JPCERT-PR-2011-0002

発行日 : 2011-04-12

JPCERT/CC 活動概要 [2011 年 1 月 1 日 ～ 2011 年 3 月 31 日]

【活動概要トピックス】

—トピック 1 —
震災や原発事故に乗じた標的型攻撃やフィッシングサイトへの対応

JPCERT/CC では、3 月 11 日の東日本大震災発生の数日後に、震災や原子力発電所の事故に関連する言葉をメールの件名や添付ファイル名に使用した標的型攻撃に関する報告を受けました。これらの攻撃の一部に、Adobe 製品の未修正の脆弱性を使用するマルウエアを確認したため、マルウエアを解析して得られた結果に基づき、マルウエアが通信する先のサイトを管理する ISP 及び関係する CSIRT に対してサイトの停止を依頼し、翌日に当該サイトの停止を確認しました。

また、17 日には、英語でかかれた日本赤十字社を騙るサイトが公開されていることを確認しました。JPCERT/CC 及びフィッシング対策協議会では、日本赤十字社及び海外 CERT 組織との情報連携を通じて、フィッシングサイトであることの確認や、注意喚起の発行、サイトの稼働停止の依頼、海外の利用者向けの情報発信等の対応を行いました。

社会的に関心が寄せられる事件や事故が発生した場合に、それに便乗したサイバー攻撃が発生するのは毎回のことですが、このようなタイミングを狙った攻撃、とりわけ事故対応や被災地の復旧、復興にあたる関係者を狙うもの等については、JPCERT/CC においても最優先で対処しています。

企業等のシステム管理等を担当される方々におかれては、現下の状況にあって、情報セキュリティ対策以外にも様々な事々への対処を迫られているものと考えられるところ、JPCERT/CC では、注意喚起等の具体的な対応を促す種類の情報の提供にあたっては、対策/対処が必須となる事案についてポイントを絞って発信するよう努めたいと考えています。

―トピック 2―

韓国の政府系サイトを対象とする DDoS 攻撃への対応

3 月上旬に、主に韓国の政府系サイトを対象とした DDoS 攻撃が発生しました。この攻撃は、マルウエアに感染した多数のコンピュータが指令サイトからの指令を受けて行ったものでしたが、この攻撃に使用された指令サイトやマルウエアに感染したコンピュータの一部が日本国内に存在していたため、KrCERT/CC からの依頼に基づき、関係サイトの管理者や ISP 各社に対し、攻撃の停止のための対応を依頼しました。
本件事案は、日韓間の攻撃ではなく、攻撃に用いられたリソースの一部が日本国内にも存在したことに伴う対応連携の事例ですが、コンピュータセキュリティインシデントは国境を越えて発生する場合が多く、日本国内の組織等が攻撃を受ける被害者になる事案だけでなく、攻撃に加担させられて攻撃元になってしまう事案についても、このような国際間のインシデント対応連携が日常的に発生しています。

―トピック 3―

脆弱性情報の取扱いに関するガイドラインの ISO/IEC への提案

ISO/IEC JTC-1/SC27 の WG3（小委員会）において、策定作業中の、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「脆弱性情報開示 (Vulnerability Disclosure)」に加え、新たな標準化作業項目として「脆弱性取扱いプロセス」に関するガイドラインの策定が提案され、2 月に、国際投票に付されました。国際投票での承認を経て、今後は、製品やサービスの提供者が脆弱性について、外部とやり取りする情報を規定する「脆弱性情報開示」と内部での対応プロセスを規定する「脆弱性取扱いプロセス」の 2 つの標準化作業が併行して進むことになります。これらの標準化作業に JPCERT/CC も参加し、脆弱性情報の取扱いに関する知見や国内で整備された文書などを参考資料として提供するなどの貢献を行いました。

―トピック 4―

制御システム・セキュリティカンファレンス開催

2 月 10 日、東京（品川）で第 3 回 制御システム・セキュリティカンファレンスを開催しました。前年度の 3 倍にあたる参加定員 300 人の会場はほぼ満席となり、制御システムのセキュリティ対策への関心の高まりが感じられました。昨年確認された「Stuxnet」による制御システムへの攻撃が、制御システム業界の環境や事業者の意識の変化を引き起こしているものと考えられます。今年度のカンファレンスでは、制御システム担当者から見た Stuxnet の詳細や、この 1 年間における制御システム・セキュリティ関連の話題のアップデート、インシデントからの回復フェーズにおける課題の整理などの多様なテーマで、講演、パネルディスカッションが行われました。
JPCERT/CC では、引き続き、この分野の課題への取組みと情報発信を強化していく予定です。

制御システムセキュリティカンファレンス 2011
https://www.jpcert.or.jp/ics/conference2011.html

―トピック 5 ―

JPCERT/CC が APCERT 議長チームに

アジア太平洋地域に所在する CSIRT からなるコミュニティ「APCERT」（Asia Pacific Computer Emergency Response Team）の年次総会及び関連会合が、3 月 21 日から 25 日まで、韓国済州島において開催されました。

APCERT の運営方針等を決定する運営委員の一部改選、議長チーム・副議長チームの選出、事務局チームの選任のために行われた選挙において、JPCERT/CC は、運営委員に再選されるとともに、議長チームに選出されました。また、事務局チームとしての活動も継続することになりました（JPCERT/CC は、2003 年 2 月の APCERT 発足時から、運営委員及び事務局として継続的に APCERT の円滑な業務の推進に貢献してきています。）。

今後は、議長チームとして、APCERT のミッションであるアジア太平洋地域におけるインターネット環境の安全性向上にさらなる貢献を行うべく、様々な活動を積極的に提案・実施していく予定です。

APCERT
http://www.apcert.org/index.html

JPCERT CC®

—活動概要—

目次

本活動は、経済産業省より委託を受け、「平成２２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、「平成２２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、「2-4-3.C/C++セキュアコーディング出張セミナー」、「7.講演活動一覧」及び「8.執筆・取材記事一覧」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. インシデント対応支援

JPCERT/CC が本四半期に受け付けた、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、報告件数ベースで 1936 件、インシデント件数ベースでは 1883 件でした(注 1)。

> 【注 1】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。また、「インシデント件数」は、各報告に含まれるインシデントの件数の合計を示します。ただし、1 つのインシデントに関して複数の報告が寄せられた場合には 1 件のインシデントとして扱います。

JPCERT/CC が国内外のインシデントに関連するサイトとの調整を行った件数は 596 件でした。前四半期の 731 件と比較して 18%減少しています。「調整」とは、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などに対し、現状の調査や問題解決のための対応を依頼する活動です。

JPCERT/CC は、国際的な調整・支援が必要となるインシデントにおいて、日本の窓口組織として、国内や国外 (海外の CSIRT など) の関係機関と調整活動を行っています。この活動を通じて、インシデントの認知と対処、インシデントによる被害拡大の抑止に貢献しています。

インシデント報告対応活動の詳細については、別紙「JPCERT/CC インシデント報告対応レポート」をご参照ください。

JPCERT/CC インシデント報告対応レポート
https://www.jpcert.or.jp/pr/2011/IR_Report20110412.pdf

1-1-1. インシデントの傾向

本四半期に報告を頂いたフィッシングサイトの件数は、405 件で、前四半期の 538 件から 25%減少しました。また、前年度同四半期（373 件）との比較では、9%の増加となっています。
本四半期のフィッシングサイトが装っていたブランドの国内・国外別の内訳を[表 1-1] に示します。

[表 1-1: フィッシングサイトの国内・国外ブランド別の件数]

フィッシングサイト	1 月	2 月	3 月	国内外別合計（割合）
国内ブランド	24	29	31	84(21%)
国外ブランド	77	94	76	247(61%)
ブランド不明	21	24	29	74(18%)
月別合計	122	147	136	405(100%)

本四半期は、前四半期のような特定ブランドのフィッシングサイト報告ではなく、様々な国外ブランドのフィッシングサイト報告を多数いただいたため、国外ブランドを装ったフィッシングサイトの件数が 247 件と、前四半期の 202 件から 22 % 増加しました。なお、国内のブランドを装ったフィッシングサイトの件数は、84 件と、前四半期の 284 件から大幅に減少しています。

本四半期のフィッシングサイトの調整先は、国内が 61%、国外が 39%でした。前四半期の割合（国内 53%、国外 47%）と比較して、本四半期は国内への調整が増えました。これは、前述の報告いただいた様々な国外ブランドのフィッシングサイトの多くが国内に設置されていたためです。

本四半期に報告が寄せられた Web サイト改ざんの件数は、49 件でした。前四半期の 199 件から 75%減少しています。これは、いわゆる Gumblar による Web サイト改ざんに関する報告が、11 月頃から減少したためです。いわゆる Gumblar の報告減少については、前四半期に引き続き一部の亜種の攻撃がおさまってきていることや、世間での注目度が下がっていることが一因になっていると考えられます。
いわゆる Gumblar については、報告件数は減少傾向にありますが、前四半期にあった Internet Explorer の未修正(現在は修正済み)の脆弱性を悪用した攻撃や、Java の脆弱性を悪用するような脅威度の高い攻撃が発生する可能性があるため、JPCERT/CC では、引き続き攻撃の分析や動向調査を行っています。

Web サイト改ざん等のインシデントを認知された場合は、JPCERT/CC にご報告ください。
JPCERT/CC では、当該案件に関して攻撃元への対応依頼等の必要な調整を行うとともに、同様の被害の拡大を抑えるため、攻撃方法の変化や対策を分析し、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。

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

JPCERT/CC のホームページや、RSS、約 25,000 名の登録者を擁するメーリングリストなどを通じて、本四半期においては、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ついて、次のような注意喚起情報を発行しました。

