JPCERT-PR-2008-0001

JPCERT/CC 活動概要 [2007 年 10 月 1 日 ～ 2007 年 12 月 31 日]

2008-01-15 発行

◆活動概要トピックス◆

【トピック 1】ソフトウェア等の脆弱性問題の最先端動向を討議する脆弱性研究者ミーティングを開催

大きな転換期にさしかかりつつあるとも考えられているソフトウェア等の脆弱性問題に関する今後の見通しを得るべく、この分野における最先端の研究を行っている海外の研究者4名を交え、国内外の研究者が注目する新たな脅威と脆弱性の動向に関する最新の研究成果の発表、脆弱性情報のハンドリングを行っている CSIRT チーム・メンバーとの意見交換を行いました。こうした脆弱性問題の研究者と関連情報のハンドリングを行っているチーム間でのミーティングは今回が初めての試みでしたが、脆弱性問題の研究における最先端動向等、今後の脆弱性ハンドリングのあり方を考えるための得がたい情報を得ることができました。

海外から参加した 4 名の研究者の発表概要を以下にご紹介します。

1. Marko Laakso 氏 (Oulu University Secure Programming Group)

フィンランドの Oulu 大学セキュア・プログラミング・グループ(OUSPG)に所属。

通信プロトコル研究の第一人者。

発表概要:たったひとつの脆弱性も、それを含む製品やコードの使われ方によって影響が広がる。通信プロトコルの抽象化されたコンポーネントに脆弱性が存在する場合には、影響が多岐に及ぶ。さらに、実装サービスの多様性が増したことで、攻撃対象となりうる空間も増え、脆弱性がうまれる可能性は高くなる。通信プロトコルでは、下位層での処理を期待した上位層の実現も、脆弱性の原因となりうる。脆弱性を減らすための取り組みは、技術面の取り組みのみならず、開発者に対する啓発活動、経済性、法的責任やインセンティブにも配慮する事が重要である。

2. Halvar Flake 氏 (SABRE Security)

SABRE Security(ドイツ)の最高責任者兼研究チームリーダ。これまでリバースエンジニアリングおよび脆弱性研究に従事する世界的な研究者として、リバースエンジニアリングやコード解析分野における最先端の研究成果を Blackhat Briefings、CanSecWest、SSTIC、DIMVA などの著名なセキュリティカンファレンスにて講演。

発表概要:一部の製品に関しては、ベンダのコード品質の向上により、ファジング(fuzzing)の様な手当たり次第の攻撃をかける手法による脆弱性の発見が困難になってきた。そのため、静的解析の重要性が高まり、自動化されたデバッガが重要になってきている。そうした解析手法の具体的な例を示した。

3. Will Dormann 氏 (CERT/CC)
CERT/CC（アメリカ）の脆弱性アナリストとして、研究や技術分析、ソフトウェア等の脆弱性情報のコーディネーション業務に従事。
発表概要：ウェブページに機能追加する為の COM オブジェクトである ActiveX コントロールの、脆弱性の発見、検証と解析手法を実演をまじえて説明。

4. Gerardo Richarte 氏 (Core Security Technologies)
Core Security Technologies（アルゼンチン）の共同創立者であり、情報セキュリティ（特にエクスプロイト・プログラムの開発）に関して、世界でも第一線に立つ著名な専門家として活躍。
発表概要：Core Security Technologies で過去 10 年間に発見したセキュリティバグは、52%がブルートフォース攻撃、29%がコードレビューにより見つけられている。また、暗号化技術を応用し、互いに通信するワームについて報告し、事実上この様なワームに対する実効的な対策が無い事態に至るのは時間の問題だと指摘した。

【トピック 2】Internet Governance Forum におけるセキュリティワークショップで、情報セキュリティ対応機能構築のための国際協力の課題を明らかに。
2007 年 11 月 11 日リオデジャネイロで開催された国連主催の国際会議 Internet Governance Forum (IGF) において、JPCERT/CC の伊藤友里恵がセキュリティワークショップのひとつ "International Cooperation on the Capacity Building of Information Security" のモデレータを務め、情報セキュリティインシデント対応機能構築における課題や、その解決策についてディスカッションを行いました。
このパネルは、日本経団連と、ISOC(Internet Society：インターネット協会) の共同提案により開催されたもので、ブラジル、ベトナム、ガーナを代表したパネリストから、開発途上国における情報セキュリティ対策の課題について見解が述べられ、それに対して、アメリカ及び日本のパネリストも交え、国際社会がどう協力し、支援していくことが必要なのかについての意見交換が行われました。
この結果、国際的なサイバーインシデントレスポンスにおけるコーディネーションポイントの構築、その運用のためのリソースやツール、ベストプラクティスの共有などの支援だけでなく、そのための基盤になる法制度等の政策から、民間企業におけるセキュリティ対策のインセンティブ付与、エンドユーザーへの啓発活動までの、多層的なノウハウの共有が必須であることが指摘されました。

