JPCERT CC®

JPCERT-PR-2011-0003

発行日 : 2011-07-11

JPCERT/CC 活動概要 [2011 年 4 月 1 日 ～ 2011 年 6 月 30 日]

【活動概要トピックス】

—トピック 1 —
攻撃者グループの活動への対応

本四半期は、政府や企業等の活動や経営方針等に対する自らの意見を主張する手段としてサイバー攻撃を行っているとされる攻撃者グループによって、国際的に活動を行う国内大手企業やその海外関連会社などが、不正侵入、情報窃取、ウェブサイトの改ざん、サービス妨害攻撃（計画）等の攻撃対象とされたとみられる事例が散見されました。

JPCERT/CC では、このような攻撃に関しては、自ら、および国内外の関係機関の協力を得て、関連情報を収集し、分析を行って、攻撃対象となった事業者等に情報提供を行ったり、対応の支援を行ったりする活動を行っています。本四半期においても、ⅰ）攻撃の予告や計画に関する情報に関しては、収集した情報を攻撃対象となる可能性のある事業者に提供したほか、要請があればJPCERT/CC における分析結果（攻撃の展開予測、攻撃ツールの分析やそれに基づく対策案等）も提供し、また、ⅱ）既に実施された攻撃に関する情報に関しては、攻撃対象となった企業に対して、攻撃によって流出した可能性のある情報や改ざんされたサイトなどに関する情報を提供し、要請に応じてインシデントに係る事後対応の支援を行いました。

なお、これらの事例の中に、多数のユーザアカウント情報が流出した事例が含まれていたことから、窃取された ID やパスワードの不正利用による被害拡大を防ぐため、流出した可能性のあるパスワード等を他のサービスでも利用している場合にはその変更を行うことや、この機に乗じてパスワード等の情報の詐取を行おうとする不審なメール等への注意を呼びかける注意喚起を発行しました。

―トピック 2―

第 23 回 FIRST Conference 開催―山口英理事が運営委員に

6 月 11 日から 17 日にかけて、ウィーン（オーストリア）において第 23 回 FIRST 年次総会（FIRST Conference）が開催されました。FIRST Conference は、様々な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）の活動のひとつとして毎年開催されている、技術コンファレンスと加盟メンバーによる年次総会とを含む催しです。

技術コンファレンスでは、JPCERT/CC からは、①内部犯行に関する調査についての講演(小宮山 功一朗)、②日本におけるボット対策事業（サイバークリーンセンタープロジェクト）に関する講演(中津留 勇)、および③「SPECIAL Panel Session: The day disaster struck the northeastern part of Japan」と題するパネル討論の司会（内山 貴之)を行いました。

このうち、②のサイバー・クリーン・センター(CCC)プロジェクトについては、2009 年の FIRST Conference でも報告をしていましたが、今回の講演は、2010 年度で終了した同プロジェクトの 5 年間の活動を総括した内容で行いました。同プロジェクトに類似したボット対策のための取組がドイツやオーストラリアなどでも進められており、参加者の関心を集めました。

また、③のパネル討論は、FIRST に加盟している日本の CSIRT の団体「JFIRST」の有志が、震災に見舞われた日本の状況に対する海外メンバーの関心の高さを受けて急遽企画したもので、日本の通信インフラ企業、セキュリティコンサルティング企業、ISP、インターネット総合サービスプロバイダの CSIRT の代表者をパネリストに迎え、2011 年 3 月 11 日に発生した東日本大震災の直後やその後数ヵ月間に各 CSIRT が直面した問題やその対応に関する経験を参加者と共有しました。

年次総会では、FIRST 運営委員（Steering Committee：SC）の改選において、JPCERT/CC の山口英理事が運営委員として選出されました。2 年の任期で、FIRST の運営に当たります。サイバー攻撃への対処に関し、国境を越えた CSIRT 間の連携の重要性の認識が高まりを見せる中、任期満了により退任した伊藤友里恵（JPERT/CC 国際部部長）に代わり山口英理事が、日本の顔として、国際的な CSIRT コミュニティの運営に貢献できることの意義は大きいと考えています。

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

―トピック 3―

制御システムセキュリティ評価ツール 「SSAT」の提供開始

制御システムに対する脅威が Stuxnet によって分かりやすい形で顕在化したことから、制御システムを保有する事業者においても、危機意識が高まり、対策の検討が始まっています。SSAT は、そうした事業者のために、SICE/JEITA/JEMIMA のセキュリティ合同ワーキンググループの活動において、英国 CPNI 版をもとに開発された、制御システム向けの無償セキュリティアセスメントツールです。本年 2 月から開始した SSAT の試用提供については、本四半期末現在で申込件数が 70 件を超えました。

試用いただいた企業等から、「SSAT により、具体的な問題点が明確になった」、「自社向けにカスタマイズしたい」などの声も届いており、今後は、これらの御意見を取り入れた機能改善に取り組む予定です。

本活動は、経済産業省より委託を受け、「平成２３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２３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・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。

JPCERT CC®

—活動概要—

目次

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 1567 件、インシデント件数ベースでは 1562 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 654 件でした。前四半期の 596 件と比較して 10%増加しています。「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_Report20110711.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、325 件で、前四半期の 405 件から 20%減少しました。また、前年度同四半期（388 件）との比較では、16%の減少となっています。
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] に示します。

[表 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	4 月	5 月	6 月	国内外別合計（割合）
国内ブランド	43	32	43	118(36%)
国外ブランド	53	83	37	173(53%)
ブランド不明	4	24	6	34(10%)
月別合計	100	139	86	325(100%)

本四半期は、国内のブランドを装ったフィッシングサイトの件数が 118 件と、前四半期の 84 件から 40 % 増加しました。これは、国内のポータルサイトを装ったフィッシングサイトが多数確認されたためです。また、国外ブランドを装ったフィッシングサイトの件数は 173 件と、前四半期の 247 件から 30 % 減少しました。これは、前四半期に多く確認されていた、海外の電子決済サービスを装ったフィッシングサイトの件数が減少したためです。

本四半期におけるフィッシングサイトの調整先の割合は、国内が 42%、国外が 58% と、前四半期の割合（国内 61%、国外 39%）と比較して、国外への調整が増えました。これは、国内のポータルサイトを装ったフィッシングサイトの多くが海外の無料ホスティングサービスを使用していたためです。その他、国内のポータルサイトを装ったフィッシングサイトでは、移動体通信ネットワークの IP アドレスとダイナミック DNS サービスのドメインを使用したサイトの稼働も確認しており、これら 2 種類のパターンが多くを占めています。

本四半期に報告が寄せられた Web サイト改ざんの件数は、34 件でした。前四半期の 49 件から 31%減少しています。これは、2009 年度から多発していたいわゆる Gumblar による Web 改ざんへの対策が各サイトで進んだことにより大幅に減少したためです。報告件数は減少傾向にありますが、 4 月の初めには大規模な SQL インジェクション攻撃の発生が確認されており、新たな攻撃に備えて 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」（一般公開）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」（提供先限定）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(https://www.jpcert.or.jp)や RSS、約 25,000 名の登録者を擁するメーリングリスト、早期警戒情報の受信者用のポータルサイト WAISE（Watch and Warning Analysis Information for Security Experts)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：14 件　https://www.jpcert.or.jp/at/

2011-04-13　2011 年 4 月 Microsoft セキュリティ情報 (緊急 9 件含) に関する注意喚起 (公開)
2011-04-18　Adobe Flash Player の脆弱性に関する注意喚起 (公開)
2011-04-22　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 (公開)
2011-04-28　情報流出に伴う ID とパスワードの不正使用に関する注意喚起 (公開)
2011-05-11　2011 年 5 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起 (公開)
2011-05-13　Adobe Flash Player の脆弱性に関する注意喚起 (公開)
2011-05-31　ISC BIND 9 の脆弱性を使用したサービス運用妨害攻撃に関する注意喚起 (公開)
2011-05-31　ISC BIND 9 サービス運用妨害の脆弱性に関する注意喚起 (更新)
2011-06-01　ISC BIND 9 サービス運用妨害の脆弱性に関する注意喚起 (更新)
2011-06-08　Oracle Java SE のクリティカルパッチアップデートに関する注意喚起 (公開)
2011-06-15　2011 年 6 月 Microsoft セキュリティ情報 (緊急 9 件含) に関する注意喚起 (公開)
2011-06-15　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 (公開)
2011-06-15　Adobe Flash Player の脆弱性に関する注意喚起 (公開)
2011-06-15　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 (更新)

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 66 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。