発行件数：9 件　https://www.jpcert.or.jp/at/

2011-01-12　2011 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
2011-02-08　主に UNIX / Linux 系サーバを対象としたインターネット公開サーバのセキュリティ設定に関する注意喚起に関する注意喚起
2011-02-09　2011 年 2 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起
2011-02-09　Adobe Flash Player の脆弱性に関する注意喚起
2011-02-09　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起
2011-02-15　2011 年 2 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起 (更新)
2011-02-17　2011 年 2 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起 (更新)
2011-03-09　2011 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
2011-03-22　Adobe Flash Player および Adobe Reader / Acrobat の脆弱性に関する注意喚起

1-2-1-2. Weekly Report

JPCERT/CC が収集し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　https://www.jpcert.or.jp/wr/

Weekly Report で扱った情報セキュリティ関連情報の項目数は、合計 91 件、「今週のひとくちメモ」のコーナーで紹介した情報は、次の 12 件でした。

2011-01-13　Thunderbird 3.0 のサポート終了
2011-01-19　DNSSEC の導入と運用の検討
2011-01-26　Windows DLL プリロード問題の対策ガイダンス
2011-02-02　情報セキュリティ月間
2011-02-09　IN-ADDR.ARPA ゾーンの管理形態の更新
2011-02-16　Windows 7 SP1 および 2008 R2 SP1 のリリースについて
2011-02-23　セキュリティアップデートの適用確認の勧め
2011-03-02　組織の連絡窓口の運用体制を確認する
2011-03-09　担当ノート: 制御システムセキュリティと制御システムセキュリティカンファレンス
2011-03-16　東北地方太平洋沖地震
2011-03-24　Cisco 3 月定例バンドル公開延期
2011-03-30　日本標準時の標準電波送信所の停波について

1-2-1-3. 早期警戒活動事例

本四半期における早期警戒活動事例のいくつかを以下に紹介します。

1) 震災や原発事故に乗じた標的型攻撃への対応

JPCERT/CC では、3 月 11 日の東日本大震災発生の数日後に、震災や原子力発電所の事故に関連する言葉をメールの件名や添付ファイル名に使用した標的型攻撃に関する報告を受けました。これらの攻撃の一部に、Adobe 製品の未修正の脆弱性を使用するマルウエアを確認したため、国内重要インフラ組織等に早期警戒情報の提供を行いました。また、マルウエア感染による被害を低減させるため、マルウエアを解析して得られた結果に基づき、マルウエアが通信する先のサイトを管理する ISP 及び関係する CSIRT に対してサイトの停止を依頼し、依頼の翌日に当該サイトの停止を確認しました。

2) DDoS 攻撃または攻撃予告への対応

本四半期も、国内外の政府サイトや民間サイトなどを標的とした DDoS 攻撃や攻撃予告が発生しました。

1 月下旬に、韓国の掲示板サイトに日本の掲示板サイト等への DDoS 攻撃予告 (攻撃予定日は 2 月 11 日) が書き込まれたことを受け、JPCERT/CC では、KrCERT/CC 等の海外関連組織と情報連携して攻撃予告に関する情報収集を行うとともに、攻撃範囲が拡大した場合に備えて緊急対応体制をとりました。幸い、本事案については、攻撃に向けた動きが攻撃予定日までに沈静化したこともあり、実際の攻撃は発生しませんでした。

また、3 月上旬には、主に韓国の政府系サイトを対象とした DDoS 攻撃が発生しました。この攻撃は、マルウエアに感染した多数のコンピュータが指令サイトからの指令を受けて行ったものでしたが、この攻撃に使用された指令サイトやマルウエアに感染したコンピュータの一部が日本国内に存在していたため、KrCERT/CC からの依頼に基づき、関係サイトの管理者や ISP 各社に対し、攻撃の停止ための対応を依頼しました。加えて、国内重要インフラ組織等に対し、参考情報の提供を行いました。

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 ページ等でも公開しています。

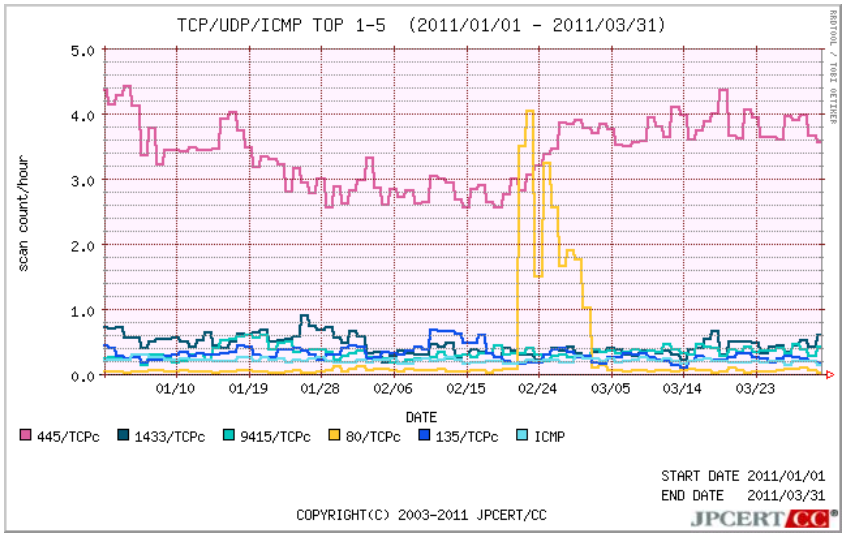
1-3-1. ポートスキャン概況

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
https://www.jpcert.or.jp/isdas/readme.html

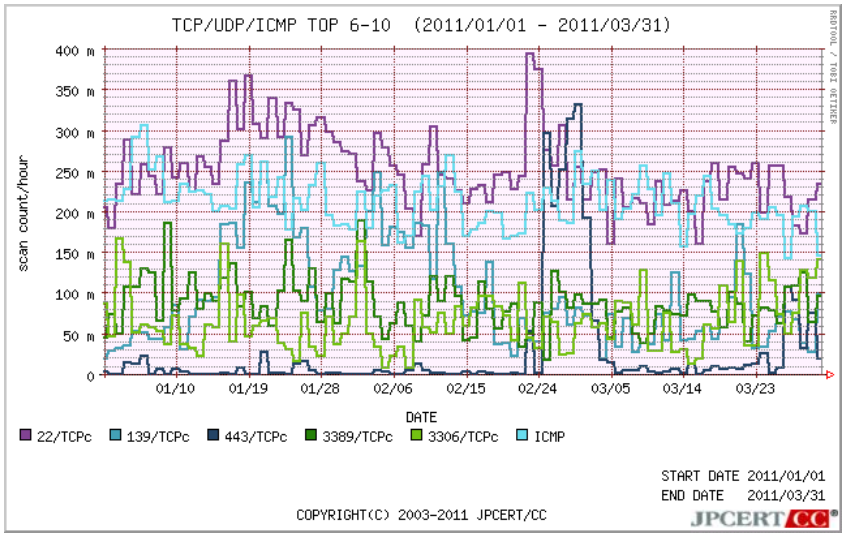
本四半期に ISDAS で観測されたアクセスの宛先ポートの上位 1 位～5 位および 6 位～10 位のそれぞれについて、アクセス数の時間的の推移を[図 1-1]と[図 1-2]に示します。

- アクセス先ポート別グラフ top1-5 (2011 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]

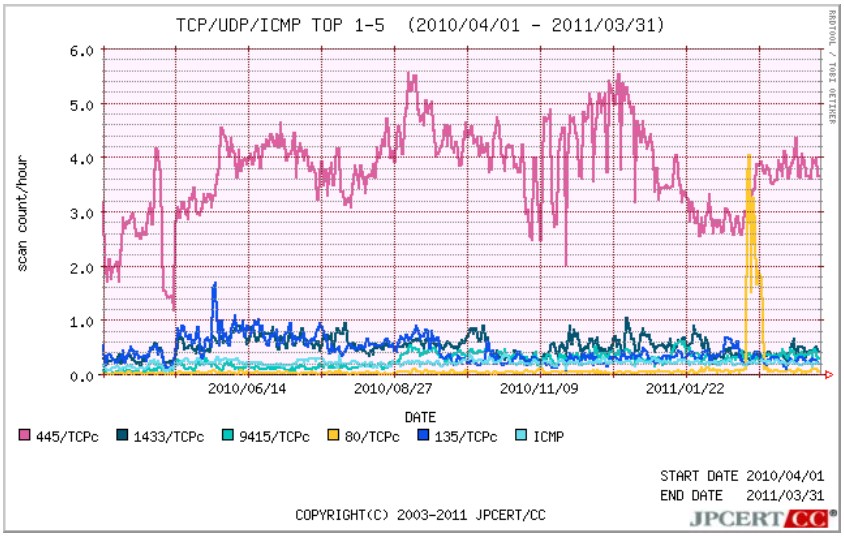
- アクセス先ポート別グラフ top6-10 (2011 年 1 月 1 日-3 月 31 日)



[図 1-2：アクセス先ポート別グラフ top6-10]

