

ClamAV Days クラムエーヴイデイズ

In the Internet, open source developers met. Their relation defense the net, and users selects their apps.

KOJIMA Hajime

kjm@rins.ryukoku.ac.jp

ClamAV って何?

- UNIX/Linux 用のアンチウイルスソフト
 - <http://www.clamav.net/>
- 内容物
 - ウィルススキャナ
 - スタンドアロン版 clamscan
 - デーモン版 clamd / clamdscan
 - シグネチャ更新用デーモン freshclam
 - milter デーモン clamav-milter
 - sigtool

開発

- 開発主体: ClamAV team
 - SourceFire に買収された
<http://www.sourcefire.com/products/clamav/>
 - 今のところは「パトロンがついた」程度の認識でよい？
- 開発は活発
 - 新たな機能追加もリリース毎に行われている
- セキュリティホールもときどき見つかる
 - リリース毎に fix されている

Clam AntiVirus - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

http://www.clamav.net/lang-pref/ja/ 甲南大学

セキュリティ マスメディア アンチウイルス PC 情報 F1 SSH Cygwin Cisco Extreme iconv ねた 宴会

Clam AntiVirus



Main Menu

- Home
- ClamAVについて
- サポート
- Download
- 貢献者
- ウイルス提供
- バグ報告
- 連絡先

News feeds

- [in the press](#) (9)
- [misc](#) (64)
- [security](#) (2)

About ClamAV™ [en] [jp] [de] [it] [es] [fr] [ru] [pl] [pt] [nl] [hu] [simp. cn] [trad. cn]

Clam AntiVirus is an open source (GPL) anti-virus toolkit for UNIX, designed especially for e-mail scanning on mail gateways. It provides a number of utilities including a flexible and scalable multi-threaded daemon, a command line scanner and advanced tool for automatic database updates. The core of the package is an anti-virus engine available in a form of shared library.[\(Read more...\)](#)

Latest releases

Latest [ClamAV™ stable release](#) is: 0.92.1
 Latest [ClamAV™ RC release](#) is: 0.93rc1
 Total number of signatures: 229303
 ClamAV Virus Databases:
[main.cvd](#) ver. 45 released on 09 Dec 2007 15:59 +0000

完了

McAfee SiteAdvisor

http://www.clamav.net/

特徴

- フリー
- 使い物になる
- 拡張できる

フリー

フリー

- ライセンス: GNU GPL version 2
 - ソースとバイナリを再配布できる
 - 改変可能、ただし改変版を公開する場合は改変部分のソースも要公開

フリーなので.....

- Windows 移植版
 - ClamWin: Cygwin を利用したもの
 - <http://www.clamwin.com/>
 - オンデマンドスキャンのみ
 - 安定して動作する
 - Moon Secure AntiVirus: ClamAV エンジンを利用した Windows ネイティブアプリ
 - <http://sourceforge.net/projects/moonav/>
 - オンアクセススキャンにも対応
 - 複数エンジン搭載
 - まだ安定していない？

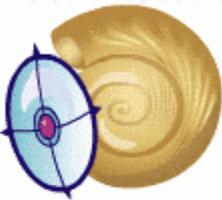
Free Antivirus for Windows - Open source GPL virus scanner - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

http://www.clamwin.com/ ClamWin

セキュリティ マスメディア アンチウイルス PC 情報 F1 SSH Cygwin Cisco Extreme iconv ねた

Free Antivirus for Windows - Open s...



CLAM WIN
A FREE ANTIVIRUS FOR WINDOWS

Replacing proprietary anti-virus softw...

One of the major software programs every day, is a virus scanner. This sin... can be found on almost every PC in th... ClamWin Free Antivirus provides a fr... these costly proprietary anti-virus pr... Free Software Magazine

PLEASE ENABLE JAVASCRIPT! ALTHOUGH THE SITE CAN BE USED WITHOUT IT, IT IS NOT RECOMMENDED!

Saturday, 15 March 2008 Open source GPL virus scanner

MAIN MENU

- Home +
- About +
- Screenshots +
- Download +
- Make a Donation +
- How You Can Help +

[Vista Compatible ClamWin Free Antivirus Released](#)

