JPCERT/CC®

JPCERT-PR-2012-01

発行日 : 2012-07-12

JPCERT/CC 活動概要 [2012 年 4 月 1 日 ～ 2012 年 6 月 30 日]

【活動概要トピックス】

—トピック 1—
「DNS Changer マルウエア感染確認サイト」を開設

JPCERT/CC は、5 月 22 日に DNS Changer に感染した PC を簡単にチェックできる検査サイトを開設しました。

DNS Changer の問題については、前四半期より感染 PC の確認方法や感染が確認された場合の対処方法などの情報提供や注意喚起を行ってきましたが、日本にもまだ相当数の感染 PC が存在していることが、この問題に取り組む DCWG（DNS Changer Working Group）により確認されています。その多くは利用者が感染に気付いていない PC であると思われ、この状態を放置しておくと、暫定ネームサーバが停止される 7 月 9 日以降、多数の感染 PC がインターネットへアクセスができなくなり、混乱を生じる可能性があります。こうした事態を回避するため、JPCERT/CC では、アクセスするだけで DNS Changer 感染の有無をチェックできるサイトを開設し、広く検査を呼び掛けています。さらに、国内大手ポータルサイトである Yahoo! Japan にも周知と当該サイトへの誘導をお願いするなど、暫定ネームサーバ停止後のインターネット接続の混乱の軽減に努めています。

DNS Changer マルウエア感染確認サイト
http://www.dns-ok.jpcert.or.jp/
DNS 設定を書き換えるマルウエア (DNS Changer) 感染に関する注意喚起
https://www.jpcert.or.jp/at/2012/at120008.html
DNS Changer マルウエア感染確認サイト公開のお知らせ
https://www.jpcert.or.jp/pr/2012/pr120002.html
今一度、DNS Changer マルウエア感染の確認を
https://www.jpcert.or.jp/present/#year2012

—トピック 2—
Java セキュアコーディングセミナーを海外初展開

JPCERT/CC は、タイのバンコクおよびインドネシアのバンドンにて、Java/Android に関するセキュアコーディングセミナーを開催しました。

タイのバンコクでのセミナーは、ThaiCERT とマヒドン大学の協力のもと、4 月 26 日、27 日の 2 日間の日程で開催されました。JPCERT/CC が実施する Java および Android に関するセキュアコーディングセミナーとしては、初の海外開催でした。現地では、スマートフォン等のアプリケーション開発が増えていることから Android プログラミングに対する注目度が高く、定員を超える応募があり、およそ 60 名の方に受講いただきしました。

インドネシアのバンドンのセミナーは、現地の大学生に向けて企画されたもので、インドネシア国内 40 の大学が参加する Academic CSIRT および Maranatha Christian University の協力を得て、5 月 31 日から 6 月 2 日までの 3 日間の日程で開催されました。インドネシアでは Java を学ぶ学生の比率が非常に高く、こちらも定員を超える応募があり、100 名以上の受講者が集まりました。

Java のセキュアコーディングに関するセミナーは、両国にとって過去にあまり例がないもので、主催者、受講者からも高い評価を得ることができました。JPCERT/CC では、C/C++に続いて、Java/Android についてもセキュアコーディングスタンダードを国内外へ広めていくことで、アジア地域全体のセキュリティ向上につなげたいと考えています。

—トピック 3—
FIRST 年次総会に参加

国際的な CSIRT 組織で構成される FIRST (Forum of Incident Response and Security Teams) の年次総会とカンファレンスが開催されました（開催地マルタ：6 月 17 日～22 日）。FIRST カンファレンスでの講演内容は例年各国の情報セキュリティ上の課題を反映したものとなります。本年のカンファレンスは、‘Security is not an island’ をテーマに、主にセキュリティとインシデント対応に関する実務的な側面に焦点をあてて行われ、“APT”に対する各組織での対策や攻撃に使用されたマルウエアや手法を紹介するセッションや、情報共有連携に関するセッションがそれぞれ複数あり、注目を集めていたことが特徴的でした。

JPCERT/CC は CSIRT 連携のあり方を考えるパネルディスカッションに参加し、また災害時の BCP とセキュリティの問題に関する事例報告を行いました。

"Global and Regional CERT Collaboration to Reduce Cyber Conflict Risk Pane"と題したパネルでは国際部部長 伊藤友里恵がモデレータを担当しました。サイバー攻撃などの脅威が増大する中で、

CSIRT が緊密な連携により未然に衝突を回避する役割を果たすことの重要性が話し合われました。"What we found about BCP on 3/11"と題した事例報告では早期警戒グループの満永拓邦が登壇し、2011 年の東日本大震災の経験についてヒアリングした結果から企業活動の継続性を高めるため対策の有効性について発表しました。

JPCERT/CC は、山口英国際担当理事が継続的に FIRST の運営委員としてその活動に深く関わっており、年次総会や技術部会の会合などでも積極的に研究成果の発表や情報共有を行うなど、その活動を支援しています。このような活動は、インシデント対応時における各国 CSIRT との国際連携のための下地作りとなっています。

24th Annual FIRST Conference
http://conference.first.org/index.aspx

―トピック 4―
JPCERT/CC ホームページをモバイル端末向けに拡張

JPCERT/CC は、4 月 3 日にモバイル端末向けのホームページを公開しました。

旧来の PC のメールや Web ブラウザに加えて、モバイルデバイスやソーシャルメディアの普及に伴い、これらの新メディアを通じた情報入手の機会が増えています。JPCERT/CC でも、モバイル端末向けホームページを開設し、新しいデバイスや情報メディアを通じても、提供情報をご利用いただけるようにいたしました。

モバイル端末向けホームページでは、注意喚起や脆弱性対策情報（JVN）といった即時性の高いコンテンツや、セキュアコーディングスタンダードを始めとする各種公開資料などを中心に情報を編集しています。スマートフォンやタブレットは、タッチスクリーンによる操作など PC とは異なるユーザインタフェースを持つため、これらに適した情報のレイアウトを工夫しています。また、SNS などの新しいメディアの情報発信機能を活用するために、公開情報を Twitter やメールに投稿・転送しやすくするソーシャルメディアとの連携、およびコンテンツ共有の利便性を向上させる機能も強化いたしました。

JPCERT/CC モバイル端末向けホームページ
https://www.jpcert.or.jp/m

本活動は、経済産業省より委託を受け、「平成２４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。
「7.フィッシング対策協議会事務局の運営」については「平成２４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もので、一部協議会の会費収入によって実施した事業が含まれています。
また、「2-5.セキュアコーディング啓発活動」、「6.国際連携活動関連」、「9.講演活動一覧」、「10.執筆一覧」及び「11.開催セミナー等一覧」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®

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 4072 件、インシデント件数ベースでは 3832 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 756 件でした。前四半期の 754 件と比較して 0.3%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、状況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/2012/IR_Report20120712.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 367 件で、前四半期の 324 件から 13%増加しました。また、前年度同期（325 件）との比較では、13%の増加となりました。
本四半期のフィッシングサイトが装っていたブランドの国内・国外別の内訳を[表 1-1]に示します。

[表 1-1 フィッシングサイトの国内・国外ブランド別の件数]

フィッシングサイト	4 月	5 月	6 月	国内外別合計（割合）
国内ブランド	29	19	20	68(19%)
国外ブランド	83	87	55	225(61%)
ブランド不明（注 2）	31	24	19	74(20%)
月別合計	143	130	94	367(100%)

(注 2)「ブランド不明」は、報告されたフィッシングサイトが停止していたなどの理由により、JPCERT/CC がブランドを確認することができなかったサイトの件数を示します。

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 68 件と、前四半期の 58 件から 17%増加しました。国外ブランドを装ったフィッシングサイトの件数は 225 件と、前四半期の 221 件から 2%増加しました。

本四半期の国内金融機関を装ったフィッシングサイトは、前四半期と同様にダイナミック DNS サービスのドメインを使用したものが大半であり、それ以外に短縮 URL や CDN などのサービスを使用した事例の報告も受けています。フィッシングサイトの標的となるブランドは、大手の銀行に限らず、様々なブランドのインターネットバンキングを装ったサイトを確認しています。

フィッシングサイトの調整先の割合は、国内が 50%、国外が 50%と、前四半期の割合（国内 65%、国外 35%）と比較して、国外への調整が増えました。

本四半期に報告が寄せられた Web サイト改ざんの件数は、139 件でした。前四半期の 142 件から 2%減少しています。

本四半期には、マルウエア配布サイトへの誘導ページが設置された Web サイトの報告を多数受領しました。国内で確認したこれらの誘導サイトの多くは、ルートディレクトリ下にランダムな英数字 6～8 文字の名前を持つディレクトリが作成され、そのディレクトリ下にマルウエア配布サイトへ誘導する JavaScript を含んだ html ファイルが設置されていました。
誘導先のマルウエア配布サイトは、2012 年 2 月に公開された Java の脆弱性(CVE-2012-0507)など、複数の脆弱性を使用して誘導した PC をマルウエアに感染させます。古い Java を使用している場合には危険性があります。

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が影響を受ける可能性のある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、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：12 件　https://www.jpcert.or.jp/at/

2012-04-11　2012 年 4 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起
2012-04-11　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起
2012-05-07　Adobe Flash Player の脆弱性 (APSB12-09) に関する注意喚起
2012-05-09　2012 年 5 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起
2012-05-09　PHP の脆弱性に関する注意喚起
2012-05-10　PHP の脆弱性に関する注意喚起
2012-05-16　ロジテック社製ブロードバンドルータの脆弱性に関する注意喚起

2012-05-25　ロジテック社製ブロードバンドルータの脆弱性に関する注意喚起
2012-06-05　ISC BIND 9 サービス運用妨害の脆弱性に関する注意喚起
2012-06-11　Adobe Flash Player の脆弱性 (APSB12-14) に関する注意喚起
2012-06-13　2012 年 6 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起
2012-06-29　2012 年 6 月 Java SE の脆弱性を狙う攻撃に関する注意喚起

1.2.1.2. Weekly Report

JPCERT/CC が収集したセキュリティ関連情報のうち重要と判断した情報の抜粋をレポートにまとめ、原則として毎週水曜日（週の第 3 営業日）に発行しています。レポートには、「ひとくちメモ」として、情報セキュリティに関する豆知識情報も掲載しています。

