

富士通社製 PRIMEQUEST 520 における
Sophos Anti-Virus 4.x for Linux 動作検証報告書

本レポートは2008年10月30日に貴社プラットフォームソリューションセンターで実施した Itanium プラットフォーム上における Sophos Anti-Virus 4.x for Linux の動作検証の方法および結果をまとめた書です。

1. はじめに

2008年8月より、当社製品 Sophos Anti-Virus 4.x for Linux は Itanium プラットフォームに対応致しましたが、今回の検証では、製品としての QA (品質検査) は既に完了していることを前提に、PRIMEQUEST 520 を用いて、運用的観点からの検証の実施結果を報告します。

2. 検証概要

運用上発生しうる、次の操作を行い、機能の動作状況を確認する。

- インストール
- IDE ファイル更新 (手動)
- インストール後のシャットダウンと起動
- 擬似ウイルスファイルの検知
- ログファイル作成
- アンインストール
- アンインストール後のシャットダウンと起動

3. 検証環境

(ア) 試験環境 1 (RHEL4.6)

- | | | |
|---|------|--|
| ① | HW: | PRIMEQUEST520 |
| ② | CPU: | Itanium2 1.42GHz x 4 (8 core) |
| ③ | MEM: | 64GB |
| ④ | HDD: | 36GB |
| ⑤ | OS: | Red Hat Enterprise Linux 4.6(kernel-2.6.9-69.EL) |
| ⑥ | SW: | Sophos Anti-Virus 4.x for Linux(Itanium IA64 版 Version 4.35.0) |
| ⑦ | IDE: | ides.zip(2008/10/29 午後 2 時頃 Sophos サイトより取得) |

(イ) 試験環境 2 (RHEL5.2)

- | | | |
|---|------|--|
| ① | HW: | PRIMEQUEST520 |
| ② | CPU: | Itanium2 1.42GHz x 4 (8 core) |
| ③ | MEM: | 64GB |
| ④ | HDD: | 73GB |
| ⑤ | OS: | Red Hat Enterprise Linux 5.2(kernel-2.6.18-92.el5) |
| ⑥ | SW: | Sophos Anti-Virus 4.x for Linux(Itanium IA64 版 Version 4.35.0) |
| ⑦ | IDE: | ides.zip(2008/10/29 午後 2 時頃 Sophos サイトより取得) |

4. 検証結果

	検証項目数		結果
	設定数	実施数	
試験環境 1 (RHEL4.6)	7	7	良好
試験環境 2 (RHEL5.2)	7	7	良好

5. 検証詳細

試験環境 1 (RHEL4.6)

	試験項目	試験内容	確認方法	結果	備考
1	インストール	root アカウントで対象ホストにログインし、SAV for Linux 4.x のインストールを行う。問題なくインストールが終了することを確認する。	インストールの直後に下記のコマンドを実行。 # echo \$0 戻り値が「0」であった場合、インストールが問題なく行われたことを意味する。	良好	戻り値：0を確認
2	IDE ファイル更新	手でIDE ファイル更新を行い、問題なく、更新が行われたことを確認する。	一時ディレクトリに ides.zip を解凍し、解凍された IDE ファイルを /usr/local/sav ディレクトリにコピーする。その後、下記のコマンドを用いて IDE 数を確認する # sweep -v	良好	インストール直後の IDE 数 535485 が、更新後、536403 になったことが確認された。
3	インストール後のホスト再起動 (※)	インストール後も問題なくホストの再起動が行えることを確認する。	reboot コマンドを用いて再起動を行い、起動後、/var/log/messages に関連するエラーがないかを確認する。	良好	
4	擬似ウイルス検知	テストウイルス eicar.com が問題なく検知できることを確認する。	試験用の一時ディレクトリ (/root/test) を作成し、そこに eicar.com をコピーする。その後、下記のコマンドを用いてウイルス検索を行い、問題なく検知されることを確認する。 # sweep /root/test	良好	問題なく、eicar.com が検知できることが確認された。
5	ログファイル作成	オプションを用いた場合、ウイルス検索時のログファイルが問題なく作成されることを確認する。	「4」と同様に下記のコマンドを実行し、ログファイルが作成され、また、ログファイルの内容が正しいことを確認する。 # sweep -p=scan_result.log /root/test	良好	指定した名前のログファイル scan_result.log が作成され、内容が正しいことが確認された。
6	アンインストール	問題なくアンインストールが行われることを確認する。	手動にて下記を実行する 1. /usr/local/bin/sweep を削除 2. /usr/local/lib/libsavi* を削除 3. /usr/local/man/man1/sweep.1 を削除 4. /usr/local/sav ディレクトリを削除 5. /etc/sav.conf を削除	良好	

