JPCERT-PR-2008-0003

JPCERT/CC 活動概要 [2008 年 1 月 1 日 ～ 2008 年 3 月 31 日]

2008-04-07-発行

【 活動概要トピックス 】

―トピック 1 ―

国内ユーザを狙ったフィッシングサイトの増加、マルウェア配付サイトへの誘導を行う大規模な Web 改ざん事案への対応

国内の金融機関やオークションサイトを装ったフィッシングサイトについては、これまでにも報告されていましたが、2008 年 1 月 28 日以降、立て続けに複数の報告があり、さらに、国内 ISP を装ったフィッシングサイトに関する初めての報告がありました。これを受けて、対象サイト管理者への調整を行うとともに、2008 年 2 月 7 日「国内ブランドを装ったフィッシングサイトに関する注意喚起」を発行しました。
また、2008 年 3 月、国内外の多数の Web サイトが SQL インジェクション攻撃により改ざんされる事案が発生しました。改ざんされたサイトにはマルウェア配布サイトへ誘導するスクリプトが埋め込まれ、閲覧者のコンピュータにマルウェアをインストールさせてしまう危険性があったため、マルウェア配付サイトの管理者などに対する調整を行うとともに、2008 年 3 月 14 日、システム管理者や一般ユーザへの周知を目的とした「SQL インジェクションによる Web サイト改ざんに関する注意喚起」を発行しました。
これらのインシデントに関する有害サイトは、国内外の関係者の協力により、2008 年 4 月 1 日現在においては閉鎖が確認されていますが、いったん閉鎖が確認されても、後日、再度立ち上がってしまうことがあり得ます。同種の事案では、実際にそのようなケースが多いことから、引き続き注意が必要です。また、改ざんされた Web サイトの管理者におかれては、修正及び再発防止に心がけていただけるようお願いいたします。

JPCERT/CC Alert:国内ブランド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/2008/at080002.txt

JPCERT/CC Alert:SQL インジェクションによる Web サイト改ざんに関する注意喚起
http://www.jpcert.or.jp/at/2008/at080005.txt

株式会社ラック
日本をターゲットとした SQL インジェクションによるホームページ改ざん行為と、同行為により改ざんされたページへのアクセスによるマルウェア感染について
http://www.lac.co.jp/news/press20080312.html

JPCERT CC®

― トピック 2 ―

ルータ等の組込みソフトに関する脆弱性関連情報の公開がじわり増加

早期警戒パートナーシップに基づき 2008 年 1 月から 3 月の間に調整･公開をした脆弱性関連情報の傾向として、ルータ等の製品の組込みソフトウエアに関する脆弱性の比重の増加があげられます。その背景には、脆弱性の研究者や発見者の関心が、研究や対策が進んできている OS や汎用アプリケーション製品から、組込み系のソフトウエアに移行しているという事情があるものと考えられます。研究者の関心の移行は、攻撃の脅威の傾向を反映するものであるとも考えられることから、製品開発者、利用者においても一層の注意が必要であると考えられます。

脆弱性関連情報の詳細は　http://jvn.jp/

― トピック 3 ―

アジア太平洋地域 6 カ国に対する CSIRT トレーニングを実施

近年、インシデントが国境を越えて発生する中で、円滑なインシデント対応のための国際連携がますます重要になっています。JPCERT/CCは、アジア太平洋地域各国に対し、インシデント対応調整の窓口となるNational CSIRT機能の構築のためのノウハウの提供や技術支援を行なっています。その一環として、2008年3月、財団法人海外技術者研修協会*1に主催をお願いする形で、アジア太平洋地域6カ国[*2]を対象に、CSIRT 機能構築の支援、インシデント対応レベルの底上げ及び相互の連携強化を目的とする5日間のCSIRTトレーニングを実施しました。

財団法人海外技術者研修協会 ：http://www.aots.or.jp/index.html
参加 6 カ国：インドネシア、カンボジア、スリランカ、バングラデシュ、フィリピン、モンゴル

― トピック 4 ―

重要インフラ情報セキュリティフォーラム 2008 を開催

JPCERT/CC は、独立行政法人情報処理推進機構（IPA）とともに、コンピュータセキュリティインシデントによる社会的、経済的なリスクを低減するため、セキュリティ対策の主要素であるコンピュータ・システムの脆弱性対策とネットワークセキュリティ対策等について、国内外関係組織と連携しさまざまな取り組みを行なっています。
その活動の一環として、2008 年 2 月、重要インフラ事業（情報通信、金融、電力、航空、鉄道、ガス、政府・行政サービス、医療、水道、物流等の事業）に携わる方々や、これらの事業者各社に対してシステムやサービスを提供している事業者の方々、これらの分野における情報セキュリティの問題に関心をお持ちの方々等を対象に、「重要インフラ情報セキュリティフォーラム 2008」を開催し、情報セキュリティに関する管理的対策や技術的対策等に関する多様な研究、検討の状況等について御講演を

いただきました。大勢の方々にご参加をいただき、重要インフラ事業分野における情報セキュリティへの関心の高さを実感することができました。

重要インフラ情報セキュリティフォーラム 2008 の詳細は
http://www.jpcert.or.jp/event/ci-2008.html

JPCERT CC®

【 活動概要 】

§1.情報提供活動

JPCERT/CC のホームページ、RSS、約 24,000 件のメーリングリストなどで情報提供をしています。

I. 注意喚起

深刻且つ影響範囲の広い脆弱性などに関する情報を提供しています。

発行件数： 6 件 http://www.jpcert.or.jp/at/

2008-03-14 SQL インジェクションによる Web サイト改ざんに関する注意喚起
2008-03-12 2008 年 3 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)
2008-02-13 国内ブランドを装ったフィッシングサイトに関する注意喚起 (更新)
2008-02-13 2008 年 2 月 Microsoft セキュリティ情報 (緊急 6 件含) に関する注意喚起 (公開)
2008-02-07 国内ブランドを装ったフィッシングサイトに関する注意喚起 (公開)
2008-01-09 2008 年 1 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起 (公開)

II. JPCERT/CC レポート

JPCERT/CC が得たセキュリティ関連情報から重要と判断した抜粋情報で、毎週水曜日(祝祭日を除く)に発行しています。また、ひとくちメモとして、セキュリティに関する豆知識情報も提供しています。

発行件数：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 104 件、「今週のひとくちメモ」のコーナーで紹介した情報は 12 件です。

