JPCERT-PR-2007-0006

JPCERT/CC 活動概要［2007 年 4 月 1 日 ～ 2007 年 6 月 30 日 ］

2007-07-19 発行

2007-07-19 更新

活動概要トピックス

【トピックス 1】サイバークリーンセンター活動実績を公開

サイバークリーンセンターの活動内容をまとめた「平成 18 年度サイバークリーンセンター活動報告」および、2007 年 5 月度と 6 月度の「サイバークリーンセンター活動実績」が https://www.ccc.go.jp/ で公開されました。活動実績は今後毎月公開されます。

サイバークリーンセンターは、総務省・経済産業省 連携プロジェクトであるボット対策事業のポータルサイトです。JPCERT/CC は本プロジェクトにボットプログラム解析グループとして参加し、収集されたボット検体の特徴や技術の解析を行い、駆除ツールを作成しています。さらに、効率的な解析手法の検討なども行うほか、駆除ツール開発事業者と連携してその対策技術の開発も行っています。

【トピックス 2】JPCERT/CC の伊藤友里恵が FIRST の Steering Committee メンバーに再選

JPCERT/CC の業務統括である伊藤友里恵が、本年 6 月 21 日に開催された、CSIRT（Computer Security Incident Response Team)(*1)の国際的なフォーラムである FIRST（Forum of Incident Response and Security Teams）(*2)の年次会合における選挙において、Steering Committee （運営委員会）メンバーに再選され(*3)ました。JPCERT/CC は、1998 年に日本で最初の CSIRT メンバーとして FIRST に参加し、伊藤友里恵は 2005 年から同フォーラムの理事および運営委員を務めています（理事の職についても継続いたします)。今回の改選により、アジア地域選出の理事兼運営委員は、伊藤友里恵のみとなっています。

JPCERT/CC では、国内外組織を対象とした FIRST 加盟支援活動を行っております。

*1 CSIRT (Computer Security Incident Response Team シーサート)とは：

CSIRT とは、コンピュータセキュリティインシデント(リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示や、さらにそれらに至るための行為（事象）など)対応、対策支援、分析や教育、研究開発などを含めて様々な活動を行っています。

JPCERT/CC は国内外 CSIRT のコーディネーションセンター、日本の窓口である National CSIRT として活動しています。

*2 FIRST（Forum of Incident Response and Security Teams ファースト）とは：

FISRT とは、信頼性のあるコンピュータインシデントレスポンスチームで構成されている、世界

的に認められた国際組織です。加盟チーム間の信頼性の高いコミュニケーションおよび強固な連携によるコンピュータセキュリティインシデントへの対応、インシデント対策プログラムなどの普及啓発活動、技術情報の提供、方法論の開発、CSIRT の構築支援などを行っています。現在、世界経済地域から約 200 のインシデントレスポンスチームが加盟しています。JPCERT/CC は Steering Committee （運営委員会）メンバーとして、FIRST の運営に協力しています。
FIRST および参加チームに関する詳細は以下の URL をご参照下さい。
http://www.first.org/

*3 FIRST Steering Committee については、以下の URL をご参照ください。
http://www.first.org/about/organization/sc.html

【トピックス 3】JPCERT/CC 製品開発者リスト登録が 199 社となる

一般公表前の脆弱性関連情報は、ソフトウェア/ハードウエアシステム等におけるセキュリティ上の欠陥に係わる情報であり、その取扱には細心の注意を要します。脆弱性関連情報の公表前の脆弱性関連情報を必要に応じて公開することで、脆弱性情報の悪用、または障害を引き起こす危険性を最小限に食い止めるために、JPCERT/CC は、2004 年 7 月 7 日に経済産業省より公示された「ソフトウェア等脆弱性関連情報取扱基準」(*4)において、日本国内の脆弱性関連情報流通のための調整機関として指定されました。
JPCERT/CC では、脆弱性情報が発生した際、影響を受ける可能性のある製品開発者を特定し、迅速かつ確実な脆弱性情報を提供することを目的に、日本国内の製品開発者リストを策定し、その連絡先情報の整備をしてきました。2007 年 6 月 30 日現在でこの開発者リストへ登録参加を表明した開発者は 199 社となりました。

*4: ソフトウェア等脆弱性関連情報取扱基準
http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf

【トピックス 4】日本コンピュータセキュリティインシデント対応チーム協議会発足

株式会社日立製作所（執行役社長：古川 一夫)、株式会社インターネットイニシアティブ（代表取締役社長：鈴木 幸一)、有限責任中間法人 JPCERT コーディネーションセンター（代表理事：歌代 和正)、株式会社ラック（代表取締役社長：髙梨 輝彦)、日本電信電話株式会社（代表取締役社長：和田 紀夫(現 取締役会長)) およびソフトバンク BB 株式会社（代表取締役社長 兼 CEO：孫 正義）の 6 社は、4 月 17 日、国内におけるコンピュータのセキュリティを脅かす事態への対応を行う CSIRT (シーサート)活動の推進ならびに各社の有する関連組織との間の緊密な連携体制の構築などを目的とした、日本コンピュータセキュリティインシデント対応チーム協議会を共同で設立しました。JPCERT/CC は本協議会事務局を担当しています。
詳細は http://www.jpcert.or.jp/press/2007/RLS_csirt-concil_0417.pdf

【トピックス 5】組織内 CSIRT 構築支援マテリアル、ボット研究、標的型攻撃についての

JPCERT CC®

調査などの資料を公開

JPCERT/CC は、組織的なインシデント対応体制である「組織内 CSIRT」の構築を支援するための「組織内 CSIRT 構築支援マテリアル」、CSIRT が共通する課題や運営ノウハウをまとめた「コンピュータセキュリティインシデント対応チーム(CSIRT)のためのハンドブック」、ボットネット研究資料「マルウェアの最近の傾向とウェブアプリケーションの脆弱性を狙うボットの実態」、国内企業へのアンケート調査資料「標的型攻撃についての調査」など資料を公開しました。詳しくは　http://www.jpcert.or.jp/research/　をご覧ください。

活動概要

§1. インシデント報告

JPCERT/CC が 2007 年 4 月 1 日から 2007 年 6 月 30 日までの間に報告を受けたコンピュータセキュリティインシデント(*1)に関する報告の件数は 652 件(*2)でした。

