Hitachi Incident Response Team
2009.12.02 11:34:08 +09'00'

HITACHI
Inspire the Next

チェックしておきたいぜい弱性情報2009＜2009.11.24＞

Hitachi Incident Response Team
http://www.hitachi.co.jp/hirt/
寺田真敏

HITACHI
Inspire the Next

Contents

11月24日までに明らかになったぜい弱性情報のうち、気になるものを紹介します。それぞれ、ベンダーなどの情報を参考に対処してください。

1 TCPパケットを用いたDoS攻撃

- 1990年代中盤（TCP/IPパケット自身がDoS攻撃の実体⇒トラフィック増による負荷増）、
  2004年（TCP通信の切断）、2009年（TCP通信維持による負荷増）

1980 | 1985 | 1990 | 1995 | 2000 | 2005 | 2010

△ RFC791: Internet Protocol
RFC793: Transmission Control Protocol

△ A Weakness in the 4.2BSD Unix TCP/IP Software (Robert T. Morris)

△ Security Problems in the TCP/IP Protocol Suite (Steve Bellovin)

△CA-1995-01: IP Spoofing Attacks and Hijacked Terminal Connections

△CA-1996-01: UDP Port Denial-of-Service Attack

△CA-1996-21: TCP SYN Flooding and IP Spoofing Attacks

△SYN cookies (Server SYN Cookie) (D.J.Bernstein)

△CA-1996-26: Denial-of-Service Attack via ping

△CA-1997-28: IP Denial-of-Service Attacks - Teardrop, Land

△CA-1998-01: Smurf IP Denial-of-Service Attacks

△CA-2001-09
TCP初期シーケンス番号の統計学的なぜい弱性

△JVNTA04-111A
TCPにサービス運用妨害を伴うぜい弱性

△CVE-2008-4609
TCPのゼロ・ウィンドウ・サイズ

△CVE-2009-1926
TCPの孤立した接続状態

1 TCP通信のサスペンド実験

- TCP通信のサスペンド実験
  - HTTP　Linux+Apache
    Windows+IIS
  - FTP　UNIX系
    Windows+IIS

```
[HIRT]$ sh hu.sh
--02:38:31--  http://jvnrss.ise.chuo-u.ac.jp/jtg/iw2009/TCP_ZeroWindow.dat
Resolving jvnrss.ise.chuo-u.ac.jp... 133.91.65.202
Connecting to jvnrss.ise.chuo-u.ac.jp|133.91.65.202|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 86448164 (82M) [text/plain]
Saving to: `TCP_ZeroWindow.dat'

 0% [                                       ] 610,107      594K/s
[1]+  Stopped                 sh hu.sh
[HIRT]$ _
```

⇒30分以上、TCPコネクションは維持された。

Linux+Apacheの事例

No.	Time	Protocol	Info
1	7:40:17	TCP	53328 > 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=665617 TSER=0 WS=3
2	7:40:18	TCP	80 > 53328 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1412 TSV=2752632423 TSER
3	7:40:18	TCP	53328 > 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=665984 TSER=2752632423
4	7:40:18	HTTP	GET /jtg/iw2009/TCP_ZeroWindow.dat HTTP/1.0
5	7:40:18	TCP	80 > 53328 [ACK] Seq=1 Ack=160 Win=5792 Len=0 TSV=2752632451 TSER=665985
6	7:40:18	HTTP	HTTP/1.1 200 OK (text/plain)
7	7:40:18	TCP	53328 > 80 [ACK] Seq=160 Ack=1401 Win=8736 Len=0 TSV=666089 TSER=2752632451
8	7:40:18	HTTP	Continuation or non-HTTP traffic
			ダウンロード継続
881	7:40:20	HTTP	Continuation or non-HTTP traffic
882	7:40:20	TCP	53328 > 80 [ACK] Seq=160 Ack=789601 Win=168 Len=0 TSV=667841 TSER=2752632679
883	7:40:20	HTTP	[TCP Window Full] Continuation or non-HTTP traffic
			サスペンド開始
884	7:40:21	TCP	[TCP ZeroWindow] 53328 > 80 [ACK] Seq=160 Ack=789769 Win=0 Len=0 TSV=668119 TSE
885	7:40:21	HTTP	[TCP Window Full] [TCP Retransmission] Continuation or non-HTTP traffic
886	7:40:21	TCP	[TCP ZeroWindow] 53328 > 80 [ACK] Seq=160 Ack=789769 Win=0 Len=0 TSV=668220 TSE
			サスペンド継続
929	8:10:40	TCP	[TCP Keep-Alive] 80 > 53328 [ACK] Seq=789768 Ack=160 Win=5792 Len=0 TSV=27528146
930	8:10:40	TCP	[TCP ZeroWindow] 53328 > 80 [ACK] Seq=160 Ack=789769 Win=0 Len=0 TSV=1725233 TS
931	8:12:41	TCP	[TCP Keep-Alive] 80 > 53328 [ACK] Seq=789768 Ack=160 Win=5792 Len=0 TSV=27528267
932	8:12:41	TCP	[TCP ZeroWindow] 53328 > 80 [ACK] Seq=160 Ack=789769 Win=0 Len=0 TSV=1792533 TS