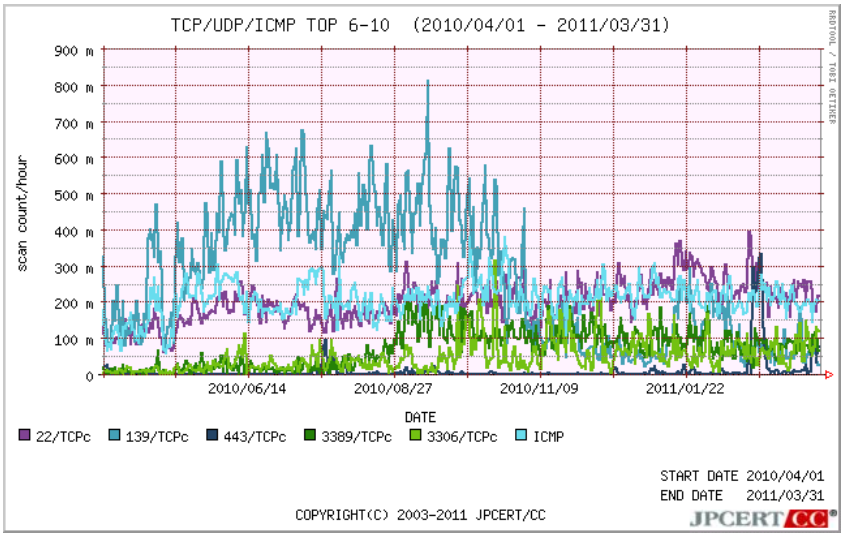
また、より長期間のスキャン推移を見るため、2010 年 4 月 1 日から 2011 年 3 月 31 日までの期間における、アクセスの宛先ポートの上位 1 位～5 位および 6 位～10 位のそれぞれについて、アクセス数の時間的の推移を[図 1-3]と[図 1-4]に示します。

- アクセス先ポート別グラフ top1-5 (2010 年 4 月 1 日-2011 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 (2010 年 4 月 1 日-2011 年 3 月 31 日)



[図 1-4: アクセス先ポート別グラフ top6-10]

本四半期においては、2 月下旬に、Port 80/443 など主にサービスで使用しているポートを対象としたパケットが観測されました。これらは、主にミャンマーの IP アドレスを詐称しており、短時間に多数送信されていました。ただし、これらは Web サーバなどの提供中のインターネットサービスに対する Syn-flood 攻撃自体が本来の目的では無く、応答したパケットがミャンマーに送信されることをねらったものであると考えられます。

そのほか、引き続き、Windows や Windows 上で動作するソフトウエアへの Scan 活動や、Telnet、SSH サーバやターミナルサービスなどコンピュータを遠隔操作で使う場合にサーバ側が待ち受けているポートへの Scan 活動が観測されています。OS やアプリケーションについて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、強固な認証方法を使っているか、今一度確認することが重要です。

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) が互いに協調し連携して共通の問題を解決する場として設立された日本シーサート協議会（Nippon CSIRT Association: NCA）の事務局として、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、メーリングリストの管理等の活動を行っています。
本四半期に新たに 3 組織が加盟し、今期末時点で 19 の CSIRT が参加しています。不定期に開催されている 6 つの WG をはじめとする定常的な活動に加えて、本四半期は、2010 年 12 月に開催した国際連携ワークショップの概要やその様子などをまとめた参加レポートを公開しました。
また、2011 年 2 月には CSIRT についての啓発資料「What's CSIRT ~CSIRT のススメ~」を一般に公開しました。これは、CSIRT 構築を検討している段階の国内組織向けに作成されたパンフレットで、CSIRT の基本的考え方やサービス内容、利点などが一覧できるよう記載されています。「What's CSIRT ～CSIRT のススメ～」に関する詳細は、次の URL をご参照ください。

What's CSIRT ～CSIRT のススメ～
http://www.nca.gr.jp/imgs/CSIRT.pdf

日本シーサート協議会の活動の詳細については、次の 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/

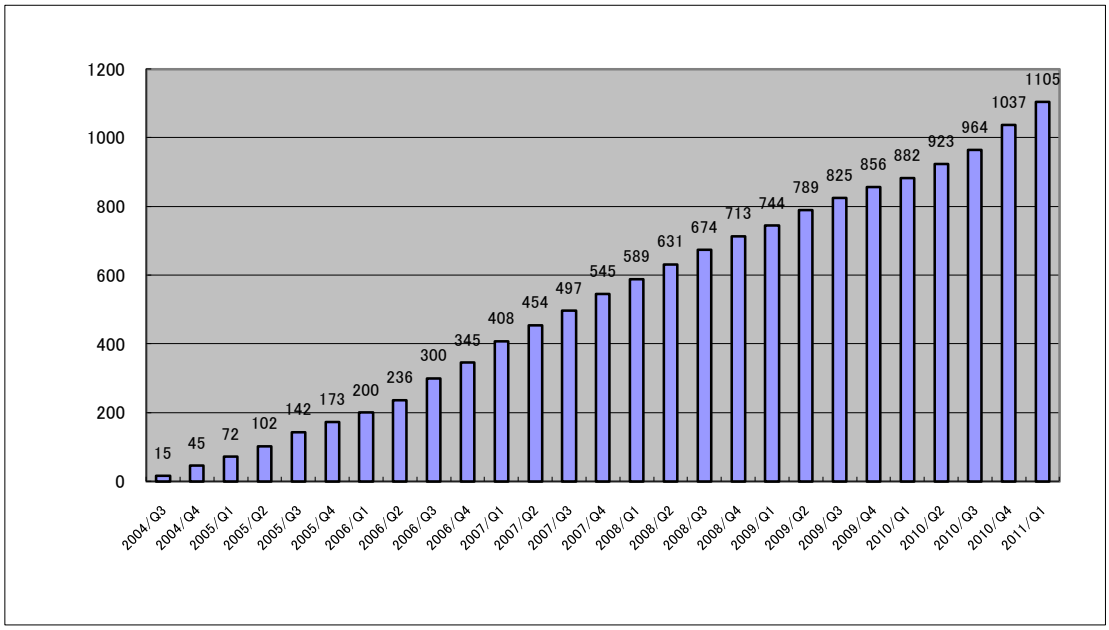
2. 脆弱性関連情報流通促進活動

JPCERT/CC は、ソフトウエア製品利用者の安全確保を図ることを目的として、発見された脆弱性情報を適切な範囲に適時に開示して製品開発者による対策を促進し、用意された対策情報と脆弱性情報を脆弱性情報ポータル JVN (Japan Vulnerability Notes：独立行政法人情報処理推進機構（IPA）との共同運営) に公表することで広く注意喚起を行う活動を行っています。さらに、脆弱性を作りこまないためのセキュアコーディングの普及や、制御システムの脆弱性の問題にも取り組んでいます。

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

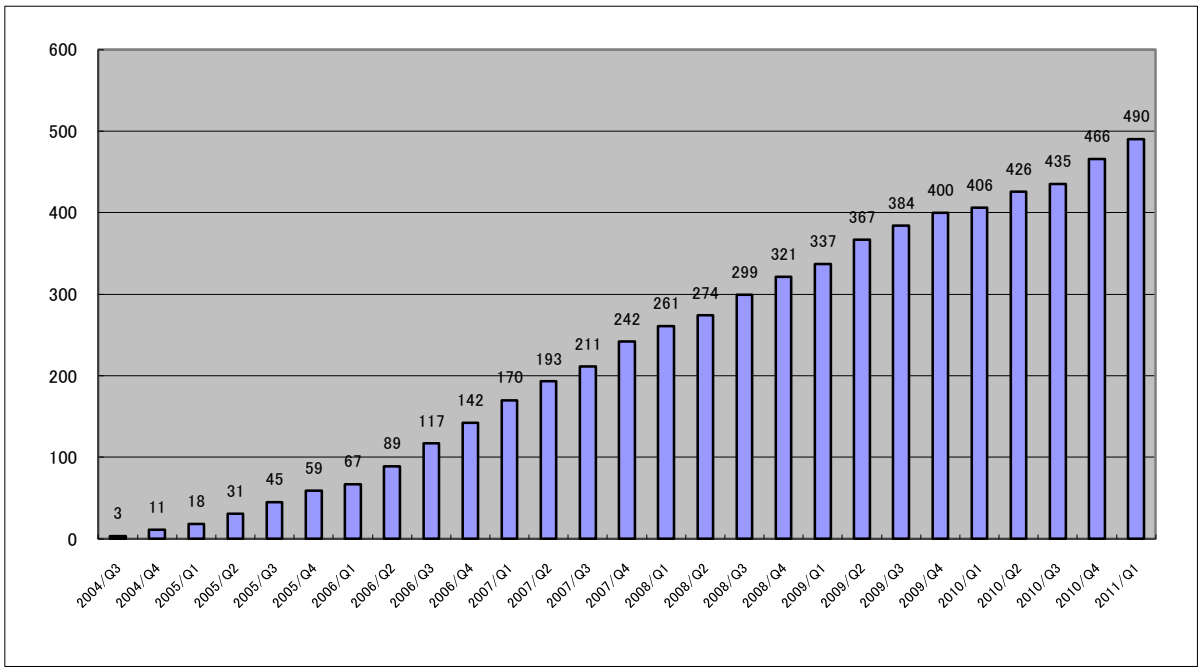
JPCERT/CC は、経済産業省告示「ソフトウエア等脆弱性情報取扱基準」（以下「本基準」といいます。）において、製品開発者とのコーディネーションを行う「調整機関」に指定されており、本基準を踏まえてとりまとめられた「情報セキュリティ早期警戒パートナーシップガイドライン」に詳述された調整機関の役割を担う活動を行っています。

本四半期に JVN において公開した脆弱性情報は 68 件(累計 1105 件) [図 2-1] でした。本四半期に公開された個々の脆弱性情報に関しては、JVN(https://jvn.jp/)をご覧ください。



[図 2-1: 累計 JVN 公開累積件数]

