を動作させるためには、700MB 弱のメモリが定常状態で余分に使用されると考え、確保しておいた方が良いと思われます。

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。

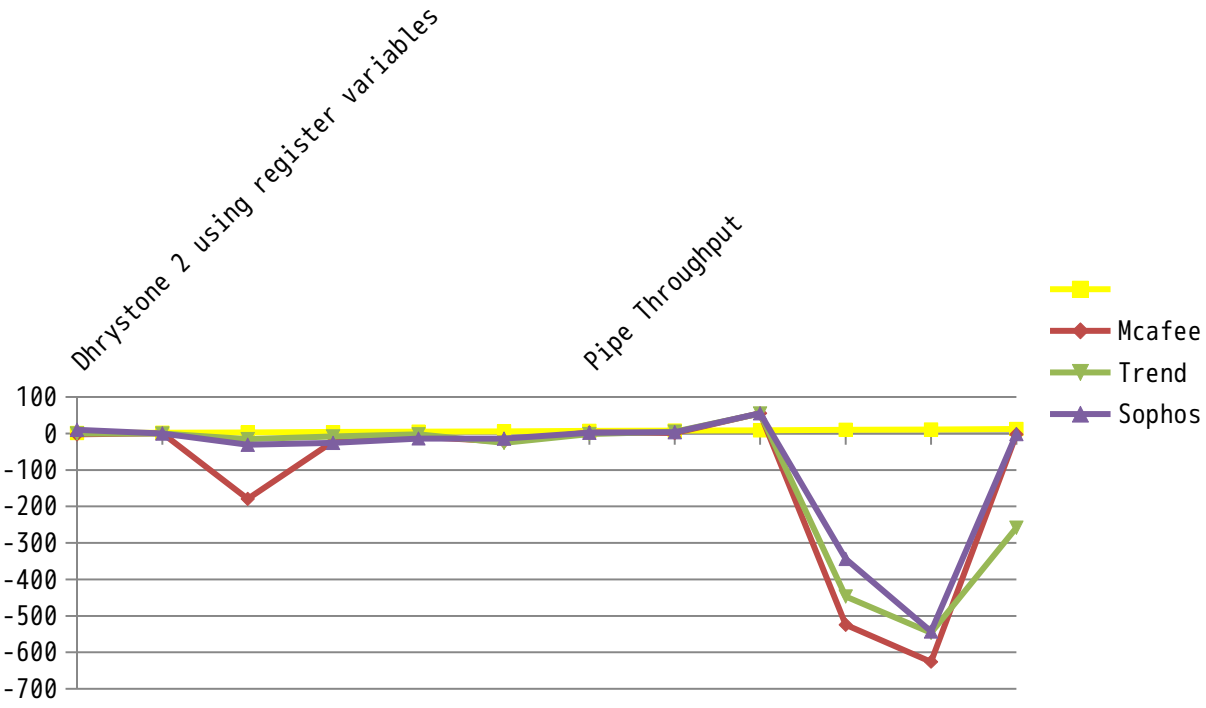
III – 1– 2– 1 総合スコア（System Benchmarks Index Score）

	Mcafee	Trend	Sophos
Benchmark Run: 2 CPUs 1 parallel process:	-102	-82.1	-49.56
Benchmark Run: 2 CPUs; 2 parallel processes	-270.98	-198.56	-127.64

単純に総合スコアを見た場合には、特にスキャン処理を実施していなくても Sophos<Trend<Mcafee の順で、AntiVirus ソフトウェアをインストールする前と比べて性能が劣化していきます。

III- 1- 2- 2　各テスト項目ごとのスコア

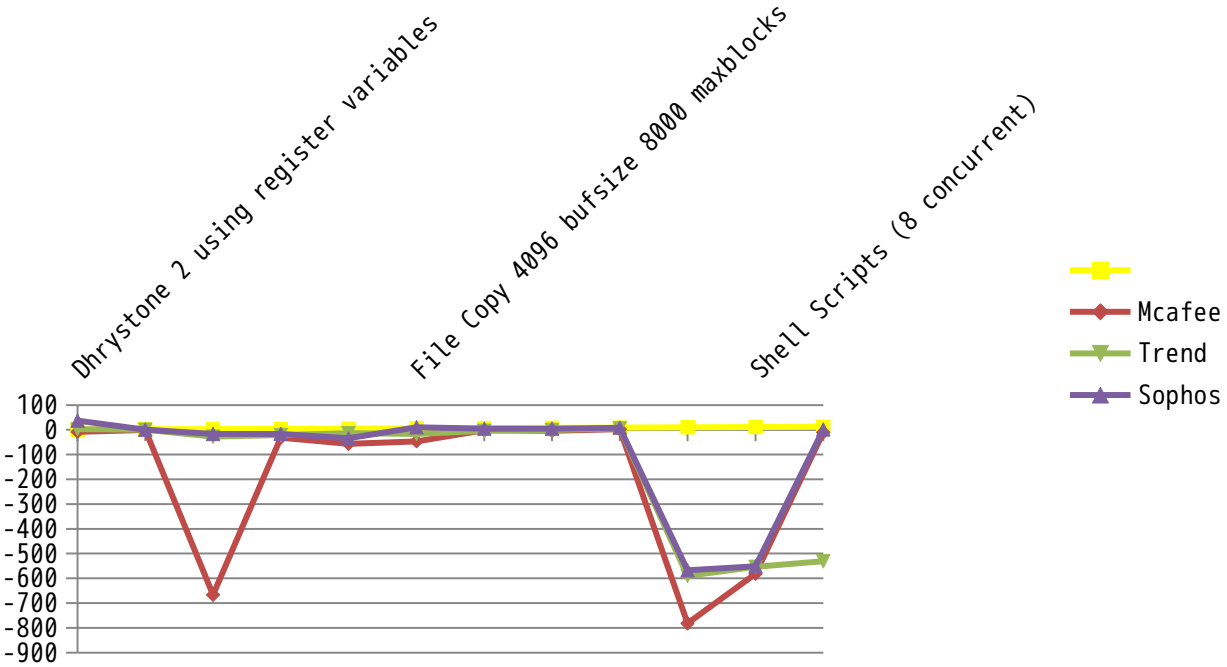
Benchmark Run: 2 CPUs; 1 parallel process