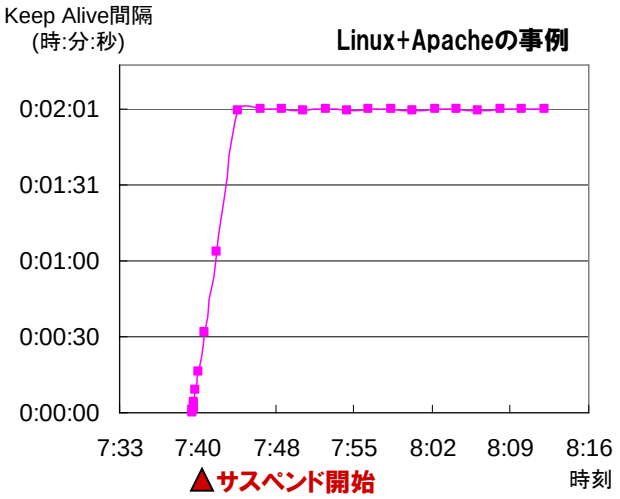
1 TCP通信のサスペンド実験

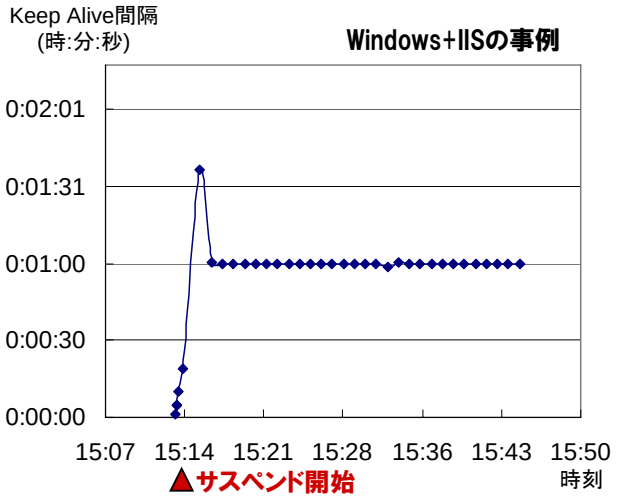
- TCP通信のサスペンド実験
  - HTTP　Linux+Apache
    Windows+IIS
  - FTP　UNIX系
    Windows+IIS

```
[HIRT]$ sh hu.sh
--02:38:31--  http://jvnrss.ise.chuo-u.ac.jp/jtg/iw2009/TCP_ZeroWindow.dat
Resolving jvnrss.ise.chuo-u.ac.jp... 133.91.65.202
Connecting to jvnrss.ise.chuo-u.ac.jp|133.91.65.202|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 86448164 (82M) [text/plain]
Saving to: `TCP_ZeroWindow.dat'

 0% [                                       ] 610,107      594K/s
[1]+  Stopped                 sh hu.sh
[HIRT]$ _
```

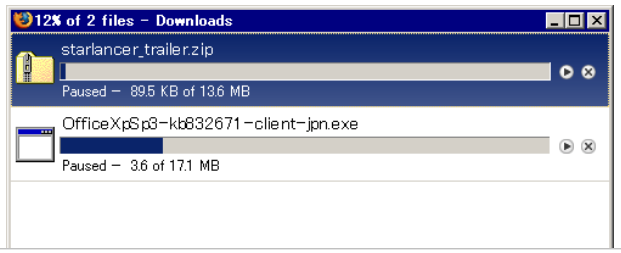
⇒Keep Aliveの間隔は、1～2分





1 TCP通信のサスペンド実験

- TCP通信のサスペンド実験
  - HTTP　Linux+Apache
    Windows+IIS
  - FTP　UNIX系
    Windows+IIS



Windows+IISの事例

No.	Time	Protocol	Info
1	21:43:26	TCP	1853 > 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2
2	21:43:27	TCP	80 > 1853 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 WS=1
3	21:43:27	TCP	1853 > 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
4	21:43:27	HTTP	GET /download/2/0/2/202b86d7-5b15-4420-8b5c-5f80ba92d453/OfficeXpSp3-kb832671-clien
5	21:43:28	TCP	[TCP Window Update] 80 > 1853 [ACK] Seq=1 Ack=1 Win=100252 Len=0
6	21:43:28	HTTP	HTTP/1.1 206 Partial Content
7	21:43:28	HTTP	Continuation or non-HTTP traffic
			ダウンロード継続
2497	21:43:32	HTTP	Continuation or non-HTTP traffic
2498	21:43:32	HTTP	Continuation or non-HTTP traffic
2499	21:43:42	HTTP	Continuation or non-HTTP traffic
			サスペンドとダウンロード再開
2500	21:43:59	TCP	1854 > 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2
2501	21:44:00	TCP	80 > 1854 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 WS=1
2502	21:44:00	TCP	1854 > 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
2503	21:44:00	HTTP	GET /download/2/0/2/202b86d7-5b15-4420-8b5c-5f80ba92d453/OfficeXpSp3-kb832671-clien
2504	21:44:00	TCP	[TCP Window Update] 80 > 1854 [ACK] Seq=1 Ack=1 Win=100252 Len=0
2506	21:44:00	HTTP	HTTP/1.1 206 Partial Content
2508	21:44:00	HTTP	Continuation or non-HTTP traffic
2509	21:44:00	HTTP	Continuation or non-HTTP traffic

⇒HTTPの場合には、Rangeヘッダで再開
　Range: bytes=5332545-
⇒FTPの場合には、RESTコマンドで再開
　REST 111104

1 TCP通信のゼロ・ウィンドウ・サイズ実験

- TCPのゼロ・ウィンドウ・サイズ実験
  - クライアント：CentOS 5.2 ＋ Client SYN Cookie ベースのプログラム
  - サーバ：Windows XP (SP3) ＋ Apache 2.2.14
  - [FIN, ACK] に対してゼロ・ウインドウ・サイズの [ACK] を応答する。

No.	Time	Protocol	Info
1	14:00:31	TCP	10735 > 80 [SYN] Seq=0 Win=1024 Len=0 TSV=1258143259 TSER=0 MS
2	14:00:31	TCP	80 > 10735 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 TSV=
3	14:00:31	HTTP	GET / HTTP/1.0
4	14:00:31	TCP	80 > 10735 [ACK] Seq=1 Ack=19 Win=16366 Len=0 TSV=154598 TSER=
5	14:00:31	HTTP	HTTP/1.1 200 OK (text/html)
6	14:00:31	TCP	80 > 10735 [FIN, ACK] Seq=330 Ack=19 Win=16366 Len=0 TSV=154601
7	14:00:31	TCP	**[TCP ZeroWindow] 10735 > 80 [ACK] Seq=19 Ack=330 Win=0 Len=0 T**
8	14:00:36	TCP	80 > 10735 [FIN, ACK] Seq=330 Ack=19 Win=16366 Len=0 TSV=154649
9	14:00:45	TCP	80 > 10735 [FIN, ACK] Seq=330 Ack=19 Win=16366 Len=0 TSV=154745
10	14:01:05	TCP	80 > 10735 [FIN, ACK] Seq=330 Ack=19 Win=16366 Len=0 TSV=154937
11	14:01:43	TCP	80 > 10735 [FIN, ACK] Seq=330 Ack=19 Win=16366 Len=0 TSV=155321
12	14:03:00	TCP	80 > 10735 [FIN, ACK] Seq=330 Ack=19 Win=16366 Len=0 TSV=156089
13	14:03:00	TCP	**[TCP ZeroWindow] 10735 > 80 [ACK] Seq=19 Ack=330 Win=0 Len=0 T**

