JPCERT-PR-2009-0002

JPCERT/CC 活動概要［ 2009 年 1 月 1 日 ～ 2009 年 3 月 31 日 ］

2009-04-07 発行

【 活動概要トピックス 】

—トピック　1—
制御システムセキュリティ関連講演会の開催とタスクフォースの発足

JPCERT/CC は、関心が高まりつつある「制御システムのセキュリティ」をテーマに、制御系システム開発関係者を招いて 2 月 18 日にワークショップを、さらに 19 日には広くユーザ企業も対象にしたカンファレンスを開催しました。

これらのイベントでは、国内外から招いた識者により制御系システムにおける情報セキュリティ上の脅威とその対策の重要性が紹介され、この問題の現状と今後の課題について、開発者とセキュリティ担当者との間で認識を共有することができました。

ワークショップでは、参加した開発関係者有志による継続的な情報共有を目的とした「制御システムベンダセキュリティ情報共有タスクフォース」を発足させることが確認されました。現在、このタスクフォースを安全な制御系システム構築のための情報共有の基盤とすべく、JPCERT/CC が事務局となって、本格運用に向けた準備を行なっています。

—トピック　2—
SQL インジェクション攻撃により改ざんされたサイトの増加

2008 年 12 月末から再び、SQL インジェクション攻撃により改ざんされたサイトの報告が増加しました。報告件数にして、前四半期の 2 倍になっています。JPCERT/CC では、報告を受けたサイトを実際に確認し、改ざんやマルウェアが確認できたものについて、当該サイトへの連絡・調整を行っています。

SQL インジェクション攻撃による被害は、攻撃されたサイトだけに留まるものではなく、改ざんされたサイトを閲覧したユーザにも影響を与える可能性があります。また、一時的に改ざんされた部分を修正したとしても、根本的な SQL インジェクション対策を行っていない場合、再度改ざんされてしまう場合があります。自らが管理しているサイトに関し、対策が漏れているものがないか、定期的に確認の徹底を図っていただくことを推奨します。

SQL インジェクションの対策については
http://www.jpcert.or.jp/at/2008/at080005.txt

―トピック　3―

キーロガー機能を持つマルウェアによる被害拡散防止

キーロガー機能を持ったマルウェアは、感染した PC のキー入力からパスワードや ID のような個人情報等の情報を収集し、その情報は攻撃者のサーバに蓄えられます。JPCERT/CC では、このような不正に取得された情報について、海外のセキュリティ関連組織から継続的に提供を受けています。

この情報の中には、金融機関や ISP のサービス利用に関する情報等が含まれていることがあります。そのような場合には、提供を受けた情報の中から金銭被害等の実害につながる可能性がある情報を抽出し、関係する企業や関係組織との間で情報共有を行います。たとえば、2008 年度の統計では、35 組織に対し、件数で 105 件、アカウント数で数千 ID に上る情報の共有を行いました。共有先の企業等においては、それぞれのポリシーに従い、被害の事前防止やユーザへの注意喚起などへの利用・参照をご検討いただいています。

―トピック　4―

C/C++ セキュアコーディング・ハーフデイキャンプ・セミナーを開催

より多くの製品開発者の方々に、ソフトウエアの脆弱性が作りこまれる根本的な原因や、C/C++ 言語で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、「C/C++ セキュアコーディング・ハーフデイキャンプ・セミナー」を開催しました。本セミナーは、2008 年中に実施して参加者からの反響が大きかった「C/C++ セキュアコーディングトワイライトセミナー」をほぼ同じ内容で再構成したものです。

前回の「トワイライトセミナー」では、より多くの方々にセキュアコーディングの波及効果を広げるため、全 7 回（2 時間×7）にセッションを分散させて実施しましたが、後半セッションにもリピーターが集中し、多くの方にセミナーに参加できないご迷惑をおかけしてしまいました。この反省を踏まえて今回のセミナーは、全 3 回（4.5 時間×3）の構成で実施しました。

日程とテーマは、以下のとおりです。

2009 年 1 月 29 日　第 1 回 ＜文字列・整数＞
2009 年 2 月 26 日　第 2 回 ＜ファイル入出力 part1, part2, part3＞
2009 年 3 月 26 日　第 3 回 ＜動的メモリ管理・書式指定文字列＞

前回、今回ともに「単なる知識習得に留まらず、セキュリティ意識の向上、セキュアな製品開発へのモチベーション向上に繋がった。」といった意見が寄せられています。また、社内勉強会や個別企業への出張セミナーなどの実施の要望もお受けしました。今後は、これらの活動を通じて得

られた開発現場での課題などを抽出し、引き続き、ソフトウエアのセキュリティ品質の底上げを支援していく予定です。

―トピック　5―
効果的な IT セキュリティ予防接種手法に関する調査

JPCERT/CC では、2008 年 4 月から、15 社以上の企業にご協力いただき、「IT セキュリティ予防接種」を実施しました。このプロジェクトは、標的型攻撃メール対策の一手法としての「IT セキュリティ予防接種」の効果測定と、より効率的な実施の方法等の調査を目的として実施したものです。

本調査は、製造業、金融業、地方自治体など多岐にわたる企業・組織のご協力のもとに行われました。人数にして延べ 2,600 名に対して 2 度（インターバル 2 週間）の IT セキュリティ予防接種を実施し、無記名のアンケートとメールの開封率によって効果などを測定しました。

「IT セキュリティ予防接種」は、標的型攻撃メール対策を目的として、社員が不審なメールの添付ファイルを開かないようにしたり、誤って開いてしまった場合に社内で適切な連絡を行えるようにしたりするための訓練であり、対象者に不審メールを模した無害なメールを送り、受信者が適切な取り扱いが行えるかを試すものです。