III. 技術メモ

一般的な技術情報やインシデントに対応する際の注意事項などを紹介した文書を提供しています。

2008-03-31 インターネットを介したサービスにおける適切な HTTPS の運用 (Version 1)

JPCERT CC®

§2. インシデント報告

2008 年 1 月 1 日から 2008 年 3 月 31 日までの間に JPCERT/CC が受け付けたメール、FAX のうち、コンピュータセキュリティインシデント（以下、インシデント）に関する報告は 545 件でした。インシデントの件数を IP アドレス別に計上すると 684 件となりました。

インシデントによる被害の拡大・再発防止のため、今後とも JPCERT/CC への情報提供にご協力お願い致します。
インシデントの報告方法については、以下の URL をご参照ください。

http://www.jpcert.or.jp/form/

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。

.jp	228 件
.org	135 件
.com	82 件
.br	41 件
.pl	19 件
.edu	12 件

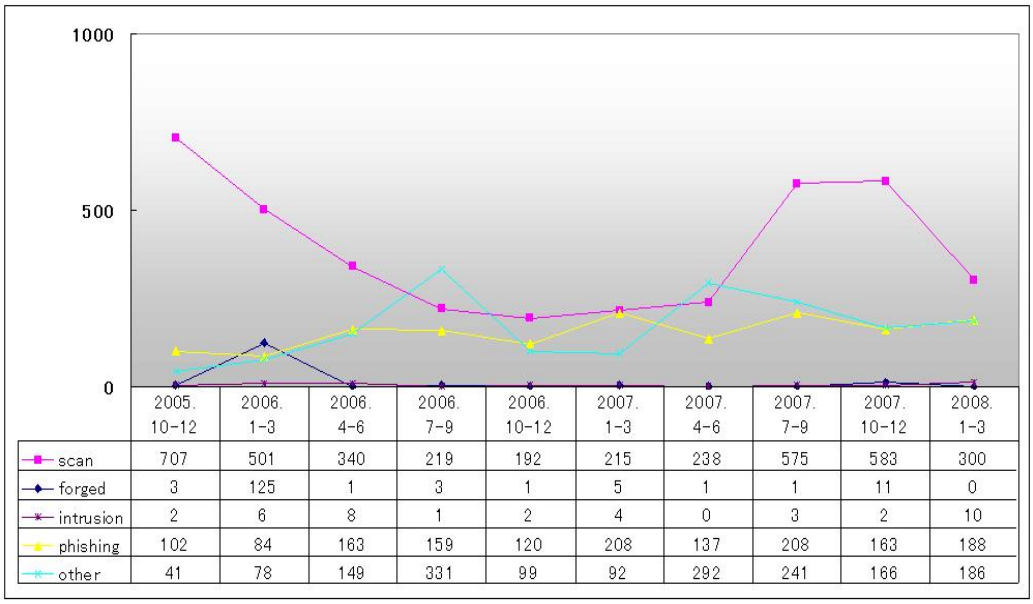
II. インシデント報告より派生した通知連絡

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 492 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. インシデントのタイプ別分類

JPCERT/CC が報告を受けたインシデント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、SQL インジェクションに関する報告の増加による「intrusion」の増加、「phishing」では国内金融機関のフィッシングサイトが増加し、国内 ISP を騙ったサイトが新たに出現した点などが挙げられます。

なお、フィッシングは多くの場合、サーバへの侵入「intrusion」を伴います。下記件数には現れていませんが、フィッシングの加害者とならないためにも、サーバ管理者の方は侵入へのセキュリティ対策を心がけてください。



	2005. 10-12	2006. 1-3	2006. 4-6	2006. 7-9	2006. 10-12	2007. 1-3	2007. 4-6	2007. 7-9	2007. 10-12	2008. 1-3
scan	707	501	340	219	192	215	238	575	583	300
forged	3	125	1	3	1	5	1	1	11	0
intrusion	2	6	8	1	2	4	0	3	2	10
phishing	102	84	163	159	120	208	137	208	163	188
other	41	78	149	331	99	92	292	241	166	186

図 1-1 インシデントタイプ別報告件数推移

(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 300 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。セキュリティ対策を施さずにホストを放置していると、脆弱性の存在を検出され、ホストへの侵入等深刻なインシデントに繋がる可能性があります。

80（http）	151 件（*1）
22（ssh）	123 件（*1）
5900（vnc-server）	6 件（*1）
10000（ndmp）	4 件（*1）
21（ftp）	3 件（*1）
20000（dnp）	3 件
総合的なプローブ、スキャン	11 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。

(2)　送信ヘッダを詐称した電子メールの配送（forged）

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の報告はありませんでした。

(3)　システムへの侵入（intrusion）

JPCERT/CC では、管理者権限の盗用が認められる場合を含むシステムへの侵入について 10 件の報告を受領しています。侵入方法としては、次のような事例が報告されています。

- 脆弱なパスワードを総当り攻撃、辞書攻撃で解読され侵入された
- コマンドインジェクション攻撃

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

今回受領した報告において、侵入後に行なわれた操作として指摘されている行為のうち、主なものを以下に紹介します。

- システムの改ざん（ファイルの置き換え、ログの消去、Web ページの改ざんなど）

(4)　フィッシング（phishing）

JPCERT/CC では、銀行やオークション、ISP などのオンラインサービスを装った Web サイトへサービス利用者を誘導し、サービス利用者の口座番号、暗証番号、個人情報などの重要な情報を盗み取ろうとするフィッシングについて、188 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。

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

フィッシングに関する FAQ
http://www.jpcert.or.jp/ir/faq.html

(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、マルウェア情報など）について 186 件の報告を受けました。マルウェア情報については、影響が大きいと考えられるもの、分析依頼を受けているものについて適宜分析を実施し、対策に関する情報の提供やインシデント対応を実施しました。

IV. インシデント報告以外のメール、FAX について

JPCERT/CC では、インシデント対応等に関する質問や何らかの対応が必要だったメール、FAX を 85 件受けました。一部を以下で紹介します。

- 情報を盗み取るマルウェアに関する報告
- APCERT 事務局窓口宛に来たインシデント報告の対応

§3. 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の一部を JPCERT/CC Web ページなどで公開しています。

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

2008 年 1 月 1 日から 2008 年 3 月 31 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 3-1、3-2 に示します。

- アクセス先ポート別グラフ top1-5 (2008 年 1 月 1 日-3 月 31 日)