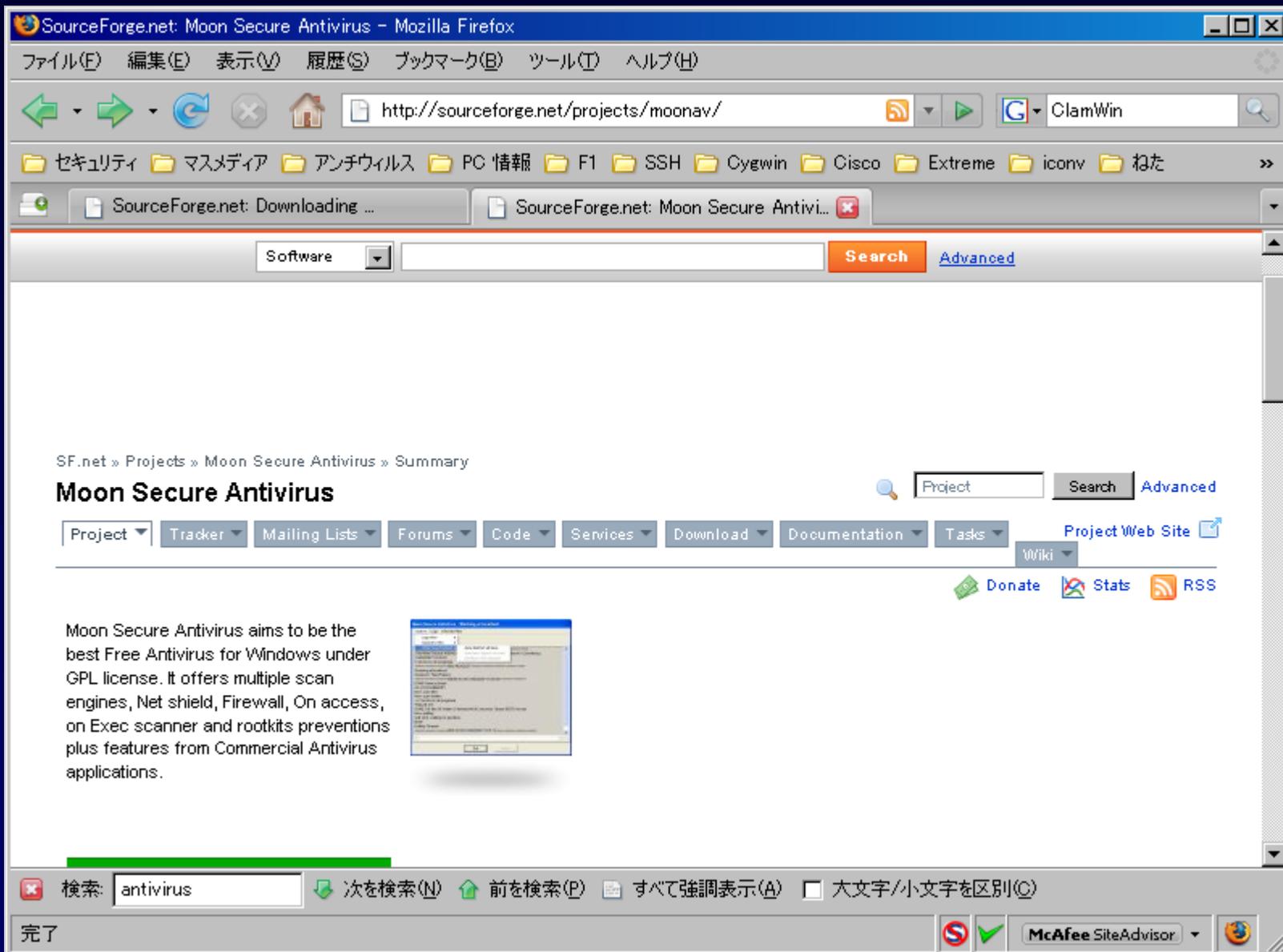
Our team is happy to announce the first release compatible with Microsoft Windows Vista. This release also updates ClamAV engine and adds some improvements:
[Read more...](#)

[About ClamWin Free Antivirus](#)

ClamWin is a **Free Antivirus** program for Microsoft Windows 98/Me/2000/XP/2003 and Vista. *ClamWin Free Antivirus* comes with an easy installer and [open source](#) code. You may download

完了 McAfee SiteAdvisor

http://www.clamwin.com/



http://sourceforge.net/projects/moonav/

使しい物になる

使い物になる

- 安定して動作
- ぶっちゃけ、検出力は今ひとつ
 - エンジンの性能
 - 検体採取体制
- オンアクセススキャンには未対応
- 商用アンチウイルスソフトの補助としてなら十分有用
 - 商用ソフトよりも対応がよい場合もある

milter 対応

- sendmail のメールフィルタリング API
 - 8.10 以降 (オプション)、8.12 以降 (標準)
 - postfix 2.3 以降 (標準)
- こんな感じで sendmail.mc に設定する

```
INPUT_MAIL_FILTER(`clmilter',  
`S=local:/var/run/clamav/clmilter.sock, F=  
T=S:4m;R:4m')dnl  
define(`confINPUT_MAIL_FILTERS', `clmilter')
```
- postfix なら main.cf に

```
smtpd_milters = unix:/var/run/clamav/clmilter.sock  
milter_default_action = accept
```

