JPCERT CC®

JPCERT-PR-2011-0004

発行日：2011-10-11

JPCERT/CC 活動概要 [2011 年 7 月 1 日 ～ 2011 年 9 月 30 日]

【活動概要トピックス】

—トピック 1 —
脆弱性取扱において連絡がとれない製品開発者一覧の公表を開始

9 月 29 日より JVN 上に「連絡不能者一覧」のページを設けて、脆弱性が改善されないままになったソフトウェアの開発者に関する情報を公表し、関係者に連絡を取るための情報を広く求め始めました。これは、昨年度改定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および JPCERT/CC 脆弱性関連情報取扱いガイドラインに基づいた措置です。

脆弱性が発見され届出されたものの、製品の開発者と連絡がとれない場合の取扱方法について、旧来のガイドラインでは明確に規定されていなかったため、進展の見込みがないまま長期わたって取扱が滞留している案件が少なからず累積し、脆弱性対策や関連情報の円滑な流れを停滞させる要因の一つとなっていました。

「連絡不能者一覧」の公開は、そうした状況に陥っている脆弱性情報の取扱を進めるため、製品開発者ないし関係者についての情報を広く一般に求めるために新たに採用された調整手順の一つです。具体的には、連絡先が不明または JPCERT/CC からの連絡に対して一定期間にわたりまったく応答が無い製品開発者の名称を公表し、JPCERT/CC と IPA が連絡を求めていることを周知し、それでも新たな情報が得られない場合には、さらに製品名も追加公表して、開発者に関する情報を求めることになっています。本改定の趣旨をご理解いただき、本制度の円滑な運用と実効性の向上にご協力いただけるようお願い致します。JPCERT/CC では、脆弱性の低減を通じて、ソフトウェア等製品利用者のさらなるサイバーリスク軽減のために努力していきます。

脆弱性関連情報における連絡不能な製品開発者の一覧を公表
https://www.jpcert.or.jp/press/2011/PR20110929-jvn.pdf

―トピック 2―
国内金融機関や政府機関への攻撃における調整活動

今四半期に発生した攻撃活動で、JPCERT/CC が調整に関与したもののうち特徴的だった事案は、8 月に発生した国内金融機関を装ったフィッシングメールとフィッシングサイトの出現、および、海外からなされたと推定される 9 月以降における政府機関などのサイトへの攻撃でした。

8 月の事案では、従来も散見されたフィッシングサイトに誘導するフィッシングメールに、マルウエアが添付されたフィッシングメールという新しいタイプが加わり、合わせて 2 種類の攻撃法を確認しました。前者については、フィッシングサイトの確認、サイト閉鎖のための海外の National CSIRT および ISP との調整業務にあたりました。後者については、添付されたマルウエアに感染すると取引時に入出力される機微な個人情報が漏えいする恐れがあるので、マルウエアを解析するなどして情報の送信先サーバーを割り出し、これを停止するためにサーバー管理者への依頼、停止の確認などの措置を取りました。

9 月の事案では、9 月初旬に中国のサイトにて行われた攻撃予告の情報をキャッチし、入手した DDoS 攻撃対象リストなどから、標的とされた組織や攻撃対象を割り出し、当該組織に対して事前に情報提供を行いました。また、攻撃予告日の数日前から攻撃が行われた事を受け、攻撃予告日まで特別対応態勢を敷き、中国の CNCERT/CC と情報共有および連携作業により、実際に DDoS 攻撃や Web 改ざん攻撃が行われた組織に対してインシデント対応を行いました。本件は日中両国における歴史的事件に関連するデモンストレーションであると思われます。JPCERT/CC では、このように毎年定例的になされる攻撃活動についても、事前情報収集と事後対応を行っています。

―トピック 3―
アジア・大洋州地域における CSIRT 構築支援

経済産業省が財団法人海外貿易開発協会（JODC）に委託した「貿易投資円滑化支援事業」のプロジェクトのひとつである、ミャンマーで CSIRT 構築・支援を行う事業において、現地に専門家を派遣する組織に JPCERT/CC が選ばれました。アジア・大洋州地域（オセアニア）における CSIRT の構築や連携促進に関する JPCERT/CC の活動実績を評価しての決定と考えられます。

この決定を受け、9 月には JPCERT/CC 職員 2 名が講師を務めた、ネットワークフォレンジック研修がヤンゴンの mmCERT で実施されました。さらに 12 月にもマルウエア解析（動的解析・静的解析）の研修が予定されています。

また、独立行政法人国際協力機構（JICA）が進める大洋州の島嶼国が共同設置する CSIRT である PacCERT の構築事業においても、アフリカ及びアジア諸国での CSIRT 構築支援の実績を持つ数少ない国内組織として、JPCERT/CC の知見が求められ、プロジェクトに参画しています。

本四半期には、職員 2 名を派遣し、フィジーで開催された South Pacific ICT EXPO 2011(SPICTEX 2011)において CSIRT の役割や重要性について講演するとともに、今後の支援計画の協議や情報交換を現地の関係者と行いました。SPICTEX 2011 は、大洋州で初となる ICT 関連の国際会議として周辺諸国の ICT 関係者が一堂に会しました。そのため、多くの各国関係者と接触することができ、彼らとの交流および議論を通じて、PacCERT 構築の重要性のアピール、情報セキュリティに関する情報交換、および現地チャネルづくりが実現できました。

今回の派遣によって築いた大洋州諸国との関係は、PacCERT 構築のプロセスにおいて、人的ネットワーク作りと各国との調整に役立つものと考えます。

―トピック 4―

Java セキュアコーディングスタンダード（並行処理編）の公開

「CERT Oracle Java セキュアコーディングスタンダード」(原題: The CERT Oracle Secure Coding Standard for Java)は、カーネギーメロン大学ソフトウェア工学研究所が、Oracle 社、および Java の専門家とともに開発した Java のコーディング規約集です。JPCERT/CC は、この開発に貢献するとともに、ドキュメントを日本語に翻訳し、公開しています。

この「CERT Oracle Java セキュアコーディングスタンダード」の中から、並行処理プログラミングに関連するガイドラインをまとめた技術報告書(technical report)「Java Concurrency Guidelines」について、8 月に日本語版を公開しました。

マルチスレッドプログラミングによる並行処理が原因で発生する障害の再現や解析、テストは複雑でコストもかかるものですが、本ドキュメントに記載されたコーディング規約に従って、安全なプログラムを開発することで、開発及びテスト等のコスト低が期待できます。

近年、スマートフォンや各種モバイルデバイスの普及に伴って Java のプログラミング需要が高まっておりますが、セキュリティ対策が追い付いていない現状が危惧されています。JPCERT/CC では、C/C++に関するセキュアコーディング関連に続き、Java セキュアコーディングについての啓発や情報提供が急務になっていると考え、この分野の技術資料の開発などの活動に努めています。

Java セキュアコーディングスタンダード 並行処理編
https://www.jpcert.or.jp/securecoding_materials.html#certjavacon

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」、「4.国際連携活動関連」、「**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 1718 件、インシデント件数ベースでは 1676 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 642 件でした。前四半期の 654 件と比較して 2% 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_Report20111011.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、226 件で、前四半期の 325 件から 30%減少しました。また、前年度同四半期（487 件）との比較では、54%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	7 月	8 月	9 月	国内外別合計（割合）
国内ブランド	9	4	18	31(14%)
国外ブランド	53	77	35	165(73%)
ブランド不明	9	9	12	30(13%)
月別合計	71	90	65	226(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 31 件と、前四半期の 118 件から 74 % 減少しました。これは、前四半期まで多数報告されていた国内ポータルサイトを装ったフィッシングサイトが大幅に減少したためです。
国内ポータルサイトを装ったフィッシングサイトは、2009 年 6 月以降、大量に確認されていました。これらのフィッシングサイトは、侵入された第三者のサーバに設置されたものではなく、レンタルサーバや、動的 DNS サービスを使用したモバイルネットワーク上の PC に設置されていたことが特徴的でした。
2011 年 6 月末に国内ポータルサイトを装ったフィッシング詐欺を行っていたグループが逮捕され、このグループの活動が停止したことにより、本四半期における国内ポータルサイトを装うフィッシングサイトの報告は大幅に減少しました。
一方、国外ブランドを装ったフィッシングサイトの件数も 165 件と、前四半期の 173 件から 5% 減少しました。