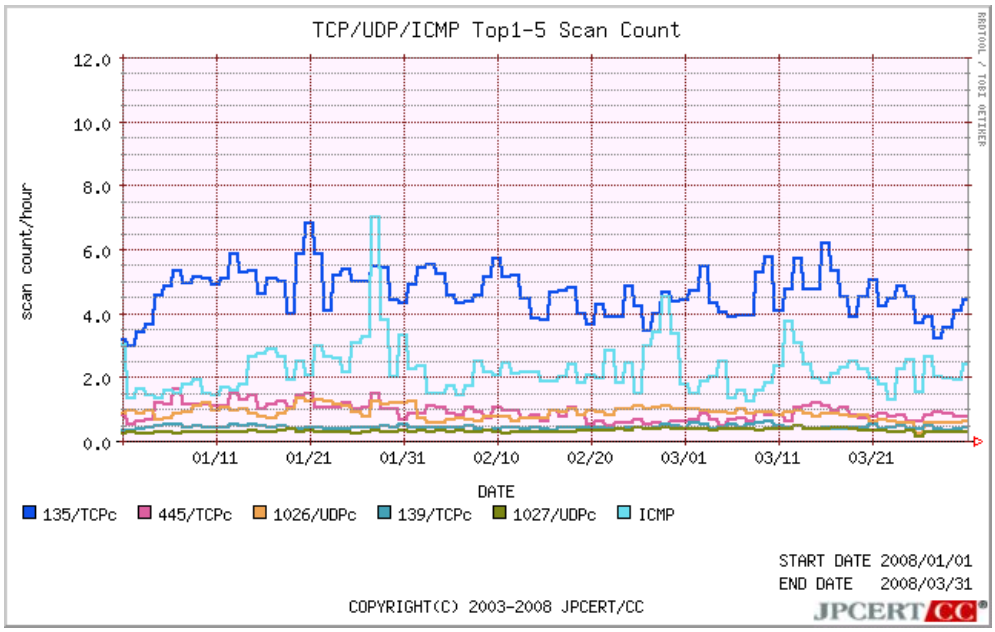


図 3-1: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2008 年 1 月 1 日-3 月 31 日)

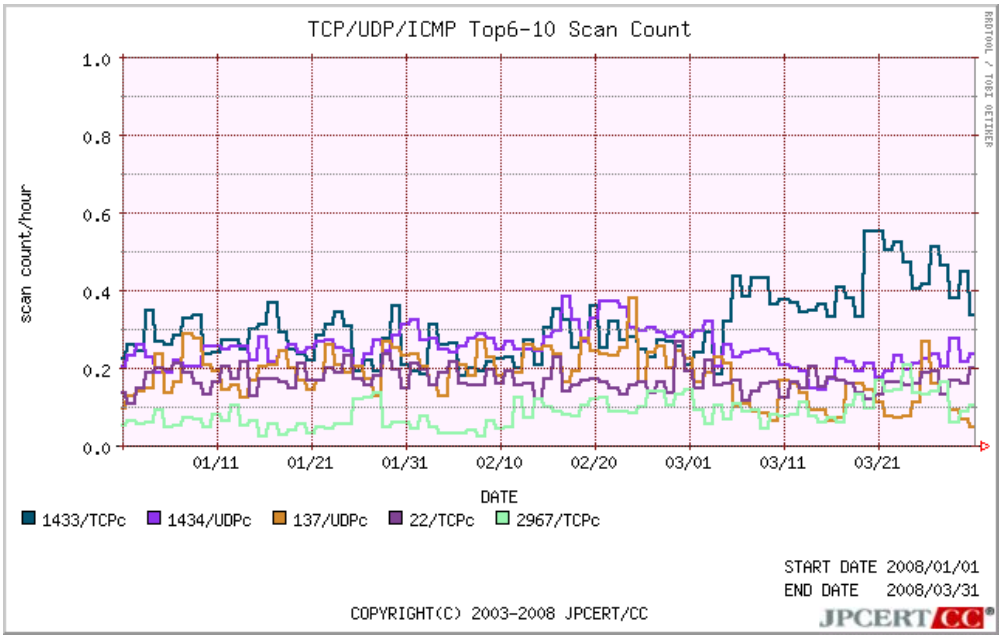


図 3-2: アクセス先ポート別グラフ top6-10

また、より長期間のスキャン推移を表すグラフとして、2007 年 4 月 1 日から 2008 年 3 月 31 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 3-3、図 3-4 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-2008 年 3 月 31 日)

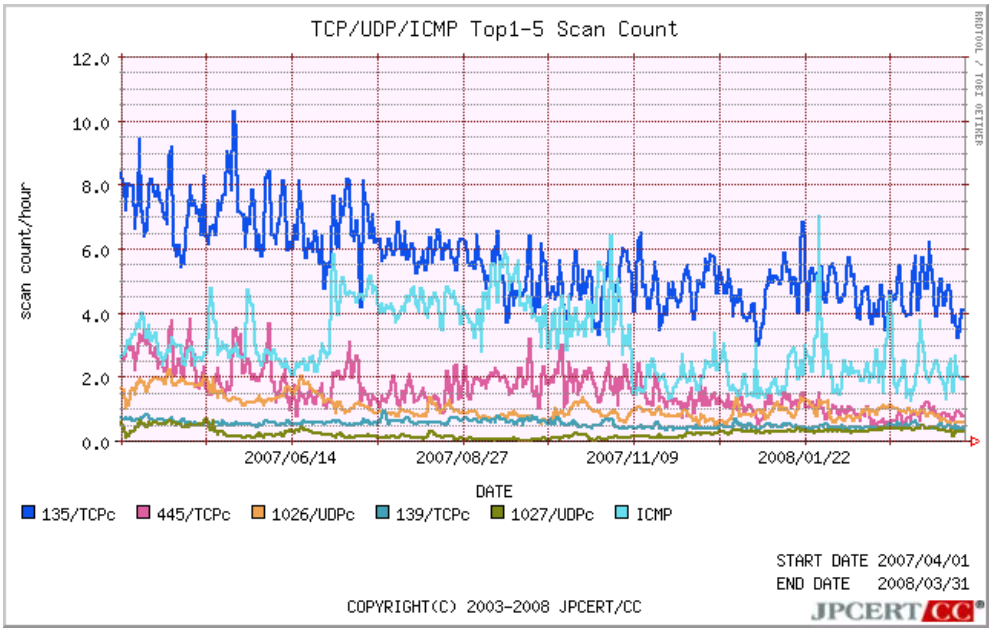


図 3-3: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2007 年 4 月 1 日-2008 年 3 月 31 日)