2011-04-06　大きなサイズの DNS 応答の取り扱いの問題
2011-04-13　研修向け情報セキュリティマニュアルのご紹介
2011-04-20　Adobe Flash プラグインの更新に注意
2011-04-27　長期休暇を控えて 2011/04
2011-05-11　Microsoft Safety Scanner
2011-05-18　マイクロソフトセキュリティインテリジェンスレポート 第 10 版
2011-05-25　Windows Vista SP1 サポート終了
2011-06-01　World IPv6 Day
2011-06-08　Apple Mac OS X の「ファイルの隔離」機能
2011-06-15　Microsoft Standalone System Sweeper のベータ提供
2011-06-22　Android アプリケーションインストール時の注意
2011-06-29　Firefox の高速リリースサイクルについて

1-2-1-3. 早期警戒情報

国民の社会活動に大きな影響を与えるインフラ、サービス及びプロダクトなどを提供している組織における情報セキュリティ関連部署や組織内 CSIRT に向けて、脅威情報や分析・対策情報を「早期警戒情報」として提供しています。

https://www.jpcert.or.jp/wwinfo/

1-2-2. 情報収集・分析・提供（早期警戒活動）事例

本四半期は、政府や企業等の活動や経営方針等に対する自らの意見を主張する手段として行われたとみられるサイバー攻撃によって、国際的に活動を行う国内大手企業やその海外関連会社などが被害を受けた事例が散見されました。

こうした活動家によるサイバー攻撃は、欧米企業などを対象として古くから行われてきましたし、歴史的な記念日を中心として日本の政府関係組織等に向けた反日感情に基づく攻撃が行われたことも少なからずあったところですが、本四半期においては、国内大手企業やその海外関連会社等を標的にしたネットワーク経由での不正侵入、情報窃取や Web サイトの改ざん、サービス妨害攻撃(計画)などが次々と明らかになり、中には、メディアの注目を大きく集めた事例もありました。

このような活動家によって行われる攻撃は、多数の者の間で攻撃に関する相談が行われたり、参加の呼び掛けが広く行われたりすることから、事前に攻撃の計画に関する情報を得ることができる場合があり、また、攻撃予告や攻撃に関する事後的な声明が公表されたりする場合もあるため、攻撃や被害の発生の事実が明らかになり易い傾向にあるといえます。そのような意味では、とりわけ攻撃予告等が行われたり、攻撃への参加が呼び掛けられたりするものについては、経済的な利得や特定の種類の情報の窃取等のために潜行して行われる種類のサイバー攻撃がなかなか表面化せずに被害ばかりが拡大するのとは対照的に、事前に情報を得て対策につなげたり、対応を迅速に行うことで被害を縮減することができたりするという利点もあるところですが、攻撃の対象となった組織は、結果的に攻撃への対応ぶりについても注目を集めてしまい、場合によっては便乗する別のグループによる 2 次、3 次の攻撃の対象となってしまうこともあることから、その負担は重いものとならざるを得ないところです。

JPCERT/CC では、このような攻撃に関しては、自ら、および国内外の関係機関の協力を得て、関連情報を収集し、分析を行って、攻撃対象となった事業者等に情報提供を行ったり、対応の支援を行ったりする活動を行っています。本四半期においても、攻撃の予告や計画に関する情報に関しては、攻撃対象となる可能性のある事業者に対し、収集した情報と、要請があれば JPCERT/CC における分析結果（攻撃の展開予測、攻撃ツールの分析やそれに基づく対策案等）を提供し、また、既に実施された攻撃に関する情報に関しては、攻撃対象となった企業に対して、攻撃によって流出した可能性のある情報や改ざんされたサイトなどに関する情報を提供し、要請に応じてインシデントに係る事後対応の支援を行いました。

なお、このような意見表明等の手段として行われる活動家によるサイバー攻撃については、上述のとおり目立ちやすいために、メディア等に取り上げられる機会も多くなりがちですが、必ずしも、実際に発生しているサイバー攻撃に占める割合が急激に増加しているわけではない点に留意する必要があります （攻撃者による公表が行われないタイプの、より深刻な情報窃取型の攻撃も減っておらず、それらに対する警戒や対策が重要です。)。また、このような目的によるサイバー

攻撃においては、過度の注目を行ったり、攻撃対象となった事業者等について合理的でない批判を行ったりすれば、攻撃者をより満足させる結果となり、同様の攻撃を継続、増長させることにつながりかねないことから、社会としての冷静な対応が求められるところです。

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。

インターネット定点観測システム
https://www.jpcert.or.jp/isdas/index.html

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 位及び 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 4 月 1 日-6 月 30 日)

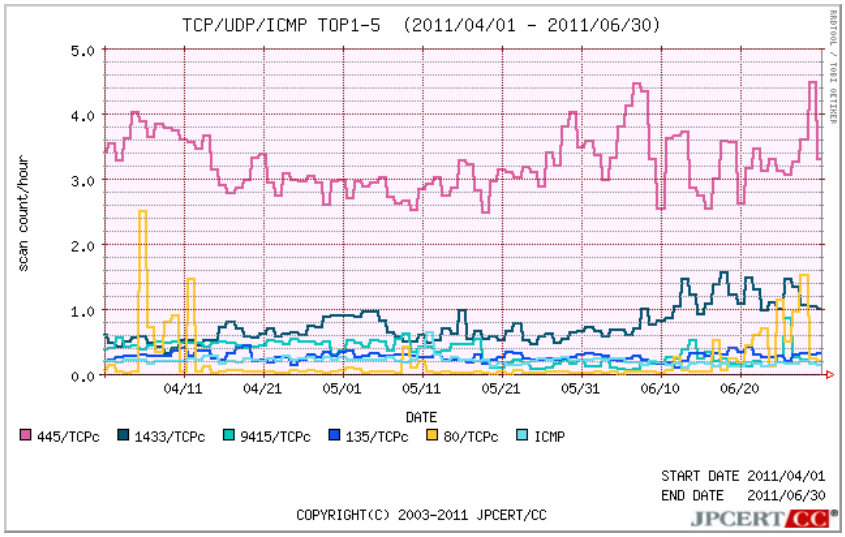


図 1-1：アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2011 年 4 月 1 日-6 月 30 日)

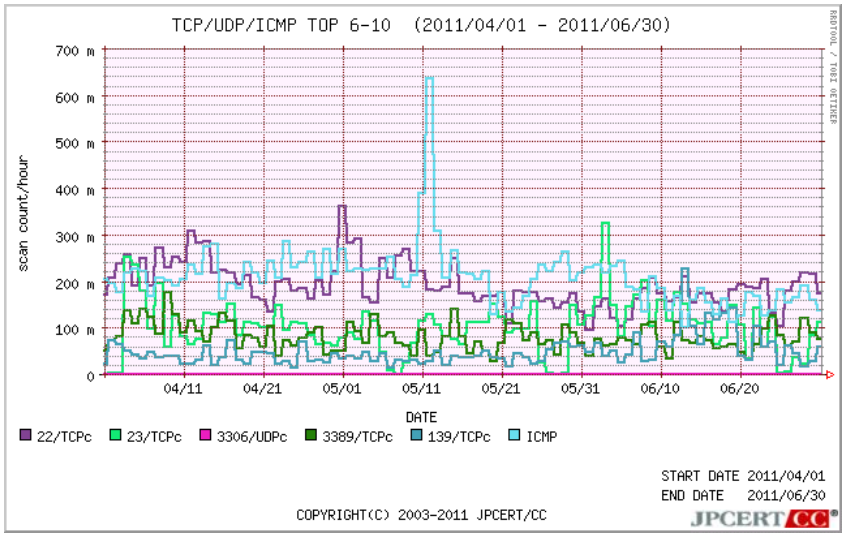


図 1-2：アクセス先ポート別グラフ top6-10

また、より長期間のスキャン推移を見るため、2010 年 7 月 1 日から 2011 年 6 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 位及び 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 7 月 1 日-2011 年 6 月 30 日)

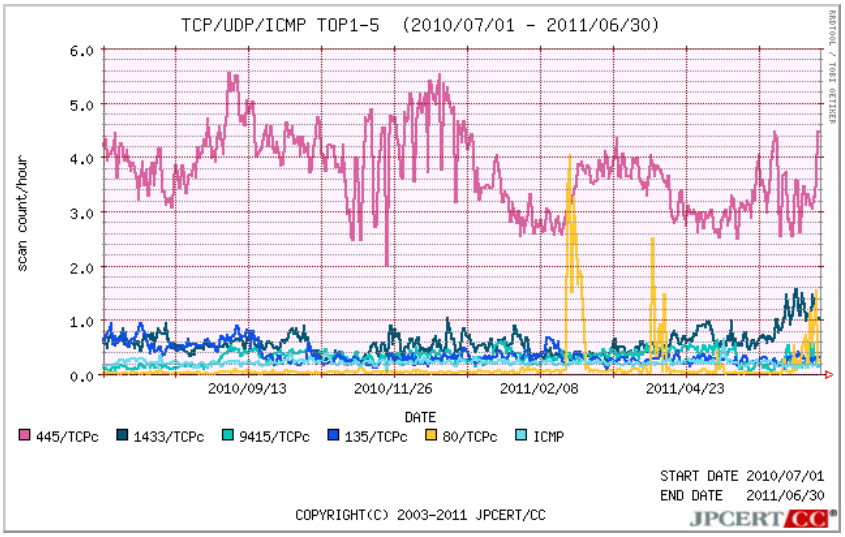


図 1-3: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2010 年 7 月 1 日-2011 年 6 月 30 日)

