JPCERT CC®

JPCERT-PR-2008-0005

JPCERT/CC 活動概要 [2008 年 4 月 1 日 ～ 2008 年 6 月 30 日]

2008-07-07 発行

【 活動概要トピックス 】

― トピック 1 ― CSIRT 運用フェーズマテリアルなど 5 種類の調査・研究資料を公開

JPCERT コーディネーションセンターは、昨年度に行った調査、研究をまとめた報告書を順次公開しました。

情報セキュリティに関する脅威は、攻撃手法の多様化や複雑化に伴って変化し続けており、企業等の組織にとっては、インシデントの発生を前提とした自律的な対応体制を運営することが一層重要になってきているといえます。JPCERT/CC では、昨年度の CSIRT（Computer Security Incident Response Team）構築関係のマテリアル公開に続き、以下の(1)にある組織内 CSIRT の運用フェーズに関する解説書を公開しました。

また、制御系システムとは、大規模な石油化学プラントの制御や、電力システムの監視制御、ダムや水供給システムの監視制御など、製造業を含むさまざまな産業領域で利用されている自動制御やリモート監視のためのシステムですが、制御系システムに関連するソフトウエアに脆弱性が発見される事案が散見され始めています。こうした背景を踏まえ、JPCERT/CC では、制御系システムの現状を把握し、それに関わる脆弱性の取り扱いを円滑化するため、以下の(2)および(3)にある調査を行いました。

さらに、ソフトウエアの開発段階における脆弱性対策の活動の一環として、ｉ）「製品開発工程において脆弱性の発生につながるような欠陥が作りこまれないこと、仮に作りこまれたとしても出荷前の検証等の段階で発見して対応が行われること」の実現に資するための活動として、以下の(4)にある「C/C++ セキュアコーディングスタンダード」の有効性評価に関する報告書を、ⅱ）発見された脆弱性に対するユーザ側での対応の効率化を支援するためのツールに関するの評価を行った成果として、以下の(5)にある脆弱性対応意思決定支援システムに関する研究成果論文を、それぞれ公開しました。

(1) CSIRT マテリアル 「運用フェーズ」:

各団体や組織の情報セキュリティ責任者その他の関係者の皆様が、組織内 CSIRT の構築を検討し、実際に CSIRT の構築・運営を行う際に参考となるよう、組織内 CSIRT の必要性や位置づけ、組織内 CSIRT の運用、インシデントハンドリング概論および具体的なハンドリングフローなどを読みやすくまとめた解説書

(2)「制御系プロトコルに関する調査研究」報告書 調査報告書サマリ、調査報告書(本編)目次：

これまで海外で発見され、関係機関から連絡を受けている制御系システムに関する脆弱性情報は、制御系システムで使用される「プロトコル」の脆弱性がその中心となっていることか

ら、制御系の「プロトコル」について、主としてセキュリティ面からの調査を行った報告書
※本編は、希望者のみに個別提供

(3) 国内の制御系システム、制御系プロトコルに関する調査報告書：
制御系システム分野の方々とセキュリティ専門家との共通理解の一助となるよう、国内の制御系システムにおける標準的な通信プロトコルの利用動向と、同業界内のセキュリティ強化に向けた動きを調査した報告書

(4) ソースコード解析ツールを活用した CERT セキュアコーディングルールの有効性評価：
ソフトウエア製品の開発や出荷前の検証（品質確認）において、より安全なソフトウエア製品を提供するための対策としての、「C/C++セキュアコーディングスタンダード」ルールセットおよび、これを組み込んだソースコード解析ツールの有効性について実証的な評価分析を行った報告書

(5) Vulnerability Response decision Assistance (脆弱性対応意思決定支援システム)：
ソフトウエア等の脆弱性の問題に関し、製品を利用する組織が、効率よく、また属人性を排した統一的な脆弱性への対応ができるよう、JPCERT/CC と CERT/CC が共同で設計を行った意思決定を支援するためのシステムに関するコンセプト論文

― トピック 2 ― C/C++セキュアコーディングトワイライトセミナースタート
脆弱性のない安全なプログラムを開発するために
～ソフトウエアの脆弱性が作りこまれる根本的な原因を学び、問題を回避する～

JPCERT コーディネーションセンターは、情報家電や組込み機器等のソフトウエアやファームウエアの開発に利用されている C/C++言語について、脆弱性を含まない安全なプログラムをコーディングする具体的なテクニックとノウハウを学んでいただくため、本年 6 月 4 日から、毎月第 1 水曜日に、全 7 回の予定で無料セミナーを開催しています。
組込み製品は、脆弱性の修正を出荷後に適用することが困難なケースも多いため、そもそも製品開発者が脆弱性を製品に作りこまないことが非常に重要です。JPCERT/CC では、脆弱性を抱えたまま市場に出回る製品の数を減少させるための活動として、このセミナーを実施しています。
本セミナーは、C/C++言語を使ってプログラム開発に携わる全ての方を対象としています。
具体的なコーディングテクニックのみならず、ソフトウエアに作り込まれた脆弱性によるリスクや、安全なソフトウエア開発への投資の意義についても理解を深めていただけると考えています。

