JPCERT-PR-2009-0001

JPCERT/CC 活動概要 [2008 年 10 月 1 日 ～ 2008 年 12 月 31 日]

2009-01-16 発行

【 活動概要トピックス 】

― トピック 1 ―

制御セキュリティ対策事業、開発者を対象としたタスクフォースの設立とワークショップ、カンファレンスの開催に向けた準備

近年、制御システム分野においても、一般の情報システムと同様に、情報セキュリティ対策の必要性が強く認識され始めています。国際的にも、制御システムにおける脆弱性の調整案件数が増えている中、制御システムに関わる技術者がセキュリティ関連情報を収集し対策を行う作業の負担を軽減し、セキュリティレベルの向上に必要な課題を効果的に解決するためには、製品ベンダ、ユーザ企業および情報セキュリティ分野の専門家による脅威や対策に関する情報の共有と連携が一層重要になってきています。

そこで、JPCERT コーディネーションセンター（以下「JPCERT/CC」といいます。）は、制御システムに関するセキュリティ関連課題を共有し、解決に向けた関係者間のより強固な連携の構築に向け実りある議論を行い、ひいては国内における制御システムの情報セキュリティ対策の実効的推進に資することを目的として、制御システム開発者を対象とする「制御システムセキュリティワークショップ 2009」、ユーザ企業、政府機関も含めた啓発プログラム「制御システムセキュリティカンファレンス 2009」を、それぞれ 2 月 18 日、19 日に開催することとしました。これに向けて、この分野の米国におけるオピニオン・リーダーであるデジタルボンド社の創立者であるデール・ピーターソン氏をはじめ、米国国土安全保障制御システムセキュリティプログラム局長のショーン・マクガーク氏、アイダホ国立研究所マーティ・エドワーズ氏らの来日講演をアレンジするとともに、制御システムにおけるセキュリティ関連情報を開発者間で共有するコミュニティとして、国内の関係団体と連携しつつ、「制御システム開発者セキュリティ情報共有タスクフォース」を立ち上げ、継続的に情報共有を中心とする活動をしていく体制構築を進めました。

― トピック 2 ―

C/C++セキュアコーディングセミナー　大手メーカー個別セミナーや連続セミナーを実施、受講者がのべ 1000 名を超える

従来のプログラミング教育は、仕様を満たし保守の容易なプログラムをどのようにコーディングするかを主眼としたものでした。しかし 現在のようなネット時代の開発においては、攻撃に耐えうる堅固なプログラム作りへの十分な配慮が必要です。不用意なプログラミングの結果、予期せ

ぬ脆弱性を作り込む可能性があるからです。JPCERT/CC では、より安全なソフトウエア開発のためのセキュアコーディングセミナーを開催しています。本セミナーは、ソフトウエア開発者が、脆弱性によるリスクを把握し、安全なソフトウエア開発への投資の意義を理解するとともに、実践的なコーディング・スキルを身に付けられるように設計されています。特定のアプリケーションに限らず、 C/C++ 言語を使ったプログラム開発に携わる全ての方を対象としています。
経済産業省との共催による「トワイライトセミナー」は、2008 年 6 月より毎月開催し、同年 12 月の第 7 回（最終回）までの間に毎回ほぼ定員いっぱいの計 250 名の開発者に受講していただきました。ご好評にお応えして、1 月からはハーフデイキャンプとしてリニューアルし全 3 回の予定で追加実施を計画しています。

C/C++セキュアコーディング ハーフデイキャンプの詳細
http://www.jpcert.or.jp/event/half-day_Camp-program.html

他方、大手製品開発企業等からの依頼に基づき、個別企業向けのセキュアコーディングセミナーを数社に対して提供しました。本年 4 月から 12 月までの間に、累計で約 750 名に受講していただき、各社から高い評価をいただきました。

個別企業向けのセミナーに関するお問い合わせ先
C/C++ セキュアコーディングセミナー―事務局：secure-coding@jpcert.or.jp

― トピック 3 ―

脆弱性脅威分析用の情報を定型フォーマットで表現する「VRDA (ヴァーダ) フィード」の試行配信を開始

2008 年 10 月 31 日より、情報システムの利用者における適切な脆弱性対応のための意思決定を支援する目的で、「VRDA フィード」の試行配信を開始しました。「VRDA (Vulnerability Response Decision Assistance) フィード」とは、情報システムの利用者が脆弱性への対応について判断を行う際に必要となる脆弱性の脅威を把握するための情報を、それぞれの分析基準項目ごとに分析値としてとりまとめ、定型データフォーマットで表現して配信するものです。この VRDA フィードを活用することにより、脆弱性関連情報の収集・読解・脅威分析に関するコストの低減を図ることができます。
本来、 VRDA フィードは、脆弱性対応のための意志決定支援を行うシステムである「KENGINE」（試行運用中）のためのデータ配信システムとして準備されたものですが、KENGINE ユーザ以外の方にも、広く、有効に使っていただけるデータであると考え、一般に公開することといたしました。

脆弱性脅威分析用情報の定型データ配信「VRDA フィード」に関する詳細
http://www.jpcert.or.jp/vrdafeed/

脆弱性への対応意志決定支援を行うシステムである「KENGINE」とその実装仕様の基となる VRDA コンセプトに関する詳細
http://www.jpcert.or.jp/research/#VRDA

