JPCERT-PR-2007-0008

JPCERT/CC 活動概要 [2007 年 7 月 1 日 ～ 2007 年 9 月 30 日]

2007-10-26 発行

◆活動概要トピックス◆

【トピック 1】 アジア太平洋地域の CSIRT 間連携の強化

JPCERT/CC は、国際間連携の必要性が高いインターネットセキュリティの分野において、より円滑な情報交換や協力関係を構築する目的で、諸外国のサイバーインシデント緊急対応機関との連携体制の構築を進めています。

本年 7 月から 9 月の間は、ASEAN 加盟国(*1)を含むアジア太平洋地域における National CSIRT(*2)ｎ間の連携強化に特に注力しました。JPCERT/CC は、この 2 ヶ月で韓国、台湾、インドネシア、カンボジア、シンガポール、フィリピン、ブルネイ、ベトナム、マレーシア、ミヤンマー、モンゴル、ラオスの各 National CSIRT、または情報セキュリティ担当機関を訪問し、CSIRT 設立プラン立案の支援、技術支援、トレーニングや CSIRT のオペレーションに効果的なツールの提供などについて、今後の実施計画、覚書の締結などを進めました。

*1: ASEAN（東南アジア諸国連合）加盟国において、各国のサイバーインシデント緊急対応窓口となる National CSIRT を立ち上げることが ASEAN ICT Focus 2005-2010 で言及されており、現在、各国において CSIRT の立ち上げや既存の CSIRT 活動の見直しを行っています。

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

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)への緊急対応、対策支援、分析や教育などの活動を行う機関または機能のことをいいます。

JPCERT/CC は、国際的なインシデントの調整に関し、日本の窓口 CSIRT として活動しています。

【トピック 2】 JPCERT/CC 製品開発者リスト登録者が 200 を越える

脆弱性関連情報は、ソフトウェア等において、コンピュータ不正アクセス、コンピュータウイルス等の攻撃により機能や性能を損なう原因となり得る、安全性上の問題箇所に係わる情報であり、その取扱いには細心の注意を要します。JPCERT/CC は、脆弱性関連情報を適切に公開することにより脆弱性による脅威や危険性を最小限にすることを目的として策定された、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」(*3)において、製品開発者における脆弱性対策情報の作成及び公開の調整を行う「調整機関」に指定されています。

JPCERT/CC では、報告があった脆弱性情報について、影響を受ける可能性のある製品開発者を特定し、迅速かつ安全に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作成し、脆弱性対応を依頼する場合の連絡先に関する情報を整備してきました。2007 年 9 月 30 日時点で、

この開発者リストへの登録に合意していただいた製品開発者は 207 社となり、プロトコルレベル、モジュール製品やライブラリ製品に関する脆弱性のような、複数の製品開発者にまたがって広く影響の出る問題の調整についても、迅速に対応できる体制が整ってきました。この製品開発者リストの整備が進むことで、より迅速な調整が行えるようになるだけでなく、各要素技術を実装している製品開発者を把握することで、脆弱性が及ぼす影響・インパクト分析をより精緻に行うことができるようになります。

*3: ソフトウエ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 3】 脆弱性を作りこまない、安全なソフトウェア開発を行うための C/C++セキュアコーディングセミナーを実施

ソフトウェア等に関して発見される脆弱性の件数は年々増加しており、米国 CERT/CC の統計では、2006 年の脆弱性報告数は 8,000 件を超えています。そのうち、多くの脆弱性は既知のプログラミングエラーによって引き起こされる脆弱性であることが分かっています。このことから、JPCERT/CC では、製品開発者に対し、これらのプログラミングエラーがいかにして脆弱性として作りこまれるのかを解説するセミナーの実施を始めました。特定のアプリケーションに限らず C/C++ 言語を使ってプログラムを開発する業務に携わる全ての方を対象としています。

【トピックス 4】 JPCERT/CC RSS の配信を開始

JPCERT/CC は、皆様にセキュリティ関連情報をいち早くお届けするため、2007 年 8 月より JPCERT/CC RSS(RDF Site Summary)の配信を開始しました。
JPCERT/CC RSS では、JPCERT/CC がメーリングリストおよび、Web で提供している「注意喚起」、「緊急情報」、「JPCERT/CC レポート」の最新情報を配信しています。
詳しくは http://www.jpcert.or.jp/rss/ をご覧ください。

JPCERT CC®

◆活動概要◆

§1. インシデント報告

2007 年 7 月 1 日から 2007 年 9 月 30 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 706 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 1028 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。