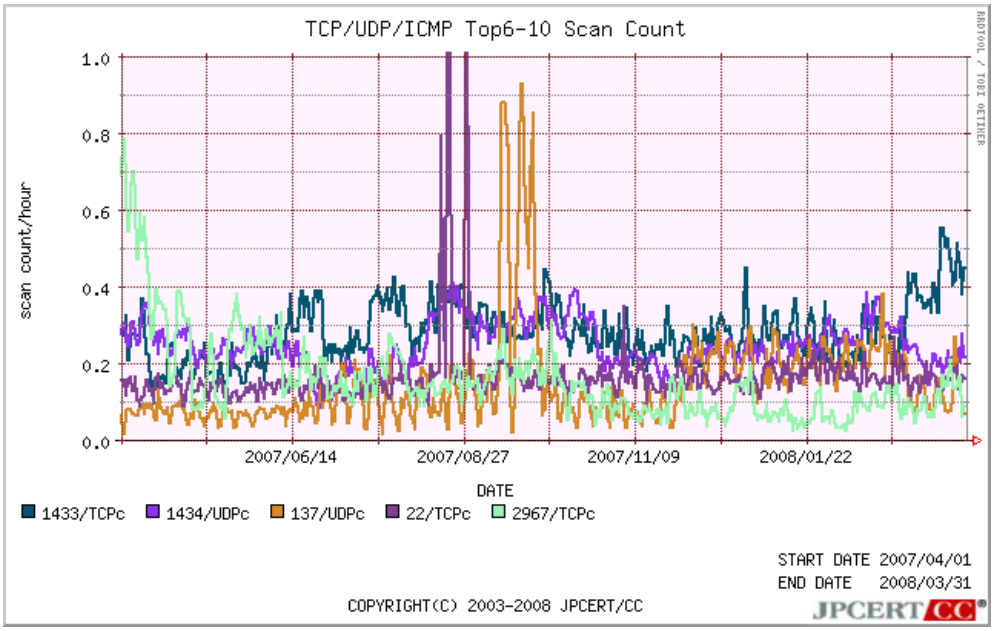


図 3-4: アクセス先ポート別グラフ top6-10

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 月上旬に初めて観測されました。その後、このスキャンは増減を繰り返してはいますが、前期の観測結果では観測当初と比較して少ないレベルまで減少しました。今期の観測動向で特筆すべき事項が無い場合には、来期の文書からは削除する予定です。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。製品開発者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 年 11 月 1 日-2008 年 3 月 31 日)

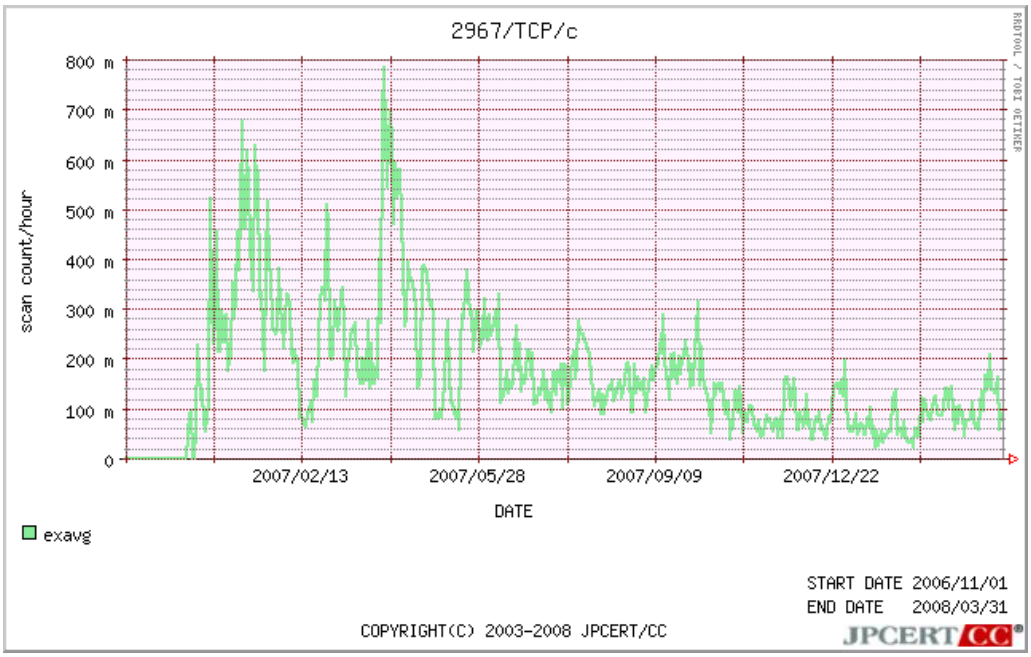


図 3-5: アクセス先ポート別グラフ TCP 2967 番ポート

(2) TCP5900 番ポートへのスキャンを継続的に観測

TCP5900 番ポートへのスキャンを引き続き観測しており、今期一時的にスキャン数が増加しました。スキャン数が増加した要因は不明ですが、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ています。製品開発者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 (2006/4/1-2008/3/31)