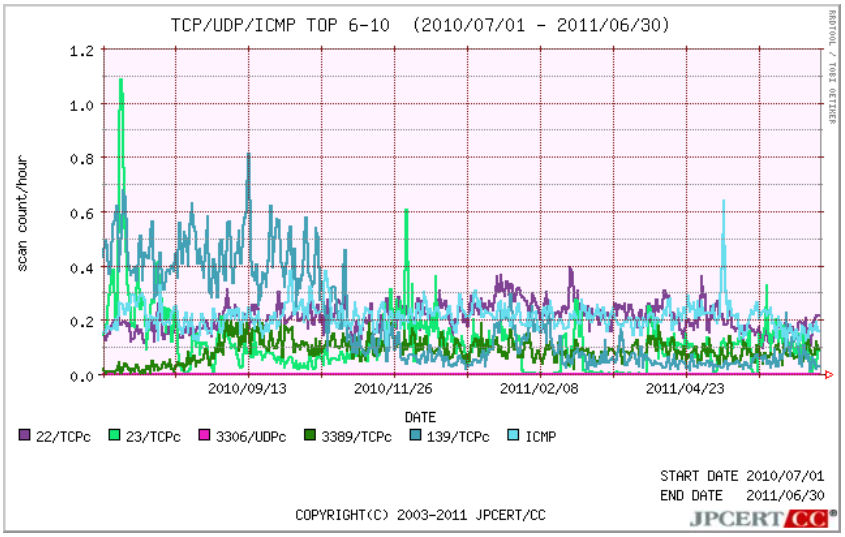


図 1-4: アクセス先ポート別グラフ top6-10

これまでの傾向と同様、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。そのほか、アクセス制御が不十分な、Proxy サーバや SIP サーバなどの Scan が引き続き観測されています。

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 サイト、メーリングリストの管理等の活動を行っています。

本四半期においては、アンラボ(ALJ CERT)と凸版印刷(TOPPAN-CERT)が、新規に加盟しました。本期末時点で 21 の組織が加盟しています。
4 月には、第 7 回ワーキンググループ会が開催され、参加した 19 の組織と 5 つの WG から、昨年度の活動内容や今年度の活動目標などが発表されました。また、JPCERT/CC 国際部マネージャの小宮山から、「アフリカにおける CSIRT 構築支援」という演題で、JPCERT/CC がアフリカ諸国で展開している CSIRT 構築支援プログラムを紹介しました。
5 月には、インシデント情報活用フレームワーク検討 WG から、Web サービスの連携によって作成されるコンテンツ (マッシュアップコンテンツ) を悪用した、ホームページ誘導型マルウェア(mstmp)に関する技術調査記事が公開されました。

Web サービス連携を使用した Web サイト経由での攻撃 mstmp について
http://www.nca.gr.jp/2011/mstmp/

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。

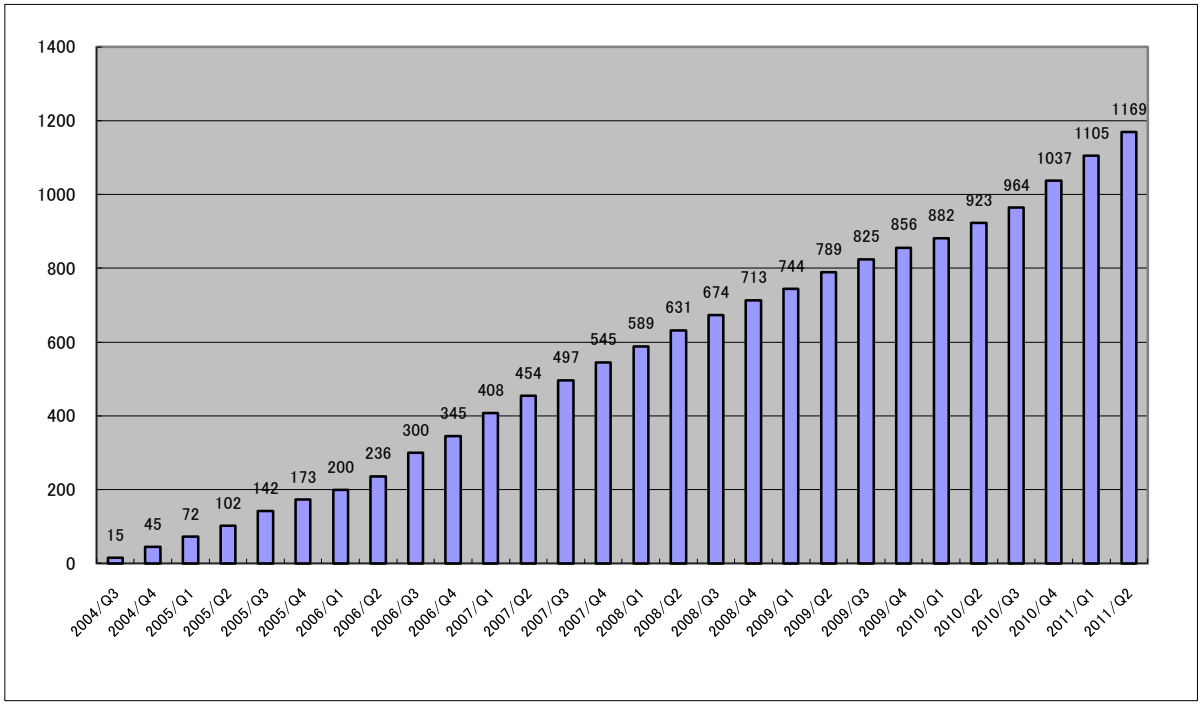
日本シーサート協議会 Web ページ
http://www.nca.gr.jp/

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。

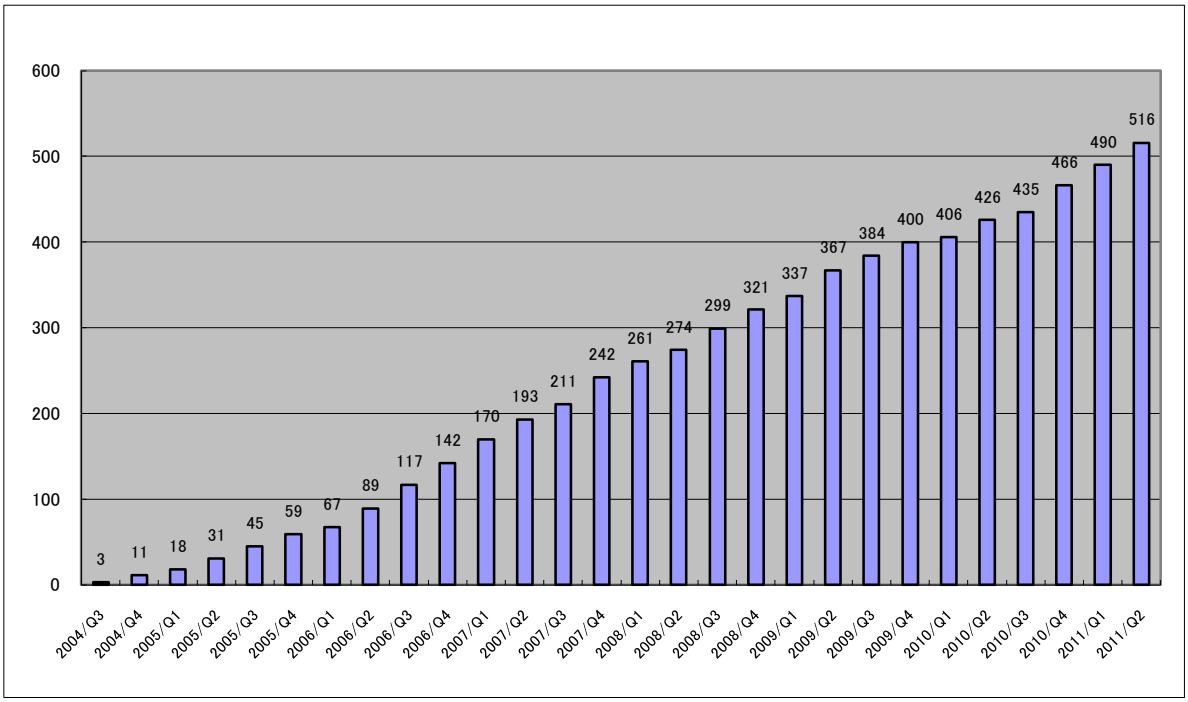
2-1. Japan Vulnerability Notes (JVN) において公開した脆弱性情報および対応状況