Test	Mcafee	Trend	Sophos
Dhrystone 2 using register variables	-2.14	0.3	10.34
Double-Precision Whetstone	0.38	-0.26	-0.48
Execl Throughput	-179.26	-15.58	-31.04
File Copy 1024 bufsize 2000 maxblocks	-22.12	-8.28	-25.52
File Copy 256 bufsize 500 maxblocks	-9.22	-2.58	-13.68
File Copy 4096 bufsize 8000 maxblocks	-22.16	-25.86	-14
Pipe Throughput	2.44	-1.88	1.92
Pipe-based Context Switching	1.48	5.06	3.28
Process Creation	55.68	54.82	55.2
Shell Scripts (1 concurrent)	-524.44	-446.96	-343.74

Shell Scripts (8 concurrent)	-625.92	-546.56	-543.2
System Call Overhead	-2.02	-258.28	-1.36

Benchmark Run: 2 CPUs; 2 parallel processes



Test	Mcafee	Trend	Sophos
Dhrystone 2 using register variables	-7.74	2.14	36.84
Double-Precision Whetstone	-0.24	0.18	0.18
Execl Throughput	-667.12	-27.16	-16.94
File Copy 1024 bufsize 2000 maxblocks	-31.64	-21.12	-17.2
File Copy 256 bufsize 500 maxblocks	-56.4	-13.64	-34.6
File Copy 4096 bufsize 8000 maxblocks	-46.32	-17.1	9.72
Pipe Throughput	-1.58	-3.94	4.54
Pipe-based Context Switching	-3.7	-0.9	5.26
Process Creation	3.06	5.66	8.4
Shell Scripts (1 concurrent)	-781.92	-590.42	-567.3
Shell Scripts (8 concurrent)	-581.62	-553.94	-551
System Call Overhead	-10.72	-531.22	1.24

UnixBench の各項目が示す概略は以下のようになります。

- **Dhrystone 2 using register variables**
  Dhrystone ベンチマークと呼ばれる整数演算処理のベンチマークになります。
- **Double-Precision Whetstone**
  Whetstone というベンチマークツールを使用した、浮動小数演算処理の性能のベンチマークになります。
- **Execl Throughput**
  execl 関数を実行して、システムコール処理性能をベンチマークします。
- **File Copy 1024 bufsize 2000 maxblocks**
  ファイルのコピーを繰り返すテストで、2MByte のファイルを 1024Byte ごとに処理します。
- **File Copy 256 bufsize 500 maxblocks**
  ファイルのコピーを繰り返すテストで、500KByte のファイルを 256Byte ごとに処理します。
- **File Copy 4096 bufsize 8000 maxblocks**
  ファイルのコピーを繰り返すテストで、8MByte のファイルを 4096Byte ごとに処理します。
- **Pipe Throughput**
  512Byte のデータのパイプ処理を繰り返しスループットをテストします。
- **Pipe-based Context Switching**
  2 つのプロセス間で更新される値をパイプで渡すことで、OS と CPU の処理性能をみます。
- **Process Creation**
  プロセスのフォークを繰り返すことで、OS と CPU の処理性能をみます。
- **Shell Scripts (1 concurrent)**
  sort、grep などのテキスト処理を繰り返すシェルスクリプトを実行することで、CPU の処理性能をみます。
- **Shell Scripts (8 concurrent)**
  上記の「1 concurrent」のシェルスクリプトを 8 個同時に実行することで、CPU の処理性能を見ます。
- **System Call Overhead**
  getpid()システムコールを繰り返し実行することで、OS と CPU の処理性能をみます。

III– 1– 2–3　考察

ホワイトペーパー第一部（用語説明）でも解説したとおり、AntiVirus のオンアクセススキャンは、通常 Read/Write/Execute などのシステムコールをフックして、アクセス先のファイルのスキャン処理を行います。そのため、グラフを見て分かる通り、処理が増えるため全体の数値が悪くなるのは理論上当然ですが、特に

- **Execl Throughput**
- **File Copy *** bufsize *** maxblocks**
- **Process Creation**
- **Shell Scripts (8 concurrent)**

など、sys_read/sys_write/sys_exec のシステムコールが発生するテストに於いて、通常のシステムに比べて一段と数値が悪くなっています。

- **System Call Overhead**

に関しては、getpid()だけなので本来数値が悪くならないはずですが（Sophos, Mcafee）、Trend だけは数値が悪くなっているため、getpid()を実行する際になんらかの処理を行っているものと推定されます。

その他の純粋にＣＰＵ内だけの処理

- **Dhrystone 2 using register variables**
- **Double-Precision Whetstone**
- **Pipe Throughput**

に関しては、数値上大きな変動がみられません。

このため、オンアクセススキャンを有効にしている場合には、特にファイルアクセスやプロセス実行時など、システムコールを使用する際にオーバーヘッドが掛かるということがわかります。