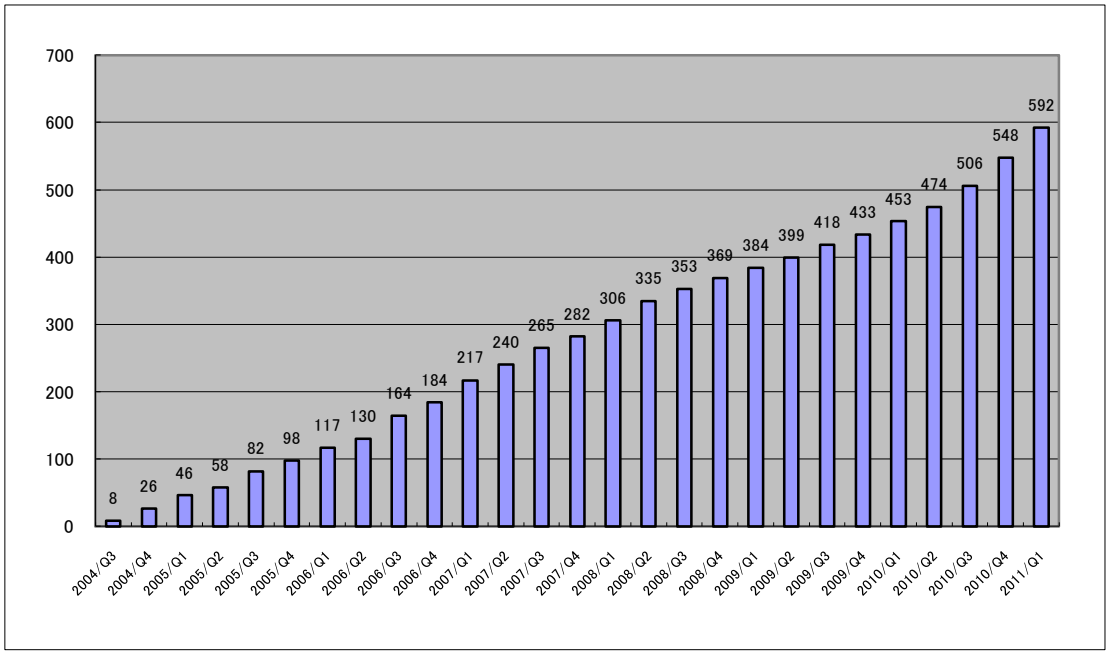
このうち、本基準に従って調整を行い、JVN で公開した脆弱性情報は 24 件(累計 490 件) [図 2-2] でした。本四半期に JVN にて公開された案件の約半数の 15 件が海外製品開発者の製品であり、本枠組みに基づく JPCERT/CC の調整活動が海外の開発者にも浸透してきていると考えられます。また、本四半期は、製品開発者自身による自社製品に関する脆弱性の届出が 5 件あり、JVN での公開が非常に速やかに行われたことも、本四半期の JVN 公開件数に影響していると言えます。以上から、国内外ともに、製品開発者による脆弱性問題への取り組みが前向きに行われている傾向にあると言えます。



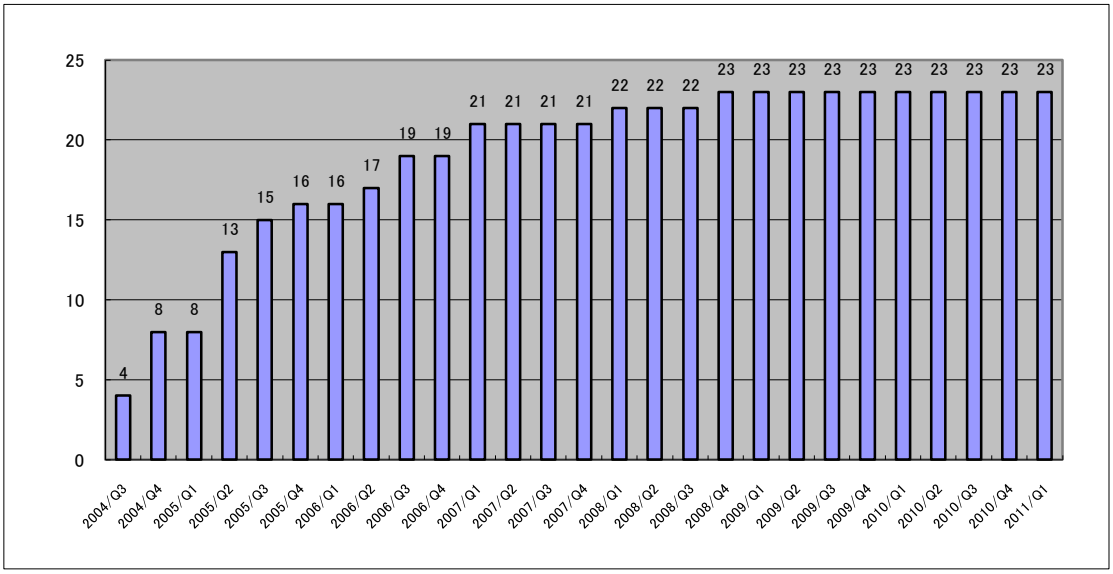
[図 2-2: 累計 JVN_JP(JVN#)公開累積件数]

また、CERT/CC とのパートナーシップに基づいて調整を行い、JVN において公開した脆弱性情報は 44 件(累計 592 件) [図 2-3]でした。本四半期中に公開された脆弱性情報の中には、Microsoft 製品に関するものが 7 件、Apple 製品に関するものが 7 件、Adobe 製品に関するものが 3 件、ISC に関するものが 2 件ありました。この他、本四半期は、制御系製品に関する脆弱性情報が 7 件と多く公開されたことが特徴的でした。これは、米国 The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) からの公開件数の増加の影響です。

なお、英国 CPNI とのパートナーシップに基づいて調整を行い、JVN にて公開した脆弱性情報は 0 件(累計 23 件) [図 2-4] でした。



[図 2-3: VN_CERT/CC(JVNVU#および JVNTA)公開累積件数]



[図 2-4: 累計 VN_CPNI(CPNI) 公開累積件数]

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 は、国内のみならず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、同じ国際調整機関である米国 CERT/CC、英国 CPNI、フィンランド CERT-FI などの海外 CSIRT と協力関係を結び、それぞれが報告を受けた脆弱性情報の共有、各国の製品開発者への情報通知、各国製品開発者の対応状況の集約、脆弱性情報の公開時期の設定などの連携した調整活動を行っています。

また、2008 年 5 月 21 日から運用を開始した JVN 英語版サイト(https://jvn.jp/en)へのアクセス数も徐々に増加しており、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ていることがうかがえます。昨今は、海外の組織から公開されるアドバイザリの多くが、JVN 英語版サイトへのリンクを掲載しています。

JPCERT/CCは、JVN上で公開する脆弱性情報に対して、2008年8月から個別に米国MITRE社への申請を行ってCVE (Common Vulnerabilities and Exposures) 番号を取得してきましたが、2010年6月23日に、米国MITRE社より、CNA（CVE Numbering Authorities、CVE採番機関）に認定されたことに伴い、自ら、よりタイムリにCVE番号を採番できることになりました。本四半期は、24件の脆弱性情報についてCVEを採番し、JVNに掲載しました。2008年にCVEの採番を開始して以降、約95%の案件に対しCVE番号が付与されています。
CNA および CVE に関する詳細は、次の URL をご参照ください。

News & Events “JPCERT/CC Becomes CVE Numbering Authority”
https://cve.mitre.org/news/index.html#jun232010a
CVE Numbering Authorities
https://cve.mitre.org/cve/cna.html
About CVE
https://cve.mitre.org/about/index.html

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
https://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
https://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(2010 年版)
https://www.jpcert.or.jp/vh/partnership_guide2010.pdf
JPCERT/CC 脆弱性情報取り扱いガイドライン
https://www.jpcert.or.jp/vh/vul-guideline2010.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

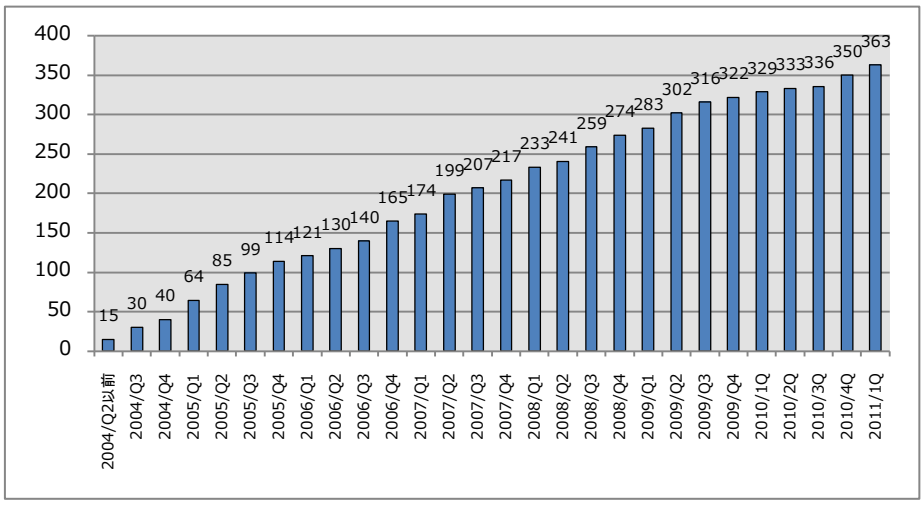
本基準では、受付機関に独立行政法人情報処理推進機構（以下「IPA」といいます。http://www.ipa.go.jp/)、調整機関に JPCERT/CC が指定されています。JPCERT/CC は IPA が受け付けた届出情報の転送を受けて、製品開発者への情報提供を行い、対策情報公開に至るまでの調整を行っています。最終的には、 IPA と共同で、脆弱性情報ポータル JVN において対策情報を公開しています。両組織間においては緊密な情報の交換、脆弱性情報の分析等を行っています。なお、本基準における IPA の活動および四半期毎の届出状況については、次の URL をご参照ください。

