JPCERT CC®

JPCERT-PR-2010-0002

発行日 : 2010-04-08

JPCERT/CC 活動概要 [2010 年 1 月 1 日 ～ 2010 年 3 月 31 日]

【活動概要トピックス】

—トピック 1— Web サイト改ざん型の攻撃の報告は減少に転じたが、依然として高いレベルで発生—本四半期のインシデント報告の傾向

—トピック 2— オープン技術の浸透を受けて活発な議論—制御システムセキュリティカンファレンス 2010

—トピック 3— サイバー 演習・CSIRT 機能構築支援・セキュアコーディングセミナー—アジア地域での多角的連携活動

—トピック 4— フィッシングサイト URL 情報の提供や、啓発・教育コンテンツの拡充—フィッシング対策協議会事務局の運営

—トピック 1 —
Web サイト改ざん型の攻撃の報告は減少に転じたが、依然として高いレベルで発生—本四半期のインシデント報告の傾向

前四半期に続き、いわゆる Gumblar 攻撃とそれに類似する攻撃による Web サイトの改ざんに関する報告が数多く寄せられています。報告件数の推移をみると、本年 1 月をピークに減少傾向にあるものの、本四半期における報告件数は 809 件と依然として報告され続けています。また、いったん修正されたサイトが、再度改ざんされる事例も確認しており、対策が広く実施されたとは言い難い状況にあります。

JPCERT コーディネーションセンター（以下「JPCERT/CC」といいます。）では、いただいた報告やその分析結果、関係機関から提供された関連情報等を活用し、改ざんされたサイトを閲覧した利用者の PC から窃取された情報が送信される先の特定及び活動の停止に関する調整、改ざんされたサイトの運営者への連絡、利用者への注意喚起等の活動を行っています。

適切な対策の浸透と被害の拡大抑止のため、Web サイト改ざん型の攻撃に関連する情報をお持ちの方は、JPCERT/CC への情報提供に御協力いただけますようお願いいたします。

注意喚起 － FTP アカウント情報を盗むマルウエアに関する注意喚起
https://www.jpcert.or.jp/at/2010/at100005.txt

注意喚起 － Web サイト改ざん及びいわゆる Gumblar ウイルス感染拡大に関する注意喚起
https://www.jpcert.or.jp/at/2010/at100001.txt

―トピック 2 ―

オープン技術の浸透を受けて活発な議論―制御システムセキュリティカンファレンス 2010

2 月 9 日、経済産業省及び JPCERT/CC が主催する「制御システムセキュリティカンファレンス 2010」を都内にて開催しました。本カンファレンスは昨年からスタートしたもので、今回が第 2 回となります。昨年は、制御システムにおけるセキュリティ対策の必要性と重要性を業界内で共有することができ、コミュニティ活動やガイドラインの作成などの成果につなげることができました。第 2 回に当たる今回は、「ベンダの役割、ユーザの役割」をテーマとし、国際的な制御システムセキュリティ検討 WG（MPCSIE）メンバーによる講演、制御システムセキュリティ評価ツールのデモ、パネルディスカッションなど、より具体的な内容で開催しました。午後のパネルディスカッションでは、ユーザ、ベンダ、開発者、それぞれの立場からのパネラーによって、活発な議論と意見交換が行われ、会場からの質問からも関心の高まりが感じられました。

制御システムセキュリティカンファレンス 2010
https://www.jpcert.or.jp/ics/conference2010.html

制御システムセキュリティカンファレンス 2010 においての講演資料
https://www.jpcert.or.jp/present/index.html#ic

―トピック 3 ―

サイバー演習・CSIRT 機能構築支援・セキュアコーディングセミナー―アジア地域での多角的連携活動

財団法人海外技術者研修協会（AOTS）による「情報セキュリティ研修コース - CSIRT 体制強化 - 」（1 月 13 日～22 日）が実施されました。JPCERT/CC は、研修プログラムの作成と研修コースの講師を担当しました。この研修は、急速な IT 化が進むアジア・太平洋地域における、各国の CSIRT の機能構築と運営体制の強化を目的に、ASEAN 各国の政府機関、企業、コミュニティのセキュリティ専門家を日本に招き、インシデント対応の実践的な技術やノウハウを指導するものです。今回は、インドネシア、カンボジア、タイ、フィリピン、ベトナムの 5 カ国から 24 名の参加がありました。

また、1 月 28 日には、2005 年から毎年実施されている「APCERT 合同サイバー演習（APCERT Drill 2010）」に参加しました。本演習は、毎年 1 回、国境をまたいだインシデントに各国の CSIRT が連携して対応するための訓練として実施されているものです。今回は、アジア・太平洋地域の 14 の国及び経済地域から、過去最多となる 16 チームが参加して、オンライン取引の Web サイトに対するサービス停止や金銭窃取といった攻撃への対応やリカバリの演習が行われました。
さらに、2009 年の秋にタイ及びインドネシアで実施して好評を得た「C/C++セキュアコーディン

グセミナー」を、ベトナムの首都ハノイで 1 月に開催しました。ベトナムを含む東南アジア地域では、日本企業をはじめとする大手ソフトウェアベンダーのオフショア開発に対応するため、セキュアなソフトウエアの開発への関心が高まっており、他の国からも同様のセミナー実施の要請を受けているところです。

JPCERT/CC では、このような国際連携活動やナレッジの共有・普及啓発活動を通じ、引き続き、アジア・太平洋地域における情報セキュリティ対策に関する連携、協力体制の強化を支えていきたいと考えています。

APCERT knocks down Cyber Crimes with Financial Incentives in Drill Exercise 2010
http://www.apcert.org/documents/pdf/Drill2010_PressRelease.pdf

―トピック 4 ―
フィッシングサイト URL 情報の提供や、啓発・教育コンテンツの拡充―フィッシング対策協議会事務局の運営

JPCERT/CC では、2009 年度のフィッシング対策協議会（以下「協議会」といいます。）事務局の運営を受託し、協議会としてのフィッシングサイトに関する報告の受付や注意喚起の発行、関連する技術情報などの提供等の活動を行いました。協議会では、2010 年 2 月から、収集したフィッシングサイトの URL 情報を、JPCERT/CC を通じて、フィッシング対策のための製品やサービスを提供する会員企業に提供するなど、利用者のリスク低減につながる情報共有活動を新たに開始しました。

また、協議会として、米国 APWG の教育プログラム（「フクロウ先生のフィッシング警告ページ」）に参加し、フィッシングサイトであったページに日本語の警告が表示されるようにするとともに、ゲーム形式でフィッシング対策を学ぶことができる教育コンテンツ（「フィッシングフィル」）を協議会の Web サイトで公開するなど、一般利用者向けのフィッシング対策の普及、啓発活動を推進しました。

Yahoo! JAPAN、フィッシング対策協議会およびJPCERT/CCと連携し、「Yahoo!ツールバー」のフィッシング警告機能をさらに強化
https://www.jpcert.or.jp/press/2010/PR20100126_ap.pdf
「フクロウ先生のフィッシング警告ページ」
http://education.apwg.org/r/?forcelang=jp
フィッシング対策を学べるゲーム 「フィッシング フィル」
http://www.antiphishing.jp/phil/

JPCERT CC®

—活動概要—

目次

1. 早期警戒 7
1-1. インシデントハンドリング 7
1-1-1. インシデントの傾向と分析 7
1-1-1-1. Web ページの改ざんの届出件数増加 7
1-2. 情報収集・分析 8
1-2-1. 情報提供 8
1-2-2. 脅威の動向について 9
1-3. インターネット定点観測システム(ISDAS) 10
1-3-1. ポートスキャン概況 10
1-4. 日本シーサート協議会 (NCA) 事務局運営 12
2. 脆弱性関連情報流通促進活動 13
2-1. Japan Vulnerability Notes (JVN) において公開した脆弱性情報および対応状況 13
2-2. 海外 CSIRT との脆弱性情報流通協力体制の構築、国際的な活動 15
2-3. 日本国内の脆弱性情報流通体制の整備 15
2-3-1. 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 16
2-3-2. 日本国内製品開発者との連携 16
2-3-3. 製品開発者との定期ミーティングの実施 17
2-3-4. 「責任ある脆弱性情報開示」の国際標準化活動への参加 18
2-4. セキュアコーディング啓発活動 18
2-4-1. セキュアコーディングセミナー in ベトナム 18
2-4-2. C/C++ セキュアコーディングセミナー資料(2009 年度版)公開 19
2-4-3. ウェブマガジン連載 19
2-4-4. 「CERT C セキュアコーディングスタンダード」レコメンデーションを追加公開 19
2-5. 制御システムセキュリティにおける啓発活動 20
2-5-1. 制御システムセキュリティカンファレンス開催 20
2-5-2. 制御システムのサイバーセキュリティなど新たに３つの文書を公開 20
2-5-3. セキュリティ・アセスメント・ツールの調査 21
2-5-4. 制御システムベンダーセキュリティ情報共有タスクフォースへの情報発信 22
2-5-5. 制御システム関連学界活動 22
3. ボット対策事業 23
3-1. ボット対策事業の活動実績の公開 23
4. 国際連携活動関連 24
4-1. 海外 CSIRT 構築支援および運用支援活動 24