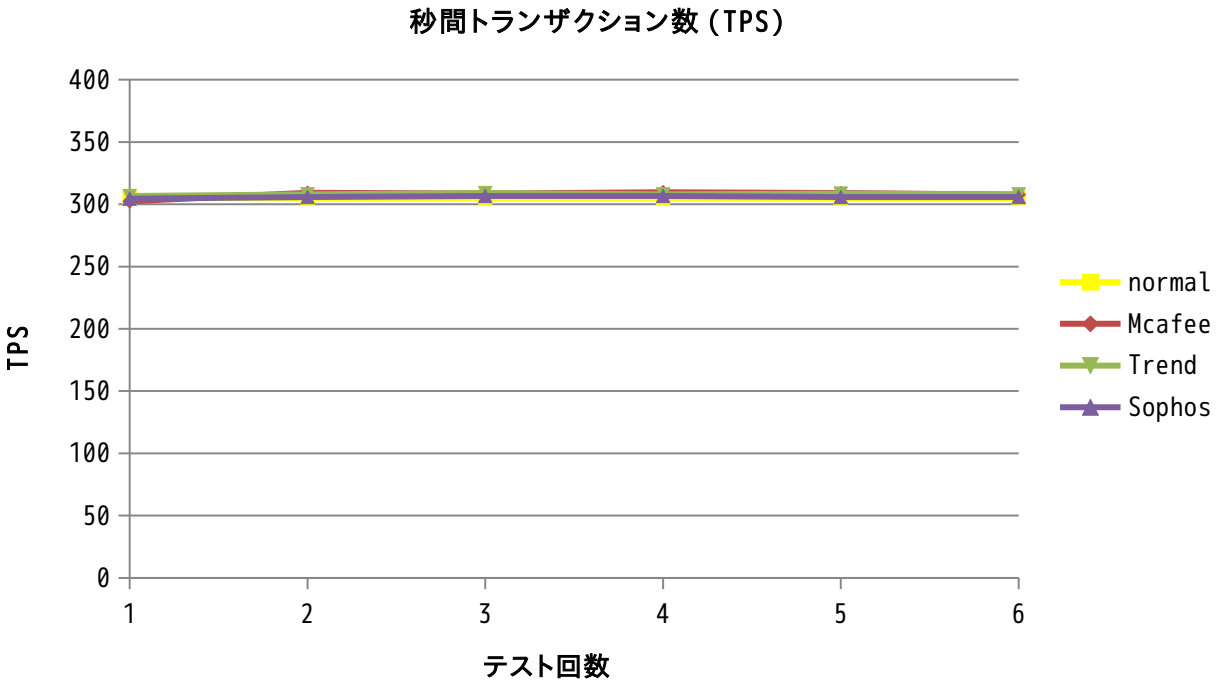
III – 1 - 3 SysBench 結果

下記の SysBench スクリプトを用いて、MariaDB の性能を測定します。

```
#!/bin/sh

num=5
i=0

while [ $i -lt $num ]; do
sysbench --test=oltp --db-driver=mysql --oltp-table-size=10000 \
--mysql-password=[パスワード] --num-threads=1 --max-requests=0 \
--max-time=60 --oltp-read-only=off run >> mysql_$1.log 2>&1

i=`expr $i + 1`
done
```

一般的に、DB は TPS(トランザクション毎秒)で性能を測るため、秒間当たりの処理トランザクション数（sysbench の transactions:の項）を性能の指標として使用します。

III- 1- 3-1　MariaDB の処理性能



	normal	Sophos	Trend	Mcafee
単位：　TPS(トランザクション毎秒)	304.67	304.57	306.67	302.45
	306.18	305.78	308	309.25
	305.29	306.74	308.96	308.65
	306.62	306.61	307.9	309.71
	307.17	305.87	308.62	308.98
平均	305.986	305.914	308.03	307.808

III- 1- 3-2　MariaDB の処理性能の考察

DB の処理性能を表す TPS(トランザクション毎秒)を計測すると、AntiVirus を入れない場合には約 306TPS となります。各社の AntiVirus 製品をインストールした後でも、凡そ 305-308TPS の間で秒間のトランザクションは処理できており、AntiVirus をインストールしたことによる DB の性能劣化は見られないことがわかります。