発行件数：12 件　https://www.jpcert.or.jp/wr/

Weekly Report で扱った情報セキュリティ関連情報の項目数は、合計 68 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。

2012-04-04　Java (JRE/JDK) のバージョンに注意
2012-04-11　nicterWeb が公開されました
2012-04-18　Firefox 3.6 と Thunderbird 3.1 のサポート終了
2012-04-25　スマートフォンのアプリに注意
2012-05-09　Java SE 7u4/6u32 のリリースと EOL
2012-05-16　Java 7 への対応
2012-05-23　DNS Changer マルウエア感染確認サイト公開のお知らせ
2012-05-30　PHP の更新を確認しましょう
2012-06-06　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 12 版
2012-06-13　今一度、DNS Changer マルウエアの確認を
2012-06-20　Android アプリ開発者向け情報
2012-06-27　Adobe Reader 9 および Acrobat 9 のサポート期間について

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「早期警戒情報」を、JPCERT/CC が推奨する対策を添えて提供しています。

早期警戒情報の提供について
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) Windows コモン コントロールの脆弱性（MS12-027）を狙う攻撃に関する情報収集・提供

2012 年 4 月 11 日に公開された Windows コモン コントロールの脆弱性（MS12-027）を使用したマルウエア添付型メールが、早くも公開の翌週に国内に出現しました。この攻撃に使用された電子メールにはドキュメントファイルが添付されており、このファイルを開くと、ファイル内に組み込まれた攻撃コードによって PC が RAT(Remote Access Trojan)に感染します。攻撃に使用された RAT は、感染した PC の内部データを窃取して外部へ送信する機能を有しており、企業や組織の機密情報が窃取されることが懸念されたため、重要インフラ等事業者における被害発生防止を目的に、早期警戒情報を発行し、セキュリティ更新プログラムの適用やマルウエアによる通信形跡の有無の確認、同通信の遮断などの対策を促しました。

(2) 攻撃者グループの攻撃活動への対応

昨年来、政府や企業等の活動や経営方針等に対して自らの意見を主張する手段としてサイバー攻撃を行う、いわゆるハクティビストの活動が活発化しています。2012 年 4 月には、国内の企業を含む民間企業 50 数社の Web サイトに対して 5 月下旬にサイバー攻撃（DDoS 攻撃や企業から窃取した情報の開示）を行う旨の予告が行われ、実際に一部 Web サイトに対して小規模な DDoS 攻撃が行われました。

予告の中で攻撃対象とされた国内企業に対して、JPCERT/CC では 5 月中旬に、事前の情報提供を行うとともに、攻撃が発生した場合に備えてインシデント対応のための事前調整などを行いました。また、攻撃予定日までの期間に攻撃関連情報（正確な攻撃日時、攻撃手法やツール、攻撃への参加状況など）の収集・分析を行った結果、攻撃予定日に小規模ながら攻撃が行われる可能性が高まったため、攻撃対象の国内企業へ分析結果を追加提供しました。

攻撃予定日には、攻撃者グループのチャット上で攻撃指示が行われ、海外の 1 企業に対して小規模な DDoS 攻撃が行われたものの、懸念された企業の機密情報の開示や国内の民間サイトに対しての DDoS 攻撃は見受けられませんでした。

1.3. インターネット定点観測システム

インターネット定点観測システムでは、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。ポートスキャンの動向を観測する目的は、ネットワーク経由の攻撃の準備活動としてポートスキャンがなされることを踏まえて、既に公開され

ている脆弱性情報や攻撃ツール、攻撃コードを悪用した攻撃活動の動向と、新たに公開された脆弱性情報等による攻撃活動の立上り状況を把握することです。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。

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. 定点観測システム観測データを元にしたインシデント対応事例

定点観測システムの観測データを分析して判明した、PC のマルウエア感染や、侵入されて攻撃用ツールが設置されたことによって行われた Scan などについてのインシデント対応事例について紹介します。

1） これまで、組込 Linux を使用したネットワーク機器にインターネットから不正に侵入し、Telnet の通信ポート(23/tcp)に対して Scan を行うツールを設置するインシデントが、日本を除くアジア地域で多数確認されていましたが、本四半期は同様のインシデントが国内でも確認されました。JPCERT/CC では、Scan 元 IP アドレスの管理者に、海外のインシデント事例を提供するとともに対応を依頼した結果、同 IP アドレスからの Scan は観測されなくなりました。

2） 2011 年 8 月に感染活動が活発化した Morto.Worm などが行うリモートデスクトップ接続の待ち受けポートに使用される 3389/tcp ポートに対するスキャンが継続しています。今期観測された事例のうち Scan 元が国内にあった事例について、IP アドレスの管理者にインシデント通知を行ったところ、既存のアンチウイルスソフトでは検知できない未知のマルウエアに感染していたことが確認されました。今回、通常のセキュリティ製品では検知できないマルウエア（亜種）に感染した PC を特定することで、該当 PC のマルウエアの駆除およびその後の感染活動の拡大の抑止につなげることができました。

1.3.2. ポートスキャン概況

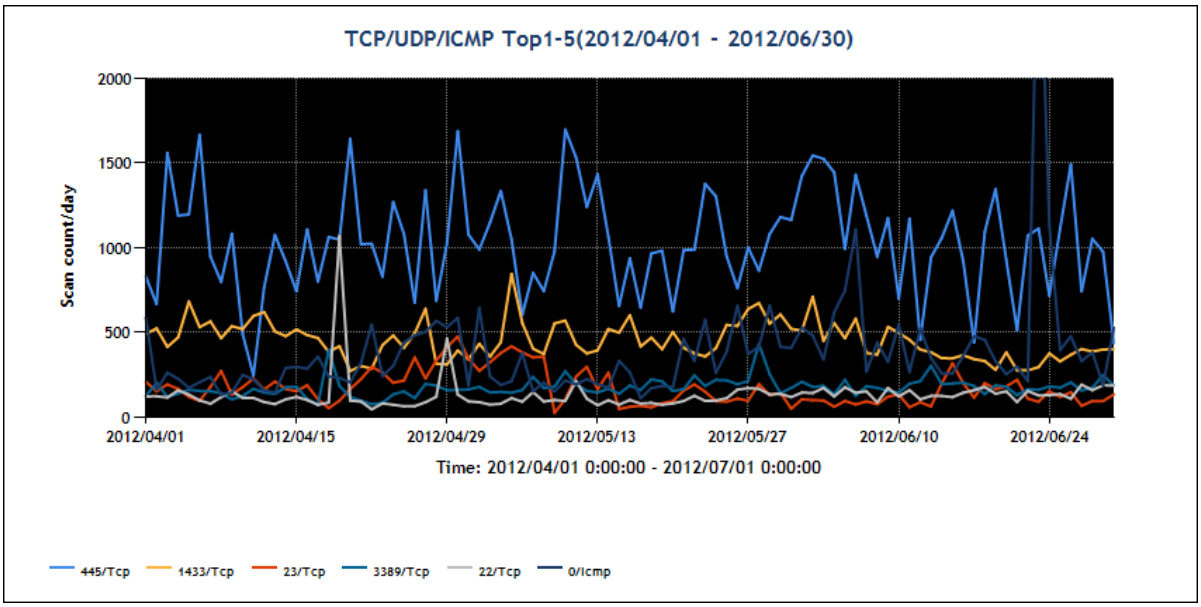
インターネット定点観測システムで観測されたポートスキャンの頻度や内訳の推移をグラフとして JPCERT/CC の Web ページで公開しています。宛先ポート別グラフは、各センサーに記録された宛先ポートごとに観測されたパケット数を表しています。

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

本四半期に定点観測システムで観測された宛先ポート別の上位 1 位～5 位及び 6 位～10 位のそ

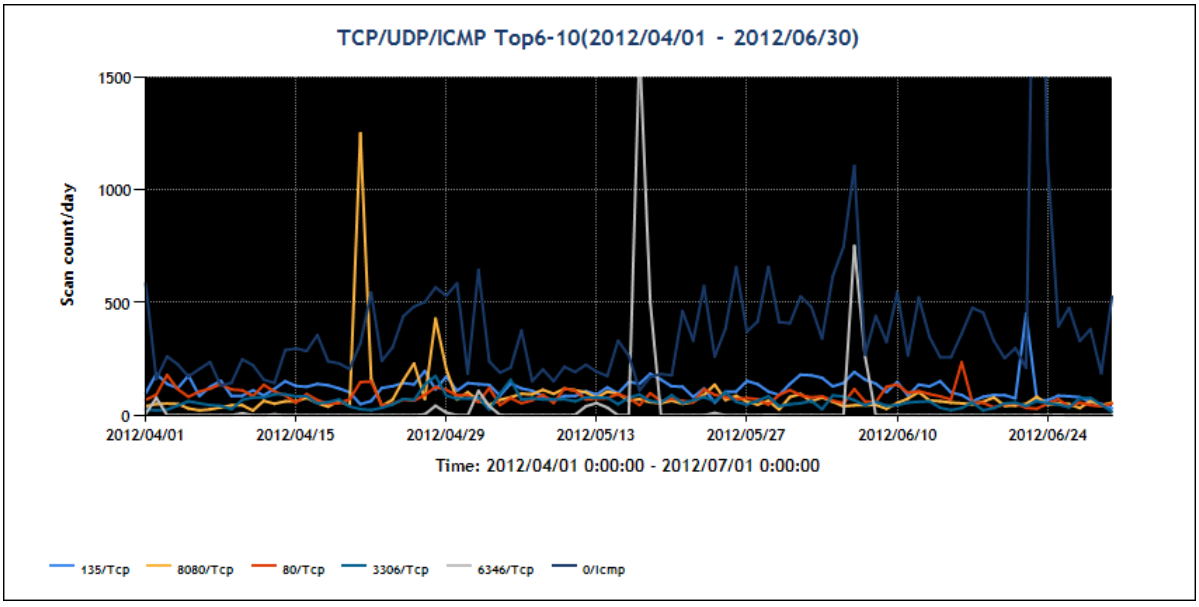
れぞれについて、パケット数の時間的推移を[図 1-1]と[図 1-2]に示します。

- 宛先ポート別グラフ top1-5 (2012 年 4 月 1 日-6 月 30 日)



[図 1-1 宛先ポート別グラフ top[1-5]