4-1-1. アジア太平洋地域における活動 24
4-1-2. その他地域における活動 24
4-2. 国際 CSIRT 間連携 25
4-2-1. アジア太平洋地域における活動 25
4-2-2. その他の地域における活動 27
4-3. APCERT 事務局運営 27
4-4. FIRST Steering Committee への参画 27
5. フィッシング対策協議会事務局の運営 28
5-1. フィッシング対策協議会の活動実績の公開 28
5-2. 情報収集と動向分析の強化 28
5-3. 一般ユーザからの問合せ業務改善 28
5-4. フィッシングサイトの URL を会員（対策サービス事業者）へ情報提供開始 29
6. 公開資料 33
6-1. 制御システムのサイバーセキュリティ：多層防御戦略 33
6-2. 人的セキュリティガイドライン 33
6-3. 推奨プラクティス：工業用制御システムにおけるサイバーセキュリティインシデント対応能力の開発 33
6-4. 電子メールソフトのセキュリティ設定について 33
6-5. 制御システムセキュリティカンファレンス 2010 講演資料 34
6-6. 重要インフラ情報セキュリティフォーラム 2010 講演資料 34
7. 講演活動一覧 34
8. 執筆・取材記事一覧 36
9. 開催セミナー一覧 37
10. 後援・協力一覧 38

本活動は、経済産業省より委託を受け、「平成２１年度コンピュータセキュリティ早期警戒体制の整備（不正アクセス行為等対策業務）」事業として実施したものです。
ただし、「2-4-3.**ウェブマガジン連載**」、「4-1-1-1. AOTS による**「情報セキュリティ研修コース –CSIRT 体制強化–」への協力**」、「4-1-2-1. ICT **国際協力セミナーにパネリストとして参加**」、「4-2-1-2.**台湾「情報セキュリティ防御能力の向上」**」、および「平成２１年度コンピュータセキュリティ早期警戒体制の整備（フィッシング対策協議会運営）」事業として経済産業省から受託して実施した「**5.フィッシング対策協議会事務局の運営**」に記載の活動については、この限りではありません。
また、「**6.講演活動一覧**」及び「**7.執筆・執筆記事一覧**」には、受託事業以外の自主活動に関する記載が一部含まれています。

1. 早期警戒

1-1. インシデントハンドリング

JPCERT/CC が本四半期に受け付けた報告のうち、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。）に関する報告は 2,488 件（Web フォーム、メール、FAX で報告を受けた延べ数は 3,498 通 *1)、インシデント対象の IP アドレス別の集計では 3,193 アドレスでした。報告の数が前四半期と比較して約 2 割増加しました。

*1:同一サイトに関するインシデント情報が、異なる報告者から報告されることがあるため、報告件数とメール及び FAX の延数に差異が発生しています。

JPCERT/CC が国内外の関連するサイトとの調整を行った件数は 1,005 件でした。前四半期と比較して約 7 割増加しています。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 が埋め込まれているサイト、ウイルス等のマルウエアが設置されたサイト、「scan」のアクセス元等の管理者および関係協力組織に対し、現状の調査と問題解決のための対応を中立的な調整機関の立場から依頼する活動が、ここでいう「調整」です。

JPCERT/CC は、国際的な連携の元でインシデント対応の調整を行う日本の窓口組織として、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。

JPCERT/CC インシデントハンドリング業務報告の詳細
https://www.jpcert.or.jp/pr/2010/IR_Report20100408.pdf

1-1-1. インシデントの傾向と分析

1-1-1-1. Web ページの改ざんの届出件数増加

システムへの不正侵入に関するインシデントは、809 件でした。前四半期の 372 件から大幅に増加しました。本四半期の報告のすべてが、Web サイトで公開しているファイルに不審な JavaScript が埋め込まれる改ざんに関するものでした。これらは、前四半期から報告が続いている改ざんと同様の事例です。

JPCERT/CC では、Web サイトの管理者に対して「改ざんの修正」の依頼を行うほか、改ざんされたサイトを閲覧した利用者の PC から窃取された情報が送信される先の特定及び活動の停止に関する調整を行っています。

なお、いったん修正されたサイトが、再度、改ざんされる事例をいくつか確認しています。改ざんへ対応に当たっては、挿入された不審なスクリプトを削除する等の表面的な修正だけではなく、改ざんを誘発した原因の追究とその除去が重要です。また、管理している Web ページが改ざんされていないか（閲覧者をマルウエア配布サイトに誘導する不審なスクリプトの挿入等の形跡がないか）定期的に確認してください。

改ざんサイトを発見した場合は、JPCERT/CC にご報告ください。JPCERT/CC では、攻撃方法の変化等により脅威の内容や有効な対策に変化が生じた場合には、随時、注意喚起等の情報発信を行います。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。

インシデントの報告方法の詳細
https://www.jpcert.or.jp/form/

インシデントの報告 （Web フォーム）
https://form.jpcert.or.jp/

1-2. 情報収集・分析

JPCERT/CC 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。これらの様々な脅威情報を多角的に分析し、必要に応じて脆弱性やウイルス検体の検証なども併せて行いながら、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等を対象とした「早期警戒情報」など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。

1-2-1. 情報提供

本四半期においては、JPCERT/CC のホームページ、RSS、約 24,000 名の登録者を擁する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。

1-2-1-1. 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：11 件　https://www.jpcert.or.jp/at/

2010-03-31　Microsoft Internet Explorer の脆弱性 (MS10-018) に関する注意喚起（公開）
2010-02-10　2010 年 2 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）
2010-02-03　FTP アカウント情報を盗むマルウエアに関する注意喚起 （公開）
2010-01-22　Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起 （更新）
2010-01-18　Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起 （公開）
2010-01-13　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 （公開）
2010-01-13　Adobe Reader 及び Acrobat の未修正の脆弱性に関する注意喚起 （更新）
2010-01-13　Web サイト改ざん及びいわゆる Gumblar ウイルス感染拡大に関する注意喚起（更新）
2010-01-13　2010 年 1 月 Microsoft セキュリティ情報（緊急 1 件）に関する注意喚起（公開）
2010-01-08　Web サイト改ざん及びいわゆる Gumblar ウイルス感染拡大に関する注意喚起（更新）
2010-01-07　Web サイト改ざん及びいわゆる Gumblar ウイルス感染拡大に関する注意喚起（公開）

1-2-1-2. Weekly Report

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情報の抜粋をレポートにまとめ、原則として毎週水曜日（週の第 3 営業日）に発行しています。レポートには、「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 59 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。

1-2-2. 脅威の動向について

前四半期に続き、いわゆる Gumblar ウイルスによる Web サイトの改ざんが見つかっています。セキュリティベンダやウイルス対策ソフトベンダなどの情報のウイルス情報や Web サイトの改ざん情報、JPCERT/CC への Web 改ざんに関するインシデント届出推移などによると、このタイプの攻撃は 2 月中旬まで増加傾向を示していましたが、2 月中旬以降一転減少傾向に入っています。しかしながら、JPCERT/CC へ報告される改ざんされた Web サイトに関する情報は、未だ毎週数百サイトと高止まりしていることから引き続き注意が必要です。
OS やアプリケーションについて最新のセキュリティアップデートの適用を励行するとともに、ウイルス対策ソフトの定義ファイルを最新に維持してください。

1-3. 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ポートスキャン情報を収集しています。これらの観測情報は、公開されてい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の脅威度などを総合的に評価するために利用しています。また、観測情報の一部は JPCERT/CC Web ページなどでも公開しています。

1-3-1. 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、ポートスキャンの頻度や内訳の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、各センサーに記録されたアクセス先ポートごとのスキャン件数の平均値を表しています。

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

本四半期に ISDAS で観測されたアクセスの宛先ポートの上位 1 位～5 位および 6 位～10 位のそれぞれについて、アクセス数の時間的の推移を図 1-1 と図 1-2 に示します。

- アクセス先ポート別グラフ top1-5 (2010 年 1 月 1 日-3 月 31 日)

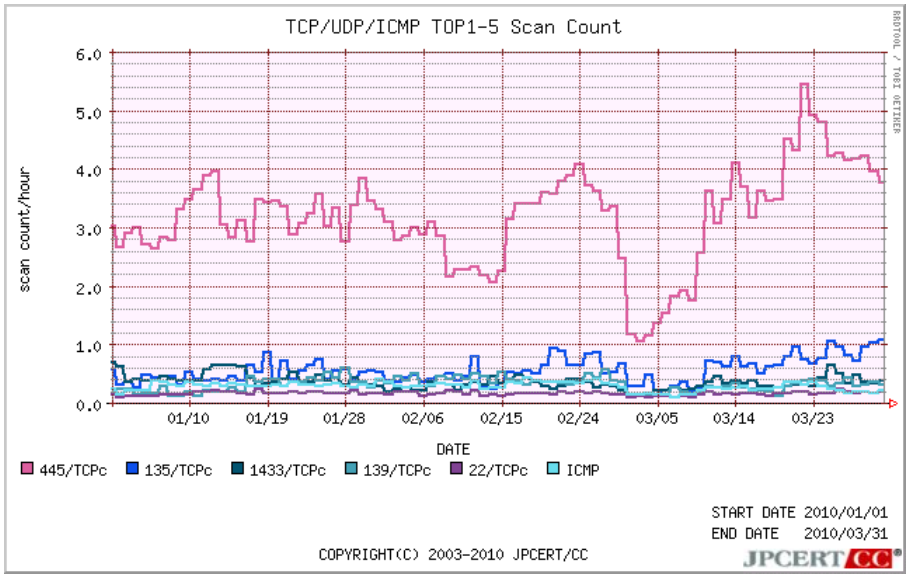


図 1-1 : アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2010 年 1 月 1 日-3 月 31 日)