III – 2 オンデマンドスキャン

スキャン対象として、Windows2008 の C:\Users(ファイル数 1573、サイズ 643MB)をコピーしたフォルダを Linux 上に用意します。

また、スキャンオプションとしては

- 圧縮ファイルのスキャン無し
- 再帰的スキャン（サブディレクトリの中身もスキャン）

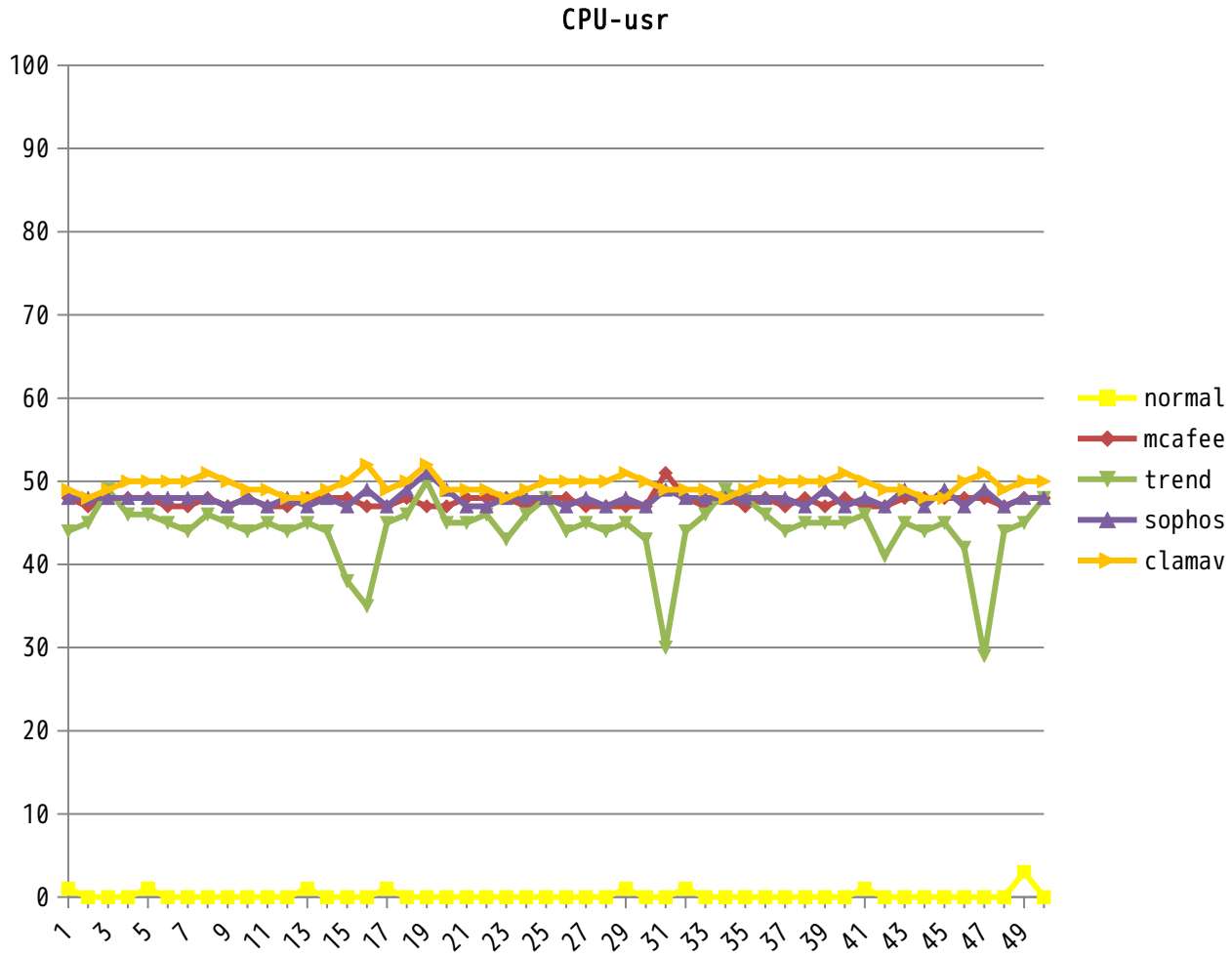
を選んでいます。

また、性能試験の項目でも説明したとおり、オンアクセススキャンは敢えて無効にし、純粋にオンデマンドスキャンがシステムに及ぼす影響を測定しています。

テスト対象となる AntiVirus 製品は、オンアクセススキャンのテストで使用した 3 製品に加えて、OSS 製品である clamav を追加しています。