フィッシングサイトの調整先の割合は、国内が 58%、国外が 42% と、前四半期の割合（国内 42%、国外 58%）と比較して、国内への調整が増えました。
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は海外レンタルサーバを使用していましたが、このタイプのフィッシングサイトが減少したことによって海外への通知が減ったためです。

また、フィッシングサイトのうち、金融関連のサイトを装ったものが 67% を占めました。
前四半期のブランド種別割合では金融関連サイトが 45%、ポータルサイトが 35 % を占めていましたが、本四半期は国内ポータルサイトを装ったフィッシングサイトの減少により、フィッシングサイトのブランド種別においてポータルサイトが占める割合が 4 % まで減少し、相対的に金融関連サイトが占める割合が 45%から 67% に増加しました。

本四半期に報告が寄せられた Web サイト改ざんの件数は、73 件でした。前四半期の 34 件から 115% 増加しています。
7 月から 8 月にかけて、検索サイトの画像検索結果を悪用した攻撃に組み込まれたサイトと、オープンソースの E コマースサイト構築アプリケーションである osCommerce を使用したサイトに対する改ざんが多数報告されました。

画像検索結果を悪用した攻撃では、攻撃者が脆弱なサーバに悪意のあるファイルを設置したうえ、画像検索サイトで検索頻度の高いキーワードと関連付けしていて、利用者が画像を閲覧した際に、ウイルス対策ソフトを装ったマルウエアをダウンロードさせるサイトに利用者を誘導する仕組みになっていました。

osCommerce を使用したサイトに対する改ざんでは、title タグなどの後ろに iframe や JavaScript が埋め込まれており、ページの読み込み時に不審なサイトにアクセスさせる仕組みになっていました。

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 Web 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：10 件　https://www.jpcert.or.jp/at/

2011-07-06　ISC BIND 9 サービス運用妨害の脆弱性に関する注意喚起
2011-07-08　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)
2011-07-13　2011 年 7 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起
2011-08-10　2011 年 8 月 Microsoft セキュリティ情報 (緊急 2 件含) に関する注意喚起
2011-08-10　Adobe Flash Player の脆弱性に関する注意喚起
2011-08-31　Apache HTTP Server のサービス運用妨害の脆弱性に関する注意喚起
2011-09-07　Remote Desktop (RDP) が使用する 3389 番ポートへのスキャンに関する注意喚起
2011-09-14　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起
2011-09-15　Apache HTTP Server のサービス運用妨害の脆弱性に関する注意喚起（更新）
2011-09-22　Adobe Flash Player 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：13 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 59 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 13 件でした。

2011-07-06　2011 年 7 月にサポート終了する Microsoft 製品
2011-07-13　ISC BIND のサポート状況について
2011-07-21　平成 22 年度版ウェブ健康診断仕様公開
2011-07-27　SSH ブルートフォース攻撃
2011-08-03　情報処理の高度化等に対処するための刑法等の一部を改正する法律
2011-08-10　Java SE 6 サポート終了に備えて
2011-08-17　Web ブラウザのセキュリティ関連アドオン
2011-08-24　Web 経由で配信されるマルウエア動向
2011-08-31　CSIRT スタータキット
2011-09-07　CNCERT/CC Weekly Report
2011-09-14　スマートフォン&タブレットの業務利用に関するセキュリティガイドライン
2011-09-22　Adobe Reader 8.x および Acrobat 8.x のサポート終了
2011-09-28　Apache HTTP Server の脆弱性（CVE-2011-3192）の対策はお済みですか？

1-2-1-3. 早期警戒情報

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、大きな影響を与えうる脅威について分析・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

本四半期における情報収集・分析・提供(早期警戒活動)の事例を紹介します。

1) BIND の脆弱性情報に関する情報収集・提供

Internet Systems Consortium, Inc.（以下、ISC という）から 7 月上旬に BIND 9 のサービス運用妨害の脆弱性に関する情報が公開されました。本脆弱性が悪用されると BIND 9 を使用した DNS サーバ（権威 DNS サーバ、キャッシュ DNS サーバ）がサービス不能状態になって、ドメイン名を使ったサービス（Web の閲覧や、メールの送受信など）が利用できなくなること、また BIND が広く使われていることを勘案して、重大な問題と JPCERT/CC では判断し、国内の企業、組織のシステム管理者を対象に、修正済みのバージョンへの更新をうながす注意喚起を行いました。

ISC BIND 9 サービス運用妨害の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2011/at110019.html

2) 歴史的な記念日のサイバー攻撃予告への対応

歴史的な記念日には、日本の政府関係組織等に向け反日的なサイバー攻撃が毎年のように発生してきたことから JPCERT/CC では、そうした特定の日の前後には特に注意深く情報収集を行っています。本四半期には、8 月 15 日と 9 月 18 日の 2 つの特別日がありました。

8 月 15 日に関しては、8 月上旬、韓国の掲示板サイトに「日本の民間サイトおよび匿名掲示板サイトにサイバー攻撃を行う」との予告が書き込まれ、これを確認した JPCERT/CC では、実際に攻撃の可能性があると判断し、攻撃対象とされた民間サイトの管理者に情報共有を行うとともに、韓国の KrCERT/CC と連携して攻撃に関する情報収集を行いました。さらに、攻撃範囲が拡大した場合に備えて緊急対応態勢をとるとともに、政府や自治体を含む重要インフラ事業者、国内の大手企業などの主要な Web サイトの稼働状況の継続的な観測（Web サイトの応答時間の測定）などを行いました。結果的には、一部匿名掲示板サイトで一時的に閲覧できなかったりするなどの影響が発生しましたが、主な政府サイトや民間サイトへの影響は確認されませんでした。

さらに 9 月 18 日については、9 月上旬、中国のサイトに「日本のサイトに対してサイバー攻撃を行う」との予告がなされ、この情報を確認した JPCERT/CC では、政府や自治体を含む重要インフラ事業者等への攻撃が発生する可能性があると判断し、重要インフラ事業者等に事前の対策をうながすための早期警戒情報を提供しました。さらに、攻撃が発生した場合に備えて緊急態勢をとるとともに、政府や自治体を含む重要インフラ事業者、国内の大手企業などの主要な Web サイトの稼働状況の継続的な観測（Web サイトの応答時間の測定）などを行いました。なお、本件では、一部政府や民間サイトで DDoS 攻撃の影響と思われる Web サイトの応答時間の悪化と、民間サイトでの Web ページの改ざんが生じました。前者のサイト管理者に対しては、攻撃対象となっている旨の情報提供を JPCERT/CC から行い、後者のサイトの管理者には、状況確認と問題解決を促しました。

3) Apache HTTP Server の攻撃ツール公開

8 月下旬、Apache HTTP Server（以下、Apache という）を対象とした攻撃ツールが公開されました。JPCERT/CC では、攻撃ツールを入手してテストを行い、Apache が動作するサーバが攻撃を受けた場合に、他のサービスも含めてシステム全体がサービス不能状態に陥る可能性があることを確認しました。また、この攻撃ツールが未修正の脆弱性を使用していることと、Apache が非常に多くの Web サイトで利用されていることを考慮し、ベンダから修正プログラムが公開されるまでの期間は、国内の重要インフラ事業者などを対象に早期警戒情報として通知先を限定した情報提供を行い、ベンダからの修正プログラムが公開されたタイミングにあわせて、国内の企業、組織のシステム管理者を対象に広く注意喚起を行いました。