1 TCP通信のゼロ・ウィンドウ・サイズ実験

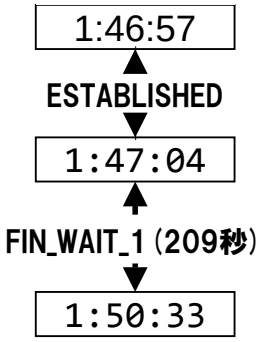
- TCPのゼロ・ウィンドウ・サイズ実験
  - クライアント：CentOS 5.2 ＋ Client SYN Cookie ベースのプログラム
  - サーバ：Windows XP (SP3) ＋ Apache 2.2.14
  - ゼロ・ウインドウ・サイズのHTTP要求の送信と、[ACK] に対してゼロ・ウインドウ・サイズの [ACK] を応答する。

No.	Time	Protocol	Info
1	15:24:28	TCP	61823 > 80 [SYN] Seq=0 Win=1024 Len=0 TSV=1258146236 TSER=0 MS
2	15:24:28	TCP	80 > 61823 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 TSV=
3	15:24:28	HTTP	**[TCP ZeroWindow] GET / HTTP/1.0**
4	15:24:29	TCP	80 > 61823 [ACK] Seq=1 Ack=19 Win=16366 Len=0 TSV=204978 TSER=
5	15:24:32	TCP	[TCP ZeroWindowProbe] 80 > 61823 [ACK] Seq=1 Ack=19 Win=16366 Le
6	15:24:38	TCP	[TCP ZeroWindowProbe] 80 > 61823 [ACK] Seq=1 Ack=19 Win=16366 Le
7	15:24:50	TCP	[TCP ZeroWindowProbe] 80 > 61823 [ACK] Seq=1 Ack=19 Win=16366 Le
8	15:25:14	TCP	[TCP ZeroWindowProbe] 80 > 61823 [ACK] Seq=1 Ack=19 Win=16366 Le
9	15:26:02	TCP	[TCP ZeroWindowProbe] 80 > 61823 [ACK] Seq=1 Ack=19 Win=16366 Le
10	15:26:02	TCP	**[TCP ZeroWindowProbeAck] [TCP ZeroWindow] 61823 > 80 [ACK] Se**
11	15:27:38	TCP	[TCP ZeroWindowProbe] 80 > 61823 [ACK] Seq=1 Ack=19 Win=16366 Le
12	15:29:38	TCP	[TCP ZeroWindowProbe] 80 > 61823 [ACK] Seq=1 Ack=19 Win=16366 Le
13	15:31:38	TCP	[TCP ZeroWindowProbe] 80 > 61823 [ACK] Seq=1 Ack=19 Win=16366 Le
14	15:33:38	TCP	[TCP ZeroWindowProbe] 80 > 61823 [ACK] Seq=1 Ack=19 Win=16366 Le
15	15:35:38	TCP	[TCP ZeroWindowProbe] 80 > 61823 [ACK] Seq=1 Ack=19 Win=16366 Le

1 TCP通信のタイムアウト実験

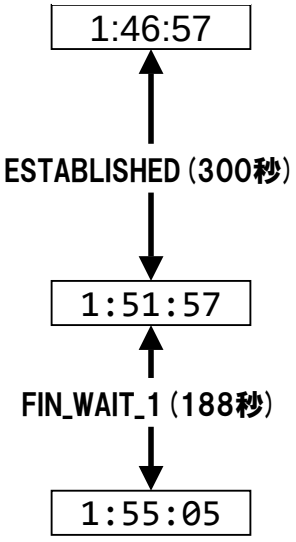
- TCPのゼロ・ウィンドウ・サイズ実験
  - クライアント：CentOS 5.2 ＋ nc 1.84 ＋ iptables
  - サーバ：Windows XP (SP3) ＋ Apache 2.2.14
  - TCPコネクション確立後に、ncを強制終了し、応答しない。

クライアントの
TCP遷移状態



No.	Time	Protocol	Info
1	1:46:57	TCP	50034 > 80 [SYN] Seq=0 Win=5840 Len=0
2	1:46:57	TCP	80 > 50034 [SYN, ACK] Seq=0 Ack=1 Win=
3	1:46:57	TCP	50034 > 80 [ACK] Seq=1 Ack=1 Win=5840
			iptables INPUT/OUTPUTフィルタ
	1:47:04		nc 強制終了
			以降、クライアントは無応答
4	1:51:57	TCP	80 > 50034 [FIN, ACK] Seq=1 Ack=1 Win=1
5	1:52:00	TCP	80 > 50034 [FIN, ACK] Seq=1 Ack=1 Win=1
6	1:52:06	TCP	80 > 50034 [FIN, ACK] Seq=1 Ack=1 Win=1
7	1:52:18	TCP	80 > 50034 [FIN, ACK] Seq=1 Ack=1 Win=1
8	1:52:42	TCP	80 > 50034 [FIN, ACK] Seq=1 Ack=1 Win=1
9	1:53:30	TCP	80 > 50034 [FIN, ACK] Seq=1 Ack=1 Win=1