*1: コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの（その疑いがある場合）を含みます。リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示や、さらにそれらに至るための行為（事象）などがあります。

*2: JPCERT/CC が受けた報告(メール、FAX)の件数です。したがって、日本国内または世界中のインシデント発生件数、傾向等を類推できるものではありません。

I. インシデント報告の送信元による分類

JPCERT/CC が受けたインシデント報告の送信元をトップレベルドメインで分類したもののうち、件数の多いものは以下の通りです。

.com	186 件
.jp	186 件
.org	158 件
.br	70 件
.edu	23 件
.net	14 件

II. インシデント報告より派生した通知連絡

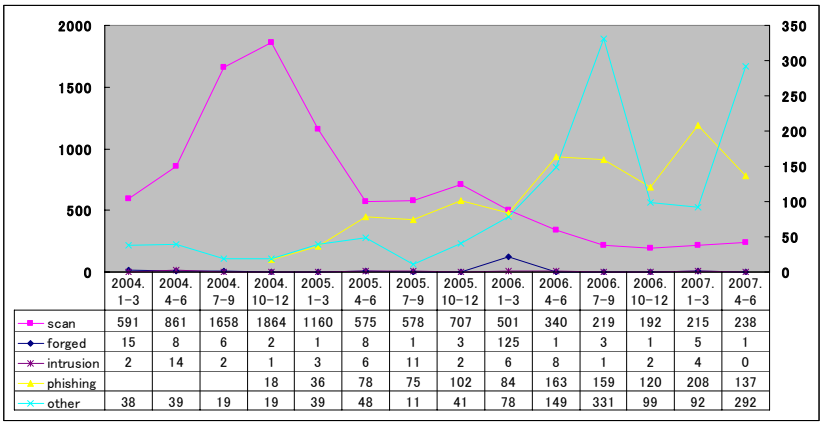
JPCERT/CC から国内外の関連するサイトに通知連絡した件数は 256 件です。

この通知連絡数は、アクセス元などへの連絡仲介依頼を含むインシデント報告に基づいて行われたものです。

III. インシデント報告のタイプ別分類

JPCERT/CC が報告を受けたインシデント件数のタイプ別分類は以下の図となります。また、報告を受けたインシデントの傾向としては、マルウェアに関する報告の増加による「other」の増加、「phishing」では国内組織のフィッシングが増加、「scan」では TCP 22 番ポートへのスキャンが依然として多い、といった点が挙げられます。

なお、1 件の報告につき複数のインシデントが含まれることがあるため、インシデントの件数は報告件数と一致しません。



	2004. 1-3	2004. 4-6	2004. 7-9	2004. 10-12	2005. 1-3	2005. 4-6	2005. 7-9	2005. 10-12	2006. 1-3	2006. 4-6	2006. 7-9	2006. 10-12	2007. 1-3	2007. 4-6
scan	591	861	1658	1864	1160	575	578	707	501	340	219	192	215	238
forged	15	8	6	2	1	8	1	3	125	1	3	1	5	1
intrusion	2	14	2	1	3	6	11	2	6	8	1	2	4	0
phishing				18	36	78	75	102	84	163	159	120	208	137
other	38	39	19	19	39	48	11	41	78	149	331	99	92	292

図 1-1: インシデント報告のタイプ別分類

scan　　：プローブ、スキャン、その他不審なアクセス
forged　　：送信ヘッダを詐称した電子メールの配送
intrusion　：システムへの侵入
phishing　：フィッシング
other　　：その他

(1) プローブ、スキャン、その他不審なアクセス（scan）

JPCERT/CC では、防御に成功したアタックや、コンピュータ/サービス/脆弱性の探査を意図したアクセス、その他の不審なアクセス等、システムへの影響が生じない、または、無視できるアクセスについて 238 件の報告を受けました。

このような探査は、一般的に自動化ツールを用いて広範囲に渡る任意のホストに対して行なわれています。脆弱性を放置していると、脆弱性の存在を検出され、ホストへの侵入等さまざまなアタックを受ける可能性があります。参考文献 [1] [2] [3] [4] [5] [6] をご参照ください。

22　(ssh)	84 件 (*1)
445　(microsoft-ds)	15 件 (*1)
1023	13 件 (*1)

5554	(sgi-esphttp)	13 件 (*1)
9898	(monkeycom)	13 件 (*1)
23	(telnet)	10 件 (*1)
21	(ftp)	7 件 (*1)
5900	(vnc-server)	7 件 (*1)
139	(netbios-ssn)	6 件 (*1)
総合的なプローブ、スキャン		98 件 (*2)

*1: ワームによる感染の試みやワームなどによって設置されたバックドアからの侵入の試みと思われるアクセスが報告されています。

*2: 総合的なプローブ、スキャンとは、同一発信元からの複数ポートに対するスキャンなど、いくつかのプローブ、スキャン情報をまとめてご報告いただいたものです。

参考文献:[7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19][20] [21] [22] [23] [24] [25] [26] [27] [28] をご参照ください。また、以下の URL もご参照ください。

TCP2967 番ポートへのスキャン増加に関する注意喚起
http://www.jpcert.or.jp/at/2006/at060021.txt

TCP139 番ポートへのスキャン増加に関する注意喚起
http://www.jpcert.or.jp/at/2006/at060012.txt

RealVNC サーバの認証が回避される脆弱性に関する注意喚起
http://www.jpcert.or.jp/at/2006/at060005.txt

TCP1025 番ポートへのスキャンの増加に関する注意喚起
http://www.jpcert.or.jp/at/2005/at050012.txt

Microsoft 製品の脆弱性を使って伝播するワームに関する注意喚起
http://www.jpcert.or.jp/at/2005/at050008.txt

Microsoft 製品に含まれる脆弱性に関する注意喚起
http://www.jpcert.or.jp/at/2005/at050007.txt

TCP1433 番ポートへのスキャンの増加に関する注意喚起
http://www.jpcert.or.jp/at/2005/at050006.txt

JPCERT CC®

VERITAS Backup Exec に含まれる脆弱性に関する注意喚起
http://www.jpcert.or.jp/at/2005/at050004.txt

OpenSSH の脆弱性を使ったシステムへの侵入に関する注意喚起
http://www.jpcert.or.jp/at/2005/at050003.txt

phpBB の脆弱性を使って伝播するワームに関する注意喚起
http://www.jpcert.or.jp/at/2004/at040011.txt

Windows LSASS の脆弱性を使って伝播するワーム W32/Sasser
http://www.jpcert.or.jp/at/2004/at040006.txt