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求められています。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、[図 2-5]に示すとおり、2011 年 3 月 31 日現在で 363 社となっています。

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



[図 2-5:累計製品開発者登録数]

また、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、IPA が主催する脆弱性研究会にて検討が行われ、その結果を反映した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定版が 2011 年 3 月 28 日に公表されま

した。これを受け、JPCERT/CC では、JPCERT 脆弱性関連情報取扱いガイドラインについて、具体的な運用手順を盛り込むための改訂を行い、2011 年 3 月 31 日に公開しました。

2-3-3. 製品開発者との定期ミーティングの実施

JPCERT/CCでは、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報ハンドリング業務に関する製品開発者との意見交換、また製品開発者間の情報交換を目的として、脆弱性情報ハンドリングにご協力いただいている製品開発者の皆様とのミーティングを定期的に開催しております。
本四半期は 2011 年 3 月 25 日にミーティングを開催し、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および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. 「脆弱性情報開示」の国際標準化活動への参加

ISO/IEC JTC-1/SC27 の WG3 において進められている、脆弱性情報の取扱いおよび開示に関する国際標準の策定作業に引き続き参加しました。

まず、脆弱性情報の取扱い手順(Vulnerability Handling Process)の標準化については、2010 年 10 月にベルリンで開催された ISO/IEC JTC-1/SC27 の国際会議(半年ごとに各地を持ち回り開催)での結論を受けて、2010 年 11 月に新作業項目提案(New Work Item Proposal)が発行され、2 月上旬までに参加各国が投票を行うことになっていました。この新作業項目は、既に標準化作業が始まって 4 年近くになる「脆弱性開示(Vulnerability Disclosure)」から分離されたもので、脆弱性に関する情報を入手した際に製品開発者が行うべき手順を規定します。外部から見たふるまいに関する標準と、内部での取扱いに関する標準とが対になって策定と普及されることになります。本提案に対し、JPCERT/CC から情報処理学会規格調査会 SC27WG3 小委員会に提案し、審議を経たうえで、同会を通じて、標準化作業の開始に日本として賛成する投票が行われました。投票結果は、総投票数 38 ヶ国に対して、賛成が 24 ヶ国、反対が 2 ヶ国(蘭豪)、棄権が 12 ヶ国でした。

次に、製品開発者による脆弱性関連情報の受取と発信の方法を示したガイドラインである「脆弱性情報開示」(29147 ; Vulnerability Disclosure (VD) ; 旧称 Responsible Vulnerability Disclosure)については、2010 年 10 月にベルリンで開催された会議での合意に基づいてエディタが改訂を行った第 2 次委員会草案(CD: Committee Draft)が、2010 年 12 月に参加各国に送付されており、3 月上旬までに賛否の投票を行うことになっていました。これに対しては、JPCERT/CC から情報処理学会規格調査会 SC27WG3 小委員会に提案し、審議を経たうえで、同会を通じて、委員会草案から次の段階に進めることに日本として反対する投票を、40 項目以上の修正提案を添えて行っていただきました。投票結果は、総投票数 35 ヶ国に対して、現状のまま承認が 12 ヶ国、修正コメント付き承認が 3 ヶ国、反対が 4 ヶ国(日本のほか米英豪)、棄権が 16 ヶ国でした。

脆弱性の取扱いに関連して 2 つの標準開発が併行して進められることとなりそうですが、JPCERT/CC では、SC27 国際会議への参加ならびに日本の標準化組織である情報規格調査会を通じて、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. 札幌で「C/C++セキュアコーディングセミナー」を開催

1 月 27 日、28 日の 2 日間にわたり、札幌市内において C/C++セキュアコーディングセミナーを開催しました。

本セミナーは、今年度、福岡、大阪、名古屋と主要都市にて開催してきたところですが、今年度最後の開催地である札幌においても、多くの参加者の方に熱心にご聴講いただきました。

講義内容としては、「part1. セキュアコーディング概論・文字列」と「part2. 整数・コードレビュー」の 2 つのコースを 2 日間で実施しました。
「part1. セキュアコーディング概論・文字列」は、受講者にセキュアコーディングの必要性や重要性の理解を促す「セキュアコーディング概論」にはじまり、C/C++言語における「文字列」の脆弱性に関する講義、その講義内容について受講者の理解を深めるための「演習」という構成で実施しました。「part2. 整数・コードレビュー」は、C/C++言語における「整数」の脆弱性に関する講義とその内容に関する「演習」、最後にこれらのセミナーで学んだ知識を総動員し、脆弱性を抱えたサンプルコードを受講者自らがレビューして修正方法を考える「セキュリティコードレビュー」という構成で実施しました。

受講者アンケートでは継続して開催を望む声を多くいただきました。

2-4-2. C/C++セキュアコーディングセミナー@東京 Part6 ROSE

脆弱性を作り込まないプログラミング手法に関する「C/C++セキュアコーディングセミナー@東京」を 8 月から開催しています。2 月 24 日、3 月 3 日には静的コード解析ツール「ROSE」に関するセミナーを開催いたしました。

オープンソースのコンパイラフレームワークである ROSE は、ソースコードを解析し、その結果得られた抽象構文木(AST)に対して様々な処理を行うための仕組みを提供する、C++言語で記述された API です。セミナーでは、ROSE をはじめとする開発ツール一式があらかじめインストールされた仮想イメージ（VMWare/Virtualbox）を使用し、第 3 回のセミナーでも紹介した「CERT C セキュアコーディングスタンダード」のルールに違反したコードを検知するツール「rosecheckers」

の使い方やルールの違反を検出するチェッカーの実装例、脆弱なコードを検出する際の課題等について解説しました。C/C++セキュアコーディングセミナーの開催概要等については、次の URL をご参照ください。

イベント情報：https://www.jpcert.or.jp/event/

2-4-3. C/C++セキュアコーディング 出張セミナー

JPCERT/CC では、C/C++言語を使用した開発を行う企業・組織を対象に、C/C++セキュアコーディングに関する出張セミナー(有償)のご要望を承っています。マネジメント層へのセキュリティ啓発や新人研修のメニュー等としてもご利用いただいています。本四半期は、国内大手メーカ 2 社に対し、計 2 回の出張セミナーを実施しました。
出張セミナーのご依頼、お問合わせは、secure-coding@jpcert.or.jp までご連絡下さい。

2-4-4. CERT C セキュアコーディングスタンダード日本語版に新カテゴリーを追加

C 言語を用いたセキュアコーディングを実践する上で、プログラマがリファレンスとして利用できるようまとめられたコーディング規約集である CERT C セキュアコーディングスタンダードに、新たなカテゴリー「並行性 (concurrrency)」に関するルールとレコメンデーションを追加して、1 月 11 日に公開しました。本スタンダードは、これにより、16 のカテゴリーを持つことになりました。CERT C セキュアコーディングスタンダードの詳細については、次の URL をご参照ください。

CERT C セキュアコーディングスタンダード日本語版
https://www.jpcert.or.jp/sc-rules/

2-4-5. C/C++セキュアコーディングセミナー資料 2010 年度版を公開

2010 年度に開催した C/C++ セキュアコーディングセミナーで使用した以下の講義資料（2010 年度版）を 3 月 31 日に公開しました。

- 文字列
- 整数
- CERT C セキュアコーディングスタンダード
- 動的メモリ管理
- 書式指定文字列
- Working with rosecheckers

C/C++言語でのソフトウェア開発に携わるプログラマ、プロジェクトマネージャ、コードレビュアー、品質管理担当者、プログラマ・エンジニアの教育担当者の方々はぜひご利用ください。公開資料については、以下の URL をご参照ください。

C/C++ セキュアコーディングセミナー資料
https://www.jpcert.or.jp/research/materials.html

2-5. 制御システムセキュリティに関する啓発活動

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 2 月 10 日に東京（品川）で開催いたしました。3 回目となる今回は、Stuxnet に端を発した迫りくる脅威への危機感の高まりを重要な環境変化ととらえ、「現実化した脅威とその対策課題」をテーマに、組織的・体制的領域、技術的領域、および運用上の領域に潜む多くの課題について、「改善」「防御」「回復」の各視点から具体的な施策を見出すことを目的に開催いたしました。
午前に行われた第一部では、第二部への前段として、制御システムセキュリティに関するこの一年の動向と Stuxnet のあらましを JPCERT/CC から報告し、続く午後からの第二部では、前述の３つの視点ごとに、国内外のユーザー、開発者、ベンダーによる講演、並びに講演者等によるパネルディスカッションを行いました。
今年度は、前年度の 3 倍となる 300 名を参加定員といたしましたが、会場はほぼ満席となり、また講演ごとの質疑も活発に行われ、制御システムのセキュリティに対する関心が非常に高くなってきたことが伺われ、全日程は成功裏に終了いたしました。

プログラム等の詳細については、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 2011
https://www.jpcert.or.jp/ics/conference2011.html
制御システムセキュリティカンファレンス 2011 においての講演資料
https://www.jpcert.or.jp/present/#year2011

2-5-2. セキュリティ・アセスメント・ツールの調査

前四半期に引き続いて準備を進め、2 月 28 日から、制御システム用セキュリティ・アセスメント・ツールの関係者への提供を開始しました。
準備段階においては、SICE/JEITA/JEMIMA 合同 WG（ワーキンググループ）の活動の一環として、評価対象とする仮想的な制御システム（モデルシステム）を設定して考察する手法により、英国 CPNI が開発した SSAT に関し、JPCERT/CC による邦訳版の試用と意見交換を行いました。合同 WG の成果については、前述の制御システムセキュリティカンファレンスにおいて合同 WG の代