サーバの
TCP遷移状態

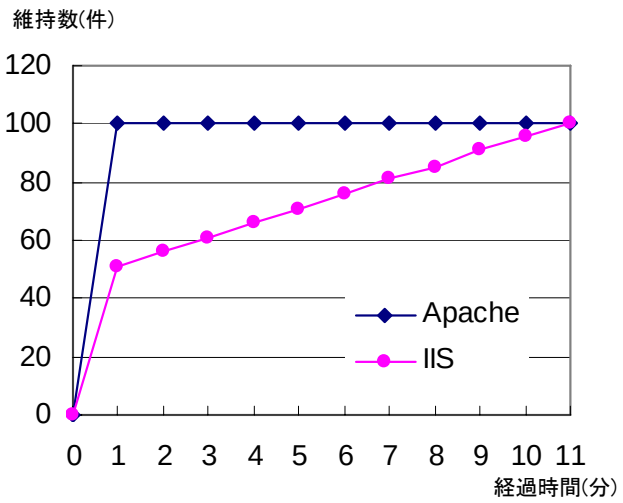


1 TCP通信のコネクション確立実験

- TCP通信のコネクション確立実験
  - クライアント：Windows XP SP3 ＋ TCP通信プログラム
  - サーバ：Windows XP (SP3) ＋ Apache 2.2.14 ならびに、IIS 5.1
  - 100件のHTTP要求を、TCPコネクション確立状態で維持する（60秒間隔で新規・更新操作）。

No.	Time	Protocol	Info	
3	11:18:10	TCP	1640 > 80 [SYN] Seq=2967504901	
4	11:18:10	TCP	80 > 1640 [SYN, ACK] Seq=23292	
5	11:18:10	TCP	1640 > 80 [ACK] Seq=2967504902	
33	11:18:10	HTTP	GET / HTTP/1.1	
638	11:19:57	HTTP	Continuation or non-HTTP traffic	GET要求の続き
997	11:22:23	HTTP	Continuation or non-HTTP traffic	GET要求の続き
1326	11:24:23	HTTP	Continuation or non-HTTP traffic	GET要求の続き
1701	11:25:54	HTTP	Continuation or non-HTTP traffic	GET要求の続き
1939	11:27:14	HTTP	Continuation or non-HTTP traffic	GET要求の続き
2149	11:28:14	HTTP	Continuation or non-HTTP traffic	GET要求の続き
2353	11:29:14	HTTP	Continuation or non-HTTP traffic	GET要求の続き
2553	11:30:14	HTTP	Continuation or non-HTTP traffic	GET要求の続き
2754	11:31:14	HTTP	Continuation or non-HTTP traffic	GET要求の続き
2954	11:32:14	HTTP	Continuation or non-HTTP traffic	GET要求の続き
3157	11:33:14	HTTP	Continuation or non-HTTP traffic	GET要求の続き

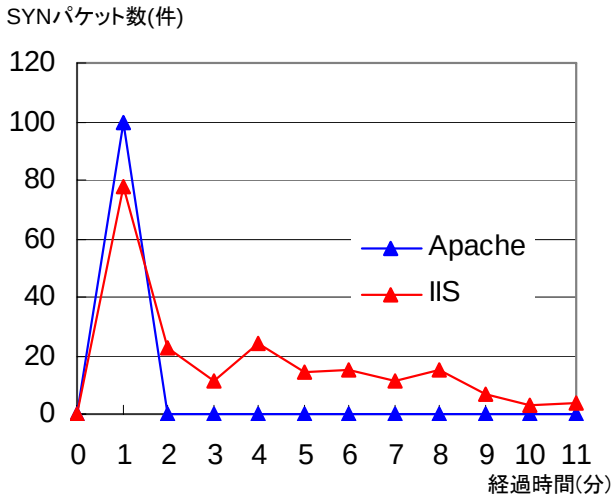
TCPコネクション確立状態を維持したHTTP要求の事例



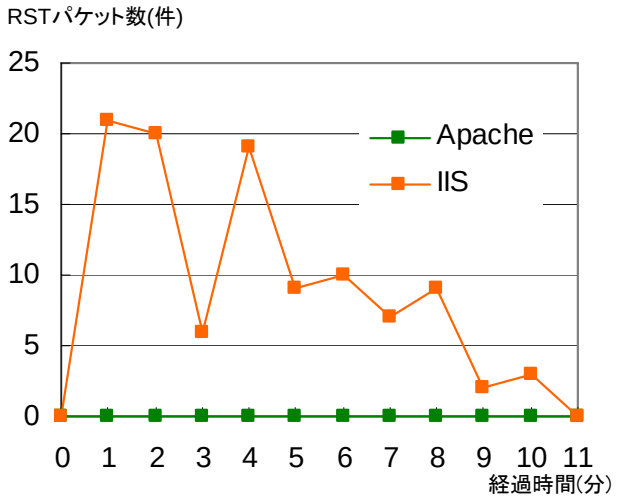
TCPコネクションを確立した状態の
HTTP要求数

1 TCP通信のコネクション確立実験

- TCP通信のコネクション確立実験
  - クライアント:Windows XP SP3 ＋ TCP通信プログラム
  - サーバ:Windows XP (SP3) ＋ Apache 2.2.14 ならびに、IIS 5.1
  - 100件のHTTP要求を、TCPコネクション確立状態で維持する(60秒間隔で新規・更新操作)。