Status Tracking Note TRJVN-2004-02 W32/Sasser ワーム
http://jvn.jp/tr/TRJVN-2004-02/

JP Vendor Status Note JVNCA-2004-02 大量に電子メールを配信するワーム
http://jvn.jp/cert/JVNCA-2004-02/

Netsky.Q のサービス運用妨害攻撃に関する注意喚起
http://www.jpcert.or.jp/at/2004/at040002.txt

Microsoft ASN.1 Library の脆弱性に関する注意喚起
http://www.jpcert.or.jp/at/2004/at040001.txt

TCP139 番ポートへのスキャンの増加に関する注意喚起
http://www.jpcert.or.jp/at/2003/at030007.txt

Microsoft IIS 5.0 の脆弱性に関する注意喚起
http://www.jpcert.or.jp/at/2003/at030003.txt

TCP135 番ポートへのスキャンの増加に関する注意喚起
http://www.jpcert.or.jp/at/2003/at030005.txt

Windows RPC の脆弱性を使用するワームに関する注意喚起
http://www.jpcert.or.jp/at/2003/at030006.txt

OpenSSL の脆弱性を使って伝播する Apache/mod_ssl ワーム

http://www.jpcert.or.jp/at/2002/at020006.txt

TCP1433 番ポートへのスキャンの増加に関する注意喚起
http://www.jpcert.or.jp/at/2002/at020002.txt

80 番ポート(HTTP)へのスキャンの増加に関する注意喚起
http://www.jpcert.or.jp/at/2001/at010023.txt

Microsoft IIS の脆弱性を使って伝播するワーム
http://www.jpcert.or.jp/at/2001/at010018.txt

Microsoft IIS の脆弱性を使って伝播するワーム"Code Red II"
http://www.jpcert.or.jp/at/2001/at010020.txt

(2) 送信ヘッダを詐称した電子メールの配送(forged)

JPCERT/CC では、差出人アドレスなどの送信ヘッダを詐称した電子メールの配送について 1 件の報告を受けました。

電子メールの送信ヘッダを詐称して、第三者へメールの配送が行なわれています。 この結果、エラーメールが詐称された差出人アドレスに送信され、コンピュータのリソースやネットワーク帯域が消費される可能性があります。また、差出人アドレスを詐称された場合、これらのメールの発信元であるという疑いをもたれる可能性があります。送信ヘッダを詐称した電子メールの配送については、参考文献 [20] [22] [29]をご参照ください。

(3) システムへの侵入(intrusion)

システムへの侵入についての報告はありませんでした。侵入を受けた場合の対応については、以下の URL で公開している文書「コンピュータセキュリティインシデントへの対応」の V.および VI. を参照してください。

コンピュータセキュリティインシデントへの対応
http://www.jpcert.or.jp/ed/2002/ed020002.txt

(4) フィッシング(phishing)

JPCERT/CC では、銀行などのサイトであると詐称して、Web のフォームなどから入力された口座番号やキャッシュカードの暗証番号といった重要情報を盗み取るフィッシングについて 137 件の報告を受けました。

フィッシングに用いる Web サイトの構築を目的とした行為には、システムへ侵入する、ドメインを乗っ取るなどの行為があります。

国内金融機関を装ったフィッシングサイトに関する注意喚起
http://www.jpcert.or.jp/at/2007/at070009.txt

DNS サーバの設定とドメイン名の登録に関する注意喚起
http://www.jpcert.or.jp/at/2005/at050005.txt

Web 偽装詐欺(phishing)の踏み台サーバに関する注意喚起
http://www.jpcert.or.jp/at/2005/at050002.txt

システムがフィッシングに用いられた場合の対応については、以下の URL で公開している文書「コンピュータセキュリティインシデントへの対応」V.および VI.を参照してください。

コンピュータセキュリティインシデントへの対応
http://www.jpcert.or.jp/ed/2002/ed020002.txt

また、フィッシングに対する Web ブラウザの設定に関しては、参考文献[30]をご参照ください。

(5) その他(other)
JPCERT/CC では、上記(1)から(4)に含まれないインシデント(サービス運用妨害 "DoS"、コンピュータウイルスや SPAM メールの受信、マルウェア情報、その他問い合わせなど)について 292 件の報告を受けました。

ID やパスワードを聞き出そうとする電話に関する注意喚起
http://www.jpcert.or.jp/at/2007/at070015.txt

DNS の再帰的な問合せを使った DDoS 攻撃に関する注意喚起
http://www.jpcert.or.jp/at/2006/at060004.txt

§2. インターネット定点観測システム(ISDAS)運用

インターネット定点観測システム(以下、ISDAS)では、インターネット上に設置した複数のセンサーから得られる情報を収集しています。これら観測情報は、世の中に流布する脆弱性情報などとあわせてインターネット上のインシデントについての脅威度などを総合的に評価するために使用されます。また、ここで収集した観測情報を一般に提供するサービスをあわせて行なっています。

I. ポートスキャン概況

インターネット定点観測システムの観測結果は、スキャン推移を表すグラフとして JPCERT/CC

の Web ページを通じて公開しています。 アクセス先ポート別グラフはスキャンログをアクセス先ポート別に集計し、総計をセンサーの台数で割った平均値を用い作成しています。

JPCERT/CC インターネット定点観測システムの説明
http://www.jpcert.or.jp/isdas/readme.html

2007 年 4 月 1 日から 2007 年 6 月 30 日までの間に ISDAS で観測されたアクセス先ポートに関する平均値の上位 1 位～5 位、6 位～10 位までの推移を図 2-1、2-2 に示します。

- アクセス先ポート別グラフ top1-5 (2007 年 4 月 1 日-6 月 30 日)