IGF 2007 の詳細 http://info.intgovforum.org/wsl2.php?listy=SEC

【トピック 3】アジア太平洋における 12 の経済地域 CSIRT チームが合同でインシデント対応ドリルを実施
JPCERT/CC は、APCERT（アジア太平洋コンピュータ緊急対応チーム）と合同で、2007 年 11 月

下旬、サイバー攻撃への即時対応能力を確認するインシデント対応ドリル(以下「本ドリル」)を実施しました。
本ドリルは、経済地域、国境を越えて発生し、広範囲に影響が派生するインシデントに対応する枠組みの構築を目的とし、年に1度実施しているものです。今回で 5 度目となる本ドリルは特に、国境やタイムゾーンを跨ぐサイバーインシデントに対する迅速なインシデント対応技術及び意思決定能力の向上を目標に、中国のオリンピック開催時に大規模なサイバー攻撃が起こった場合を想定したシナリオを使って実施しました。
今回のドリルには、アジア太平洋地域の 12 経済地域(日本、オーストラリア、ブルネイ、中国、香港、インド、韓国、マレーシア、シンガポール、タイ、台湾、ベトナム)から 13 チームが参加し、CSIRT 間の連携の強化と、対応の効率化につながる成果を得ることができました。

APCERT に関する詳細 http://www.apcert.org/

【トピック 4】国際的な連携強化を目的に海外の脆弱性ハンドリング・チームとの年次技術交流会を開催

JPCERT/CC と CERT/CC(アメリカ)の脆弱性情報ハンドリングチームは、緊密な協力関係の下で、連携して脆弱性情報分析、調整業務を進めています。機密性の高い情報を、異なる組織のミッションや、ポリシーを越えて共有し、対応していくため、毎年1回技術交流会を開催し、必要な情報共有基盤やツールの整備、課題の共有を行っています。3 回目を迎えた今回は、CERT-FI (フィンランド) をゲストとして迎え、11 月下旬に東京で開催しました。
この技術交流会では、脆弱性情報ハンドリングに関する業務の体制、運用システム、環境、今後の課題、及びより効率的な実施体制などについて討議し、この結果を今後の業務に反映することで、複雑化、多様化しさらに増加の一途を辿る脆弱性情報を、より迅速かつ効率的にハンドリングしていくことを相互に確認しました。
今回ゲストとして参加した CERT-FI からは、活動概要のほか、脆弱性調整業務の負荷を軽減するシステム構築のアイデアやノウハウが共有されました。また、CERT-FI に随行した同国の OUSPG (Oulu University Secure Programming Group)の脆弱性研究者と、脆弱性を積極的に見つけ出すための活動や技法について意見交換、情報交換を行ないました。

【トピック 5】総務省・経済産業省連携事業「ボット対策プロジェクト」 駆除ツール「CCC クリーナー」新機能追加

総務省・経済産業省連携の「ボット対策プロジェクト」において提供しているボットプログラム駆除ツール「CCC クリーナー」に、新たに「Microsoft Windows Vista への対応」および「検出状況等送信機能」を追加しました。

新機能追加についてのプレスリリースの詳細
http://www.jpcert.or.jp/news/2007/release_20071107.html

【トピック 6】“SecurityDay 2007”を 5 団体で共同開催

日本インターネットプロバイダー協会 (JAIPA)、日本データ通信協会 (Telecom-ISAC Japan)、日本ネットワークセキュリティ協会 (JNSA)、日本電子認証協議会 (JCAF)及び JPCERT/CC の共催により、「SecurityDay2007 ～日本の情報セキュリティのあり方を考える～」を開催し、100 名を超える情報セキュリティに関わる方々の参加を得て、近時の情報セキュリティに関する課題について発表、検討、意見交換を行いました。

SecurityDay 2007 についての詳細
http://www.jpcert.or.jp/event/sec2007-seminar.html

JPCERT CC®

◆活動概要◆

§1.情報提供活動

JPCERT/CC のホームページ、RSS 配信や、登録いただいているメーリングリスト(登録者数:約24,000 名)に対し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ました。