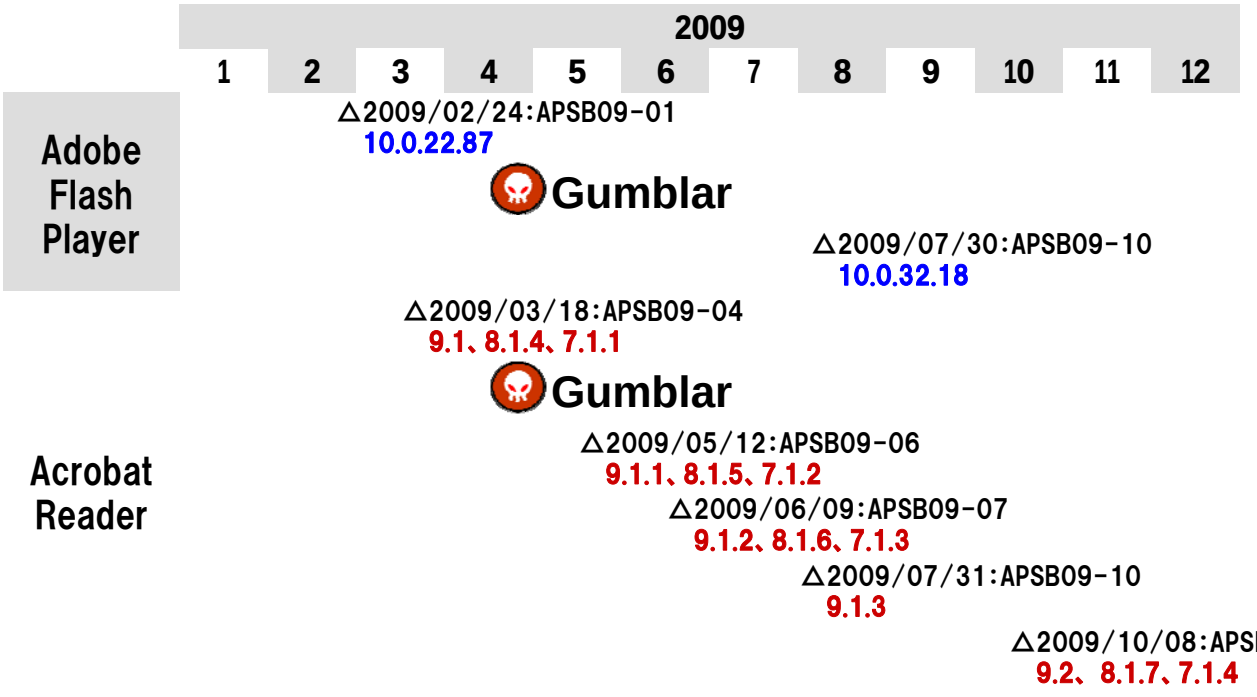
TCPコネクション確立要求数
(クライアント⇒サーバへのSYNパケット数)



拒否されたTCPコネクション確立要求数
(サーバ⇒クライアントへのRSTパケット数)

2 Adobe Flash Player、Acrobat Reader

- 2008年Adobe Flash Playerのアップデート: 9.0.124.0、9.0.151.0 (10.0.12.36)
  2008年Acrobat Readerのアップデート: 8.1.2、8.1.2 Security Update 1、8.1.3 (9.0)



3 X.509証明書のドメイン名処理

- ドメイン名にNULL文字("¥x00")を含むX.509証明書の取り扱いに関するぜい弱性で、SSLクライアントとSSLサーバ証明書を発行する認証局で、証明書に記載されたドメイン名の取り扱いが異なることに起因する。

2009年8月
- CVE-2009-2408:Mozilla Firefox、Thunderbird
- CVE-2009-2666:fetchmail
- CVE-2009-2474:WebDAVクライアント・ライブラリ neon

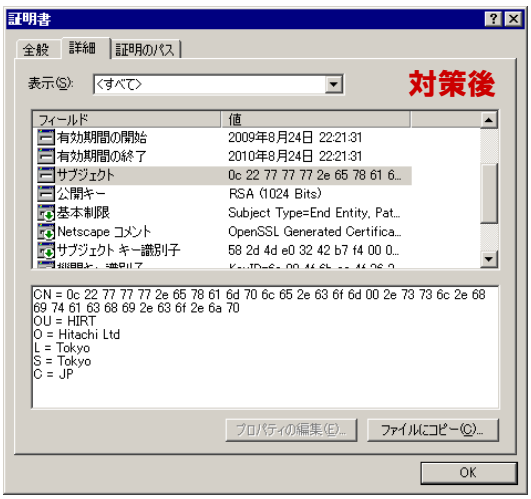
2009年10月
- CVE-2009-3455:アップルSafari
- CVE-2009-3456:Google Chrome
- CVE-2009-3475:Internet2 Shibboleth Service Provider software
- CVE-2009-3490:Gnu Wget
- CVE-2009-3454:マイクロソフト Internet Explorer (CVE-2009-2510に変更)
- CVE-2009-3477:RIM BlackBerry Device Software (Blackberry Browser)
- CVE-2009-3639:ProFTPD
- CVE-2009-3767:OpenLDAP