Apache HTTP Server のサービス運用妨害の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2011/at110023.html

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

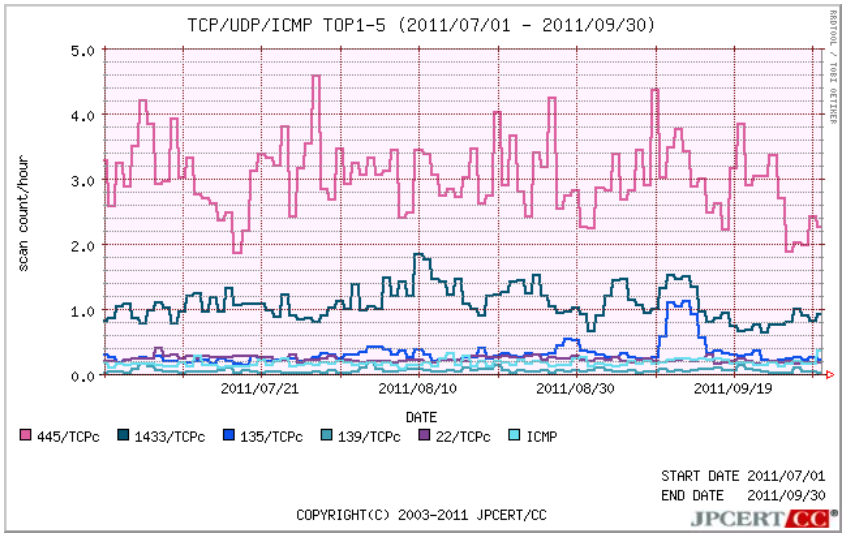
1-3-1. ポートスキャン概況

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

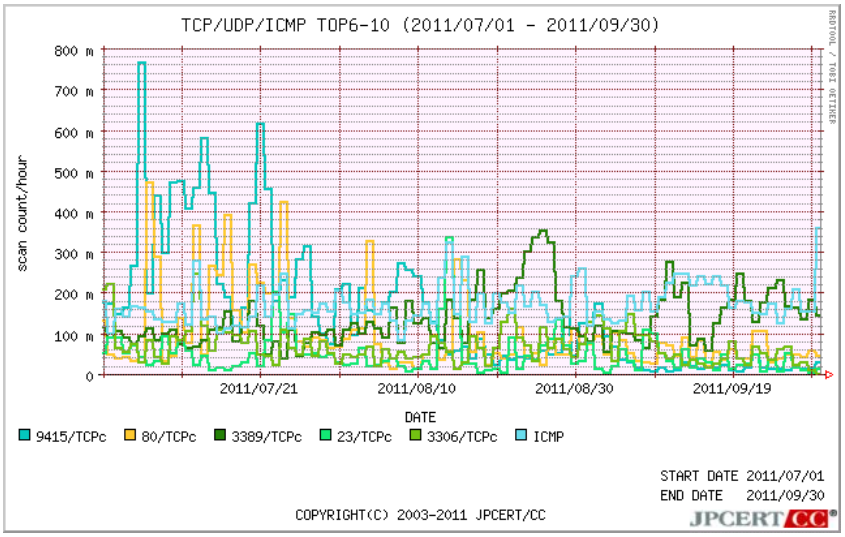
本四半期に ISDAS で観測されたアクセスの宛先ポートの上位 1 位～5 位及び 6 位～10 位のそれぞれについて、アクセス数の時間的の推移を[図 1-1]と [図 1-2]に示します。

- アクセス先ポート別グラフ top1-5 (2011 年 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]

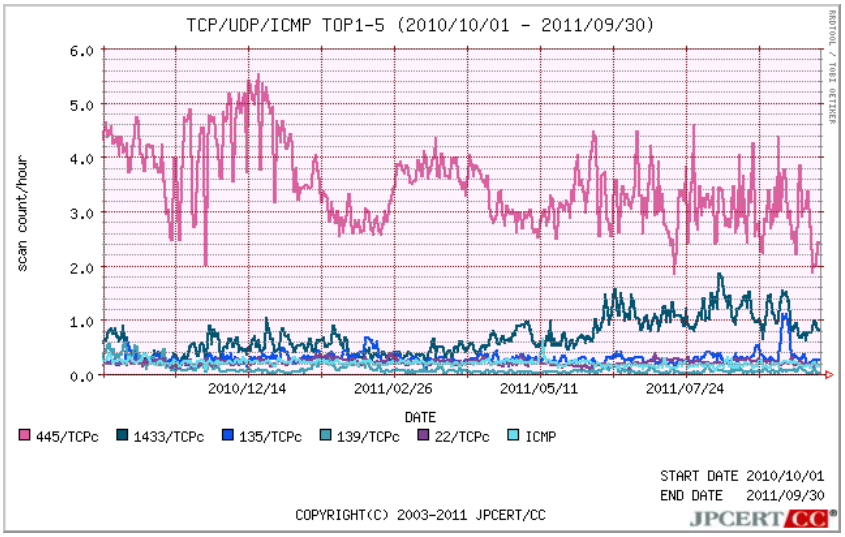
- アクセス先ポート別グラフ top6-10 (2011 年 7 月 1 日-9 月 30 日)



[図 1-2：アクセス先ポート別グラフ top6-10]

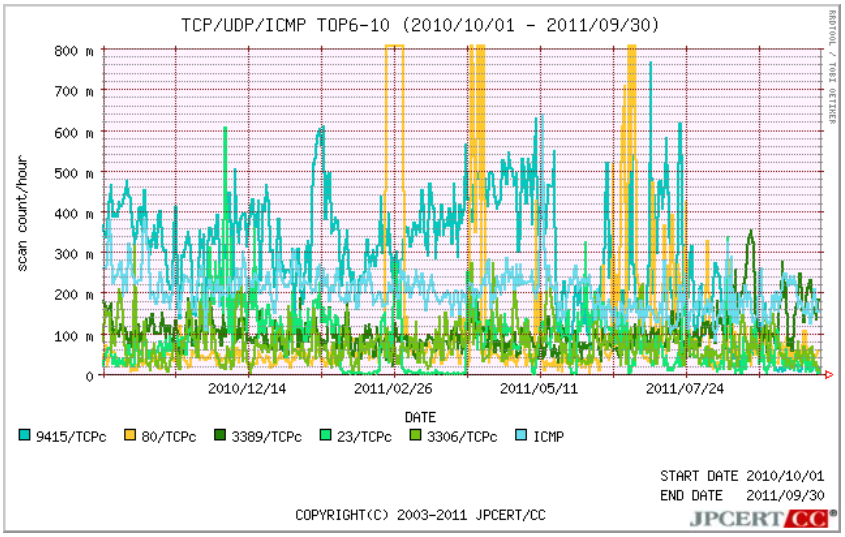
また、より長期間のスキャン推移を見るため、2010 年 10 月 1 日から 2011 年 9 月 30 日までの期間における、アクセスの宛先ポートの上位 1 位～5 位及び 6 位～10 位のそれぞれについて、アクセス数の時間的の推移を[図 1-3]と[図 1-4]に示します。

- アクセス先ポート別グラフ top1-5 (2010 年 10 月 1 日-2011 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 (2010 年 10 月 1 日-2011 年 9 月 30 日)



[図 1-4: アクセス先ポート別グラフ top6-10]