結果として、対象企業の全体において不審メールの開封率が 15%ほど下がるといった効果が得られましたが、JCERT/CC では、開封率の低下だけでなく、対象者のセキュリティ意識の向上に着目し、より効果的な「予防接種」方法の確立を目指しています。

―トピック　6―
アジア太平洋地域 4 か国とインシデントドリルを実施

JPCERT/CC は、国際間連携強化のため、さまざまな取り組みを行っていますが、2008 年度においては、中でも、アジア太平洋地域各国の CSIRT 立ち上げと運用支援に力を入れて取り組みました。

この活動の一環として、2009 年 2 月 4 日から 12 日までの期間、財団法人 海外技術者研修協会（AOTS）の主催の「インシデント対応技術トレーニング」に協力しました。この研修は、インドネシア、フィリピン、ベトナム、カンボジア 4 か国の CSIRT や企業のセキュリティ対応担当者、計 18 名を日本に招き、ハンズオン形式でインシデント対応技術のトレーニングを行うものです。

JPCERT/CC は、トレーニングプログラムの内容を検討し、講師を担当しました。また、脆弱性情報分析、マルウェア分析、インシデント高度分析など、このトレーニングで得た知識・経験が実際に活用できるかどうかを確認する目的で、4 か国合同で国際サイバーインシデントに対処する

ドリル（演習）を実施しました。

―トピック　7―
APCERT 年次会合の開催

2009 年 3 月 3 日から 5 日にかけて、台湾の高雄市においてアジア太平洋地域の CSIRT の集まりである APCERT の年次会合が開催されました。各地域におけるインシデント対応事例の紹介や、調査・研究活動の紹介、各 CSIRT 間での交流活動等が行われました。

このような会合を通じて各国の情報やスキルの共有が促進されることにより、国際間でのインシデント対応が必要となる事例に、より円滑に対応できるようになっていきます。
本年の会合の特徴として、アジア太平洋地域においても、制御システムに関するインシデント対応への関心の高まっていることが確認できました。

APCERT Annual Conference 2009 の詳細は
http://apcert2009.cert.org.tw/

―トピック　8―
重要インフラ情報セキュリティフォーラム 2009 を開催

JPCERT/CC は、「情報セキュリティの日」の関連行事として、独立行政法人情報処理推進機構(IPA)との共催により、2009 年 2 月 19 日に「重要インフラ情報セキュリティフォーラム 2009」を開催しました。

本フォーラムは、重要インフラ事業者(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、物流等の事業に係わる方）及び重要インフラ事業者にシステムを提供するベンダ等を主な対象として、情報セキュリティ上の課題や対策等に関する講演を中心に実施したもので、約 500 名にご参加いただきました。

午前のセッションでは、内閣官房情報セキュリティセンターの担当参事官による「重要インフラの情報セキュリティ対策に係る第２次行動計画」に関する講演と、「重要インフラにおけるヒューマンエラーと情報セキュリティ」をテーマとするパネルディスカッションが行われました。

午後のセッションは２つのトラックに分かれ、「ヒューマンマネジメントトラック」では「新型インフルエンザ対策」、「IT 予防接種による組織の防御力強化」等、事業マネジメントの観点から IT セキュリティに携わる方々に有用なテーマの講演を、「専門技術トラック」においては、「重要インフラがかかえる潜在型攻撃によるリスク」、「制御システムセキュリティの課題と対策」等、重要インフラ事業者のシステム管理者や重要インフラ事業者向けのシステム提供を行っているベン

ダ等にとって有用な技術的論点に関するテーマの講演、パネルディスカッションを実施し、活発な意見交換が行われました。

講演資料の詳細は
http://www.jpcert.or.jp/present/

【 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：8 件　http://www.jpcert.or.jp/at/

2009-03-19　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起（更新）
2009-03-12　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起（更新）
2009-03-11　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起（公開）
2009-03-11　2009 年 3 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）
2009-02-25　Adobe Flash Player の脆弱性に関する注意喚起（公開）
2009-02-11　2009 年 2 月 Microsoft セキュリティ情報（緊急 2 件含）に関する注意喚起（公開）
2009-02-05　[続報]TCP 445 番ポートへのスキャン増加に関する注意喚起
2009-01-14　2009 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のうち重要と判断した抜粋情報をレポートにまとめ、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、情報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：12 件　http://www.jpcert.or.jp/wr/

JPCERT/CC レポート内で扱った情報セキュリティ関連情報の項目数は、合計 62 件、「今週のひとくちメモ」のコーナーで紹介した情報は 12 件でした。

III. 資料公開

各分野の情報セキュリティに関する調査・研究の報告書や論文、セミナー資料を公開しました。

(1)「技術メモ ― クリックジャッキング対策 ～X-FRAME-OPTIONS について～ 」

クリックジャッキングは、Robert Hansen 氏、Jeremiah Grossman 氏が報告した Web 利用者を標的とした攻撃手法です。2008 年 9 月 27 日に OWASP NYC AppSec 2008 カンファレン

スにおいて詳細が発表される予定でしたが、ベンダからの要請により直前にキャンセルされ、そのことが IT 関連のマスコミで大きく取り上げられました。

両氏の発表とその後のセキュリティ研究者等の調査により、主要な Web ブラウザすべてがこの問題を抱えることが明らかになったものの、原因が Web ブラウザの動作する仕組みに関わる根本的な欠陥に起因するため、容易に修正できないとされていました。

