Windows と Linux のセキュリティ: 噂の真相

日本 Windows NT ユーザ会 (JWNTUG)
Event Planning Working Group
小島 肇

今日のおはなし

- 噂 1: Linux は Windows よりも安全だ
- 噂 2: Apache は IIS よりも安全だ
- 噂 3: Netscape / Mozilla, Opera は IE よりも安全だ
- 噂 4: Microsoft はセキュリティ fix が遅いしセキュリティ情報も開示しない
- まとめにならないまとめ

念のため

- このプレゼンテーションは、JWNTUG を代表するものでも、JWNTUG の総意でもありません。あくまで小島個人の意見に基づくものです。
- このプレゼンテーションから得た情報は、あくまで at your own risk でご活用ください。

噂 1:
Linux は Windows よりも安全だ

実態事例 (1)

- Eiji James Yoshida 氏がまとめられている「改ざんされたサイトの Open Port (TCP) ランキング (2002.05.01-31)」[*] より:

OS	件数 (/1111)
Windows 系	316
Linux	314
Linux を除いた UNIX 系	178
その他 (不明含む)	303

[*] http://www.geocities.co.jp/SiliconValley/1667/index.htm

実態事例 (2)

- SecurityFocus.com の 2002 Q1 TOP 10 attacks [*]
  1. Code Red - MS Indexing Server/Indexing Services ISAPI Buffer Overflow Attack
  2. Nimda - Microsoft IIS 4.0/5.0 Extended UNICODE Directory Traversal Attack
  3. Matt Wright Formmail Attack
  4. WU-FTPD File Globbing Heap Corruption Attack
  5. SSH CRC32 Compenation Detection Attack
  6. Generic CDE dtspcd Buffer Overflow Attack
  7. Generic System V Derived Login Buffer Overflow Attack
  8. Generic SNMP PROTOS Test Suite Attacks
  9. Shaft DDoS Client To Handler Attack
  10. PHP Post File Upload Buffer Overflow Attack

[*] http://www.securityfocus.com/corporate/research/top10attacks_q1_2002.shtml

実態事例 (3)

- 2002.01.01〜2002.06.10 のセキュリティ fix の数

OS / ベンダー	patch 数
Microsoft	26
RedHat Linux 7.2	46
Debian GNU/Linux	35
Sun	6
FreeBSD	27

注意! 上記の数字は一概に比較できない:累積的 patch の存在、セキュリティアナウンスが不十分なベンダー (Sun) 等

真相: Linux だから安全、ではない

- どんな OS であっても、日々発見される security hole を随時 fix していく必要がある
  - B レベルの "Trusted OS" にすら security hole はある
- 不要なソフトウェアはインストールしない、不要なサービスは起動しない
  - インストールしなければ fix も必要ない
- ファイアウォール等による防衛は有効
  - ただし限界もある
  - web サーバ、web ブラウザ…

類似の噂: Open Source なら Closed Source より安全だ

- 「多くの目がある」神話
  - 絶対数
  - 商売
- Open Source なら安全、ではない
  - Open Source ならベンダーに依存せずに安全性を確認できる
  - Open Source ならベンダーに依存せずに fix できる
  - 自分自身 and/or コミュニティの力
  - Use the source, Luke!