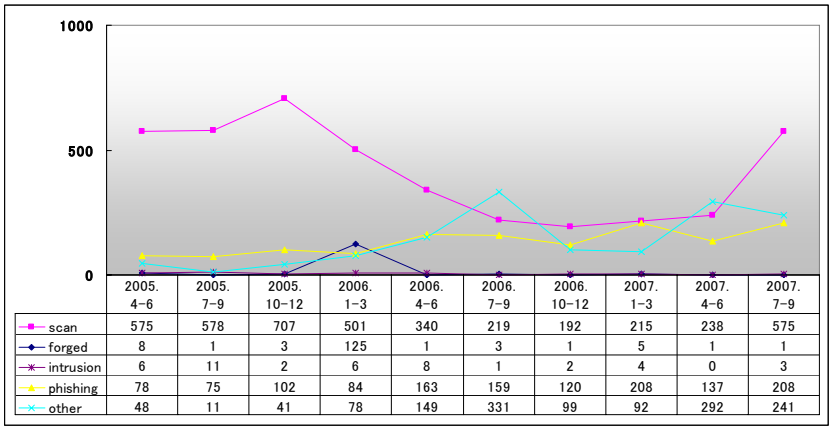
.jp	263	件
.com	160	件
.org	114	件
.net	67	件
.br	39	件
.pl	24	件
.edu	22	件

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 729 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、フィッシング、マルウェアに関する報告が依然として多く、「scan」では TCP80 番ポートへのスキャンが増加しました。これは web アプリケーションの脆弱性をターゲットにした攻撃の影響と考えられます。
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. 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	2007. 7-9
scan	575	578	707	501	340	219	192	215	238	575
forged	8	1	3	125	1	3	1	5	1	1
intrusion	6	11	2	6	8	1	2	4	0	3
phishing	78	75	102	84	163	159	120	208	137	208
other	48	11	41	78	149	331	99	92	292	241

(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 575 件の報告を受けました。

参考文献 [1] [2] [3] [4] [5] [6] をご参照ください。

80 (http)	354	件 (*1)
22 (ssh)	107	件 (*1)
21 (ftp)	6	件 (*1)
1023	5	件 (*1)
445 (microsoft-ds)	5	件 (*1)
5554 (sgi-esphttp)	5	件 (*1)
9898 (monkeycom)	5	件 (*1)
総合的なプローブ、スキャン	94	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)

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 [7] [8] [9]をご参照ください。

(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 3 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など

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、208 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。

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[10]をご参照ください。

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 236 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、各対策を実施しました。

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 52 件受けました。一部を以下に紹介します。

- 架空請求についての質問
- APCERT 事務局窓口宛に来たインシデント報告の対応

§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

2007 年 7 月 1 日から 2007 年 9 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 7 月 1 日-9 月 30 日)

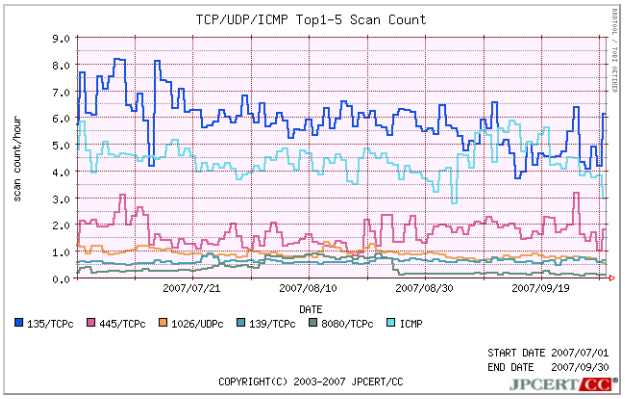


図 2-1: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2007 年 7 月 1 日-9 月 30 日)

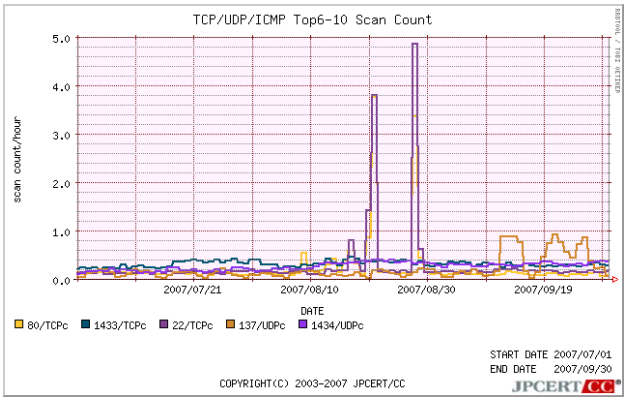


図 2-2: アクセス先ポート別グラフ top6-10

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 10 月 1 日から 2007 年 9 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 10 月 1 日-2007 年 9 月 30 日)