その後、マイクロソフト社の Microsoft Internet Explorer 8（以降、IE8）にてクリックジャッキングの解決を目的とした X-FRAME-OPTIONS と呼ばれる機能の追加が行われました。

IE8 に追加されたクリックジャッキング対策機能は、Web サイト側がこの機能に対応することではじめて効果が期待されるものであり、単に利用者が IE8 を導入しただけでは対策となりえません。Web サイトの制作者及び運営者は、利用者に不測の損害を与えないよう、この新機能を正しく理解し、適切な設定を行うことが必要です。

JPCERT/CC では、Web サイト制作者及び運営者を対象に、クリックジャッキング攻撃の概要とその対策の一つである X-FRAME-OPTIONS の概要、記述方法、設定値による挙動の違いについて解説した技術メモを公開しました。

技術メモ ― クリックジャッキング対策 ～X-FRAME-OPTIONS について～
http://www.jpcert.or.jp/ed/2009/ed090001.pdf

(2) 重要インフラ情報セキュリティフォーラム 2009 講演資料

2009 年 2 月 20 日に開催した本フォーラムの講演資料を公開しました。

講演資料の詳細
http://www.jpcert.or.jp/present/

§2. 早期警戒 ーインシデントハンドリングー

JPCERT/CC が 2009 年 1 月 1 日から 2009 年 3 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 564 件、延べでは 946 通（*1)、IP アドレス別の集計では 684 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ことがあるため、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調査対応依頼をした件数は 388 件です。この「通知連絡」とは、連絡調整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ため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、調査対応依頼を行うものです。JPCERT/CC は、このようなコーディネーション活動により、当該サイトにおける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に貢献しています。

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_Report090407.pdf

I. インシデントの傾向と分析

国内のサイトを装ったフィッシングサイトの届出が、前四半期の 10 件から、今期は 25 件に増えています。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の停止」のための調査対応依頼を行っています。また、SQL インジェクション攻撃の届出も増加しています。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 サイトの管理者と、改ざんされたコンテンツにより誘導される先の 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。

フィッシングや、SQL インジェクションなど Web サイト、Web アプリケーションに関連する多数のインシデントが定常的に報告されるようになっています。正規サイトであっても改ざんされている可能性がありますので、一般ユーザにおかれても、これらの脅威から自身を守るために、①OS や Web ブラウザを最新に保つ、②ウイルス対策ソフトを導入し、ウイルス定義ファイルを常に最新の状態に保つ、といった基本的な対策の励行をお勧めします。詳細は以下の資料をご覧ください。

技術メモ － 安全な Web ブラウザの使い方
http://www.jpcert.or.jp/ed/2008/ed080002_1104.pdf

システム管理者におかれては、管理しているサイトが改ざんされていないか、使用しているソフトウエアなどに脆弱性がないかなどについて定期的に確認してください。

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

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し（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。）、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、6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）

【 2009年Q1(1-3月)の動向について】
2009年Q1(1-3月)は、2008年Q4 に引き続き USB メモリ等を介して感染を広げるConficker ワーム（別称：Downadup、DOWNAD 等）の被害が発生しています。海外の事例と比べて国内での被害事例は比較的少ないようですが、国内でも企業や組織の内部ネットワークに侵入され、多数のコンピュータが感染した事例も報告されていますので、十分な注意が必要です。
JPCERT/CC では、Conficker ワームの感染時の特徴である445/tcpポートへのアクセスをインターネット定点観測システム（ISDAS）にて監視し、国内での感染動向を注視しています。

Conficker ワーム関連注意喚起：
2008年10月24日

Microsoft Server サービスの脆弱性（MS08-067）に関する注意喚起
http://www.jpcert.or.jp/at/2008/at080018.txt

2008年11月4日
TCP 445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/at080019.txt

2009年2月5日
[続報]TCP 445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/2009/at090002.txt

昨今のコンピュータウイルスは、非常に短い間隔で自身を更新していくため、ウイルス定義ファイルによって検知するタイプのウイルス対策ソフトでは検知・駆除ができないケースがあり、システムの復旧は困難を極めます。不審な点があるメールを開かない、他人のUSBメモリなどのリムーバブルストレージを不用意に接続しないなどの対策を検討してください。

(参考)
JVNTA09-020A
Microsoft Windows 自動実行機能の無効化における注意点
http://jvn.jp/cert/JVNTA09-020A/

§4. 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、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しています。また、このシステム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 ページにおいて公開しています。 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。

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

2009 年 1 月 1 日から 2009 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 4-1、4-2 に示します。