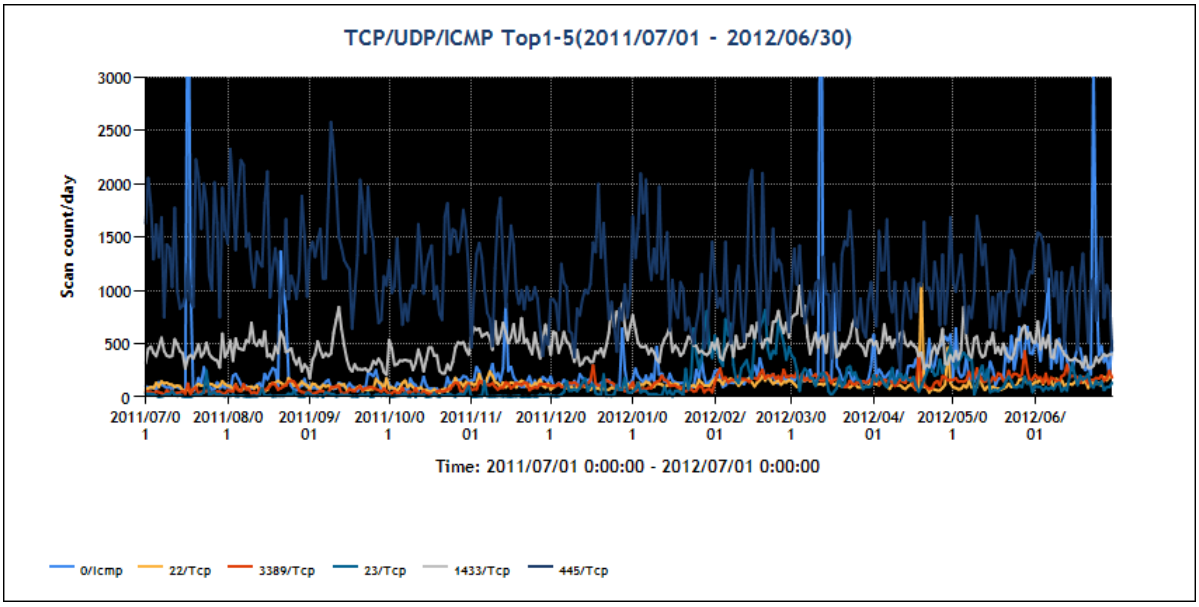
- 宛先ポート別グラフ top6-10 (2012 年 4 月 1 日-6 月 30 日)



[図 1-2 宛先ポート別グラフ top[6-10]

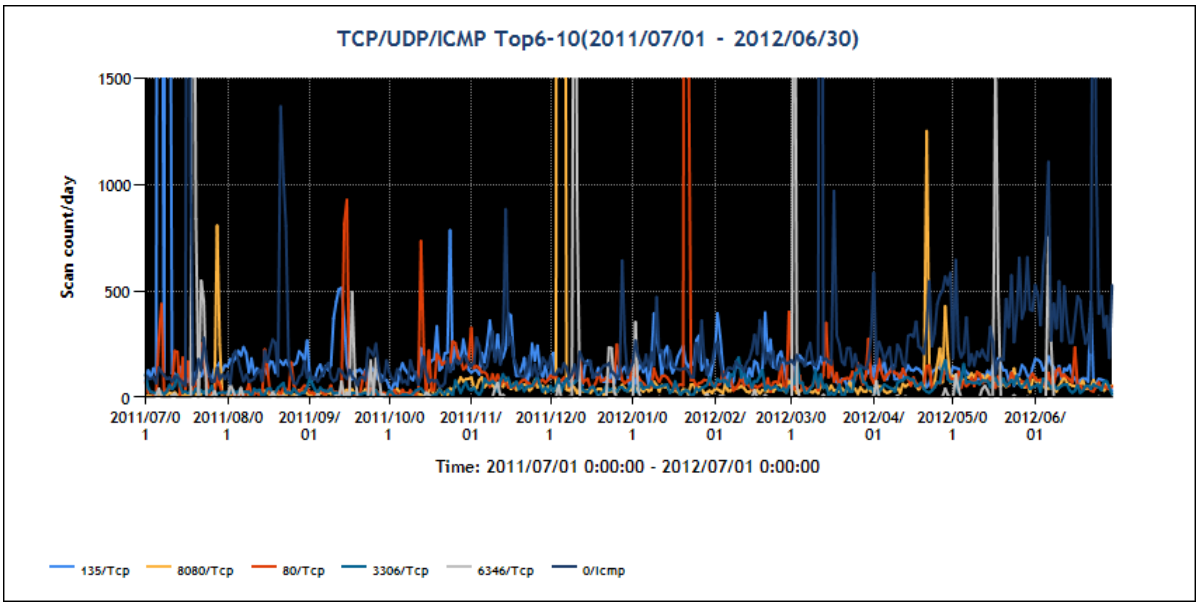
また、より長期間のパケット数の推移を見るため、2011 年 7 月 1 日から 2012 年 6 月 30 日までの期間における、宛先ポート別の上位 1 位～5 位及び 6 位～10 位のそれぞれについて、パケット数の時間的推移を[図 1-3]と[図 1-4]に示します。

- 宛先ポート別グラフ top1-5 (2011 年 7 月 1 日-2012 年 6 月 30 日)



[図 1-3 宛先ポート別グラフ top[1-5]

- 宛先ポート別グラフ top6-10 (2011 年 7 月 1 日-2012 年 6 月 30 日)



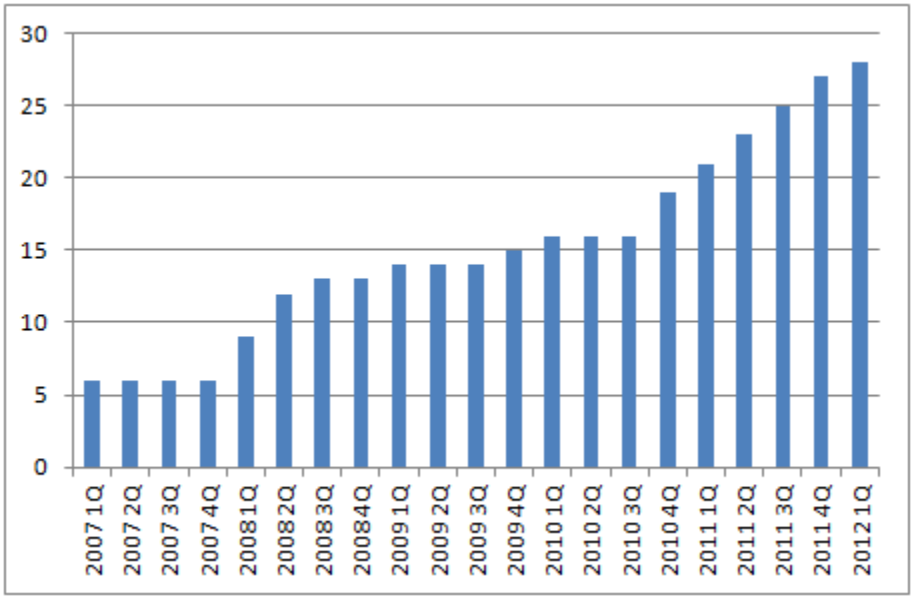
[図 1-4 宛先ポート別グラフ top[6-10]

順位には変動がありますが、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多く観測されています。

1.4. 日本シーサート協議会 (NCA) 事務局運営

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、JPCERT/CC は、協議会の問合せ窓口、会員情報の管理、加盟のためのガイダンスの実施および手続の運用、Web 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、高エネルギー加速器研究機構(KEK CSIRT)と株式会社フォーカスシステムズ(FSIRT)が、新規に加盟しました。本期末時点で 28 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]

4 月には、海外向けに日本シーサート協議会の活動を紹介する英語サイトを公開しました。英語サイトには、協議会の概要説明の他、WG 活動や協議会メンバ紹介なども掲載しており、主に海外 CSIRT コミュニティに対して協議会のプレゼンス向上を図る予定です。

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

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。

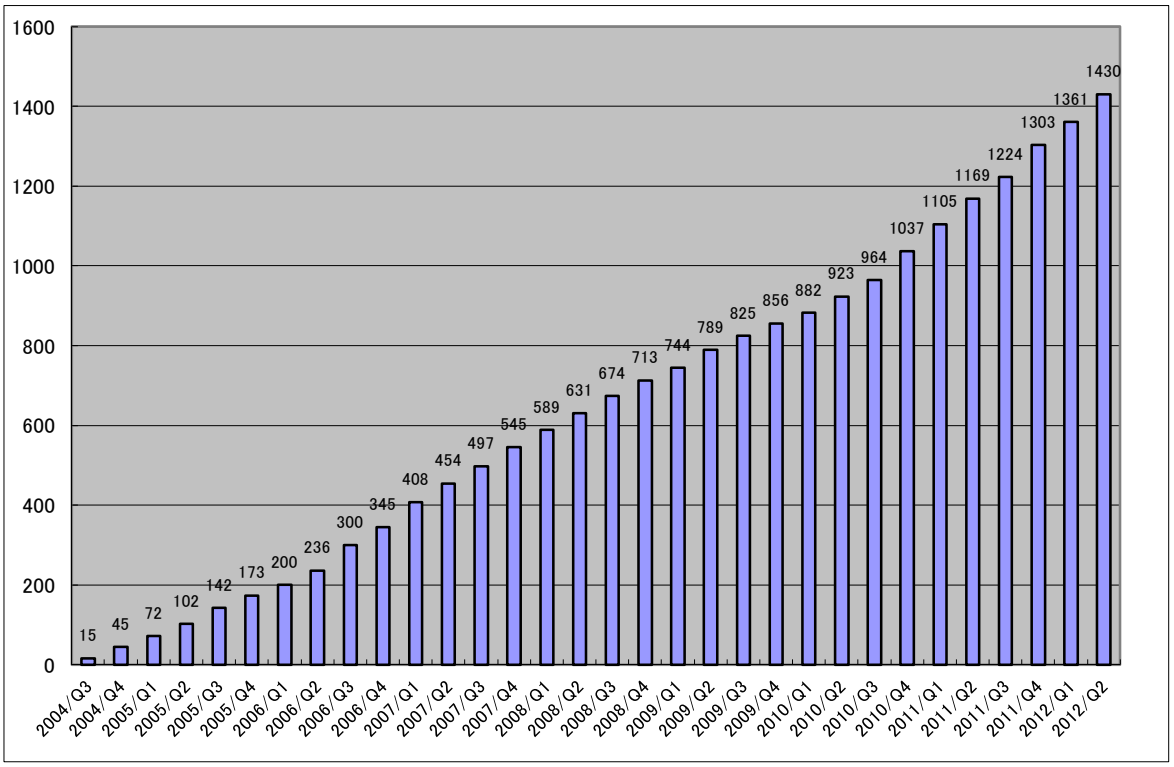
日本シーサート協議会 Web ページ
http://www.nca.gr.jp/