発行件数:5 件　http://www.jpcert.or.jp/at/

2007-10-10　2007 年 10 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)
2007-11-14　2007 年 11 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)
2007-11-30　アップル QuickTime の未修正の脆弱性に関する注意喚起 (公開)
2007-12-12　2007 年 12 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)
2007-12-14　アップル QuickTime の未修正の脆弱性に関する注意喚起 (更新)

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に加え、ひとくちメモとしてセキュリティに関する豆知識情報を、毎週水曜日(祝祭日を除く)に発行しました。

発行件数: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 89 件、「今週のひとくちメモ」のコーナーで紹介した情報は 13 件でした。

§2. インシデント報告

2007 年 10 月 1 日から 2007 年 12 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 650 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 925 件となりました。

JPCERT CC®

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。

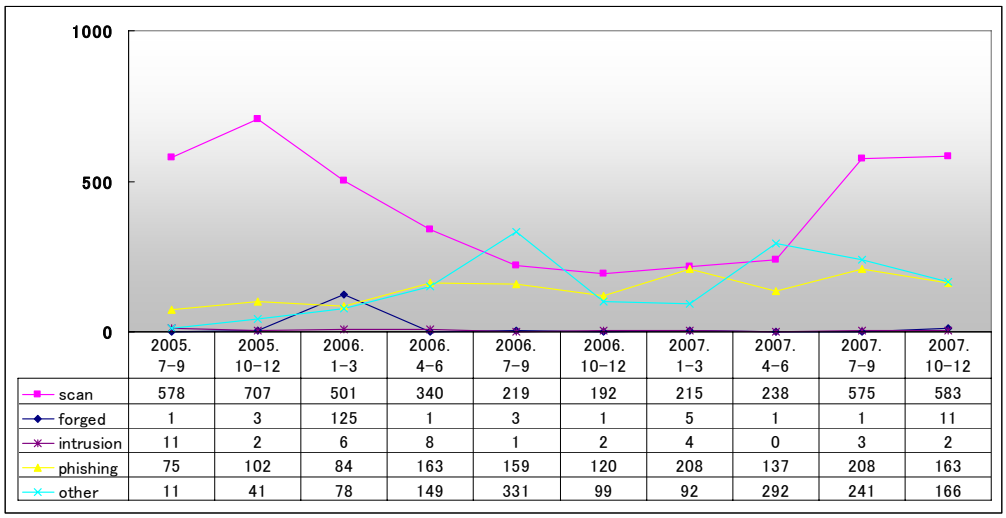
.jp	193 件
.com	174 件
.net	98 件
.de	28 件
.cn	13 件
.nl	12 件
.pl	11 件

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 622 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、TCP80 番ポートをターゲットとしたスキャン、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、前四半期と同程度の報告を受けています。
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. 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	2007. 10-12
scan	578	707	501	340	219	192	215	238	575	583
forged	1	3	125	1	3	1	5	1	1	11
intrusion	11	2	6	8	1	2	4	0	3	2
phishing	75	102	84	163	159	120	208	137	208	163
other	11	41	78	149	331	99	92	292	241	166

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 583 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)	332 件(*1)
22(ssh)	110 件(*1)
5900	7 件(*1)
1433 (ms-sql-s)	7 件(*1)
5554 (sgi-esphttp)	6 件(*1)
9898 (monkeycom)	6 件(*1)
総合的なプローブ、スキャン	107 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 11 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 2 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、163 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 166 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 40 件受けました。一部を以下に紹介します。

- 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

[参考文献]

[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

§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 (Internet Scan Data Acquisition System：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

ISDAS 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 10 月 1 日から 2007 年 12 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 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 10 月 1 日-12 月 31 日)

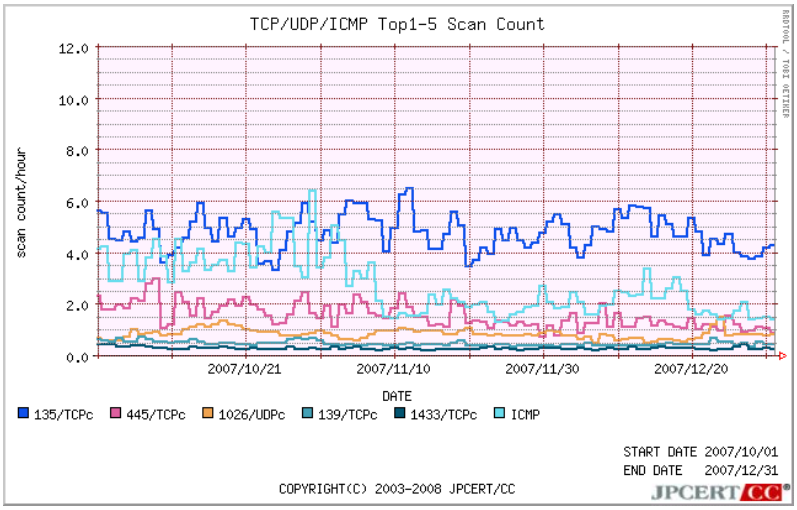


図 2-1: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2007 年 10 月 1 日-12 月 31 日)