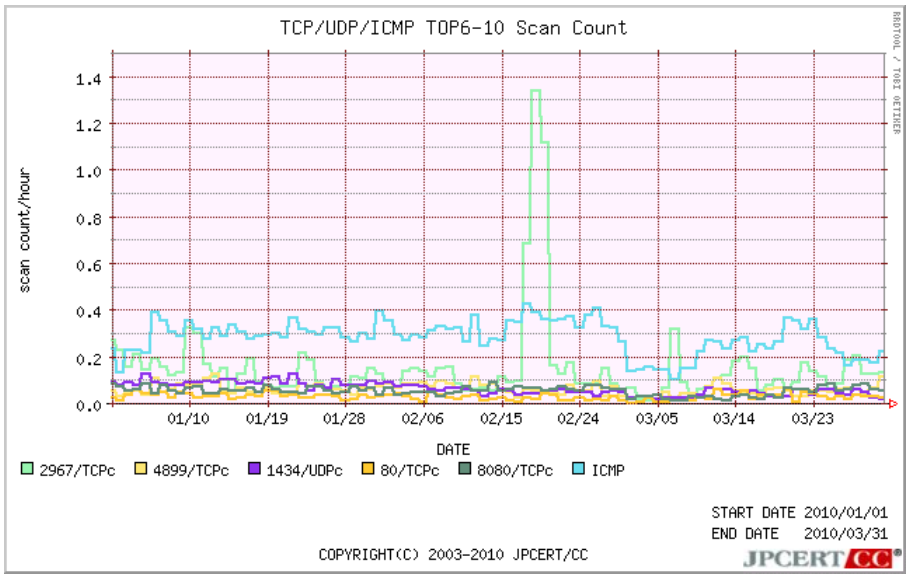


図 1-2 : アクセス先ポート別グラフ top6-10

また、より長期間のスキャン推移を見るため、2009 年 4 月 1 日から 2010 年 3 月 31 日までの期間における、アクセスの宛先ポートの上位 1 位～5 位および 6 位～10 位のそれぞれについて、アクセス数の時間的の推移を図 1-3 と図 1-4 に示します。

- アクセス先ポート別グラフ top1-5 (2009 年 4 月 1 日-2010 年 3 月 31 日)

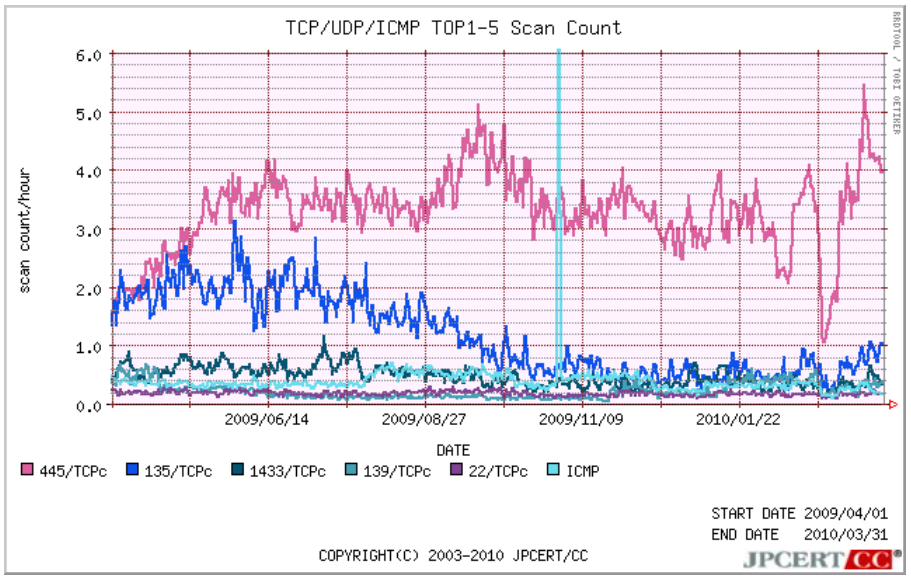


図 1-3: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2009 年 4 月 1 日-2010 年 3 月 31 日)

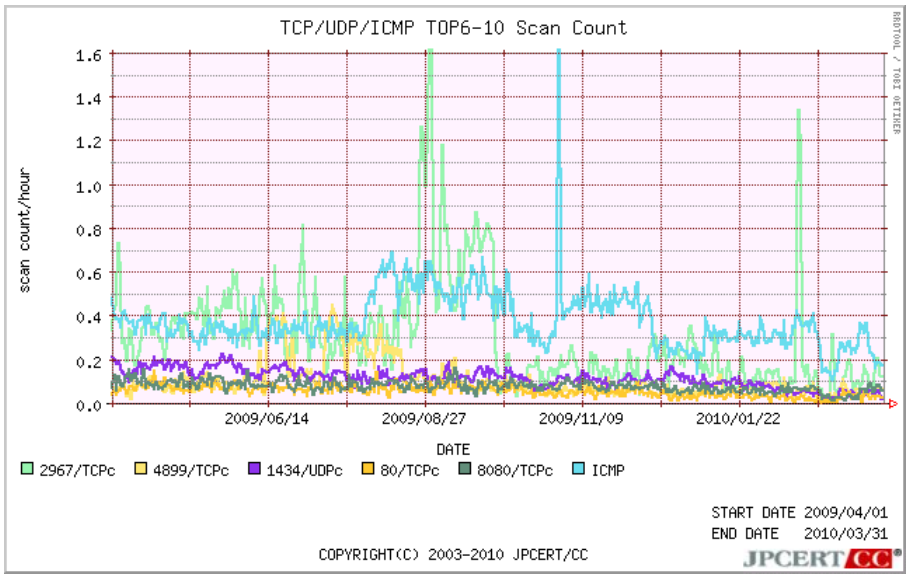


図 1-4: アクセス先ポート別グラフ top6-10

これまでと同様に、Windows や Windows 上で動作するソフトウエア、リモート管理を行うためのプログラムが利用するポートを対象とした攻撃や弱点探索活動が上位を占めています。新しい脆弱性が見つかっていないソフトウエアに対しても Scan が行われています。既知の脆弱性の対策漏れが探索されている可能性もありますので、OS やアプリケーションに脆弱性を修正する修正プログラムを適用しているか、ファイアウォールやウイルス対策ソフトなど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。また、Microsoft 社 Windows 2000 製品群の延長サポートは 2010 年 7 月 13 日（米国時間）で終了となる予定です。これらの製品をまだお使いの場合、速やかにサポートされている製品への移行を検討してください。

1-4. 日本シーサート協議会 (NCA) 事務局運営

JPCERT/CC は、国内のシーサート(CSIRT: Computer Security Incident Response Team)の活動を支援する日本シーサート協議会の事務局運営を行っています。事務局では、協議会の問合せ窓口、会員情報の管理、加盟のためのガイダンスの実施および手続の運用、Web ページ、メーリングリスト等の管理を行っています。

活動の詳細については、以下の URL をご参照ください。

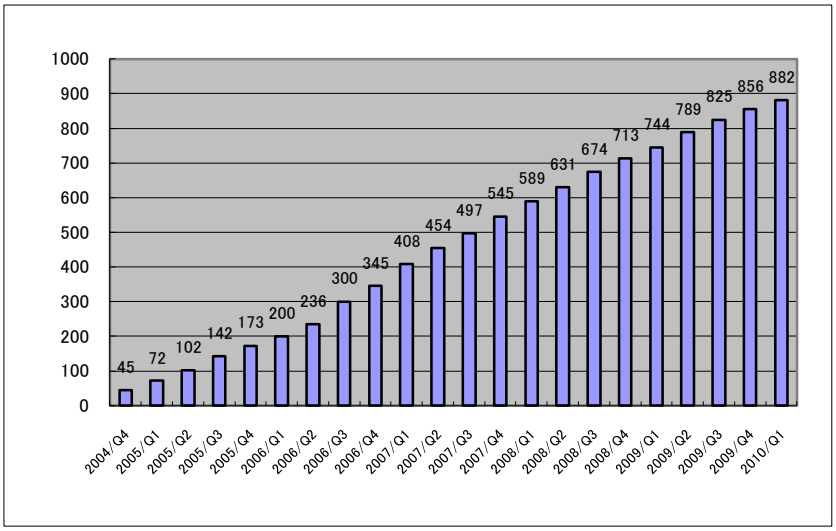
日本シーサート協議会 Web ページ
http://www.nca.gr.jp/

2. 脆弱性関連情報流通促進活動

JPCERT/CC では、脆弱性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促進業務を進めています。

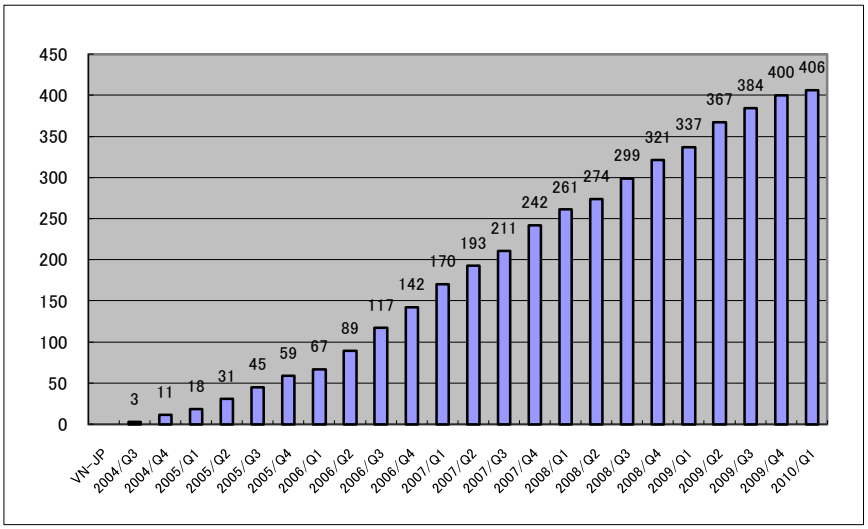
2-1. Japan Vulnerability Notes (JVN) において公開した脆弱性情報および対応状況

本四半期に JVN において公開した脆弱性情報および対応状況は 26 件 (総計 882 件) [図 2-1] でした。各公開情報に関しては、JVN(http://jvn.jp/)をご覧ください。



[図 2-1　累計 JVN 公表件数]