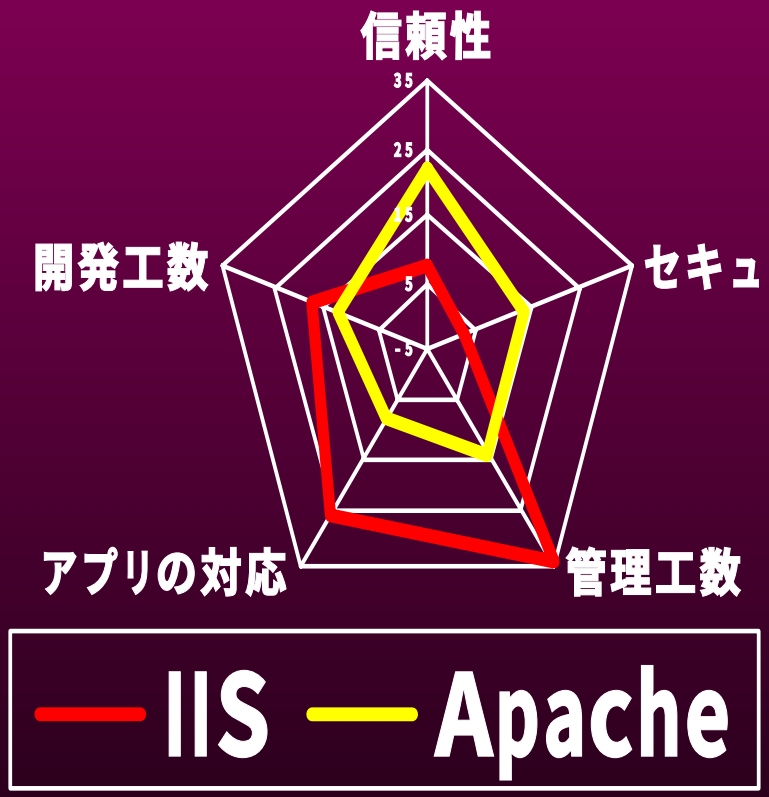
噂 2:
Apache は IIS よりも安全だ

実態事例

- 続々と発見される IIS の弱点
  - MS00-078/086/01-026: UNICODE BUG
  - MS01-023: IPP ISAPI buffer overflow
  - MS01-033: Index server buffer overflow
  - MS01-035: FrontPage Server Extensions buffer overflow
  - MS01-044: cumulative patch (SSI buffer overflow 等)
  - MS02-018: cumulative patch (ASP chunk encoding / HTTP header / SSI / .HTR buffer overflow, CSS 等)
  - MS02-028: Heap overrun in HTR Chunked Encoding
- いずれも危険性が高い

Web開発者の声

– JWNTUG アンケートから –



IIS
- 信頼性がある 7%
- セキュリティがある 2%
- 管理が容易 34%
- アプリの対応 26%
- 開発が容易 18%

Apache
- 信頼性がある 22%
- セキュリティがある 13%
- 管理が容易 14%
- アプリの対応 7%
- 開発が容易 12%

管理・開発が容易な IIS vs. **信頼性・セキュリティの高い** apache **という意識**

Apache は bug free ではない

- 何度か重要な修正が行われている
  - 1.3.12: クロスサイトスクリプティング脆弱性の fix
  - 1.3.14: 大規模な virtual hosting サイトにおいて Host: ヘッダ処理に問題があり攻撃者が任意のファイルにアクセス可能、CGI ソースの漏洩
  - 1.3.22: 特殊な Host: ヘッダにより任意の .log ファイルを上書き可能
- 古い Apache を動かしている hosting 業者は多い
  - 1.3.13 以前は特に危険
- Win32 版にはさらに、致命的なものも含む、さまざまな弱点が
  - 1.3.24: Win32 Apache Remote command execution

Apache は bug free ではない (続)

- よく使われる 3rd party モジュール
  - PHP
    - » PHP 4 .htaccess attribute transfer vuln. (bid 2206)
    - » PHP 4 engine disable source viewing vuln. (bid 2205)
    - » PHP post file upload buffer overflow (bid 4183)
  - WebDAV
    - » mod_encoding (20011026a, 20011211a)
  - mod_ssl
    - » buffer overflow (bid 4189)
  - Apache tomcat
    - » クロスサイトスクリプティング脆弱性 (bid 2982)

web application の弱点

- web サーバに依存しない
  - SSI, CGI, ASP, JSP, PHP, ColdFusion, …
- 情報漏洩
  - 特定ファイルを get するだけで漏洩するパターン多し
- なりすまし
  - 安易な「認証」
  - cookie の漏洩→セッションハイジャック
- クロスサイトスクリプティング脆弱性
  - cookie の漏洩→セッションハイジャック
  - サイトの (virtual な?!) 改ざん