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

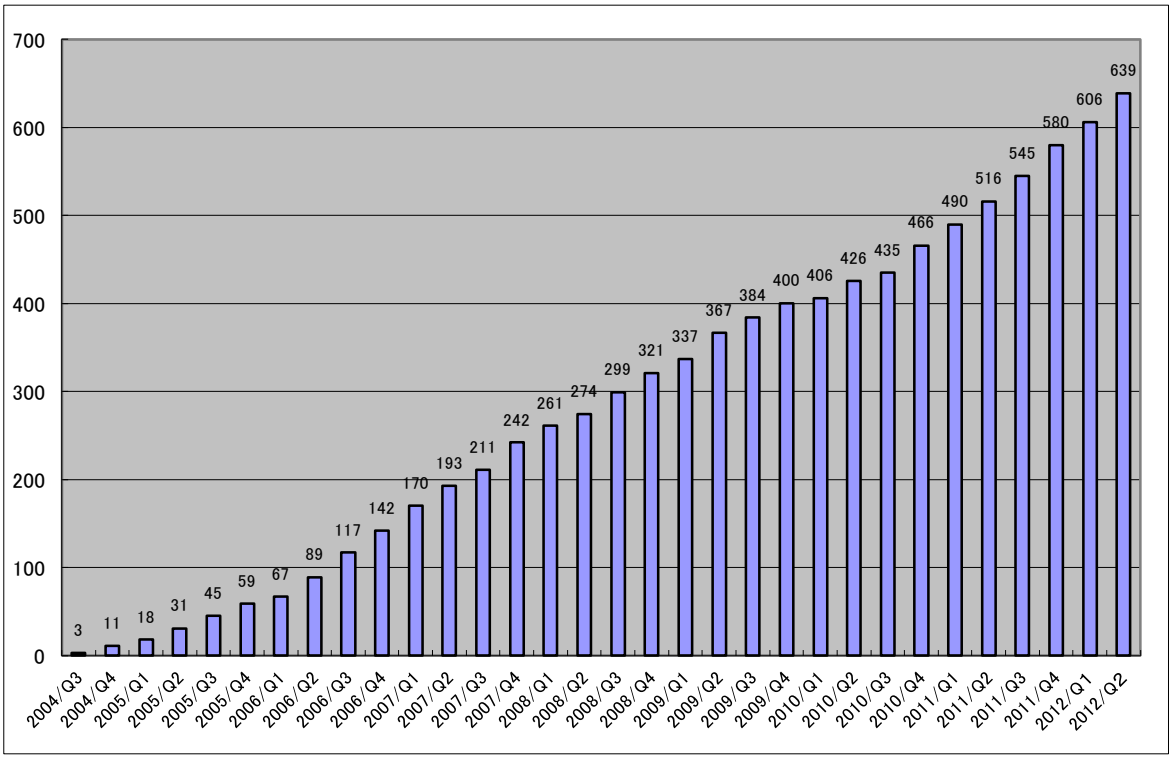
JPCERT/CC は、経済産業省告示「ソフトウエア等脆弱性情報取扱基準」（以下「本基準」といいます。）において、製品開発者とのコーディネーションを行う「調整機関」に指定されており、本基準を踏まえてとりまとめられた「情報セキュリティ早期警戒パートナーシップガイドライン」に詳述された調整機関の役割を担う活動を行っています。
本四半期に JVN において公開した脆弱性情報は、69 件(累計 1430 件) [図 2-1] でした。本四半期に公開された個々の脆弱性情報に関しては、JVN(https://jvn.jp/)をご覧ください。



[図 2-1　JVN 公開累積件数]

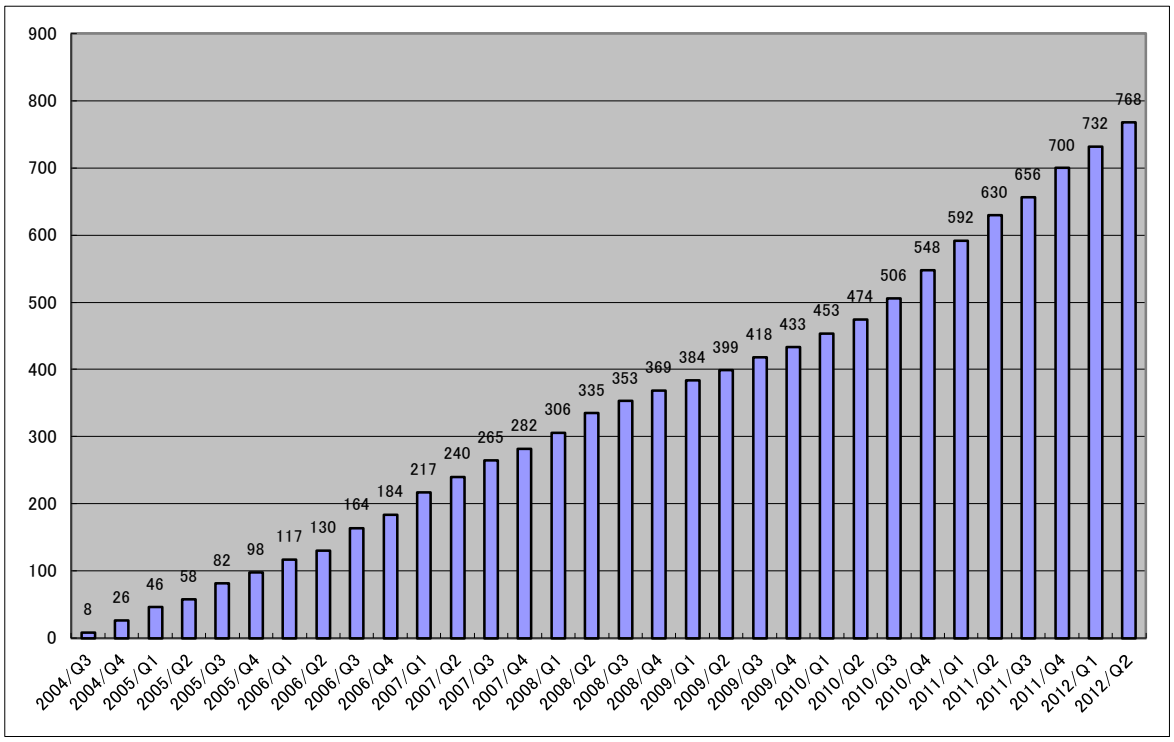
このうち、本基準に従って調整を行い、JVN で JVN#として公開した脆弱性情報は、33 件(累計 639 件) [図 2-2] でした。そのうちの半数を超える 12 件（約 36%）が海外製品開発者の製品で

す。こうした統計値にも現れているように、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してもらえるようになってきています。Android およびその関連製品の届出の増加という前四半期からの傾向が続き、本四半期には、携帯端末の脆弱性および Android アプリケーションの脆弱性を 5 件公開しました。また、Twitter をはじめとする SNS（ソーシャルネットワーキングサービス）の普及に伴い、SNS 関連製品における脆弱性届出も増加傾向にあります。本四半期には、SNS 関連ソフトウエアに関する脆弱性情報を 4 件公開しました。



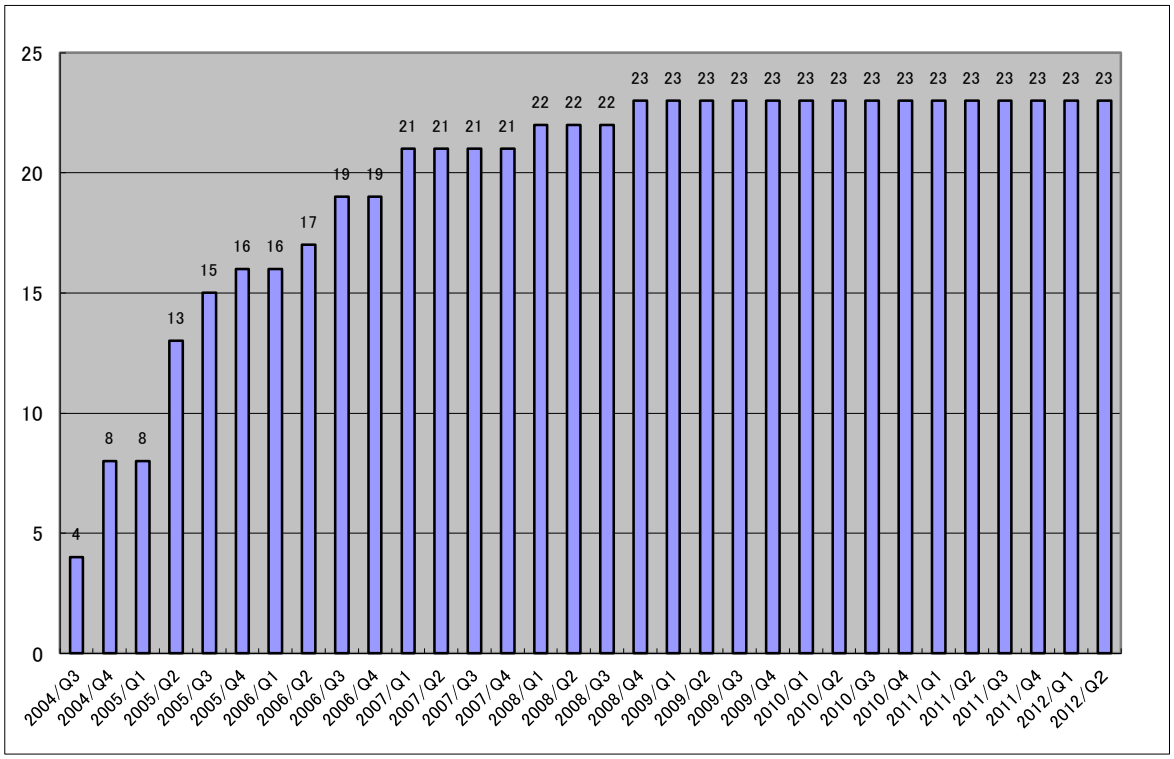
[図 2-2　JVN_JP(JVN#)公開累積件数]