- アクセス先ポート別グラフ top1-5（2009 年 1 月 1 日-3 月 31 日）

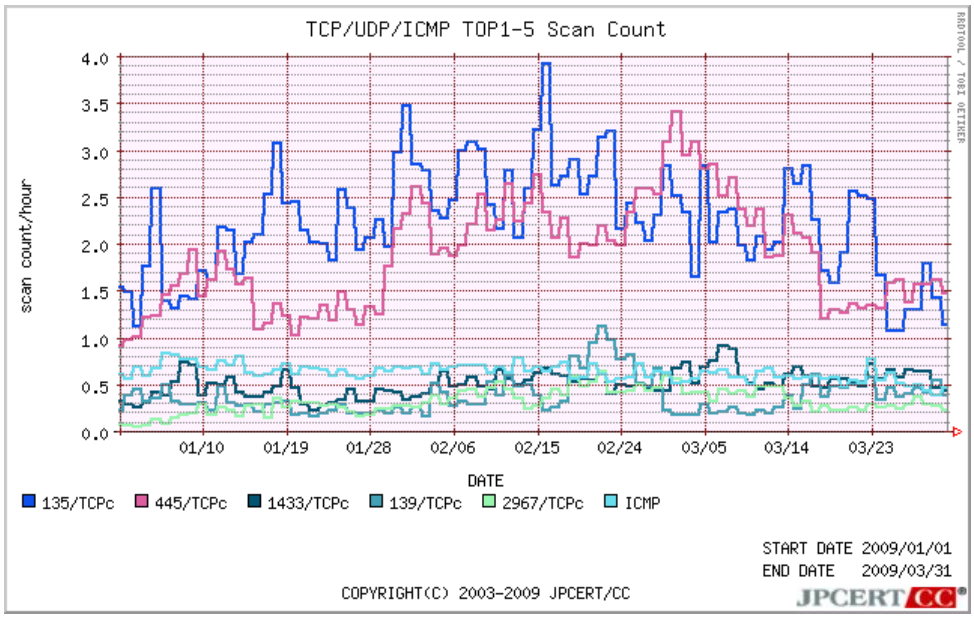

図 4-1: アクセス先ポート別グラフ top1-5(2009 年 1 月 1 日-3 月 31 日)

- アクセス先ポート別グラフ top6-10（2009 年 1 月 1 日-3 月 31 日）

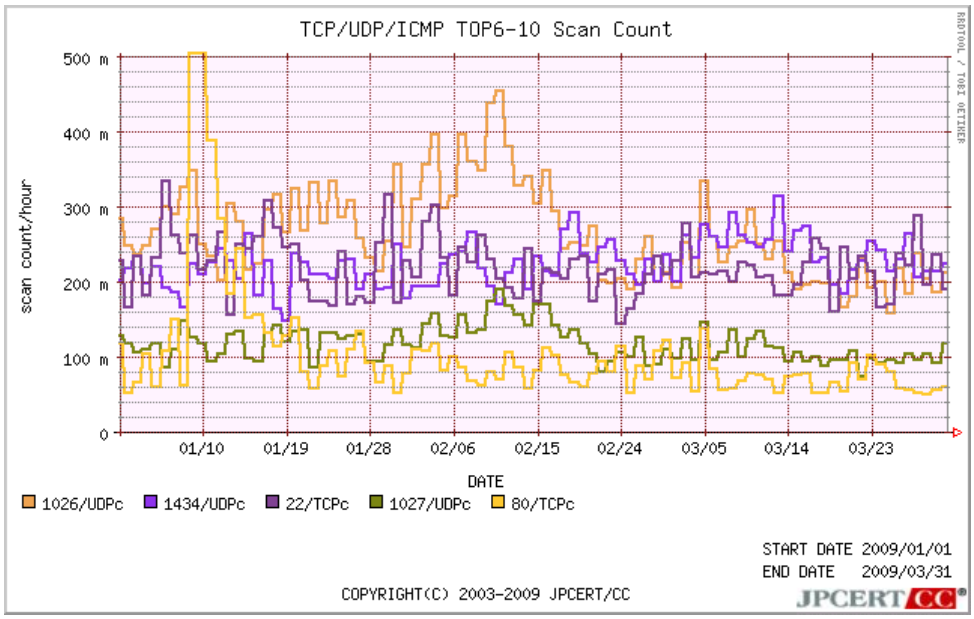

図 4-2: アクセス先ポート別グラフ top6-10(2009 年 1 月 1 日-3 月 31 日)

また、より長期間のスキャン推移を御覧いただくため、2008 年 4 月 1 日から 2009 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 4-3、図 4-4 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-2009 年 3 月 31 日）

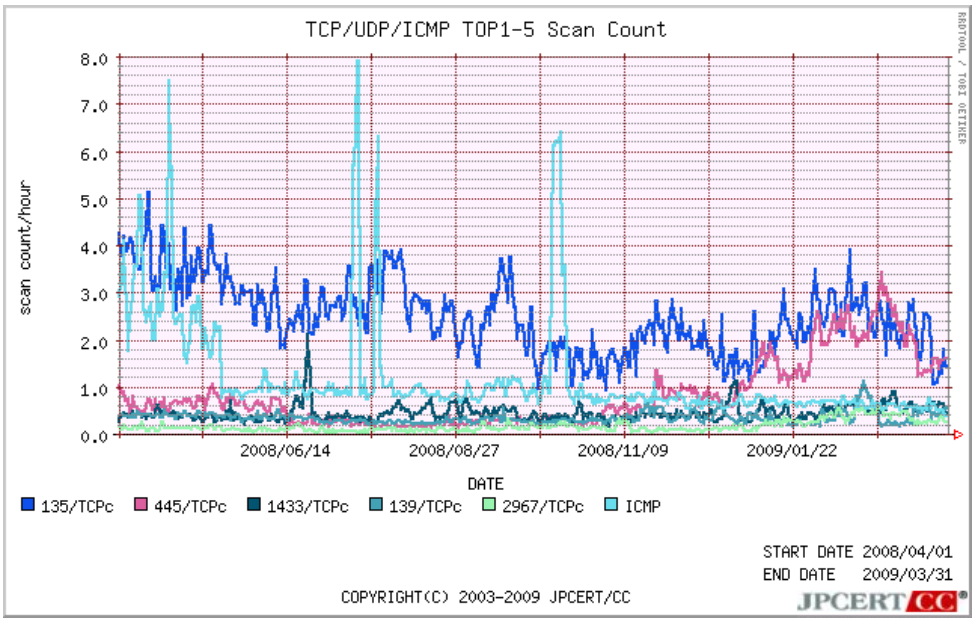

図 4-3: アクセス先ポート別グラフ top1-5(2008 年 4 月 1 日-2009 年 3 月 31 日)