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 64 件(累計 1169 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 2-5　累計 JVN 公開累積件数]

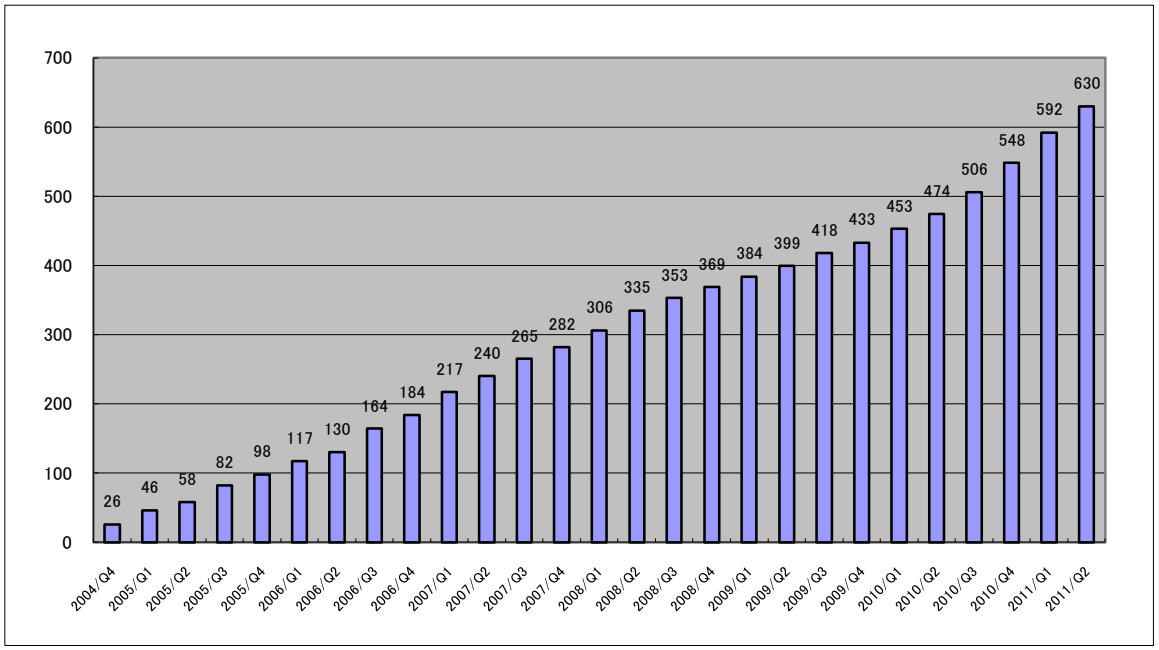
このうち、本基準に従って調整を行い、JVN で JVN#として公開した脆弱性情報は 26 件(累計 516 件) [図 2-2] でした。本四半期に JVN#として公開された案件の半数にあたる 13 件が海外製品開発者の製品であり、本枠組みに基づく JPCERT/CC の調整活動が海外の開発者にも理解され協力が得られるようになってきていると考えられます。また、本四半期には製品開発者自身による自社製品に関する JPCERT/CC への脆弱性の届出が 1 件ありました。これは、製品開発者による自社製品の脆弱性の公開に関する取組みが進展している傾向の一端と言えます。



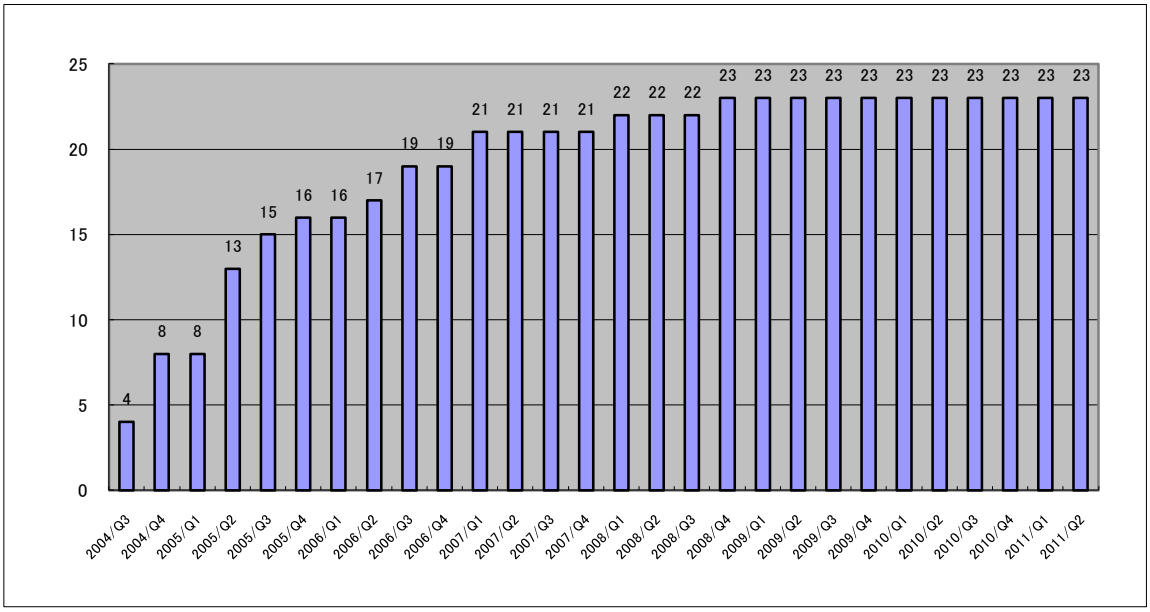
[図 2-6　累計 JVN_JP(JVN#)公開累積件数]

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 38 件(累計 630 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 3 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 2 件公開されました。本四半期に公開された脆弱性は、特定分野や特定の製品に集中したという傾向は見られず、どちらかというと多種多様の製品にわたっていました。脆弱性の公表は今回が初めてとなる製品開発者名や製品名の脆弱性情報も多く見られました。

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 2-7　VN_CERT/CC(JVNVU#および JVNTA)公開累積件数]



[図 2-8　累計 VN_CPNI(CPNI) 公開累積件数]

2-2.　情報セキュリティ早期警戒パートナーシップの改訂とその運用

前項 2-1 で述べたように、情報セキュリティ早期警戒パートナーシップに基づく本活動が定着し、着々と対策がとられ、情報公開が進んでいる一方で、製品開発者との連絡が取れないなどの理由から調整が進められない、いわゆる「長期滞留案件」も 2004 年の本活動開始から 7 年の間に多数たまってきています。昨年度より引き続き、こうした状況の改善を期して、この問題の分析と対応方針についての検討を行っています。

そのひとつとして、昨年度公表さ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改定版および JPCERT/CC 脆弱性関連情報取扱いガイドラインにおいて、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となった際に当該の製品開発者への連絡手段を広く一般に求める手順を定めており、これを受けて今夏より、JVN 上に「連絡不能開発者一覧」というコーナーを設け、連絡不能となっている製品開発者名の公表を開始する予定となっています。その準備として、本四半期においては、「連絡不能開発者一覧」のメニューボタンを JVN のトップページ上に追加し、専用ページを設けました。また、こうした準備と並行して、連絡不能となっている製品開発者への再通達等のアプローチを繰り返し行いました。その結果、本四半期に連絡が取れるようになり、JVN 公表に到った案件が 1 件ありました。さらに、製品開発者との調整についても、本四半期から手順の一部を変更しています。この変更は、当初は製品開発者に戸惑いを与えたようでしたが、古い脆弱性情報であっても、不特定多数の利用者の存在が否定できない限り、JVN での脆弱性情報公開を通して問題と対策方法を広く周知し製品利用者の安全に資すべきであるという変更の趣旨を理解していただくことができました。こうした活動の結果、本四半期において 14 件のいわゆる長期滞留案件を JVN で情報公開することができました。今後も、JPCERT/CC は、迅速な JVN 公表を目指して製品開発者との調整を進めてまいります。

さらに、こうした対応によってもなお最終的に調整ができない場合についても、知らされないまま脆弱性をもった製品を使い続けて利用者が脅威にさらされるリスクを軽減することを目的に、JVN で公表を行うべく、その手順や手続き等について、IPA および関係機関との検討を行っています。