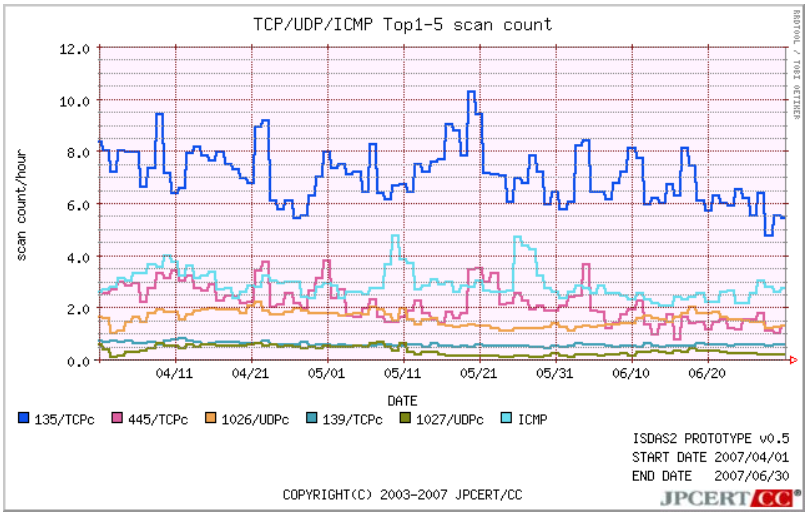


図 2-1: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2007 年 4 月 1 日-6 月 30 日)

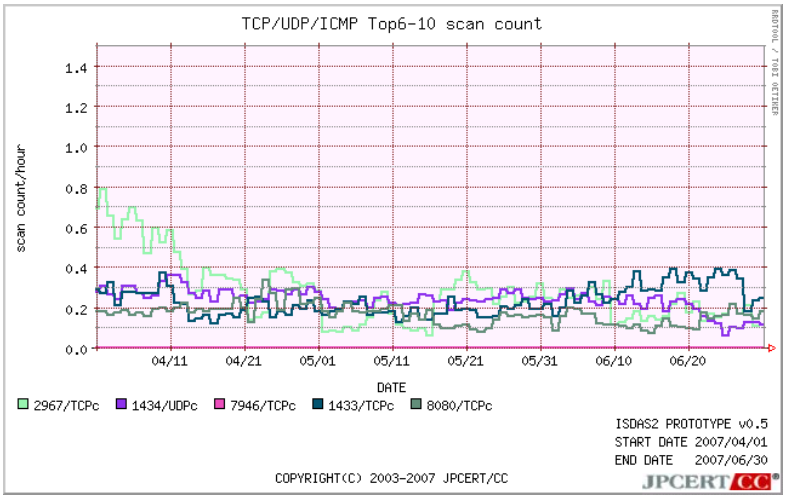


図 2-2: アクセス先ポート別グラフ top6-10

また、より長期間のスキャン推移を表すグラフとして、2006 年 7 月 1 日から 2007 年 6 月 30 日までの期間における、アクセス先ポートに関する平均値の上位 1 位～5 位、6 位～10 位までの推移を図 2-3、図 2-4 に示します。

- アクセス先ポート別グラフ top1-5 (2006 年 7 月 1 日-2007 年 6 月 30 日)

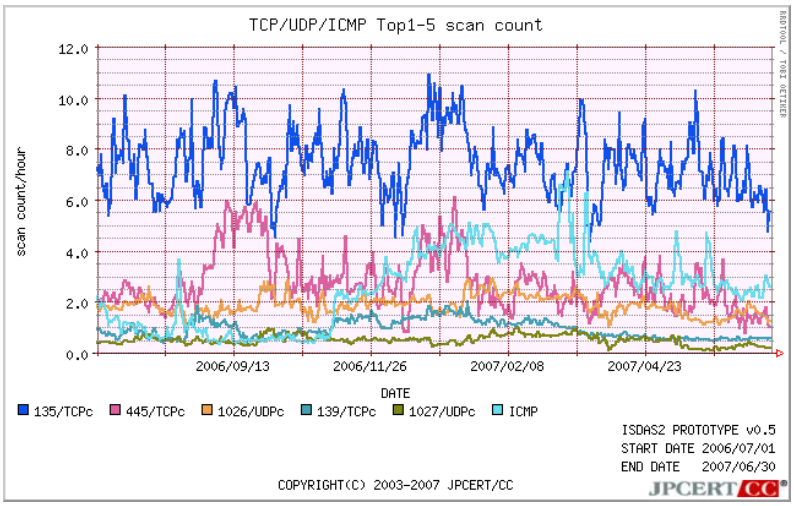


図 2-3: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2006 年 7 月 1 日-2007 年 6 月 30 日)

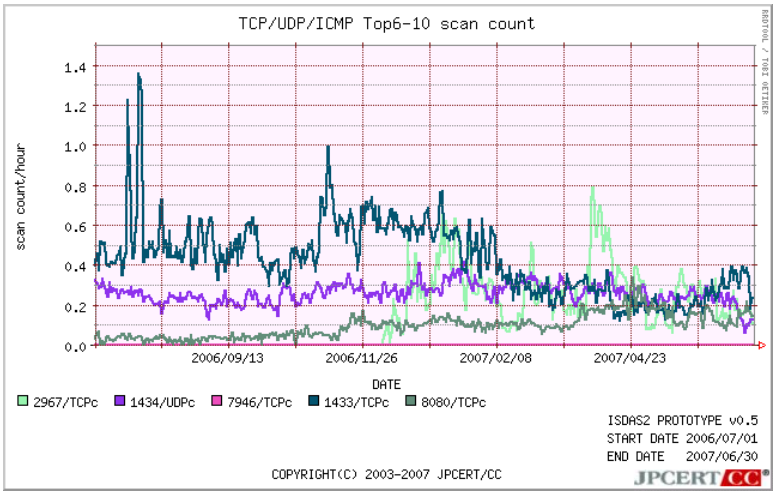


図 2-4: アクセス先ポート別グラフ top6-10

今期のスキャン先ポートの傾向も、Windows 環境を対象としたものが上位を占めています。OS やアプリケーションに脆弱性がないバージョンを使用しているか、Firewall・アンチウイルスなどの製品が正しく機能しているか、今一度確認することが重要です。

II. おもなインシデントにおける観測状況

ISDAS システムにおいて下記に示すスキャン事例を観測しました。

(1) TCP2967 番ポートへのスキャンを継続的に観測

TCP2967 番ポートへのスキャンは、2006 年 12 月初旬に初めて観測されてより一定のスキャン数を維持しています。本観測については同ポートを使用した Symantec 製品の脆弱性を狙ったスキャンであると考えられています。ベンダが配布する修正済みソフトウェアを適用することにより、本攻撃の影響を回避することが可能です。