― トピック 4 ―

アジア太平洋地域における 14 の CSIRT （シーサート）が合同でサイバー演習を実施

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、2008 年 12 月、サイバー攻撃への即時対応能力を確認するサイバー演習を実施しました。本演習は、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各経済地域 CSIRT 間の連携の強化を目的とし、毎年実施しているものです。今回で 6 度目となる本演習は、拡大し続ける地下市場での盗用データの取引や不正なオンラインサービスを行うサイバー犯罪組織による大規模なサイバー攻撃を想定し、国境やタイムゾーンを跨ぐ攻撃に対する迅速な対応技術及び意思決定能力の向上を目標に、9 時間に渡る、5 つのタイムゾーンを横断しての演習となりました。今回の演習には、アジア太平洋地域の 13 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、スリランカ、タイ、台湾、ベトナム）から 14 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 プレスリリース
APCERT Nailed Down Online Underground Economy in the Annual Regional Drill Exercise 2008
http://www.apcert.org/documents/pdf/APCERT-drill-2008.pdf

APCERT に関する詳細 http://www.apcert.org

― トピック 5 ―

「マルウェア対策研究人材育成ワークショップ 2008(MWS2008)」への参画

「マルウェア対策研究人材育成ワークショップ 2008(MWS 2008)」（共催：ボット対策プロジェクト（https://www.ccc.go.jp/）運営委員会及び情報処理学会）は、ボット対策プロジェクトで収集しているボット観測データを「研究用データセット」として活用し、以下の 3 つの分野に関する研究を行うワークショップです。

(1)検体解析技術の研究
(2)感染手法の検知ならびに解析技術の研究

(3)ボットの活動傾向把握技術の研究

MWS 2008 は、今年度が第 1 回目の実施で、コンピュータセキュリティシンポジウム 2008(CSS 2008)との併催という形式で実施されました。

JPCERT/CC は、MWS 2008 の実行委員として、プログラムの作成や運営に携わった他、ボット対策プロジェクトに関する活動報告の中で、「プログラム解析グループ」としての活動状況およびボットの傾向等に関する発表を行いました。

マルウェア対策研究人材育成ワークショップ は、本年も開催される予定であり、この取り組みにより、ボットやマルウェアに関する専門的な知識を持つ研究者/実務者の育成が促進され、対策技術の高度化につながることが期待されています。

マルウェア対策研究人材育成ワークショップ 2008(MWS 2008)の詳細
http://css2008.la.coocan.jp/mws2008/

【 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を通じて次のような情報提供を行いました。

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ました。

発行件数：7 件　http://www.jpcert.or.jp/at/

2008-12-18　Microsoft Internet Explorer の脆弱性 (MS08-078) に関する注意喚起(公開)
2008-12-10　2008 年 12 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)
2008-11-12　2008 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)
2008-11-05　Adobe Acrobat 及び Adobe Reader の脆弱性に関する注意喚起(公開)
2008-11-04　TCP 445 番ポートへのスキャン増加に関する注意喚起(公開)
2008-10-24　Microsoft Server サービスの脆弱性 (MS08-067) に関する注意喚起(公開)
2008-10-15　2008 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)

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)に発行しました。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掲載しています。

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 60 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。

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、セミナー資料を提供しました。

(1) 「技術メモ ― 安全な Web ブラウザの使い方 」

現在の Web を取り巻く環境に潜む脅威は、過去に比べて、量的に増しているばかりでなく、質的にも、ウイルスやワームなどに、フィッシングなどの新しいタイプの脅威も加わって多様性を増してきています。またブラウザの多機能化やコンテンツの多様化に伴い、攻撃手法や攻撃対象も進化しています。さらに Web で提供される情報サービスが増えてきた結果、データの破壊などのいわゆるコンピュータ上での被害にとどまらず、個人・企業情報の盗難

や流出、金銭被害や信用の毀損といった大きなダメージを伴う事故も増加の一途をたどっています。 インターネット利用者を狙った大規模な攻撃・マルウェア感染は、Web ページに悪意のあるコードを仕掛ける等の手法による受動的な攻撃・感染が主流となっています。
そのような状況から、PC で Web ブラウザを用いる場合に、安全に、そして手軽に使うために利用者が守るべき注意点を解説した技術メモを公開しました。

・技術メモ ― 安全な Web ブラウザの使い方 (PDF:1.54MB) (PGP 署名)

(2) 制御システムセキュリティイベント(MOF 2008、PCSF 2008)講演資料

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いう事案も散見され始めています。

JPCERT/CC は、2008 年 8 月 26 日(火)～8 月 28 日(木)、米国カリフォルニアにおいて開催された The Process Control System Industry Conference(PCSF2008)においてパネラとして講演を行いました。その際の講演資料を改訂し公開しました。

・Vulnerability in Control System Handling and Disclosure Policy
(PDF:1.59 MB) (PGP 署名)

また国内では、2008 年 9 月 10 日(水)～9 月 12 日(金)、東京ビックサイトにおいて開催されたマニュファクチャリング オープン フォーラム 2008(MOF 2008)においてもパネラとして講演を行い、この際に用いた次の講演資料を公開しました。

・産業用イーサネットのイントラ接続の可能性と相互接続を考える ～制御系システムセキュリティとサイバーセキュリティ～ (PDF:6.74 MB) (PGP 署名)

(3) DNS キャッシュポイズニング勉強会講演資料

2008 年 7 月、DNS キャッシュポイズニングの脆弱性に対する攻撃方法の詳細が、海外のセキュリティ研究者により公開されました。DNS キャッシュサーバが遠隔の第三者による偽の DNS 情報で汚染されることにより、ドメイン名の解釈が不正となり本来の宛先への通信を横取りされるなど、深刻な問題が発生する可能性があります。
JPCERT/CC では、引き起こされる被害を最小限に抑えるため、サーバ管理者の方を対象に DNS の仕組みと本脆弱性の本質と対策手法の勉強会を開催し、その際の資料を公開しました。
・DNSキャッシュポイズニングの脆弱性について (PDF: 5.52MB)(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 10 月 1 日から 2008 年 12 月 31 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」といいます。）に関する届出は 562 件でした。実際に届出を受けたメール及び FAX の数は、延べ 917 通（*1）で、インシデントの件数を IP アドレス別に集計すると 642 アドレスになります。