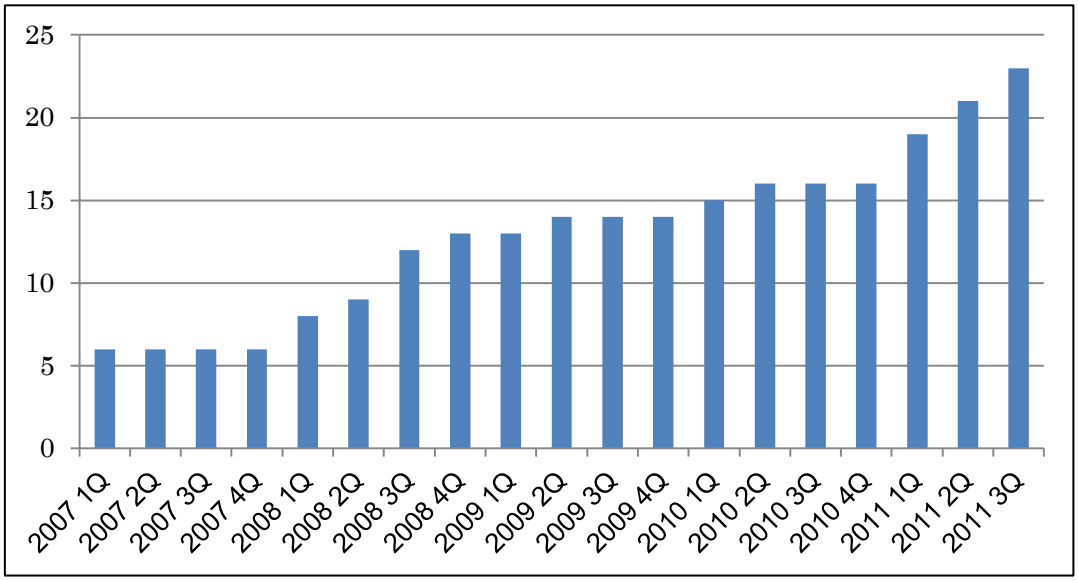
これまでの傾向と同様、 Windows や Windows 上で動作するソフトウエアへの スキャン 活動や、Telnet、SSH サーバなどコンピュータを遠隔操作で使う場合にサーバ側が待ち受けているポートへのスキャン活動が観測されています。そのほか、アクセス制御が不十分な、Proxy サーバへの スキャン が引き続き観測されています。

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、インフォセック(InfoCICSIRT)と A3 セキュリティ(A3-CSIRT)が、新規に加盟しました。本期末時点で 23 の組織が加盟しています。これまでの参加組織数の推移は[図 1-5]のとおりです。



[図 1-5 日本シーサート協議会 加盟組織数の推移]

７月には、新たなワーキンググループとして Honeynet Project Japan Chapter WG が立ち上がりました。「Honeynet Project」は、囮として攻撃対象になるネットワーク「Honeynet」を構築し、攻撃者の侵入や侵害行為を記録することにより攻撃者の手法や行動を明らかにする事で、インターネットのセキュリティ向上に役立てる活動を行っている国際的なセキュリティプロジェクトです。このワーキンググループは、Honeynet Project の日本支部として、日本シーサート協議会メンバと Honeynet Project とが連携できるような環境の提供をめざす予定です。

8 月には、第 5 回総会ならびに第 8 回ワーキンググループ会が開催されました。総会では運営委員の改選が行われ、JPCERT/CC から村上晃が就任し、今年度も事務局は JPCERT/CC が行うことになりました。ワーキンググループ会では、参加した 21 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、総会の翌週に行われた第 50 回運営委員会において、村上晃が運営委員長に再任されました。

なお、組織内シーサート課題検討 WG は CSIRT を構築する際に必要となる取り組むべき課題や定義すべき事項についてまとめた「CSIRT スタータキット」の資料を作成しました。この資料は 8 月に日本シーサート協議会の Web サイトにて公開されました。

CSIRT スタータキット

http://www.nca.gr.jp/imgs/CSIRTstarterkit.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。

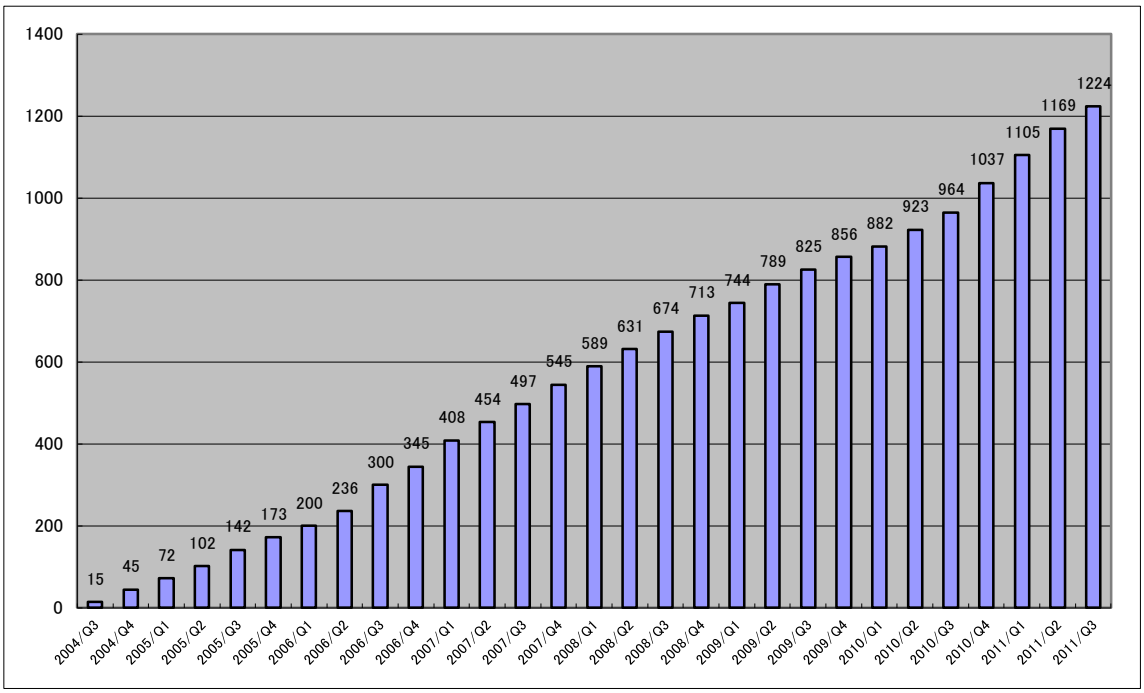
日本シーサート協議会 Web ページ
http://www.nca.gr.jp/

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。

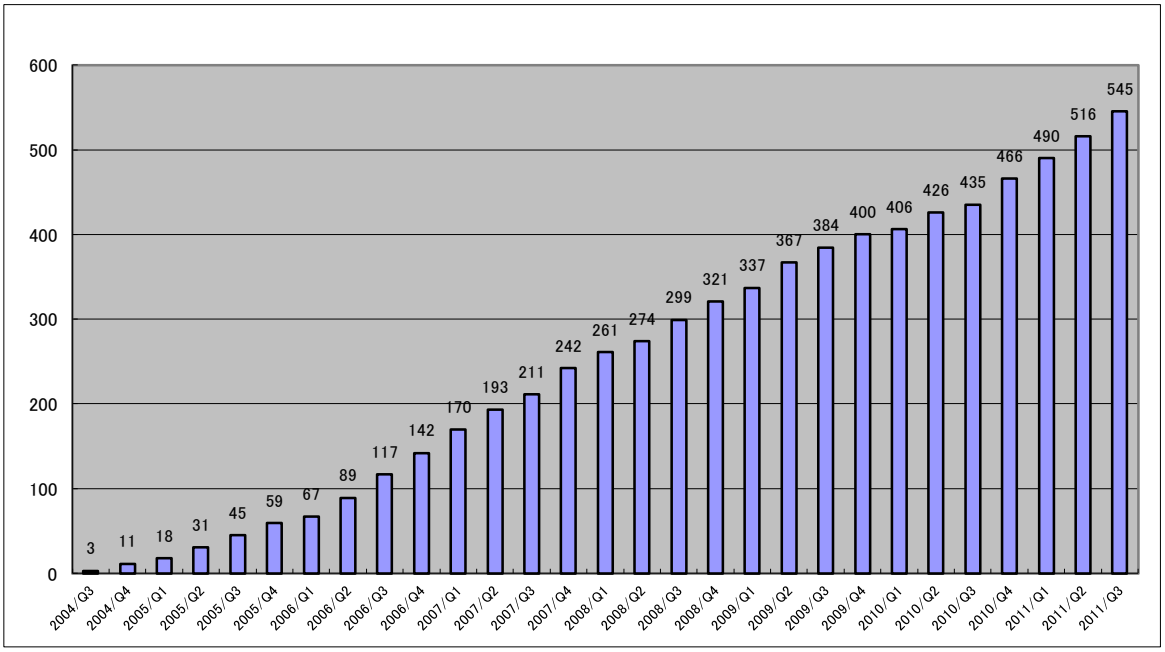
2-1. Japan Vulnerability Notes (JVN) において公開した脆弱性情報および対応状況