3 X.509証明書のドメイン名処理

認証局が発行するSSLサーバ証明書のドメイン名

www.example.com¥x00.ssl.hitachi.co.jp

ぜい弱なSSLクライアント実装ではドメイン名を先頭から読み始め、
NULL文字が出現したところで処理を終了

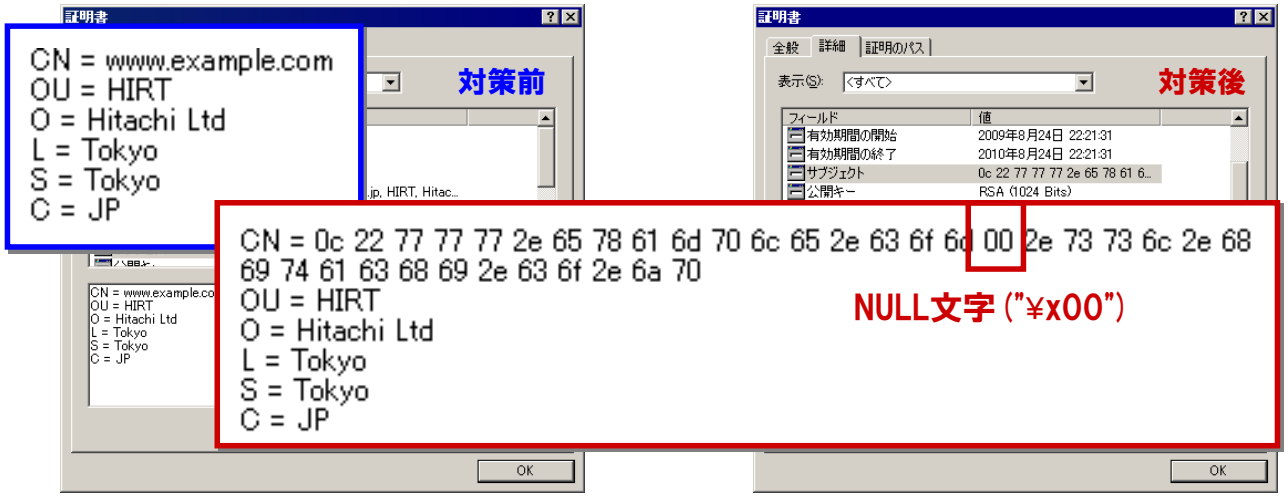


3 X.509証明書のドメイン名処理

認証局が発行するSSLサーバ証明書のドメイン名

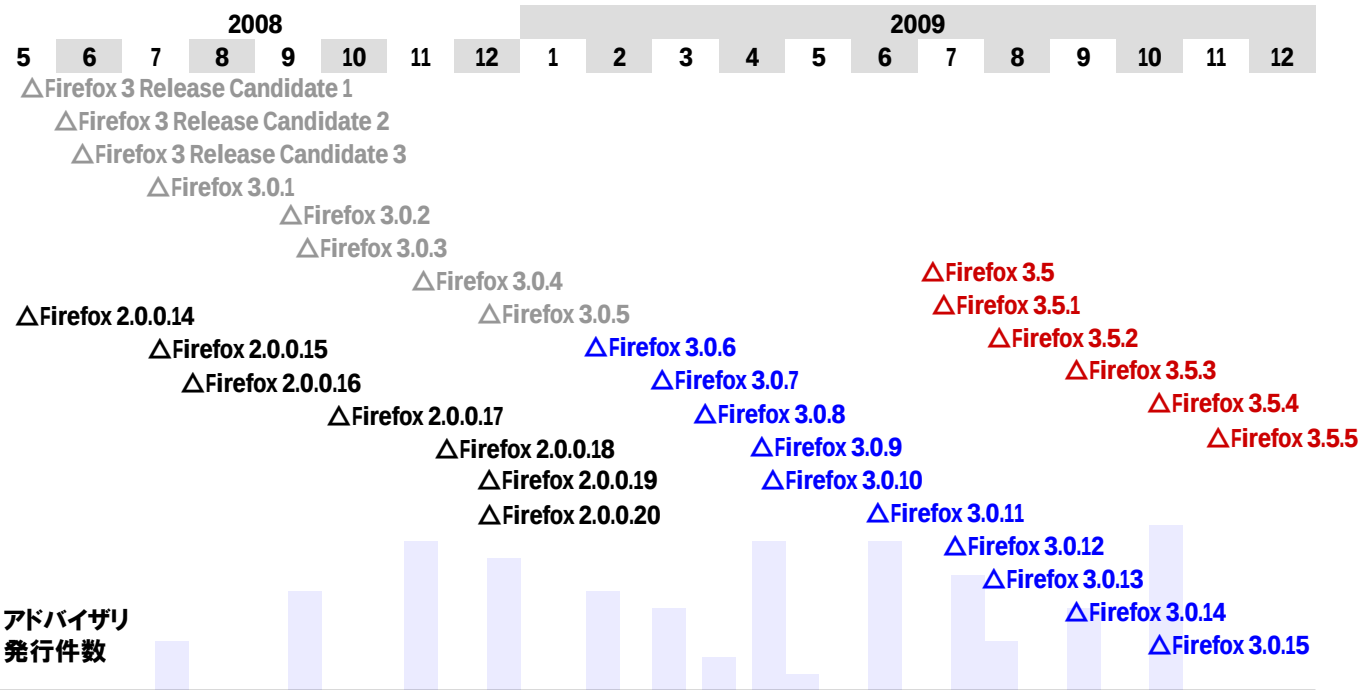
www.example.com¥x00.ssl.hitachi.co.jp

ぜい弱なSSLクライアント実装ではドメイン名を先頭から読み始め、
NULL文字が出現したところで処理を終了



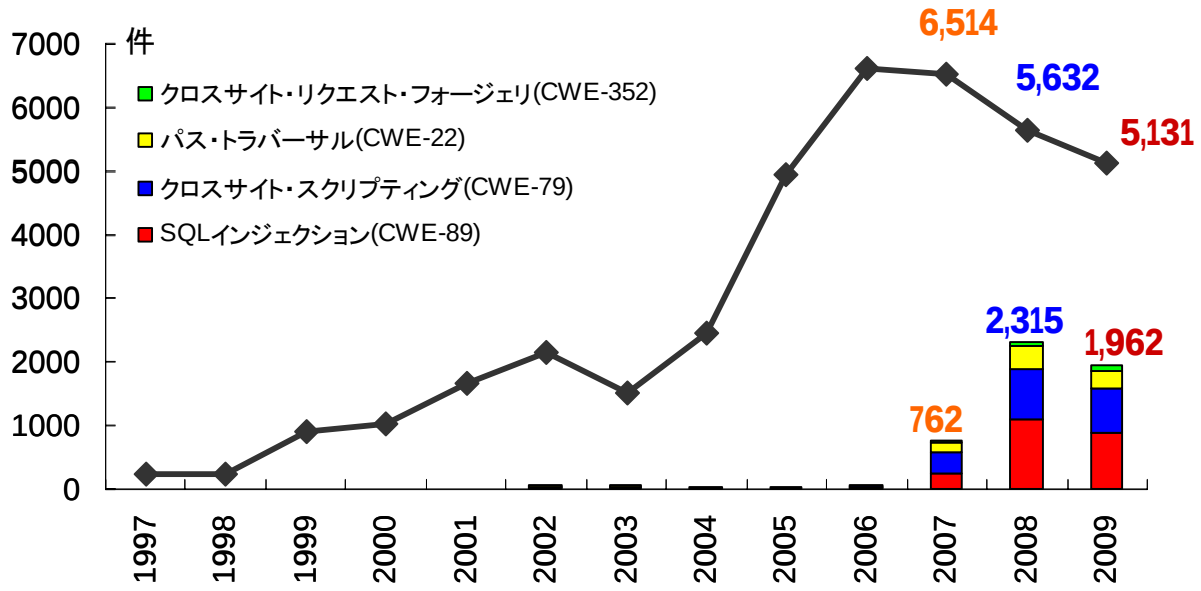
4 Mozilla Firefox

□ 2008年Firefoxのアップデート：2.0.0.12～2.0.0.20



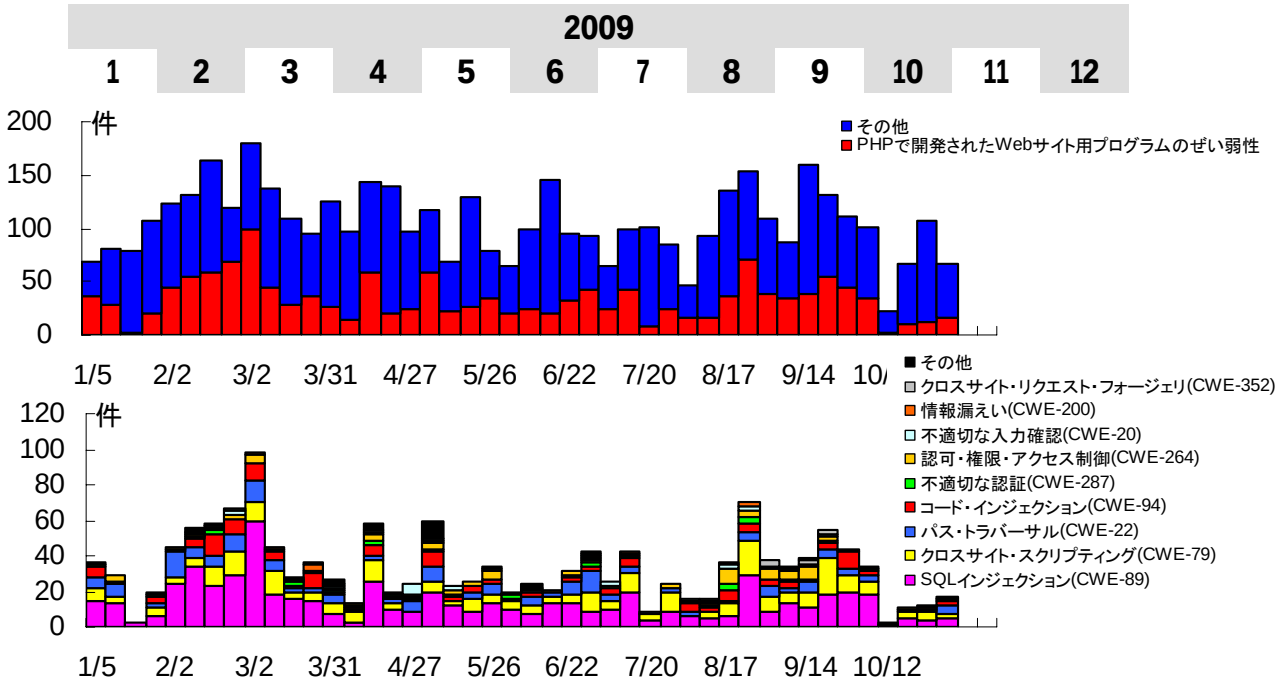
5 Webサイト用プログラム