2-3. 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、国際調整機関である米国の CERT/CC、英国の CPNI、フィンランドの 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。

国際的な活動の一つとして、2008 年 5 月 21 日に JVN 英語版サイト(http://jvn.jp/en)の運用を開始し、3 年が経過しました。JVN 英語版での情報公開は、日本語版公開とほとんど時差なく、ほぼ同時公開で運用を行っています。日本国内で取り扱われた脆弱性案件に関しての、海外への発信という点では、第一次情報発信源となることも多く、海外の主要セキュリティ関連組織などからも注目されています。
また、JPCERT/CCは、米国MITRE社より、2010年6月23日付でCNA（CVE Numbering Authorities、CVE採番機関）に認定されました。以後、JPCERT/CCはCNAとして、自ら、よりタイムリーにCVE番号を採番できることになりました。本四半期は、15件の脆弱性情報についてJPCERT/CC

がCVEを採番し、3件の脆弱性情報について製品開発者としてCNA認定されているOracleが自らCVEを採番し、合計18件のCVEがJVN上に掲載されました。2008年にCVEの採番を開始して以降、約93%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

2-4.　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。

2-4-1.　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

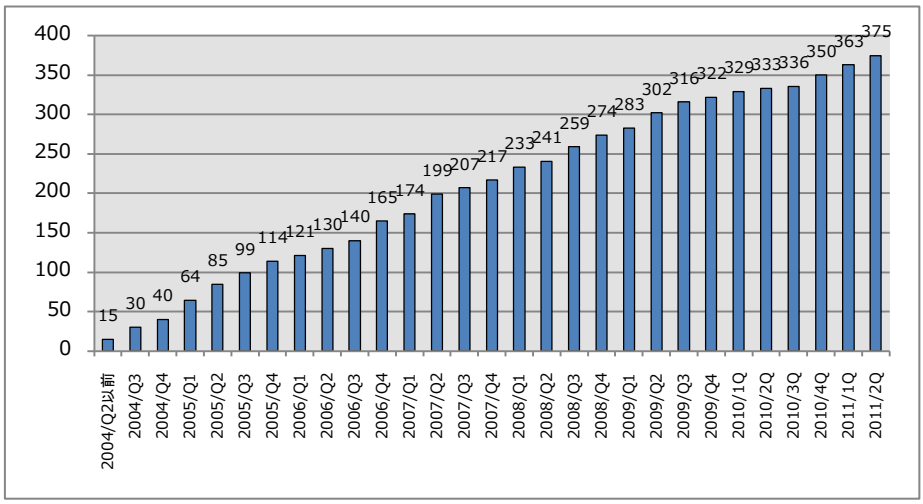
を公開しています。両組織間においては緊密な情報の交換、脆弱性情報の分析等を行っています。なお、本基準における IPA の活動および四半期毎の届出状況については、次の URL をご参照ください。

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

2-4-2. 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 6 月 30 日現在で 375 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]

本四半期から、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」の中のフォーラム機能の運用を開始しました。フォーラムは脆弱性情報ハンドリングに関連する話題や製品のセキュリティ品質向上に役立つ話題などの情報交換を目的とした掲示板で、製品開発者やJPCERT/CCの脆弱性情報ハンドリング担当者が自由に利用でき、投稿した内容を閲覧できる対象者を細かに指定することも可能となっています。
製品開発者と JPCERT/CC との間の情報伝達チャンネルとしての利用だけでなく、多数の製品開発者が連携した対応を求められる複雑な脆弱性案件における関係者間の議論や情報共有の場としても活用が期待されています。

2-4-3. 「脆弱性情報開示」の国際標準化活動への参加

脆弱性情報の取扱手順(Vulnerability Handling Process (VHP)； 30111)および開示(Vulnerability Disclosure (VD)；29147；旧称 Responsible Vulnerability Disclosure)に関する 2 件が並行して進められている ISO/IEC JTC-1/SC27 の WG3 における国際標準の策定作業、およびインシデント管理に関する同 WG4 における検討作業に参加しました。

半年ごとに開催されている ISO/IEC JTC1/SC27 の標準化国際会議が 4 月中旬にシンガポールの Nan-yan Technological University (NTU；南洋理工大学)で開催され、両標準化文書についても検討がなされました.

VD は会議に先立つ 3 月に第 2 次委員会草案(CD；Committee Draft)としての投票に付されていましたが、これと並行してなされた投票により VHP の標準化作業への着手が正式に決定したため、ベンダーの外側から見えるインターフェースは VD に残し、ベンダー内部の外部から見えない対応は VHP に移して VD からは削除するとの原則の下で、その内容を仕分けした上で、オーストラリア:1 件、カナダ:29 件、ドイツ:17 件、日本:42 件、韓国:1 件、英国:75 件、米国:68 件)の合計 233 件のコメントへの対応について協議しました．この検討作業に実質的に参加した国は、カナダ(エディタ)と米国、英国、ドイツ、南アフリカ、日本でしたが、開発プロセスの観点からの声高な発言で、前々回から議論を混乱させてきた南アフリカは、投票に際してもコメントを付さず、編集会議での発言もほとんどありませんでした。文書内容に大幅な変動が生じたため、改訂のための十分な時間をエディタに与える意味から、改訂後の CD を投票に付さず、コメントだけを各国に求めて、次回の SC27 標準国際会議に臨むことになりました。

正式に標準化作業の着手が決まった VHP については、エディタに米国の Katie Moussouris さん(Microsoft 社)が就任することになりました。作業への参加者は VD と共通で、この脆弱性の取扱に関する検討グループは、他に大きな案件を持たない WG3 の中にあって最大の人数を擁するに到っています。その後 6 月には、エディタにより第 1 次作業草案(WD: Working Draft)が取りまとめられ，各国からの修正コメントを募り始めています。

脆弱性の取扱いに関連した 2 つの標準開発が正式に始まりましたが、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。

インシデント管理については、既に WG4 において「情報セキュリティ・インシデント管理」(ISIM: Information Security Incident Management)が FDIS (Final Draft for International Standard)の段階まで進んでいますが、これを補完する標準として、「インシデントの管理と運用と対応」(IMOP: Incident Management, Operation and Response)の標準の必要性が検討されています。検討の要と

なるラポータは、英韓日がアサインされており、4 月中旬の SC27 国際会議ではラポータからの報告を受けて議論がなされました。英国と韓国のラポータは、かなりの規模の複数セクションからなる標準に ISIM を改組することを想定しつつ、標準化に前向きの方針を提案しました。これを受けた議論の結果、今後のインシデント対応の標準化活動に関する各案(1:27035 で終了、2:27035 を改訂、3:27035 を複数部に拡大再構成、4:新しい標準を追加)の長所と欠点を検討評価するために、調査期間(Study Period)をさらに半年間延長することになりました。

インシデント管理に関する標準化の動向についても、JPCERT/CC では引き続き 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たフォローアップを継続していく所存です。

2-5. セキュアコーディング啓発活動

2-5-1. タイで「C/C++セキュアコーディングセミナー」を開催

日系の組込みソフトウェア企業等が多く進出しているタイにおいて、現地のソフトウェア技術者や学生を対象に C/C++セキュアコーディングに関するノウハウを提供することは、現地のセキュリティ啓発に資するのみならず、日本のソフトウェアセキュリティ向上にも資するとの期待を込めて、次のとおりタイ国内の 2 カ所でセミナーを実施しました(使用言語は英語)。

(1) セミナー名：「C/C++ セキュアコーディング 2day セミナー ThaiCERT@バンコク」
開催日：5 月 9 日、10 日
開催地：バンコク市内のホテル
主催：ThaiCERT, JPCERT/CC

「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、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。

セミナーは、ThaiCERT と協力して企画、開催しました。講義内容にも会場等の手配にも、受講者から高い評価を得ることができ、JPCERT/CC と ThaiCERT との一層の連携強化にも資するものとなりました。

(2) セミナー名：「C/C++ セキュアコーディング 1 day tutorial @JCSSE2011」
開催日：5 月 11 日
開催地：マヒドン大学 (Mahidol University)
主催：IEEE, IEEE Thailand Section, JPCERT/CC

5 月 11 日から 13 日の 3 日間にわたって開催された Software Engineering を学ぶ学生や研究者が一堂に会する国際会議「JCSSE2011」における、1 日チュートリアルとして実施しました。主な受講者は、会議に参加した学生や、地元のマヒドン大学 ICT 学部の学生でした。
講義は、先述の(1)で実施した「part2. 整数・コードレビュー」と同等の構成で行いました。コードレビューのセッションでは、参加者から活発な発表がなされるなど、理解の深さと強い学習意欲が印象的でした。

