JPCERT CC®

JPCERT-PR-2010-0004
発行日 : 2010-10-07

JPCERT/CC 活動概要 [2010 年 7 月 1 日 ～ 2010 年 9 月 30 日]

【活動概要トピックス】

—トピック 1 —
ACID—ASEAN 加盟国および周辺各国・地域による合同サイバーインシデント演習に参加

ACID（ASEAN CERT Incident Drill）は、国境を越えて発生するサイバーセキュリティインシデントに備え、ASEAN（東南アジア諸国連合）加盟国および近隣の各国・地域の CSIRT 間の連携の強化を図ることを目的に毎年実施されているサイバーインシデント演習です。今回が 5 度目の実施となるこの ACID は、日本、オーストラリア、ブルネイ、中国、インド、インドネシア、韓国、マレーシア、ミャンマー、ノルウェー、フィリピン、シンガポール、タイ、ベトナムの 14 か国から、15 チームが参加して行われました。
本年は、シンガポールの National CSIRT である SingCERT の主導により、ボットネットによる大規模なセキュリティインシデントを想定したシナリオに基づき、マルウエアの動作を解析し、漏洩した情報の追跡を行うなど、迅速なインシデント調査および各国との連携によるインシデント対応の能力の向上を目標とした、実践的な演習が行われました。

—トピック 2 —
継続的な人材育成活動—文部科学省 先導的 IT スペシャリスト育成推進プログラム への協力

IT Keys (IT specialist program to promote Key Engineers as security Specialists:
(奈良先端科学技術大学院大学，大阪大学，京都大学，北陸先端科学技術大学院大学))及び ISS スクエア（研究と実務融合による高度情報セキュリティ人材育成プログラム: (情報セキュリティ大学院大学，中央大学，東京大学)）は、いずれも文部科学省「先導的 IT スペシャリスト育成推進プログラム」として実施されているプログラムです。
JPCERT/CC は、本年度も、IT Keys について、同プログラムにおける実地演習に協力するボット対策推進事業（サイバークリーンセンタープロジェクト）の参加機関の一つとして、「リスクマネジメント演習」の静的分析演習を中心に、教材となる検体を使ったボット分析の実地演習の指導を

行いました。この実地演習は、プログラム終了後のアンケートにおいて、非常に高い評価を得ることができました。また、ISS スクエアについては、プログラム参加校から 2 名のインターンを受け入れ、マルウエアの分析作業やソフトウェアの脆弱性情報の取り扱いについて、実践的な業務の体験してもらいました。

JPCERT CC®

—活動概要—

目次

本活動概要に記載した事業内容は、経済産業省より「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)」事業における“不正アクセス行為対策業務”及び“フィッシング対策協議会事務局の運営”として委託を受けて実施したものです。
なお、「2-4-3.C/C++セキュアコーディング出張セミナー」、「2-4-4.開発者向けウェブマガジン」「**7.講演活動一覧**」及び「**8.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 2,441 件、インシデント件数ベースでは 2,761 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 701 件でした。前四半期の 847 件と比較して約 17%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/2010/IR_Report20101007.pdf

1-1-1. インシデントの傾向

本四半期は、「フィッシングサイト」の報告が多く寄せられました。本四半期に報告が寄せられたフィッシングサイトの件数は、487 件で、前四半期の 388 件から約 25%増加しました。また、前年度同四半期（303 件）との比較では、約 61%の増加となっています。これらフィッシングサイトの国内・国外ブランド別の内訳を以下に示します。

[表　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	7 月	8 月	9 月	国内外別合計（割合）
国内ブランド	74	101	103	278 (57%)
国外ブランド	38	44	41	123 (25%)
国内外の別不明	13	30	43	86 (18%)
月別合計	125	175	187	487(100%)

本四半期は、国内ブランドを装ったフィッシングサイトの件数が 278 件と、前四半期の 157 件から大幅に増加しました。この増加は、国内のポータルサイトを装ったフィッシングサイトの増加によるものです。なお、国外のブランドを装ったフィッシングサイトの件数は、123 件と、前四半期の 186 件から減少しています。

本四半期のフィッシングサイトにおける調整先については、国内が 62%、国外が 38%でした。前四半期の割合（国内 55%、国外 45%）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、前述の国内ポータルサイトを装った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、353 件でした。前四半期の 561 件から約 37%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の件数が減少したためですが、前年度同四半期（2009 年 7 月から 9 月まで）における Web 改ざんの報告件数が 28 件であったことに鑑みれば、いまだに多数の報告が寄せられている状況にあります。このことからも、Web サイト改ざんの攻撃が常態化していると考えられますので、引き続き OS やアプリケーションの修正プログラムの適用を励行してください。

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。

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 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、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：8 件 https://www.jpcert.or.jp/at/

2010-09-21 Adobe Flash Player の脆弱性に関する注意喚起 (公開)
2010-09-15 2010 年 9 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起 (公開)
2010-08-20 Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 (公開)
2010-08-11 Adobe Flash Player の脆弱性に関する注意喚起 (公開)
2010-08-11 2010 年 8 月 Microsoft セキュリティ情報 (緊急 8 件含) に関する注意喚起 (公開)
2010-08-03 Windows シェルの脆弱性 (MS10-046) に関する注意喚起 (公開)
2010-07-14 2010 年 7 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起 (公開)
2010-07-14 Windows のヘルプとサポートセンターの未修正の脆弱性に関する注意喚起 (更新)

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：13 件　https://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 83 件、「今週のひとくちメモ」のコーナーで紹介した情報は 13 件でした。