- NVD (National Vulnerability Database) に登録された (≒CVE: Common Vulnerabilities and Exposuresが割り当てられた) ぜい弱性総件数とWebサイト用プログラムのぜい弱性件数の推移



5 PHPで開発されたWebサイト用プログラム

- 2009年、NVDに登録されたPHPで開発されたWebサイト用プログラムのぜい弱性 (1,472件) ＋その他 (3,147件) ＝総件数 (4,619件)



6 コラム：まず、チェックできる仕組み作りから

Hitachi Incident Response Team

□ 対策方法は簡単ではあるが、最新の状態に維持することは難しい。

出典：(独)情報処理推進機構

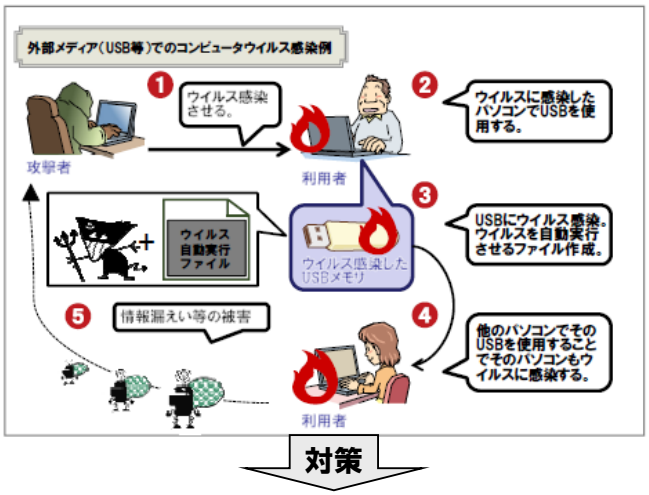
■組織への脅威
- 【1 位】DNS キャッシュポイズニングの脅威
- 【2 位】巧妙化する標的型攻撃
- 【3 位】恒常化する情報漏えい

■利用者への脅威
- 【1 位】多様化するウイルスやボットの感染経路
- 【2 位】脆弱な無線 LAN 暗号方式における脅威
- 【3 位】減らないスパムメール
- 【4 位】ユーザ ID とパスワードの使いまわしによる危険性