表から発表され、SSAT を効果的に利用することで先のモデルシステムのセキュリティがどのように改善できるかが報告されました。JPCERT/CC は、この邦訳版の試用を通じて SSAT の適用に係る知見を得るとともに、翻訳ミスや用語の統一、その他の問題点についてこのツールの改善を行ないました。併せて合同 WG 参加者の意見、要望を SSAT に反映した改良を行い、「日本版 SSAT」として提供を開始しました。提供開始から 1 月が経過した 3 月 31 日現在、既に 54 件のお申込みをいただいております。

日本版 SSAT についての詳細および試用申込みについては、以下の URL をご参照ください。

制御システム関連ツール
日本版 SSAT(Scada Self Assessment Tool)
https://www.jpcert.or.jp/ics/ssat.html

2-5-3. 制御システム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隔月で配信しています。本四半期は 1 月 28 日、2 月 28 日（号外）、3 月 31 日にそれぞれ配信いたしました。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、JPCERT/CC からのお知らせとともに掲載しています。また、「制御システム脅威事例」として、本四半期は、合わせて 8 件の脆弱性情報を掲載しました。このニュースレターは、制御システム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、次の URL をご参照ください。

制御システムセキュリティ情報共有タスクフォース
https://www.jpcert.or.jp/ics/taskforce.html

このタスクフォースは、当初「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」として発足いたしましたが、本四半期より制御システムユーザー、制御製品ベンダー、制御システムベンダー、システムインテグレーター、研究者まで対象を広げ、より多くの関係者との情報共有の場として、その役割を担う一歩を踏み出しました。
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。

2-5-4. 関連学界活動

ほぼ毎月開かれている SICE (計測自動制御学会)、JEITA（電子情報技術産業協会）、JEMIMA (日本電気計測器工業会)による合同セキュリティ検討 WG（ワーキンググループ）の活動に参加し、制御システムのセキュリティに関し、制御システムの専門の方々と意見交換を行いました。本四

半期は主として、前述のセキュリティ・アセスメント・ツール、日本版 SSAT の普及活動を行いました。

2-6　VRDA フィードによる脆弱性情報の配信

JPCERT/CC は、大規模組織の組織内 CSIRT などでの利用を想定して、KENIGINE などのツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST (National Institute of Standards and Technology)の NVD (National Vulnerability Database) を外部データソースとして利用した、VRDA (Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を、2010 年 6 月より行っています。VRDA フィードについての詳しい情報は、以下の URL を参照下さい。

VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

本四半期に配信した VRDA フィード配信件数のデータソース別の内訳、言語別の VRDA フィードの利用傾向をそれぞれ[表 2-1]と[表 2-2]に示します。[表 2-1]では、言語別に VRDA フィードインデックス（Atom フィード）と、脆弱性情報（脆弱性の詳細情報）の利用数を示します。VRDA フィードインデックスは、個別の脆弱性情報のタイトルと脆弱性の影響を受ける製品の識別子（CPE）を含みます。また、[表 2-2]では、HTML と XML の二つのデータ形式で提供している脆弱性情報について、データ形式別の利用割合を示しています。

[表 2-1: VRDA フィード配信件数]

2011 年 1 月～3 月			年度累計
MyJVN API	NVD	計	
583 件	1186 件	1769 件	5659 件

[表 2-2: 言語別 VRDA フィード利用傾向]

言語	VRDA フィードインデックスの利用数	脆弱性情報の利用数	脆弱性情報のデータ形式別利用割合	
			HTML	XML
日本語版	59,055(66,221)	31,665(18,567)	97%(97%)	(3%)
英語版	3,900(3,366)	12,472(15,585)	94%(93%)	6%(7%)

（括弧内の数値は前四半期）

[表 2-1]に示したように、前四半期から VRDA フィードインデックスの利用数に大きな変化は見られませんが、脆弱性情報の利用数については、日本語版と英語版がおおよそ半々であった前四半期とは異なり、日本語版の利用数が英語版を大きく上回りました。これは、前四半期と比較し

て、英語版の利用数は変化が無かったのに対して、日本語版の利用数が 70%程度増加したことに起因しています。脆弱性情報のデータ形式別利用傾向は、両言語版ともに HTML 形式の利用が圧倒的に多く、XML 形式で表現された脆弱性情報の利用は限られているという傾向に変化はありませんでした。

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ました。また、効率的なボット解析手法の検討や、さらには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いました。

2006 年 12 月に活動を開始したボット対策プロジェクトは、本年度をもって終了いたしました。プロジェクトの終了に先立ち、2007 年 2 月に開始した注意喚起活動が 1 月末をもって終了し、注意喚起対象者への CCC クリーナーの提供も 2 月末をもって終了しました。総務省・経済産業省連携プロジェクトとしてのボット対策プロジェクトは終了いたしましたが、プロジェクトの参加組織はこれまでと同じ志のもと、それぞれの立場でボット対策を継続して推進していきます。JPCERT/CC は、入手したボットプログラムの解析を通して得られた情報をもとに攻撃元等へのコーディネーションを実施する等、今後も活動を継続していく予定です。

このプロジェクトの毎月の活動実績が「サイバークリーンセンター活動実績」として公開されていますので、他のアーカイブ情報と併せ、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/
2011 年 1 月度 サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/201101/1101monthly.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

海外の National CSIRT (Computer Security Incident Response Team) 等に対し、トレーニングやイベントでの講演等を通して CSIRT の構築・運用支援活動を行い、各国のインシデント対応調整能力の向上に協力するとともに、各国 National CSIRT 等と JPCERT/CC との間の相互信頼と連携の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

AOTS による「情報セキュリティ研修コース　～CSIRT 研修指導者育成～」への協力(2011 年 1 月 19 日-28 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 研修指導者育成～」のプログラムディレクター及び講師を 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 ヶ国から、計 26 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管理職/スタッフ) を日本に招聘し、各国において CSIRT 構築の研修を行うリーダー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。
研修では、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、マルウエア解析、Web サイト脆弱性の理解、ネットワーク定点観測脅威情報に関する高度分析・連携、より効果的な技術演習の手法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、富士通株式会社の館林システムセンターおよび日本 IBM 株式会社の東京セキュリティ・オペレーション・センターを訪問し、システム運用やセキュリティオペレーションの先端事例について見学と意見交換をしました。

4-1-2. その他地域における活動

アフリカでの CSIRT 構築支援活動
JPCERT/CC は、多くの国が CSIRT 構築を検討している段階にあるアフリカ大陸において、Internet Summit of Africa や Afrinic などのアフリカ各国の技術者が集う会合で CSIRT 構築のためのトレーニングを行う等、アフリカ諸国の全体的なセキュリティ対策レベルの向上を図る取組みに協力しています。
本四半期は、メーリングリストでの議論を通じて、アフリカでの CSIRT 構築支援のためのトレーニングマテリアル作成などに協力しました。

4-2. 国際 CSIRT 間連携

インシデント対応に関する海外の National CSIRT との間の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。また、アジア太平洋地域の CSIRT の協力連携の枠組みである APCERT (Asia Pacific Computer Emergency Response Team)や、インシデント対応組織による世界的なフォーラムである FIRST (Forum of Incident Response and Security Teams) に参加し、主導的な役割を担うなど、多国間の CSIRT 連携の取組にも積極的に参画しています。

4-2-1. アジア太平洋地域における活動

4-2-1-1. APCERT 年次総会 2011 への参加(2011 年 3 月 22 日-24 日)

アジア太平洋地域の CSIRT コミュニティである APCERT の年次総会が韓国の済州島で開催され、JPCERT/CC を含め 19 の加盟チームが参加しました(2011 年 3 月末現在、18 経済地域から 27 チームが加盟しています。)。会合の概要は、以下のとおりです。

1)日程：3/22(火)　午前：APCERT 戦略策定会議(Strategic Planning Meeting)
　　午後：APCERT ステアリングコミッティー(運営委員会)
　　3/23(水)　午前：APCERT 年次総会(Annual GeneralMeeting)
　　午後：APCERT カンファレンス（限定公開）
　　3/24(木)　終日：APCERT カンファレンス（一般公開）
2)場所：Lotte Hotel Jeju, 済州島, 韓国
3)概要：APCERT 年次総会は、各経済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・研究活動などを共有することを目的に、毎年開催されています。
本年度の年次総会では、組織運営のビジョンについて、JPCERT/CC の提案をたたき台として討議が重ねられ、“APCERT will work to create a safe, clean and reliable cyber space in the Asia Pacific region through global collaboration”として共有されました。APCERT の目標が、加盟チーム相互の連携構築にとどまらず、アジア太平洋地域の情報セキュリティ向上への寄与にあることが確認されたものです。このビジョンのもとで、4 つのワーキンググループの新設、他組織・他地域との連携強化や各チームが実施しているプロジェクトの APCERT 内への展開をはじめ、様々な活動が実施されていくことになります。

また、ステアリングコミッティー(運営委員会)のメンバーの一部改選が行われ、JPCERT/CC が再選されました（任期は 2013 年 3 月まで)。さらに、APCERT 議長チームが改選され、JPCERT/CC が選任されました（任期は 2012 年 3 月まで)。これにより、JPCERT/CC は、1 年の間、APCERT の代表として様々な活動をリードすることとなりました。

[図 4-1: APCERT 年次総会集合写真]

4-2-1-2. TSUBAME ネットワークモニタリングワークショップの開催(2011 年 3 月 25 日)