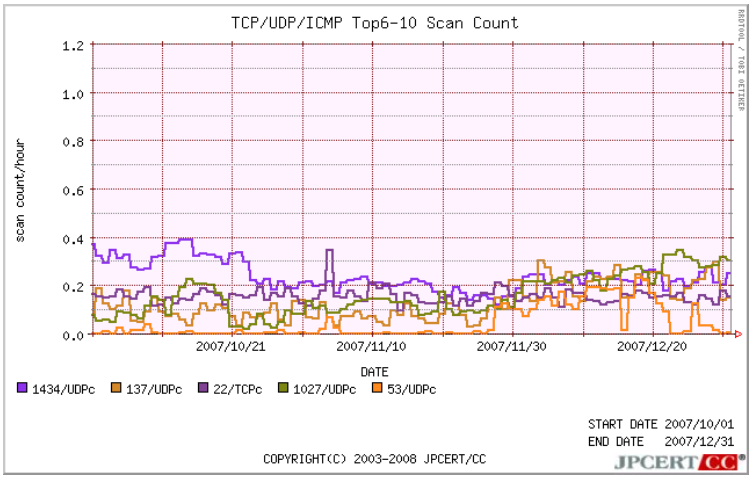


図 2-2: アクセス先ポート別グラフ top6-10

また、より長期間のスキャン推移を表すグラフとして、2007 年 1 月 1 日から 2007 年 12 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 2-3、図 2-4 に示します。

- アクセス先ポート別グラフ top1-5 (2007 年 1 月 1 日-2007 年 12 月 31 日)

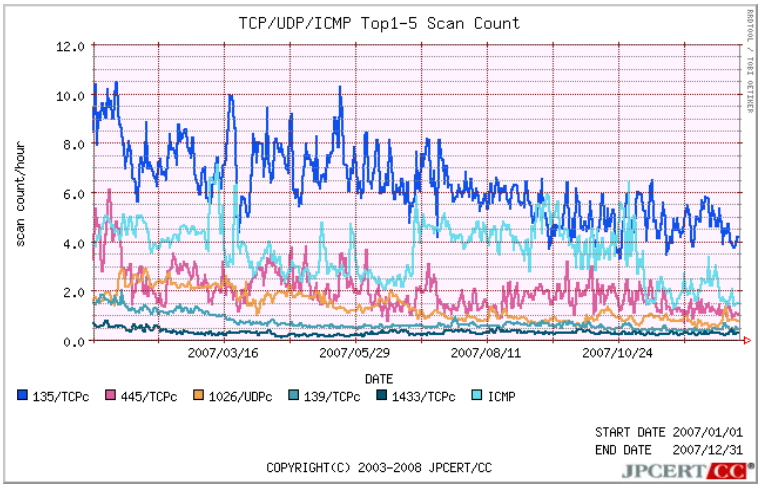


図 2-3: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2007 年 1 月 1 日-2007 年 12 月 31 日)

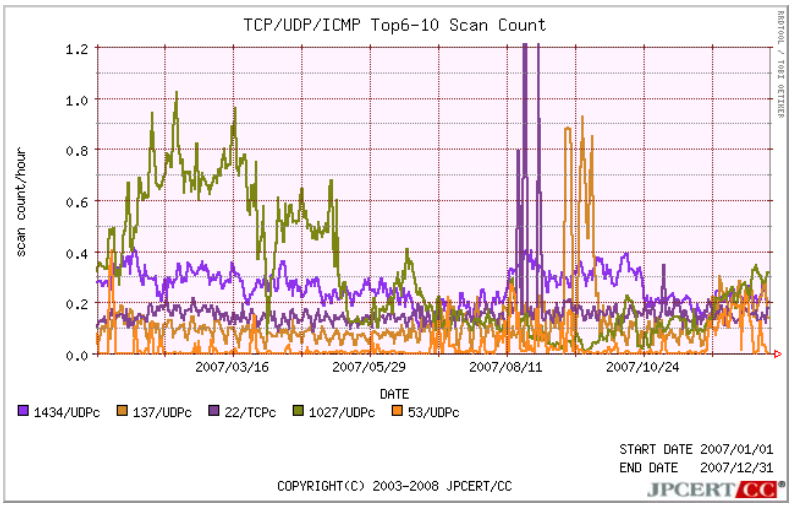


図 2-4: アクセス先ポート別グラフ top6-10

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、ファイアーウォール ・ウイルス等対策ソフトウェア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 年 11 月 1 日-2007 年 12 月 31 日)