- アクセス先ポート別グラフ top6-10（2008 年 4 月 1 日-2009 年 3 月 31 日）

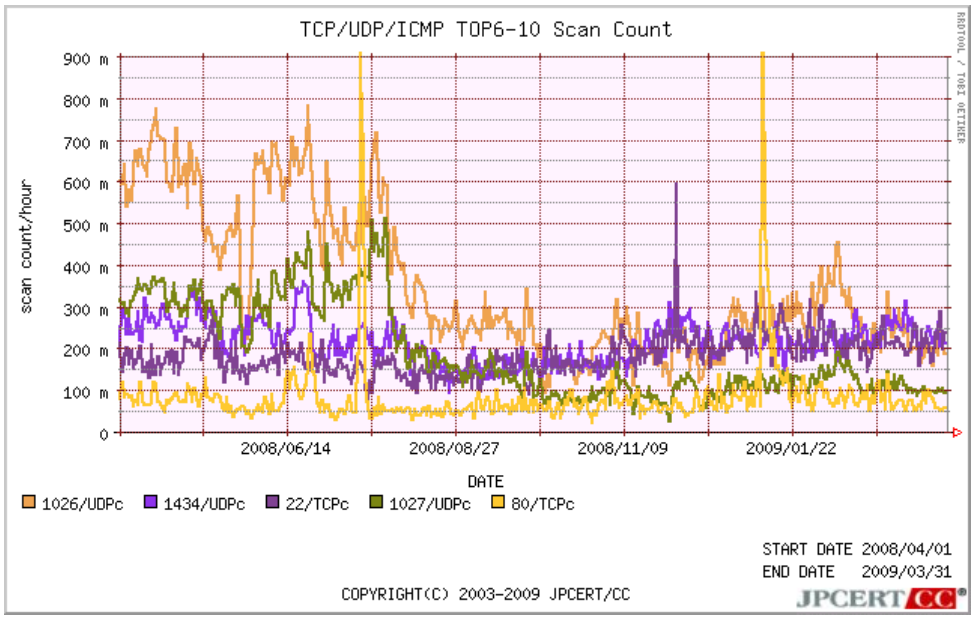

図 4-4: アクセス先ポート別グラフ top6-10(2008 年 4 月 1 日-2009 年 3 月 31 日)

引き続き Scan 検知数の上位を占めている、Windows マシンを対象とした Scan が、今期は一段と増加しました。2008 年 10 月下旬に、Microsoft Windows の特定のバージョンに対し遠隔より攻撃可能な脆弱性が見つかり、「MS08-067」として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。その後も、この脆弱性が修正されていない端末を探すためか、Port445/TCP に対する活発な scan が続いていたところ、2 月の上旬に Scan が急増したため、再度注意喚起を行いました。

OS やアプリケーションについて脆弱性がないバージョンを使用しているか、Firewall や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。

[続報]TCP 445 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/2009/at090002.txt

II. 調査

(1) 効果的な IT セキュリティ予防接種手法の調査(2008 年度版)

JPCERT/CC では、2007 年度に実施した「標的型攻撃対策手法に関する調査報告」を基に、2008 年度においては、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いました。また、どのような事前教育や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もあわせて実施いたしました。延べ 15 社 2600 名を超える方々に実際に IT セキュリティ予防接種を受けていただき、アンケートへのご回答をいただきました。この結果、IT セキュリティ接種には不審なメールの開封率を下げるという直接的な効果だけでなく、ユーザの意識を高め、事故に強い組織を作るという効果があることが分かりました。調査結果の詳細及び IT セキュリティ予防接種の実施手法については、2009 年 5 月に報告書を公開する予定です。

(2) IPv6 脆弱性に関する調査

JPCERT/CC では、2007 年度に実施した IPv6 プロトコルと IPv6 に付随したサービスに関する脆弱性の調査において見つかった問題点について、2008 年度において、外部有識者を交えて対策の検討を行い、検討結果をまとめました。この結果については、IPv6 関連の製品を開発している企業・団体の技術者を対象とする説明会において、IPv6 製品を開発する場合の注意点と合わせて説明し、参考資料として配付しました。この説明会は、より多くの関係者にご参加いただけるよう、複数回開催し、約 45 社 110 名の方々にご参加いただきました。

§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」に指定されています。

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

2009 年 1 月 1 日から 2009 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 31 件 (総計 744 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。