*1:同一サイトのインシデント情報が異なる届出者の方から届けられるため、届出件数とメール及び FAX の数が異なっています。

上記のうち、JPCERT/CC が国内外の関連するサイトに通知連絡した件数は 264 件です。この「通知連絡」とは、連絡仲介の依頼を含むインシデントの届出に基づいて、フィッシングサイトが設置されているサイトや、改ざんにより JavaScript や iframe が埋め込まれているサイト、ウイルス等のマルウェアが設置されたサイト、マルウェアに感染した後に別のマルウェアを取得する為にアクセスする先のサイト、「scan」のアクセス元等の管理者及び関係協力組織に対し、調査対応依頼の連絡を行ったものです。JPCERT/CC では、これらコーディネーション活動を行うことで、当該サイトのインシデントの認知と解決、インシデントによる被害拡大の抑止を行っています。

I.インシデントの傾向と分析

前四半期に引き続き、国内のサイトを装ったフィッシングサイトの届出を多数受領しています。JPCERT/CC では国内外のフィッシングサイトが設置されているサイトの管理者に対して、「フィッシングサイト公開の停止」を目的とする調査対応依頼を行っています。オンラインサービスを利用する際は、個人情報を入力する前に、入力するサイトが正規のサイトであるかを確認することを推奨します。

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

また、SQL インジェクション攻撃が増加しています。JPCERT/CC では、SQL インジェクション攻撃により改ざんされた Web サイトの管理者に対する調査対応依頼を行っています。システム管理者におかれては、公開しているサイトが改ざんされていないか定期的に確認するとともに、今一度 SQL インジェクション攻撃に対する対策が取られているかを確認されるよう推奨します。

独立行政法人 情報処理推進機構
「安全なウェブサイトの作り方　改訂第 3 版」
http://www.ipa.go.jp/security/vuln/websecurity.html

2008 年 10 月に公開された Microsoft Server サービスの脆弱性 (MS08-067) を攻撃するマルウェアが公開されているとの届出を受けました。また、この脆弱性を攻撃するマルウェアによる「scan」

の届出を受けました。JPCERT/CC では、マルウェアの公開サイトや「scan」のアクセス元に対して、マルウェア配布の停止、アクセスの停止等を目的とする調査対応依頼を行っています。昨今、脆弱性の情報が公開されて間もないうちに、その脆弱性に対する攻撃が発生し、脅威が増大しています。ベンダからセキュリティ更新プログラムが公開された場合は、速やかに適用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/2009/IR_Report090116.pdf

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の詳細：http://www.jpcert.or.jp/form/

§3. 早期警戒 －情報収集・分析－

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・拡大の抑止を目指しています。

今期は、7 件の注意喚起を発行いたしました。（注意喚起の一覧は、１章を参照）

I. 2008 年 Q4 (10-12 月) の動向について

2008 年 Q4(10-12 月)は、USB メモリを介して感染するウイルスや、偽セキュリティソフトの被害が増加しました。加えて、比較的多くのユーザが閲覧する著名なサイトが SQL インジェクション攻撃などにより改ざんされるというケースも増えています。一般的な正規のサイトであっても、攻撃者によって内容が改ざんされ、ユーザが当該 Web サイトを閲覧した時にウイルスに感染する危険性があります。常日頃、OS やソフトウエア、ウイルス対策ソフトなどを最新の状態に保つなど、少しでもウイルスに感染する危険性を減らしていくことが必要です。

また、インターネットでは利便性の高い様々なサービスが提供されていますが、これらサービスの不具合や不適切な設定などにより、個人情報が不用意に公開されたり、流出したりするケースが発生しています。サービス提供者、利用者ともに、個人情報や機密情報の取り扱いに十分に注意していく必要があります。

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」といいます。) 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。これらの観測情報は、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て作成しています。
今期は、Microsoft Windows の特定のバージョンに対し遠隔より攻撃可能な「MS08-067」の脆弱性が見つかり、修正プログラムが提供されました。JPCERT/CC では、11 月 4 日に注意喚起を発行し、修正プログラムの適用を呼びかけました。

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 10 月 1 日から 2008 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 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 10 月 1 日-12 月 31 日)

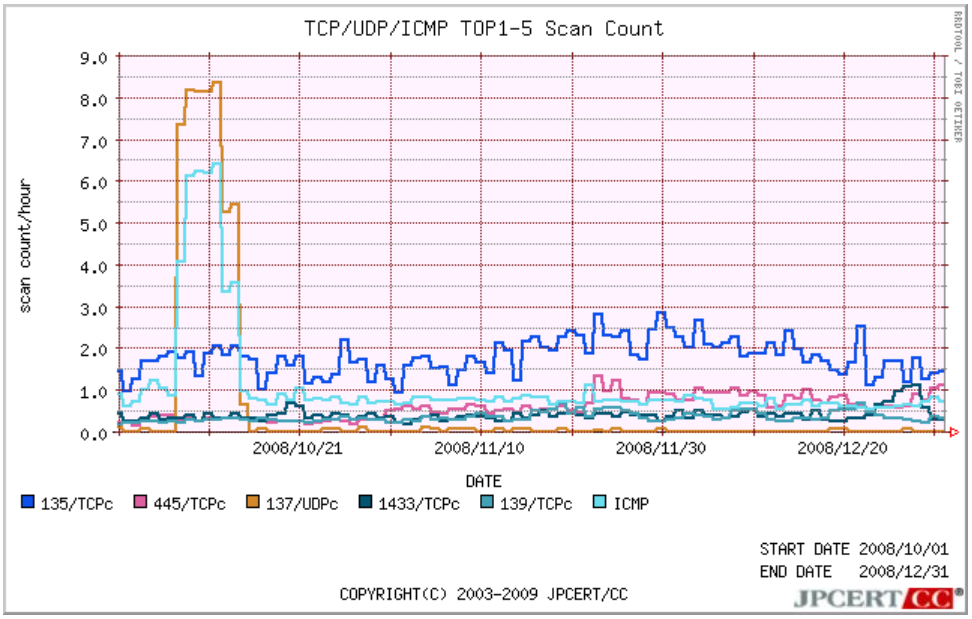

図 3-1: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2008 年 10 月 1 日-12 月 31 日)