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 JVNVU#および JVNTA として公開した脆弱性情報は、36 件(累計 768 件) [図 2-3]でした。これらの中には、Apple 製品に関するものが 7 件、Adobe 製品に関するものが 1 件、HP(Hewlett Packard)製品に関するものが 1 件、Oracle 製品に関するものが 1 件、Symantec 製品に関するものが 1 件、Microsoft 製品に関するものが 5 件ありました。本四半期にこのカテゴリで公開された脆弱性情報には、大手製品開発者の製品に混じって、本四半期に初めて JVN にて公表された製品開発者の製品も数多くありました。また OSS 製品（ライブラリ、サーバ製品、OS 等）における脆弱性情報が 4 件と約 12%を占めました。



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

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 2-4　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止まってしまっている、いわゆる「長期滞留案件」の件数も 2004 年の本活動開始から約 8 年の間に徐々に増えてきています。昨年度から、こうした状況の改善を期して、脆弱性情報の取扱手順を定めたガイドラインの改定についての検討を専門家の方々から構成された委員会で行ってきました。

その第一段階として、2010 度に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では、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に関する情報を広く一般に求める手順が追加されました。これを受けて 2011 年 9 月 29 日から、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掲載を開始しました。初回公開時には、50 件の連絡不能開発者案件を掲載しましたが、その翌日には早速、3 件の案件を抱える 1 製品開発者から連絡がありました。また、2011 年 10 月には、2 件の案件を抱える製品開発者及び 3 件の案件を抱える製品開発者との連絡が取れるようになりました。さらに、12 月には、2 件の案件を抱える 1 製品開発者との連絡がついて、それぞれ調整手続きを始めることができました。連絡不能開発者一覧の掲載によって、1 週間以内に約 1 割、3 ヶ月以内に約 2 割の開発者と連絡がついて調整を開始できたこととなり、連絡不能開発者一覧の掲載が「滞留案件」の解消に一定の効果があることが確認されました。

本四半期においては、6 月 22 日に、連絡不能開発者一覧として製品開発者 2 件を追加公表しました。また同日、「連絡不能開発者一覧」に前回の公開（3 月 16 日）後も連絡がとれないままの 8 件について、掲載済みの製品開発者名に加えて、脆弱性が報告された製品名およびバージョンを追記して、連絡不能開発者一覧を更新しました。6 月末日時点では、合計 98 件の連絡不能開発者が公表されています。

さらに、第二段階として、こうした対応によってもなお調整ができない場合に関し、脆弱性の存在が検証できた製品について、その内容を JVN で公開するための手順や手続き等を、IPA および関係機関とともに検討しました。第二段階目の活動は、本年度内の開始を視野に、さらなる検討および体制整備等準備を進めています。

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、4 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、29 件の脆弱性情報について JPCERT/CC が CVE を採番し、JVN 上に掲載しました。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

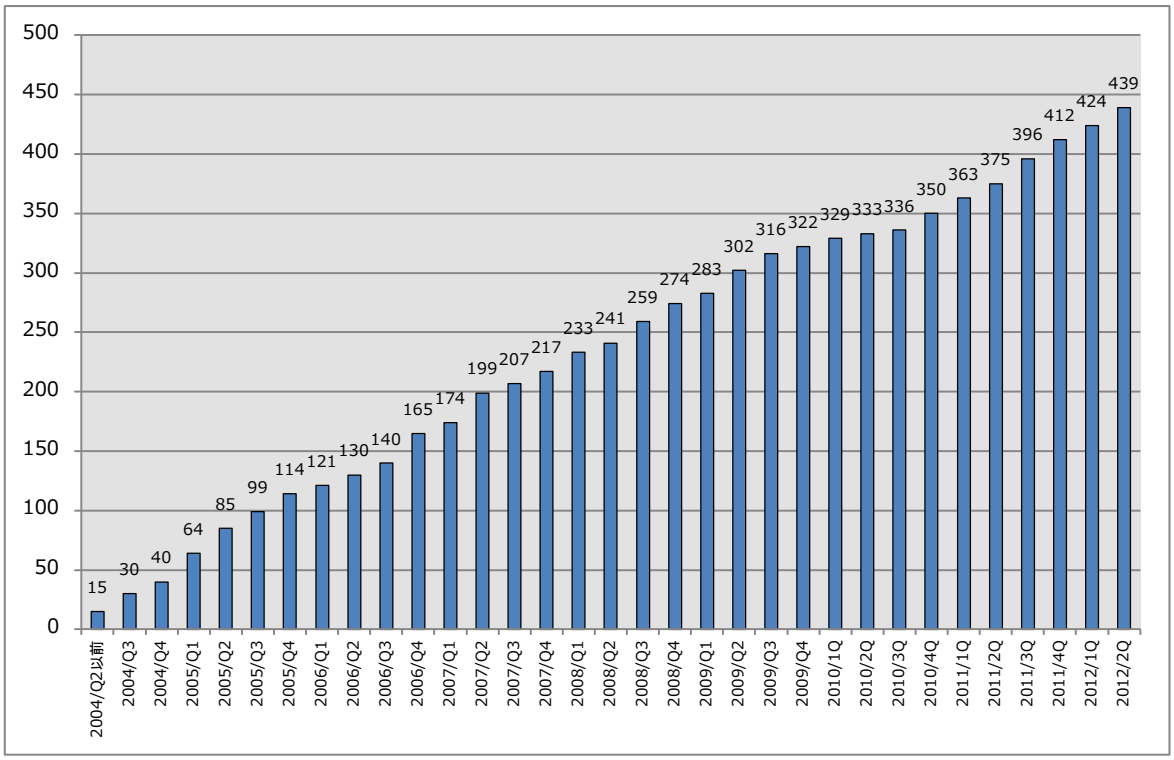
本基準では、受付機関に IPA、調整機関に JPCERT/CC が指定されています。JPCERT/CC は IPA が受け付けた届出情報の転送を受けて、製品開発者への情報提供を行い、対策情報公開に至るまでの調整を行っています。最終的には、 IPA と共同で、脆弱性情報ポータル JVN において対策情報を公開しています。両組織間においては、脆弱性情報の分析結果や脆弱性情報の取扱い状況等の情報交換を行うなど、緊密な連携をおこなっています。なお、本基準における IPA の活動および四半期毎の届出状況については、次の URL をご参照ください。

独立行政法人情報処理推進機構(IPA) 脆弱性対策
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、2012 年 6 月 30 日現在で 439 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]

2.5. セキュアコーディング啓発活動

2.5.1. バンコクで「Java および Android セキュアコーディングセミナー」を開催

タイを代表する CERT 機関である ThaiCERT とマヒドン大学の協力のもと、バンコク市内にて Java および Android セキュアコーディングセミナーを計 2 日間、開催し、JPCERT/CC の久保正樹、戸田洋三が講師を務めました。4 月 26 日は Java 言語に関して、27 日(金)には Android アプリ開発に関して、どちらもセキュリティ上の問題や脆弱性を作り込まないコーディング手法等について演習を交えて解説しました。定員を上回る参加応募があり、各回 60 名弱のプログラマにご参加いただきました。

初日の Java セキュアコーディングに関するセミナーでは、ソフトウエアの脆弱性について概観し、Java 言語で書かれたアプリケーションに関する脆弱性の事例紹介、Java セキュアコーディングスタンダード（https://www.jpcert.or.jp/java-rules/）のルールの紹介を行い、脆弱なサンプルコードを使ったクイズ形式の演習を実施しました。

2 日目の Android セキュアコーディングセミナーでは、今日の Android 端末をめぐるセキュリティ問題を概観し、OWASP Top 10 Mobile Risks をベースに Android アプリ開発でセキュリティ上注意すべきポイントについて解説しました。また、脆弱性を作り込んだ Android アプリのソースコードを配付し、受講者が実機を使って問題の特定と修正を行う演習を行いました。

タイ国内の開発者においては、スマートフォン等の携帯端末向けアプリ開発で使用される Java/Android に対する関心が高いにも関わらず、セキュリティを考慮したアプリ開発に関するノウハウや情報源が不足しており、脆弱な製品が生み出されやすい状況にあります。そうした状況の改善に取り組むべく、参加者にセキュリティへの強い関心を持っていただくことを目的の一つとしてこのセミナー実施し、成果を得ることができました。また、セキュリティ教育コースとしても高い評価を得ることができ、JPCERT/CC と ThaiCERT との連携強化にも資するものとなりました。

[図 2-6 セミナー初日の受講者の様子(バンコク)]

2.5.2. バンドンで「Java セキュアコーディングセミナー」を開催

今回で 3 度目となるインドネシアにおけるセキュアコーディングセミナーは、インドネシア国内 40 の大学が参加する Academic CSIRT（ http://www.acad-csirt.or.id ）と Maranatha Christian University 情報科学部の協力を得て、西ジャワ州の州都であるバンドンにて、5 月 31 日(木)から 6 月 2 日(土)の 3 日間にわたり開催されました。JPCERT/CC からは久保正樹、戸田洋三の両名が講師として現地に赴きました。

座学では、Java セキュアコーディングスタンダードのカテゴリ(オブジェクトの生成、メソッド、宣言と初期化、数値型と演算等)に沿って、言語の基本概念をさらいつつ、脆弱なコードとその解決方法を具体的なコードを交えて解説しました。演習では実機を使ってのセキュリティコードレビューやコードの修正、クイズ形式の問題演習を行いました。

約 150 名の応募があり、他州からの参加者を含む、計 100 名強の学生、大学教員、セキュリティコンサルタント、プログラマの方々にご参加いただきました。

JPCERT/CC では今後も、タイ、インドネシアをはじめとする ASEAN 諸国に対して、脆弱性を作り込まないセキュアなソフトウエア開発に関する啓発活動を継続してまいります。

[図 2-7 演習に取り組む受講者(バンドン)]

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

昨年度に引き続き、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(講師：久保正樹)、第 4 回(講師：戸田洋三)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エ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む必要があるかを解説しました。第 4 回「セキュアコーディング、実践」では、ソフトウエ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ともに、コード例を使ってセキュリティコードレビューを実際に体験する演習を行いました。