真相: IIS は確かにアレゲだが Apache で安心してはいけない

- IIS もきちんと設定すれば Apache 並にはできる
  - file/directory パーミッションを修正
  - 不要なサンプルを削除
  - 不要な ISAPI を削除
  - IIS Lockdown, URLScan, guard 3 による防衛
  - patch は速やかに適用
- セキュリティ情報を注視し、適切に対応する必要があるのは IIS も Apache も同じ
  - IIS 6 で少しは楽になるといいな (^^;;)

噂 3:

Netscape / Mozilla, Opera **は** IE **よりも安全だ**

実態事例

- 続々と発見される IE の弱点。
  - 今年だけでも MS02-005 / 008 / 009 / 013 / 015 / 022 / 023 / 027
    - » 多くが累積的 patch なので、実数は遥かに多い
    - » 厳密には、MS02-022 は MSN チャットコントロールの問題だし、02-013 は Java VM の問題だが、ユーザからは IE の問題に見える
  - まだ patch が発表されていない弱点も散見
    - » ローカル HTML リソースのクロスサイトスクリプティング脆弱性 (MS02-023 未 fix 分)
    - » gopher:// buffer overflow (bid 4930, MS02-027)
    - » ftp:// クロスサイトスクリプティング脆弱性 (bid 4954)
    - » Unpatched IE security holes: http://jscript.dk/Unpatched/
- 正直言ってこの多さはシャレにならない。

では Netscape, Opera なら安心なのか?

- IE ほどではないがセキュリティホールが発見されている。
  - Netscape 6.1〜6.2.2 / mozilla 0.9.7〜1.0RC1 でローカルファイル漏洩
  - Opera 6.01 以前で cookie / ローカルファイル漏洩
  - Opera 6.01, 6.02 で任意のローカルファイルが漏洩
- Opera はセキュリティ情報が公開されない!
  - どんな問題があったのか、また本当に fix されたのかがベンダー情報からはわからない
  - 日本語版配布元が独自にセキュリティ情報を発信中
- Netscape は日本語情報が維持されていない
  - 英語情報はそれなり

現状の IE は、bug だけでなく…

- 危険なデフォルト値
  - スクリプトからクリップボードを操作できてしまう
  - MIME Content-Type: を無視する
    - » Content-Type: text/plain な文書によるクロスサイトスクリプティング脆弱性
    - » fusianasan アタック (.gif による攻撃)
    - » ユーザが挙動を変えられない→Opera は選択できる
  - セキュリティゾーンのデフォルト設定
    - » 少しずつ安全側に来ているが…
- アクティブスクリプトを無効にすれば多くの場合弱点を回避できるが…
  - microsoft.com 自身すらきちんと操作できない (苦笑)

真相: 現状ではそのとおりだが Netscape, Opera にも注意

- インターネット = WWW 時代に IE の現状は許容できない
- メインが Netscape / Opera でサブブラウザが IE ?
  - セキュリティ情報には注意。特に Opera はベンダー情報が信用できないため、初心者に勧めていいのか疑問。Netscape も日本語情報は心もとない。
  - IE コンポーネントを利用する 3rd party ブラウザは?
- 今こそ「web ブラウザは OS の一部です」の実現を! (半分本気)
  - OS 並の安定性・安全性が必要
  - 意図しない停止 (ブラウザクラッシャー等) も許容できない

噂 4:
Microsoft はセキュリティ fix が遅いしセキュリティ情報も開示しない

実態事例

- ftp:// クロスサイトスクリプティング脆弱性 (bid 4954)
  - IE 詳細設定「FTP サイト用のフォルダビューを使用する」
  - Explorer フォルダオプション「フォルダで web コンテンツを使う」
  - 上記 2 つが同時に有効な場合 (デフォルトで有効) に ftp:// URL でクロスサイトスクリプティング脆弱性が発生、マイコンピュータ権限でスクリプトが実行されてしまう
- 半年も前に連絡したにもかかわらず、いまだに「調査中」だという

ある程度時間がかかるのは仕方がない (らしい)

