

Sophos Server Protection SAV for Linux

Sophos Server Protectionとは

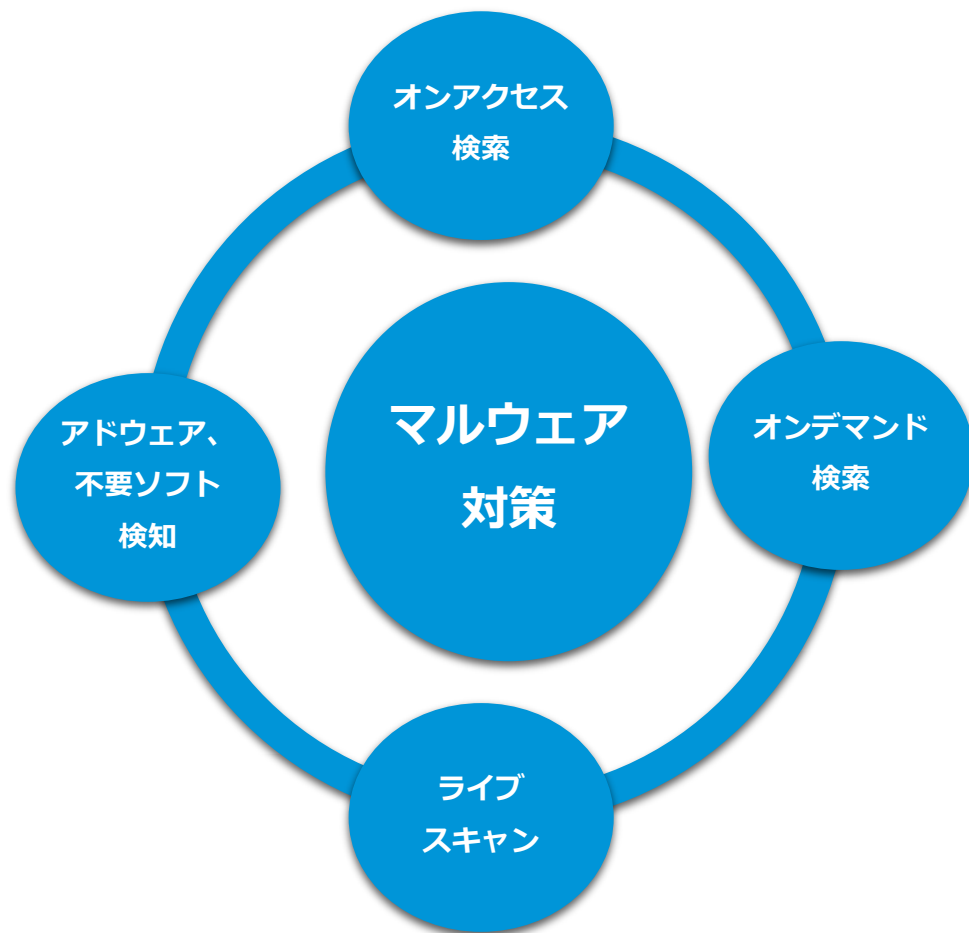
- Sophos Server Protection は、サーバー向けマルウェア対策製品であり、様々な脅威からサーバーを保護します。Linux をサポートし、マルチプラットフォーム対応を特長とする製品です。
 - Genotype®(遺伝子)技術によるプロアクティブな脅威の検出
 - Decision Caching™による高速化（UNIXは非対応）
 - SophosLabs によるリアルタイムのライブスキャン（UNIXは非対応）
 - Linux上でもWindows系マルウェアを検出
 - 多様な対応オペレーティングシステム
 - Red Hat, Oracle Linux, SUSE, CentOS , Ubuntu , Amazon Linux