2.5.4. 開発者向けウェブマガジン Codezine に「Java セキュアコーディング入門」連載中

翔泳社の開発者向けウェブマガジン CodeZine に「Java セキュアコーディング入門」と題したシリーズで Java セキュアコーディングの解説記事を連載しています。Java 言語を使ったコーディング上の注意点や脆弱性を作り込まない作法を、最近話題の Android アプリケーションの脆弱性についても取り上げつつ解説しています。本四半期は、熊谷裕志が以下の記事を執筆しました。次回以降の連載も是非ご一読ください。

第 6 回「スマートフォンアプリへのブラウザ機能の実装に潜む危険――WebView クラスの問題について」(6 月 25 日公開)

CodeZine（コードジン）Java セキュアコーディング入門
http://codezine.jp/article/corner/437

2.5.5. JSSEC「Android アプリのセキュア設計・セキュアコーディングガイド」公開

6 月 11 日、「Android アプリのセキュア設計・セキュアコーディングガイド」の初版が JSSEC のホームページで公開されました。

「Android アプリのセキュア設計・セキュアコーディングガイド」(6 月 1 日版)
http://www.jssec.org/dl/android_securecoding.pdf

サンプルコード一式
http://www.jssec.org/dl/android_securecoding.zip

JPCERT/CC セキュアコーディングチームのメンバらが本ガイド執筆のお手伝いをさせていただきました。Android アプリケーション開発者向けのセキュア設計、コーディング上のノウハウをまとめた参考書として、多くの Android アプリ開発者に活用していただければ幸いです。

2.5.6. セキュアコーディング 出張セミナー

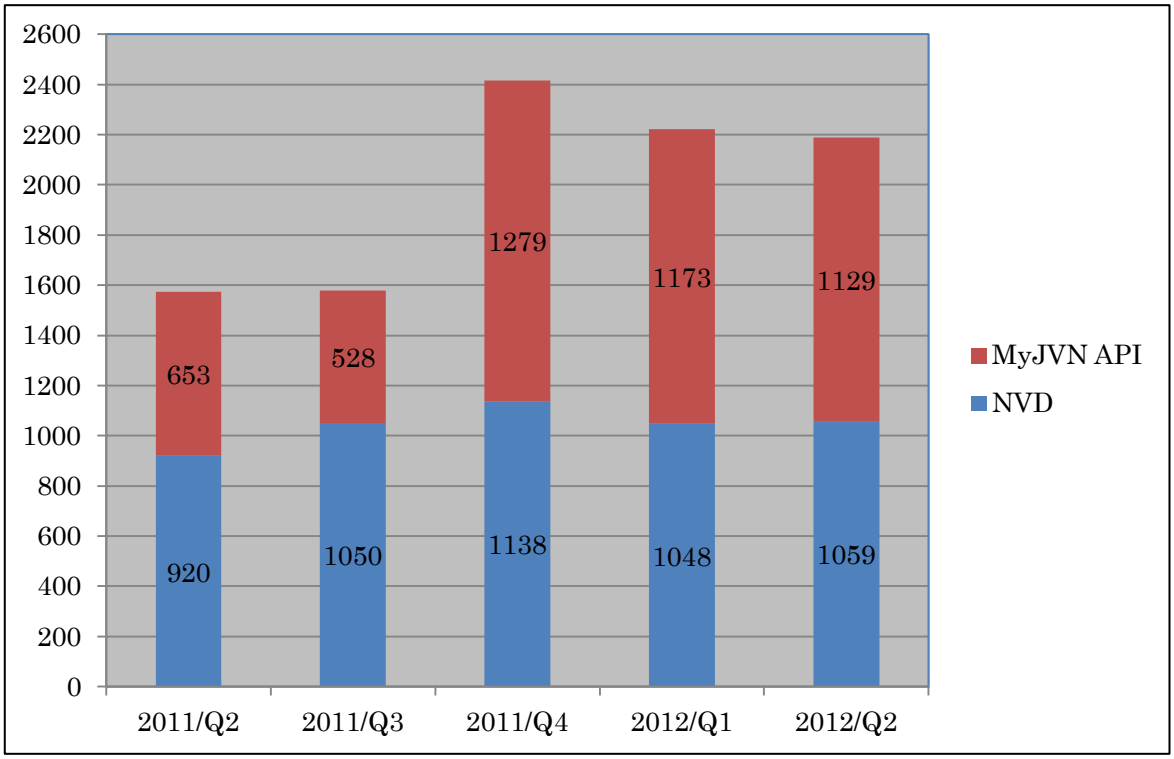
JPCERT/CC では、ソフトウエア製品等の開発を行う企業・組織を対象に、セキュアコーディングに関する出張セミナー（有償）の実施を承っています。マネジメント層へのセキュリティ啓発や新人研修のメニュー等としてもご利用いただけます。今年度から、これまで提供していた C/C++言語におけるセキュアコーディングセミナーに加え、新たに Java 言語版および Android アプリケーション開発に関するセキュアコーディング出張セミナーの提供を開始しました。出張セミナーのご依頼、お問合わせは、secure-coding@jpcert.or.jp までご連絡下さい。

2.6. VRDA フィードによる脆弱性情報の配信

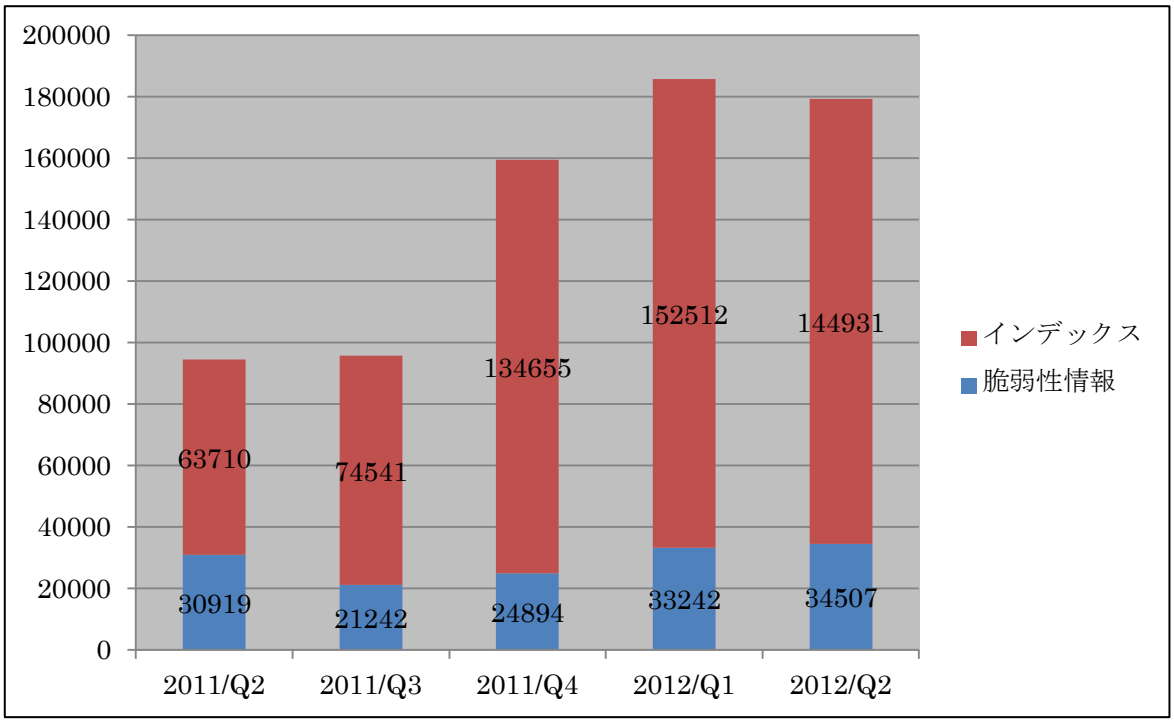
JPCERT/CC は、大規模組織の組織内 CSIRT などでの利用を想定して、KENGINE などのツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST (National Institute of Standards and Technology)の NVD (National Vulnerability Database) を外部データソースとして利用した、VRDA (Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、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を [図 2-8] に、VRDA フィードの利用傾向を [図 2-9] と [図 2-10] に示します。 [図 2-9] では、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。 [図 2-10] 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。

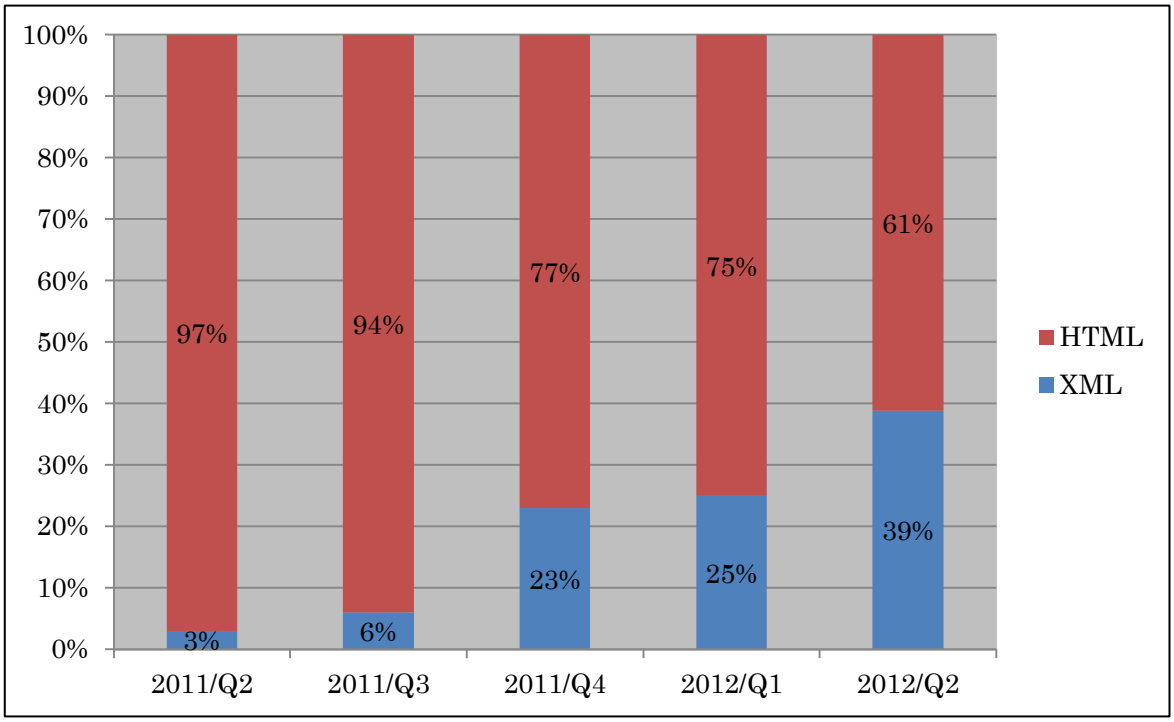


[図 2-8 VRDA フィード配信件数]