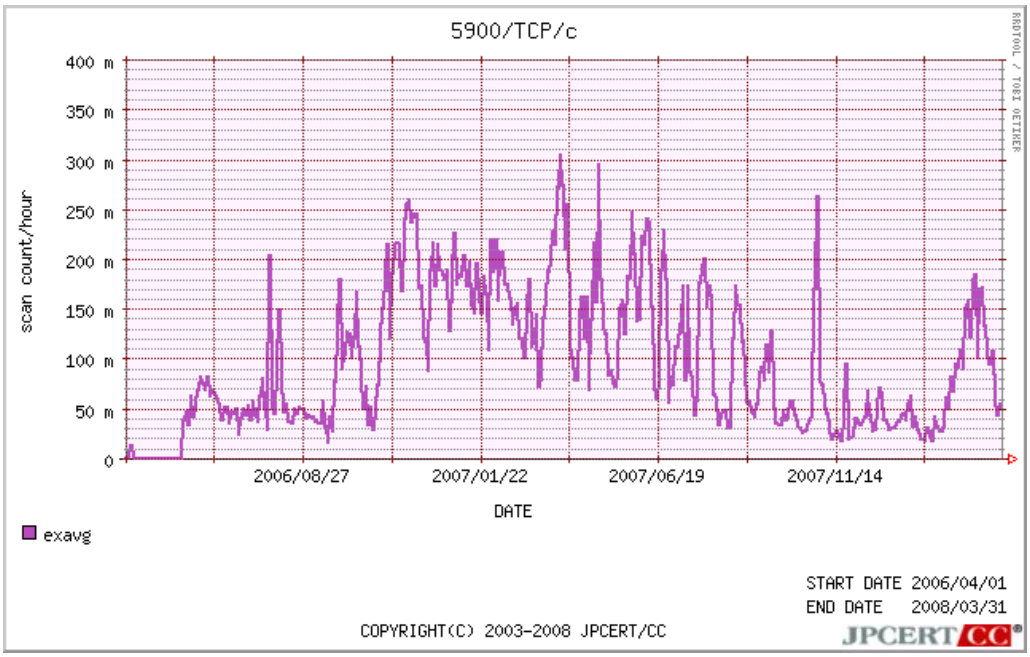


図 3-6: アクセス先ポート別グラフ TCP 5900 番ポート

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 パケットを継続的に観測

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非常に多い状態が続いていましたが、11 月上旬ぐらいから半減しており、今期も同レベルを維持しており、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 (2008/1/1-2008/3/31)

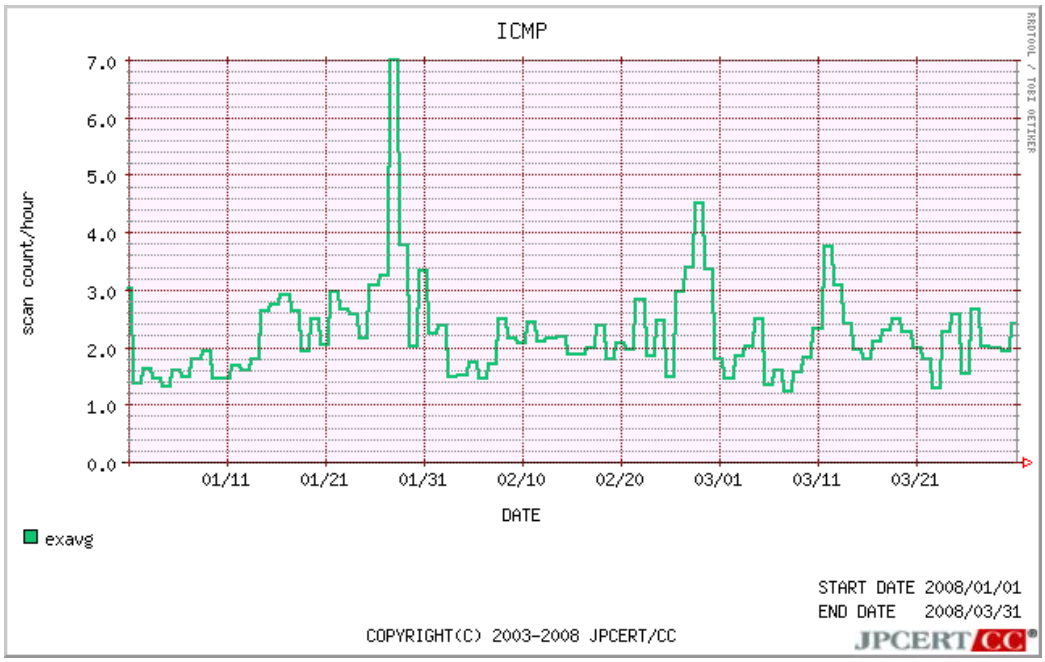


図 3-7: ICMP パケット受信グラフ

(4) TCP5168 番ポートへのスキャンを継続的に観測

TCP5168 番ポートへのスキャンは、2008 年 8 月下旬に初めて観測されました。本観測については同ポートを使用した Trend Micro の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。TCP5168 番へのスキャンは、脆弱性情報が公開されたときに多く観測されましたが、現在は沈静化しているため、今期の観測動向で特筆すべき事項が無い場合には、来期の文書からは削除する予定です。製品開発者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 5168 番ポート (2008/8/16-2008/12/31)

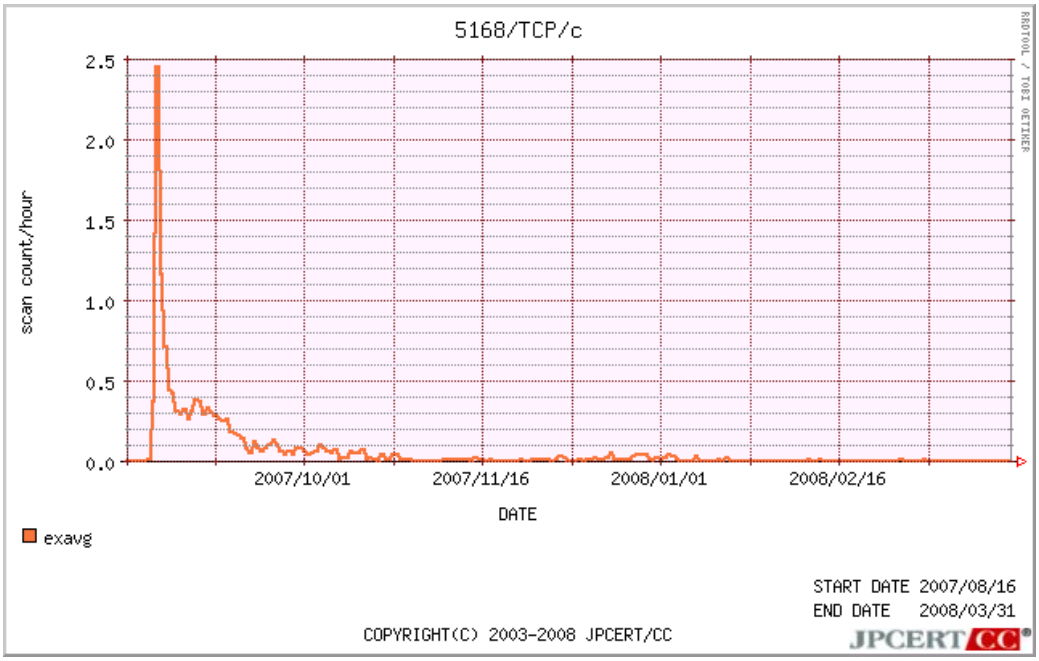


図 3-8: アクセス先ポート別グラフ TCP 5168 番ポート

TCP 5168 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/2008/at070019.txt

§4. 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適時に開示し、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「ソフトウエア等脆弱性関連情報取扱基準」(以下、本基準)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 (http://www.cert.org/)や英国 CPNI (http://www.cpni.gov.uk/) 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. Japan Vulnerability Notes (JVN) において公開した脆弱性情報および対応状況