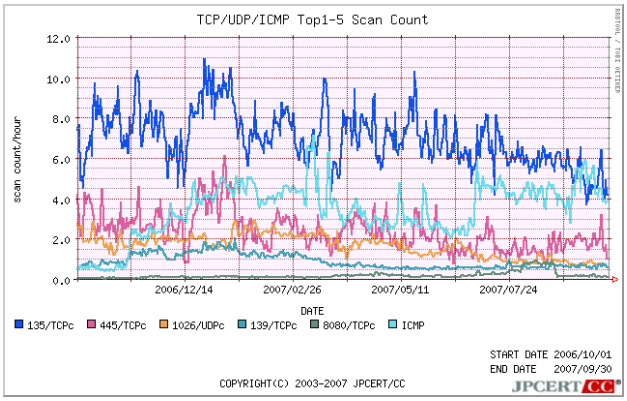


図 2-3: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2006 年 10 月 1 日-2007 年 9 月 30 日)

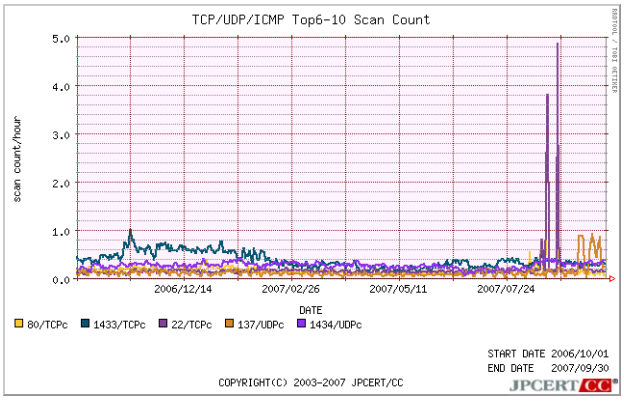


図 2-4: アクセス先ポート別グラフ top6-10

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。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 (2006/11/1-2007/9/30)

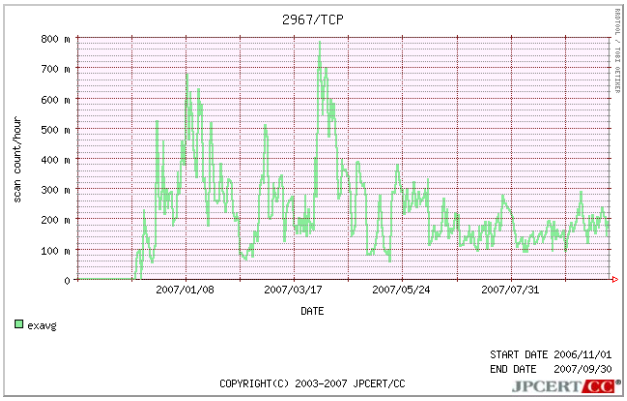


図 2-5: アクセス先ポート別グラフ TCP 2967 番ポート

(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 (2006/4/1-2007/9/30)

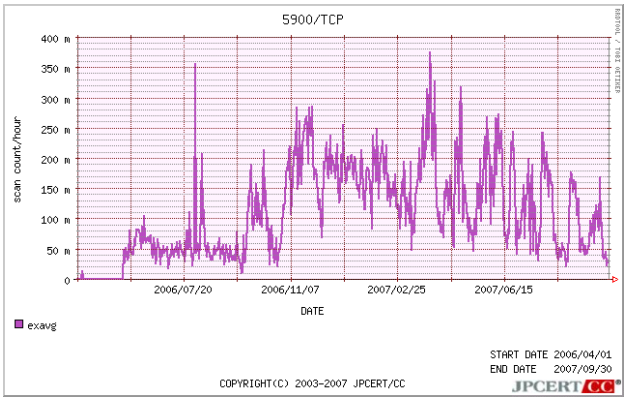


図 2-6: アクセス先ポート別グラフ TCP 5900 番ポート

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昨年同時期に比べて 4 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 (2007/7/1-2007/9/30)