ウイルスシグネチャを自作できる

● MD5 を利用したシグネチャの例

- `% sigtool --md5 ossec-agent-win32-0.9.exe`
`d4b2e9fcc540bf1ae4bfb00618cf2559:205698:ossec-agent-win32-0.9.exe`
- `# sigtool --md5 ossec-agent-win32-0.9.exe >> /var/db/clamav/test.hdb`
- `% clamscan ossec-agent-win32-0.9.exe`
`ossec-agent-win32-0.9.exe: ossec-agent-win32-0.9.exe FOUND`
- `% clamdscan ossec-agent-win32-0.9.exe`
`/home/kjm/ossec-agent-win32-0.9.exe: ossec-agent-win32-0.9.exe`
`FOUND`

ウイルスシグネチャを自作できる

● 特徴抽出したシグネチャの例

- % strings withlove.exe
(中略)

```
fPPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADD  
INGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXP  
ADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDING  
PADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDIN  
GXXPADDINGPADDINGXXPADDING
```

- % echo -n PADDINGPADDINGXXPADDINGPADDINGXX | sigtool --hex-
dump
50414444494e4750414444494e47585850414444494e4750414444494e47585
8%

ウイルスシグネチャを自作できる

- 特徴抽出したシグネチャの例(つづき)
 - % cat test.db
hoge.hoge-1=50414444494e4750414444494e47585850414444494e47504
14444494e475858
 - % clamscan --database=test.db withlove.exe install_flash_player.exe
withlove.exe: hoge.hoge-1 FOUND
install_flash_player.exe: OK
- 他にもいろいろ……。参照:
 - docs/signatures.pdf
 - ClamAV のソース

拡張できる

拡張できる

- 3rd party 製シグネチャ
 - SaneSecurity - Phishing and Scam Signatures for ClamAV
 - <http://www.sanesecurity.co.uk/>
 - <http://www.st.ryukoku.ac.jp/~kjm/security/20071201-matcha139/Sanesecurity.ppt>
- MTA 用ツール
 - Qmail: Qmail-Scanner
 - <http://qmail-scanner.sourceforge.net/>
 - Exim: Exim 4.5 以降でネイティブサポート

拡張できる

- ClamAV 付き http proxy
 - HAVP (HTTP AntiVirus proxy)
 - <http://www.server-side.de/index.htm>
- Apache モジュール
 - mod_clamav
 - http://software.othello.ch/mod_clamav/
 - mod_streamav
 - <http://streamav.sourceforge.net/>

拡張できる

- ClamFS - FUSE を使ったユーザ空間ファイルシステム
 - <http://clamfs.sourceforge.net/>
- Dazuko - A Virtual Device Driver to Allow Online File Access Control
 - http://dazuko.dnsalias.org/wiki/index.php/Main_Page
 - Linux, FreeBSD
- samba-vscan - samba の VFS (virtual file system) 機能を利用
 - <http://www.openantivirus.org/projects.php#samba-vscan>