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 55 件(累計 1224 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]

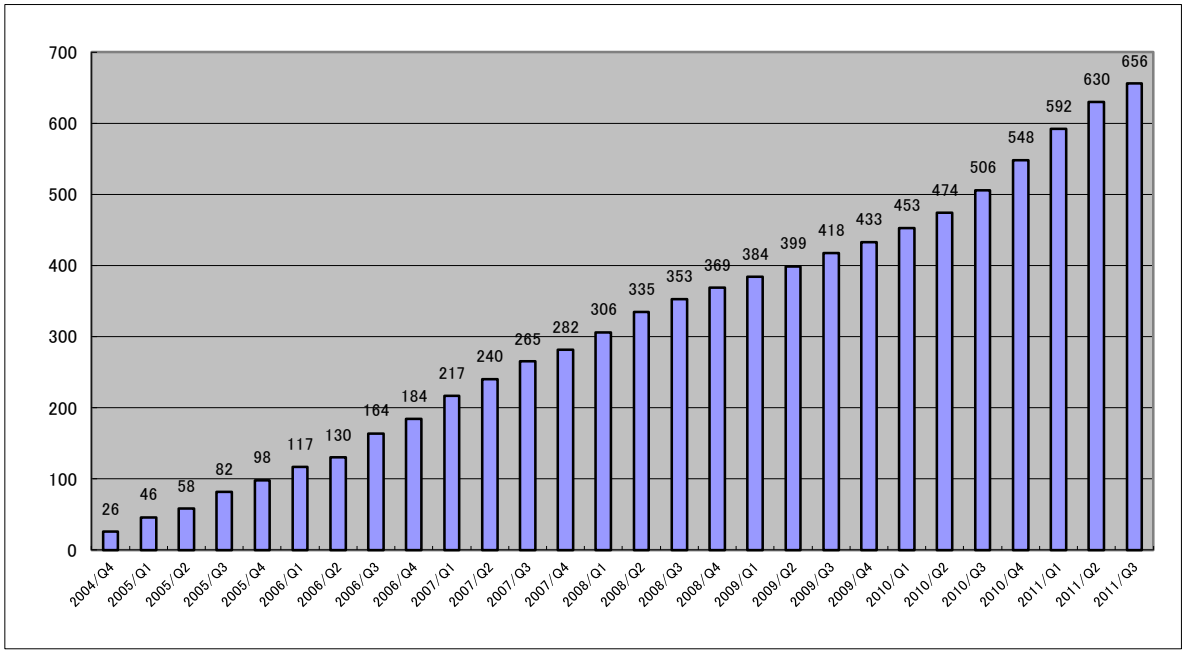
このうち、本基準に従って調整を行い、JVN で JVN#として公開した脆弱性情報は 29 件(累計 545 件) [図 2-2] でした。本四半期に JVN#として公開された案件の半数にあたる 15 件が海外製品開発者の製品であり、本枠組みに基づく JPCERT/CC の調整活動が海外の開発者にも理解され協力が得られるようになってきていると考えられます。



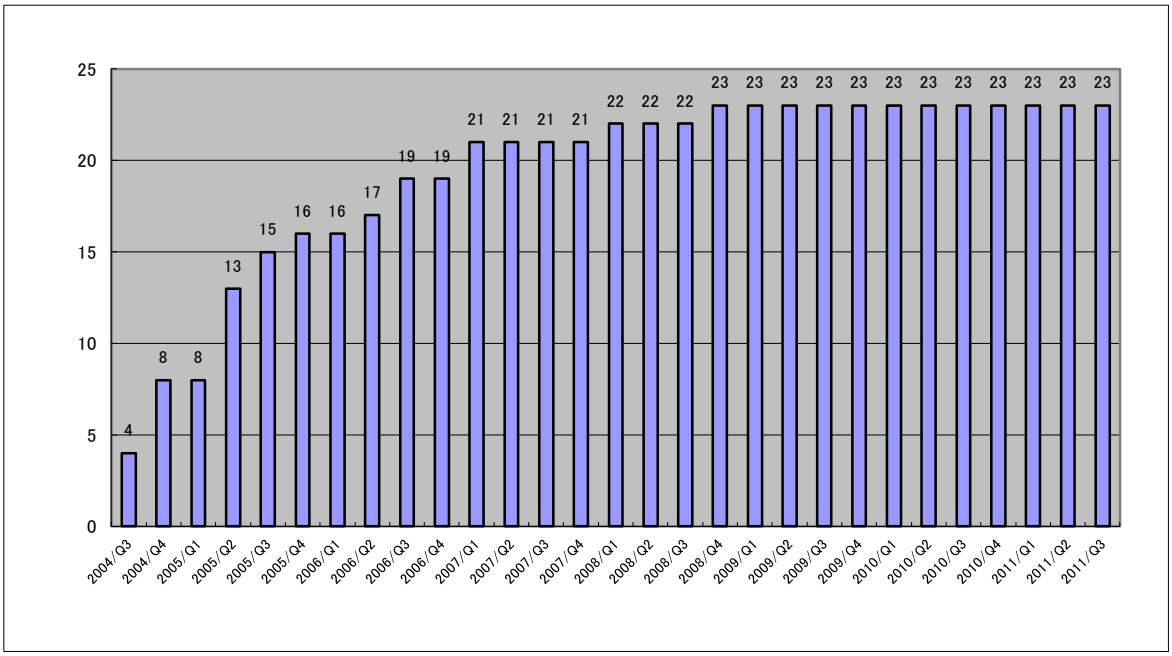
[図 2-2　累計 JVN_JP(JVN#)公開累積件数]

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 26 件(累計 656 件) [図 2-3]でした。そのうち 1 件は、主調整機関として CERT-FI が周知・調整行った国際展開案件でした。本四半期中に JVNVU#および JVNTA として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 5 件、Oracle に関するものが 2 件、Adobe 製品に関するものが 1 件、HP(Hewlett Packerd)に関するものが 1 件、ISC に関するものが 2 件、Apache HTTP Server に関するものが 1 件ありました。このうち ISC BIND および Apache HTTP Server に関しては、いわゆるゼロデイ攻撃や攻撃ツールが観測された脆弱性であり、またいずれもオープンソースソフトウエアであるために、派生製品やベースとして導入し開発された製品群が多く、また利用者も非常に多いソフトウエアであるため、それぞれの開発者からの早急な修正対応が求められるものでした。本四半期に JVNVU#および JVNTA として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。JVN での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が 9 件ありました。