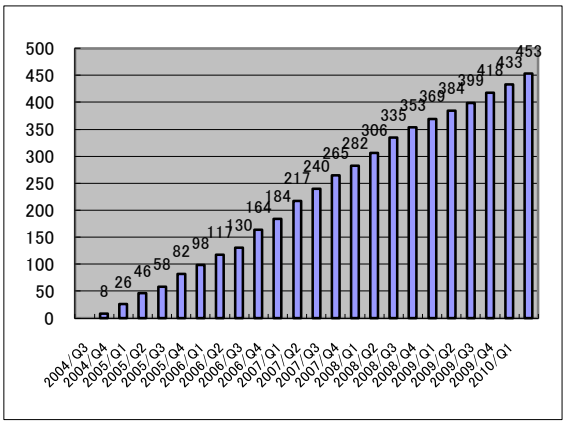
このうち、本基準に従って、独立行政法人情報処理推進機構 (IPA) に報告され、公開された脆弱性情報は 6 件(累計 406 件) [図 2-2] でした。これは、本年度の各四半期における公表状況と比較して、かなり少ないと言えます。この公開件数の減少は、IPA へ届出られる脆弱性関連情報の減少を反映していると考えられます。



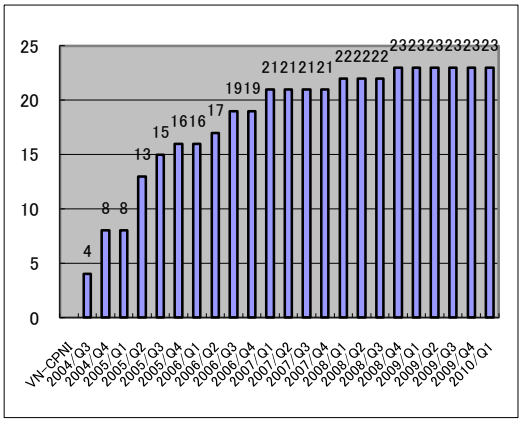
[図 2-2　累計 VN-JP 公表件数]

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 20 件(累計 453 件) [図 2-3]でしたが、このうち 2 件(JVNVU#188937 および JVNVU#571860)は、フィンランド CERT-FI とのパートナーシップに基づき調整が行われたものでした。しかしながら、現在の JVN には CERT-FI との間の調整案件に関する採番カテゴリが存在しないことから、これら 2 件については、便宜的に VN-CERT/CC として公開したものです。なお、英国 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 2-4] でした。

本四半期中に VN-CERT/CC として公開された脆弱性情報としては、Microsoft 製品に関するものが 8 件と特に目立ちました。このうち約半数にあたる 3 件が、初回情報公開時においては「対策方法なし」のゼロデイ脆弱性情報として公開されたことが特徴的でした。



[図 2-3　VN-CERT/CC 公表件数図]



[図 2-4　累計 VN-CPNI 公表件数]

2-2. 海外 CSIRT との脆弱性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情報の円滑な流通のため、米国 CERT/CC や英国 CPNI などの海外 CSIRT との間で、報告された脆弱性情報の共有、各国の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集約等、脆弱性情報の公開のための調整活動を行っています。

また、国際的な活動の一環として、2008 年 5 月 21 日から JVN 英語版サイト(http://jvn.jp/en)の運用を開始し、それに併せて 2008 年 8 月から CVE(Common Vulnerabilities and Exposures) 識別子の取得を積極的に推進しました。その結果、運用開始後に JVN で公開されたものの約 9 割に CVE 識別子が付与されています。実際に、JVN 英語版サイトへのアクセス数も半年前と比較して倍増しており、海外の主要セキュリティ関連組織などからも注目されるようになったため、海外の組織から公開されるアドバイザリにも、多くの場合 JVN 英語版サイトへのリンクが掲載されるようになっています。

CVE には、CVE 互換(CVE Compatibility)という認定制度があり、「脆弱性対策情報提供サイト等が、CVE 識別番号の正確な表示、適切な情報関連付け、CVE 識別番号による情報の検索などといった一定の条件を満たしていること」を、米国 MITRE 社が認定しています。IPA および JPCERT/CC は、2009 年 1 月に、CVE 互換宣言（Declaration of CVE Compatibility）を行い、約 1 年の審査期間を経て 2010 年 1 月に正式な CVE 互換の脆弱性対策情報提供サイトとして認定されました。

詳しくは、CVE 互換認定に関する米国 MITRE 社発行のプレスリリース等、次の URL をご参照ください。

News and Events January 8, 2010
“Three Products and Services from Tow Organizations now registered as Officially CVE-Compatible”
http://www.cve.mitre.org/news/index.html#jan082010a

CVE-Compatible Products and Services
http://cve.mitre.org/compatible/compatible.html#j

2-3. 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、次の URL をご参照ください。

脆弱性情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
脆弱性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_guide2009.pdf
JPCERT/CC 脆弱性情報取り扱いガイドライン
http://www.jpcert.or.jp/vh/guideline_2009.pdf

本四半期の主な活動は以下のとおりです。

2-3-1. 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

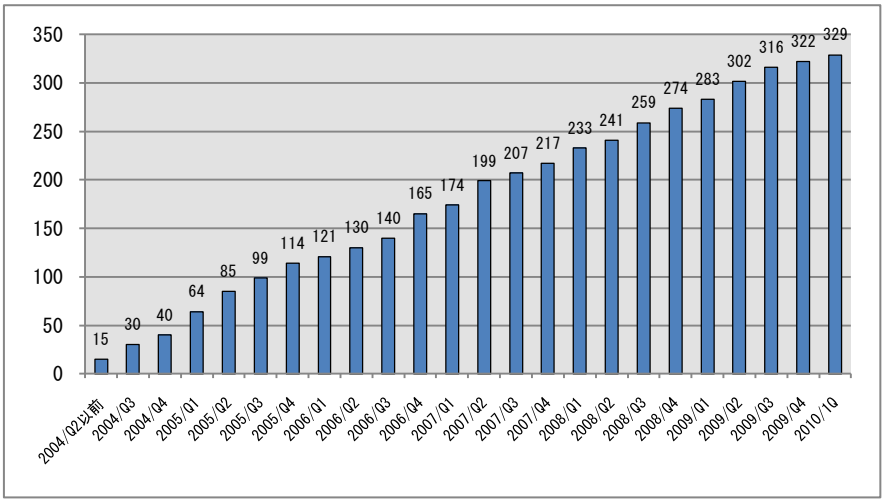
本基準では、受付機関に IPA (http://www.ipa.go.jp/)、調整機関に JPCERT/CC が指定されています。JPCERT/CC は IPA が受け付けた届出情報の転送を受けて、製品開発者への情報提供を行い、対策情報公開に至るまでの調整を行っています。最終的に IPA と共同で JVN にて対策情報を公開しています。両組織間においては緊密な情報の交換、脆弱性情報の分析等を行っています。なお、本基準における IPA の活動および四半期毎の届出状況については次をご参照ください。

http://www.ipa.go.jp/security/vuln/

2-3-2. 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、製品開発者の皆様に製品開発者リストへの登録をお願いしています。製品開発者の登録数は、以下のグラフに示すとおり、2010 年 3 月 31 日現在で 329 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 2-5　累計製品開発者登録数]

本四半期から、脆弱性情報ハンドリングにおける、製品開発者と JPCERT/CC の調整業務を支援するツール「JVN ベンダポータルシステム」の運用を開始しました。本システムは従来の JVN システムにあった、製品開発者が自身の脆弱性対応状況に関する JVN への掲載内容を入力する機能を大幅に拡張したもので、脆弱性関連情報の受け渡しから JVN 掲載内容の入力までの情報連絡全般や、製品開発者自身による登録情報の入力・管理、製品開発者間での情報共有等をサポートします。また従来のシステムを利用するうえでの制約（PC 環境の制限や SSL クライアント証明書が必要であること等）を解消し、製品開発者に広くご利用いただけるよう改善を行いました。
本システムの利用により、脆弱性関連情報の取扱いの安全性を維持しつつ、同時にハンドリング業務が効率化されることが期待されます。

また、2009 年 7 月 10 日に改定した「JPCERT/CC 脆弱性関連情報取扱いガイドライン」に基づき、脆弱性情報への対応が必要な製品開発者と連絡がとれない等の理由により調整が困難なケースへの対応について、関係機関と協議をしながら、具体的な運用手順の整備を進めています。

2-3-3.　製品開発者との定期ミーティングの実施

脆弱性情報ハンドリング業務に関する意見交換や技術情報の共有等を目的として、「JPCERT/CC 製品開発者リスト」に登録されている国内製品開発者の連絡担当者にお集まりいただきミーティングを開催しました。
- 2010 年 2 月 18 日に、脆弱性情報ハンドリング業務における製品開発者と JPCERT/CC との間のコミュニケーションを支援するツールである「JVN ベンダポータルシステム」の紹介と、運用方法やハンドリング業務手順等について製品開発者とのディスカッションをおこないました。
- 2010 年 3 月 25 日に、脆弱性情報ハンドリングに関する活動状況の報告、海外における脆弱性やセキュリティに関する動向や技術情報等を紹介するとともに、それらについて製品開発者との意見交換を行ないました。

2-3-4. 「責任ある脆弱性情報開示」の国際標準化活動への参加

ISO/IEC JTC-1/SC27 WG3 において検討されている、製品開発者による脆弱性関連情報の受取と発信のためのガイドラインである RVD (29147: Responsible Vulnerability Disclosure)の標準化は、11 月に開催された SC27 の国際会議において合意された改訂方針に基づき第 4 次作業草案をエディタが用意し、これが 2010 年 1 月中旬に SC27 事務局を通じて参加各国に配付されました。

これまでの議論の中心になっていた、標準規格の全体構成および前半部分の記述については完成度が向上したが、後半部分は本格的な議論が未着手であるとの認識の下、後半部分を中心として、国内委員会でのメール議論も反映しつつ、総数で 70 項目余りに及ぶ修正提案を作成し、WG3 代表者を通じて、日本の修正提案として事務局に提出しました。