1-2-2. 脅威の動向について

前期に引き続き、いわゆる Gumblar ウイルスや、SQL インジェクション攻撃によるコンテンツ改ざんなど Web サイト訪問者に対する PC への攻撃活動が続いています。ブラウザのアドオンにも注意し、Adobe Flash や Acrobat、Oracle Java などの脆弱性修正が行われた場合は早々に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。同時に未修正の脆弱性に対するワークアラウンドの実施などもあわせて検討してください。

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
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 (2010 年 7 月 1 日-9 月 30 日)

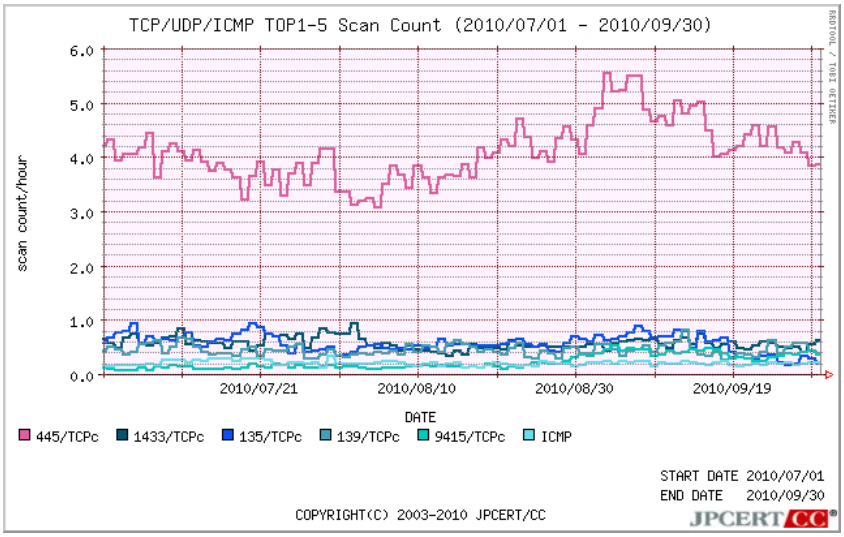


図 1-1：アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2010 年 7 月 1 日-9 月 30 日)

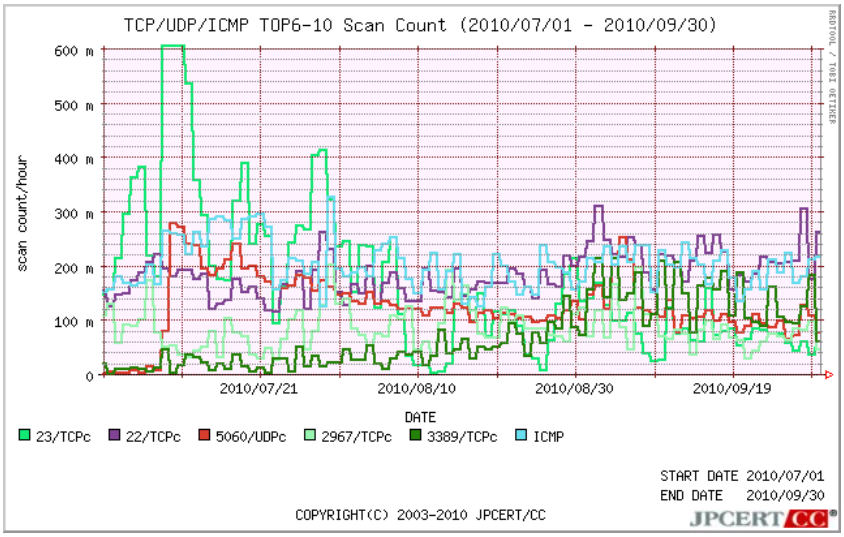


図 1-2：アクセス先ポート別グラフ top6-10

また、より長期間のスキャン推移を見るため、2009 年 7 月 1 日から 2010 年 9 月 30 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 10 月 1 日-2010 年 9 月 30 日)

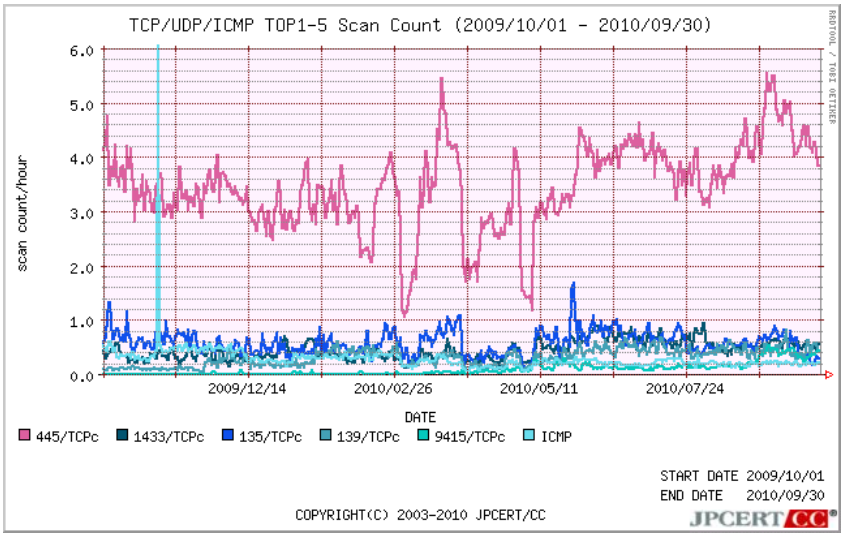


図 1-3: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2009 年 10 月 1 日-2010 年 9 月 30 日)