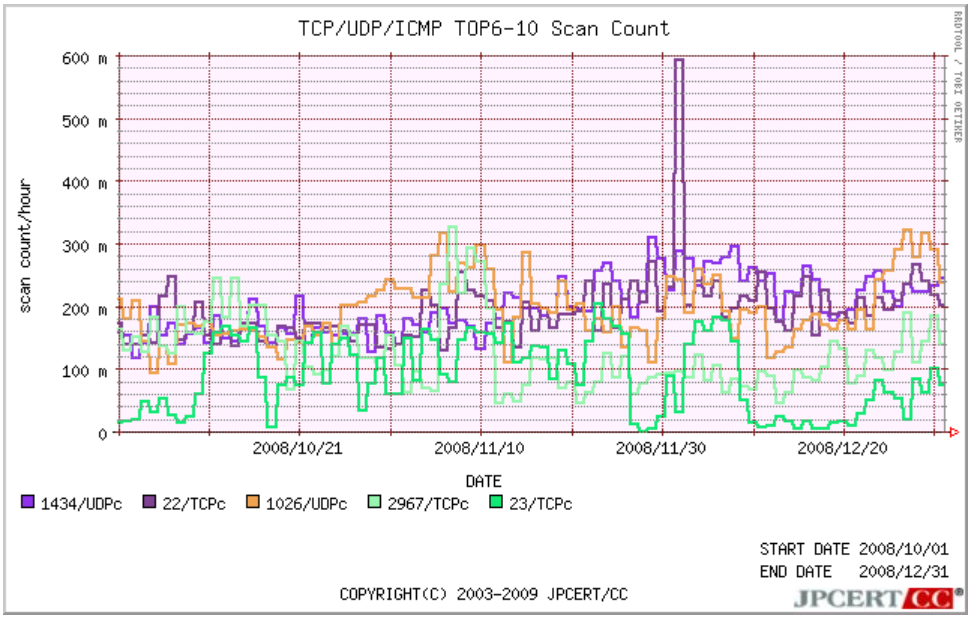

図 3-2: アクセス先ポート別グラフ top6-10

また、より長期間のスキャン推移を表すグラフとして、2008 年 1 月 1 日から 2008 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 3-3、図 3-4 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-2008 年 12 月 31 日)

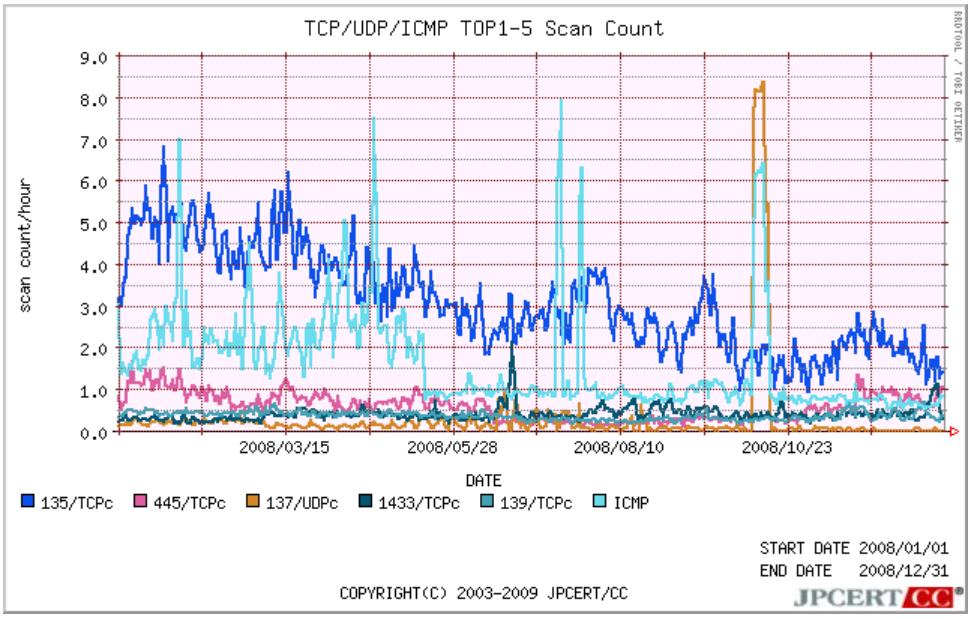

図 3-3: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2008 年 1 月 1 日-2008 年 12 月 31 日)