[図 2-9 VRDA フィード利用件数]

[図 2-9] に示したように、VRDA フィードインデックスと脆弱性情報の利用数は、それぞれ前四半期と同程度となりました。



[図 2-10 脆弱性情報のデータ形式別利用割合]

[図 2-10] 脆弱性情報のデータ形式別利用傾向は、前四半期と比較して XML 形式の脆弱性情報の利用割合が大きく増加しました。

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。

近年、サイバー攻撃に関する情報共有が注目されており、その中では標的型攻撃等で使われたメールの特徴情報をもとに攻撃を早期発見して防御するという取り組みが行われています。メールを媒体とする攻撃ではメールの送信元となったサーバやアカウントが不正に利用されている可能性があります。また、同じ送信元を使って攻撃が繰り返されることも珍しくありません。そのような、「背景にあるインシデント」を掘り起こすために、アーティファクト分析ではメールの送信元等も含めて国内外から提供された情報を総合的に分析しています。そのような分析の結果をもとに情報提供を行うことで、他のインシデントの早期発覚に役立てていただけるよう活動しています。

4. 制御システムセキュリティ強化に向けた活動

4.1. 情報発信活動

制御システムセキュリティインシデントに関わる事例や標準の動向、その他の技術動向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まとめ、本年度より月刊で、制御システム関係者向けにニュースレターとして提供しています。本四半期は計 3 回（5 月 2 日、6 月 1 日、6 月 21 日）配信しました。
本ニュースレター配信先の制御システムセキュリティ情報共有コミュニティについては、現在 215 名のメンバの方にご登録いただいています。今後も内容の充実を図っていく予定です。参加資格や申込み方法については、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コミュニティ
https://www.jpcert.or.jp/ics/ics-community.html

4.2. 国内外情報収集活動

国土保安省（DHS）の下で Control Systems Security Program（CSSP）として進められている活動の一環として、2012 年 5 月に米国ジョージア州サバナにおいて「ICSJWG コンファレンス」が開催されました。今回は ICS-CERT の連携先関係者を招待した「国際パートナー・ディ」

も初めて開催され、経済産業省による日本の近況紹介も行われました。JPCERT/CC はこれら両行事に参加し、制御システムセキュリティにおける米国の取り組みや現状についての情報収集に努めました。また、海外組織との今後の連携を強化すべく海外パートナーとの情報共有や収集情報の展開にも取り組んでいきます。

ICSJWG 2012 Spring Conference Agenda
http://www.us-cert.gov/control_systems/icsjwg/presentations/spring2012/agenda-tue.html
http://www.us-cert.gov/control_systems/icsjwg/presentations/spring2012/agenda-wed.html

4.3. 日本版 SSAT 配布状況

JPCERT/CC では、制御システムの構築と運用に関するセキュリティ上の問題項目を手軽に抽出し、バランスの良いセキュリティ対策を行っていただくこと目的として、簡便なセキュリティ自己評価ツール日本版 SSAT の配布を行なっています。このツールに対してベンダや業界団体がカスタマイズを加えるなどして再配布することも許諾しています。本四半期は、JPCERT/CC に対して 7 件の申込みがあり、直接配布件数の累計が 101 件となりました。

4.4. 関連団体との連携活動

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、制御システム向けのチェックツールの作成に向けて、各業界のユーザからの意見も伺いながらブラッシュアップをはかる活動を行いました。

4.5. 制御システム業界におけるインシデントおよび脆弱性ハンドリング活動開始準備

制御システム業界におけるインシデントおよび脆弱性ハンドリングの調整機関として活動を開始すべく準備に着手しました。インシデントハンドリングに関しては、各関係者との調整、情報共有の検討など、脆弱性ハンドリングに関しては、制御システム向け脆弱性研究会の開催準備を行いました。

5. 国際標準化活動

5.1. 「脆弱性情報開示」の国際標準化活動への参加

脆弱性情報の開示(Vulnerability Disclosure (VD)；29147；旧称 Responsible Vulnerability Disclosure) および取扱手順(Vulnerability Handling Process (VHP)； 30111) に関して、それぞれ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、ベンダ内部での対応を規定することになっています。

今期においては、5 月 7 日～11 日に開催された SC27 ストックホルム会議に参加し、前期に参加各国から提出されていた修正コメントをもとに、両標準案について検討作業を行いました。

「脆弱性情報の開示」については、第 4 次委員会草案(CD； Committee Draft)に対して合計 157 件(カナダ:2 件、ドイツ:3 件、日本:30 件、韓国:2 件、英国:5 件、米国:41 件、FIRST:74 件)のコメントが寄せられていました。個々の修正に加えて、文書全体の取扱が議論され、日本としては CD のままでの改訂を求めましたが、プロジェクト・エディタが強硬に国際標準草案(DIS)とするよう主張し、これに英米も折れる形で DIS に進むことが決まりました。この結果、文書はプロジェクト・エディタが改訂の上、6 月 22 日までに SC27 事務局に提出されて国際投票に付される予定です。なお DIS の最初の国際投票では各国における翻訳のための時間的を確保するため，6 か月間の猶予期間が取られるため、今秋に予定されている次回の SC27 国際会議では議論されず、次の国際会議での審議は来春になります。

「脆弱性取扱手順」については、第 2 次作業草案(WD； Working Draft)に対して合計 59 件(日本:7 件、英国:9 件、米国:18 件、FIRST:25 件)のコメントが寄せられていました。個々の修正に加えて、文書全体の取扱が議論され、FIRST からも提案があって，今回の改訂で委員会草案(CD)のステージに進めることが合意されました。

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。

5.2. インシデント管理の国際標準化活動への参加

5 月 7 日から 11 日にわたりスウェーデンで開催された ISO/IEC JTC-1/SC27 ストックホルム会合に出席し、インシデント管理や CSIRT の運営に関する国際標準の策定を行う WG4 の活動に参加しました。本会合において、ISO/IEC 27035:2011 (インシデント管理；Information security incident management)の早期改訂が正式に承認され、次の 3 つのパートからなるマルチパート

標準へ再構成すべく、標準化活動が進められることになりました。

Part 1. インシデント管理の原理（Principles of Incident Management）
Part 2. インシデントの管理と対策のためのガイドライン（Guidelines for Incident Management Readiness）
Part 3. インシデント対応の運用のためのガイドライン（Guidelines for Incident Response Operations）

会合での主な論点は、Part3 用に韓国が用意した草案(N10713)と、インシデントのカテゴリ化と分類に関して記述した既存の標準 27035 の附属書を独立させて本標準シリーズの Part4 とする中国の提案(N10711)の取扱でした。前者については、内容の確認作業が行われ、日本からは草案の構成などに関するコメントを行いました。後者については、過去の標準化の作業を踏まえ、まずは標準文書の附属書(Annex)の形でドキュメントの成熟化を図るべきであるとの立場を日本として表明しました。これに他国も賛同して中国の提案をひとまず退け、附属書については、新規 Part2 の附属書として引き継がれる形で標準化作業を進めることで合意が得られました。

Part 1 については、既存の 27035:2011 の§4. Overview を骨子とし、他のパートのオーバービューを追加した内容のドラフトドキュメントが、Part 1 を担当するエディターによって用意される予定です。Part 2 については、英国がエディターを出し、草案を用意することになっていましたが、予定していたメンバが急遽担当できなくなったため、変わって米国がエディターを務め作業を引き継ぐことになりました。

今後はこれら 3 つのパートの 1st Working Draft 作成に向けた作業が行われます。なお、会合において、Part3 のタイトルが変更されました(旧タイトル：Guidelines for CSIRT Operations)。

インシデント管理と CSIRT の運営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。

6. 国際連携活動関連

6.1. 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) 等のインシデント対応調整能力の向上を目指し、トレーニングやイベントでの講演等を通じた CSIRT の構築・運用支援を行っています。

6.1.1. アジア太平洋地域(オセアニア)における活動

6.1.1.1. APEC-TEL 45 CSIRT ワークショップ(2012 年 4 月 6 日)

4 月 6 日にベトナムで開催された APEC-TEL 45 Security and Prosperity Steering Group 会合において「CSIRT ワークショップ」が行われました。JPCERT/CC は APEC-TEL 関係者からの協力依頼を受け、本ワークショップに講師として参加しました。
同ワークショップは APEC-TEL45 に参加する、主に APEC 加盟各国の情報セキュリティ政策担当者を対象に、CSIRT を構築するためのベストプラクティスを共有し、当該国での CSIRT 構築を支援すること、および、既に CSIRT が存在する場合にはその能力の向上を図り、高度化する情報セキュリティ上の脅威に対応することを目的にしています。JPCERT/CC は本ワークショップで、現在行っているマルウェア解析の業務やネットワーク定点観測システム TSUBAME プロジェクトなどによって得られた知見を参加者と共有すると共に、CSIRT を構築するプロセスについて解説を行いました。

6.1.1.2. 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。

6.1.2. その他地域における活動

6.1.2.1.アフリカ CSIRT 構築支援 等(2012 年 5 月 7 日-12 日)

JPCERT/CC は、5 月にガンビアで開催された国際会議 AfNOG-13 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。また 5 月 12 日に開催された AfricaCERT Cybersecurity Day に参加しました。
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-13 はガンビアの携帯電話サービス事業者などのスポンサーにより、ガンビア最大の都市セレクンダで開催されました。
JPCERT/CC が担当した CSIRT トレーニングは、AfNOG-13 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。同様のトレーニングは 2010 年春から実施しており、今回で 4 回目の開催となります。JPCERT/CC は、5 月 7 日から 11 日まで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。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 がネットワークフォレンジックに関するトレーニング(図 x-x 参照)を行いました。トレーニングには、約 25 名のインターネット運用者及び政策担当者が集いました。

