Sophos Server Protection
SAV for Linux

SOPHOS

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。

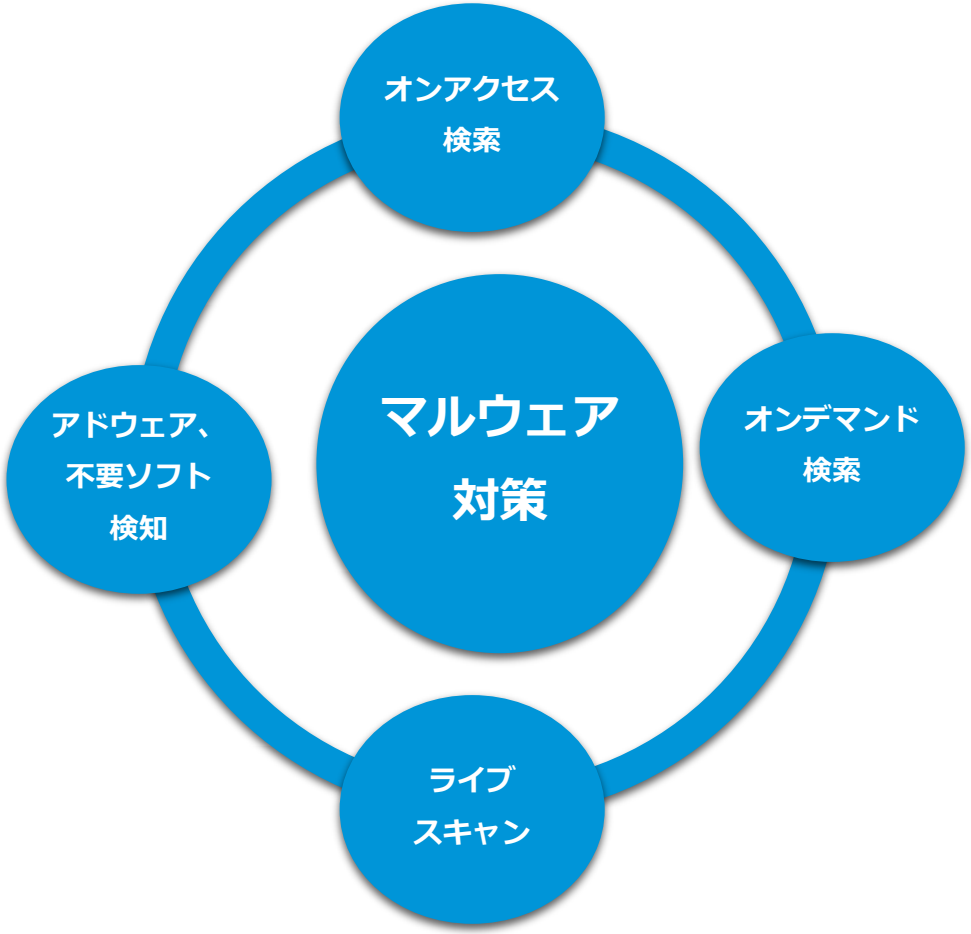
  - Genotype®(遺伝子)技術によるプロアクティブな脅威の検出
  - Decision Caching™による高速化（UNIXは非対応）
  - SophosLabs によるリアルタイムのライブスキャン（UNIXは非対応）
  - Linux上でもWindows系マルウェアを検出
  - 多様な対応オペレーティングシステム
    - Red Hat, Oracle Linux, SUSE, CentOS , Ubuntu , Amazon Linux

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 ファイアーウォール	×	×	×	×	×	×	×
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。