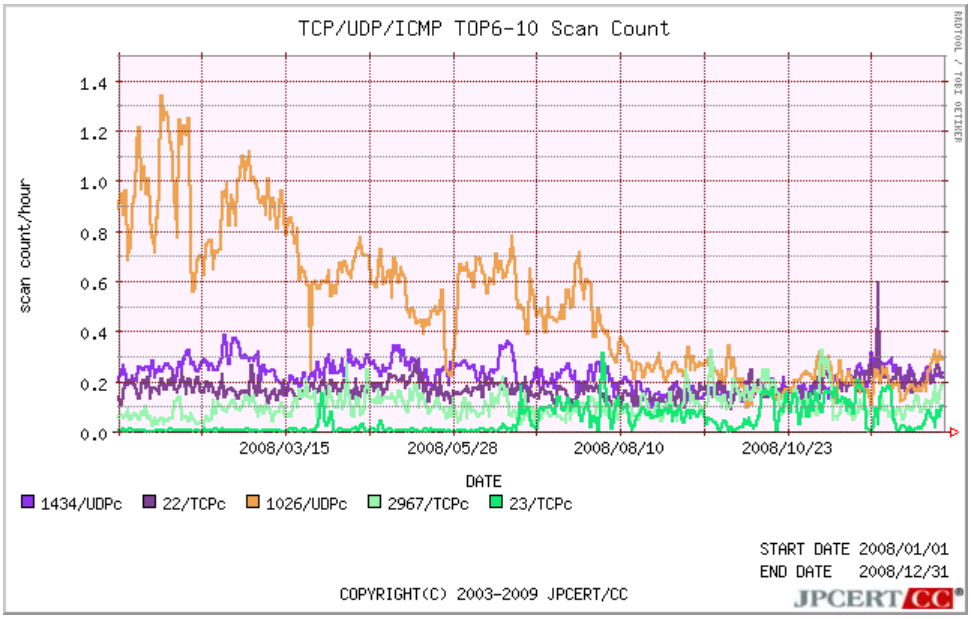

図 3-4: アクセス先ポート別グラフ top6-10

III.調査

1. 効果的な IT セキュリティ予防接種手法の調査(平成 20 年度)

JPCERT/CC では、平成 19 年度の調査結果をもとに、より大規模に IT セキュリティ予防接種を実施し、その効果を測定する調査を行っています。現在は、公募に応じてくださった企業にご協力いただき、実際に各社の従業員に対して IT セキュリティ予防接種を実施し、IT 予防接種の運用手法の検証を進めています。

2.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がないか調査を行いました。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、外部有識者を交えて対策の検討を行い、調査結果をまとめています。今後、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、サイバー演習の実施支援等を通じた CSIRT 構築支援及び脅威情報（早期警戒情報など）の共有等の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、CSIRT マテリアル等の資料提供、訪問による打ち合わせ、講師依頼対応などの

支援活動を行いました。
特に、今期は、組織等において実施されたサイバー演習の実施支援を通じて、CSIRT 機能として必要な既存のインシデントレスポンス能力等の検証及び改善活動に関わるなど、より具体的な施策に関与させていただく形で構築支援を行いました。

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(日本シーサート協議会：NCA)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 10 月 1 日から 2008 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 39 件 (総計 713 件) [図 5-1] 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。

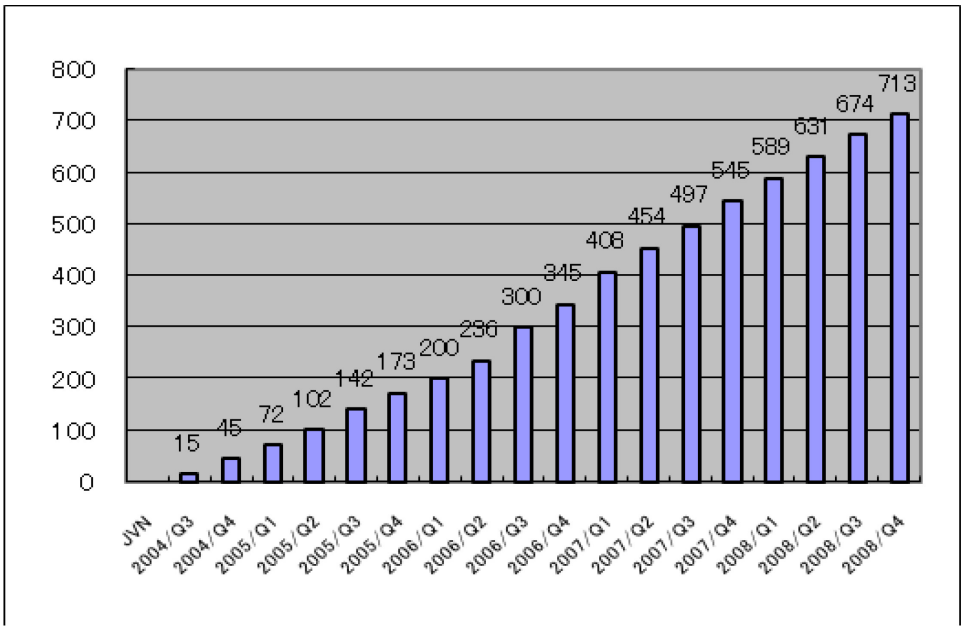

図 5-1: 累計 JVN 公表件数

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 22 件(累計 321 件) [図 5-2] でした。