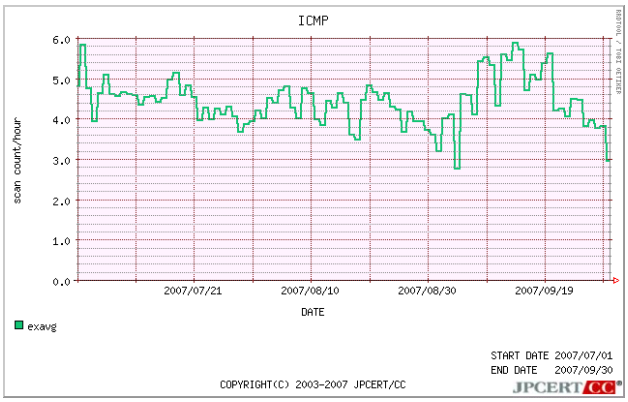


図 2-7: ICMP パケット受信グラフ

(4) TCP5168 番ポートへのスキャン増加を観測

TCP5168 番ポートへのスキャンは、2007 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。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 5168 番ポート (2007/8/16-2007/9/30)

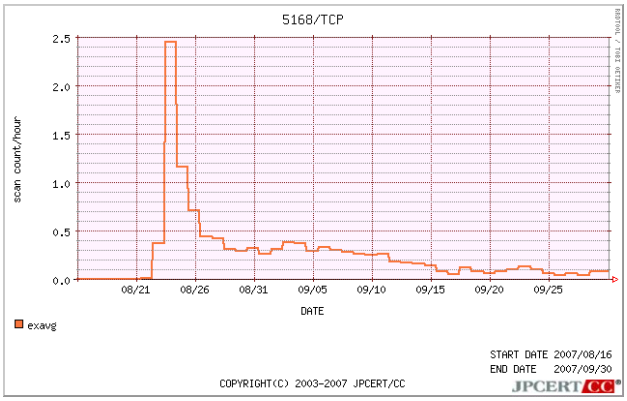


図 2-8: アクセス先ポート別グラフ TCP 5168 番ポート

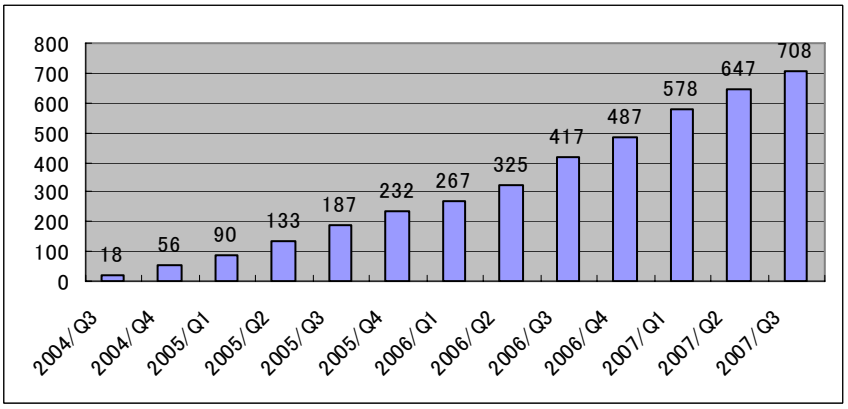
TCP 5168 番ポートへのスキャン増加に関する注意喚起
http://www.jpcert.or.jp/at/2007/at070019.txt

§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」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。

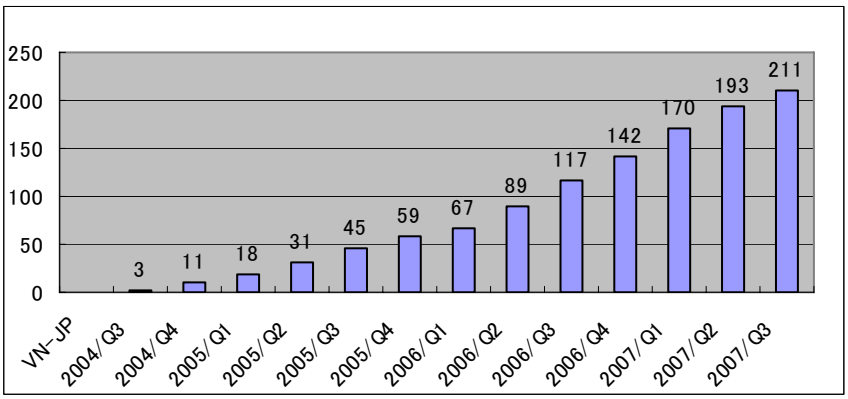
I. Japan Vulnerability Notes (JVN) において公開した脆弱性情報および対応状況