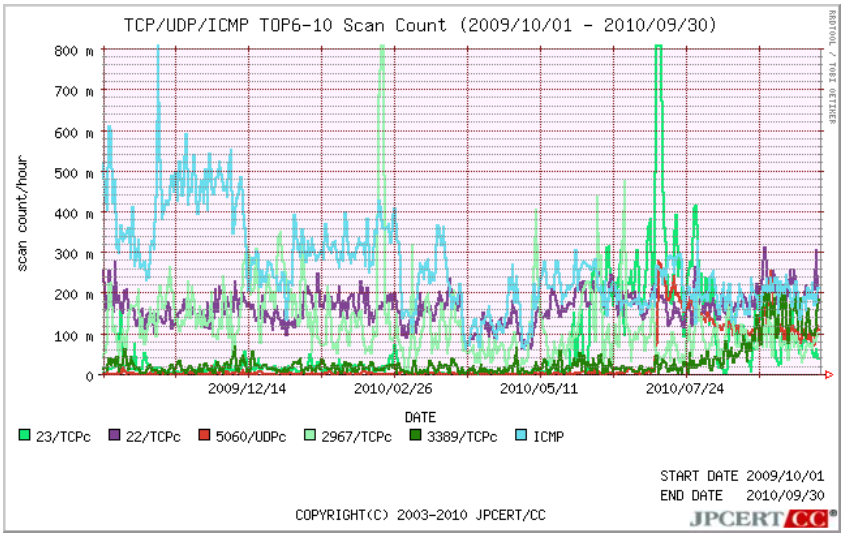


図 1-4: アクセス先ポート別グラフ top6-10

引き続き Windows や Windows 上で動作するソフトウエアへの Scan 活動に加え、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ポートへの Scan 活動が増えています。旧知の脆弱性が対策されていないサーバや、弱い認証方法を使っているサーバ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、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。
2010 年 8 月に日本シーサート協議会の第 4 回総会が開催され、新規加入 CSIRT チームの紹介や各 WG の活動概要の報告などが行われました。総会後の WG 会では、各チームの CSIRT 活動報告や、具体的なインシデント対応方法や実際の作業で得られた注意点などに関する議論が行われました。

日本シーサート協議会の活動の詳細については、以下の URL をご参照ください。

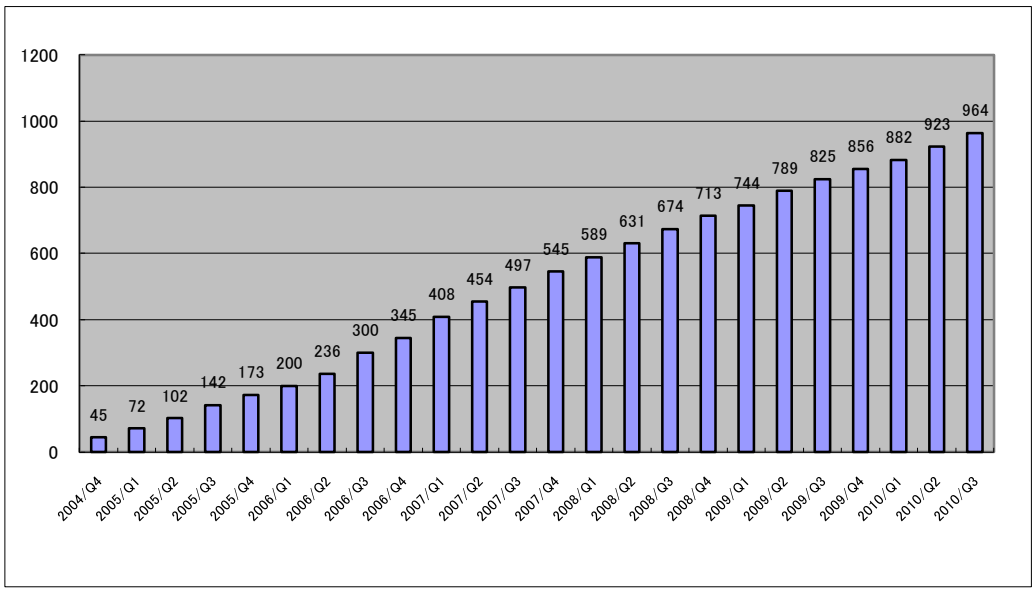
日本シーサート協議会 Web ページ
http://www.nca.gr.jp/

2. 脆弱性関連情報流通促進活動

JPCERT/CC 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) に公開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。

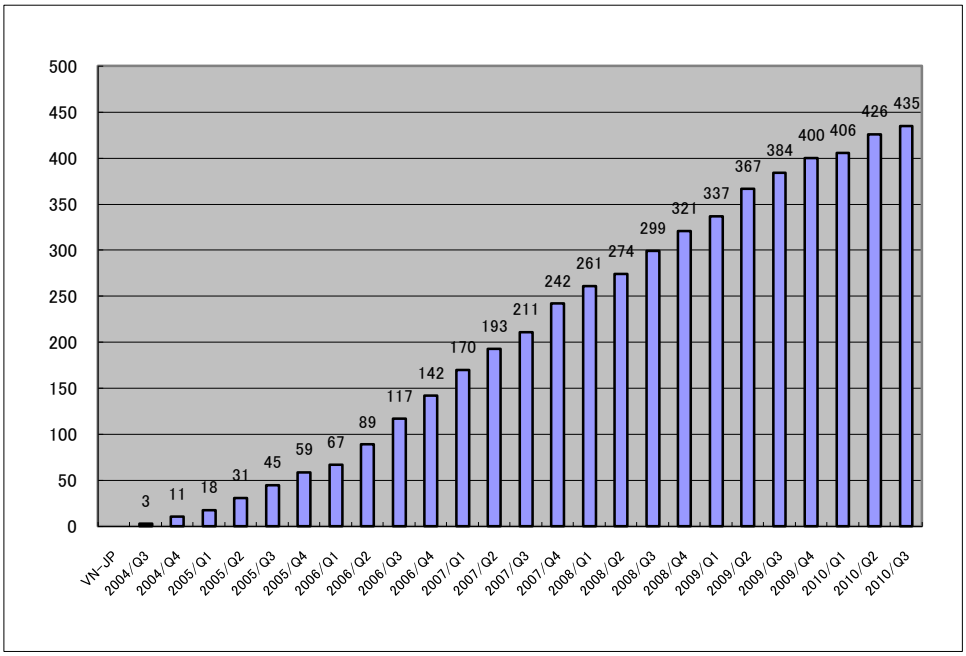
2-1. Japan Vulnerability Notes (JVN) において公開した脆弱性情報および対応状況