■システム管理者・開発者への脅威
- 【1 位】正規のウェブサイトを経由した攻撃の猛威
- 【2 位】誘導型攻撃の顕在化
- 【3 位】組込み製品に潜む脆弱性

■ 利用者への脅威

【1 位】多様化するウイルスやボットの感染経路［総合：4 位］



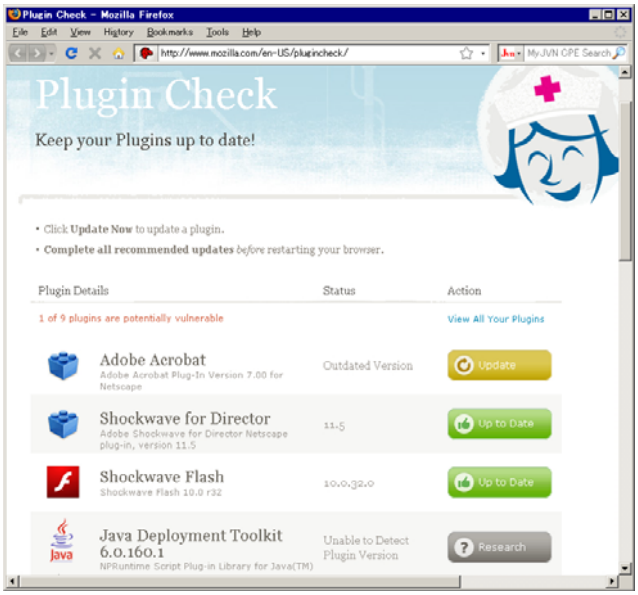
対策

OSやアプリケーション、ActiveXなどのプラグイン、ウイルス対策プログラムの定義ファイルを随時最新の状態にするなどの対策が有効である。

6 コラム：まず、チェックできる仕組み作りから

Hitachi Incident Response Team

□ チェックのためのツールは整備されつつある。



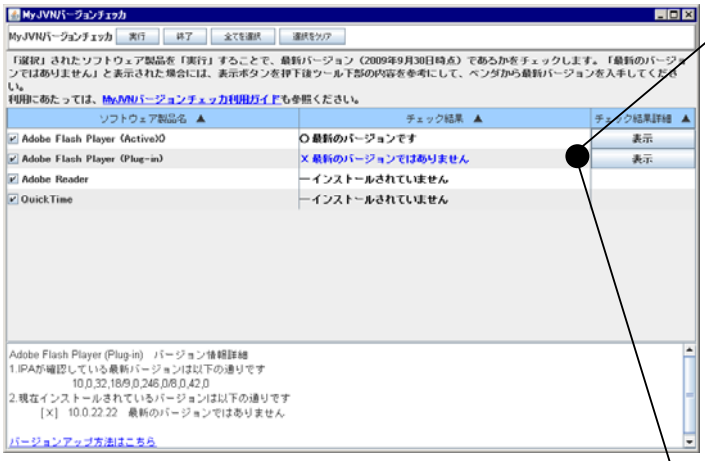
Firefoxプラグインのバージョンチェック
http://www.mozilla.com/en-US/plugincheck/

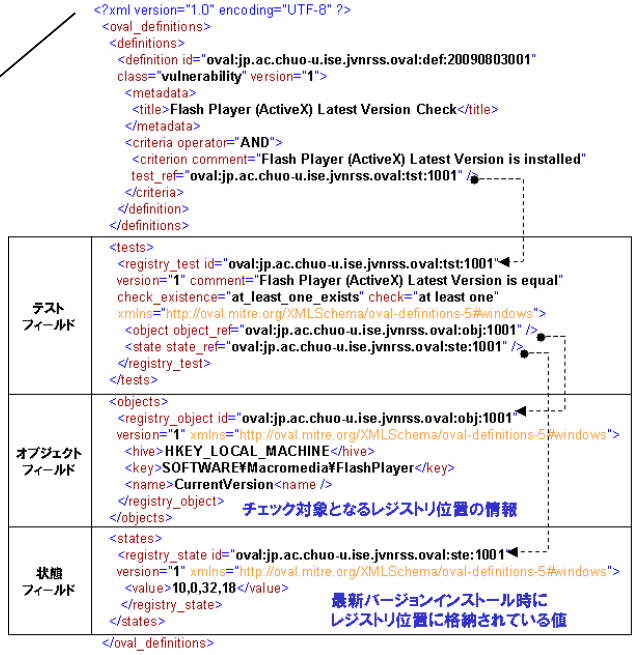
最新版がインストールされている場合	左記以外
Flash Playerバージョンチェック WIN 10,0,32,18 詳細 Powered by JVNRSS FST	Flash Playerバージョンチェック WIN 10,0,22,87 詳細 Powered by JVNRSS FST
Flash Playerバージョンチェック 調査結果 WIN 10,0,32,18 最新版 10,0,32,18 戻る	Flash Playerバージョンチェック 調査結果 WIN 10,0,22,87 最新版 10,0,32,18 戻る

Flash Playerのバージョンチェック
http://www.hitachi.co.jp/hirt/

6 コラム：まず、チェックできる仕組み作りから

- ステップアップ：国際的な共通基準を活用した機械化処理の基盤整備
  共通仕様（例えば、OVAL：Open Vulnerability and Assessment Language、セキュリティ検査言語）に基づき作成された定義ファイルが流通することにより、確認手続きを共有でき、さらに、その定義ファイルに従ってチェックするプログラムを誰もが開発できる。





MyJVNバージョンチェッカ
http://jvndb.jvn.jp/apis/myjvn/

7 参考情報

- HIRT:【CSIRTメモ】チェックしておきたいぜい弱性情報
  http://www.hitachi.co.jp/hirt/publications/csirt/index.html
- JVN (Japan Vulnerability Notes)
  http://jvn.jp/
- MyJVN
  http://jvndb.jvn.jp/apis/myjvn/
  - 脆弱性対策情報の利活用基盤MyJVNの提案
    情報処理学会 コンピュータセキュリティ シンポジウム 2008（Oct.8-10, 2008）
  - MyJVNを用いた脆弱性対策情報提供サービスの検討
    情報処理学会 コンピュータセキュリティ 研究報告 Vol.2009 No.20, pp.283-288
    (Mar. 5-6, 2009)
- NVD (National Vulnerability Database)
  http://nvd.nist.gov/
- OVAL (Open Vulnerability and Assessment Language：セキュリティ検査言語)
  http://oval.mitre.org/
- CVE (Common Vulnerability and Exposures：共通脆弱性識別子)
  http://cve.mitre.org/

HITACHI
Inspire the Next

END

チェックしておきたい
ぜい弱性情報2009
＜2009.11.24＞

Hitachi Incident Response Team
http://www.hitachi.co.jp/hirt/
寺田真敏