2007 年 7 月 1 日から 2007 年 9 月 30 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 43 件 (総計 708 件) です。各公開情報に関しましては、JVN(http://jvn.jp/)をご覧ください。



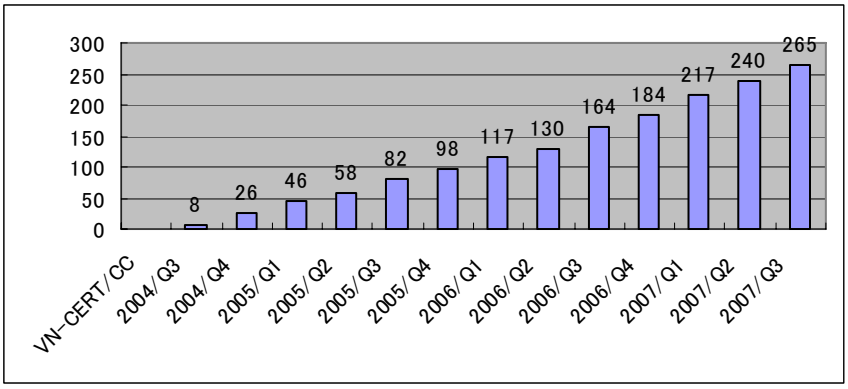
JVN 公表件数

このうち、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」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 18 件(総計 211 件)です。

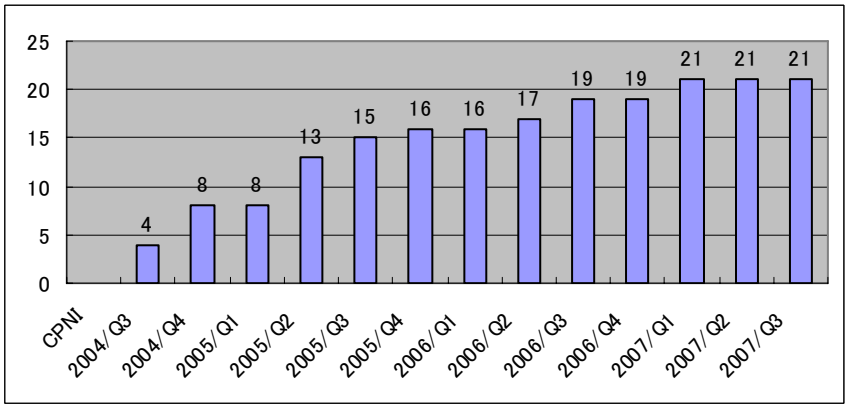


VN-JP 公表件数

また、海外 CSIRT とのパートナーシップに基づき、JPCERT/CC が公開した脆弱性情報は 25 件です。



VN-CERT/CC 公表件数



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、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、製品開発者への通知の共同オペレーション、公開日の調整、各国製品開発者情報等、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。

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「ソフトウエ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。

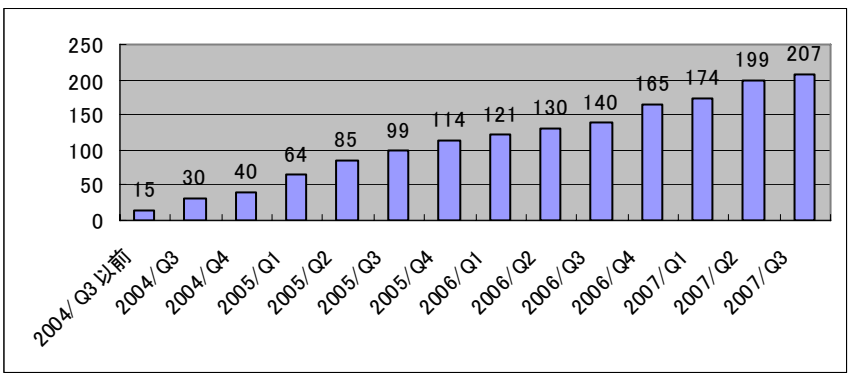
本基準等については以下の URL をご参照ください。

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_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 (http://www.ipa.go.jp/)、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。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。2007 年 9 月 30 日現在で 207 社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、http//www.jpcert.or.jp/vh/agreement.pdf をご参照ください。



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製品脆弱性対策管理者にお集まりいただき、2007 年 7 月 27 日に脆弱性情報ハンドリングワークショップを開催しました。ここでは脆弱性関連情報ハンドリング業務や関連活動の最新状況を紹介するとともに、意見交換を行ないました。