- なにしろシェアが違いすぎ
  - ちょっとでも互換性がなくなればたちまち大顰蹙
  - 数多くの OS 種類、PC98x1 版、各国語版
  - 本当にいろいろな使われ方をしている
- ストレステストの実施
  - 48h
- とはいえ半年棚ざらしはないだろう…
  - IE 関連は、たいていは 1.5〜2 か月くらいで fix できているようだ
  - OS だと 3〜4 か月?
    - » MS02-024 (DebPloit、NT/2000) は 2.5 か月
    - » MS02-017 (Multiple UNC、NT/2000/XP) は 5.5 か月

ときどき発生する変な対応

- 事例: LAC 発見の「Content-Disposition 脆弱性の新しい変種」
  - Microsoft からの修正がなかなか出ないので LAC が問題の存在を公開
    http://www.lac.co.jp/security/intelligence/SNSAdvisory/48.html
  - Microsoft は 3rd party software の問題であると反論
    http://www.microsoft.com/technet/security/topics/snsrprt.asp
  - ところがこの文書は唐突に Microsoft TechNet Security ページから link されなくなってしまう。この際何の説明もない。
  - MS02-023 で fix された

Microsoft の情報提供

- 情報提供は最高水準
  - web page での日本語情報提供 (時差ほとんどなし)
  - mail での日本語情報提供 (時差ほとんどなし)
  - 肝心の情報が隠蔽されているきらいはあるが…
    - » 書いたら書いたで「わからない」と言われる (らしい)
    - » どこまで公開するのか?
    - » CVE (脆弱性情報データベース) 対応
- セキュリティ問題の対応窓口
  - 日本語で e-mail できない; secure@microsoft.com
  - 無料電話 (0120-69-0196) あるが時間が限られる
    - » 平日 9:30-12:00, 13:00-19:00
  - MSKK セキュリティ担当者自体は 24h 対応しているようだが…

情報公開についての いくつかのことがら

- 脅威度判定は自分で行うしかない
  - Microsoft が示すのはあくまで目安
  - その目安も少しずつ変化している
    - » きつ目に変化 (歓迎すべき)
- OEM ベンダーからの情報も watch すべき
  - Microsoft 標準とは中身が微妙に違ったり
    - » プリインストールされているソフトウェア
    - » Microsoft, OEM ベンダー, 3rd party
  - Microsoft が全てを理解し対応することは不可能
  - 情報を出さない OEM ベンダーは?
  - Software Update Services ですこしは幸せになれるのか?

真相: もっと早く反応してくれ! (by アムロ・レイ)

- 1 か月で fix できないのか?
  - ふつうの感覚では 1 か月が我慢の限度だと思う
    - » 自分でやってもそう思った
    - » 1 週間しか我慢できない Guninski さんは例外 (笑)
  - 原理的に無理であるならそれを明記すべきなのでは
    - » 「これこれこのような理由で通常 2 か月かかります」とか
- 情報提供はすばらしい
  - なぜか誰もほめてあげない (泣)
  - Sun なんかより遥かにマシなのに

まとめにならないまとめ

何かを盲信するのはやめよう

- Microsoft を盲信している人はいないと思うが、Linux / Open Source を盲信している人は…
  - それなりに信用できるのは djb 教くらい?
    - djbdns, qmail, … (http://cr.yp.to)
    - 限られた機能を徹底的なセキュリティ・安定性と共に…
    - 「利便性とセキュリティは反比例」
- 適材適所
  - 現実問題、Windows 無視無視の状況は考えにくい
  - Windows の弱点を Open Source プロダクトでカバーする、あるいはその逆
  - 何かにこだわりすぎると、それが原因で苦労する
  - 捨てる! 勇気

よい方向には進んできている

- 1999 年と比べれば、雲泥の差
  - 2000 年の終りごろから急速に改善
  - CodeRed / Nimda が決定打
  - 日米時差攻撃はほぼ不可能になった
- まだまだやるべきことは多い
  - patch の度にテストが必要
    - » 間に合わない!
  - 「仕様」「互換性」という名のセキュリティホール
    - » 「デフォルトで secure」の重要性
  - .NET が状況を変えるか?
    - » 変わるとしても時間がかかる。その間のセキュリティは?!