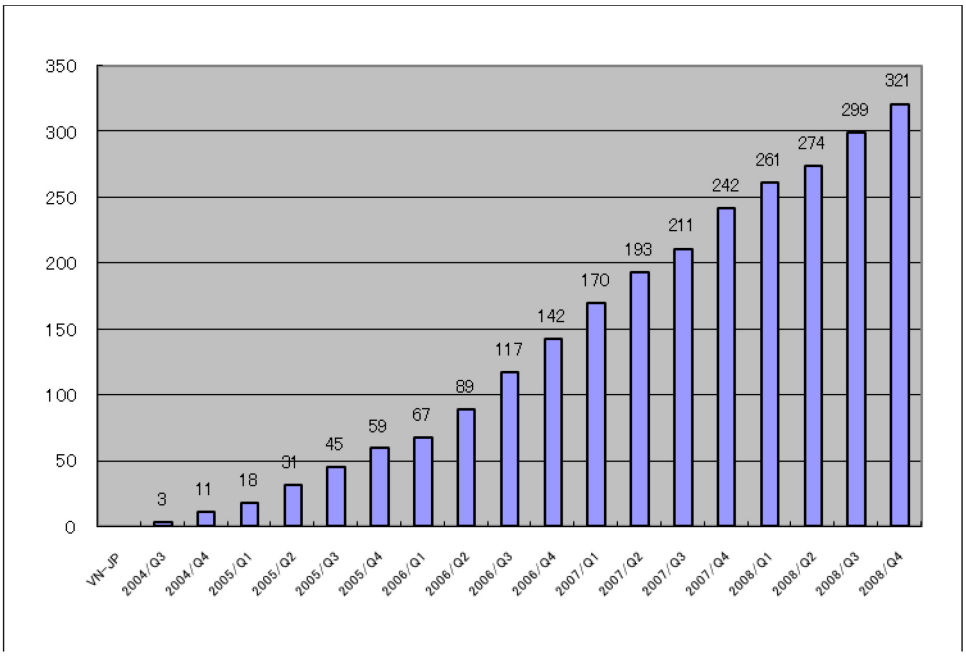

図 5-2: 累計 VN-JP 公表件数

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 16 件(累計 369 件) [図 5-3]、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 23 件) [図 5-4] でした。

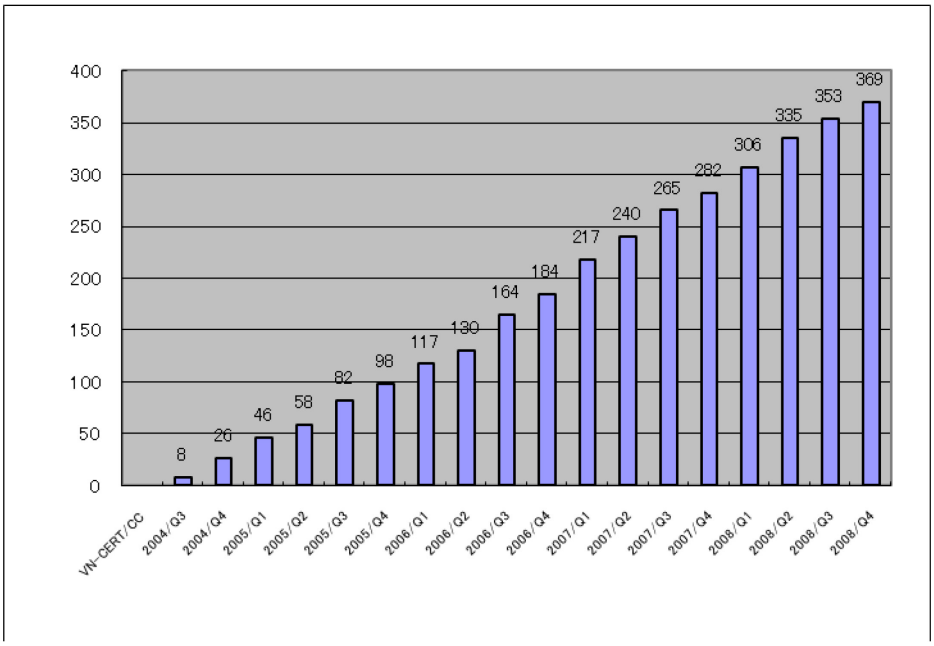

図 5-3: 累計 VN-CERT/CC 公表件数

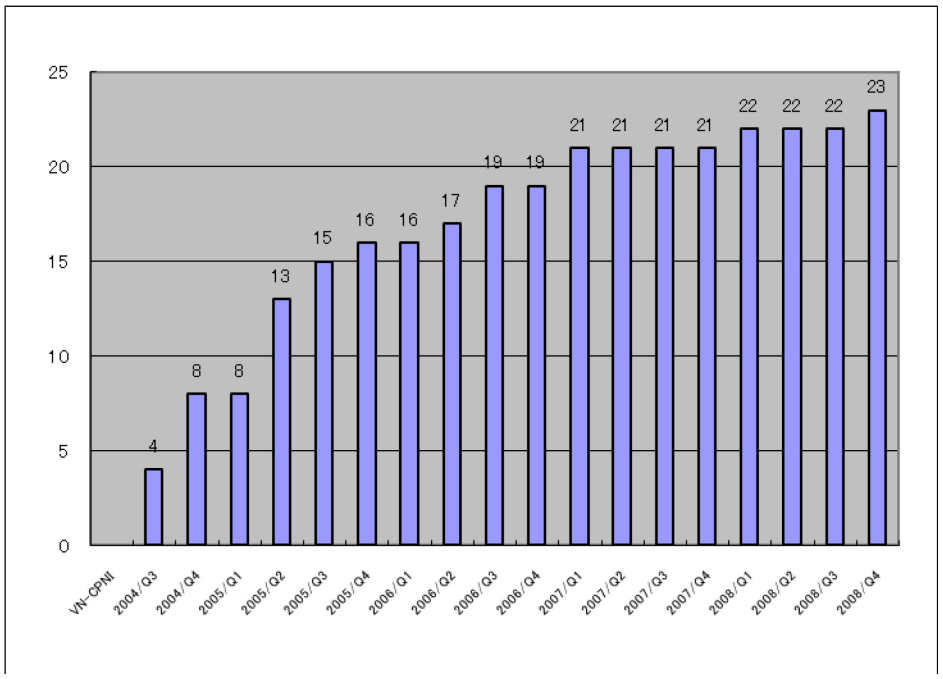

図 5-4: 累計 VN-CPNI 公表件数

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 12 月 31 日現在で 274 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。