2-5-2. インドネシアで「C/C++セキュアコーディングセミナー」を開催

インドネシアを代表する CERT 組織である Id-SIRTII の協力の下、ジャカルタに次ぐ第二の大都市であるスラバヤにおいて、以下のとおりセミナーを実施しました(使用言語は英語)。

セミナー名：「C/C++ セキュアコーディングスラバヤ2dayセミナー Id-SIRTII@スラバヤ
開催日：5 月 25 日、26 日
開催地：スラバヤ工科大学
主催：Id-SIRTII, スラバヤ工科大学情報科学部, JPCERT/CC

スラバヤ工科大学は、東ジャワ地域における情報技術分野の高等教育拠点として優秀な人材を輩出してきました。折しもセミナーの前日には Id-SIRTII とスラバヤ工科大学が研究・教育を協力して行う旨の MOU を締結するなど、情報セキュリティの分野における COE を目指した先進的な取組みを行っています。また、スラバヤに開発や生産拠点を構える日本企業も多く、今後さらに多くの IT 企業の進出が期待されていることもあり、こうした企業で必要とされる優秀な人材、なかでもセキュアなソフトウェア開発ができるエンジニアの育成に資することを目的として、本セミナーを開催しました。

セミナーは先述のバンコク 2day セミナーと同じ構成で行われ、情報科学を学ぶ学生や先生方が多数参加されました。

2-5-3. 国立情報学研究所　トップエスイープロジェクト「セキュリティ概論」講義

トップエスイープロジェクトの講座「セキュリティ概論」の第 3 回、第 4 回の講義を担当し、セキュアコーディングに関する講義を行いました。第 3 回の「セキュアコーディング, その重要性」では、セキュリティの観点からソフトウェア開発の現状を概観し、今なぜセキュアコーディング

に取り組まなくてはならないかを解説しました。第 4 回「セキュアコーディング，実践」では、ソフトウェアの脆弱性につながる代表的なコーディングエラーの実例を検討すると同時に、セキュリティコード分析を実際に体験する演習を行いました。

2-5-4. 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。

2-6. 制御システムセキュリティに関する啓発活動

2-6-1. 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 6 月 2 日に配信いたしました。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。
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に配付しています。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

2-6-2. 日本版 SSAT

日本版 SSAT 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制作に取り組み、前四半期に提供を開始した、制御システム用セキュリティ・アセスメント・ツールです。提供開始から 2011 年 6 月 30 日現在までに、73 件の試用申込みをいただきました。試用後のアンケートでは、約 6 割の方からツールの有効性に関して実用的であるとのご意見をいただいています。今後のアップデートも視野に普及活動と改善検討を進めていきます。

なお、本ツールに関し、工業技術社より発行されている「計装」6 月号の特集「制御システムのセキュリティ対策と今後の課題」に納められた紹介記事「制御システムセキュリティ評価ツールの公開と活用のすすめ」を執筆しました。

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

2-6-3. 関連国内学界活動

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、前年度公開したセキュリティ・アセスメント・ツール「日本版 SSAT」の今後のバージョンアップなどに関連した活動や意見交換を行いました。

2-6-4. 海外連携活動

米国政府は、国土保安省 (DHS) の下で、制御システムのセキュリティ強化施策を Control Systems Security Program (CSSP)として進めています。このプログラムによる活動には、産業制御システム業界に関わるユーザやベンダ、その他関係者を巻き込んだ官民連携による「ICSJWG (Industrial Control Systems Joint Working Group)」や、制御システムに関する脆弱性やインシデントへの対応のために DHS 内に設置された「ICS-CERT (Industrial Control Systems CERT)」が含まれます。

ICSJWG が半年ごとに定期開催している研究集会が「ICSJWG コンファレンス」で、5 月上旬にテキサス州ダラスで開催されました。JPCERT/CC もこれに参加し、運用と管理と技術の領域における米国での取組みと現状について情報収集に努めました。日本でも米国でも、Stuxnet の登場をきっかけに、制御システムのセキュリティへの取組みが強化され始めています。そうした活動をサポートすべく、JPCERT/CC では、海外の先進事例の収集とその国内展開や、海外パートナーとの情報共有にこれからも取り組んでいきます。

また、ICS-CERT との関係においては、6 月中旬に、今後の一層の連携強化に向けて ICS-CERT 本部を訪ね、双方の活動状況に関するアップデート、今後の連携に向けた調整等を行いました。

ICS-CERT
http://www.us-cert.gov/control_systems/ics-cert/

ICSJWG
http://www.us-cert.gov/control_systems/icsjwg/index.html

2-7. 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 月から行っています。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 2-2]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 4 月～6 月			年度累計
MyJVN API	NVD	計	
653 件	920 件	1555 件	1555 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	59,914 (59,055)	19,195 (31,665)	97% (97%)	3% (3%)
英語版	3,796 (3,900)	11,724 (12,472)	97% (94%)	3% (6%)

（括弧内の数値は前四半期）

[表 2-2]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、前四半期と比較して日本語版と英語版の差が小さくなっています。英語版の利用数に大きな変化が無かったのに対して、日本語版の利用数が 40%程度減少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. アーティファクト分析

JPCERT/CC では、インシデントに関して報告いただいた情報や収集した情報を確認し実態を把握するためにアーティファクト分析という活動を行っています。アーティファクト分析では、ウイルスやボット等のマルウエアに限らず、攻撃に使われるツールを始めとするプログラムや攻撃手法等（アーティファクト）を技術的な観点から調査・解析します。アーティファクト分析を行うことで、より効果的なインシデント対応や、より精度の高い情報発信を目指すとともに、そのために必要な分析環境と分析能力の高度化に努めています。

アーティファクト分析の活動は、JPCERT/CC が行うインシデント対応や情報発信を背面から支えているほか、前期までは「ボット対策プロジェクト」の一環としても遂行されてきました。総務省と経済産業省が連携して 5 年計画で実施された本プロジェクトは、個人利用者のセキュリティ対策における各事業者の役割定義や研究者間でのアーティファクト情報共有、アーティファクト分析技術の教育普及などで多面的な成果をあげつつ、2010 年度で終了しました。本四半期は、関連機関間で、このプロジェクトの成果を継承し、発展させていくための調整を進めました。

3-1. 23rd Annual FIRST Conference におけるボット対策プロジェクトに関する発表

6 月中旬に開催された FIRST Conference において「Cyber Clean Center Project - A five year retrospective」と題したプロジェクトの発表を行いました。本プロジェクトに関しては、これまでも、2009 年の京都での FIRST Conference で発表を行い、2010 年のマイアミでの FIRST Conference でもライトニングトークで経過報告をしました。海外では、オーストラリアやドイツなど複数の国や地域でボット対策のためのプロジェクトが開始されており、日本のボット対策プロジェクトが少なからず影響を及ぼしたものと確信しています。

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

本四半期は、アジア太平洋地域における CSIRT 構築支援および運用支援活動はメールでの問合せが中心でした。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) などの国際組織への加盟を希望するアジア諸国の CSIRT に対して、その活動を紹介し、加盟手続きに関する支援等を行いました。

4-1-2. その他地域における活動

4-1-2-1. アフリカ CSIRT 構築支援(2011 年 5 月 30 日-6 月 4 日)

JPCERT/CC は、5 月と 6 月にまたがってタンザニアで開催された国際会議 Afnog 12 に参加するとともに、5 日間にわたるアフリカ諸国向けの CSIRT トレーニングを行いました。

Afnog はアフリカ諸国のインターネット運用者及び政策担当者の連携と教育を目的とする非営利組織です。Afnog はアフリカ各地で年次会議を開催し、トレーニングと最先端の技術を紹介する講演などを提供しています。Afnog 12 は、その名の通り 12 回目となる Afnog の年次会議で、今回はタンザニア政府などのスポンサーにより、タンザニアの首都ダルエスサラーム近郊で開催されました。

JPCERT/CC が担当した CSIRT トレーニングは、Afnog のトレーニングプログラムの一つとして、アジア地域との連携を促進する AAF（Africa Asia Forum on Network Research & Engineering）が主催したプログラムです。JPCERT/CC は、5 月 30 日から 6 月 4 日のトレーニングの間、講師として講義を行うだけでなく、アフリカ人インストラクターの指導を行いました。同様のトレーニングは 2010 年春から今回で 3 回目の開催となります。今回は、5 日間の日程の前半 3 日間が、過去のトレーニングを修了したアフリカ人講師によるトレーニングに充てられ、後半 2 日間は JPCERT/CC が Web セキュリティに関するトレーニングを行いました。トレーニングには、約 30 名のインターネット運用者及び政策担当者が集い、今後アフリカ各国の CSIRT 構築を推進するキーパーソンとして熱心に受講されていました。