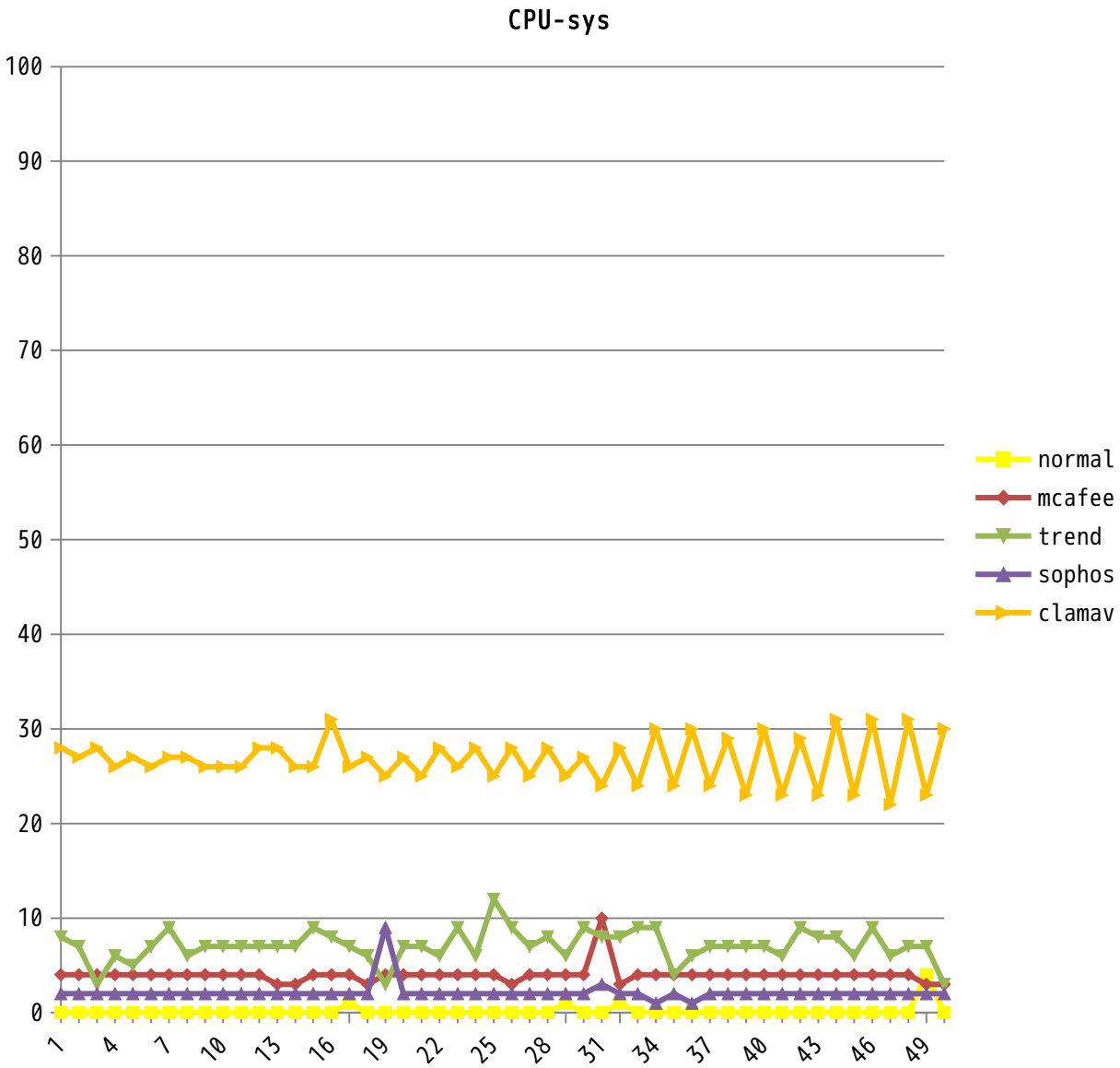
III – 2 - 1 vmstat 結果

III – 2– 1– 1 CPU



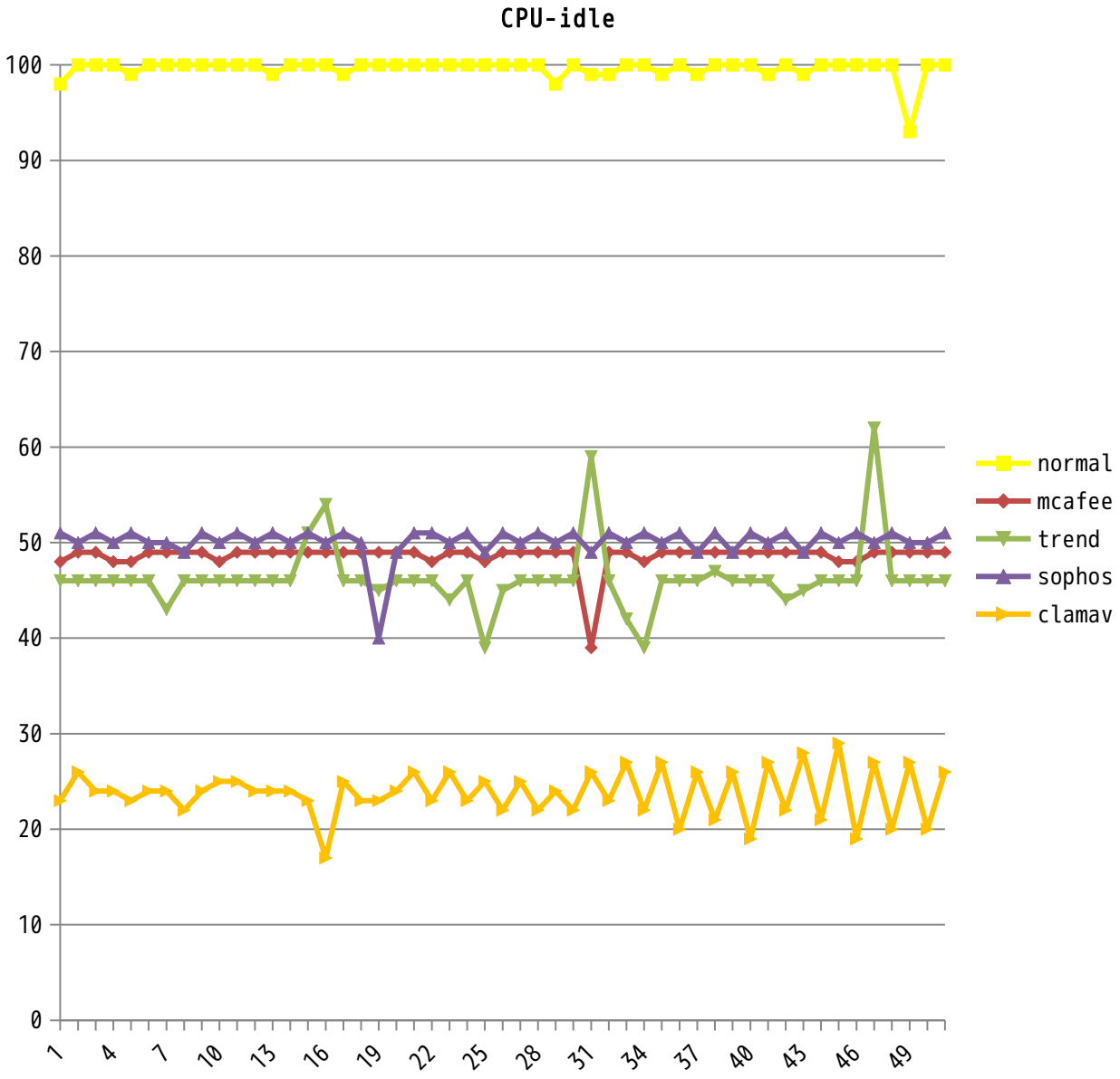
代表値

usr				
normal	mcafee	trend	sophos	clamav
1	48	44	48	49
0	47	45	48	48
0	48	49	48	49
0	48	46	48	50



代表値

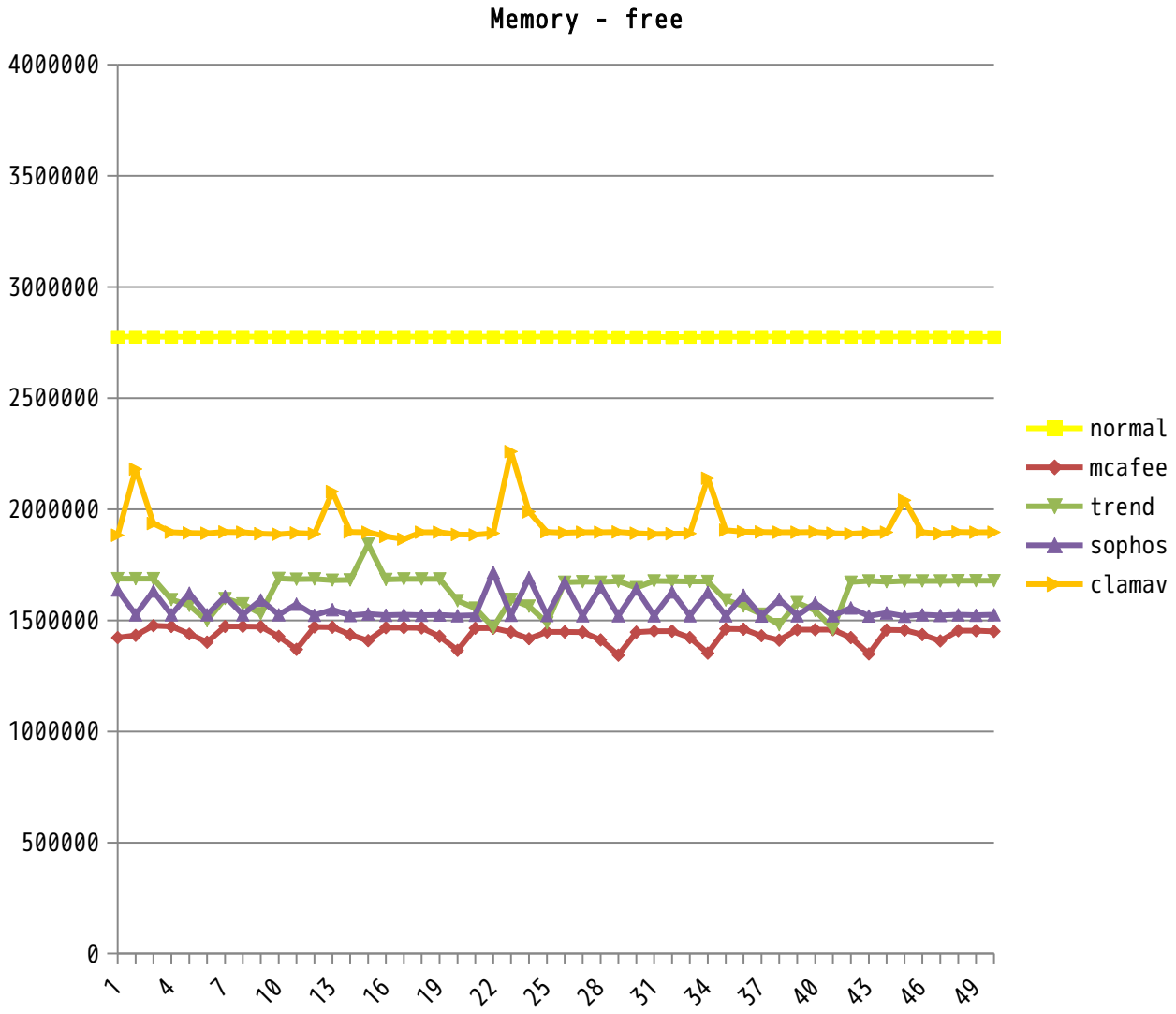
sys				
normal	mcafee	trend	sophos	clamav
0	4	8	2	28
0	4	7	2	27
0	4	3	2	28
0	4	6	2	26