Server Protectionで利用可能な機能

	Server Protection Enterprise			Central Server Protection Advanced		Central Server Protection Standard	
	Windows	Linux	UNIX	Windows	Linux	Windows	Linux
オンアクセス検索	○	○	×	○	○	○	○
オンデマンド検索	○	○	○	○	○	○	○
HIPS(振る舞い検知)	○	×	×	○	×	○	×
MTD	×	×	×	○	○	×	×
Live Protection	○	○	×	○	○	○	○
Web Protection	○	×	×	○	×	○	×
ダウンロードレピュテーション	○	×	×	○	×	○	×
デバイスコントロール	○	×	×	○	×	×	×
アプリケーションコントロール	○	×	×	○	×	×	×
タンパープロテクション	○	×	×	○	×	○	×
データコントロール	○	×	×	×	×	×	×
パッチアセスメント	○	×	×	×	×	×	×
Webコントロール	○	×	×	○	×	×	×
クライアント ファイアウォール	×	×	×	×	×	×	×
サーバーロックダウン	×	×	×	○	×	×	×

Linux Server マルウェア対策

Linuxのウイルス対策には以下があります。



オンアクセス検索

リアルタイムでウイルスを検知します。

オンデマンド検索

スケジュールもしくは手動でウイルスを検知します。

ライブスキャン

怪しいプログラムを発見したとき、ソフォスのサーバーに自動問い合わせし、最新の定義ファイルで検知できるか確認します。

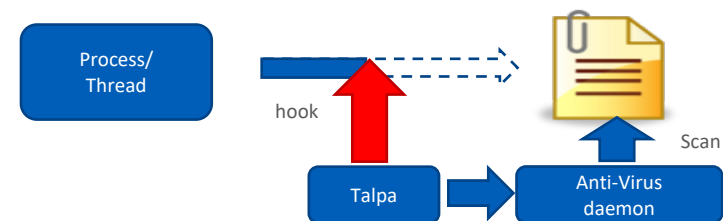
アドウェア、不要ソフトの検知

アドウェアやスパイウェアと呼ばれる、ウイルスではないが業務の邪魔をするプログラムを検知します。

Linuxオンアクセス検索TalpaとFanotify

- Talpa

- オンアクセス検索を実行するためのファイルのOpen、Closeを監視、制御をおこなうカーネルフックモジュール。
- オープンソースでソフォスが開発。（他社ではDazukoの利用が多い）
- サポートOSについては、カーネルバージョンごとにTalpaバイナリが提供され、インストールおよびアップデート時にカーネルに組み込まれる。
- 非サポートOSおよび改造カーネルについては、GCCの開発環境であればインストールおよびアップデート時に自動でコンパイルされオンアクセス検索が可能。（リーズナブルエンデバーサポート扱い）