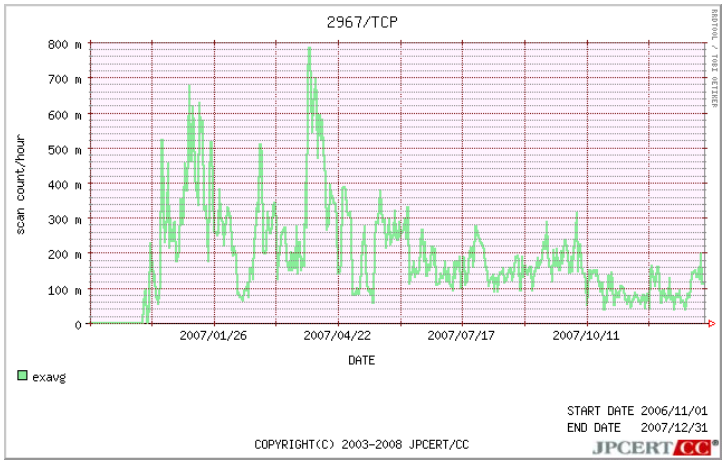


図 2-5: アクセス先ポート別グラフ TCP 2967 番ポート

(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 年 4 月 1 日-2007 年 12 月 31 日)

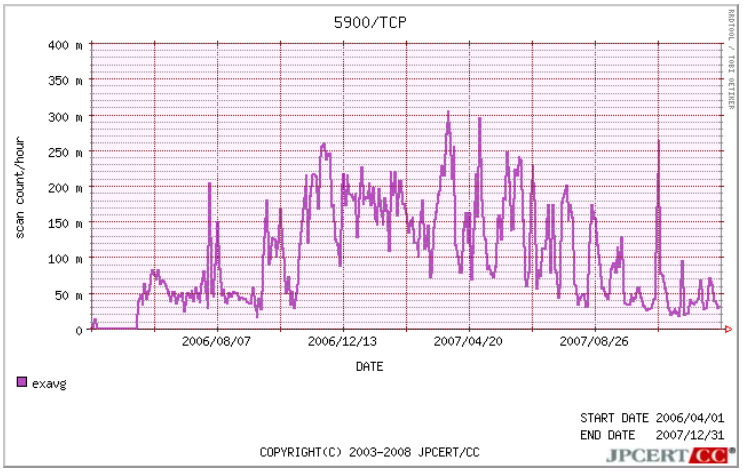


図 2-6: アクセス先ポート別グラフ TCP 5900 番ポート

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います。前年の同時期に比べて 2 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 年 10 月 1 日-2007 年 12 月 31 日)

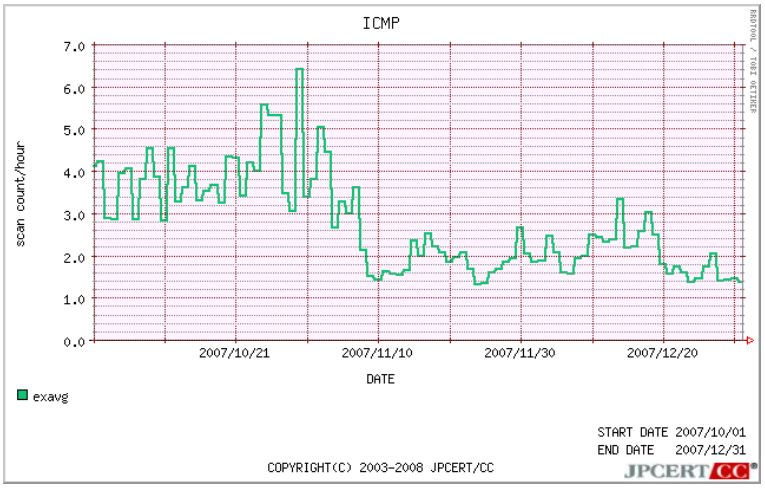


図 2-7: ICMP パケット受信グラフ

(4) TCP5168 番ポートへのスキャンは沈静化

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。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、現在は沈静化しております。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 5168 番ポート (2007 年 8 月 16 日-2007 年 12 月 31 日)