プログラムおよび日程の詳細はこちらをご覧ください。
http://www.jpcert.or.jp/event/twilight-seminar.html

JPCERT CC®

― トピック 3 ― Japan Vulnerability Notes (JVN) 英語版の公開

国内で利用されるソフトウエア等の脆弱性に関する情報は、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」に従って取り扱われ、IPA と JPCERT/CC が共同で運営する JVN および JVN iPedia において公開されています。昨今、製品のグローバル化により、国内製品の脆弱性に関する情報は、国内のみならず海外でも重要性が高まっており、海外の利用者やベンダとの間の英語による情報共有の需要も高まっています。このような状況を踏まえ、IPA と JPCERT/CC は、国内で取り扱った製品の脆弱性関連情報を諸外国の調整機関や開発者、利用者と共有する取り組みの一環として、JVN および JVN iPedia の英語版を開設することとし、2008 年 5 月 21 日から公開しました。

製品開発者の協力も得ながら、英語化した情報発信を日本から直接行うことにより、英語圏の利用者に対し、正確な情報を迅速に提供することが可能になります。また、日本国内の脆弱性関連情報の取組みへの理解を促し、海外の製品開発者からの JVN および JVN iPedia への情報提供増加に寄与することも期待しています。

http://jvn.jp/en/

― トピック 4 ― 第 20 回 FIRST Annual Conference 開催、来年の開催地は京都に決定

本年 6 月 22 日から 27 日まで、カナダのバンクーバーにおいて、第 21 回 FIRST Annual Conference が開催されました。今回は、全世界 48 ヵ国から 400 人以上の代表が集結し、日本からも多くの CSIRT メンバが参加して、世界でも最大規模のセキュリティ会議となりました。今年のテーマである"Crossing Borders: Towards the Globalization of Security"のもと、フィッシング対応やネットワークモニタリングに関する技術的なトピックから CSIRT 運営や活動評価などマネージメントに関するトピックまで、情報セキュリティ全般にかかる様々な話題がとりあげられました。また、JPCERT/CC の業務統括である伊藤友里恵がセッションチェアをつとめる"FIRST Law Enforcement/CSIRT Cooperation SIG"も開催され、活発な意見交換がされました。

さらに、本カンファレンスにおいて，来年の FIRST Annual Conference の開催地が京都に決定したことが正式に発表されました。JPCERT/CC は、開催国のローカルホストとして、国内の CSIRT メンバや関係機関の協力を得ながら、京都会合の成功に向けた準備を進めていく予定です。

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

深刻か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： 12 件 http://www.jpcert.or.jp/at/

2008-06-25 Adobe Acrobat 及び Adobe Reader の脆弱性に関する注意喚起 (更新)
2008-06-24 Adobe Acrobat 及び Adobe Reader の脆弱性に関する注意喚起 (更新)
2008-06-24 Adobe Acrobat 及び Adobe Reader の脆弱性に関する注意喚起 (公開)
2008-06-11 SNMPv3 を実装した複数製品の認証回避の脆弱性に関する注意喚起 (公開)
2008-06-11 2008 年 6 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)
2008-05-29 Adobe Flash Player の脆弱性に関する注意喚起 (更新)
2008-05-28 Adobe Flash Player の未修正の脆弱性に関する注意喚起 (公開)
2008-05-19 Debian GNU/Linux に含まれる OpenSSL/OpenSSH の脆弱性に関する注意喚起 (更新)
2008-05-16 Debian GNU/Linux に含まれる OpenSSL/OpenSSH の脆弱性に関する注意喚起 (公開)
2008-05-14 2008 年 5 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)
2008-04-09 2008 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)
2008-04-08 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 (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：11 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 82 件、「今週のひとくちメモ」のコーナーで紹介した情報は 11 件です。

III. 資料公開

各分野のセキュリティに関する調査・研究の報告書や論文を提供しています。

JPCERT CC®

(1)CSIRTマテリアル運用フェーズマテリアル

組織内 CSIRT の必要性や位置づけ、組織内 CSIRT の運用、インシデントハンドリング概論および具体的なハンドリングフローなどについて、 実務の経験に裏づけされた知見やノウハウに基づき、図表等を用いて平易に解説したものです。

各団体や組織の情報セキュリティ責任者その他の関係者の皆様が、組織内 CSIRT の構築を検討されたり、実際に CSIRT の構築・運営を行われたりする際に、 これらの資料を支援ツールとして御活用いただき、ひいては、実効的な CSIRT 機能の構築・運営が普及することを期待しています。

・「CSIRT ガイド」(PDF:1.32MB) (PGP 署名)
・「インシデントハンドリングマニュアル」(PDF:421KB) (PGP 署名)

(2)「制御系プロトコルに関する調査研究」報告書

近年、制御系システムで使用されるソフトウエアの脆弱性が発見、報告、公開されるようになってきており、その重要性に鑑み、社会的な関心が高まってきています。JPCERT/CC においても、そのような制御系システムに関連する脆弱性情報のハンドリングおよび関連情報の公開を行っており、その数は増えつつあります。

これまで発見、公開されている制御系システムに関わる脆弱性は、主として、海外で発見され、海外の関係機関から連絡を受けた脆弱性情報であるとともに、 対象としては制御系システムで使用されるプロトコルに関する脆弱性がその中心となっています。

JPCERT/CC では、このような状況を踏まえ、制御系プロトコルに関して、幅広く調査を行うことが今後の制御系システムに関わる脆弱性の取り扱いを進める うえで重要であると考え、調査を行いました。

本報告書は、制御系システムの脆弱性取扱いに関連して、現在制御系システムで使用されている標準的なプロトコルについて、主としてセキュリティ機能に着目して、 調査結果をとりまとめたものです。