[図 4-1 トレーニングの模様]

Afnog 及び CSIRT トレーニングと AAF についての詳細は、次の URL をご参照下さい。

Afnog 及び Afnog 12 公式ページ
http://www.afnog.org/
AAF（Africa Asia Forum on Network Research & Engineering)
http://www.africaasia.net/2011-5-CERT.html

また、トレーニングに先立ち、タンザニアの隣国であり、東アフリカ地域にあって経済発展がもっとも著しいケニアの首都ナイロビを訪問し、ケニア政府の ICT 政策担当高官との意見交換や、CSIRT 構築を進めている民間企業の訪問を通じて、アフリカのインターネットセキュリティ事情に関する情報を収集するとともに、今後のアフリカ地域各国 National CSIRT との連携に備えて相互の連絡先や連絡方法等について確認、調整を行いました。

JPCERT/CC は、アフリカ地域に起因するインシデントが日本国内で発生する可能性も考慮しながら、そのような事態が発生した場合にも迅速かつ円滑な対応活動を行うことができるよう、このような連携強化に向けての基盤作りにも努めています。

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、APCERT や、FIRST 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 (Asia Pacific Computer Emergency Response Team)

JPCERT/CC は APCERT に加盟しています。2003 年 2 月の APCERT 発足時から継続して Steering Committee のメンバに選出されており、また、事務局を担当しています。2011 年 3 月からは、議長チームとして様々な活動をリードしています。JPCERT/CC の APCERT における役割及び APCERT の詳細については、次の URL をご参照ください。

JPCERT/CC within APCERT
https://www.jpcert.or.jp/english/apcert/

4-2-1-1-1. Steering Committee 電話会議の実施

4 月 20 日及び 6 月 8 日に Steering Committee のメンバ間で電話会議を行い、今後の APCERT 運営方針について議論を行いました。

4-2-1-1-2. APCERT の PR 活動

6 月 1 日 - 2 日にロンドンで開催された EastWest Institute 主催の Worldwide Cybersecurity Summit 及び後述の National CSIRT Meeting において、APCERT を代表し、組織のビジョンや活動紹介を行いました。

4-2-1-2. 情報セキュリティに関する国際標準化活動への参加(2011 年 4 月 11 日-15 日)

JPCERT/CC は、4 月 11 日から 15 日までシンガポールにて開催された ISO/IEC JTC-1/SC27 に日本の代表団の一員として参加しました。

SC27WG3 においては 2008 年 4 月から開始された「脆弱性開示」(VD: Vulnerability Disclosure；29147)及び今回から始まった「脆弱性取扱手順」(VHP: Vulnerability Handling Process；30111)のガイドラインの策定作業が行われており、JPCERT/CC は、脆弱性情報の取扱いに関する知見をもとに諸提案を行っています。

SC27WG4 においては、インシデント管理に関する標準を拡充すべきか否かの検討が行われています。今回は調査報告が行われ、さらに半年間期間を延長して調査を継続することになりました。

SC27 への参画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。

4-2-2. その他の地域における活動

4-2-2-1. FIRST (Forum of Incident Response and Security Teams)

JPCERT/CC は FIRST に加盟しています。FISRT の詳細については、次の URL をご参照ください。

FIRST
http://www.first.org/

4-2-2-1-1. FIRST Steering Committee への参画

2011 年 6 月に行われた FIRST の年次会合における選挙を経て、JPCERT/CC の理事 山口英が FIRST の Steering Committee のメンバとして同組織の運営に関与することが決定しました。任期は 2 年間です。FIRST Steering Committee のメンバ構成については、次の URL をご参照ください。

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

なお、2009 年より FIRST の Steering Committee のメンバとして、同組織の運営に関与してきた JPCERT/CC 国際部部長 伊藤友里恵は 2011 年 6 月を以って任期を満了し退任となりました。伊藤は連続 3 期に渡り FIRST の Steering Committee のメンバを務めました。伊藤は、議長国チームの一員として APCERT の活動に参加するなど、JPCERT/CC の国際連携活動に今後も引き続き携わります。

4-2-2-1-2. 23rd Annual FIRST Conference Vienna への参加(2011 年 6 月 11 日-17 日)

FIRST の第 23 回年次会合が 6 月 11 日から 17 日までオーストリアのウィーンで開催されました。本会合は、サイバーインシデントの予防、対応、技術分析等に関する最新情報の交換、および国や文化等の壁を越えたインシデント対応チームの連携強化を目的に毎年開催されており、今年は “Security Lessons – what can history teach us” のテーマのもと、様々な話題が取り上げられました。

また、本年度は、JPCERT/CC から以下の 3 つの口頭発表又はパネルディスカッションへの参加を行い、各国の CSIRT に対して日本の現状を伝えるとともに、引き続きの連携、協力を依頼しました。

- 『Looking into Malicious Insiders』 発表者 小宮山 功一朗
- 『Cyber Clean Center Project - A five year retrospective』発表者 中津留勇
- 『SPECIAL Panel Session: The day disaster struck the northeastern part of Japan』モデレーター 内山貴之

このうち 3 番目のパネルディスカッションは、FIRST に加盟している日本の CSIRT の団体「JFIRST」の有志が、震災に見舞われた日本の状況に対する海外メンバーの関心の高さを受けて急遽企画したものです。
日本の通信インフラ企業、セキュリティコンサルティング企業、ISP、インターネット総合サービスプロバイダの CSIRT の代表者をパネリストに迎え、「The Great East Japan Earthquake - What we did as CSIRTs-」と題して、2011 年 3 月 11 日に発生した東日本大震災の直後やその後数ヵ月間、CSIRT が直面した問題やその対応について、各パネリストがその経験を参加者と共有しました。
各パネリストからは、共通して、常日頃から災害に備えることの重要性と、想定外の事案に対しても柔軟に対応することの重要性が強調されました。また、災害時における SNS を活用したコミュニケーションの有効性も指摘されていました。

そのほか、JPCERT/CC では、この機会を利用して、アジア太平洋地域や欧州各国の National CSIRT や今回の会合からはじめて参加した National CSIRT などとの個別の意見交換や、APCERT 加盟 CSIRT が集う意見交換会を企画/主催するなど、国際間の CSIRT 連携をさらに強化させるための様々な活動も併せて行いました。

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今後も努めてまいります。第 23 回 FIRST 年次会合年次会合についての詳細は、以下の URL をご参照ください。

23rd Annual FIRST Conference Vienna
http://conference.first.org

また、本四半期は、株式会社 NTT データの組織内 CSIRT である NTTDATA-CERT のスポンサー（加盟チームに関する保証を与え、FIRST の規約に従い加盟手続を支援するチーム）を務め、同組織は 4 月 20 日に正式に FIRST 加盟に至りました。
2011 年 6 月末現在、日本からの FIRST 加盟チームは、19 チームとなっています。

4-2-2-2. National CSIRT Meeting への参加(2011 年 6 月 18 日-19 日)

第 23 回 FIRST 年次会合後に、引き続きオーストリアのウィーンにて、CERT/CC が主催する National CSIRT Meeting が開催されました。世界各国の National CSIRT が一堂に会し、国を代表するインシデント対応チームとしての活動や課題を共有するとともに、共同プロジェクトや研究調査について発表や議論を行ない、今後の一層の連携強化に繋がる成果を得ることができました。JPCERT/CC からは、APCERT の新ビジョン「APCERT will work to help create a safe, clean and reliable cyber space in the Asia Pacific Region through global collaboration」を紹介するとともに、本ビジョンに基づく活動計画を発表し、好評を得ました。National CSIRT Meeting についての詳細は、以下の URL をご参照ください。

Annual Meeting for CSIRTs with National Responsibility
http://www.cert.org/csirts/national/meeting/

4-2-2-3. 中国語圏における情報収集発信

JPCERT/CC では中国語圏（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積極的に行っています。
本四半期は、5 月 11 日に北京で開催された「第 15 回中国国際ソフトウェア博覧会 2011」に参加し、中国におけるクラウドコンピューティングの情報セキュリティに関する情報収集を行うとともにキーパーソンとの意見交換を行いました。収集した情報は、日本国内の関係者会合などへ展開する予定です。

4-2-3. ブログや Twitter を通した情報発信

英語ブログ(blog.jpcert.or.jp)や Twitter(twitter.com/jpcert_en)を利用し、日本やアジア太平洋地域の情報セキュリティに関する状況や JPCERT/CC の活動等について情報発信を行っています。
本四半期は、タイ、インドネシアで開催されたセキュアコーディングセミナーの報告や FIRST Conference の模様に関してブログにエントリーを掲載しました。

Secure Coding Seminar in C/C++ Successfully Completed!
http://blog.jpcert.or.jp/2011/06/secure-coding-seminar-in-cc-successfully-completed.html