(4) OpenSource Conference 2007 Kansai 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、2007 年 7 月 20 日～21 日に開催された OpenSource Conference 2007 Kansai に参加しました。脆弱性関連情報ハンドリング業務や活動の最新状況を紹介し、オープンソースソフトウェア分野に対する。JPCERT/CC のプレゼンスの向上、及び、現状の脆弱性情報流通体制に関しての意見交換、情報交換を行いました。

§4 ボット対策事業

JPCERT/CC は、総務省・経済産業省連携事業である「サイバーサイバークリーンセンター」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、プロジェクトにおいて収集されたボット検体の特徴や技術の解析、および、その解析結果の駆除ツール（CCC クリーナー）への反映を実施しています。さらに、効率的なボットプログラムの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ボット対策技術の開発も行っています。

1. 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/
2007 年 7 月度　サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200707/0707monthly.html
2007 年 8 月度　サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200708/0708monthly.html
2007 年 9 月度　サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200709/0709monthly.html

JPCERT CC®

§5. 公開文書

2007 年 7 月 1 日から 2007 年 9 月 30 日までの間に JPCERT/CC が公開した文書は、注意喚起 4 件、JPCERT/CC レポート 13 件、及びプレスリリース 2 件です。詳細は以下の通りです。

I. 注意喚起 4 件　http://www.jpcert.or.jp/at/

2007-09-21　ファイル圧縮・解凍ソフト Lhaplus の脆弱性に関する注意喚起(公開)

2007-08-23　TCP 5168 番ポートへのスキャン増加に関する注意喚起(公開)

2007-08-15　2007 年 8 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)

2007-07-11　2007 年 7 月 Microsoft セキュリティ情報 (緊急 3 件含)に関する注意喚起(公開)

II. JPCERT/CC レポート 13 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 91 件、「今週の一口メモ」のコーナーで紹介した情報は 13 件です。

III. プレスリリース　2 件　http://www.jpcert.or.jp/press/

(1)2007 年 7 月 19 日　ソフトウェア等の脆弱性関連情報に関する届出状況
[2007 年第 2 四半期(4 月～6 月)]

(2)2007 年 7 月 19 日　JPCERT/CC 活動概要 [2007 年 4 月 1 日 ～ 2007 年 6 月 30 日]

§6. その他の活動

2007 年 7 月 1 日から 2007 年 9 月 30 日までの間に JPCERT/CC が実施した、上記§1.～5.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 FIRST の運営に協力しています。

IV. 日本シーサート協議会への参画 http://www.jpcert.or.jp/press/2007/RLS_csirt-concil_0417.pdf

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ーとして協力するとともに、事務局を担当しています。

V.その他講演など

(1)2007 年 7 月 18 日　SANS Future Vision 2007 Tokyo

パネルディスカッション「情報セキュリティの近未来展望」に参加しました。

http://www.event-information.jp/sans-fv/session.html

(2)2007 年 7 月 26 日 CSI ネットワークマスター虎の穴 第 9 回「情報セキュリティマスター編～情報セキュリティの最新動向を知る～」

「インターネットセキュリティの最新動向とその対策～脆弱性情報と組織内 CSIRT～」

「ボットネットに見る脅威の変化と今後の対応」について講演しました。

http://www.cic-infonet.jp/C-LINE/441.pdf

(3) 2007 年 8 月 29 日　中央大学　情報セキュリティ人材育成公開講座

「国内外におけるインシデント対応最前線」について講演しました。

http://www2.tamacc.chuo-u.ac.jp/kikoh/sec_ikusei/sec2007/isec2007.pdf

(4) 2007 年 9 月 19 日　FISC 金融情報システムセンター　平成 19 年度安全対策基準改定に関する検討部会

「日本国内の組織内 CSIRT の現状と必要性について」を講演しました。

http://www.fisc.or.jp/

(5) 2007 年 9 月 21 日　情報セキュリティ大学院大学シンポジウム「ネットワークの匿名性とプライバシー保護」

「情報セキュリティに関する脅威の動向と関連する施策の現状」について講演し、パネルディスカッション「ネットワークの匿名性とプライバシー保護 ～各界からのアプローチ～」に参加しました。

http://www.iisec.ac.jp/news_events/events2007/sympo_070921/index.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] IN-2004-01: W32/Novarg.A Virus

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

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

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

[9] Email Bombing and Spamming

http://www.cert.org/tech_tips/email_bombing_spamming.html

[10] Frequently Asked Questions About Malicious Web Scripts Redirected by Web Sites

http://www.cert.org/tech_tips/malicious_code_FAQ.html