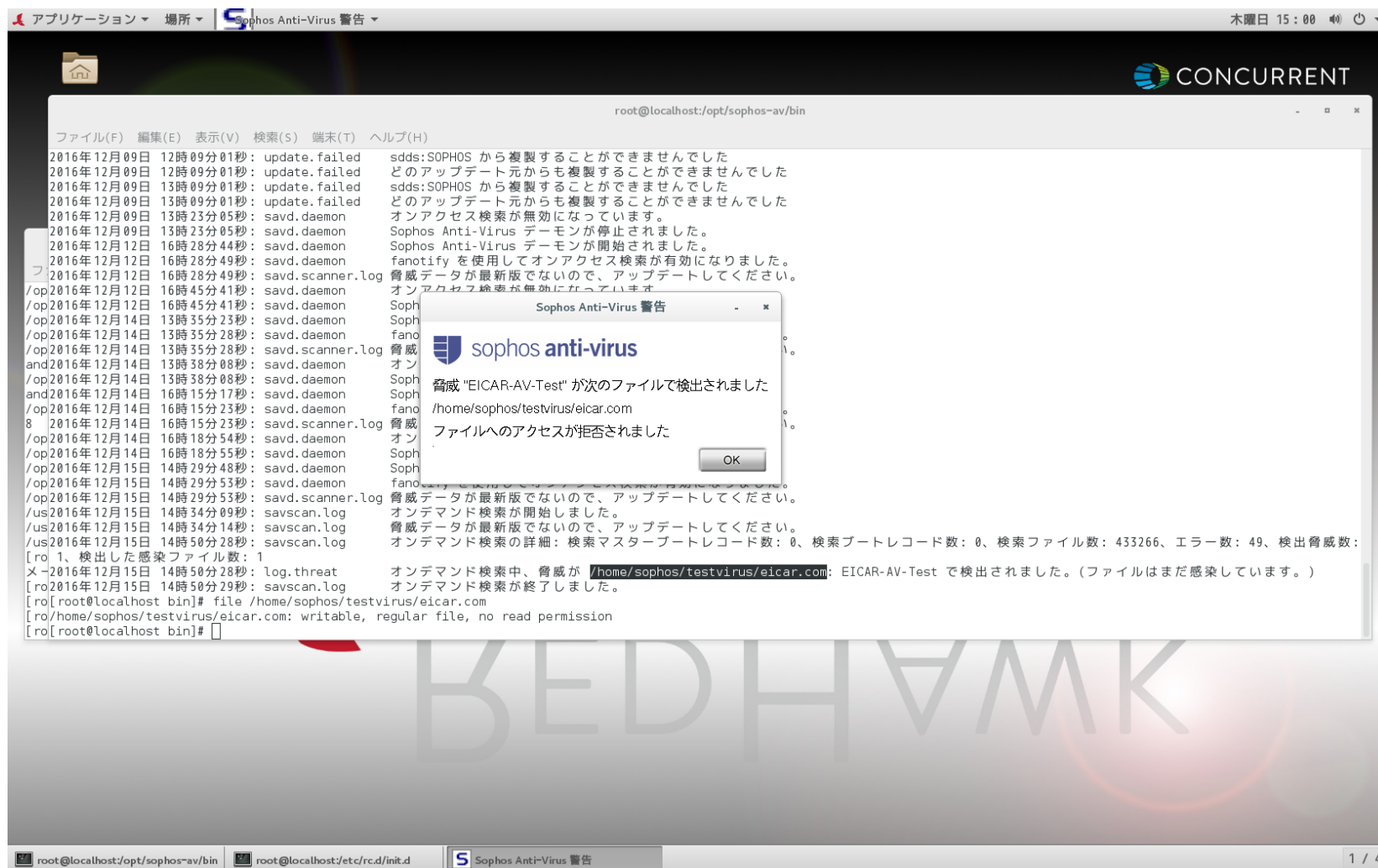


- Fanotify

- OS標準で用意されているファイルのOpen、Closeを監視、制御をおこなうカーネルモジュール。
- SAV for Linux Ver9で利用可能
- カーネル 2.6.38以降で実装され、RHELではVer7以降で利用可能。