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 2-3　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.　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 2011 年 9 月 29 日より、JVN 上に「連絡不能開発者一覧」というページを設け、連絡不能となっている製品開発者名の公表を開始しました。本四半期において、「連絡不能開発者一覧」に掲載された件数は 50 件ありました。JPCERT/CC はこれら 50 件の製品開発者に関する JVN 講読者からの幅広い情報提供を求めています。また、「連絡不能開発者一覧」の公開前準備期間として、2011 年 4 月から 9 月までの 5 ヶ月間、定期的かつ繰り返し開発者への連絡を行い、9 月中に連絡をいただけない場合は「連絡不能開発者一覧」へ掲載されることついて、事前通知および説明を行いました。その結果、前四半期および本四半期に連絡が取れるようになり、さらには JVN 公表に到った案件が 11 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 9 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調整ができない場合についても、脆弱性をもった製品を、そうと知らされないまま使い続けて、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、一定の要件を満たせば 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間差なく、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。その後はJPCERT/CCが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、20件の脆弱性情報についてJPCERT/CCがCVEを採番し、2件の脆弱性情報について製品開発者であるSamba開発チームが自らCVEを採番、またCNAとして認定を受けている製品開発者であるマイクロソフトが1件のCVEを採番、2件の長期滞留案件に関しては過去に既に第三者によるCVE取得が行われており、合計25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、MITREやその他の組織への確認や照合を必要とする特殊なケースを除いた、90%を超える案件に対しCVE識別子付与されています。
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

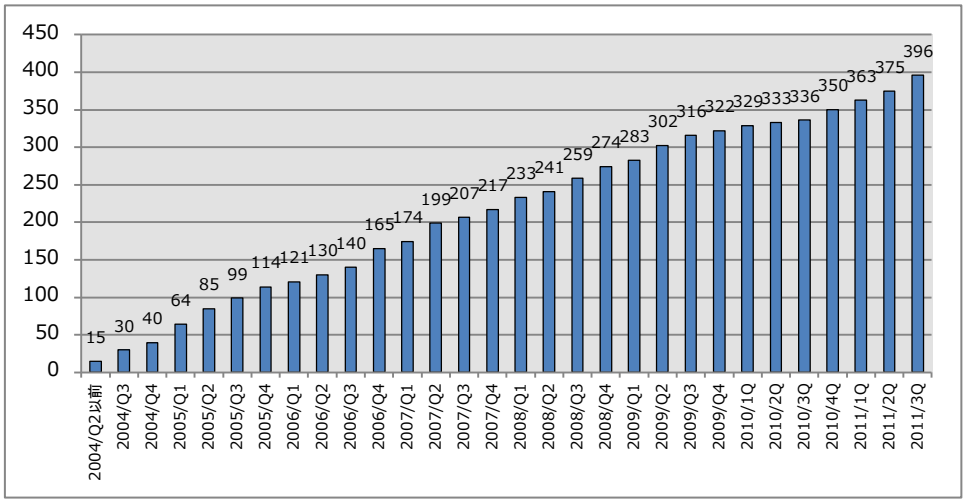
本基準では、受付機関に独立行政法人情報処理推進機構（以下「IPA」といいます。http://www.ipa.go.jp/)、調整機関に JPCERT/CC が指定されています。JPCERT/CC は IPA が受け付けた届出情報の転送を受けて、製品開発者への情報提供を行い、対策情報公開に至るまでの調整を行っています。最終的には、 IPA と共同で、脆弱性情報ポータル JVN において対策情報を公開しています。両組織間においては、脆弱性情報の分析結果や脆弱性情報の取扱い状況等の情報交換を行うなど、緊密な連携をおこなっています。なお、本基準における IPA の活動および四半期毎の届出状況については、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、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 9 月 30 日現在で 396 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]

2-4-3. 脆弱性情報流通体制の普及啓発

オープンソースソフトウエアやその他の製品開発者およびコミュニティに対して、日本国内の脆弱性情報流通体制の認知を向上し、相互理解を深めるため、2011 年 8 月 20 日に開催された OpenSource Conference 2011 Nagoya へ参加しました。脆弱性情報ハンドリング業務内容と活動状況、その他の JPCERT/CC の活動内容について紹介し、オープンソースソフトウエア分野における脆弱性対応について出展コミュニティや一般来場者との意見交換、情報交換を行いました。

[図 2-6　OpenSource Conference 2011 Nagoya 講演の様子]

2-4-4.　国際標準化活動

2-4-4-1.「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に参加しています。VD (29147)は、ベンダーの外側から見える、インターフェースに相当する部分だけを規定し、VHP (30111)は、外部からは見えない部分を含む、ベンダー内部での対応を規定することになっています。

4 月中旬にシンガポールの Nan-yan Technological University (NTU；南洋理工大学)で開催された ISO/IEC JTC1/SC27 の標準化国際会議での論議の結果に基づいて、両標準化文書について担当のプロジェクト・エディタが修正ないし起草した草案が、第 3 次委員会草案 (CD； Committee Draft) および第 1 次作業草案 (WD； Working Draft) として 6 月から 7 月にかけて SC27 事務局を通じて参加各国に送付されました。これらに対して、9 月上旬までに各国がコメントを付して提出し、これをベースに 10 月に、ナイロビ(ケニヤ)で開催予定の次回の標準化国際会議で議論されることになっています。

日本からも JPCERT/CC が中心になって、両標準のカバー範囲の整合が取れていない点や、VHP については脆弱性取扱のための組織体制の整備にも言及する必要がある点などを、VD に対して 25 件、VHP に対して 9 件のコメントを作成し提出しました。

JPCERT/CC では、脆弱性の取扱いに関連した 2 つの国際標準について、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。

2-4-4-2. インシデント管理の国際標準化活動への参加

インシデント管理については、WG4 において標準化が進められてきた「情報セキュリティ・インシデント管理」(ISIM: Information Security Incident Management)が、9 月 1 日、ISO/IEC 27035:2011 first edition として出版され、ひとまず標準化が完了しています。

27035 を補完する標準として現在その必要性が検討されている「インシデントの管理と運用と対応」(IMOP: Incident Management, Operation and Response)については、英国と韓国のラポータが、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ており、現在、以下に示す 4 つのパートからなる標準が提案されています。

Part 1. インシデント管理のためのフレームワーク(Incident management framework)
Part 2. インシデントの対応準備 (Incident response readiness)
Part 3. インシデントの管理と運用と対応 (Incident management, operation, and response)
Part 4. インシデントハンドリング (Incident handling)

この提案に対して、標準化に必要な WG4 内での人的リソースの確保や既存の CSIRT における取組みとの整合性に関する懸念を骨子(趣旨)とする、日本からの寄書を作成し、SC27 事務局を通じて提出しました。次回ナイロビ会議で、英国と韓国からのラポータ報告とともに、IMOP の標準化のあり方をめぐる審議の中で、参加国代表に説明する機会が与えられる予定です。

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. 「Java セキュアコーディング 並行処理編」を公開

JPCERT/CC が翻訳、公開した「Java セキュアコーディング 並行処理編」(原著 CERT/CC「Java Concurrency Guidelines」) は、カーネギーメロン大学ソフトウエア工学研究所の CERT プログラムと Oracle の共同作業の成果である「CERT Oracle Secure Coding Standard for Java」の中から、次のカテゴリに含まれる並行処理プログラミングに関連したガイドラインをまとめた CERT プログラムによる技術資料です。

・可視性とアトミック性 (VNA)
・ロック (LCK)
・スレッド API (THI)
・スレッドプール (TPS)

・スレッドの安全性に関する雑則 (TSM)

マルチスレッドプログラミングによる並行処理が原因で発生する障害の再現や解析、テストは容易でないケースが少なくありません。対応コストが高い問題の発生の多くを回避することができる、セキュアな Java マルチスレッドプログラミングのための手引きとしてご活用ください。

Java セキュアコーディング 並行処理編
https://www.jpcert.or.jp/securecoding_materials.html#certjavacon

2-5-2. 「Android Bazzar and Conference 2011 Summer」と「オープンソースカンファレンス 2011Nagoya」にて講演