代表値

id				
normal	mcafee	trend	sophos	clamav
98	48	46	51	23
100	49	46	50	26
100	49	46	51	24
100	48	46	50	24

III – 2– 1– 2 Memory



代表値

free				
normal	mcafee	trend	sophos	clamav
2776160	1421788	1686720	1636856	1883072
2776144	1431912	1687068	1525476	2181008
2776144	1475632	1686912	1632656	1935296
2776176	1473188	1593420	1525040	1896288
2775756	1438360	1566704	1622472	1892988

III – 2– 1– 3 考察

vmstat による計測を見る限り、オンデマンドスキャンを実施している状態では、CPU をスキャンジョブで使用するために一定以上の負荷がかかっていることがわかります。
CPU 性能の劣化度合は商用製品はほぼ同じですが、若干の差で
Trend < Mcafee, Sophos < clamav
となっており、やはり商用製品ならではのエンジン部分の作りこみが見られます。また、OSS の clamav も商用製品には及びませんが、性能劣化度合は大分近いものとなっています。

メモリに関しても、各 AntiVirus ベンダのスキャンエンジンなどで使用（通常は、アーカイブの展開が発生する可能性を考えて、エンジン部分である程度のメモリ量を確保しています）が発生するため、メモリの Free サイズなどは減少しています。
そのため、メモリの Free サイズに関しては、
Normal > Mcafee(1.3GB 程減少)> Trend,Sophos (1.1GB 程減少) > clamav (850MB 程減少)
となっており、メモリの使用サイズに関しては clamav の方が少なめになっています。

III – 2 - 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。

III – 2– 2– 1 総合スコア（System Benchmarks Index Score）

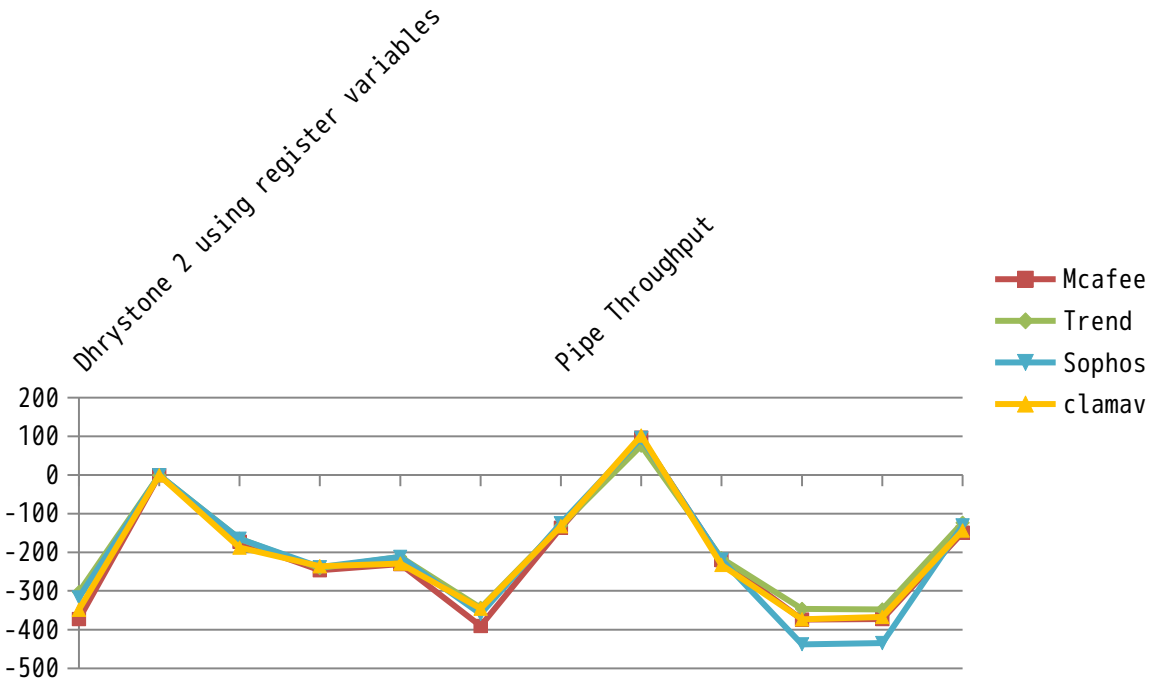
	Mcafee	Trend	Sophos	ClamAV
Benchmark Run: 2 CPUs 1 parallel process:	-179.64	-166.56	-183.42	-177.86
Benchmark Run: 2 CPUs; 2 parallel processes	-265.96	-318.74	-336.36	-360