この後、SC27 事務局が参加各国およびアライアンス参加団体からの修正提案を取りまとめた上で配付し、4 月中旬にマレーシアの Melaka で開催される次の SC27 国際会議で、その取扱いが議論される予定になっています。JPCERT/CC では、引き続き、この国際標準が我が国の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に整合したものとなるよう努めていく所存です。

2-4. セキュアコーディング啓発活動

2-4-1. セキュアコーディングセミナー in ベトナム

1 月 13 日から 15 日の 3 日間、ベトナムの首都ハノイにおいて C/C++セキュアコーディングセミナーを実施しました。海外でのセキュアコーディングセミナーの実施は、タイ、インドネシアに続いて 3 カ国目です。JPCERT/CC とベトナムを代表する CERT 機関である Vietnam Computer Emergency Response Team (VNCERT)の協力のもと、ベトナム国内の C/C++プログラマを対象に 3 日間コースの教育を行い、好評のうちに終了しました。

本セミナーは、セキュアコーディングに必要な知識に関する講義だけでなく、受講者が主体的に参加するハンズオンを重視して構成しました。その内容は、C/C++プログラミングで問題になりやすい文字列と整数に関する脆弱性の各論クラス、それぞれのクラスについて受講者が理解度を把握するための演習問題、実際に脆弱なコードをレビューしつつその修正方法を検討するハンズオンの 3 部構成で行われました。

参加者の中には、日本の大手メーカーからオフショア開発を受託する企業のプログラマもみられました。[図 2-6]の教室風景からも窺えるように、クラスの随所で活発な質疑応答や議論が行われ、受講者の意識の高さ、技術レベルの高さが感じられる 3 日間のセミナーとなりました。

[図 2-6　演習問題に取り組む受講者]

2-4-2.　C/C++ セキュアコーディングセミナー資料(2009 年度版)公開

2009 年度に「C/C++ハーフデイキャンプ」と題して開催した C/C++セキュアコーディングセミナーで使用した講義資料(2009 年度版)を公開しました。

https://www.jpcert.or.jp/research/materials.html

2-4-3. ウェブマガジン連載

CERT C セキュアコーディングスタンダードの内容をより分かりやすく解説した連載記事「脆弱性の体質改善――C/C++セキュアコーディング入門」を、Web マガジン CodeZine(コードジン) に連載しています。

「安全なシグナルハンドラを実装するには」「sizeof オペレータを正しく使おう」「配列コピー時に犯しやすい誤りに注意する」といったタイトルで、ソフトウエアの脆弱性につながりがちなコーディングエラーとその対策方法を紹介しています。

次回以降の連載では、読者が実際にコードレビューを行いコード上の問題について考える、より実践的な内容をお届けする予定です。

CodeZine
http://codezine.jp

2-4-4. 「CERT C セキュアコーディングスタンダード」レコメンデーションを追加公開

「CERT C セキュアコーディングスタンダード」は、C 言語のソフトウエア開発においてソフト

ウエアの脆弱性につながりやすいコーディングエラーを特定し、その対策方法について解説したコーディング規約です。

既に公開済みのルールとレコメンデーションに加え、新規レコメンデーションを公開しました。これらは、昨年 9 月に出版した書籍『CERT C セキュアコーディングスタンダード』(アスキー)には含まれないレコメンデーションです。書籍と合わせてご利用ください。

https://www.jpcert.or.jp/sc-rules/

2-5. 制御システムセキュリティにおける啓発活動

2-5-1. 制御システムセキュリティカンファレンス開催

昨年度に続き、制御システムセキュリティカンファレンスを 2010 年 2 月 9 日に東京(永田町)で開催致しました。今回は「ベンダの役割、ユーザの役割」をテーマに、制御システム関係者の複雑な役割の絡みあいを整理し、それぞれが何をすれば、セキュリティがより向上するのかという「気づき」の場を提供することを目的と致しました。
午前に行われた第一部では、国際的な制御システムセキュリティ検討 WG(MPCSIE)メンバーによる講演と JPCERT/CC による制御システムセキュリティ評価ツールの紹介を、午後に行われた第二部では、JPCERT/CC によるサイバー攻撃ツールのデモや、国内のユーザ、開発者、ベンダによる講演、パネルディスカッションを実施し、好評裡に終了致しました。

プログラム等の詳細は次の URL をご参照ください。

制御システムセキュリティカンファレンス 2010
https://www.jpcert.or.jp/ics/conference2010.html

制御システムセキュリティカンファレンス 2010 においての講演資料
https://www.jpcert.or.jp/present/#year2010

2-5-2. 制御システムのサイバーセキュリティなど新たに３つの文書を公開

次の３つの文書を新たに作成し、JPCERT/CC Web ページの制御システムセキュリティコーナー(http://www.jpcert.or.jp/ics/)で 3 月 31 日に公開しました。

1) 「制御システムのサイバーセキュリティ：多層防御戦略」
製造業、輸送業、エネルギーなど主要な産業や社会を支える重要インフラでは、制御システムが

多用されています。これらのシステムは、旧来システムから、新しい IT 技術を取り入れたオープン・システムに移行しつつあり、制御システムの多種多様で独自の構造が、共通の通信プロトコルやオープンアーキテクチャ標準に置き換えられています。これには、プラスとマイナスの両側面の影響があります。
こういった事実を背景として、この文書では制御システムネットワークを使用している組織向けに、多層情報アーキテクチャを維持しつつ、「多層防御戦略」を策定するための指針と方向性を示しています。

2) 「人的セキュリティガイドライン」
2003 年 8 月 14 日に米国で発生した最大規模の停電の原因は、人員の能力不足と教育・訓練不足、コミュニケーション不足、設備の不備であったことが判明し、停電の調査委員会は、政府機関による法規制、監視、違反への罰則を勧告しました。この後さまざまな産業や政府機関が人的セキュリティガイダンスを提供していますが、この文書では、米国で全国的に認知されている 7 つの産業団体と政府機関の推奨事項に基づいて作成された人的セキュリティプログラムガイダンスについて、信頼、能力、運用上安全な環境、という 3 つのカテゴリを対象として紹介しています。

3) 「推奨プラクティス：工業用制御システムにおけるサイバーセキュリティインシデント対応能力の開発」
工業用制御システムは、従来のビジネス情報システムと同様、悪意のあるさまざまな攻撃を受ける可能性が増しています。攻撃目的は様々であり、攻撃元もまた、不満を持つ従業員、競合相手、そして不注意でサイトをマルウエアに感染させてしまう友好的な相手の場合と様々です。この文書は、制御システムを利用する施設が、攻撃元を問わずサイバーインシデントに備え、対応するのに役立つ推奨事項を、①サイバーインシデントに関する計画の作成、 ②インシデントの防止、③インシデント管理、 ④インシデント後分析、の 4 つのセクションに分けて解説しています。そして、インシデントから得た教訓を活かし、潜在的攻撃に備えてシステムを強化する方法も提案しています。

今後も、先のセキュリティカンファレンスのアンケート結果等を参考に、ニーズや時宜を得た文書の翻訳や紹介を行っていく予定です。

2-5-3. セキュリティ・アセスメント・ツールの調査

前四半期に引き続き、セキュリティ・アセスメント・ツールを関係者に提供するための活動を進めました。米国 DHS が開発した CSET(CS^{2}SAT の後継版)と英国 CPNI が開発した SSAT の 2 種類のツールについて、入手方法の調査および試用を行うとともに、両者の特徴やその違いを理解した上で、どのような業界への適用が最も効果的かについて関係者の意見を聴取するため以下の説明会を開催し、併せて関連文書の一部日本語化などを進めました。
2009 年 12 月 11 日 SICE/JEITA/JEMIMA 合同 WG （前四半期間）

2 月　9 日 制御システムセキュリティカンファレンス 2010
2 月 15 日 A協会（都市ガス事業者の団体）
2 月 16 日 Bセンター（セキュリティ評価業務を行っている法人）
2 月 24 日 C社（セキュリティ・サービス一般企業）

これらのツールについては、広く公開する前にモニターによるフィールド・トライアルを行うため、SICE/JEITA/JEMIMA 合同 WG への説明後、WG 内への展開、アンケートを依頼しています。

2-5-4. 制御システムベンダーセキュリティ情報共有タスクフォースへの情報発信

制御システム開発関係者にセキュリティ関係の情報を提供するニュースレターを、2 回(1 月 28 日および 2 月 18 日（号外）)配信しました。タスクフォースメンバー向けに、セキュリティインシデントに係る事例や関係する標準の動向、技術情報に関するニュースなどを収集して掲載しています。今回はセキュリティカンファレンスの告知や、米国・国土安全保障省 (DHS) からの「制御系システムのサイバーセキュリティ演習」参加募集案内を号外としてお知らせしました。今後とも、タスクフォースメンバーの要望等を収集し、内容の充実を図っていく予定です。
このニュースレターは、制御システムベンダーセキュリティ情報共有タスクフォースのメンバーであれば、どなたでも受信できます。タスクフォースへの参加資格や申込方法については、以下の URL をご参照ください。

制御システムベンダーセキュリティ情報共有タスクフォース
http://www.jpcert.or.jp/ics/taskforce.html

なお、来期には、タスクフォースへの参加資格の拡充（制御系ユーザーも参加可能とする等）を検討する予定です。

2-5-5. 制御システム関連学界活動

1 月 8 日、1 月 15 日、2 月 3 日、および 3 月 10 日に SICE(計測自動制御学会)ネット部会や、JEMIMA(日本電気計測工業会)などによる合同セキュリティ検討 WG の活動に参加し、制御システムのセキュリティをめぐって，制御システムの専門の方々と意見交換を行いました。来期以降のアクションプランのひとつである「ユーザ企業のために対策が必要な脆弱性情報抽出方法の検討」を開始するため、WG メンバーからのヒアリング、提案等を通してさらに強く連携を深めて行きたいと考えています。