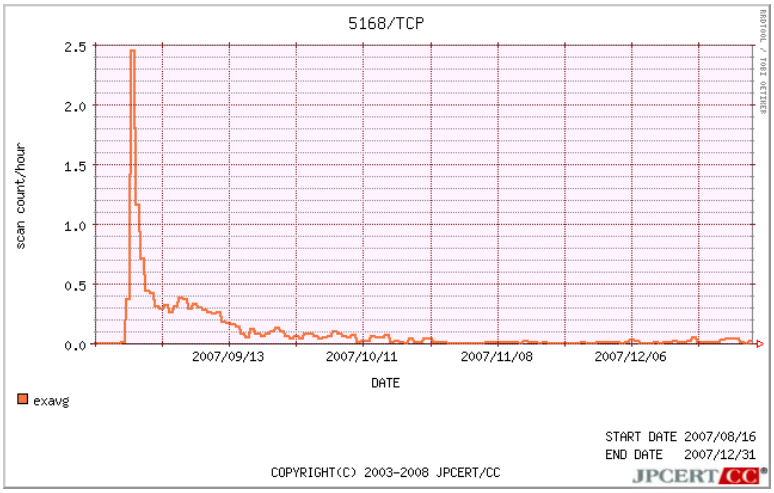


図 2-8: アクセス先ポート別グラフ TCP 5168 番ポート

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

§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

2007 年 10 月 1 日から 2007 年 12 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 48 件 (総計 545 件)[図 3-1] でした。これまでに引き続きクロスサイトスクリプティングの脆弱性が多数を占めています。また、受動的な攻撃につながる脆弱性が目立ったことも本四半期の特徴です。各公開情報に関しましては、JVN(http://jvn.jp/)をご覧ください。