- アクセス先ポート別グラフ TCP2967 番ポート（2006/11/01-2007/6/30）

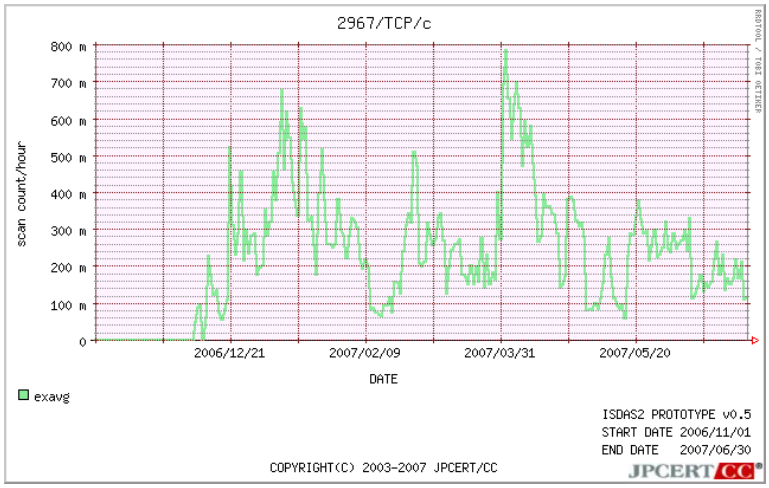


図 2-6: アクセス先ポート別グラフ TCP 2967 番ポート

TCP2967 番ポートへのスキャン増加に関する注意喚起

http://www.jpcert.or.jp/at/2006/at060021.txt

(2) TCP5900 番ポートへのスキャン増加を観測

TCP5900 番ポートへのスキャンを引き続き観測しています。本観測については同ポートを使用したサービスである RealVNC の脆弱性を狙ったスキャンの可能性が考えられます。ベンダが配布する修正済みソフトウェアを適用することにより、本攻撃の影響を回避することが可能です。

- アクセス先ポート別グラフ TCP 5900 番ポート（2006/4/1-2007/6/30）

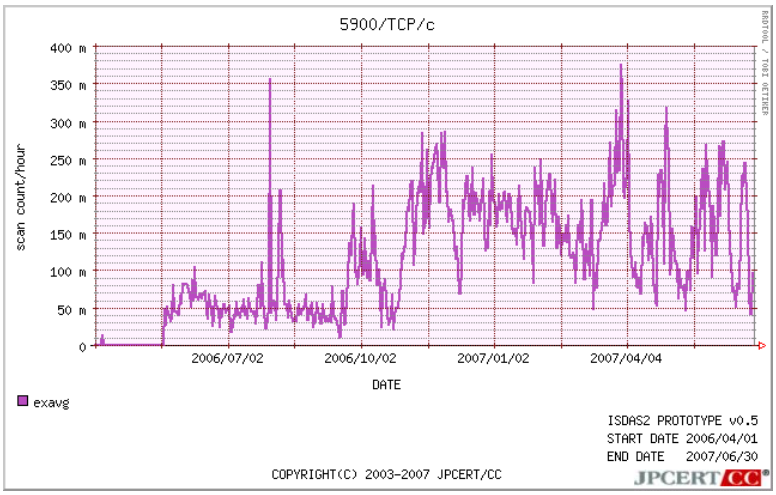


図 2-7: アクセス先ポート別グラフ TCP 5900 番ポート

RealVNC サーバの認証が回避される脆弱性に関する注意喚起
http://www.jpcert.or.jp/at/2006/at060005.txt

(3) ICMP パケットの増加を観測

2006 年 11 月上旬より ICMP のパケットの増加を観測しています。これら ICMP パケットは、一部ウイルスの活動時に送信されている可能性があります。(この場合送信元 IP アドレスは詐称されている可能性があります) ICMP パケットの受信数が昨年同時期に比べて 3 倍近いレベルを維持していることから、未だこのような活動を行うウイルスが一部で流行していると推測されます。ウイルス等対策ソフトウェアの定義ファイルを最新に保つことにより、このウイルスの影響を低減することが可能です。

- ICMP パケット受信グラフ（2007/4/1-2007/6/30）

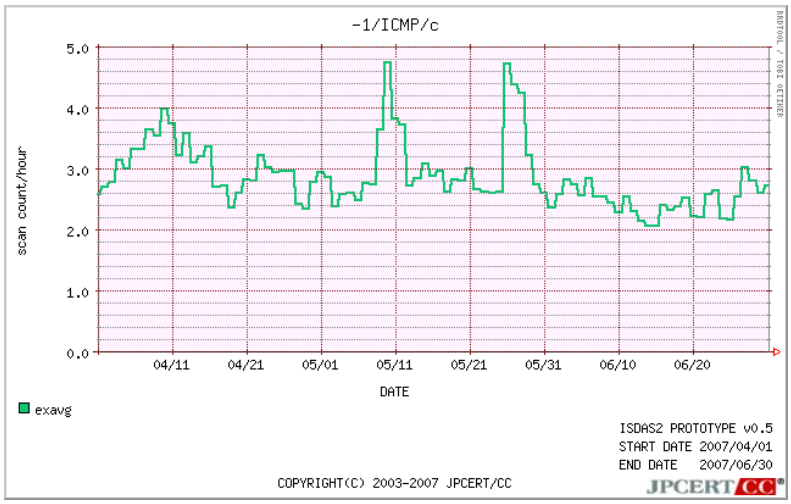


図 2-8: ICMP パケット受信グラフ

JPCERT CC®

§3. 脆弱性情報流通

JPCERT/CC では、脆弱性関連情報を適切な範囲に開示し、対策の促進を図るための活動を行なっています。国内では、経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」において、製品開発者とのコーディネーションを行なう調整機関として指定されています。また、米国 CERT/CC や英国 CPNI との協力関係を結び、国内のみならず世界的な規模で脆弱性関連情報の流通対策業務を進めています。

I. コーディネーションを行い公開した脆弱性情報および対応状況

2007 年 04 月 01 日から 2007 年 06 月 30 日までの間に、JPCERT/CC が日本国内の製品開発者（ベンダ）などの関連組織とのコーディネーションを行ない、公開した脆弱性情報および対応状況は 31 件です。

このうち、経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」に従って、独立行政法人情報処理推進機構（IPA）に報告され、公開された脆弱性情報は 23 件です。