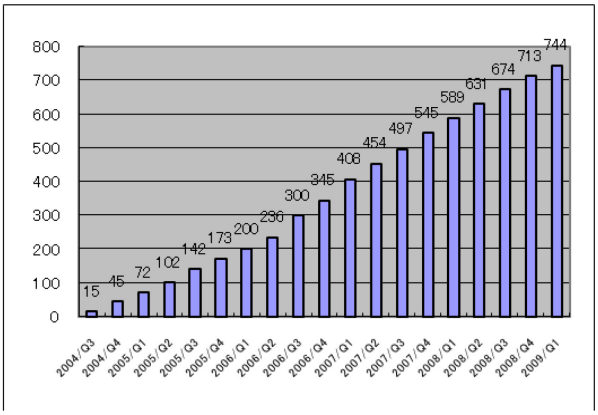

図 5-1: 累計 JVN 公表件数

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 16 件(累計 337 件)［図 5-2］でした。

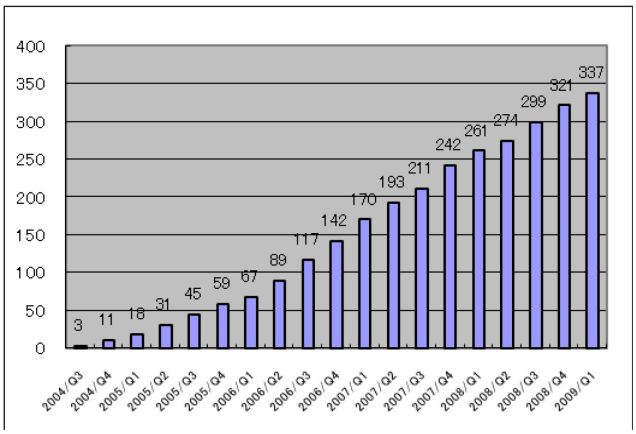

図 5-2: 累計 VN-JP 公表件数

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 15 件(累計 384 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 0 件(累計 23 件)［図 5-4］でした。

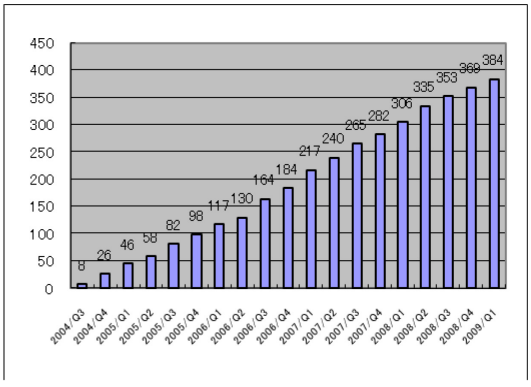

図 5-3: 累計 VN-CERT/CC 公表件数

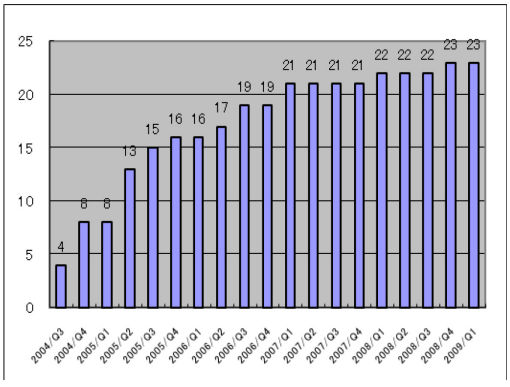

図 5-4: 累計 VN-CPNI 公表件数

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等、脆弱性関連情報の受領から公開までの情報を随時共有する枠組みを運用し、脆弱性関連情報の適正な流通のための国際連携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、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 におい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」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、連絡先情報の整備のため、製品開発者の皆様に連絡先情報の登録をお願いしています。2009 年 3 月 31

日現在、 283 社［図 5-5］の製品開発者の皆様にご登録をいただいています。
JPCERT/CC 製品開発者リストへ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。

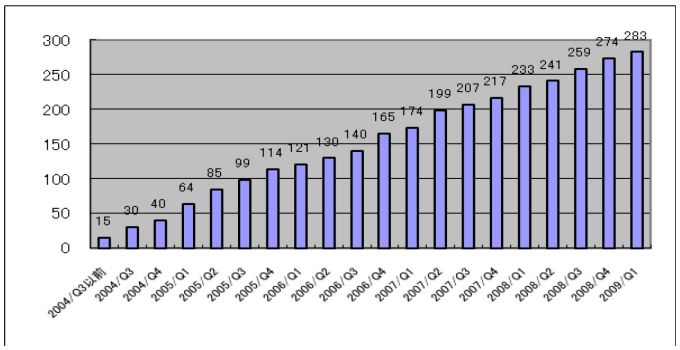

図 5-5: 累計製品開発者登録数

(3) 制御システムセキュリティ関連講演会の開催とタスクフォースの発足

2009 年 2 月 18 日、国内外の識者を招いて制御系システム開発関係者を対象としたワークショップを開催しました。制御システムのセキュリティレベルの向上にあたっては、制御システム関連製品の開発や制御システムの構築にあたる技術者においてセキュリティ脅威および対策に関する情報と認識を共有し、効果的な対策を進めることが重要です。このワークショップでは、攻撃手法のデモを交えた制御系システムにおける問題の提起や対策の検討に関するプレゼンテーションが行なわれました。また、参加した開発関係者有志による継続的な情報共有を目的とした「制御システムベンダセキュリティ情報共有タスクフォース」(以下「タスクフォース」といいます。) への参加の呼びかけを行ないました。

ワークショップは好評のうちに終了し、タスクフォースについても多くの製品開発者の皆様の参加表明を受ける事ができ、現在、その本格運用に向けて準備を行なっています。

また翌 2 月 19 日には、ユーザ企業も含めた制御系システム関係者を対象としたセキュリティカンファレンスを開催しました。制御系システムにおけるセキュリティレベルの向上には、課題を効果的に解決するため、製品ベンダ、構築技術者、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重要です。このカンファレンスでは、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を目的とした国内外の識者によるプレゼンテーションが行なわれ、参加した多くの制御系システム関係者の間で、最新の脅威情報の共有と解決に向けての提案、セキュリティ対策活動の必要性の認識の共有が行われました。