登録等の詳細については、http://www.jpcert.or.jp/vh/agreement.pdf をご参照ください。

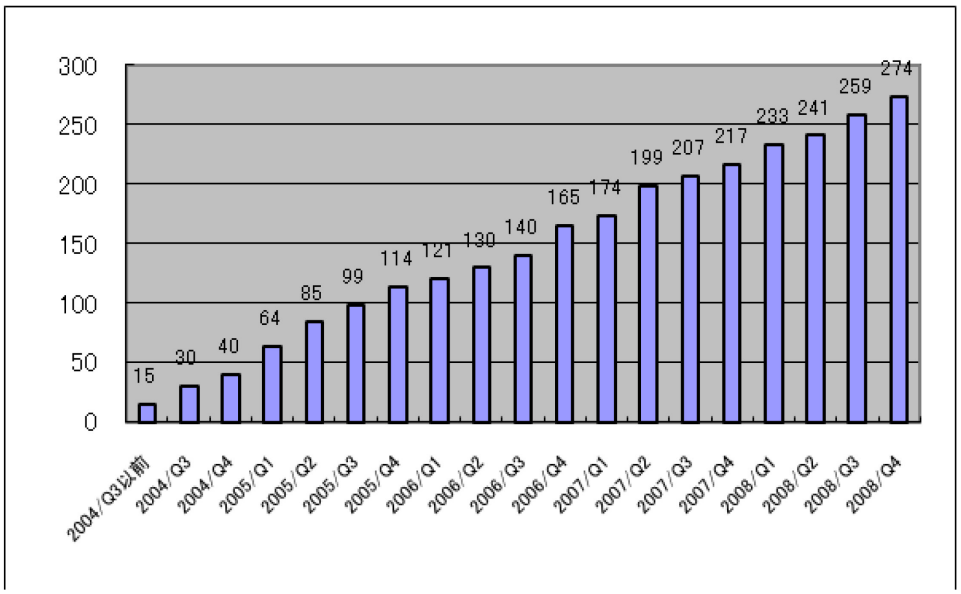

図 5-5: 累計製品開発者登録数

(3) C/C++ セキュアコーディング トワイライトセミナーの継続開催

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、問題を作り込まないプログラミングスキルを習得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ました。多くのプログラム開発関係者の方に参加いただき、2008 年 10 月 1 日<ファイル入出力> Part2、11 月 5 日<ファイル入出力> Part3、12 月 3 日 <書式指定文字列> を開催しました。各回ともに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、開発現場が抱える問題等についての意見交換を行ないました。

§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（月次）及び平成 19 年度の活動報告の公開

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 Web 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 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/200810/0810monthly.html
2008 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/200808/0811monthly.html

§7. 国際連携活動関連

I. 海外連携強化等

アジア太平洋地域における CSIRT 構築支援活動や講演、トレーニングを行い、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を図っています。

(1) CamCERT 構築支援活動　2008 年 9 月 25 日-10 月 24 日 / 11 月 10-21 日 / 12 月 16 日-

カンボジアのナショナル CSIRT である CamCERT に対して、ICT 管理能力の向上や、カンボジア国内および各国とのインシデント対応等の連携強化を目的とした CSIRT 構築支援活動を行いました。

(2) スリランカにおける情報セキュリティ啓発セミナー Cyber Security Week 参加

2008 年 10 月 28-31 日

スリランカのナショナル CSIRT である SLCERT が主催した、スリランカ国内でほぼ初めての試みとなる情報セキュリティ啓発セミナーに参加し、スリランカの政府関係者および IT 関連事業者等に対して、インシデント情報分析に関するワークショップおよびインシデント対応に関する講演を行いました。

(3) バングラデシュにおける情報セキュリティ啓発セミナー

Conference /Workshop on Information Security 参加　2008 年 11 月 4-6 日

バングラデシュを代表する CSIRT である BDCERT が主催した、バングラデシュ国内で初めての大規模な情報セキュリティ啓発セミナーに参加し、バングラデシュ政府関係者および IT 関連事業者等に対して、CSIRT の活動と必要性に関する講演およびインシデント対応に関する技術的なハンズオントレーニングを行いました。

(4) ベトナムにおける情報セキュリティ啓発セミナーおよび CSIRT 構築に関するトレーナー研修 Vietnam Information Security Day / Train The Trainer (T3) 参加　2008 年 11 月 26-27 日
ベトナムのナショナル CSIRT である VNCERT が主催したイベントに参加し、VNCERT 職員およびベトナム IT 関連事業者に対して、組織における脆弱性マネジメントに関する講演、および組織内 CSIRT の活動、必要性、構築法に関するトレーニングを行いました。

(5) アジア太平洋地域の CSIRT と日本の CSIRT の合同サイバー演習　2008 年 12 月 4 日
APCERT（アジア太平洋コンピュータ緊急対応チーム）と合同で、サイバー攻撃への即時対応能力を確認するサイバー演習を実施しました。(トピック 5 参照)

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。
今期は、バングラデシュを代表する CSIRT である BDCERT の APCERT 加盟をスポンサーし、2008 年 12 月 18 日 BDCERT が APCERT に加盟しました。

III. 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。

IV. 第 21 回 FIRST Conference 京都
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ます。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、「国内開催委員会」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

プログラム、講演申込み、参加申込みなどの詳細：http://www.first.org/

§8. 講演活動一覧

(1)業務統括　伊藤　友里恵

「内部犯行インシデントと対策」

経営情報学会 言語派組織情報研究部会 /2008 年 10 月 4 日

(2)早期警戒グループ　リーダ　名和　利男

「企業内におけるインシデントレスポンス能力の実情とその強化策」

ネットワーク・セキュリティワークショップ in 越後湯沢 2008 年 10 月 9 日(木)