JVN#44532794　rktSNS におけるクロスサイトスクリプティングの脆弱性
JVN#74063879　sHTTPd におけるクロスサイトスクリプティングの脆弱性
JVN#05187780　Hiki において任意のファイルが削除可能な脆弱性
JVN#90438169　雷電 HTTPD におけるクロスサイトスクリプティングの脆弱性
JVN#16535199　Apache Tomcat の Accept-Language ヘッダの処理に関するクロスサイトスクリプティングの脆弱性
JVN#27203006　Internet Explorer における MHTML により任意のスクリプトが実行される脆弱性
JVN#95019167　Internet Explorer における MHTML によるダウンロードのダイアログボックス回避の脆弱性
JVN#64851600　Apache Tomcat 付属のサンプルプログラムにおけるクロスサイトスクリプティングの脆弱性
JVN#07100457　Apache Tomcat におけるクロスサイトスクリプティングの脆弱性
JVN#63602912　dot Project におけるクロスサイトスクリプティングの脆弱性
JVN#23891849　ADPLAN におけるクロスサイトスクリプティングの脆弱性
JVN#89497739　Meneame におけるクロスサイトスクリプティングの脆弱性
JVN#19240523　HP System Management Homepage におけるクロスサイトスクリプティングの脆弱性
JVN#38605899　Mozilla Firefox におけるクロスサイトスクリプティングの脆弱性
JVN#92832583　Advance-Flow におけるクロスサイトスクリプティングの脆弱性
JVN#81294906　ホームページ・ビルダー付属の CGI サンプルプログラムにおける OS コマンドインジェクションの脆弱性
JVN#44724673　Java Web Start において許可されていないシステムクラスが実行される脆弱性

JVN#36628264　Lunascape の RSS リーダ機能において任意のスクリプトが実行される脆弱性
JVN#06735665　キヤノン ネットワークカメラサーバーVB100 シリーズにおけるクロスサイトスクリプティングの脆弱性
JVN#19445002　APOP におけるパスワード漏えいの脆弱性
JVN#91305178　InfoBarrier4 の自己復号型ファイルにおける脆弱性
JVN#84646028　open-gorotto におけるクロスサイトスクリプティングの脆弱性
JVN#62334841　「私本管理 Plus Ver2 GOOUT」におけるディレクトリトラバーサルの脆弱性

また、残りの 8 件は海外 CSIRT とのパートナーシップに基づき、JPCERT/CC が日本国内のベンダのコーディネーションを行い、脆弱性情報を公開しました。

JVNTA07-177A　MIT Kerberos に複数の脆弱性
JVNVU#267289　IPv6 Type0 ルーティングヘッダの問題
JVNVU#754281　RSA BSAFE Cert-C および Crypto-C にサービス運用妨害(DoS) の脆弱性
JVNVU#684664　libpng におけるサービス運用妨害(DoS)の脆弱性
JVNVU#718460　BIND におけるサービス運用妨害(DoS)の脆弱性
JVNVU#704024　MIT Kerberos 5 krb5_klog_syslog()におけるスタックオーバーフローの脆弱性
JVNVU#220816　MIT Kerberos 5 telnet deamon における任意のユーザとしてログインできる脆弱性
JVNVU#419344　MIT Kerberos 5 GSS-API ライブラリにおけるメモリ二重開放の脆弱性

II. 海外 CSIRT との脆弱性関連情報流通協力体制の構築、国際的な活動

JPCERT/CC では、国際的な枠組みにおける脆弱性関連情報の円滑な流通のため、海外の CSIRT との協力関係を構築、強化しています。具体的には、報告された脆弱性関連情報の共有、ベンダへの通知の共同オペレーション、公開日の調整、各国ベンダ情報等、公開情報の共有を行っています。また、情報流通を効率化するための共通ガイドラインやシステム構築、データ交換フォーマット、アドバイザリの標準フォーマットの策定等を共同で進めています。

主な関係機関は米国 CERT/CC、英国 CPNI です。各機関の詳細については参考文献 [31] [32] をご参照ください。また以下の URL もご参照ください。

脆弱性関連情報コーディネーション概要
http://www.jpcert.or.jp/vh/

III. 日本国内の脆弱性情報流通体制の整備

JPCERT/CC では、経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」(以下、本基準) に従って、日本国内の脆弱性情報流通体制を整備しています。

本基準については参考文献 [33] をご参照ください。また以下の URL もご参照ください。

脆弱性関連情報コーディネーション概要
http://www.jpcert.or.jp/vh/

「情報セキュリティ早期警戒パートナーシップ」の運用を開始
http://www.jpcert.or.jp/press/2004/0708.txt

情報セキュリティ早期警戒パートナーシップガイドライン（改訂版）
http://www.jpcert.or.jp/vh/partnership_guide2007.pdf

JPCERT/CC 脆弱性関連情報取り扱いガイドライン
http://www.jpcert.or.jp/vh/guideline.pdf

主な活動は以下の通りです。

(1) 受付機関である独立行政法人情報処理推進機構（IPA）との連携
本基準では、受付機関に IPA、調整機関に JPCERT/CC が指定されています。このことから、JPCERT/CC は IPA と緊密に情報交換を行っています。また、脆弱性検証ツールに関しても IPA との連携のもと分析を行っています。IPA の詳細については参考文献［34］をご参照ください。本基準における IPA の活動および四半期毎の届出状況については、参考文献［35］をご参照ください。

(2) 日本国内ベンダとの連携
本基準では、JPCERT/CC が脆弱性情報を提供する先として、日本国内のベンダリスト(製品開発者リスト)を作成し、各ベンダの連絡先情報を整備することが示されています。JPCERT/CC では、連絡先情報の整備に際し、ベンダの皆様に製品開発者としての登録をお願いしています。登録の詳細については、以下の URL をご参照ください。なお、2007 年 06 月 30 日の時点で 199 社のベンダの皆様に、ご登録をいただいています。

JPCERT コーディネーションセンター製品開発者リスト登録規約
http://www.jpcert.or.jp/vh/agreement.pdf

(3) Japan Vulnerability Notes (JVN)の運用　　http://jvn.jp/
JPCERT/CC は IPA と共同で、JVN を運用しています。JVN は、JPCERT/CC が取り扱った脆弱性情報に関して日本国内の製品開発者の脆弱性への対応状況を公開するサイトです。これらの脆弱性情報には、本枠組みに参加している日本国内の製品開発者の対応状況も含まれています。
JVN では上記「I. コーディネーションを行い公開した脆弱性情報および対策状況」以外に当該期間中に 15 件の脆弱性情報を公開しました。