総合スコアを見た場合には、
1 parallel process の場合には Trend<ClamAV<Mcafee<Sophos の順で、
2 parallel process の場合には Mcafee<Trend<Sophos<ClamAV の順で
AntiVirus ソフトウェアをインストールする前と比べて性能が劣化していきます。

III- 1- 2- 2　各テスト項目ごとのスコア

各項目の詳細は III-1-2-2 に準じます。

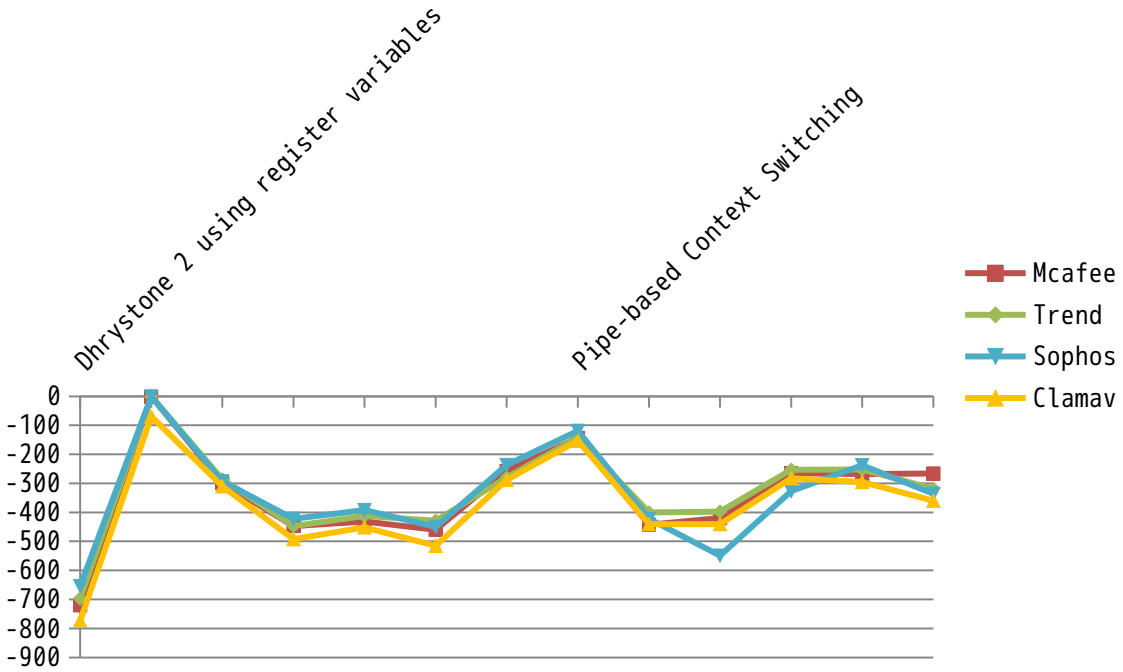
Benchmark Run: 2 CPUs; 1 parallel process



Test	Mcafee	Trend	Sophos	Clamav
Dhrystone 2 using register variables	-372.96	-303.3	-317.02	-348.66
Double-Precision Whetstone	-1.08	-0.92	-0.98	-1.26
Execl Throughput	-172.86	-165.04	-165.22	-188.18
File Copy 1024 bufsize 2000 maxblocks	-246.54	-241	-238.64	-236.36
File Copy 256 bufsize 500 maxblocks	-230.68	-212.42	-212.12	-228.88
File Copy 4096 bufsize 8000 maxblocks	-390.58	-343.78	-359.66	-345.98
Pipe Throughput	-136.98	-131.72	-125.24	-132.66
Pipe-based Context Switching	96.1	75.34	95.26	101.94
Process Creation	-220.56	-215.4	-218.92	-232.7
Shell Scripts (1 concurrent)	-374.04	-346.46	-437.94	-373.14
Shell Scripts (8 concurrent)	-372.88	-347.6	-435.06	-367.26

System Call Overhead	-149.02	-123.86	-130.86	-143.94

Benchmark Run: 2 CPUs; 2 parallel processes



Test	Mcafee	Trend	Sophos	Clamav
Dhrystone 2 using register variables	-720.46	-697.3	-654.06	-774.18
Double-Precision Whetstone	-0.94	-0.88	-0.8	-69.66
Execl Throughput	-299.74	-286.38	-293.16	-310.52
File Copy 1024 bufsize 2000 maxblocks	-446.96	-447.56	-422.04	-492.74
File Copy 256 bufsize 500 maxblocks	-431.78	-412.48	-391.92	-452.22
File Copy 4096 bufsize 8000 maxblocks	-460.22	-428.88	-450.32	-515.34
Pipe Throughput	-257.88	-280.08	-236.94	-288.5
Pipe-based Context Switching	-144.12	-142.16	-118.88	-152.94
Process Creation	-442.9	-400	-423.02	-440.58
Shell Scripts (1 concurrent)	-419.9	-397.9	-549.62	-441.1
Shell Scripts (8 concurrent)	-265.7	-253.58	-327.28	-282.74
System Call Overhead	-267.6	-252.18	-237.4	-295.84