・調査報告書サマリ ：(PDF:215KB) (PGP 署名)
・調査報告書 (本編) 目次 ：(PDF:54.2KB) (PGP 署名)
※調査報告書 (本編/英語版) をご希望の方は、広報 (office@jpcert.or.jp) までご連絡ください。

(3)国内の制御系システム、制御系プロトコルに関する調査報告書

制御系システムは、製造業を含むさまざまな産業領域で利用されている他、大規模な石油化学プラントの制御や、電力システムの監視制御、 ダムや水供給システムの監視制御など国民生活の基盤サービスを提供する重要なシステムとして利用されています。その一方で、制御系システムに

関連するソフトウエアに脆弱性が発見されると言う事案も散見され始めています。

国際的な枠組みで脆弱性関連情報の対応の調整を行っている JPCERT/CC においても、2006 年度以降、海外の脆弱性情報取扱い組織から制御系システムに関する脆弱性情報の報告を受けており、2008 年 2 月までに計 13 件の脆弱性情報を JVN (Japan Vulnerability Notes) 上で公開しています。通常の情報処理分野の製品に比してまだ件数は少ないものの、今後も報告件数が増えていく可能性が高いと予測されます。

このような状況を背景に、JPCERT/CC では、国内で利用されている制御システム関連製品に関する脆弱性情報の届出が行われた場合、調整機関として迅速かつ的確に影響を推定し、製品開発ベンダや製品利用業界などとの調整活動を円滑に進めることができるよう、以下 2 点につき調査し、報告書としてまとめました。

1.国内の制御系システムの通信コンポーネントにおける汎用プロトコルの利用概観の調査
2.国内の制御系システムに関するセキュリティ活動の取り組み状況調査

この報告書では、国内の制御系システムにおける標準的な通信プロトコルの利用動向と、同業界内のセキュリティ強化に向けた動きをまとめています。 この分野の方々とセキュリティ専門家との間の共通理解のための一助となることを期待します。

・国内の制御系システムにおける汎用通信プロトコルの利用状況およびセキュリティへの取組み状況に関する調査 (PDF:709KB) (PGP 署名)

(4)ソースコード解析ツールを活用した CERT セキュアコーディングルールの有効性評価報告書

市場に出荷された多くのソフトウエア製品に発見される脆弱性は、プログラミングエラーによって引き起こされています。 製品出荷後に発見される脆弱性を修正するには、場合によっては、ソフトウエアのデザイン(設計)の見直し、大規模な再コーディング、再テストが必要になる上、修正プログラムの開発・周知および配付のためのコストがかかることとなります。さらに、利用者側においても、修正プログラムの適用のためのリスクと、コストがかかることになります。
このような問題を回避するためには、製品開発工程において、脆弱性の発生につながるような欠陥を作りこまないこと、 仮に作りこまれたとしても出荷前の検証等の段階で発見して対応が行われること等が有効な対策となり得ると考えられます。そのための対策のひとつとして、「C/C++ セキュアコーディングスタンダード」というルールセットが開発されています。
CERT/CC と JPCERT コーディネーションセンターは、共同で、ソフトウエアの品質確認において、このルールセットの一部を実装した「ソースコード解析ツール」を実験的に利用することにより、「C/C++ セキュアコーディングスタンダード」の有効性と、このルールセットへの適合状況を機械的に効率よく検出することが可能であるか(実用性)を評価するプロジェクトを実施しました。

・英語版
ソースコード解析ツールを活用した CERT セキュアコーディングルールの有効性評価報告書(PDF:572KB) (PGP 署名) (2008-06-20)
※日本語版は 7 月公開予定

(5)Vulnerability Response Decision Assistance (脆弱性対応意思決定支援システム)日本語版
Vulnerability Response Decision Assistance (脆弱性対応意思決定支援システム、略称：VRDA、読み：ヴァーダ) は、ソフトウエア等の脆弱性の問題に関し、企業等の組織が効率よく、また一貫して対応することができるよう、脆弱性対応の内容に関する意思決定の効率化を支援するために、JPCERT/CC と CERT/CC が共同で設計した意思決定支援システムのコンセプトです。本論文は、VRDA コンセプトを構成する 3 つの要素について解説したものです。

1.脆弱性関連情報のデータ交換フォーマット
2.脆弱性情報に対する評価基準や対策ルールといった、その企業や組織特有の思考ロジックを定義した対応意志決定モデル
3.意思決定モデルの構築手法
・概要 ：(PDF:1.27MB) (PGP 署名)
・論文 ：Vulnerability Response Decision Assistance (脆弱性対応意思決定支援システム) (PDF:279KB) (PGP 署名)

§2. 早期警戒 ーインシデントハンドリングー
JPCERT/CC が 2008 年 4 月 1 日から 2008 年 6 月 30 日までの間に受け付けた届出のうち、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）に関する届出は 584 件です。実際に届出を受けたメール、FAX の数は、延べ 768 通（*1）で、インシデントの件数を IP アドレス別に計上すると 737 アドレスです。

*1: 届出のメール、FAX には、異なる届出者の方から同一サイトのインシデント情報が含まれるため、届出件数とメール、FAX の総数が異なっています。

上記、届出を受けた中から JPCERT/CC が国内外の関連するサイトに通知連絡した件数は 448 件です。この通知連絡の件数は、フィッシングサイトが設置されているサイトや、有害なサイトへ誘導するコードを埋め込まれた改ざんされたサイト、悪意のあるウイルス等マルウェアが置かれたサイト、Scan のアクセス元等の管理者及び関係協力組織への連絡仲介依頼を含むインシデントの届出に基づいて行ったものです。