また、JVN の利用者や製品開発者からいただいたご意見に基づき、JVN の見やすさの向上とコンテンツの充実を目的にリニューアルし、4 月 25 日に公開しました。

JVNVU#138545 JRE (Java Runtime Environment)のイメージ解析コードにバッファオーバーフローの脆弱性
JVNVU#949817 Yahoo! Messenger の Yahoo! Webcam image upload ActiveX コントロールにバッファオーバーフローの脆弱性
JVNVU#932217 Yahoo! Messenger の Yahoo! Webcam view utilities ActiveX コントロールにバッファオーバーフローの脆弱性
JVNTA07-163A Microsoft 製品における複数の脆弱性
JVNTA07-151A Mozilla 製品における複数の脆弱性
JVNVU#773720 Samba NDR MS-RPC におけるバッファオーバーフローの脆弱性
JVNVU#268336 Samba におけるコマンドインジェクションの脆弱性
JVNTA07-128A Microsoft 製品における複数の脆弱性
JVNTA07-109A Apple の Mac 製品に複数の脆弱性
JVNTA07-108A Oracle 製品に複数の脆弱性
JVNTA07-103A Microsoft DNS の RPC management インターフェースにおけるバッファオーバーフローの脆弱性
JVNTA07-100A Microsoft 製品における複数の脆弱性
JVNTA07-093B MIT Kerberos に複数の脆弱性
JVNTA07-093A Microsoft Windows アニメーションカーソルの脆弱性
JVNTA07-089A Microsoft Windows アニメーションカーソルにおけるスタックバッファオーバフローの脆弱性

§4. 公開文書

2007 年 4 月 1 日から 2007 年 6 月 30 日までの間に JPCERT/CC が公開した文書は、注意喚起 13 件(更新を含む)、JPCERT/CC レポート 12 件、調査/研究資料 25 件、及びプレスリリース 5 件です。詳細は以下の通りです。

I. 注意喚起 13 件（更新を含む） http://www.jpcert.or.jp/at/

2007-06-28 複数の脆弱性を使用する攻撃ツール MPack に関する注意喚起(公開)
2007-06-19 ID やパスワードを聞き出そうとする電話に関する注意喚起(更新)
2007-06-14 ID やパスワードを聞き出そうとする電話に関する注意喚起(公開)
2007-06-13 2007 年 6 月 Microsoft セキュリティ情報（緊急 4 件含）に関する注意喚起(公開)
2007-05-24 複数の Cisco 製品における DoS の脆弱性に関する注意喚起(公開)
2007-05-14 2007 年 5 月 Microsoft セキュリティ情報(緊急 7 件)に関する注意喚起（更新)

2007-05-09　Java Web Start の脆弱性に関する注意喚起（更新）
2007-05-09　2007 年 5 月 Microsoft セキュリティ情報（緊急 7 件）に関する注意喚起（公開）
2007-05-08　Java Web Start の脆弱性に関する注意喚起（公開）
2007-04-11　Windows アニメーション カーソル処理の未修正の脆弱性に関する注意喚起（更新）
2007-04-11　2007 年 4 月 Microsoft セキュリティ情報（緊急 5 件含）に関する注意喚起（公開）
2007-04-04　Windows アニメーション カーソル処理の未修正の脆弱性に関する注意喚起（更新）
2007-04-03　国内金融機関を装ったフィッシングサイトに関する注意喚起（公開）

II. JPCERT/CC レポート 12 件　　http://www.jpcert.or.jp/wr/
JPCERT/CC レポート内で扱ったセキュリティ関連情報の項目数は合計して 84 件、「今週の一口メモ」のコーナーで紹介した情報は 12 件です。

III. 調査/研究 資料　25 件　　http://www.jpcert.or.jp/research/
(1) マルウェアの最近の傾向とウェブアプリケーションの脆弱性を狙うボットの実態
(2) P2P 型ボット分析レポート
(3) 標的型攻撃についての調査
(4) 組織内 CSIRT 構築支援マテリアルのフルパッケージ
(5) 組織内 CSIRT の必要性
(6) 組織内 CSIRT の役割
(7) 組織内 CSIRT の活動
(8) 組織内 CSIRT の要員
(9) 組織内 CSIRT の形態
(10) 組織内 CSIRT の構築プロセス
(11) 組織内 CSIRT の実作業
(12) インシデント対応マニュアルの作成について
(13) 組織内 CSIRT の情報管理と設備について
(14) 組織内 CSIRT における電話応対について
(15) PGP の説明に役立つデータ
(16) コンピューターセキュリティインシデント対応チーム（CSIRT）のためのハンドブック
(17) グッド・プラクティス・ガイドプロセス制御と SCADA セキュリティガイド
　1. 事業リスクの理解
(18) グッド・プラクティス・ガイドプロセス制御と SCADA セキュリティガイド
　2.セキュア・アーキテクチャの実装
(19) グッド・プラクティス・ガイドプロセス制御と SCADA セキュリティガイド
　3. 対応能力の確立
(20) グッド・プラクティス・ガイドプロセス制御と SCADA セキュリティガイド
　4.意識とスキルの改善

(21) グッド・プラクティス・ガイドプロセス制御と SCADA セキュリティガイド
5.サード・パーティ・リスクの管理
(22) グッド・プラクティス・ガイドプロセス制御と SCADA セキュリティガイド
6.プロジェクトへの参画
(23) グッド・プラクティス・ガイドプロセス制御と SCADA セキュリティガイド
7.継続した統制の確立
(24) グッド・プラクティス・ガイドプロセス制御・SCADA セキュリティ
(25) SCADA およびプロセス制御ネットワークにおけるファイアウォールの利用についての
NISCC グッド・プラクティス・ガイド

IV. プレスリリースの配信 5 件　　http://www.jpcert.or.jp/press/
2007-06-04 「インターネット美化運動 2007～あなたの参加がネットを変える～」開催のおしらせ
2007-05-24　マイクロソフトと JPCERT/CC セキュリティ分野で包括的な技術協力で合意
2007-04-25　JVN のリニューアルと脆弱性対策情報データベースの公開について
2007-04-19　ソフトウエア等の脆弱性関連情報に関する届出状況
[2007 年第 1 四半期（1 月～3 月)]
2007-04-17　日本コンピュータセキュリティインシデント対応チーム協議会発足のお知らせ