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 41 件(累計 964 件) [図 2-1] でした。公開された個々の脆弱性情報に関しては、JVN(http://jvn.jp/)をご覧ください。



[図 2-1　累計 JVN 公表累積件数]

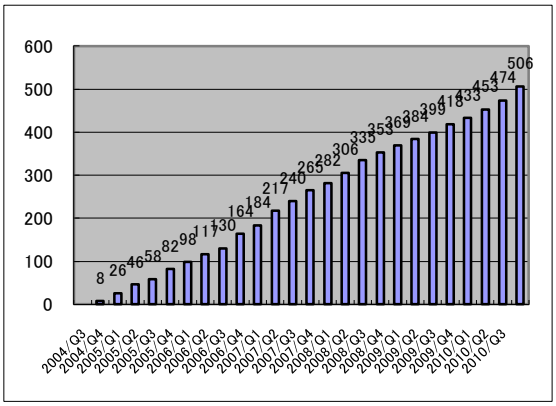
このうち、本基準に従って調整を行い、JVN で公開した脆弱性情報は 9 件(累計 435 件) [図 2-2] でした。これは、前四半期（20 件）と比較すると半減という結果になりました。この背景には、今期の新規脆弱性届出が少なかったことや製品開発者の夏期休暇等の影響があると考えられます。



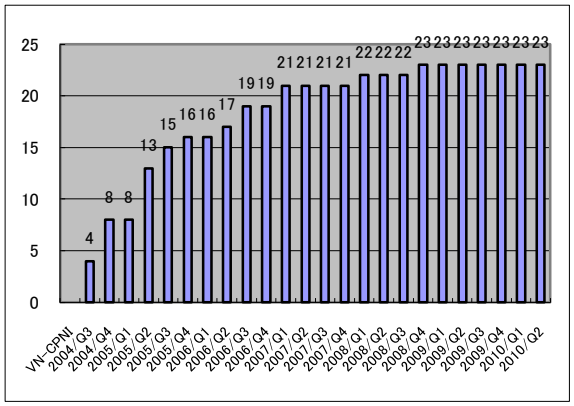
[図 2-2　累計 VN-JP 公表累積件数]

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 VN-CERT/CC として 公開した脆弱性情報は 32 件(累計 506 件) [図 2-3]でした。このうち 2 件(JVNVU#346351、JVNVU#129889)は、フィンランドの CERT-FI の主導により国際調整が行われたものでした。ここ数年、CERT-FI が主導する国際調整案件が増えており、取り扱われる案件も複数の製品開発者に影響があるプロトコル実装等の脆弱性などが多いため、今後 CERT-FI との連携をさらに強化していく必要があると考えています。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 VN-CPNI として公開した脆弱性情報は 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には、Microsoft 製品に関するものが 6 件、Adobe 製品に関するものが 6 件、Oracle 製品に関するものが 2 件含まれています。また、今期、Apple 製品に関するものが 5 件と多く公開された背景には、米国 Apple 社が自社製品の脆弱性情報を JPCERT/CC に提供し、同社製品に関する脆弱性情報の公開を JVN で行うこととなったという事情があります。



[図 2-3　VN-CERT/CC 公表累積件数]



[図 2-4　累計 VN-CPNI 公表累積件数]

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、脆弱性情報の公表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(http://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上で公表する脆弱性情報に対して2008年8月から個別に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。今期は、8件の脆弱性情報についてCVEを採番し、JVNに掲載しました。

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(改訂版)
https://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
https://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。

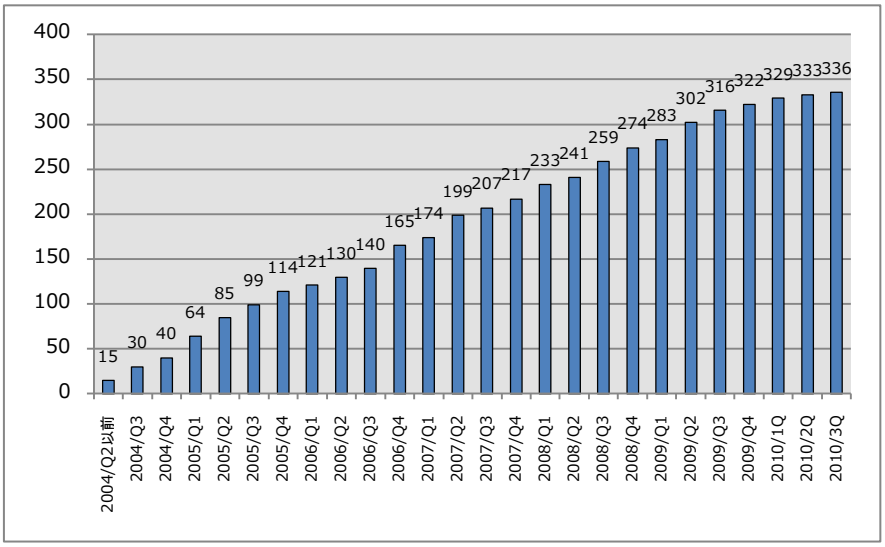
http://www.ipa.go.jp/security/vuln/

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、やや増加率が鈍化してきているものの、2010 年 9 月 30 日現在で 336 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、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、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、IPA が主催する脆弱性研究会にて検討を行うなど、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。