(3)業務統括　伊藤　友里恵

「APCERT Activity Updates - Awareness program Updates」

APEC-TEL38 Security Awareness Workshop /2008 年 10 月 14 日

(4)早期警戒グループ　リーダ　名和　利男

「大規模サイバー攻撃の現状」

警察政策学会　テロ・安保問題研究部会　2008 年 10 月 20 日(月)

(5)業務統括　伊藤　友里恵

「The Hidden Threats」

Cisco CIO Summit /2008 年 10 月 22 日

(6)早期警戒グループ　リーダ　名和　利男

「企業における情報セキュリティにかかるインシデントの実情と適切な対応プロセスについて」

サービスビジネス・コンソーシアム　2008 年 10 月 22 日(水)

(7)早期警戒グループ　グループマネージャ　鎌田　啓介

「SQL Injection, Phishing and other incident trends in Japan」

「Overview of Incident Handling 」

「Incident Analysis (semi hands on demo)」

「Overview of Traffic Monitoring」

「Traffic Monitoring Analysis (semi　hands on demo)」

Cyber Security Week /2008 年 10 月 28 日-31 日

(8)常務理事　早貸　淳子

「Recent Trend of Information Security Threats and the Situation of Countermeasures」

2008　Korea-Japan Joint Seminar “On the Information Security at U-Services in the Ubiquitous Society”/2008 年 10 月 29 日

(9)業務統括　伊藤　友里恵

「CERT Presentation」

Conference / Workshop on Information Security /2008 年 11 月 4 日

(10)早期警戒グループ　グループマネージャ　鎌田　啓介

「Incident Handling」

「Incident Analysis」

「PGP Key Signing」

「Information Gathering」

「Network Monitoring」

「Security Tools」

Conference / Workshop on Information Security /2008 年 11 月 4 日-6 日

(11)早期警戒グループ　リーダ　名和　利男

「EC 事業者に必要なセキュリティ対策」

EC ネットワーク「インターネット取引詐欺トラブル講習会」/2008 年 11 月 6 日

(12)業務統括　伊藤　友里恵

「JPCERT and Industry initiatives on Control System Security」

日米 CIP フォーラム /2008 年 11 月 18 日

(13)業務統括　伊藤　友里恵

「Vulnerability Management Best Practices」

Vietnam Information Security Day /2008 年 11 月 26 日-27 日

(14)早期警戒グループ リーダ　林　永熙

「Train The Trainer (T3) CSIRT Training Course」

Train The Trainer (T3) /2008 年 11 月 27 日

(15)Chris Horsley

「Train The Trainer (T3) CSIRT Training Course」

Train The Trainer (T3) /2008 年 11 月 27 日

(16)理事　宮地　利雄

「2008 年の脆弱性　傾向と今後の課題～コーディネーションの立場から～」

Internet Week 2008 /2008 年 11 月 27 日

(17)早期警戒グループ　小宮山　功一朗

「標的型攻撃対策：IT セキュリティ予防接種」

Internet Week 2008 /2008 年 11 月 28 日

(18) 早期警戒グループ　グループマネージャ　鎌田　敬介

「インシデントと脆弱性対応　最新動向と CSIRT 構築」

慶応義塾大学 SFC 講義 /2008 年 12 月 4 日

(19)早期警戒グループ　小宮山　功一朗

パネルディスカッション　標的型攻撃の現状と対策　～有効な対策はあるのか～

「標的型攻撃対策：IT セキュリティ予防接種」

Security Day 2008 /2008 年 12 月 16 日

(20)理事　真鍋　敬士

パネルディスカッション　変化を続けるマルウェアとどう闘うか　～僕らの苦悩と模索～

「変化を続けるマルウェアとどう闘うか　～僕らの苦悩と模索～」

SecurityDay 2008 /2008 年 12 月 16 日

(21)早期警戒グループ　グループマネージャ　鎌田　敬介

「インシデントと脆弱性対応　最新動向と CSIRT 構築」

千葉大学理学部数学情報数理学科講義/2008 年 12 月 18 日

(22)情報流通対策グループ　戸田 洋三

「インシデントと脆弱性対応　最新動向と CSIRT 構築」

千葉大学理学部数学情報数理学科講義/2008 年 12 月 18 日

§9. 掲載記事一覧

(1)早期警戒グループ　小宮山　功一朗

「フィッシング詐欺の被害状況と警戒すべき新手法　事業者とエンドユーザがとるべき対策は？」

IA japan Review Vol.8/No.3 /2008 年 12 月

(2)早期警戒グループ　グループマネージャ　鎌田　敬介

「キーロガー」による脅威と対策」

NISC 重要インフラニュースレター 評価版 第 10 号/2008 年 11 月 5 日

(3)早期警戒グループ　グループマネージャ　鎌田　敬介

「海外 CSIRT とのインシデント対応連携について」

NISC 重要インフラニュースレター 第 1 号/2008 年 12 月 17 日

§10. 開催セミナー一覧

(1) Security Day 2008

近年インターネットは、さまざまな社会経済活動の中で広く利用されるようになりその依存性が高まる一方で、インターネットを通じたコンピュータセキュリティインシデントが頻発し、ますます増大する傾向にある。これら脅威は社会的なリスクであり、それらを低減させるため、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共催 5 社が、ユーザ、運用、管理といった立場の方を対象に、参加者とともに考え議論、問題提起をするセミナーを開催しました。

- ・主催　　日本インターネットプロバイダ協会、日本ネットワークセキュリティ協会、日本クロストラスト株式会社、Telecom-ISAC-Japan
  JPCERT コーディネーションセンター
- ・開催時期　2008 年 12 月 16 日
- ・集客人数　80 名

■インシデントの対応依頼、情報のご提供は■

☐ 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/