2008 年 1 月 1 日から 2008 年 3 月 31 日までの間に JVN において公開した脆弱性情報および対応状況は 44 件 (総計 589 件)[図 4-1] でした。

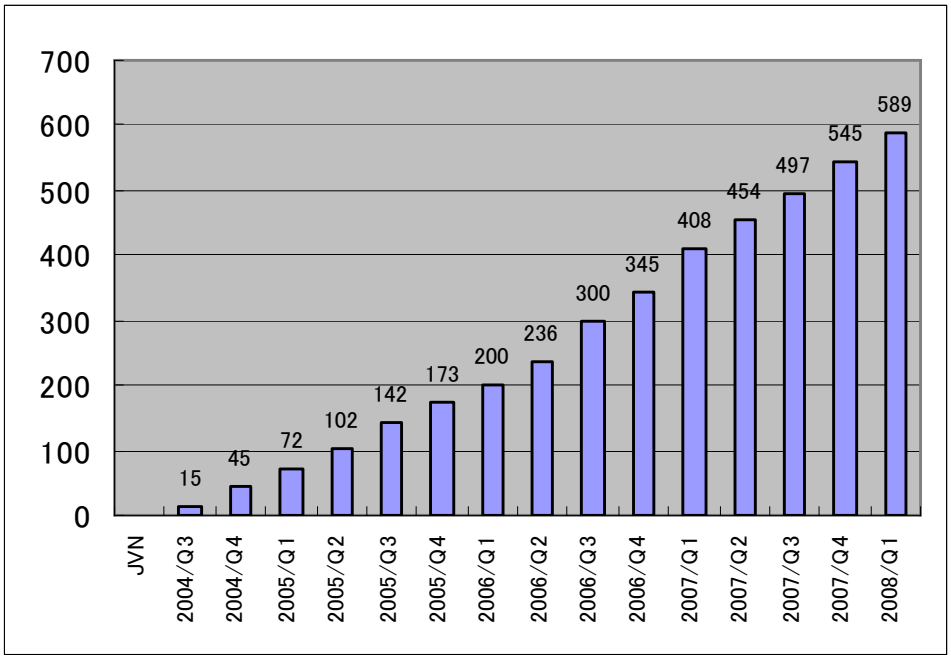


図 4-1: 累計 JVN 公表件数

前四半期に引き続き、クロスサイトスクリプティングの脆弱性に関する届出に対して、複数の製品開発者により対策が実施され公開しています。また、今期はルータ等の製品に組み込まれるソフトウェアや制御系システムのソフトウェアに関して脆弱性への対応が行われた四半期でもあります。各公開情報に関しましては、JVN(http://jvn.jp/)をご覧ください。

このうち、本基準に従って、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 19 件(累計 261 件)[図 4-2]でした。

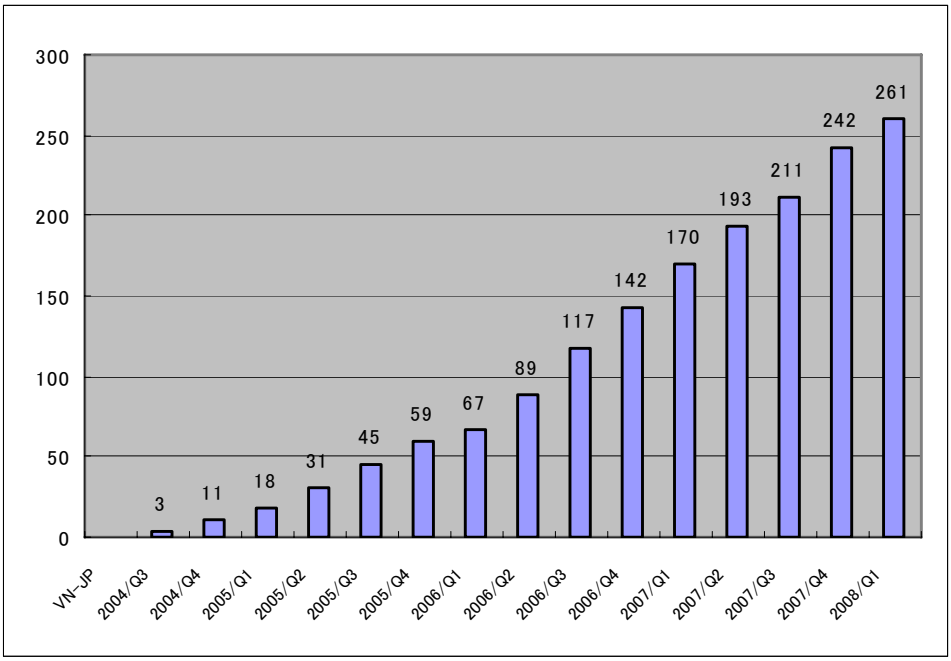


図 4-2: 累計 VN-JP 公表件数

また、CERT/CC とのパートナーシップに基づき、JVN にて VN-CERT/CC として 公開した脆弱性情報は 24 件(累計 306 件)[図 4-3]、また、CPNI とのパートナーシップに基づき、JVN にて VN-CPNI として公開された脆弱性情報は 1 件(累計 22 件)[図 4-4]でした。