§5. その他の活動
2007 年 4 月 1 日から 2007 年 6 月 30 日までの間に JPCERT/CC が実施した、上記§1.～4.以外の活動は以下の通りです。

I. APCERT 事務局運営　　http://www.jpcert.or.jp/english/apcert/
アジア太平洋地域の CSIRT の集まりである、APCERT(Asia Pacific Computer Emergency Response Team）の事務局を担当しています。

II. FIRST レプリカサーバの運用　　http://www.first.org/
FIRST (Forum of Incident Response and Security Teams）の Web サーバ www.first.org のレプリカサーバ（ミラーサーバ）を運用し、FIRST の活動に貢献しています。

III. FIRST Steering Committee への参画　　http://www.first.org/about/organization/sc.html
FIRST Steering Committee のメンバーとして、JPCERT/CC の職員が選出され、FIRST の運営に協力しています。

IV. その他講演など
(1) RSA Conference 2007(2007 年 4 月 25,26 日)において講演

プロが語る情報セキュリティの真実～脅威の現状とその対策～
https://rsacon2007.smartseminar.jp/public/application/add/36?lang=ja#C2
ソフトウェア製品における脆弱性対応の実情～問題点と対策～
https://rsacon2007.smartseminar.jp/public/application/add/36?lang=ja#C4

(2) IAjapan 第 4 回迷惑メール対策カンファレンス(2007 年 5 月 27 日)において講演

国内外のフィッシング傾向と対策
http://www.iajapan.org/anti_spam/event/2007/conf0528/program.html

(3) Interop Tokyo 2007 において講演(2007 年 6 月 14 日)

ボット対策事業「サイバークリーンセンター」プロジェクト始動
～成果と浮かび上がった厳しい実態～
http://www.interop.jp/index.html

(4) 大阪大学社会人教育講座セキュア・ネットワークセミナー2007 (2007 年 6 月 21 日)
において講演

「インターネット上のセキュリティインシデントとその対策」
http://www.senri-i.or.jp/new/200703/secure2007.html

Appendix

[1] IN-98.02: New Tools Used For Widespread Scans
http://www.cert.org/incident_notes/IN-98.02.html
[2] IN-98.04: Advanced Scanning
http://www.cert.org/incident_notes/IN-98.04.html
[3] IN-98.05: Probes with Spoofed IP Addresses
http://www.cert.org/incident_notes/IN-98-05.html
[4] IN-98.06: Automated Scanning and Exploitation
http://www.cert.org/incident_notes/IN-98-06.html
[5] IN-99-01: "sscan" Scanning Tool
http://www.cert.org/incident_notes/IN-99-01.html
[6] Packet Filtering for Firewall Systems
http://www.cert.org/tech_tips/packet_filtering.html
[7] CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow in IIS Indexing Service DLL

http://www.cert.org/advisories/CA-2001-19.html

[8] CA-2001-26 Nimda Worm

http://www.cert.org/advisories/CA-2001-26.html

[9] IN-2002-04: Exploitation of Vulnerabilities in Microsoft SQL Server

http://www.cert.org/incident_notes/IN-2002-04.html

[10] CA-2002-27 Apache/mod_ssl Worm

http://www.cert.org/advisories/CA-2002-27.html

[11] AL-2002.12 W32/BUGBEAR@MM Virus

http://www.auscert.org.au/render.html?it=2447

[12] AU-2002.008 Updated Information Regarding BugBear Virus

http://www.auscert.org.au/render.html?it=2452

[13] IN-2002-06: W32/Lioten Malicious Code

http://www.cert.org/incident_notes/IN-2002-06.html

[14] IN-2003-01: Malicious Code Propagation and Antivirus Software Updates

http://www.cert.org/incident_notes/IN-2003-01.html

[15] CA-2003-04 MS-SQL Server Worm

http://www.cert.org/advisories/CA-2003-04.html

[16] CA-2003-08 Increased Activity Targeting Windows Shares

http://www.cert.org/advisories/CA-2003-08.html

[17] CA-2003-09 Buffer Overflow in Core Microsoft Windows DLL

http://www.cert.org/advisories/CA-2003-09.html

[18] CA-2003-28 Buffer Overflow in Windows Workstation Service

http://www.cert.org/advisories/CA-2003-28.html

[19] CERT/CC Current Activity W32/Welchia Worm

http://www.cert.org/current/archive/2003/08/18/archive.html#welchia

[20] IN-2004-01: W32/Novarg.A Virus

http://www.cert.org/incident_notes/IN-2004-01.html

[21] TA04-041A: Multiple Vulnerabilities in Microsoft ASN.1 Library

http://www.us-cert.gov/cas/techalerts/TA04-041A.html

[22] TA04-028A: W32/MyDoom.B Virus

http://www.us-cert.gov/cas/techalerts/TA04-028A.html

[23] Sasser ワームについてのお知らせ

http://www.microsoft.com/japan/security/incident/sasser.mspx

[24] Microsoft Windows のセキュリティ修正プログラム (835732) (MS04-011)

http://www.microsoft.com/japan/technet/security/bulletin/MS04-011.mspx

[25] US-CERT Current Activity: W32/Sasser

http://www.us-cert.gov/current/archive/2004/06/24/archive.html#sasser

[26] US-CERT Vulnerability Note VU#909678
http://www.kb.cert.org/vuls/id/909678
[27] US-CERT Current Activity: Santy Worm
http://www.us-cert.gov/current/archive/2004/12/21/archive.html#Santy
[28] US-CERT Vulnerability Note VU#497400
http://www.kb.cert.org/vuls/id/497400
[29] Email Bombing and Spamming
http://www.cert.org/tech_tips/email_bombing_spamming.html
[30] Frequently Asked Questions About Malicious Web Scripts Redirected by Web Sites
http://www.cert.org/tech_tips/malicious_code_FAQ.html
[31] CERT Coordination Center (CERT/CC)
http://www.cert.org/
[32] Centre for the Protection of National Infrastructure (CPNI)
http://www.cpni.gov.uk/
[33] 脆弱性関連情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
[34] 独立行政法人情報処理推進機構
http://www.ipa.go.jp/
[35] 情報処理推進機構セキュリティセンター 脆弱性関連情報の取扱い
http://www.ipa.go.jp/security/vuln/