I. 分析
2008 年 3 月から断続的に発生している SQL インジェクション攻撃や、Web アプリケーションの脆弱性の探査を意図したアクセスの届出が全体的に増えていることから、攻撃の対象が、Web サ

ーバの脆弱性から Web アプリケーションの脆弱性に移行しているように推測されます。
Web サイト管理者は、Web サーバだけでなく、Web サーバ上で動作する Web アプリケーションや、データベースに対する根本的な対策を講じることを強く推奨します。

また、国内外の金融機関やオークションサイト、国内 ISP のオンラインサービスを装ったフィッシングサイトの届出が、前四半期に比べ、若干減少しています。ただし、JPCERT/CC が通知連絡したサイトのいくつかで、しばらく経った後に再び別のフィッシングサイトが設置されているケースがありました。一度侵入されたシステムは、悪意のある攻撃者によって何をされているかわかりません。例えば、既存のプログラムに特別な機能を取込ませたり、管理者に気付かれないように侵入するためのバックドアなどを設置したりする場合があります。そのすべてを排除するのは非常に困難かつコストがかかりますので、システム自体を再インストールし、適切なセキュリティ対策を実施することを推奨します。

インシデントハンドリング業務の詳細については、別紙「JPCERT/CC インシデントハンドリング業務報告」
をご参照ください。

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

インシデントによる被害拡大及び再発の防止のため、今後とも JPCERT/CC への情報提供にご協力をお願いいたします。

インシデントの届出方法については、以下の URL をご参照ください。

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

§3. 早期警戒 ー情報収集・分析ー

JPCERT/CC 早期警戒グループでは、国内の企業ユーザが利用するソフトウエア製品の脆弱性情報、国内インターネットユーザを対象としたコンピュータウイルス、Web 改ざんなどのサイバー攻撃に関する情報を収集、分析しています。
JPCERT/CC では、これら様々な脅威情報を多角的に分析（場合によっては、脆弱性、ウイルスの検証などもあわせて行います）し、その分析結果に応じて、国内の企業、組織のシステム管理者を対象とした注意喚起や、国内の重要インフラ事業者を対象とした早期警戒情報を
JPCERT/CC Web を使用して発信することにより、国内におけるサイバーインシデントの発生・拡大抑止を目指しています。

JPCERT CC®

I. 2008 年 Q2(4-6 月)の動向について

2008 年 Q2(4-6 月)は、Microsoft Windows と Apple Mac OS X のサービスパックなどの公開が相次ぎました。Microsoft Windows XP については、前回のサービスパック提供から約 3 年 5 ヶ月ぶりのサービスパックの提供となり、Microsoft Windows Vista については、2007 年 1 月の発売以来初めてサービスパックが提供されました。また、Apple Mac OS X においても、多数の修正パッチを含む修正プログラムの公開が 2 回行われました。
この他にも、国内で一般によく利用される Microsoft Internet Explorer、Apple Quicktime、Adobe Reader、Adobe FlashPlayer 等について、ゼロデイ脆弱性の公開がありました。

今期は、SQL インジェクション攻撃による Web サイト改ざんが急増しました。この攻撃により改ざんされた Web サイトの数は、一部報道によると国内外で数十万にのぼるとのことです。Web サイトが改ざんされた場合、その被害はサイト運営者のみならず、サイト閲覧者にまで拡大することになります。このため、自組織で運営している Web サイトが改ざんされていないか確認し、脆弱性検査を行うことをご検討ください。

また、特定の組織を対象としてメールの文面や件名を巧妙に作成した「標的型攻撃」が相次いで発生しています。この標的型攻撃では、多くの場合、Microsoft Word、 Microsoft PowerPoint、Adobe Acrobat などのオフィスでよく利用されるアプリケーションの既知の脆弱性が使用されます。このため、OS、アプリケーションを最新の状態に維持することで攻撃の影響を受ける可能性を低減させることができます。

昨今、金銭の詐取を目的としたとおもわれる攻撃が増えています。一例として、企業の Web ページに対して DDoS 攻撃をしかけ、攻撃を止める代わりに金銭を要求する恐喝事件が発生しています。

II. インターネット定点観測システム(ISDAS)

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。

1.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 4 月 1 日から 2008 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 (2008 年 4 月 1 日-6 月 30 日)