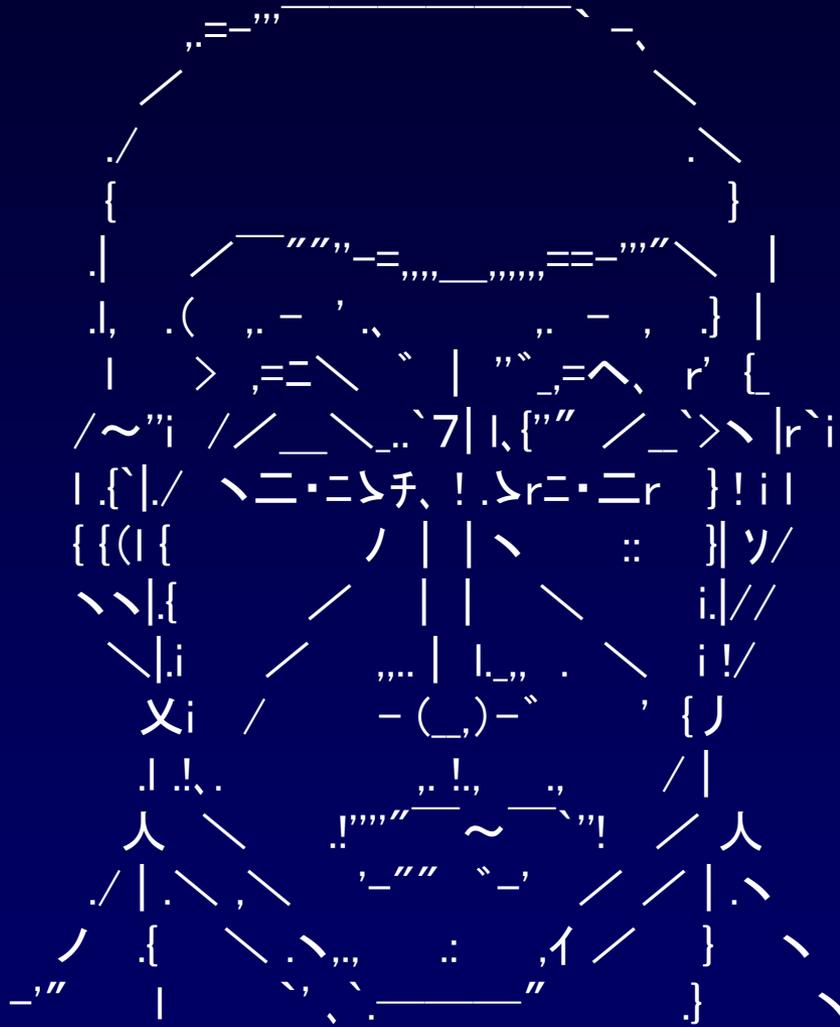
拡張できる

- その他にもいろいろ.....
 - <http://www.clamav.org/download/third-party-tools/>

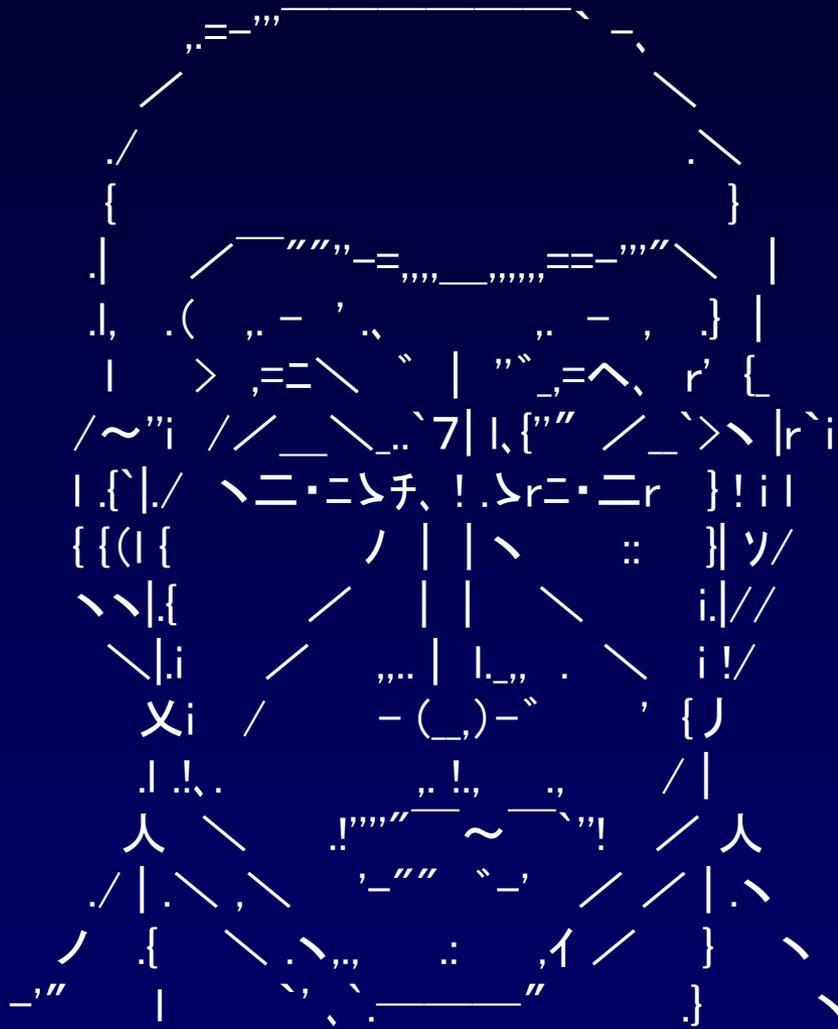
まとめ

- ClamAV は.....
 - フリー
 - 使い物になる
 - 拡張できる
- 使える道具は便利に使おう

特許の話



トレンドマイクロの者だが……



特許 No.5,623,600 の件だ……

ゴルゴの話

- Barracuda Network を提訴
 - ClamAVを同梱している製品を販売
- Barracuda が敗訴した場合、理論的には、ClamAV を利用している組織の多くが特許違反?!
- これまでのターゲット
 - マカフィーWebShield GroupShield
 - シマンテック Norton Antivirus for Internet E-mail Gateways
 - Fortinet のアプライアンス製品