本四半期は、以下の 2 つのイベントで講演を行いました。

イベント名：Android Bazzar and Conference 2011 Summer
開催日時：2011 年 7 月 17 日 (日)
講演タイトル：Android アプリ開発にもきっと役立つセキュアコーディング

イベント名：オープンソースカンファレンス 2011 Nagoya
開催日時：2011 年 8 月 20 日 (土)
講演タイトル：セキュアコーディングノススメ (Java 編)

講演では、ソフトウエア開発における脆弱性の混入を防ぎコード品質向上に寄与するセキュアコーディングについて概説し、特に Java 言語での開発を題材に、OSS での事例や Android アプリケーション開発でのポイントなどを織り交ぜて紹介しました。
オープンソースカンファレンス 2011Nagoya の講演では、定員 80 人の会場がほぼ満員となる盛況ぶりでした。また、社内の勉強会や研修資料として使いたいという意見や、セミナ事業へのお問い合わせをいただき、関心の高さが感じられました。
どちらのイベントも、プログラミングを学び始めたばかりの学生から社内で開発プロジェクトに携わっている方まで幅広い層が参加しており、このような場で定期的に講演を行うなどの活動を通じて、セキュアコーディングの普及啓発を続けていくことが重要であると考えています。

2-5-3. 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

制御システム関係者向け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本四半期は計 3 回（7 月 19 日、8 月 1 日、9 月 30 日）配信しました。セキュリティインシデントにかかわ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 JPCERT/CC からのお知らせとともに掲載しています。今後も内容の充実を図っていく予定です。

本ニュースレターの配信先の制御システムセキュリティ情報共有タスクフォースには、現在 181 名のメンバに登録いただいています。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. 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て専門家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や計測展に向けた活動や意見交換を行いました。

また、7 月 15 日にキャンパスイノベーションセンター(東京田町)で開催された日本学術振興会プロセスシステム工学 143 委員会に招かれ、「Stuxnet が塗り替えた制御システムのセキュリティ課題」と題する講演を行いました。この会合は、セキュリティ問題にフォーカスして半日日程で計画され、制御システムの利用者とベンダーからも実情が紹介され、この問題への業界内の関心の高まりを窺えました。

さらに、9 月 13 日～9 月 18 日に早稲田大学で開催された、自動制御と計測システムに関する国際会議「SICE 2011」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、「Myth and Reality on Control System Security Revealed by Stuxnet（Stuxnet で明らかにされた制御システムセキュリティの神話と現実）」と題する講演を行いました。

2-6-3. 海外連携活動

米国は国土保安省（DHS）の下、制御システムのセキュリティ強化施策として、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 と、制御システム業界に関わるユーザ、ベンダ、その他関係者の産官学が連携した ICSJWG (Industrial Control Systems Joint Working Group)などの活動を柱とする、CSSP（Control System Security Program）を進めています。CSSP では、制御システムのセキュリティに関連した複数の教育訓練プログラムを用意しています。そのうち上級者向け教育訓練のコースは、国際パートナーにも受講機会を提供しており、今年度は 9 月 12 日から 9 月 16 日までの日程で「Control Systems Cyber Security Advance Training and Workshop for International Partners」として実施されました。

今回の教育コースには、JPCERT/CC からも積極的に日本の関係者に参加を呼び掛けた結果、JPCERT/CC を含めて日本から 5 名の方に参加をいただきました。この教育コースは、制御システム関係者を対象としたサイバー攻撃からコントロールシステムを保護するためのセキュリティ知識についての座学と訓練用の模擬システムをもちい攻撃・防御のチームに分かれて実施される実戦訓練からなる興味深い内容を含んでいます。現実的なシステムとの違いはあるものの参加者の方からは、「稼働しているシステムに触れてインシデントを経験できることから、実際に問題が起きた際にどの役割の人がどのように行動する必要があるのか、組織にとって何が足りないのかなどを改めて考えるよい機会であった」「攻撃に関して実際に経験することで、どういった点が狙われやすいのかといった視点を養うことができた」といった声を伺うことができました。また、JPCERT/CC は、この教育コース参加の機会を活用して、今後の制御システムセキュリティにおける情報連携体制等について ICS-CERT との調整を行いました。

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

2-6-4. 制御システムセキュリティカンファレンス開催準備

本年度も制御システムに関する産官学の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。カンファレンスの詳細につきましては、次期四半期にご案内させていただく予定です。

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 7 月～9 月			年度累計
MyJVN API	NVD	計	
528 件	1,050 件	1,578 件	3,133 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	70,581 (59,914)	12,398 (19,195)	94% (97%)	6% (3%)
英語版	3,960 (3,796)	8,844 (11,724)	95% (97%)	5% (3%)

（括弧内の数値は前四半期）

[表 1-2]に示したように、前四半期と比較すると、日本語版の VRDA フィードインデックスの利用数の増加が見られますが、脆弱性情報の利用数は減少しています。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い傾向に変化はありません。

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アーティファクト分析という活動を行っています。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を行うためにはソフトウエアやハードウエアといった環境だけではなく、分析対象となる検体や、その検体を安全に保管・分析するための技術が必要になります。日々の業務で培ったそれらの技術を、他の組織の分析技術者や研究者と共有し、相互に分析能力を高めていくことも JPCERT/CC の重要な活動の一つです。本四半期は、他組織との間で検体やその関連情報の交換を行うとともに、分析に関わる技術を経験あるいは習得するためのインターンや講習を実施しました。

3-1. 継続的な人材育成活動—ISS スクエアへの協力

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、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 では過去 2 年間、ISS スクエアの参加大学からインターンを受け入れてきました。本年度もインターン 1 名を受け入れ、マルウエアの分析作業について実践的な業務を体験してもらいました。

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

4-1-1-1. 国際的な情報セキュリティ組織加盟手続きに関する支援

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、APCERT や FIRST 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。

4-1-1-2. 大洋州地域(オセアニア)の CSIRT 構築支援活動(2011 年 7 月 18 日-7 月 29 日)

大洋州の島嶼国をカバーする CSIRT である PacCERT の構築支援活動として、JPCERT/CC の職員が独立行政法人国際協力機構（JICA）の短期専門家としてフィジーに赴き、情報セキュリティや CSIRT の役割に関する South Pacific ICT EXPO 2011(SPICTEX 2011)での講演、現地関係者との協議を通じた課題抽出、今後の支援計画立案等の業務を行いました。

4-1-1-3. ミャンマーの CSIRT 構築支援活動(2011 年 9 月 26 日-9 月 30 日)

財団法人海外貿易開発協会（JODC）が経済産業省から受託した「貿易投資円滑化支援事業」において、ミャンマーにおける CSIRT 構築・支援を目的として現地に派遣する専門家の公募が行われ、9 月にネットワークフォレンジック（座学・ハンズオン）の 2 名、12 月にマルウエア解析（動的解析・静的解析）の 2 名が JPCERT/CC より派遣されることが決定しました。
9 月のネットワークフォレンジック研修（座学とハンズオン）は、同月 26 日から 30 日の計 5 日間、ヤンゴンで実施され、ミャンマーの National CSIRT である mmCERT のスタッフと ISP などの技術者およそ 20 名に対して、Wireshark を利用した不正な通信の分析手法などを教授しました。

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メールでの問合せ及び次の四半期に向けた計画立案が中心でした。

4-1-2-1. アフリカでの CSIRT 構築支援活動について AP* Retreat で講演(2011 年 9 月 2 日)

アジア太平洋地域のインターネット関連組織で構成される団体 AP*(http://www.apstar.org/)が韓国の釜山で開いた定期会合 AP* Retreat に参加し、JPCERT/CC がアフリカでおこなっている CSIRT 構築支援活動について講演を行いました。

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、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・大洋州地域(オセアニア)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