What CSIRTs in Japan Did in the Aftermath of the Earthquake - Special Panel Session -
http://blog.jpcert.or.jp/2011/06/what-csirts-in-japan-did-in-the-aftermath-of-the-earthquake---special-panel-session-.html

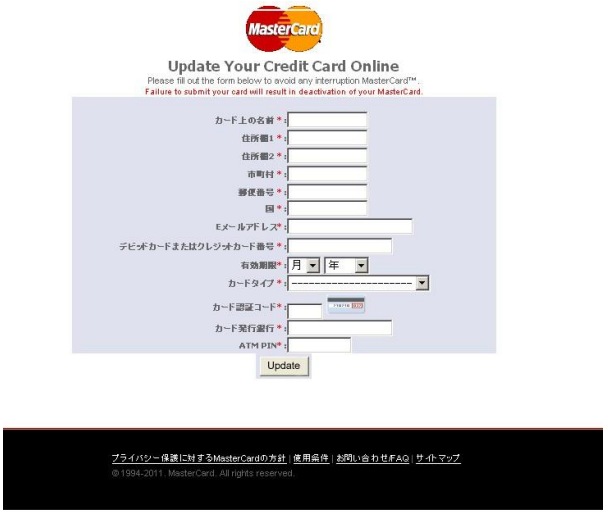
5. フィッシング対策協議会事務局の運営

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

本四半期は、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 13 件発信しました。

また、本四半期には、日本人をターゲットにしていると思われるマスターカードを騙るフィッシングサイトを複数確認しています。協議会では、4 月 25 日と 5 月 16 日に緊急情報として Web 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ました。



[図 5-1　マスターカードを騙るフィッシングサイト
https:// www.antiphishing.jp/news/alert/mastercard2011425.html]

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、新たにデジ

タルアーツ株式会社 (2011 年 5 月より)、シスコシステムズ合同会社 (2011 年 6 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 13 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. 海外カンファレンス参加

2011 年 4 月にマレーシアのクアラルンプールで開催された APWG CeCOS V 2011 Kuala Lumpur に参加し、日本国内のフィッシング詐欺の状況と事例として、東日本大震災の義援金を騙るフィッシング詐欺について紹介しました。また、海外におけるフィッシング詐欺やフィッシング対策プロジェクトについて情報収集を行い、その結果を協議会会員に展開しました。

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) 瀬古 敏智「増加するフィッシング詐欺　今、何ができるのか」
IAjapan 第 9 回 迷惑メール対策カンファレンス,2011 年 5 月 27 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 4 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/20114.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/201105.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/201106.html

5-6. 普及啓発コンテンツの充実

本四半期は、2010 年度の技術・制度ワーキンググループ活動で作成した以下の 2 つの資料を公開いたしました。

(1) フィッシング対策ガイドライン (2011 年度版)
https://www.antiphishing.jp/report/guideline/wg821.html

(2) フィッシングレポート 2011
https://www.antiphishing.jp/report/wg/phishing_report2011.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「US-CERT に聞く セキュリティ対策のベストプラクティス : ステークホルダー間の状況認識の共有と協調動作の重要性」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、「US-CERT に聞く セキュリティ対策のベストプラクティス : ステークホルダー間の状況認識の共有と協調動作の重要性」を公開しました。米国国土安全保障省(DHS)配下の情報セキュリティ対策組織である US-CERT におけるセキュリティ対策への取り組みや活動について紹介しています。

US-CERT に聞く セキュリティ対策のベストプラクティス : ステークホルダー間の状況認識の共有と協調動作の重要性
(2011 年 5 月 19 日)
https://www.jpcert.or.jp/magazine/security/field-us.html

7. 講演活動一覧

(1) 真鍋 敬士(理事,分析センター長) :
「最新インシデント動向とその対策」
沖縄県・沖縄 IT 企業信頼性確保推進コンソーシアム
第 1 回 ISMS・P マーク・CMMI 普及セミナー,2011 年 4 月 13 日

(2) 久保正樹 (情報流通対策グループ 脆弱性アナリスト) :
「セキュアコーディング, その重要性」
国立情報学研究所 トップエスイープロジェクト 「セキュリティ概論」講義,
2011 年 4 月 15 日

(3) 戸田 洋三 (情報流通対策グループ リードアナリスト) :
「セキュアコーディング, 実践」
国立情報学研究所 トップエスイープロジェクト 「セキュリティ概論」講義,
2011 年 4 月 22 日

(4) 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) :
「海外 CSIRT 構築支援（アフリカ編）」
日本シーサート協議会 第 7 回 ワーキンググループ会,2011 年 4 月 22 日

(5) 久保正樹 (情報流通対策グループ 脆弱性アナリスト) :
「Japan Phishing Report」
Workshop Seminar on Information Security－スラバヤ, 2011 年 5 月 24 日

(6) 久保正樹 (情報流通対策グループ 脆弱性アナリスト) :
「Panel Discussion: Security Trend」
Workshop Seminar on Information Security－スラバヤ, 2011 年 5 月 24 日

(7) 瀬古 敏智(早期警戒グループ情報セキュリティアナリスト,フィッシング対策協議会) :
「増加するフィッシング詐欺 今、何ができるのか」
IA japan 第 9 回迷惑メール対策カンファレンス,2011 年 5 月 27 日

(8) 伊藤 友里恵(国際部部長) :
「Making the Internet Clean, Safe and Reliable- Asia Pacific Regional Collaboration Activities」
Second Worldwide Cybersecurity Summit－ロンドン,2011 年 6 月 1 日～2 日

(9) 小宮山 功一朗 (国際部マネージャ) :
「Looking into Malicious Insiders」
23rd Annual FIRST Conference－ウィーン,2011 年 6 月 13 日

(10) 中津留 勇(分析センター 情報セキュリティアナリスト) :
「Cyber Clean Center Project - A five year retrospective」
23rd Annual FIRST Conference－ウィーン,2011 年 6 月 14 日

(11) 内山 貴之(情報流通対策グループ/国際部 情報セキュリティアナリスト) :
「SPECIAL Panel Session: The day disaster struck the northeastern part of Japan」
23rd Annual FIRST Conference－ウィーン,2011 年 6 月 14 日

(12) 満永 拓邦(早期警戒グループ 情報セキュリティアナリスト) :
「最新インシデント傾向とその対策」
マネジメントシステム評価センター,2011 年 6 月 15 日

(13) 早貸 淳子(常務理事) :
「情報窃取目的によるサイバー攻撃の高度化の現状と対策の見直しの必要性」
@IT 情報漏えい対策セミナー 防ぐ、見つける、拡散を抑える―現実的な情報漏えい対策とは,2011 年 6 月 16 日

(14) 伊藤 友里恵(国際部部長) :

「Making the Internet Clean, Safe and Reliable- Asia Pacific Regional Collaboration Activities」
Annual Meeting for CSIRTs with National Responsibility－ウィーン,2011 年 6 月 19 日

8. 執筆・取材記事一覧

(1) 梅村 香織(国際部 渉外担当)：
「APCERT 年次総会および関連会合開催報告」
社団法人 日本ネットワークインフォメーションセンター JPNIC News & Views vol.839 臨時号,2011 年 4 月 20 日

(2) 中尾 真二(事業推進基盤グループ 広報)：
「特別レポート CSIRT 構築の機運が高まるアフリカ」～日本シーサート協議会 第 7 回ワーキンググループ会から
日経 BP ITpro,2011 年 5 月 26 日

(3) 古田 洋久(情報流通対策グループ マネージャ)：
制御システムのセキュリティ対策と今後の課題
「制御システムセキュリティ評価ツールの公開と活用のすすめ」
月刊計装,2011 年 6 月 10 日

9. 開催セミナー等一覧

(1) C/C++ セキュアコーディング2dayセミナー ThaiCERT@バンコク
※本セミナーの詳細は、「2-5-1」をご参照ください。

(2) C/C++ セキュアコーディング1day tutorial @JCSSE2011
※本セミナーの詳細は、「2-5-1」をご参照ください。

(3) C/C++ セキュアコーディング2dayセミナー Id-SIRTII@スラバヤ
※本セミナーの詳細は、「2-5-2」をご参照ください。

(4) 企業向けC/C++ セキュアコーディングセミナー
※本セミナーの詳細は、「2-5-4」をご参照ください。

10. 後援・協力一覧

(1) IA japan 第 9 回 迷惑メールカンファレンス 2011（主催：財団法人インターネット協会(IA japan) 迷惑メール対策委員会） 2011 年 5 月 27 日

(2) IAF フォーラム 2011(主催：IAF(Industrial Automation Forum)) 2011 年 6 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 ：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