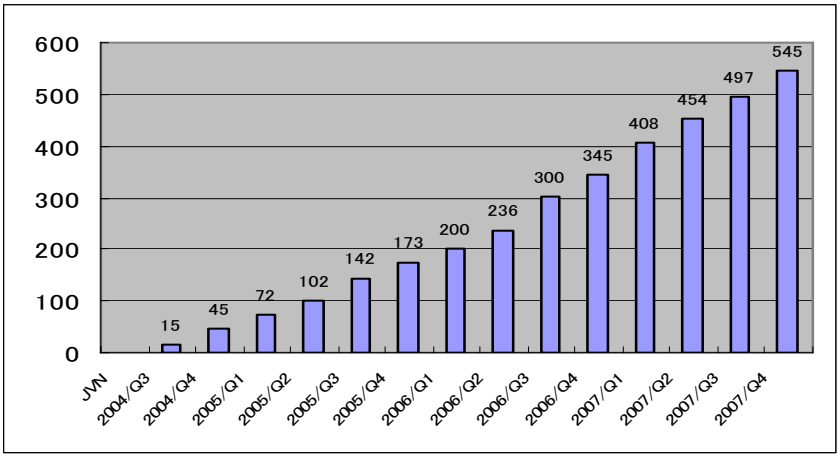


図 3-1: 累計 JVN 公表件数

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 31 件(累計 242 件)[図 3-2]でした。

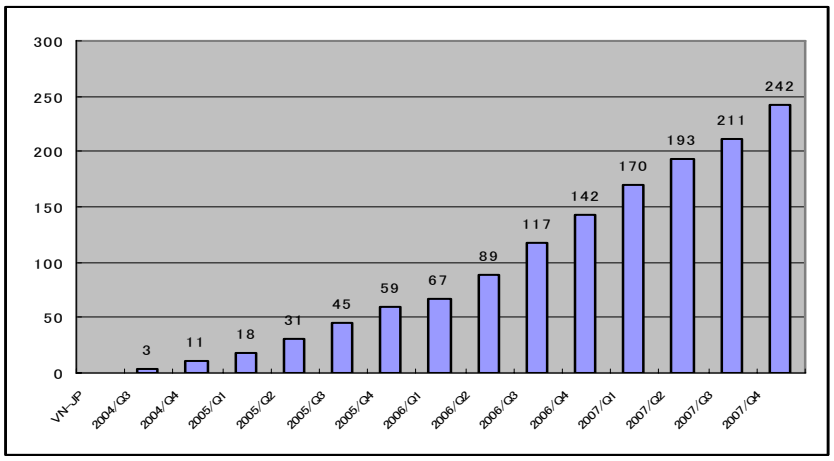


図 3-2: 累計 VN-JP 公表件数

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 17 件(累計 282 件)[図 3-3]でした。

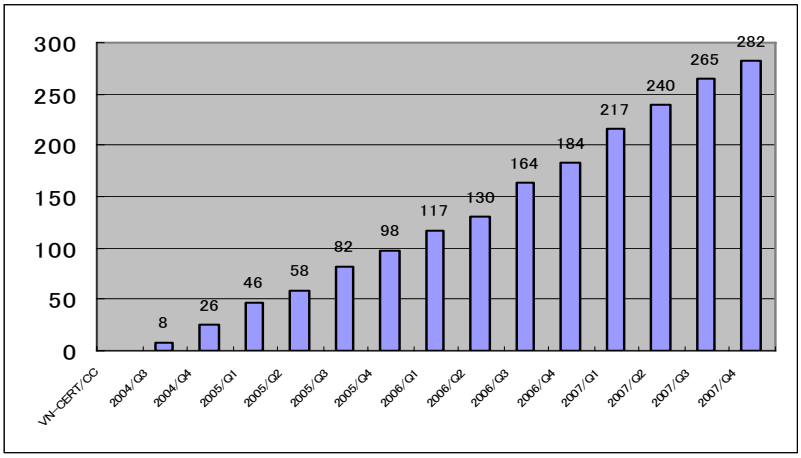


図 3-3: 累計 VN-CERT/CC 公表件数

また、CPNI とのパートナーシップに基づき、JVN にて VN-CERT/CC として公開された脆弱性情報は 0 件(累計 21 件)[図 3-4]でした。

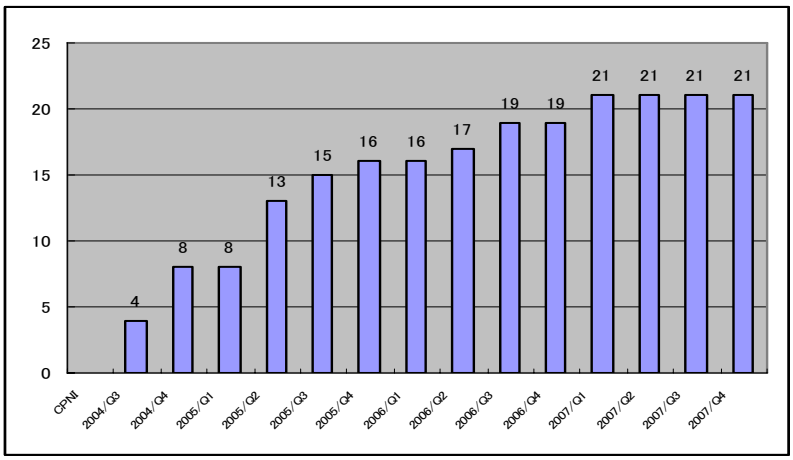


図 3-4: 累計 VN-CPNI 公表件数

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_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。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。2007 年 12 月 31 日現在で 217 社[図 3-5]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、http://www.jpcert.or.jp/vh/agreement.pdf をご参照ください。

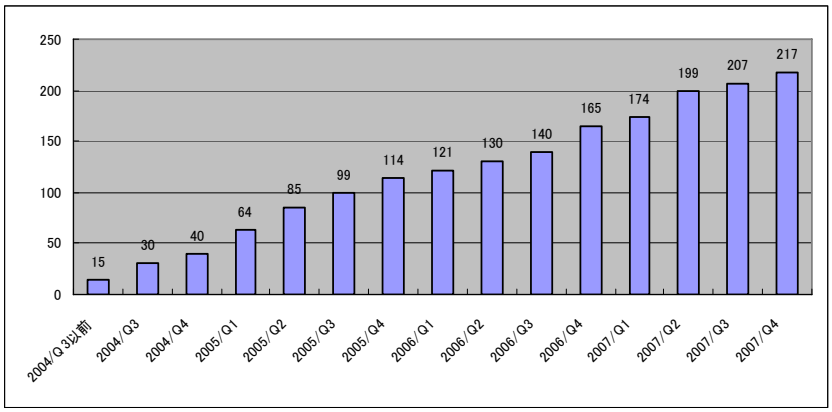


図 3-5: 累計製品開発者登録数

(3) Vulture Meeting の開催

JPCERT/CC は、CERT/CC(アメリカ)、CERT-FI(フィンランド)の CSIRT 脆弱性情報ハンドリング・チームと合同で、脆弱性情報ハンドリング業務において、より信頼度の高い協力関係と連携強化を促進するために、ミーティングを開催しました。将来の脆弱性情報ハンドリング業務のカウンターパートナー候補として CERT-FI(フィンランド)を迎え、組織の活動概要を共有し、必要機能の模索など、調整業務の負荷を軽減するシステム構築のアイデアやノウハウを共有しました。