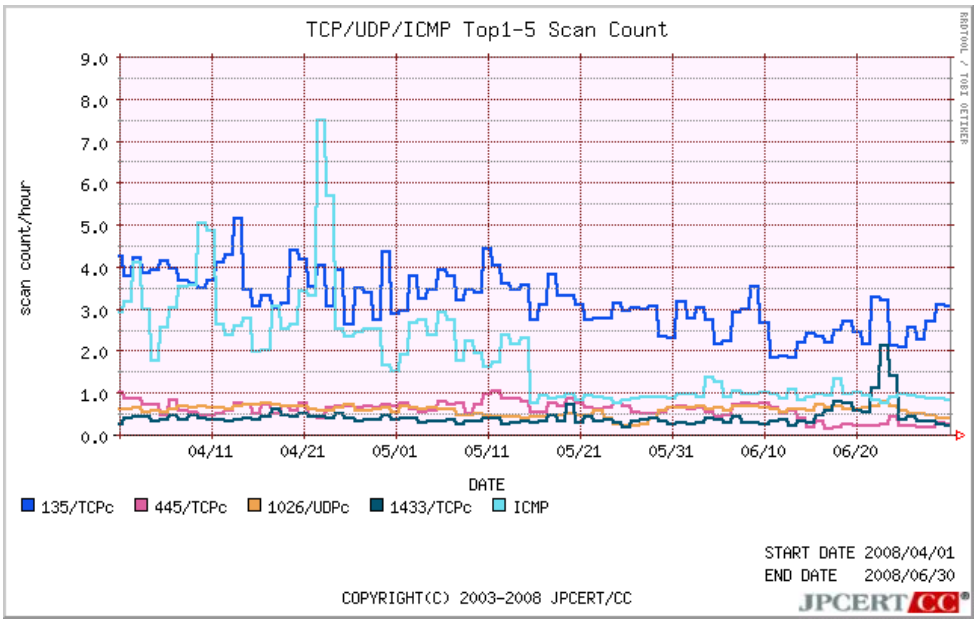

図 2-1: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2008 年 4 月 1 日-6 月 30 日)

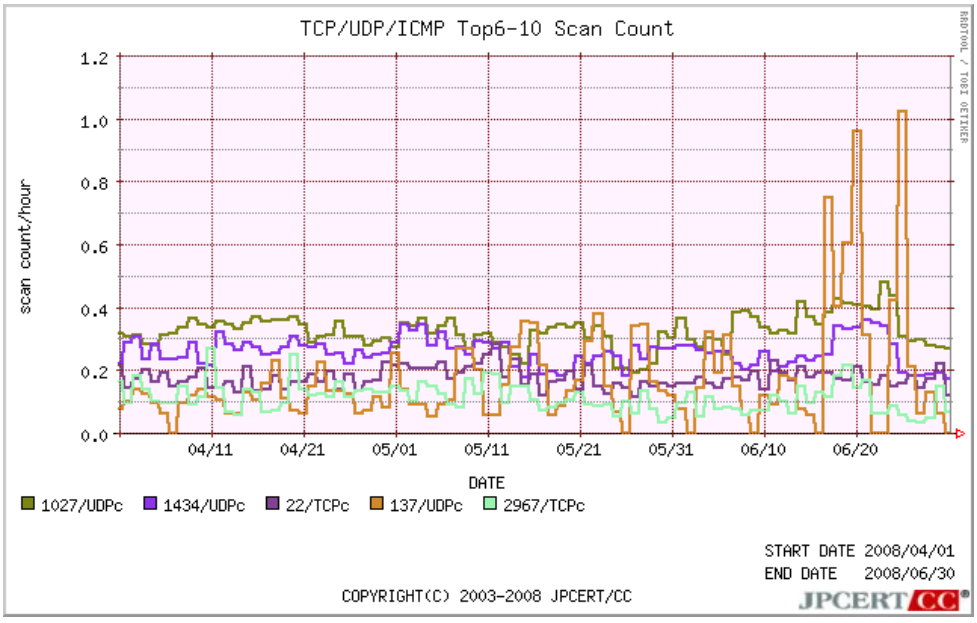

図 2-2: アクセス先ポート別グラフ top6-10

また、より長期間のスキャン推移を表すグラフとして、2007 年 7 月 1 日から 2008 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 (2007 年 7 月 1 日-2008 年 6 月 30 日)

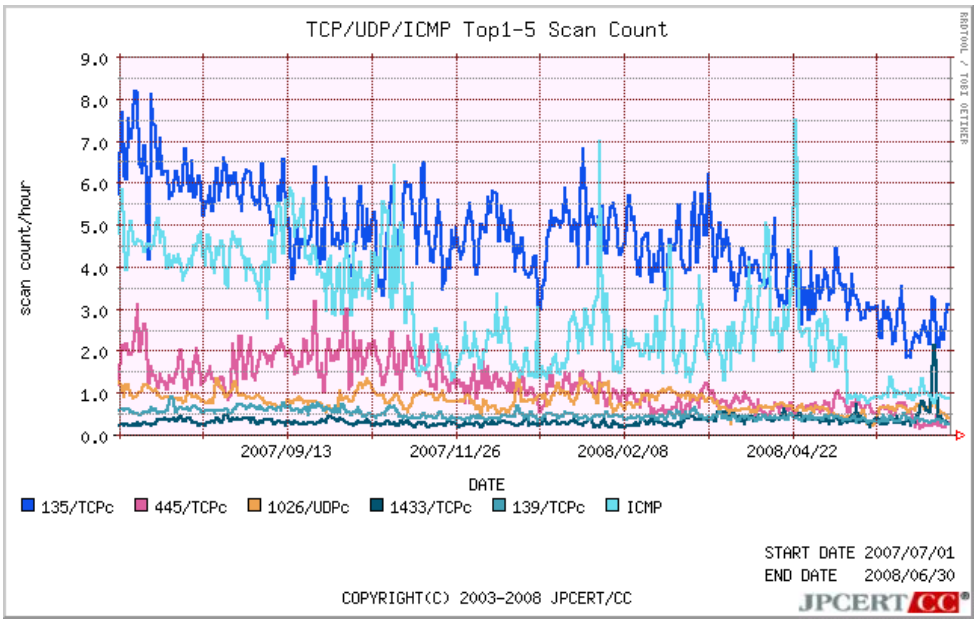

図 2-3: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2007 年 7 月 1 日-2008 年 6 月 30 日)