2-3-4. 「脆弱性情報開示」の国際標準化活動への参加

ISO/IEC JTC-1/SC27 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「脆弱性情報開示」(29147；以前の Responsible Vulnerability Disclosure (RVD)から単に Vulnerability Disclosure (VD)に名称を変更)の標準化は、前回(4 月に Melaka で開催)の SC27 国際会議での議論結果を反映して改訂され、6 月に参加各国に送付された第 1 次委員会草案(CD: Committee Draft)に対して、9 月 10 日までに参加各国が投票とコメントの起草を行いました。今回の草案では、標準規格の名称変更の他、用語の定義について ISO/IEC 12207:2008 (Software life cycle processes)および ISO/IEC 15288:2008 (System life cycle processes)と整合させる方向での見直しがなされたことが大きな変更点です。

この草案に対して日本は、50 項目以上に及ぶコメントを付けて、標準規格として改善すべき点が多数残っているとして「反対」票を投じました。SC27 の標準化活動に参加している 43 ヶ国の投

票は、コメントなし賛成が 13、コメント付き賛成が 3 (カナダ、フィンランド、韓国)、反対が 7 (オーストラリア、ベルギー、ドイツ、日本、南アフリカ、英国、米国)、棄権が 14、コメントのみ提出が 2、無投票が 4 でした。

投票結果およびコメントの取扱いは、10 月 4 日からベルリンで開催予定の SC27 国際会議で議論される予定です。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. 大阪、名古屋で「C/C++セキュアコーディングセミナー」を開催

5 月 27 日、28 日の福岡での開催に引き続き、7 月 1 日、2 日には大阪で、9 月 2 日、3 日には名古屋でそれぞれ C/C++セキュアコーディングセミナーを開催しました。

大阪は昨年に引き続き 2 度目の開催、名古屋での開催は今回が初めてでしたが、いずれも定員を上回るご応募をいただき、熱心に聴講いただきました。

講義内容は、「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」では、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」では、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。今後、次年度以降の継続開催を検討してまいります。

2-4-2. C/C++セキュアコーディングセミナー@東京、開催スタート

8 月から「C/C++セキュアコーディングセミナー@東京」を開始しています。8 月 5 日は「文字列」、9 月 15 日は「整数」の脆弱性に関して、講義と演習をセットにした形式のセミナーを実施しました。今後も引き続き月に一回のペースで異なるトピックを順に取り上げ、全 7 回のシリー

ズとして開催する予定です。10 月以降の開催予定は次のウェブページをご覧下さい。C/C++言語でのソフトウェア開発に携わる方々のご参加をお待ちしております。

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 1 社向けに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. 開発者向けウェブマガジン CodeZine に好評連載中

翔泳社の開発者向けウェブマガジン CodeZine に「実例で学ぶ脆弱性対策コーディング」と題したシリーズで C/C++セキュアコーディングの解説記事を連載しています。この四半期には次の 3 回分が掲載されました。

第 5 回 Linux のカーネルに潜む脆弱性をつぶすパッチ (7 月 6 日公開)
第 6 回 TIFF ライブラリに潜む脆弱性をつぶすパッチ（その 2）(8 月 6 日)
第 7 回 Windows の DLL だけが危ないのか？DLL hijacking vulnerability 概説（前編）(9 月 27 日)

CodeZine (コードジン)
http://codezine.jp/

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. 調査活動

2-5-1-1. 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、制御システム用セキュリティ・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。既に入手している、米国 DHS が開発した CSET(CS2SAT の後継版)と英国 CPNI が開発した SSAT の 2 種類のツールのうち、今期は特に SSAT を中心に、SICE/JEITA/JEMIMA 合同 WG に参加し、試用と意見交換を行いました。
SICE/JEITA/JEMIMA 合同 WG の成果は、今秋開催される「計測展 2010」において講演される予

定です。この講演では、モデルとして想定した制御システムにおいて、SSAT の利用によってそのセキュリティがどのように改善するかを描いています。JPCERT/CC は、この試用を通じて SSAT の適用に係る知見を得るとともに、SSAT ツールの改善を行ないました。計測展の講演にとどまらず、参加者の意見、要望をツール自体や今後の活動にフィードバックする予定です。

2-5-1-2. 制御システムを攻撃対象としたマルウエアの調査

7 月に制御システムをターゲットとした最初のマルウエアとされる stuxnet の存在が報じられ、注目を集めました。その後も関連記事がほぼ毎週のようにセキュリティベンダーのブログやニュースサイトに掲載されています。JPCERT/CC においても関心をもって情報収集に努めており、近日中に報告書をまとめるべく準備を行っています。

2-5-2. 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計 3 回 (7 月 29 日、8 月 10 日（号外）および 9 月 30 日) 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。他に、セキュリティイベントのお知らせの号外も発信いたしました。
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、次の 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
https://www.jpcert.or.jp/ics/taskforce.html