(4) 脆弱性コーディネータおよび研究者の合同ミーティングを開催

昨今多発する脆弱性問題の中で、研究者が注目する、脆弱性の新たな脅威と動向を、研究者間およびコーディネータで共有しました。これによりコーディネータは、想定される脆弱性の技術動向に関する予備知識を得て、今後のコーディネーションの参考とし、研究者は現場の現状のフィードバックを受け、今後の研究の参考としました。コーディネータと研究者の間でディスカッションを行うことにより、相互の関係の強化を図りました。

(5) OpenSource Conference 2007 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 10 月 27 日に開催された OpenSource Conference 2007 Niigata 及び 2007 年 12 月 8 日に開催された OpenSource Conference 2007 Fukuoka に参加しました。脆弱性情報ハンドリング業務内容と活動状況、及び、セキュアコーディングへの取組みについて紹介し、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 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/

2007 年 10 月度　サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200710/0710monthly.html

2007 年 11 月度　サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200711/0711monthly.html

§6. 国際連携活動関連

I. 海外 CSIRT 状況調査、連携強化、トレーニング等

インターネットセキュリティの分野において、技術的に高いレベルの攻撃者が存在する可能性があり、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組みの実施状況に関する情報収集が必須となる地域には、調査と連携強化を目的に、CSIRT 訪問を実施しました。

10 月から 12 月の訪問件数：7 件
訪問先　：　BD-CERT (バングラディッシュ)、CERT.br (ブラジル)、CERT/CC (アメリカ)、GovCERT.NL (オランダ)、RU-CERT (ロシア)、SL-CERT (スリランカ)、ThaiCERT (タイ)

II. 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。

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。

§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 構築を検討及びその活動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。

10 月から 12 月の支援件数:6 企業、2 組織、1 団体

II. 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。

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

[理事]

(1) 早貸淳子
「情報セキュリティに関する脅威の最新動向と対策状況」(PDF:1.71MB)
日経BPセキュリティ・ソリューションフォーラムin Security / 2007 年 10 月 26 日

(2) 歌代和正
「最新セキュリティ動向と CSIRT の役割」
チェック・ポイント・ソフトウェア・テクノロジーズ 株式会社
創立 10 周年記念セミナー / 2007 年 11 月 6 日

[早期警戒グループ]

(3) 鎌田敬介

「セキュリティインシデント最新動向とJPCERT/CC活動」(PDF:4.12MB)

警察大学校 / 2007 年 10 月 17 日

(3) 中谷昌幸

「近時の情報セキュリティに関する脅威の動向」(PDF:417KB)

InternetWeek 2007 / 2007 年 11 月 19 日

(4) 小宮山功一朗

「海外動向」(PDF:137KB)

InternetWeek 2007 / 2007 年 11 月 19 日

(5) 鎌田敬介

「違法・有害情報対～フィッシング・マルウェアへの対応～」(PDF:513KB)

InternetWeek 2007 / 2007 年 11 月 21 日

(6) 小宮山功一朗

「今、企業のセキュリティ対策は、何を求められているのか」(PDF:548KB)

Email Security Conference2007 / 2007 年 11 月 28 日

(7) 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 / 2007 年 12 月 14 日

(8) 名和利男

「サイバー上のインシデントに対応するための最善策 CSIRT について」

ISACA東京支部 2007 年 12 月例会 / 2007 年 12 月 19 日

§9. 掲載記事一覧

(1) 情報流通対策グループ 久保正樹

最新KEYWORD JVN

日経BP社日経NETWORK / 2007 年 11 月号 Page 20-21

(2) 常務理事　早貸淳子

「悪質化・多様化する脅威、頼りはセキュリティ対策」

株式会社日本情報産業新聞社　日本情報産業新聞 / 2007 年 11 月 26 日 Page 7

(3) 業務統括　伊藤友里恵

組織で戦うセキュリティ脅威

「攻撃者のコミュニテイは強大化、守る側も結束を固めて対抗を」

日経BP社日経コンピュータ /　2007 年 11 月 26 日号 Page 58-61