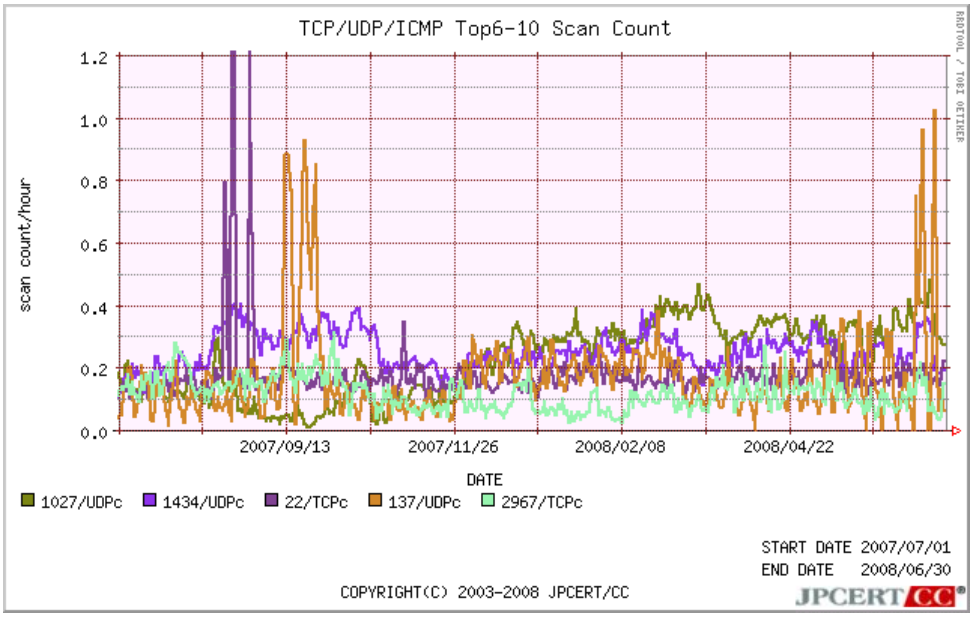

図 2-4: アクセス先ポート別グラフ top6-10

引き続き Scan 数は減少傾向が見られますが、Windows 環境を対象としたものが Scan の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。

III. 調査

1.標的型攻撃対策調査(平成 19 年度)

JPCERT/CC では、企業、組織のヒアリングから標的型攻撃の動向を調査し、それに適した標的型攻撃対策のあり方を検討しました。特に「予防接種」という疑似標的型攻撃を組織に対して行う手法で社員などのセキュリティ意識を向上し、教育効果を引き上げるというアプローチに着目しました。平成 19 年度は、企業の協力をいただいて、5 社延べ 100 人以上に予防接種を行い、対策の利点を確認いたしました。本調査の報告書は、平成 20 年 7 月に公開予定です。

2.効果的な予防接種手法の調査(平成 20 年度)

JPCERT/CC では、平成 19 年度の調査を基に、より大規模に予防接種を実施し、その効果を測定する調査を行っていきます。現在は、いかなる事前教育が必要か、 被験者に対していかなる事後教育を行うと標的型攻撃への注意力が高まるかなどの調査計画を立案しています。

3.IPv6 脆弱性に関する調査

JPCERT/CC では、平成 19 年度 IPv6 プロトコルと IPv6 を使用したサービスについて、実際にユーザが利用する上で問題となる事項の有無について調査を行いました。この調査結果より、IPv6 に関する複数の問題点が見つかりました。

JPCERT/CC では、現在これら問題について検証と対策の検討を行っています。また、IPv6 製品を開発する企業に対し、問題点と対策(案)についての情報共有を行い、IPv6 の脆弱性を狙った攻撃の未然防止を目指していきます。

§4. 早期警戒－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 あるいはその機能の構築を検討している企業、組織及び団体に対し、調査、構築支援、機能強化を目的に資料提供や訪問、講師依頼対応などの支援活動を行いました。

1. CSIRT マテリアルの追加 - 運用フェーズマテリアルの提供

http://www.jpcert.or.jp/csirt_material/operation_phase.html

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参画するとともに、同協議会の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/

§5. 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」といいます。)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 4 月 1 日から 2008 年 6 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 42 件 (総計 631 件)[図 3-1] でした。各公開情報に関しましては、JVN(http://jvn.jp/)をご覧ください。

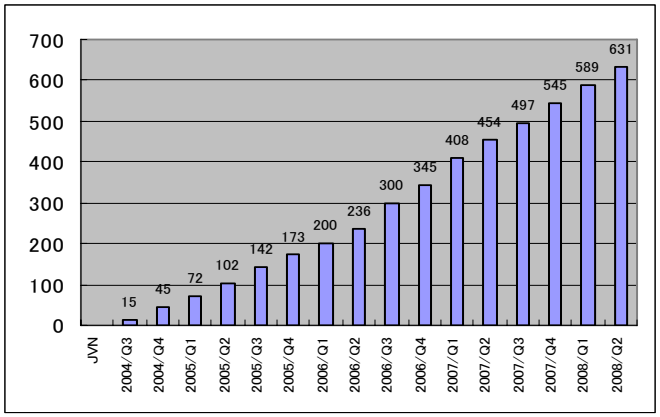

図 3-1: 累計 JVN 公表件数

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 13 件(累計 274 件)[図 3-2]でした。

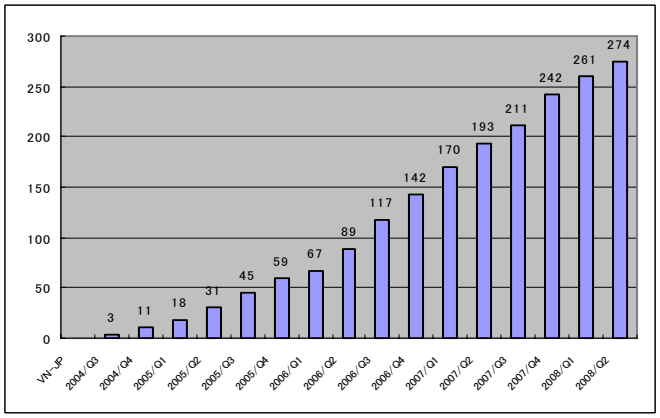

図 3-2: 累計 VN-JP 公表件数

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 29 件(累計 335 件)[図 3-3]、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 0 件(累計 22 件)[図 3-4]でした。