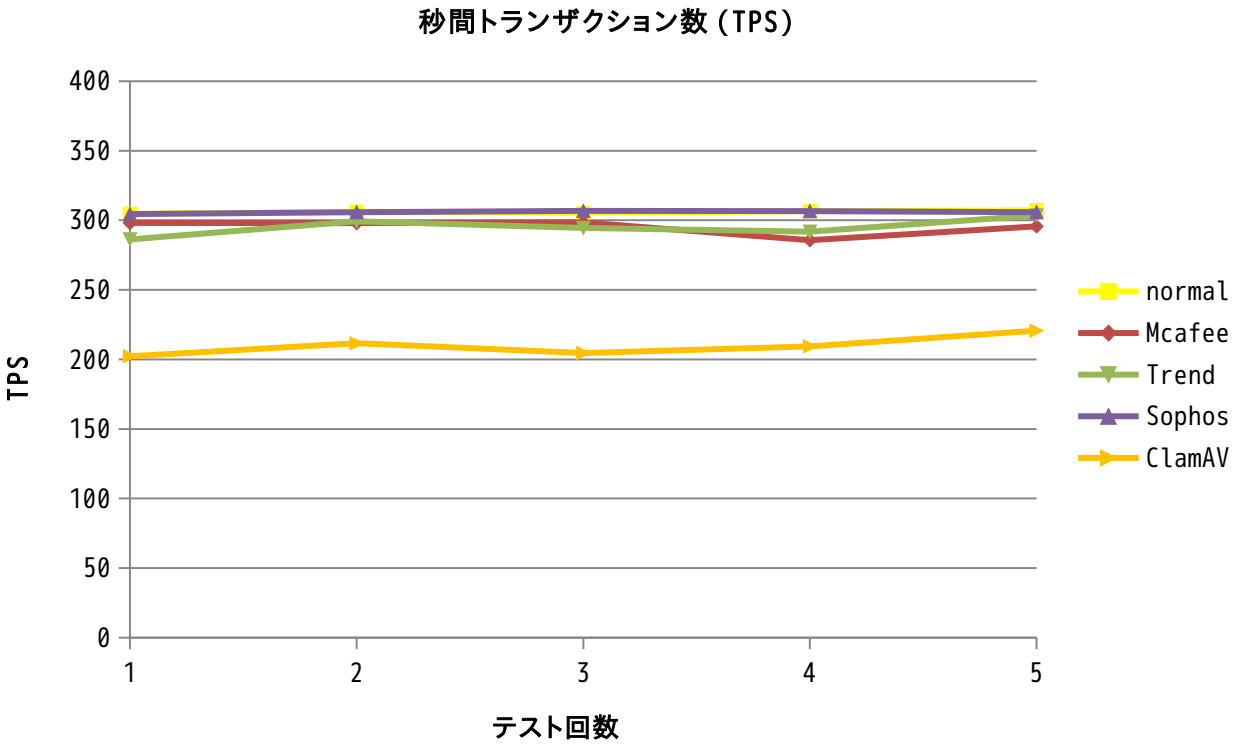
III- 2- 2-3　考察

AntiVirus のオンデマンドスキャンにより、当然のように処理が増えるため全体の数値が悪くなっています。特に CPU の機能劣化が顕著で、次にファイルアクセス、シェルの実行と機能が劣化しています。

このため、オンデマンドスキャンを実施している場合には、CPU 処理やファイルアクセスが必要な処理は特にオーバーヘッドが掛かるということがわかります。

III – 2 - 3 SysBench 結果

III-2- 3-1 MariaDB の処理性能



	normal	Mcafee	Trend	Sophos	ClamAV
単位： TPS(トランザクション毎秒)	304.67	298.13	286.34	304.57	202.26
	306.18	297.92	299.24	305.78	211.57
	305.29	298.54	294.55	306.74	204.53
	306.62	285.73	291.85	306.61	209.41
	307.17	295.63	303.5	305.87	220.61
平均	305.986	295.19	295.096	305.914	209.676

III- 2- 3-2 MariaDB の処理性能の考察

DB の処理性能を表す TPS(トランザクション毎秒)を計測すると、各社の AntiVirus 製品でスキャンを行った際には、Mcafee, Trend に関しては若干(10TPS 程度)の性能の低下がみられます。Sophos はほぼ性能は変わりませんが、ClamAV の場合にはかなり(100TPS 程度)の性能劣化が見られます。この結果から、AntiVirus をインストールした

システム上のアプリケーションに関しては、スキャンはある程度の性能劣化の影響を及ぼすことがわかります。

結論

本ホワイトペーパーでは、代表的な AntiVirus ソフトがシステムに及ぼす影響をテストしました。
結果としては

1. 代表的な AntiVirus ソフトウェアをインストールした場合、定常状態（特にスキャンなどを行わない）状態では、CPU にはあまり性能の劣化は見られませんでした。メモリに関しては、700MB 程度の使用量の増加が測定されました。
2. システム上でアプリケーションが動作する場合、ファイルへのアクセスやシステムコールを多く使用しているほど、アプリケーションに対して性能の劣化があることがわかりました。
3. MariaDB などには、AntiVirus ソフトは定常状態ではほとんど影響を与えないことがわかりました。
4. スキャンを行っている際には、CPU・メモリに関しての使用率が上がるため、システムに負荷がかかることがわかりました。
5. スキャンを行っている状態では、MariaDB の性能にも若干の劣化が発生することがわかりました。
6. OSS である clamav は、主要な商用 AntiVirus 製品に比べて、システムに及ぼす影響が若干大きいことがわかりました。しかし、メモリの使用率などの若干のアドバンテージがあることもわかりました。

これらの結果から、以下のような結論が導き出せます。

1. **各サーバに AntiVirus 製品をインストールする際は、定常状態・スキャンの実施状態共に、メモリに影響を及ぼすため、メモリを多めに確保する必要がある。**
2. **通常の運用中にスキャンをなるべく行わないように設計することで、システムに及ぼす影響は最低限に抑えられる。**
3. **オンデマンドスキャンなどが走る際にはシステムに影響を及ぼすため、システム上で動いているアプリケーションの運用などを考え、スキャン中にレスポンスを必要とするような処理を避ける様にスケジュールを考える必要がある。また、オンデマンドスキャン実施時にその他のアプリケーションのジョブを避けることが出来るのであれば、OSS の clamav でも十分に使うことが出来る。**
4. **上記の点を考慮した設計を行えば、AntiVirus をインストールすることは、セキュリティを担保するために有益である。**

今後サイオステクノロジーでは **AntiVirus** の効果的な構築のノウハウ、運用方法などの技術資料を公開していきます。安全で安定した環境をご検討されている皆様の手助けとなれば幸いです。

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