JPCERT/CC は、アジア太平洋地域の CSIRT を対象として、APCERT 年次総会に連続する日程で、「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連携を目的として、各地域のインターネット上にセンサーを配置し、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の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す。APCERT のワーキンググループ活動の一つとして位置づけられており、JPCERT/CC は、このプロジェクトの設置を提案した組織として、運営を主導しています。
本ワークショップでは、TSUBAME プロジェクトメンバを対象に、ネットワークモニタリングの事例や TSUBAME システムの新機能の紹介を行いました。またプロジェクトメンバ間でディスカッションを行い、システムの機能を活用する等により、プロジェクトメンバ間における分析結果の共有等の連携を強化することを確認しました。

4-2-1-3. APCERT 合同サイバー演習 (APCERT Drill 2011) に参加 (2011 年 2 月 22 日)

APCERT は、サイバー攻撃への即時対応能力を確認するため、2 月下旬に、合同サイバー演習を実施しました。本演習は、アジア太平洋地域で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て、毎年実施されています。今回で 8 度目となる APCERT の合同サイバー演習は、5 つのタイムゾーンにわたるエリアで約 4 時間にわたり行われました。
JPCERT/CC は、この演習にプレーヤー(演習者)として参画するとともに、ExCon と呼ばれる演習の進行調整役にも加わり、スムーズな演習の実施を支えました。

4-2-1-4. APSTAR Retreat に参加 (2011 年 2 月 20 日)

APSTAR Retreat は、APNIC、APTLD、 APIA などのアジアパシフィック地域の関連団体が集まる国際会議です。JPCERT/CC は本会合に参加し、アフリカにおける CSIRT 構築支援活動などの紹介を通して、アジアのインターネット社会がアフリカの発展に貢献することの意義を説明しました。

4-2-1-5. 中国語圏における情報収集発信

中国語圏（中国／台湾）経済区域の情報セキュリティ関係会議やセキュリティチームの活動に参加し、セキュリティ関連情報の収集や現地セキュリティ専門家との情報交換を行いました。収集した情報は、日本国内の関係者会合などで積極的に展開しています。また、現地におけるセキュリティ対策の推進やセキュリティ意識の向上に協力する観点から、日本におけるセキュリティ対策の取組等を紹介する講演や記事掲載等を行いました。

1) 1 月 18 日 「2010 中国互联网产业年会」参加
2) 3 月 11 日 台湾國際電子商務安全研討會
講演：Building a Better E-Commerce Environment
3) 3 月 29 日 台湾網際網路趨勢研討會
講演：”Cyber Clean Center”
4) 3 月号 雑誌「中国信息安全」2011 年第 12 期
記事タイトル：”日本的信息安全政策”

4-2-2. その他の地域における活動

4-2-2-1. BlackHat DC 2011 への参加(2011 年 1 月 16 日-22 日)

アメリカのワシントン DC で開催された BlackHat DC 2011 に参加しました。近年利用が広がっているクラウドサービスを利用した並列処理による暗号解析の手法の発表などが行われていました。

4-2-2-2. RSA Conference 2011 への参加(2011 年 2 月 15 日-16 日)

米国のサンフランシスコで 2 月中旬に開催された RSA Conference 2011 に参加し、講演やパネルディスカッションを通して、最新の脅威に関するトピックスや暗号技術の動向に関する情報を収集しました。また、米国の CSIRT や関連団体(APWG、Cloud Security Alliance)等との円滑な連携の継続のため、各チームの近況等に関する情報交換を行いました。

4-2-2-3. CansecWest への参加(2011 年 3 月 8 日-13 日)

カナダのバンクーバーで開催されたセキュリティカンファレンス CansecWest に参加し、情報収集を行いました。本カンファレンスでは Pwn2Own と呼ばれる、新しい脆弱性の発見コンテストがあり、本年もスマートフォンの脆弱性が明らかとなりました。JPCERT/CC は脆弱性調整機関

の立場から脆弱性発見者やそのコミュニティとの連携を図っています。

4-2-3. ブログや Twitter を通した情報発信の強化

英語ブログ(blog.jpcert.or.jp)や Twitter(twitter.com/jpcert_en)を利用し、日本の情報セキュリティに関する状況や JPCERT/CC の活動等について海外にアピールするための活動を行いました。

[図 4-2:ブログ記事の例]

たとえば 3 月 11 日の東日本大震災に乗じて、英語で書かれた義援金募集サイトのフィッシングサイトなどが発見された件については、これらによって被害を受けるのが主に英語圏のインターネットユーザであることから、英語版ブログで注意を呼びかけました。

英語版 Twitter では、海外における震災関係の報道の状況も踏まえ、震災直後から、インシデント対応調整や脆弱性関連情報調整、情報収集分析等の National-CSIRT 機能が平常時と同様に機能していることを海外向けてアピールするため、JPCERT/CC の業務が通常どおり継続されている状況をリアルタイムに発信しました。

震災直後から、JPCERT/CC には、諸外国の CSIRT や関連機関からお見舞いと各種協力の申し出が多数寄せられました。この場を借りて国内の皆様に御紹介するとともに、各国 CSIRT、関連機関の皆様に謝意を表させていただきます。

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
https://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 の他のメンバ及び FISRT の詳細については、次の URL をご参照ください。

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

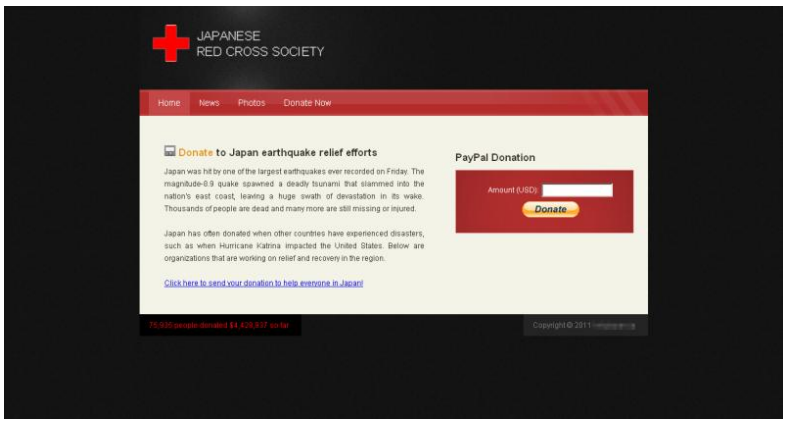
5. フィッシング対策協議会事務局の運営

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（以下、本章において「協議会」といいます。）の事務局として、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フィッシング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. 情報収集/発信の実績

協議会では、協議会 Web ページや会員向け ML により、フィッシングに関するニュースや緊急情報を 15 件発信しました。

本四半期には、東北地方太平洋沖地震に便乗して、被災地への義援金募集を騙ったフィッシングサイトが発見されました。協議会では、日本赤十字社と情報連携を通じて、フィッシングサイトであることを確認し、3 月 18 日に緊急情報として公開するとともに、JPCERT/CC のインシデント対応チームにフィッシングサイトの停止調整を依頼した結果、同日、23 時に当該フィッシングサイトの停止を確認しました。



[図 5-1:日本赤十字社を騙るフィッシングサイト
https://www.antiphishing.jp/news/alert/2011318.html]

また、この他、フィッシングの動向や新対策技術に関する有識者インタビュー記事を協議会 Web ページに 3 件掲載したほか、会員向けに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。

5-2. フィッシングサイト URL 情報を提供する対象会員の拡大

協議会では、フィッシング対策ツールバーなどを提供している事業者やウイルス対策ソフトベンダである会員のうち登録した者に対し、協議会に報告されるフィッシングサイトの URL のリストを、日に数回提供しています。提供した URL 情報をブラックリストに追加していただく等、ユーザ保護に向けた取組みに活用していただくことを目的としています。本四半期から、新たにアルプス システム インテグレーション株式会社 (2011 年 2 月より)、独立行政法人情報通信研究機構 (2011 年 2 月より)の 2 社(法人)にも提供を開始しました。これにより協議会が情報を提供している事業者等は合計で 11 社となりました。現在も複数の事業者との間で情報提供に関する協議を行っており、提供先を順次拡大していく予定です。

5-3. 協議会会員を対象とした勉強会を開催

協議会会員を対象としたフィッシング対策勉強会を、1 月 12 日（第二回勉強会）と 2 月 25 日（第三回勉強会）に開催しました。第 2 回勉強会はフィッシング対策関連製品・ソリューション等を提供しているベンダーの技術を事業者の方に紹介する場として、第 3 回勉強会は携帯向け迷惑メールの現状やフィッシングメールに対する対策についての会員間での情報交換の場として、それぞれ開催しました。各勉強会のプログラムは、次のとおりです。

フィッシング対策協議会 第２回情報共有勉強会 2011 年 1 月 12 日（水）15:00 - 18:25
発表 1　15:00-15:25　「電子メール配信における S/MIME 電子署名付与」 株式会社 HDE 宮本 和明 氏
発表 2　15:25-15:50 株式会社セキュアブレイン 田辺　潤一 氏
発表 3　15:50-16:15　「登録画像の再認によるユーザ認証とサーバ認証の同時確立」 株式会社ニーモニックセキュリティ 國米　仁 氏
発表 4　16:15-16:40　「IT 革命とパスワード管理ソフトの最新動向」 有限会社ストーンズインターナショナル　兼 （米)Siber Systems 社 日本担当　石田　公孝 氏
発表 5　16:45-17:10　「MITM 攻撃および MITB 攻撃防御機能つき IOTP 認証システム （IOTP：Infinite One-Time Password)」 日本ユニシス株式会社　八津川　直伸 氏
発表 6　17:10-17:35　「フィッシング対策製品選定例」 株式会社日立情報システムズ　白鳥　悦正 氏
発表 7　17:35-18:00　「最新オンライン犯罪に対する RSA の対策ソリューション」 EMC ジャパン株式会社　水村 明博 氏
発表 8　18:00-18:25　「最大の検出率を可能にするアンチウイルスソフト」 G DATA Software 株式会社 瀧本 往人 氏 / 河合　雄一郎 氏