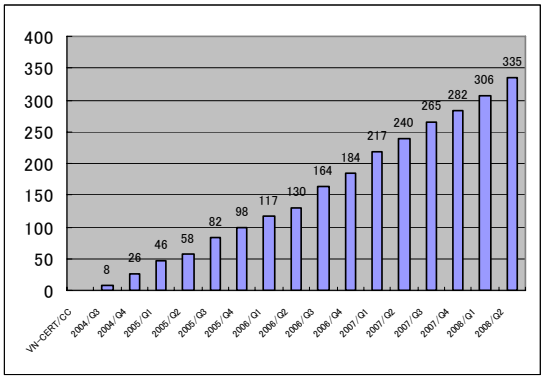

図 3-3: 累計 VN-CERT/CC 公表件数

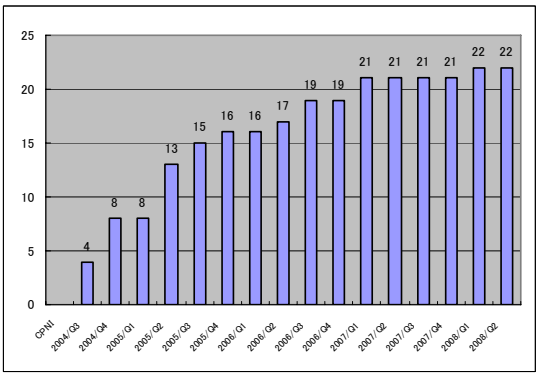

図 3-4: 累計 VN-CPNI 公表件数

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 などの海外 CSIRT との間で、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の把握等、脆弱性関連情報の公開までの情報を共有し、調整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 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/)が、調整機関にJPCERT/CC が、それぞれ指定さ

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 6 月 30 日現在で 241 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、https://www.jpcert.or.jp/vh/agreement.pdf をご参照ください。

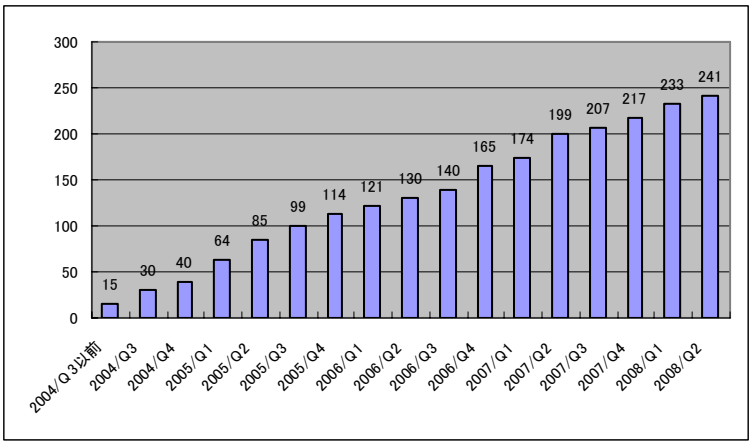

図 3-5: 累計製品開発者登録数

(3) JVN 英語版の公開

製品のグローバル化により、国内製品に関する脆弱性関連情報は、国内のみならず海外でも重要性が高まってきています。昨今の状況を踏まえ、国内で取り扱った製品の脆弱性関連情報を諸外国の調整機関や開発者、利用者と共有、また、英語圏の利用者に対し、日本国内の脆弱性関連情報の取り組みへの理解を促す取り組みの一環として、JVN 英語版を 2008 年 5 月 21 日に公開しました。

(4) C/C++ セキュアコーディング トワイライトセミナーの開催

脆弱性のない安全なプログラムを開発するために、ソフトウエアの脆弱性が作りこまれる根本的な原因を学び、問題を回避することを目的とした C/C++ セキュアコーディング トワイライトセミナーを開催しています。多くのプログラム開発関係者の方に参加いただき、 2008 年 6 月 4 日には、第 1 回として、整数に関するセキュアコーディング作法や最新状況を紹介するとともに意見交換を行ないました。毎月第 1 水曜日に、全 7 回の予定で無料セミナーを開催しています。

§6 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ウェブ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 04 月度　サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200804/0804monthly.html
2008 年 05 月度　サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200805/0805monthly.html

§7. 国際連携活動関連

I. 海外連携強化等

各国との間のインシデント対応に関する連携の枠組みの強化及び各国の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を目的とした活動を行いました。

(1) アジア太平洋地域との連携強化

一方の国内で発生したインシデントについて、原因となる問題が他方の国内にある場合における、原因の調査・排除等の対応依頼に関し、優先度を上げて相互に対応協力すること等の合意に関する覚書を、新たに、PHCERT（フィリピン）、VNCERT（ベトナム）の 2 カ国と締結し、今後のインシデント対応に関する連携を強化しました。