7	アンインストール後のホスト再起動 (※)	アンインストール後も問題なくホストの再起動が行えることを確認する	<code>reboot</code> コマンドを用いて再起動を行い、起動後、 <code>/var/log/messages</code> に関連するエラーがないかを確認する。	良好	
---	-------------------------	----------------------------------	---	----	--

※インストール後、アンインストール後のシャットダウンおよび起動は、それぞれのオペレーションの後も、正常に動作することの確認が目的であり、実際にインストールあるいはアンインストール後に機器を再起動する必要はありません。

試験環境 2 (RHEL5.2)

	試験項目	試験内容	確認方法	結果	備考
1	インストール	root アカウントで対象ホストにログインし、SAV for Linux 4.x のインストールを行う。問題なくインストールが終了することを確認する。	インストールの直後に下記のコマンドを実行。 # echo \$0 戻り値が「0」であった場合、インストールが問題なく行われたことを意味する。	良好	戻り値：0を確認
2	IDE ファイル更新	手で IDE ファイル更新を行い、問題なく、更新が行われたことを確認する。	一時ディレクトリに <code>ides.zip</code> を解凍し、解凍された IDE ファイルを <code>/usr/local/sav</code> ディレクトリにコピーする。その後、下記のコマンドを用いて IDE 数を確認する # sweep -v	良好	インストール直後の IDE 数 535485 が、更新後、536403 になったことが確認された。
3	インストール後のホスト再起動 (※)	インストール後も問題なくホストの再起動が行えることを確認する。	<code>reboot</code> コマンドを用いて再起動を行い、起動後、 <code>/var/log/messages</code> に関連するエラーがないかを確認する。	良好	
4	擬似ウイルス検知	テストウイルス <code>eicar.com</code> が問題なく検知できることを確認する。	試験用の一時ディレクトリ (<code>/root/test</code>) を作成し、そこに <code>eicar.com</code> をコピーする。その後、下記のコマンドを用いてウイルス検索を行い、問題なく検知されることを確認する。 # sweep /root/test	良好	問題なく、 <code>eicar.com</code> が検知できることが確認された。
5	ログファイル作成	オプションを用いた場合、ウイルス検索時のログファイルが問題なく作成されることを確認する。	「4」と同様に下記のコマンドを実行し、ログファイルが作成され、また、ログファイルの内容が正しいことを確認する。 # sweep -p=scan_result.log /root/test	良好	指定した名前のログファイル <code>scan_result.log</code> が作成され、内容が正しいことが確認された。
6	アンインストール	問題なくアンインストールが行われることを確認する。	手動にて下記を実行する 1. <code>/usr/local/bin/sweep</code> を削除 2. <code>/usr/local/lib/libsave*</code> を削除 3. <code>/usr/local/man/man1/sweep.1</code> を削除 4. <code>/usr/local/sav</code> ディレクトリを削除 5. <code>/etc/sav.conf</code> を削除	良好	

7	アンインストール 後のホスト再起動 (※)	アンインストール後も問題なくホス トの再起動が行えることを確認する	reboot コマンドを用いて再起動を行い、起動 後、/var/log/messages に関連するエラーがな いかを確認する。	良好	
---	---------------------------------	--------------------------------------	--	----	--

※インストール後、アンインストール後のシャットダウンおよび起動は、それぞれのオペレーションの後も、正常に動作することの確認が目的であり、実際にインストールあるいはアンインストール後に機器を再起動する必要はありません。

6. おわりに

本検証のすべての項目において、結果は良好であり、問題となる事象は確認されませんでした。

7. 問い合わせ先

電話番号 : 045-227-1800 (代表)

Email : sales@sophos.co.jp