フィッシング対策協議会 第３回情報共有勉強会 2011 年 2 月 25 日（金）13:00 - 15:00
講演 1　13:00-14:00　「携帯宛迷惑メールの現状とその対策について」 KDDI 株式会社 プラットフォーム開発本部 au one プラットフォーム開発部 開発 4 グループリーダ 本間輝彰 氏
講演 1　14:00-15:00　「企業に求められるフィッシングメール対策」 トッパン・フォームズ株式会社 企画本部 Web 開発部 E メールグループ マネージャ 加藤孝浩 氏

5-4.　講演活動

本四半期に協議会として以下の講演を行いました。

1)　小宮山 功一朗「増加するフィッシング詐欺　今、何ができるのか」
　　埼玉県コンピュータネットワーク防犯連絡協議会,2011 年 2 月 28 日

2) 山本 健太郎「増加するフィッシング詐欺　今、何ができるのか」
日本クレジット協会セキュリティ研究部会, 2011 年 3 月 7 日
3) 瀬古 敏智「増加するフィッシング詐欺　今、何ができるのか」
電子メールセキュリティーセミナー in 熊本, 2011 年 3 月 8 日

5-5. フィッシング対策協議会の活動実績の公開

協議会の Web サイトにおいて、毎月の活動報告として「フィッシング対策協議会への報告件数」などを公開しています。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 2011 年 1 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/20111.html
フィッシング対策協議会 2011 年 2 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/20112.html
フィッシング対策協議会 2011 年 3 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/20113.html

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. セキュリティ対策講座「電子メールソフトのセキュリティ設定について」PDF 版の公開

2010 年 12 月に HTML 形式で公開した啓発用資料「電子メールソフトのセキュリティ設定について」に関し、印刷配布等がし易いように PDF 版を作成し、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」(2011 年 2 月 8 日)
https://www.jpcert.or.jp/magazine/security/mail/mailsec.html

6-2. 制御システムカンファレンス 2011 の講演資料公開

2011 年 2 月 10 日にコクヨホール(東京)において開催した「制御システムカンファレンス 2011」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 2011 の講演資料　(2011 年 2 月 18 日)
https://www.jpcert.or.jp/present/

6-3. フィールドレポート「インドネシア National CSIRT Id-SIRTII に聞く マルウエアラボの設立の意義とその活動」の公開

JPCERT/CC が連携している海外組織の活動や海外のセキュリティ動向などを日本のセキュリティ関係者にも知っていただくことを目的に「フィールドレポート：海外セキュリティ関連機関・組織の動向」のコーナーを JPCERT/CC の Web サイト上に設けています。本四半期は、「インドネシア National CSIRT Id-SIRTII に聞く、マルウエアラボの設立の意義とその活動」を公開しました。インドネシアの National CSIRT である Id-SIRTII におけるマルウエアラボの立上げ経緯と活動計画について紹介しています。

インドネシア National CSIRT Id-SIRTII に聞く　マルウエアラボの設立の意義とその活動
(2011 年 2 月 21 日)
https://www.jpcert.or.jp/magazine/security/field-id.html

6-4. C/C++ セキュアコーディングセミナー2010 年度講義資料の公開

2010 年度に実施した 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を公開しました。

C/C++セキュアコーディングセミナー講義資料　(2011 年 3 月 31 日)
https://www.jpcert.or.jp/research/materials.html

※本資料の詳細は、「2-4-5」をご参照ください。

7. 講演活動一覧

(1) 戸田 洋三 (情報流通対策グループ リードアナリスト) :
「職業的情報学Ⅰ」
千葉大学理学部数学 数理情報学科,2011 年 1 月 13 日

(2) 真鍋 敬士(理事, 分析センター長), 村上 晃(分析センター マネージャ),村上 憲二(総務部部長)
「情報セキュリティ対策研修(基本編、応用編、事例編)」
国立保健医療科学院情報セキュリティ対策研修,2011 年 1 月 24 日

(3) 宮地 利雄 (理事) :
「制御システム・セキュリティ 2010 年度動向報告」

パネルディスカッション「現実化した脅威と対策課題」
制御システムセキュリティカンファレンス 2011,2011 年 2 月 10 日

(4) 小熊 信孝(情報流通対策グループ 制御システムセキュリティ) :
「Stuxnet - 制御システムを狙った初のマルウエア」
制御システムセキュリティカンファレンス 2011,2011 年 2 月 10 日

(5) 早貸 淳子(常務理事) :
「情報セキュリティ担当者専門研修」
法務省 平成２２年度 情報セキュリティ担当者専門研修,2011 年 2 月 25 日

(6) 久保 啓司(早期警戒グループ リーダ 情報セキュリティアナリスト) :
「JPCERT/CC の紹介 Web サイト経由で感染するマルウエアインデント対応の視点から」
LASDEC,2011 年 2 月 28 日

(7) 小宮山 功一朗(国際部マネージャ, 早期警戒グループ リーダ 情報セキュリティアナリスト) :
「増加するフィッシング詐欺 今、何が出来るのか」
埼玉県コンピュータ・ネットワーク防犯連絡協議会サイバーセキュリティ・カレッジ
第 11 回ネットワークセキュリティセミナー,2011 年 2 月 28 日

(8) 山本 健太郎(早期警戒グループ 情報セキュリティアナリスト) :
「増加するフィッシング詐欺 今、何が出来るのか」
日本クレジット協会 平成 22 年度第 7 回カードセキュリティ研究部会,2011 年 3 月 7 日

(9) Jack YS Lin(早期警戒グループ 情報セキュリティアナリスト) :
「中国のオンライン犯罪状況」
日本クレジット協会 平成 22 年度第 7 回カードセキュリティ研究部会,2011 年 3 月 7 日

(10) 村上 晃(分析センター マネージャ)
「組織内 CSIRT(シーサート)について」
日本クレジット協会 平成 22 年度第 7 回カードセキュリティ研究部会,2011 年 3 月 7 日

(11) 久保 啓司(早期警戒グループ リーダ 情報セキュリティアナリスト) :
「JPCERT/CC の紹介 Web サイト経由で感染するマルウエアインデント対応の視点から」
第 17 回 NORTH インターネット・シンポジウム 2011,2011 年 3 月 7 日

(12) 瀬古 敏智(フィッシング対策協議会,早期警戒グループ 情報セキュリティアナリスト) :
「増加するフィッシング詐欺 今、何が出来るのか」
電子メールセキュリティセミナーin 熊本 2011,2011 年 3 月 8 日

(13) Jack YS Lin(早期警戒グループ 情報セキュリティアナリスト) :
「Building a Better E-Commerce Environment in Japan」
2011 電子商務安全國際研討會－台湾,2011 年 3 月 11 日

(14) Jack YS Lin(早期警戒グループ 情報セキュリティアナリスト) :
「JPCERT/CC Status Report」
TWNIC 2011 網際網路趨勢研討會－台湾,2011 年 3 月 29 日

8. 執筆・取材記事一覧

(1) 歌代 和正(代表理事)：
「状況の周知と利用を 関係者の責任は重大に」
日本情報産業新聞,2011 年 1 月 1 日

(2) 中尾 真二(事業推進基盤グループ 広報)：
「NIC と連携して効果的なドメイン停止―中国フィッシング対策事情」
フィッシング対策協議会 インタビュー,2011 年 1 月 11 日

(3) 中尾 真二(事業推進基盤グループ 広報)：
「脅威のレイヤが上位にシフトし対策が困難に―トレンドマイクロ」
フィッシング対策協議会 インタビュー,2011 年 2 月 7 日

(4) Jack YS Lin(早期警戒グループ 情報セキュリティアナリスト)：
「日本信息安全政策(日本情報セキュリティ政策)」
中国信息安全测评中心 中国信息安全 2011 年第 12 期,2011 年 3 月

(5) 中尾 真二(事業推進基盤グループ 広報)：
「被害事例や件数などネガティブ情報も隠さない―ヤフー」
フィッシング対策協議会 インタビュー,2011 年 3 月 7 日

(6) 小宮山 功一朗(フィッシング対策協議会)
「ミネラルウォーター詐欺・フィッシング詐欺特集」
日本テレビ news every., 2011 年 3 月 31 日

9. 開催セミナー等一覧

(1) C/C++ セキュアコーディングセミナー2010@札幌
※本セミナーの詳細は、「2-4-1」をご参照ください。

(2) C/C++ セキュアコーディングセミナー2010@東京 part6 ROSE
※本セミナーの詳細は、「2-4-2」をご参照ください。

(3) C/C++ セキュアコーディング出張セミナー
※本セミナーの詳細は、「2-4-3」をご参照ください。

(4) 制御システムセキュリティカンファレンス2011
※本セミナーの詳細は、「2-5-1」をご参照ください。

10. 後援・協力一覧

(1) HOSTING-PRO 2011（主催：HOSTING-PRO 2011 実行委員会） 2011 年 3 月 3 日

■ インシデントの対応依頼、情報のご提供：info@jpcert.or.jp
https://www.jpcert.or.jp/form/

PGP Fingerprint ： FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4 69EC E048

■ 脆弱性情報ハンドリングに関するお問い合わせ ：vultures@jpcert.or.jp

■ 制御システムセキュリティに関するお問い合わせ ：cs-security-staff@jpcert.or.jp

■ セキュアコーディングセミナーのお問い合わせ ：secure-coding@jpcert.or.jp

■ 公開資料、講演依頼、その他のお問い合わせ ：office@jpcert.or.jp