RedHawk7.2上のオンアクセス検索結果

ウィルスファイルをアクセスすると、(この例では、fileコマンド)ポップアップが現れる。



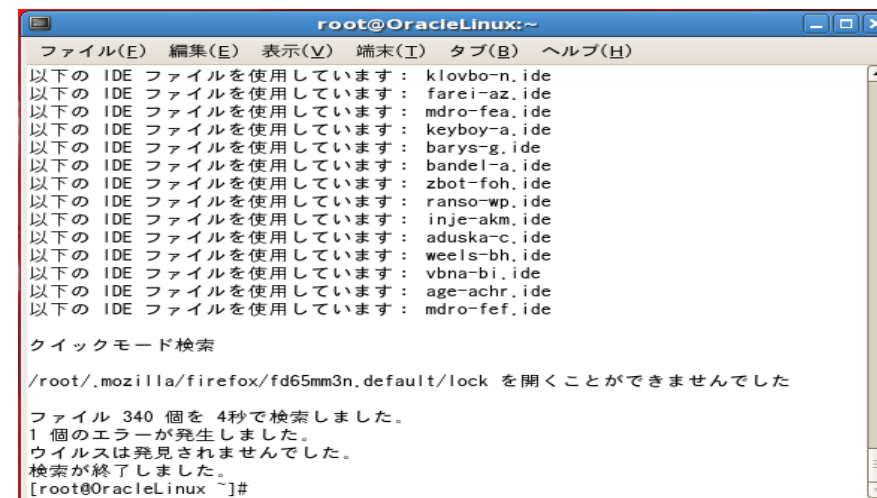
Linux のオンデマンド検索

- Sophos Anti-Virus for Linuxでは、スケジュールスキャンやコマンド(savscan)を利用して随時スキャンを行うことが可能です。



```
root@RHEL77:/opt/sophos-av/doc
ファイル(F) 編集(E) 表示(V) 検索(S) 端末(T) ヘルプ(H)
# 特定のファイルやディレクトリの除外指定は、パスの短い検索指定より優先されます。
# 拡張子が除外されたファイルは、他のオプションの設定内容に関わらず検索されません。
# アーカイブファイル内の検索が無効化されている場合、他のオプションの設定内容に関わらず、アーカイブファイルは検索されません。
# アーカイブファイル内の検索が有効化されている場合、検索の対象に指定されたディレクトリ、またはデバイスの種類に基づいて検索の対象に指定されたディレクトリ内のアーカイブファイルのみが検索されます。
# 検索の対象から除外するファイルやディレクトリの指定。
exclude=/home/users/ foo
exclude=/srv/meta
# 検索から除外するファイルの拡張子の指定。
excludeExtension=iso
excludeExtension=rpm
# アーカイブファイル内の検索の指定。
scanArchives=1
# 検索レベルの指定: normal|extensive (通常|詳細)。
scanLevel=normal
# 感染ファイルの駆除 (クリーンアップ) 試行の指定。
# 注: 駆除が可能とわかっている感染ファイルのみに対して駆除が試行されます。
# disinfect=enable|disable (有効化|無効化)
disinfect=enable
# 感染ファイルの駆除を実行できない、または無効化されている場合の対処方法の指定。
# threatAction=doNothing|delete (何もしない|削除する)
threatAction=doNothing
# 指定した日時に検索を実行するようスケジュール設定する (任意)。
# 検索を実行する曜日 (複数可) の指定。文字または数字で指定できます。
# 月曜日、水曜日および金曜日
day=monday
day=wednesday
day=5
# 検索を実行する時刻 (複数可) の指定。HH:MM という形式で指定してください。
# 1am および 6:30pm
time=01:00
time=18:30
```

クライアント側でのスケジュールスキャンの設定



```
root@OracleLinux:~
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
以下の IDE ファイルを使用しています: klovbo-n.ide
以下の IDE ファイルを使用しています: farei-az.ide
以下の IDE ファイルを使用しています: mdro-fea.ide
以下の IDE ファイルを使用しています: keyboy-a.ide
以下の IDE ファイルを使用しています: barys-g.ide
以下の IDE ファイルを使用しています: bandel-a.ide
以下の IDE ファイルを使用しています: zbot-foh.ide
以下の IDE ファイルを使用しています: ranso-wp.ide
以下の IDE ファイルを使用しています: inje-akm.ide
以下の IDE ファイルを使用しています: aduska-c.ide
以下の IDE ファイルを使用しています: weels-bh.ide
以下の IDE ファイルを使用しています: vbna-bi.ide
以下の IDE ファイルを使用しています: age-achr.ide
以下の IDE ファイルを使用しています: mdro-fef.ide

クイックモード検索

/root/.mozilla/firefox/fd65mm3n.default/lock を開くことができませんでした

ファイル 340 個を 4秒で検索しました。
1 個のエラーが発生しました。
ウイルスは見えませんでした。
検索が終了しました。
[root@OracleLinux ~]#
```

savscanコマンドを用いた手動スキャン