(4) C/C++ セキュアコーディング ハーフデイキャンプ セミナーの開催

より多くの製品開発者の方々に、ソフトウェアの脆弱性が作りこまれる根本的な原因や、C/C++

言語で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、「C/C++ セキュアコーディング・ハーフデイキャンプ・セミナー」を開催しました。本セミナーは、2008 年 6 月 4 日から 12 月 3 日にに実施して参加者からの反響が大きかった「C/C++ セキュアコーディングトワイライトセミナー」をほぼ同じ内容で再構成したものです。

前回の「トワイライトセミナー」では、より多くの方々にセキュアコーディングの波及効果を広げるため、全 7 回（2 時間×7）にセッションを分散させて実施しましたが、後半セッションにもリピーターが集中し、多くの方にセミナーに参加できないご迷惑をおかけしてしまいました。この反省を踏まえて今回のセミナーは、全 3 回（4.5 時間×3）に再構成し、集中度を上げた形で実施しました。

日程とテーマは、以下のとおりです。

2009 年 1 月 29 日　第 1 回 ＜文字列・整数＞
2009 年 2 月 26 日　第 2 回 ＜ファイル入出力 part1, part2, part3＞
2009 年 3 月 26 日　第 3 回 ＜動的メモリ管理・書式指定文字列＞

各回とも、多くのプログラム開発者の方々にご参加いただき、セキュアコーディング作法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。

また、トワイライトセミナー、ハーフデイキャンプのいずれにおいても、「単なる知識習得に留まらず、セキュリティ意識の向上、セキュアな製品開発へのモチベーション向上に繋がった。」といった意見が寄せられています。さらに、社内勉強会や個別企業への出張セミナーなどの実施の要望もお受けしました。今後は、これらの活動を通じて得られた開発現場での課題などを抽出し、引き続き、ソフトウェアのセキュリティ品質の底上げを支援していく予定です。

(5)セキュアコーディングセミナー資料の公開

「C/C++ セキュアコーディングトワイライトセミナー」及び「C/C++ セキュアコーディング・ハーフデイキャンプ・セミナー」で使用した講義資料(全 7 モジュール)については、一般公開に先立ち、JPCERT/CC 製品開発者リストに登録いただいている製品開発者向けの公開を行っています。一般公開は、2009 年度以降、順次進める予定です。

(6)安全なソフトウエア開発を行うための「企業向け C/C++ セキュアコーディング個別セミナー」の実施

JPCERT/CC では、C/C++ で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の企業向け個別セミナーを提供しており、今四半期は 2 社に対して実施しました。

セミナーごとにコース内容を調整し、各企業の開発現場のニーズに沿った形式にアレンジした上で、実際に製品開発に携わる皆様にセキュアコーディングを学んでいただける場として提供しています。個別セミナー開催のご相談は、seminar-secure@jpcert.or.jp までご連絡ください。

(7)セキュアコーディングに関するその他の啓発活動

3 月 12 日午後に開催された AsiaBSDCon 2009 の中でチュートリアルセッションとしてセキュアコーディングセミナーを企画し、講師を務めました。

BSD に関するカンファレンスの一部として設けられたチュートリアルであったこともあり，BSD 環境を利用している学生や、業務として開発に直接は関わっているわけではないがボランティアでソフトウエアを開発していらっしゃると見受けられる方々が多く参加されており、職業的プログラマの参加が多いトワイライトセミナーや個別セミナーの参加者層とは異なる層にセキュア・コーディングの考え方を普及することができました。

セキュアコーディングノススメ(日本語)
http://2009.asiabsdcon.org/timetable.ja.html#T2A

(8)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、2009 年 3 月 23 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。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、ベンダ連絡担当者との意見交換を行ないました。

また、早期警戒グループによる「IPv6 脆弱性に関する調査」結果の説明会に登録製品開発者を招き、今後、重要な技術のひとつとなると考えられる IPv6 のセキュリティ上の問題を示し、安全な製品開発のための啓発活動を行いました。

(9) The CERT C Secure Coding Standards の日本語版の公開

JPCERT/CC は、「The CERT C Secure Coding Standards(https://www.securecoding.cert.org/) 」の翻訳を行い、その日本語版を作成しました。

C 言語による開発において品質の高いコーディングを実践しようとする場合、開発現場に実際に適用できるコーディングスタンダード(規約)が重要な意味を持ちます。コーディングスタンダードを活用することで、プログラマは、ひとりよがりに陥ることなく、開発プロジェクトや組織がその要求に従って定めたルールやガイドラインに沿ってコーディングすることが可能になり、レビューや保守を行う者にとっても理解しやすいプログラムが作り出されます。また、コーディングスタンダードはソースコードを監査するための指標として用いることもできます。

「CERT C セキュアコーディングスタンダード」は、CERT/CC が開発した、セキュアコーディングを C 言語で行うためのコーディングスタンダードです。必ず従わなければならないルール(Rule)と推奨事項(Recommendation)から構成されています。そのうちの約 90 のルールを、2009 年 4 月中に公開する予定です。

§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や、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。

【 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 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/

2009 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/200901/0901monthly.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 12 月 16 日-1 月 13 日)
JICA のプロジェクトを通じて、カンボジアのナショナル CSIRT である CamCERT に対して、CSIRT

構築支援活動を行いました。これは、CamCERT の 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ものです。

(2) ベトナムにおける情報セキュリティセミナー 参加 (2009 年 1 月 9 日)
ベトナムにおける情報セキュリティ関連調査プロジェクトの成果発表の場として開催された情報セキュリティセミナーに参加しました。ベトナムにおける情報セキュリティ事情を把握するとともに、CSIRT の活動と必要性および JPCERT/CC における 2008 年の案件事例の紹介に関する講演を行いました。