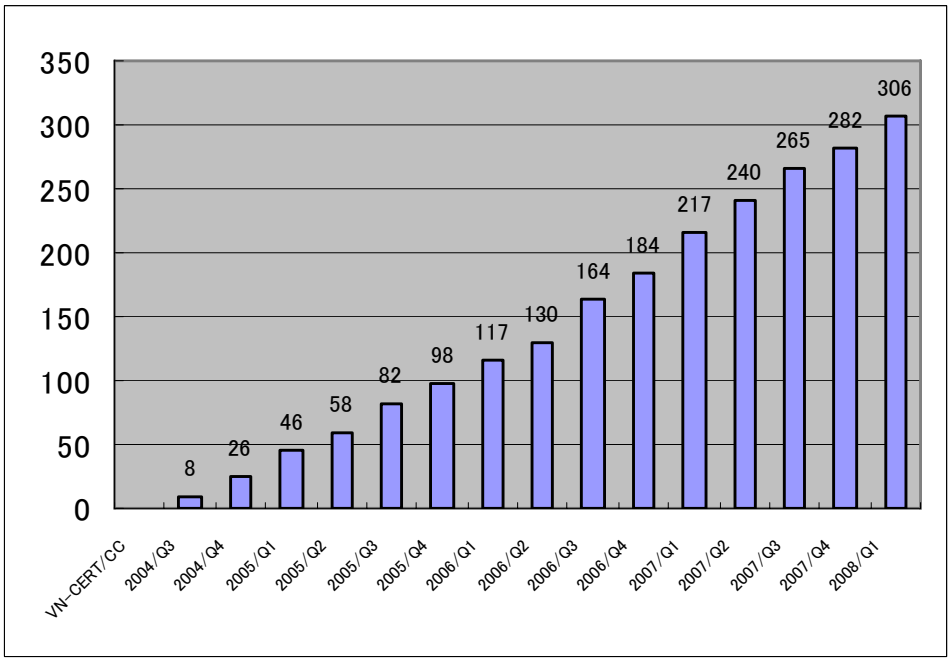


図 4-3: 累計 VN-CERT/CC 公表件数

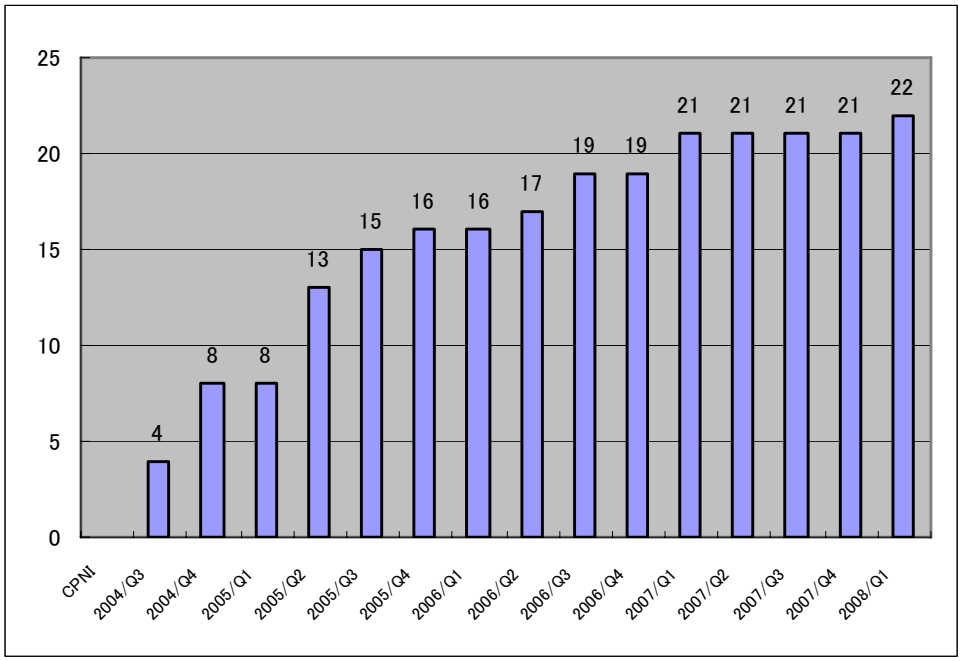


図 4-4: 累計 VN-CPNI 公表件数

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、米国の CERT/CC や英国 CPNI など海外 CSIRT と、報告された脆弱性関連情報の共有、製品開発者への情報通知のオペレーション、公開日の調整、各国製品開発者の対応状況等、公開までの情報を共有し活動を行っています。

III. 日本国内の脆弱性情報流通体制の整備

JPCERT/CC では、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。
詳細については以下の URL をご参照ください。

脆弱性関連情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
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_guide2008.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 (http://www.ipa.go.jp/)、調整機関にJPCERT/CC が指定されています。JPCERT/CC はIPA からの届出情報をもとに、製品開発者への情報提供を行ない、対策情報公開に至るまでの調整を行なっています。最終的に IPA と共同で JVN にて対策情報を公開しています。両組織間においては緊密な情報の交換、脆弱性情報の分析等を行っています。なお、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http://www.ipa.go.jp/security/vuln/ をご参照ください。

(2) 日本国内製品開発者との連携

本基準では、JPCERT/CC が脆弱性情報を提供する先として、日本国内の製品開発者リスト(製品開発者リスト)を作成し、各製品開発者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、製品開発者の皆様に製品開発者としての登録をお願いしています。2008 年 3 月 31 日現在で 233 組織[図 4-5]の製品開発者の皆様に、ご登録をいただいています。登録の詳細については、https://www.jpcert.or.jp/vh/agreement.pdf をご参照ください。

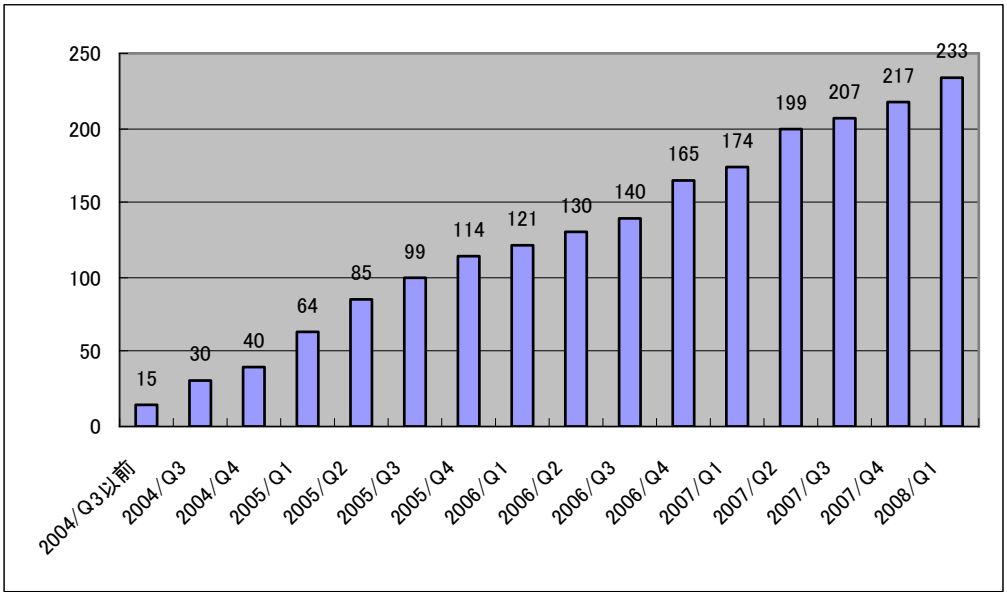


図 4-5: 累計製品開発者登録数

(3) 脆弱性情報ハンドリングワークショップの開催

JPCERT/CC 製品開発者リストに登録いただいている国内ベンダの連絡担当者にお集まりいただき、3 月 26 日に脆弱性関連情報ハンドリングワークショップを開催しました。今回は、同時期に開催されていた JWS / First TC の Vender SIG の方にも参加いただき、脆弱性関連情報に関する関連活動や最新状況を紹介するとともに、ベンダ担当者との意見交換を行ないました。