日本 Windows NT ユーザ会 (JWNTUG)

- http://www.jwntug.or.jp/index-j.html
- 会費: 無料
- いくつかの Mailing List
  - ようやく Security な ML が登場予定…
- JWNTUG Newsletter
- いくつかの event
  - Microsoft Conference (MSC) にあわせて JWNTUG Open Talk を開催
    - » Microsoft 担当者と直接議論
  - BOF in Internet Week
- We need you!

プレゼンテーションはこれでおわりです

Appendix

参照 URL - Microsoft

- Microsoft Technet セキュリティセンター
  - 英語版:
    - http://www.microsoft.com/technet/security/
  - 日本語版:
    - http://www.microsoft.com/japan/technet/security/
  - セキュリティツール (HFNetChk, URLScan など):
    - http://www.microsoft.com/japan/technet/security/tools/tools.asp
- Security Bulletin: MSxx-xxx
  - 英語版:
    - http://www.microsoft.com/technet/security/bulletin/MSxx-xxx.asp
  - 日本語版:
    - http://www.microsoft.com/japan/technet/security/prekb.asp?sec_cd=MSxx-xxx

参照 URL - Microsoft

- Microsoft サポート技術情報 (Knowledge Base)
  - 英語版 (Qxxxxxx):
    - http://www.microsoft.com/technet/support/kb.asp?ID=xxxxxx
  - 日本語版 (JPxxxxxx, Jxxxxxx):
    - http://www.microsoft.com/japan/support/kb/artivles/JPxxx/x/xx.htm
    - http://www.microsoft.com/japan/support/kb/artivles/Jxxx/x/xx.htm

参照 URL – web page

- US CERT/CC (英語)
  - » http://www.cert.org/
  - – CERT/CC Incident Notes
    - » http://www.cert.org/incident_notes/
- CIAC (英語)
  - » http://www.ciac.org/
- JPCERT/CC
  - » http://www.jpcert.or.jp/
- IPA セキュリティセンター
  - » http://www.ipa.go.jp/security/

参照 URL – web page

- CVE
  - » http://www.cve.mitre.org/
  - – CAN-XXXX-XXX
    - » http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-XXXX-XXX
- BUGTRAQ bugid XXXX
  - » http://www.securityfocus.com/bid/XXXX
- Apache Week Apache httpd 1.3 vulnerabilities
  - » http://www. apacheweek.com/features/security-13
- PHP
  - » http://www.php.net/

参照 URL – web page

- RedHat
  - » http://www.jp.redhat.com/support/errata/
- Debian
  - » http://www.debian.org/security/
- FreeBSD
  - » http://www.freebsd.org/security/
- Sun
  - » http://sunsolve.sun.com/pub-cgi/secBulletin.pl

参照 URL – web page

- Netscape Security Center
  - » http://wp.netscape.com/security/
  - » http://wp.netscape.com/ja/security/
- Opera
  - » http://www.opera.com/support/service/security/
  - » http://www.jp.opera.com/support/service/security/
- Georgi Guninski Security Research
  - » http://www.guninski.com/

参照 URL – web page

- 日本 Windows NT ユーザ会 (JWNTUG)
  - » http://www.jwntug.or.jp/
- port139
  - » http://www.port139.co.jp/
- Win セキュリティ虎の穴
  - » http://winsec.toranoana.ne.jp/
- セキュリティホール memo
  - » http://www.st.ryukoku.ac.jp/~kjm/security/memo/
  - – セキュリティアンテナ
    - » http://www.st.ryukoku.ac.jp/~kjm/security/antenna/
- ZDNet Helpdesk Security How-To
  - » http://www.zdnet.co.jp/help/howto/security/

参照 URL –メーリングリスト

- BUGTRAQ (英語)
  - » http://www.securityfocus.com/
- NTBUGTRAQ (英語)
  - » http://www.ntbugtraq.com/
- セキュリティホール memo ML
  - » http://memo.st.ryukoku.ac.jp/
- Security Talk ML
  - » http://www.office.ac/Security_Talk_ML_Guide.html
- 24 時間常時接続 ML
  - » http://cn24h.hawkeye.ac/connect24h.html
- port139 ML (新規加入休止中)
  - » http://www.port139.co.jp/ntsec_ml.htm