なお、今期中には、タスクフォースへの参加資格の拡充（制御系システムユーザーも参加可能とする等）を検討する予定です。

2-5-3. 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)、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。JPCERT/CC の今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」を推進するため、WG メンバーとの意見交換を今後も意欲的に実施して行く予定です。なお、この WG を通じてセキュリティ・アセスメント・ツールの普及を推進していることは前述のとおりです。

また、8 月 18 日～8 月 20 日に台北（台湾）で開催された、日中韓を中心とした自動制御と計測システムに関する国際会議「SICE 2010」における、自動制御学会のネットワーク部会が企画運営するセッションで、「Consideration on Vulnerability Handling for Control Systems（制御システムのための脆弱性ハンドリングに関する考察）」と題する講演を行いました。

2-5-4. 制御システム・セキュリティ・カンファレンス準備

昨年度同様、今年度も、制御システムに関する産官学の多様なスピーカーを招いて制御システムセキュリティカンファレンスを開催すべく準備に着手しました。詳細につきましては、本年 12 月頃にご案内させていただく予定です。

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。MyJVN API と NVD との連携により、配信データ件数の大幅な増加と安定したデータ配信が実現された結果、連携前に比べ VRDA フィードの利用数に明確な増加傾向が見られました。

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。
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、配信データ形式別の利用割合、言語別の利用割合を[表 **2-1** から[表 **2-3** に示します。

[表 2-1 VRDA フィード配信件数]

2010 年 7 月～9 月			年度
MyJVN API	NVD	計	累計
582 件	919 件	1501 件	2195 件

[表 2-2 配信データ形式別の利用割合]

HTML 形式	XML 形式
93%	7%

[表 2-3 言語別の利用割合]

日本語版	英語版
93%	7%

[表 **2-2** に示したように、HTML 形式の利用が圧倒的に多く、フィードリーダと Web ブラウザの組み合わせでの利用がほとんどで、XML 形式で表現された脆弱性情報を機械処理しているケースは非常に少ないようです。

現状の VRDA フィードの特徴として、複数の情報ソースをもつことによる情報量の豊かさ、情報を同一の文書フォーマットで表現して配送していること、および、XML 形式を選択した場合における機械処理の可能性をあげることができます。従来に比べて利用数が増加したことから、VRDA フィードが配送する情報量の拡大が歓迎され、脆弱性マネジメント業務における情報の収集と読解作業に活用していただけていることがうかがえます。その一方で、XML データ形式の脆弱性情報の利用の普及を図るためには、XML データを有効活用するためのソフトウエア等のツールや具体的な用途に関する情報を併せて提供する等のさらなる環境整備が必要であると言えそうです。

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。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っています。

このプロジェクトの活動内容については、平成 20 年度までの活動の成果等をとりまとめた「ボットの脅威との戦い～サイバークリーンセンター(CCC)活動レポート～」に詳細に紹介されています。また、毎月の活動実績は「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、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 7 月度 サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/201007/1007monthly.html
ボットの脅威との戦い～サイバークリーンセンター(CCC)活動レポート～
https://www.ccc.go.jp/report/h21ccc_report.pdf

3-1. IT Keys「リスクマネジメント演習」

ボット対策事業では、各種カンファレンスやセミナーを通して対策の呼びかけや活動の紹介を行っています。また、今後の対策につなげられるように、事業を通して得られたデータや知見を学術・研究分野とも共有する試みを進めています。そのような活動として、2008 年度より、文部科学省の先導的 IT スペシャリスト育成推進プログラムの一つである「IT Keys」において、「リスクマネジメント演習」の講義を担当しています。

JPCERT/CC は、サイバークリーンセンタープロジェクトの一員として本年度も講義の一部を担当し、教材検体を用いた解析演習を行いました。演習シナリオは、JPCERT/CC がボット対策事業やその他の解析作業で実際に使っているツールや手法を用いるなど、学生のみなさんになるべく実務に近い体験をしていただけるように作成しました。

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と、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

本四半期は、マルウエア等の分析能力向上を目指し、海外、特にアジア太平洋地域の CSIRT における分析チームとの連携を進めています。本四半期においてはベトナムとインドネシアの 2 ヶ国においてマルウエア分析トレーニング等を行いました。

4-1-1-1. VNCERT マルウエアラボ立ち上げ支援活動(2010 年 7 月 13 日-7 月 14 日)

ベトナムの CERT チームである VNCERT(Vietnam Computer Emergency Response Team)ではマルウエア等の分析体制の整備が進められており、JPCERT/CC としても分析技術や分析環境に関する情報交換という形で協力をしています。

本四半期は VNCERT の分析技術者との間で分析に関する各々の地域の事情等について意見交換を行うとともに、VNCERT の分析技術者 5 人に対して 1.5 日間のマルウエア分析トレーニングを実施しました。VNCERT の分析技術者は非常に積極的で、JPCERT/CC としても引き続きパート

ナーとして協力していきます。

4-1-1-2. ID-SIRTII との連携活動(2010 年 7 月 17 日-7 月 22 日)

インドネシアの CERT チームである ID-SIRTII(Indonesia Security Incident Response Team on Internet Infrastructure)との連携活動として、以下の活動を実施しました。

・インドネシア Academy CERT Meeting でのプレゼンテーションおよびマルウエア分析トレーニングの実施

インドネシア Academy CERT Meeting は、インドネシアの学術系における情報セキュリティ活動の一環として、ID-SIRTII と Swiss German University が中心となって企画、実施された Workshop です。第 1 回目となる今回は、2010 年 7 月 17 日に開催され、インドネシアの 14 大学から 100 名程度の参加者がありました。
JPCERT/CC は、この Workshop に企画段階から全面的に参画し、当日は、最近の情報セキュリティインシデントや CSIRT の活動について紹介を行なった他、半日のマルウエア分析トレーニングを実施しました。