3. 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、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担当しています。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なども行っています。

3-1. 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。詳細については、次の URL 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/

2010 年 2 月度 サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/201002/1002monthly.html

4. 国際連携活動関連

4-1. 海外 CSIRT 構築支援および運用支援活動

主にアジア太平洋地域の CSIRT (Computer Security Incident Response Team) に対し、イベントでの講演やトレーニング等を通して CSIRT の構築・運用支援活動を行い、各国とのインシデント対応調整における連携強化を図っています。

4-1-1. アジア太平洋地域における活動

4-1-1-1. AOTS による「情報セキュリティ研修コース - CSIRT 体制強化 -」への協力(2010 年 1 月 13 日-22 日)

財団法人 海外技術者研修協会 (AOTS) による「情報セキュリティ研修コース - CSIRT 体制強化 -」の講師を JPCERT/CC が務めました。本研修は、インドネシア、カンボジア、タイ、フィリピン、ベトナム の 5 か国から、計 24 名 (CSIRT、IT 関連企業、金融機関、大学、研究機関などの情報セキュリティ関連業務の職員) を日本に招聘し、インシデントに対応するための技術および CSIRT 運用の実践的なノウハウの習得、ASEAN 諸国における CSIRT 体制の強化、および自国でリーダとなる人材の育成を目的に、8 日間のコースとして実施されました。
研修のプログラムとしては、最新のインターネットセキュリティ技術動向に関する講義を始め、マルウエア、脅威情報収集、定点観測脅威情報に関する高度分析・連携について講義およびハンズオン形式のトレーニングを行ないました。また、これらの講義を通して得た知識を実際に活用できるかどうかを確認する目的で、5 か国合同で国際サイバー攻撃に対応する演習を企画し、参加者からは、訓練と経験を得られて非常に有益だったとの評価を得ることができました。

4-1-1-2. ITU 主催 第 2 回 Pacific CERT (PacCERT) 設立ワーキンググループ会合への参加 (2010 年 2 月 11 日-12 日)

ITU (Regional Office for Asia and the Pacific) がフィジーにて主催した、第 2 回 Pacific CERT (PacCERT) 設立ワーキンググループ会合に参加しました。PacCERT は、太平洋諸島の国々の CSIRT として、フィジーの University of the South Pacific 内に設立される予定です。設立は ITU が主導し、オーストラリア政府等の支援を受けて進められています。
今回の会合では、JPCERT/CC が行なっている CSIRT 構築支援活動を紹介するとともに、APCERT (アジア太平洋コンピュータ緊急対応チーム) の事務局として、アジア太平洋地域における国際 CSIRT 間連携の活動を紹介しました。

4-1-2. その他地域における活動

4-1-2-1. ICT 国際協力セミナーにパネリストとして参加(2010 年 3 月 10 日)

総務省の主催により、秋葉原コンベンションセンターで開催された「ICT 国際協力セミナー - 情報通信分野における国際協力担当者の育成に向けて - 」に参加しました。本セミナーは、今後の ICT 国際協力プロジェクトへの参画や形成を担う人材育成の支援を目的に開催され、ICT 分野における国際協力の現状や課題、支援施策等が、講演およびパネルディスカッションの形式で紹介されました。JPCERT/CC はパネルディスカッションにパネリストとして参加し、アジア太平洋地域を中心とする CSIRT の構築支援および運用支援活動を通じてこれまでに得た知見を紹介しました。

4-2. 国際 CSIRT 間連携

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、および、各国のインターネット環境の整備や情報セキュリティ関連活動への取り組みの実施状況等に関する情報収集を目的とした国際連携活動等を行っています。アジア太平洋地域における APCERT (Asia Pacific Computer Emergency Response Team) の枠組みや、国際的な FIRST (Forum of Incident Response and Security Teams) の枠組みに則って活動しています。

4-2-1. アジア太平洋地域における活動

4-2-1-1. APCERT 合同サイバー演習 (APCERT Drill 2010) の参加(2010 年 1 月 28 日)

APCERT 加盟チームとして、サイバー攻撃への即時対応能力を確認するための APCERT の合同サイバー演習に参加しました。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、2005 年から毎年実施しています。
今回の演習は、オンライン取引を行なう Web サイト (オンラインバンキング、オークション、株式取引など) が、サイバー犯罪組織から、サービスの停止、ユーザ情報の盗用、地下市場への金銭の盗用などを目的とした攻撃を受けた場合を想定し、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および意思決定能力の向上を目標に、約 4 時間にわたり、5 つのタイムゾーンを横断して行われました。
今年は、アジア太平洋地域の 14 の経済地域 (日本、オーストラリア、ブルネイ、中国、台湾、香港、インド、インドネシア、韓国、マレーシア、シンガポール、スリランカ、タイ、ベトナム) から、過去最多の 16 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 knocks down Cyber Crimes with Financial Incentives in Drill Exercise 2010
http://www.apcert.org/documents/pdf/Drill2010_PressRelease.pdf

4-2-1-2. 台湾「情報セキュリティ防御能力の向上」会合への参加(2010 年 2 月 24 日-25 日)

本会合は、日本および台湾の情報セキュリティ関係者が参加し、日本の情報セキュリティ政策や取組み、普及啓発活動などを台湾の関係者と共有することにより、台湾側のインシデント防御能力の向上に資することを目的に台湾で開催されました。
JPCERT/CC は、日本の情報セキュリティ分野における調査・研究開発に関する活動を紹介し、日本での研究事例などについて議論しました。さらに、重要インフラ分野における早期警戒情報発信などの取組みなどについて、JPCERT/CC の経験を交えて講演しました。台湾における情報セキュリティに関する研究開発の取り組みが今後活発化することが期待されます。

4-2-1-3. APCERT 年次会合 2010 への参加(2010 年 3 月 2 日-4 日)

アジア太平洋地域の CSIRT コミュニティである APCERT の年次会合がタイで開催され、APCERT 加盟チームとして JPCERT/CC も参加しました。APCERT には、2010 年 4 月 1 日現在、17 経済地域から 25 のチームが加盟しています。
本会合は、各地域における最近のインターネットセキュリティ動向、インシデント対応の事例、調査・研究活動などに関する情報を共有することを目的に、毎年開催されています。このような会合を通じて、各地域間の情報共有を促進し、信頼関係を醸成して、国際間でのインシデント対応調整がより円滑に進められるよう努めています。
今年の会合は、「Web 2.0 における攻撃およびソーシャルネットワークにおけるセキュリティ動向」をテーマに開催され、複雑化するインターネット上のコミュニケーションの場を標的とした高度な攻撃や対策に関する発表が多数行われました。APCERT 年次会合 2010 についての詳細は、以下の URL をご参照ください。

APCERT Annual Conference 2010
http://apcert2010.thaicert.org/

4-2-1-4. TSUBAME ネットワークモニタリングワークショップの開催(2010 年 3 月 5 日)

JPCERT/CC は、APCERT 年次会合と併催で、アジア太平洋地域の CSIRT を対象とした TSUBAME ネットワークモニタリングプロジェクトのワークショップをタイにて開催しました。本プロジェクトは、アジア太平洋地域における定点観測プロジェクトで、各地域のインターネット上にセンサーを分散配置し、ワームの感染活動や弱点探索を目的としたスキャンなど、セキュリティ上の脅威となるトラフィックの観測を行っているもので、APCERT のワーキンググループの一つとして、JPCERT/CC が主導的に運営しています。
本ワークショップでは、ネットワークモニタリングおよび TSUBAME システムの紹介 (一般参加者向け)、およびハンズオン形式のトレーニング (TSUBAME プロジェクトメンバ向け) をそれぞれ半日ずつ実施しました。

4-2-2. その他の地域における活動

4-2-2-1. TF-CSIRT 会合および TF-CSIRT/FIRST シンポジウムへの参加(2010 年 1 月 25 日-26 日)

TF-CSIRT および FIRST がドイツで主催した TF-CSIRT 会合および TF-CSIRT/FIRST シンポジウムに参加しました。TF-CSIRT はヨーロッパ地域における CSIRT コミュニティであり、年に 3 回程会合を開催し、各国のインターネットセキュリティ動向や欧州地域におけるプロジェクトの実施状況などについて共有しています。
JPCERT/CC は本会合に参加し、ヨーロッパ地域における CSIRT 活動の最新状況を把握し、今後、ヨーロッパ地域とのインシデント対応調整が必要となる事例に備え、連携の一層の強化を図りました。

4-2-2-2. 米国 US-CERT および CERT/CC との連携強化(2010 年 2 月 3 日, 2 月 5 日, 3 月 11 日)

2 月には、米国の US-CERT および CERT/CC を訪問し、各組織の最新の活動状況や体制について情報交換を行なうとともに、インシデントハンドリング、脆弱性情報ハンドリング、マルウエア分析などのオペレーションにおける連携体制の改善策、および CSIRT 構築支援活動を含む今後の更なる協力関係について議論しました。また、3 月には US-CERT の担当者が来訪し、JPCERT/CC の各業務のオペレーション担当者との間で運用上の手続きの改善策等についての確認、議論を行いました。

4-3. APCERT 事務局運営

JPCERT/CC は、アジア太平洋地域の CSIRT のコミュニティである、APCERT の事務局を担当しています。APCERT についての詳細は、次の URL をご参照ください。