8 月 10 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. 他組織との連携

1) APEC 地域の情報電気通信分野を担当する政府機関を中核とするワーキンググループである APEC Telecommunications and Information Working Group (APEC TEL) の Security and Prosperity Steering Group (SPSG）の会合(9 月 27 日にクアラルンプールで開催)に対して、APCERT の議長チームとして、APCERT の活動概要を紹介するビデオメッセージ送りました。

2) イスラム諸国会議機構(OIC)の創設した OIC-CERT と APCERT 間で、9 月 27 日、今後の連携強化を目的とした MoU を締結しました。同日、ドバイで開催された調印式には APCERT の議長チームとして出席しました。

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(2011 年 9 月 27 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 6 度目になります。
今年は 10 カ国（日本、ブルネイ、中国、インド、インドネシア、マレーシア、ミャンマー、シンガポール、タイ、ベトナム）から 13 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. 中国語圏における情報収集発信

JPCERT/CC 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。

7 月 21 日に台北で開催された、「第 2 回 Botnet 偵測與防治技術研討會」に参加し台湾地域におけるボットネット対策情報収集を行いました。収集した情報は日本国内の関係者会合などへ展開しました。

7 月 22-23 日に台北で開催された、「台灣駭客年會 HIT2011」に参加し、台湾地域におけるハッカーコミュニティの活動状況について情報収集を行いました。収集した情報は日本国内の関係者会合などへ展開しました。

8 月 8-10 日に大連で開催された、「2011 中国计算机网络安全应急年会」に参加し、「サイバークリーンセンター５年実施成果」と題した講演を実施し、日本のセキュリティ対策取り組みを中国セキュリティ業界関係者向けに説明しました。

9 月 1-2 日に北京で開催された、「XCon2011 中国安全焦点信息安全技術峰会」に参加し、中国地域におけるセキュリティ研究者コミュニティの活動状況について情報収集を行いました。収集した情報は日本国内の関係者会合などへ展開しました。

9 月 22 日に上海にて開催された、「COG 信息安全论坛」に参加し、中国地域における紅客連盟などのハッカー集団の活動状況について情報収集を行いました。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。

4-2-2. 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

FIRST の Steering Committee のメンバである JPCERT/CC の理事 山口英が 9 月 7 日から 9 日に米国アトランタで開催された Steering Committee 会合に参加しました。

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

4-2-2-1-2. FIRST スポンサー（他の CSIRT の加盟手続き支援）

本四半期は、国内外の CSIRT 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）を務めるべく、サイトビジットや書類作成等を行いました。
2011 年 8 月、JPCERT/CC がスポンサーとなった三井物産セキュアディレクション株式会社の CSIRT である Mitsui Bussan Secure Directions, Inc. Security Incident Response Team (MBSD-SIRT) の FIRST 加盟が決定しました。9 月には同じく JPCERT/CC がスポンサーとなったスリランカの TechCERT の加盟が決定しました。2011 年 9 月末現在、日本からの FIRST 加盟チームは、20 チームとなっています。

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、アフリカにおける CSIRT 構築支援、太洋州をカバーする CSIRT 構築支援に関してブログにエントリーを掲載しました。

CSIRT establishment in Africa
http://blog.jpcert.or.jp/2011/06/secure-coding-seminar-in-cc-successfully-completed.html

A CSIRT Covering the Pacific Island Nations
http://blog.jpcert.or.jp/2011/09/supporting-paccert-as-the-jica-expert.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 8 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 OCN や Paypal を騙るフィッシングの報告を複数受けました。協議会では、メールや Web サイトのフィッシング判定を行い、名前を騙られた事業者に情報提供するとともに、8 月 24 日と 9 月 8 日に緊急情報として Web 公開しました。
当該フィッシングサイトについては調整を行い、サイトからフィッシングページが消えた事を確認しています。

[図 5-1　OCN を騙るフィッシングサイト
https://www.antiphishing.jp/news/alert/ocn2011824.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、会員のうち、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って登録した者やフィッシング研究を行っている学術機関に対し、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が目的です。本四半期からは新たに、情報セキュリティ大学院大学 (2011 年 7 月より)、ネットムーブ株式会社 (2011 年 8 月より)の 2 組織（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 15 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. 講演活動

本四半期に協議会として次の講演を行いました。

(1) 山本 健太郎「最新のフィッシング事例と対策に関して」
神奈川県クレジット犯罪対策協議会,勉強会 2011 年 7 月 25 日

(2) 山本 健太郎「最新のフィッシング事例と対策に関して」
日本インターネットポイント協議会,勉強会 2011 年 8 月 25 日

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 2011 年 7 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201107.html
フィッシング対策協議会 2011 年 8 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201108.html
フィッシング対策協議会 2011 年 9 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201109.html

6. 公開資料

JPCERT/CC が今期に公開した調査・研究の報告書や論文、セミナー資料は次のとおりです。

6-1.セキュア開発支援資料「Java セキュアコーディング　並行処理編」

本資料についての詳細は、「2-5-1.」をご参照ください。

Java セキュアコーディング 並行処理編　(2011 年 8 月 19 日)
https://www.jpcert.or.jp/research/2011/JavaConcurrencyGuidelines_20110819.pdf

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) :
「Android アプリ開発にもきっと役立つセキュアコーディング」
Android Bazzar and Conference 2011 Summer, 2011 年 7 月 17 日

(2) 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ノススメ (Java 編)」
オープンソースカンファレンス 2011 名古屋,2011 年 8 月 20 日

(3) 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) :
「最新のフィッシング事例と対策に関して」
神奈川県クレジット犯罪対策協議会,2011 年 7 月 25 日

(4) 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) :
「JPCERT/CC の定点観測について」
ISOG-J WG2,2011 年 7 月 28 日

(5) Jack YS Lin(早期警戒グループ 情報セキュリティアナリスト) :
「日本僵尸网络治理项目-五年实施总结报告(日本ボットネット対策事業五年成果報告)」
新视点・新安全-2011 年中国计算机网络安全年会－北京,2011 年 8 月 10 日

(6) 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) :
「最新のフィッシング事例と対策に関して」
日本インターネットポイント協議会ワーキンググループ,2011 年 8 月 25 日

(7) 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) :
「ID・パスワードの管理に関して」
日本インターネットポイント協議会ワーキンググループ,2011 年 8 月 25 日

(8) 宮地 利雄(理事) :
「Myth and Reality on Control System Security Revealed by Stuxnet」
計測制御学会大会 (SICE Annual Conference) 2011,2011 年 9 月 15 日

(9) 真鍋 敬士(理事,分析センター長)：
「事例に見るセキュリティ対策のポイント」
日本マイクロソフト(株)セキュリティセミナー,2011 年 9 月 27 日

8. 開催セミナー等一覧

(1) 情報処理の高度化等対処のための刑法等の一部を改正する法律（サイバー刑法、刑事訴訟法）説明会

本年 6 月 17 日に、「情報処理の高度化等に対処するための刑法等の一部を改正する法律が成立し、いわゆるウイルス作成罪等については、7 月 14 日から施行されたことを受け、（ログの保全要請等に関する刑事訴訟法の改正については、成立から 1 年内の政令で定める日（未定）からの施行。）関係者への周知をはかるため、情報処理学会など 3 組織と共催で説明会を開催しました。

・主　催 ：一般社団法人 情報処理学会 セキュリティ委員会、社団法人 日本インターネットプロバイダ協会(JAIPA)、特定非営利活動法人 日本ネットワークセキュリティ協会(JNSA)、JPCERT/CC
・開催日時：2011 年 7 月 26 日(火) 10:00-12:00
・参加者 ：ISP、ホスティングサービスなどの運用担当者、マルウエア検体を取り扱うセキリティベンダや研究者、ソフトウエア製品の開発・提供者、企業の法務担当者など 290 名

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

(2) 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、「2-4-3」をご参照ください。

■ 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