・ID-SIRTII 主催マルウエア分析トレーニングの講義、演習の実施

ID-SIRTII では、定期的にトレーニングを開催しており、JPCERT/CC では、2010 年 7 月 19、20 日の 2 日間のマルウエア分析トレーニング講義、演習を担当しました。このトレーニングにはインドネシアの民間企業を中心に 20 名の参加者がありました。
このトレーニングでは、マルウエア分析の基礎から動的解析、静的解析などマルウエア分析の中心的な分析手法について実習を中心に実践的なトレーニングを行いました。

・ID-SIRTII 主催 情報セキュリティセミナーでのプレゼンテーションの実施

ID-SIRTII では、2 ヶ月に 1 回程度、インドネシアの地方での情報セキュリティセミナーを実施しており、2010 年 7 月 22 日にはスラウエシ島の中心都市であるマナドで開催されました。このマナドでの情報セキュリティセミナーには、地方行政府や民間企業等から 100 名程度の参加者がありました。
JPCERT/CC は、この情報セキュリティセミナーに参加し、最近の情報セキュリティやインシデントのトレンドおよびマルウエア分析のトレンドに関するプレゼンテーションを行いました。
参加者は非常に積極的で、セミナーの最後に行われたディスカッションでも、予定されていた時間を大幅に超過する程の活発な質疑応答、ディスカッションが行われました。

4-1-2. その他地域における活動

本四半期は、その他地域における CSIRT 構築支援および運用支援活動は、平素からの情報連携活動を除き、特にありませんでした。

4-2. 国際 CSIRT 間連携

海外の National CSIRT 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。さらに、CSIRT が構成する団体についても、アジア太平洋地域における APCERT (Asia Pacific Computer Emergency Response Team)や、国際的な FIRST (Forum of Incident Response and Security Teams) に参加し、その枠組みに則った活動をしています。

4-2-1. アジア太平洋地域における活動

4-2-1-1. シンガポールにおける Regional Collaboration in Cyber Security 会合への参加(2010 年 7 月 13 日-14 日)

Regional Collaboration in Cyber Security (サイバーセキュリティにおける地域連携) 会合が、NDU iCollege (U.S. National Defense University Information Resources Management College；米国国防大学情報資源管理校) および ISS (National University of Singapore, Institute of Systems Science；国立シンガポール大学システム科学研究所) の共催により、シンガポールにて二日間に亘り実施されました。JPCERT/CC は、"Cybersecurity Challenges and Strategies" (サイバーセキュリティの課題と取組)と題するパネルディスカッションに登壇し、"Toward global collaboration for protecting our business infrastructure" (業務基盤保護のためのグローバル連携に向けて)と題する発表を行ないました。この中では、国家における情報セキュリティの主要な要因、National CSIRT の役割、世界に存在する National CSIRT および地域 CSIRT コミュニティの現状、JPCERT/CC による CSIRT 構築支援活動および課題等について紹介し、サイバーセキュリティにおいて先進的に発展してきた地域が他地域の向上に向けて果たすべき役割について、他パネリストおよび参加者と共に活発な意見交換を行ないました。

4-2-1-2. ACID: ASEAN 諸国等 14 カ国の CSIRT による合同サイバーインシデント演習への参加(2010 年 9 月 21 日)

JPCERT/CC は、シンガポールの National CSIRT である SingCERT が主導した、ASEAN（東南アジア諸国連合）各国の CSIRT が合同で実施するサイバーインシデント演習である ACID

(ASEAN CERTs Incident Drill) に参加しました。本演習は、国境を越えて発生するサイバーセキュリティインシデントに備え、ASEAN 加盟国および周辺各国等の CSIRT 間の連携の強化を目的に毎年実施されているもので、今回が 5 度目になります。今年は 14 カ国（日本、オーストラリア、ブルネイ、中国、インド、インドネシア、韓国、マレーシア、ミャンマー、ノルウェイ、フィリピン、シンガポール、タイ、ベトナム）から 15 チームが参加しました。本演習では、ウェブから不正な PDF ファイルが実行され、マルウエアに感染し、ボットの Command and Control サーバに接続して各種通信が行なわれる大規模なセキュリティインシデントを想定したシナリオをもとに、マルウエア解析や漏洩した情報の捜索を含む、迅速なインシデント調査および対応能力の向上を目標とした、実践的な演習が行なわれました。

4-2-1-3. 2010 APISC Security Training Course への参加(2010 年 9 月 27 日-10 月 1 日)

韓国の National CSIRT である KrCERT/CC の主催により、ソウルで開催された 2010 APISC Security Training Course に参加し、CSIRT 構築および運用の向上に焦点を置いた TRANSITS マテリアルを用いたトレーニングを受けると共に、アジア太平洋地域を中心とした経済地域におけるインターネットセキュリティ分野の動向および各 CSIRT の活動状況等について情報収集を行ない、今後の JPCERT/CC とのインシデント対応等の連携強化について意見交換を行ないました。

4-2-2. その他の地域における活動

本四半期は、その他地域における国際 CSIRT 間連携活動は、平素からの情報連携活動を除き、特にありませんでした。

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
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
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（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

本四半期、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 19 件発信しました。また、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、勉強会の開催や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（対策サービス事業者）の拡大

協議会では、協議会会員のうちの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。本四半期は、新たに G Data SoftWare(2010 年 7 月)、トレンドマイクロ(2010 年 7 月)、セキュアブレイン(2010 年 9 月)、ソースネクスト(2010 年 9 月)の 4 社に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は合計で 7 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. 海外機関との交流