APCERT
http://www.jpcert.or.jp/english/apcert/

4-4. FIRST Steering Committee への参画

FIRST Steering Committee のメンバとして、JPCERT/CC の職員が FIRST の組織運営に関与しています。

FIRST Steering Committee
http://www.first.org/about/organization/sc.html

5. フィッシング対策協議会事務局の運営

JPCERT/CC では、経済産業省からの委託により、フィッシング対策協議会の事務局運営を行っています。協議会の総会や各ワーキンググループの運営、Web ページの管理、一般消費者からのフィッシングに関する報告、問合せの受付、報告に基づくフィッシングサイトに関する注意喚起、JPCERT/CC のインシデント対応チームに対するサイトの停止調整の依頼、国内外関連組織との共同研究などの活動を行っています。

5-1. フィッシング対策協議会の活動実績の公開

フィッシング対策協議会の Web ページでは、毎月の活動報告として「フィッシング情報届出状況」を公開しています。詳細については次の URL をご参照ください。

フィッシング対策協議会 Web ページ
https://www.antiphishing.jp

フィッシング対策協議会 2010 年 1 月 フィッシング情報届出状況
https://www.antiphishing.jp/information/information1039.html
フィッシング対策協議会 2010 年 2 月 フィッシング情報届出状況
https://www.antiphishing.jp/information/information1049.html
フィッシング対策協議会 2010 年 3 月 フィッシング情報届出状況
https://www.antiphishing.jp/information/information1060.html

5-2. 情報収集と動向分析の強化

フィッシング対策協議会 Web ページや会員向け ML では、本四半期において、フィッシングに関するニュースや緊急情報を 16 件公開しました。また、フィッシングの動向や新対策技術に関して有識者にインタビューを行い、フィッシング対策協議会の Web ページに 2 件掲載したほか、会員向けに、勉強会の開催、フィッシングに関するトピックの提供などを実施しました。先進的な対策技術の開発の観点からは、電気通信大学吉浦研究室が行っている「コンテンツベースのフィッシング検知技術」の共同研究に参画したほか、フィッシング対策ツールの検知効率調査を実施しました。これらの調査研究の成果は、フィッシング対策協議会の Web ページにて順次公開を予定しています。

5-3. 一般ユーザからの問合せ業務改善

本四半期は、フィッシング対策協議会に寄せられるフィッシング事例報告や各種の相談に対して、翌営業日までに対応を行うように業務の改善を行いました。特に、フィッシング事例への対応に

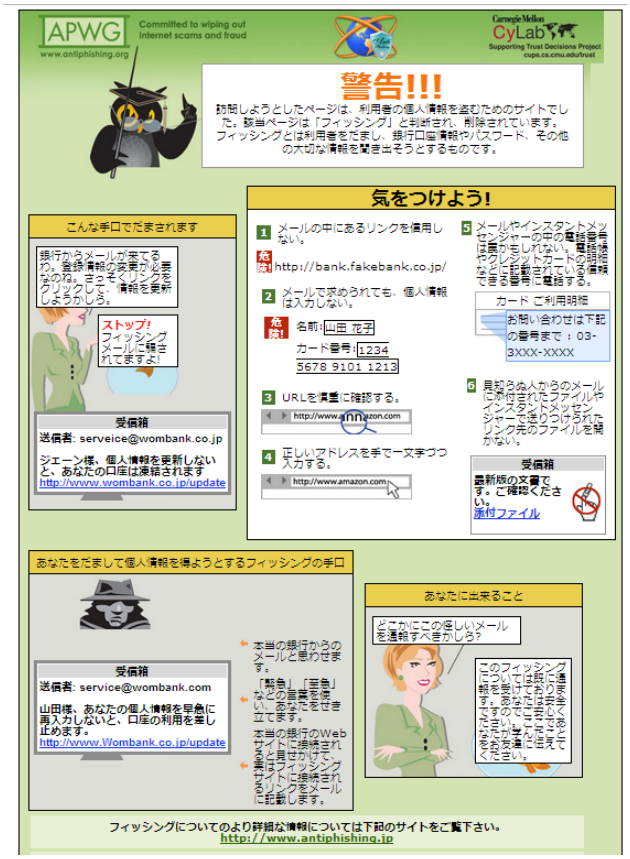
ついては、直ちに JPCERT/CC のインシデント対応チームに対しサイト停止調整の依頼を行い、フィッシング被害の拡大防止に努めました。

5-4. フィッシングサイトの URL を会員（対策サービス事業者）へ情報提供開始

よりプロアクティブなユーザ保護の取り組みとして、フィッシング対策協議会に寄せられるフィッシングサイトの URL を、協議会会員のうちのフィッシング対策ツールバーを提供している事業者やウイルス対策ソフトベンダに提供し、製品のブラックリストに追加する等の活用を図っていただくことになりました。Yahoo! Japan では、2010 年 2 月から、Yahoo ツールバーのフィッシング対策機能にこのデータを活用していただいています。現在、他の複数の事業者との間で情報提供に関する調整を行っており、提供先を拡大していく予定です。

5-5. 海外機関との連携強化

海外でのフィッシングに関する脅威の状況を把握し、国内での今後の変化を予測するために、国際的にフィッシング対策に関する活動を推進している APWG(Anti-Phishing Working Group)との連携を強化しました。具体的には、APWG の教育プログラム（「フクロウ先生のフィッシング警告ページ」）に参加し、フィッシングサイトであったページに日本語の警告が表示されるようになりました（図 1-5）。フィッシングサイトが公開されていたページにフィッシングに関する警告を表示させることで、利用者に、訪れたサイトがフィッシングサイトであったことや、フィッシングメールに誘導されてしまったことを認識してもらい、フィッシングの手口紹介やフィッシングサイトに関する注意事項などの対応を学んでもらうことが可能となります。



[図 5-1:
フクロウ先生のフィッシング教育 Web ページ:http://education.apwg.org/r/?forcelang=jp]

5-6. 普及啓発コンテンツの充実

上記 1-4-5 の「フクロウ先生のフィッシング警告ページ」については、社団法人日本インターネットプロバイダー協会（以下「JAIPA」といいます。）および、JAIPA 会員の ISP やホスティング事業者の方々と協力し、フィッシングサイトが国内に設置されていた場合についても、その跡ページに警告が表示されるよう展開を進めていきます。

フィッシング対策協議会が「フクロウ先生のフィッシング警告ページ」を日本で展開
http://www.antiphishing.jp/information/information1056.html

また、ゲーム形式でフィッシング対策を学ぶことができる教育コンテンツ（「フィッシングフィル」）（図 1-6）を 3 月 15 日から、協議会の Web サイトで公開しています。フィッシングフィルとはゲームを通してフィッシング詐欺に騙されない「URL の見分け方」を学習する教育用コンテンツです。

[図 5-2:フィッシングフィル Web ページ: http://www.antiphishing.jp/phil/]

5-7. フィッシング対策セミナーの開催

より広範にフィッシング対策の重要性を訴えるため、海外からの講演者も交えた本格的なフィッシング対策啓発セミナーを、東京（1 月 28 日）、大阪 (1 月 29 日)の 2 会場で実施しました。セミナーのプログラムは次のとおりです。

基調講演（同時通訳） 13:35-14:35 「The Anti-Phishing Working Group:Electronic Crime, Fraud and UsefulAttempts to Battle the Miscreants」 APWG（Anti Phishing Working Group）副事務総長　Foy Shiver 氏

講演 1 14:40-15:20 東京会場： 「Yahoo! JAPAN におけるフィッシング対策」 ヤフー株式会社 R&D 統括本部 開発推進室 セキュリティプラットフォーム技術　戸田 薫 氏 大阪会場： 「SNS をターゲットにしたフィッシングの実情」 株式会社ミクシィ コーポレートデザイン室 情報セキュリティグループ マネージャ/CISSP 軍司 祐介 氏
講演 2 15:35-16:15 「「.JP」におけるフィッシングの現状と対策」 株式会社日本レジストリサービス 業務部 部長補佐 白岩一光 氏
報告 16:20-17:00 「急増する日本のフィッシング被害、そしてその対策」 フィッシング対策協議会/JPCERT/CC　小宮山功一朗

注)講演 1 については東京会場と大阪会場で講演者が異なる。

6. 公開資料

JPCERT/CC の各業務において実施した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。

6-1. 制御システムのサイバーセキュリティ：多層防御戦略

本資料についての詳細は、「2-5-2.」をご参照ください。

制御システムのサイバーセキュリティ：多層防御戦略
http://www.jpcert.or.jp/research/2010/Defense_in_Depth_20100330.pdf

6-2. 人的セキュリティガイドライン

本資料についての詳細は、「2-5-2.」をご参照ください。

人的セキュリティガイドライン
http://www.jpcert.or.jp/research/2010/Personnel_Guideline_20100330.pdf

6-3. 推奨プラクティス：工業用制御システムにおけるサイバーセキュリティインシデント対応能力の開発

本資料についての詳細は、「2-5-2.」をご参照ください。

推奨プラクティス：工業用制御システムにおけるサイバーセキュリティインシデント対応能力の開発
http://www.jpcert.or.jp/research/2010/CSincident_response_20100330.pdf

6-4. 電子メールソフトのセキュリティ設定について

電子メールは広く利用されている一方で、偽造や改ざんが比較的容易にできてしまう規格上の問題を内包しています。このような問題を解決するための技術やサービスが提供されているものの、そもそもそのような対策技術の存在が広く知られていなかったり、導入の難しさから敬遠されたりして、必ずしも導入が進んでいるとはいえない状況にあります。
このような状況にあっては、電子メールソフトの利用にあたり、ユーザとして「何に注意をして」、「どのように設定すればよいのか」についての周知を図ることは非常に重要であるといえます。
そこで、電子メールの利用者が自分の身を護るためにメールソフトについて行うべき最低限の設定や確認事項を、広く利用されている主要なメールソフトについて横断的に調査し、利用者の参