(3) GTISC/ICANN Global DNS Security, Stability, and Resiliency Symposium 参加 (2009 年 2 月 3 日-4 日)
ICANN とジョージア工科大学が共催したシンポジウムに参加し、DNS オペレーター間におけるインシデント対応ネットワークおよびテクニカルネットワークの構築について、FIRST その他の国際組織の取組みを共有しました。

(4) 第 7 回 アジア情報技術フォーラム (AFIT) 参加 (2009 年 2 月 19 日-20 日)
タイ国立電子コンピュータ技術センターおよび財団法人国際情報化協力センターが、タイにおける情報セキュリティ関連調査プロジェクトの成果発表の場として開催した AFIT (The 7th Asian Forum for Information Technology) に参加しました。タイにおける情報セキュリティ事情を把握するとともに、JPCERT/CC の活動に関する講演を行い、2008 年のセキュリティインシデントに対するパネルディスカッションに参加しました。

(5) APCERT AGM & Conference 2009 参加 (2009 年 3 月 3 日-5 日)
アジア太平洋地域の CSIRT の集まりである、APCERT (Asia Pacific Computer Emergency Response Team) の年次会合が台湾で開催され、2008 年の APCERT および各加盟 CSIRT の活動成果を共有するとともに、JPCERT/CC が主導して進めているアジア太平洋地域におけるインターネット観測データ共有システムの運用について発表を行いました。

(6) South African CSIRT Workshops 参加 (2009 年 3 月 22 日-23 日)
南アフリカの CSIRT 構築支援活動として、CSIR (Council for Scientific and Industrial Research) が主催したワークショップに参加し、CSIRT の活動と必要性、および国内関係組織とのインシデント対応等の連携に関する講演を行いました。

(7) 2009 Industrial Control Systems Joint Working Group Inaugural Symposium 参加 2009 年 3 月 25 日-27 日
米国国家安全保障省 (DHS) が主催した制御システムセキュリティカンファレンスに参加し、International パネルディスカッションにおいて、本分野の国際連携の課題について議論を行いました。

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。

2009 年 3 月 3 日-5 日 台湾にて APCERT 年次会合が開催されました。

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
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) 早期警戒グループ　グループマネージャ　鎌田　啓介
「Japanese incident case studies and role of organizational internal CSIRTs」
情報セキュリティセミナーハノイ /2009 年 1 月 9 日

(2) 業務統括　伊藤　友里恵
「The Hidden Threats」
2009 FIRST Symposium /2009 年 1 月 19 日-1 月 21 日

(3) 情報流通対策グループ　脆弱性アナリスト 久保　正樹
「脆弱性を作り込まない C、C++セキュアコーディングプラクティス」
制御システムセキュリティワークショップ 2009 / 2009 年 2 月 18 日

(4) 理事　宮地　利雄
「情報通信技術セキュリティの技術史と、制御システムの課題」
「パネル：課題とその具体的解決策について」
制御システムセキュリティカンファレンス 2009 / 2009 年 2 月 19 日

(5) 業務統括　伊藤　友里恵
「パネル：制御システムセキュリティ課題と対策」
重要インフラ情報セキュリティフォーラム 2009　/ 2009 年 2 月 19 日

(6) 早期警戒グループ　情報セキュリティアナリスト　小宮山　功一朗
「標的型メール攻撃対策 ～IT 予防接種による組織の防御力強化～」
重要インフラ情報セキュリティフォーラム 2009　/ 2009 年 2 月 19 日

(7) 早期警戒グループ　グループマネージャ　鎌田　啓介
「Information Security in Thailand」
「Organizational internal computer security incident responding structure:CSIRT」
第 7 回アジア情報技術フォーラム /2009 年 2 月 19 日

(8) チーフシステムアーキテクト　富樫　一哉
「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スタンダードの有効性評価」
SRA 技術シンポジウム　/2009 年 2 月 27 日

(9) 早期警戒グループ　グループマネージャ　鎌田　啓介
「Figure Skating Brawls go Online over the East Sea」
APCERT Annual Conference 2009　/2009 年 3 月 5 日

(10) 業務統括 伊藤　友里恵
「Control System Security」
APCERT Annual Conference 2009 /2009 年 3 月 5 日

(11) 情報流通対策グループ　情報セキュリティアナリスト 戸田　洋三
「セキュアコーディングノススメ（C/C++編）」
Asia BSD Con 2009　/2009 年 3 月 12 日

(12) 業務統括 伊藤　友里恵
「Japanese Approach to a national CSIRT：ISP's benefit from a national CSIRT and its services」
South African CSIRT Workshops　/2009 年 3 月 24 日,25 日

(13) 業務統括　伊藤　友里恵
「パネル：International Panel Discussion」
2009 Industrial Control Systems Joint Working Group InauguralSymposium
2009 年 3 月 25 日-27 日

§9. 掲載記事一覧

(1) JPCERT/CC 専門委員　名和　利男
「CSIRT 構築日誌 第 7 回サイバー演習で弱点をあぶり出す」
日経 BP 社日経コミュニケーション　/ 2009 年 2 月 9 日
http://itpro.nikkeibp.co.jp/article/COLUMN/20090203/324156/

(2) JPCERT/CC
「制御システムセキュリティ ワークショップ・カンファレンス実施概要」
NISC 重要インフラニュースレター 第 5 号/2009 年 3 月 4 日

(3) 情報流通対策グループ　情報セキュリティアナリスト 戸田　洋三
「新米セキュリティ担当者が行く！CSIRT 奮闘記」
日経 BP 社日経ネットワーク 4 月号　/2009 年 3 月 28 日

■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/