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)との交流の一環として、APWG 副事務総長　Foy Shiver 氏を招き、2010 年 9 月 16 日、海外におけるフィッシングの状況の説明を受け、国内における今後の動向について考察するための説明会(情

報共有会)を協議会会員向けに実施しました。この際に行った Foy Shiver 氏へのインタビューについては、後日、協議会サイトの有識者インタビューのコーナーで公開する予定です。

5-4. 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 2010 年 7 月 フィッシング報告状況
https://www.antiphishing.jp/information/information422.html
フィッシング対策協議会 2010 年 8 月 フィッシング報告状況
https://www.antiphishing.jp/information/information457.html
フィッシング対策協議会 2010 年 9 月 フィッシング報告状況
https://www.antiphishing.jp/information/information462.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. 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」シリーズの発行開始

JPCERT/CC の活動の中で国際的に連携している海外セキュリティ関連機関・組織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、シリーズで発行する「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」を JPCERT/CC のホームページ上でスタートしました。
初回は、タイの科学技術省（Ministry of Science and Technology）の管轄する National CSIRT(Computer Security Incident Response Team)である ThaiCERT のエンジニア Jirawannakool, ThaiCERT Engineer（キティサック・ジラワンナクール）氏が来日された際に取材した、タイの情報セキュリティ事情をレポートしました。

ThaiCERT のエンジニアに聞くタイの情報セキュリティ事情
https://www.jpcert.or.jp/magazine/security/field.html

7. 講演活動一覧

(1) 宮地 利雄(理事)、真鍋敬士(分析センター長,理事)、村上 晃(分析センター マネージャー):
「インターネットセキュリティ最新動向」、「情報セキュリティの技術的な基礎論」、「情報の分類と保管」、「インシデント対応体制」
平成 22 年度法務局・地方法務局職員情報セキュリティ研修 法務省民事局,2010 年 8 月 3 日～4 日

(2) 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):
「内部犯行：人的脅威とどう向き合うか」
RSA Conference Japan 2010,9 月 10 日

(3) Jack YS Lin(早期警戒グループ 情報セキュリティアナリスト):
「IT Security Trends in Japan」
中国計算機網絡安全応急(CNCERT/CC)年会@北京, 2010 年 9 月 12 日～15 日
2010 FIRST TECHNICAL COLLOQUIUM BEIJING

(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):
「変わりゆく情報セキュリティ上の脅威と CSIRT」
重要インフラ事業者に対するセキュリティセミナー,2010 年 9 月 13 日

(5) 早貸 淳子(常務理事):
「法務担当ではない方のための『国際私法の予備知識』」
ISOG-J 特別内部セミナー「クラウド時代のセキュリティと法律の関係」,2010 年 9 月 17 日

(6) 真鍋 敬士(分析センター長,理事):
「マルウエアに見るセキュリティインシデントへの対策と対応」
ISACA 大阪支部月例会,2010 年 9 月 22 日

8. 執筆・取材記事一覧

(1) 分析センター、情報流通対策グループ、事業推進基盤グループ:
「脅威！ガンブラーウイルスの正体」
NHK 教育 IT ホワイトボックス II,2010 年 7 月 1 日

(2) 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):
「IT 犯罪最新事情 “見えない”が最も怖い」
日経 BP 社日経コンピュータ,2010 年 7 月 7 日号

(3) 中尾 真二(事業推進基盤グループ 広報):
「日本で見かけないポート番号のスキャンを確認－JPCERT/CC」
翔泳社 CodeZine,2010 年 7 月 8 日

(4) 「新米セキュリティ担当者が行く！CSIRT 奮闘記」
日経 BP 社ムック絶対わかる！最新セキュリティ対策 超入門,2010 年 8 月 1 日

(5) 中尾 真二(事業推進基盤グループ 広報)：
「検索システムが過負荷でダウン 利用者が逮捕される」
日経 BP 社日経コンピュータ,2010 年 8 月 4 日号

(6) 久保 正樹(情報流通対策グループ 脆弱性アナリスト)：
「TIFF ライブラリに潜む脆弱性をつぶすパッチ(その 2)」
翔泳社 CodeZine,2010 年 8 月 6 日

(7) 戸田 洋三(情報流通対策グループ リードアナリスト)：
「Linux の crontab コマンドの脆弱性をつぶす」
翔泳社 CodeZine,2010 年 8 月 18 日

(8) 情報流通対策グループ制御システムセキュリティ：
「制御システムセキュリティガイドライン,標準及び認証への取組みに関する分析」
工業技術社 月刊計装,2010 年 9 月 1 日号

(9) 中尾 真二(事業推進基盤グループ 広報)：
「特別レポート 最新の DDoS 攻撃や iPhone を狙うワームが報告－日本シーサート協議会の年次総会」
日経 BP 社 ITpro,2010 年 9 月 17 日

(10) 久保 正樹(情報流通対策グループ 脆弱性アナリスト)：
「Windows の DLL だけが危ないのか？DLL hijacking vulnerability 詳説（前編）」
翔泳社 CodeZine,2010 年 9 月 27 日

9. 開催セミナー一覧

(1) C/C++ セキュアコーディングセミナー2010@大阪
(2) C/C++ セキュアコーディングセミナー2010@名古屋
(3) C/C++ セキュアコーディングセミナー2010@東京

本カンファレンスについての詳細は、「2-4」をご参照ください。

10. 後援・協力一覧

(1) RSA Conference Japan 2010
2010 年 9 月 9 日～10 日

JPCERT CC®

■ 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：seminar-secure@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