照に供するために公開しました。

電子メールソフトのセキュリティ設定について
http://www.jpcert.or.jp/magazine/security/mail/index.html

6-5. 制御システムセキュリティカンファレンス 2010 講演資料

2010 年 2 月 9 日に、都市センターホテル(東京千代田区)において開催した「制御システムセキュリティカンファレンス 2010」の講演資料を公開しました。

制御システムセキュリティカンファレンス 2010 講演資料
http://www.jpcert.or.jp/present/index.html#ics

本カンファレンスについての詳細は、「2-5-1.」をご参照ください。

6-6. 重要インフラ情報セキュリティフォーラム 2010 講演資料

2010 年 1 月 25 日に、秋葉原コンベンションホール(東京千代田区)において、独立行政法人情報処理推進機構と共同開催した「重要インフラ情報セキュリティフォーラム 2010 講演資料」の講演資料を公開しました。

重要インフラ情報セキュリティフォーラム 2010 講演資料
http://www.jpcert.or.jp/present/

本カンファレンスについての詳細は、「8.開催セミナー一覧 (3)」をご参照ください。

7. 講演活動一覧

(1) 鎌田 敬介(国際部部長代理)：
「最新のインターネットセキュリティ技術動向」
The Training Program on Information Security ～ Strengthening of CSIRT [ENIS] ,
2010 年 1 月 13 日

(2) 真鍋 敬士(理事/分析センター長), 竹田 春樹(分析センター), 中津留 勇(分析センター)：
「高度マルウエア分析・連携」
The Training Program on Information Security ～ Strengthening of CSIRT [ENIS] ,
2010 年 1 月 14～15 日

(3) 鎌田 敬介(国際部部長代理)：
「情報セキュリティ技術指導手法」

The Training Program on Information Security ～ Strengthening of CSIRT [ENIS] , 2010 年 1 月 15 日

(4) 小宮山　功一朗(早期警戒グループ リーダ 情報セキュリティアナリスト)：
「高度脅威情報収集分析・連携」
The Training Program on Information Security ～ Strengthening of CSIRT [ENIS] , 2010 年 1 月 18 日

(5) 鹿野 恵祐
「定点観測脅威情報分析・連携」
The Training Program on Information Security ～ Strengthening of CSIRT [ENIS] , 2010 年 1 月 20～21 日

(6) 鎌田 敬介(国際部部長代理),クリス ホズレイ(早期警戒グループ情報セキュリティアナリスト)：
「総合演習」
The Training Program on Information Security ～ Strengthening of CSIRT [ENIS] , 2010 年 1 月 22 日

(7) 宮地 利雄(理事)：
「重要社会インフラのための制御システムセキュリティ強化に向けたガイド」
重要インフラ情報セキュリティフォーラム 2010,2010 年 1 月 25 日

(8) Jack YS LIN(早期警戒グループ 情報セキュリティアナリト)：
「Cyber Clean Center Anti-bot Countermeasures in Japan」
台湾教育部 A-ISAC & Anti-Botnet International Seminar,2010 年 2 月 1 日

(9) 宮地 利雄(理事)：
「インターネット・インシデントの動向と対策」
鹿児島大学 学術基盤情報センター情報セキュリティ講習会,2010 年 2 月 5 日

(10) 成田 広樹(情報流通対策グループ情報セキュリティアナリト)：
「制御システムセキュリティ評価ツールの紹介」
制御システムセキュリティカンファレンス 2010,2010 年 2 月 9 日

(11) 鎌田 敬介(国際部部長代理),佐藤 しおり(国際部渉外担当リーダ)：
「International CERT Development Activity of JPCERT/CC APCERT Activity」
2nd PacCERT Working Group Meeting―フィジー,2010 年 2 月 11～12 日

(12) 鎌田 敬介(国際部部長代理)：
「R&D of Information Security in Japan Critical Infrastructure Protection Activity」
情報セキュリティ防御能力の向上―台湾, 2010 年 2 月 24～25 日

(13) 戸田 洋三(情報流通対策グループ リードアナリスト)：
「事故が起こる前提で考える 中小企業のための情報セキュリティ対策のポイント
～インシデントの最新動向とその対策～」
u-Kanagawa 推進協議会　第 9 回「情報セキュリティセミナー」,2010 年 2 月 26 日

(14) 真鍋 敬士(理事/分析センター長)：

「テイクダウン(立ち下げ)のためのコーディネーション」
Web 感染型マルウエア対策コミュニティ,2010 年 3 月 2 日

(15) 鎌田 敬介(国際部部長代理)：
「TSUBAME Network Monitoring Update」,「Gumblar Worm」
APCERT Conference 2010―タイ, 2010 年 3 月 3～4 日

(16) 鎌田 敬介(国際部部長代理),鹿野 恵祐(早期警戒グループ 情報セキュリティアナリスト)：
「Introduction of Network Monitoring」,「How to use TSUBAME system」
「Overview of IPv6 Security」
TSUBAME Workshop―タイ,2010 年 3 月 5 日

(17) 鎌田 敬介(国際部部長代理)：
「情報通信分野における国際協力担当者の育成に向けて」(パネル)
総務省 ICT 国際協力セミナー , 2010 年 3 月 10 日

8. 執筆・取材記事一覧

(1) 歌代　和正(代表理事)：
「安全な環境の維持へ　国際組織間の連携を担う」
日本情報産業新聞, 2010 年 1 月 1 日

(2) 久保 正樹(情報流通対策グループ 脆弱性アナリスト)：
「動けばいいってもんじゃない」 脆弱性を作り込まないコーディング 第 4 回
安全なシグナルハンドラを実装するには―C/C++セキュアコーディング入門(4)
翔泳社 CodeZine,2010 年 1 月 4 日

(3) 早期警戒グループ：
「ホームページ改ざん 過去最悪」
NHK ニュース,2010 年 1 月 5 日

(4) 小宮山　功一朗(早期警戒グループ リーダ 情報セキュリティアナリスト)：
「Web 改ざん　不正な書き換え」
NHK 週刊ニュース, 2010 年 1 月 9 日

(5) 小宮山　功一朗(フィッシング対策協議会)：
「携帯電話の偽サイトに注意」
NHK おはよう日本, 2010 年 1 月 13 日

(6) 戸田 洋三(情報流通対策グループ リードアナリスト)：
「動けばいいってもんじゃない」 脆弱性を作り込まないコーディング 第 5 回
sizeof オペレータを正しく使おう―C/C++セキュアコーディング入門(5)
翔泳社 CodeZine,2010 年 1 月 22 日

(7) 早期警戒グループ：
「不正アクセス特集」

フジテレビ 情報プレゼンターとくダネ！,2010 年 1 月 27 日

(8) 真鍋 敬士(理事/分析センター長)：

「ネットが直面する危機」

テレビ東京　ワールドビジネスサテライト,2010 年 1 月 27 日

(9) 江田 佳領子(事業推進基盤グループ 広報マネージャ)：

「新米セキュリティ担当者が行く！CSIRT 奮闘記 現場訪問編」

日経 BP 社 日経ネットワーク 2 月号, 2010 年 1 月 28 日

(10) 富樫 一哉(事業推進基盤グループ システム開発マネージャ)：

「動けばいいってもんじゃない」 脆弱性を作り込まないコーディング 第 6 回

配列コピー時に犯しやすい誤りに注意する―C/C++セキュアコーディング入門(6)

翔泳社 CodeZine,2010 年 2 月 15 日

(11) 中尾 真二(事業推進基盤グループ 広報アドバイザー)：

「重要インフラも環境変化に則した柔軟な対応が求められる時代に―内閣官房情報セキュリティセンター」重要インフラ情報セキュリティフォーラム取材

RBB TODAY, 2010 年 2 月 15 日

(12) 中尾 真二(事業推進基盤グループ広報アドバイザー)：

「脅威の総論」――仮想化による四次元攻撃、クラウドによる「犯罪基盤 aaS」重要インフラ情報セキュリティフォーラム取材

翔泳社 CodeZine, 2010 年 2 月 15 日

(13) 江田 佳領子(事業推進基盤グループ 広報マネージャ)：

「新米セキュリティ担当者が行く！CSIRT 奮闘記 現場訪問編」

日経 BP 社 日経ネットワーク 3 月号, 2010 年 2 月 26 日

(14) 小宮山　功一朗(フィッシング対策協議会)：

「ネットハザード　巧妙化するサイバー犯罪、偽サイトで情報を盗む」

山陽新聞社,2010 年 3 月 1 日

(15) 真鍋 敬士(理事/分析センター長)：

「対ガンブラー14 社結束」

読売新聞社,2010 年 3 月 3 日

9. 開催セミナーー覧

(1) 制御システムセキュリティカンファレンス2010

本カンファレンスについての詳細は、「2-5-1.」をご参照ください。

(2) フィッシング対策セミナー

本カンファレンスについての詳細は、「1-4-6.」をご参照ください。

(3) 重要インフラ情報セキュリティフォーラム2010

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、インターネットへ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・システム への不正なアクセス、コンピュータウイルス、ボットなどによる情報の漏えい、コンピュータ・システムの障害による事業活動の停止といったインシデントの件数が増大する傾向にあります。

このような状況において、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、ネットワークセキュリティ対策等について、独立行政法人情報処理推進機構(IPA）およびJPCERT/CCでは、国内外関係組織と連携してさまざまな取り組みを行なっており、その一環として、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 業に係わる者)、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、情報セキュリティの管理的対策や技術的対策等に関する普及啓発を実施するため、「重要インフラ情報セキュリティフォーラム2010」を開催しました。

・主　　催：独立行政法人情報処理推進機構(IPA)、JPCERT/CC
・開催時期：2010年1月25日
・集客人数：262名

詳細については、以下のURLをご参照ください。
http://www.jpcert.or.jp/event/ci-2010.html

10. 後援・協力一覧

(1) HOSTING-PRO 2010
2010 年 3 月 4 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 ：
FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4 69EC E048

□ インシデント報告フォーム
http://www.jpcert.or.jp/form/