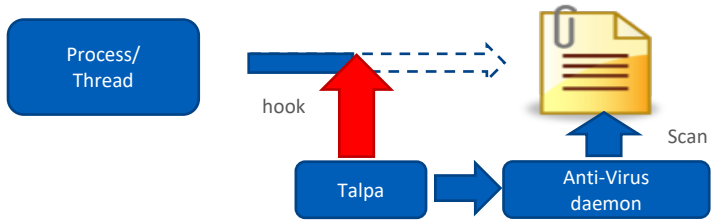
オンデマンド検索
スケジュールもしくは手動でウイルスを検知します。

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

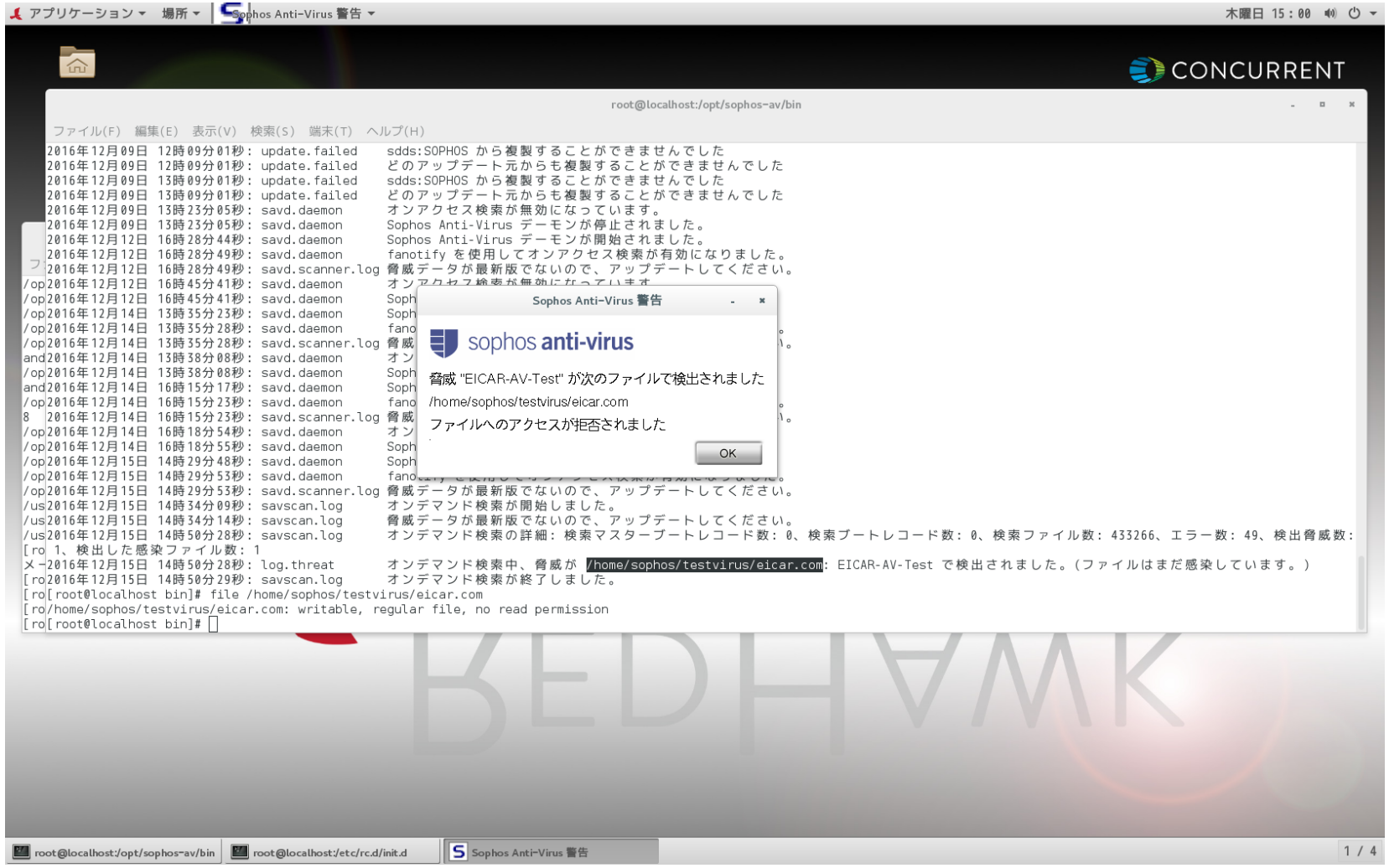
- Talpa
  - オンアクセス検索を実行するためのファイルのOpen、Closeを監視、制御をおこなうカーネルフックモジュール。
  - オープンソースでソフォスが開発。（他社ではDazukoの利用が多い）
  - サポートOSについては、カーネルバージョンごとにTalpaバイナリが提供され、インストールおよびアップデート時にカーネルに組み込まれる。
  - 非サポートOSおよび改造カーネルについては、GCCの開発環境であればインストールおよびアップデート時に自動でコンパイルされオンアクセス検索が可能。（リーズナブルエンデバーサポート扱い）



- 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。

クライアント側でのスケジュールスキャンの設定

savscanコマンドを用いた手動スキャン