(2) 2008 年 4 月 8,9 日　CNCERT/CC Conference 2008 参加

中国の深圳で開催された CNCERT/CC Conference 2008 に出席し、中国国内におけるインターネットセキュリティ対策の状況等について情報収集を行いました。また、JPCERT/CC と CNCERT/CC との間におけるインシデント対応等の連携の強化について議論を行いました。

II. 海外 CSIRT コミュニケーション、トレーニング等

アジア太平洋地域における CSIRT 構築支援およびトレーニングを行っています。

(1) Information Security Initiative Workshop for “Boosting Information Security Awareness in Cambodia”　2008 年 6 月 4 日

CamCERT、NiDA 共催、JICA カンボジア支社協賛のセミナーにおいて、JPCERT/CC の活動紹介及び、CSIRT 間の国際インシデント連携活動について紹介し、情報セキュリティ対策の重要性に加え、CSIRT 構築の必要性や重要性を訴えました。

NiDA：http://www.nida.gov.kh/

JICA: http://www.jica.go.jp/Index-j.html

(2) Cam CERT 構築支援活動　2008 年 6 月 5,6 日

カンボジア国内 CSIRT である Cam CERT を訪問し、CSIRT 構築支援活動を行いました。

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。

IV. FIRST Steering Committeeへの参画　http://www.first.org/about/organization/sc.html

FIRST Steering Committee のメンバとして、JPCERT/CC の職員が FIRST の運営に協力しています。

本年 6 月 22 日から 27 日まで、カナダのバンクーバーにおいて、第 21 回 FIRST Annual Conference が開催されました。今回は、全世界 48 ヵ国から 400 人以上の代表が集結し、日本からも多くの CSIRT メンバーが参加して、世界でも最大規模のセキュリティ会議となりました。今年のテーマである"Crossing Borders: Towards the Globalization of Security"のもと、フィッシング対応やネットワークモニタリングに関する技術的なトピックから CSIRT 運営や活動評価などマネージメントに関するトピックまで、情報セキュリティ全般にかかる様々な話題がとりあげられました。また、JPCERT/CC の業務統括である伊藤友里恵がセッションチェアを務める"FIRST Law Enforcement/CSIRT Cooperation SIG"も開催され、活発な意見交換がされました。

V. 第 21 回 FIRST Conference 京都開催決定

第 21 回目となる FIRST Annual Conference 2009 (FIRST 年次会合)が、来年 2009 年、京都において開催されることになりました。JPCERT/CC は、当センター理事で、内閣官房情報セキュリティセンター情報セキュリティ補佐官でもある山口英氏を委員長とする、「開催委員会」を発足させ、開催国のローカルホストとして、国内の CSIRT メンバや関係機関の協力を得ながら、開催準備を進めていきます。

開催テーマ:「余波:インシデント復旧の技術と教訓」
開催日程：2009 年 6 月 28 日～7 月 3 日（詳細プログラム未定）
開催場所：京都　ホテルグランヴィア

http://www.first.org/

§8. 講演活動一覧

(1) 業務統括　伊藤友里恵
「Securing work environment within CNII organization」
World CyberSecurity Summit 2008 Malaysia 2008 /2008 年 5 月 22 日

(2) 早期警戒グループ　鎌田敬介
「インシデントと脆弱性対応　最新動向と組織内 CSIRT 構築」
全国地方銀行協会/2008 年 4 月 22 日

(3) 早期警戒グループ　小宮山功一朗
「国内外のフィッシング最新動向」
全国地方銀行協会/2008 年 4 月 22 日

(4) 早期警戒グループ　小宮山功一朗
「日本のセキュリティと海の向こうのセキュリティ」
RSA Conference 2008 /2008 年 4 月 23 日

(5) 早期警戒グループ　小宮山功一朗
「最近のセキュリティの傾向」
PASSJ アフタースクール/　2008 年 5 月 31 日

(6) 早期警戒グループ　名和利男
「組織内 CSIRT を巡る最近の動向について」
社団法人電子情報技術産業協会/2008 年 6 月 24 日

(7) Chris Horsley
「マルウエア分析：自動化と監視」
CeCoSII東京 /2008 年 5 月 27 日

§9. 掲載記事一覧

(1) 早期警戒グループ　鎌田敬介
北海道新聞朝刊 最新の防護態勢を
北海道新聞社 2008 年 5 月 2 日 Page32 第 2 社会

(2) 早期警戒グループ　鎌田敬介
BAN 忍び寄るサイバー犯罪の影　コンピュータの脆弱性につけ込む金銭取得目的のプロの仕業「コンピュータセキュリティインシデント」の最新動向とその対策　Page 15
教育システム　月刊 BAN /2008 年 6 月号

(3) 早期警戒グループ　名和利男
日経コミュニケーション from CSIRT フォーラム CSIRT 構築日誌
第 1 回 CSIRT は何をする組織？　Page78
日経 BP 社日経コミュニケーション/2008 年 4 月 15 日号

(4) 早期警戒グループ　名和利男
日経コミュニケーション from CSIRT フォーラム CSIRT 構築日誌

第 2 回管理するのは常に「インシデント」　Page80
日経 BP 社日経コミュニケーション/2008 年 5 月 15 日号
(5)　早期警戒グループ　名和利男
日経コミュニケーション from CSIRT フォーラム CSIRT 構築日誌
第 3 回「素早く動けること」を念頭に　Page72
日経 BP 社日経コミュニケーション/2008 年 6 月 15 日号

■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/