(4)　Open Source Conference 2008 への参加

オープンソースソフトウェアの開発者およびコミュニティに対して、日本国内の脆弱性情報流通体制の認知を向上し、相互理解を深めるため、2008 年 3 月 1 日に開催された Open　Source Conference 2008 Tokyo/Spring に参加しました。セミナー形式の講演を行いセキュアコーディングへの取組みについて紹介することで、オープンソースソフトウェア分野における安全なソフトウェア開発と脆弱性対応に関する意見交換、情報交換をおこないました。

(5)　JANOG21 meeting への参加

2008 年 1 月 23 日（水）～2008 年 1 月 25 日（金）に開催された JANOG21 meeting に参加し、セミナー講演にて脆弱性情報ハンドリング活動とセキュアコーディングへの取組みの紹介をおこない、来場者との交流と意見交換をおこないました。

§5.ボット対策事業

JPCERT/CC 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ており、収集されたボット検体の特徴や技術の解析、および駆除ツールの作成をしています。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。

I. ボット対策事業の活動実績の公開

ボット対策事業のポータルサイトである「サイバークリーンセンター」では毎月の活動報告として「サイバークリーンセンター活動実績」を公開しています。詳細につきましてはサイバークリーンセンターのサイトをご参照ください。

サイバークリーンセンター
https://www.ccc.go.jp/
2008 年 01 月度　サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200801/0801monthly.html
2008 年 02 月度　サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200802/0802monthly.html

§6. 国際連携活動関連

I. 海外連携強化等

インシデント対応に関する連携の枠組みの強化及びインターネット環境の整備や情報セキュリティに関する取り組みの実施状況に関する情報収集及び連携強化を目的とした活動を行いました。

(1)　2008 年 2 月 25,26,27 日　台湾 APTLD(APRICOT) 参加

APTLD は Asia Pacific Top Level Domain Association の略であり、アジア太平洋地域における国別トップレベルドメイン（ccTLD）管理機関間の連携を行うため、1998 年 7 月、APNG を母体として組織されました。JPCERT/CC より、有害サイト（特にフィッシングなど）の対応協力を呼びかけました。

II. 海外 CSIRT コミュニケーション、トレーニング等

アジア太平洋地域の CSIRT 構築支援およびトレーニングを行っています。

(1) アジア太平洋地域 6 カ国に対する CSIRT トレーニング　2008 年 3 月 19 日～25 日の実施
財団法人海外技術者研修協会：http://www.aots.or.jp/index.html
参加 6 カ国：インドネシア、カンボジア、スリランカ、バングラデシュ、フィリピン、モンゴル

III. 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。

(1) 2008 年 3 月 10 日-12 日 APCERT AGM 2008 香港が開催されました。

http://apcert2008.hkcert.org/

IV. 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 FIRST の運営に協力しています。

(1) Joint Workshop on Security 2008,Tokyo および FIRST-TC Tokyo に、Organizing Committee の一員として、運営に協力しました。

§7.CSIRT 構築支援活動関連

国内の組織・団体・企業などに対し、CSIRT 構築支援やコミュニケーション活動を行っています。

I. 国内 CSIRT 構築支援活動

CSIRT 或いはその機能の構築を検討している企業、組織及び団体を調査、構築、強化を目的に訪問し、支援活動を行いました。

1 月から 3 月の支援件数：6 企業、2 組織、2 団体

II. 日本シーサート協議会への参画

日本国内の CSIRT の集まりである日本シーサート協議会に、JPCERT/CC の職員が運営委員会のメンバとして協力するとともに、事務局を担当しています。

日本シーサート協議会の詳細： http://www.nca.gr.jp/

§8. 講演活動一覧

(1) 代表理事 歌代和正
「Opening Speech」
FIRST-TC March 2008 Tokyo / 2008 年 3 月 27 日

(2) 業務統括 伊藤友里恵
「APCERT Activity Updates - Asia Pacific Computer Emergency Response Team -」
FIRST-TC March 2008 Tokyo / 2008 年 3 月 26 日

(3) 早期警戒グループ 鎌田敬介
「Inoculating vs. Targeted Trojan and Spear Phishing Attacks 」
APCERT Annual Conference 2008 /3 月 12 日

(4) 業務統括 伊藤友里恵
「Network Visualization Tool for AP Region」
APCERT Annual Conference 2008 /3 月 11 日

(5) 早期警戒グループ 鎌田敬介
『これからの情報セキュリティ対策に向けて～インシデントと脆弱性対応』
「インシデントと脆弱性の最新動向と CSIRT 構築」
グローバルテクノ株式会社 ISMS審査員CPDコース / 2008 年 3 月 7 日

(6) 早期警戒グループ 名和利男
「CSIRT 構築・運営に関わる最新トピック」
ＮＴＴ 情報流通プラットフォーム研究所 NTT-CERT / 2008 年 2 月 22 日

(7) 早期警戒グループ 小宮山功一朗
「最近の情報セキュリティインシデント傾向と大学でのインシデント事例とその対策」
文部科学省 / 2008 年 2 月 6 日

§9. 掲載記事一覧

(1) 代表理事　歌代和正

日本情報産業新聞　年頭メッセージ Page10

(2) 理事　真鍋敬士　、椎木孝斉

プロフェッショナル・セキュリティ・レビュー　Page138-142

アスキービジネス　/ 2008 年 1 月 25 日

(3) 情報流通対策グループ

日経 BP 日経ソリューションビジネス IT マーケットデータ年鑑 2008 Page125,143

日経ソリューションビジネス/ 2008 年 1 月 29 日

(4) 情報流通対策グループ

日経 BP 社日経ソリューションビジネス DATA&DATA

日経ソリューションビジネス / 2008 年 2 月 15 日

■インシデントのご報告は

☐ Email：info@jpcert.or.jp

PGP Fingerprint ：BA F4 D9 FA B8 FB F0 73　57 EE 3C 2B 13 F0 48 B8

☐ インシデント報告様式　：http://www.jpcert.or.jp/form/