[図 6-1 トレーニングの模様]

5 月 12 日に開催された AfricaCERT Cybersecurity Day は主にアフリカ諸国の情報セキュリティ政策担当者約 30 名が一堂に会して、各国の取り組みを共有すると共に、JPCERT/CC が行ったアジアでの取り組みなどのプレゼンテーションを参考に、今後のアフリカ全体の取り組みの方向性について議論を行いました。

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://afnog.org/afnog2012/index.php
AAF（Africa Asia Forum on Network Research & Engineering)
http://www.africaasia.net/

JPCERT/CC は、インターネットが急速に普及すると予想されている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。

6.2. 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。

6.2.1. アジア太平洋地域(オセアニア)における活動

6.2.1.1. APCERT (Asia Pacific Computer Emergency Response Team)

JPCERT/CC は、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/

6.2.1.1.1. APCERT Steering Committee 電話会議の実施

5 月 23 日に Steering Committee(運営委員)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。

6.2.1.1.2. APCERT と他組織間との連携

1) APEC TEL 45 SPSG への参加(2012 年 4 月 5 日-11 日)
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 TEL (APEC Telecommunications and Information Working Group) の会合がベトナムのダナンで開催されました。その中の Security and Prosperity Steering Group (SPSG) 会合において、APCERT の議長チームとして、APCERT の活動をテーマとした講演を行いました。また、APEC 地域の他 CSIRT と共に CSIRT ワークショップを開催しました。(ワークショップの詳細については、「6.1.1.1. APEC-TEL 45 CSIRT ワークショップ」をご参照下さい。)

2) National Cyber Security Framework Workshop への参加 (2012 年 4 月 12 日-16 日)
NATO（北大西洋条約機構）におけるサイバー防御機能の強化を目的とする NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) が、オーストリアのウィーンにて主催した National Cyber Security Framework Workshop に出席し、APCERT の議長チームとして、APCERT の活動およびアジアにおける最新のセキュリティ事情をテーマとした講演を行いました。

3) OECD WPISP ミーティングへの参加 (2012 年 5 月 9 日-10 日)
フランスのパリで開催された OECD（経済協力開発機構）の Working Party on Information Security and Privacy (WPISP) のミーティングに、APCERT の議長チームとして参加し、OECD-APCERT の連携の可能性について意見交換を行いました。

6.2.1.2. JPCERT/CC と ThaiCERT 間の MOU（覚書）締結式（2012 年 4 月 25 日）

4 月 25 日、タイの Ministry of Information and Communication Technology (MICT、情報通信省) のプレスルームにて、JPCERT/CC とタイの National CSIRT である ThaiCERT 間の MOU（覚書）締結式を行いました。
JPCERT/CC と ThaiCERT は、ThaiCERT が設立された 2000 年以降、各種インシデントへの対応、ネットワーク定点観測システム TSUBAME プロジェクトへの参画、アジア太平洋地域に所在する CSIRT からなるコミュニティである APCERT の運営等において連携関係を維持してきました。
ThaiCERT はこれまで National Electronics and Computer Technology Center (NECTEC) の下部機関に位置付けられていましたが、2011 年 2 月より Ministry of Information and Communication Technology (MICT、情報通信省) 傘下にある Electronic Transactions Development Agency (ETDA) の下部機関となったことに伴い、インシデント発生時における連携や情報の取り扱いに関するルール、両組織の連携強化等を再確認すべく、本 MOU を締結しました。
締結式には、ETDA 常任理事の Ms. Surangkana Wayuparb をはじめ、MICT、ThaiCERT 等の関係者約 40 名が集まりました。また、MICT の事務次官 Ms. Jirawan Boonperm と個別に面談をし、安全なインターネット環境の構築のための両組織間の連携の重要性を確認しました。
本 MOU の締結を機に、JPCERT/CC による ThaiCERT スタッフへの技術研修の実施等を検討しています。

6.2.1.3. 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。
今四半期は、5 月 26、27 日に中国上海で開催された「2012 サイバー犯罪と社会安全論壇(网络犯罪与社会安全论坛)」に参加し、中国地域におけるセキュリティ業界・コミュニティの活動状況について情報収集を行い、日本国内の関係者会合などへ展開しました。

6.2.2. その他の地域における活動

6.2.2.1. STOP. THINK. CONNECT Messaging Convention Meeting (2012 年 4 月 24 日)及び APWG 2012 CeCOS (2012 年 4 月 25 日-27 日)

チェコ共和国の首都プラハで開催された APWG Counter-eCrime Operations Summit (CeCOS VI) に参加しました。フィッシングやその他のオンライン金融犯罪の最新の手口について情報収集を行い、その内容を組織内外に共有しました。
また、APWG に先立って 4 月 24 日に行われた STOP. THINK. CONNECT Messaging Convention Meeting というユーザ啓発の為のプログラム作成の会議に参加し、ユーザ啓発の分野での国際連携のあり方について議論を行いました。

6.2.2.2. 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/

6.2.2.2.1. FIRST Steering Committee 出席（2012 年 6 月 19 日）

FIRST の Steering Committee のメンバである JPCERT/CC の理事 山口英が 6 月 19 日にマルタで開催された Steering Committee に出席しました。First の運営方針に関して議論が行われました。

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

6.2.2.2.2. 24th Annual FIRST Conference Malta への参加(2012 年 6 月 17 日-22 日)

FIRST の第 24 回年次会合が 6 月 17 日から 22 日までマルタで開催されました。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 is not an Island” 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 2 つの発表/パネルディスカッションへの参加を行いました。

- 『Global and Regional CERT Collaboration to Reduce Cyber Conflict Risk』伊藤友里恵
- 『What we found about BCP on 3/11』満永拓邦

満永は、企業や官公庁へのインタビューから得られた震災時の BCP(事業継続計画)に関する知見をもとに講演を行い、BCP が想定通り機能しなかった事例や、実際の現場で BCP に求められる要素について紹介を行いました。
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 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 24 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。

24th Annual FIRST Conference Malta
http://conference.first.org

6.2.2.2.3. FIRST スポンサー（他の CSIRT の加盟手続き支援）

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、書類作成等を行いました。
本四半期は、モーリシャスのNational CSIRTであるCERT-MUのスポンサーを務め、同組織は5月に正式にFIRST 加盟に至りました。

6.2.2.3. National CSIRT Meeting への参加(2012 年 6 月 23 日-24 日)

第 24 回 FIRST 年次会合後に、引き続きマルタにて、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 は、この場において、CSIRT 構築支援等の活動状況や、来年で発足から 10 周年を迎える APCERT の活動状況についての紹介を行いました。National CSIRT Meeting についての詳細は、以下の URL をご参照ください。

National CSIRT Meeting
http://www.cert.org/csirts/national/meeting/

6.2.2.4. 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 の活動等について継続的に情報発信を行っています。

JPCERT/CC 英語ブログ
http://blog.jpcert.or.jp/

7. フィッシング対策協議会事務局の運営

JPCERT/CC では、フィッシング対策協議会（本章において「協議会」といいます。）の事務局を担当しており、協議会においては、経済産業省からの委託により、各ワーキンググループ活動の運営や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。

7.1. 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 を通じて、フィッシングに関するニュースや緊急情報を 10 件発信しました。

本四半期も前四半期と同様に、金融機関の第二認証情報を詐取するフィッシングとオンラインゲームをかたるフィッシングの報告を、それぞれ複数受けました。協議会では、名前をかたられた事業者に、フィッシングメールやサイトの関連情報を提供しました。また、第二認証情報を詐取するフィッシングに関しては、「大和ネクスト銀行をかたるフィッシング(4 月 4 日)」、「三井住友銀行をかたるフィッシング(4 月 13 日)」、「住信 SBI ネット銀行をかたるフィッシング(5 月 7 日)」および「楽天銀行をかたるフィッシング(5 月 10 日)」[図 6-1]の 4 件の緊急情報を、オンラインゲームをかたるフィッシングについては、「真 女神転生 IMAGINE をかたるフィッシング(4 月 2 日)」を協議会の Web 上で公開しました。
さらに、当該フィッシングに使用されたサイトを停止するための調整を行い、フィッシングサイトの停止を確認しました。

[図 6-1　楽天銀行をかたるフィッシングサイト
https://www.antiphishing.jp/news/alert/rakutenbank20120510.html]

7.2.　フィッシングサイト URL 情報の提供

協議会では、会員の中で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、フィッシングに関する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 を集めたリストを、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。本四半期末の時点で協議会から情報を提供している事業者等は 16 組織、現在も複数の事業者との間で新たに情報提供を開始するための協議を行っており、提供先を順次拡大していく予定です。

7.3.　講演活動

協議会ではフィッシングに関する現状を紹介し、効果的な対策を呼びかけるため講演活動を行っています。本四半期は次のとおり講演を行いました。

(1) 山本 健太郎「最新のフィッツシングの現状と企業側の対策」
　京都府警, 第２回京（みやこ）サイバー犯罪対策協議会 2012 年 5 月 28 日

7.4.　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、報告されたフィッシングサイト数を含む、毎月の活動報告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 2012 年 4 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201204.html
フィッシング対策協議会 2012 年 5 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201205.html
フィッシング対策協議会 2012 年 6 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201206.html

8. 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。

8.1. 早期警戒情報フィールドレポート

JPCERT/CC が提供する「早期警戒情報」や「インシデント対応支援」を、組織や企業が具体的にどのように活用されているかについて、企業等を訪問して聞かせていただき、一連のインタビュー記事として JPCERT/CC ホームページに掲載しています。本四半期においては、次の組織について新たに掲載しました。

(1) 【第 2 回】株式会社三菱東京ＵＦＪ銀行～自社収集情報を補完し、対応策の根拠を補強できる情報が
欲しい～(2012 年 5 月 10 日)
https://www.jpcert.or.jp/magazine/security/fieldww-mufg.html

9. 講演活動一覧

(1) 満永 拓邦 (早期警戒グループ リーダ 情報セキュリティアナリスト) :
「最近の国内インシデントの傾向や対応事例」
SST/NetAgent 共催セミナー, 2012 年 4 月 12 日
(2) 真鍋 敬士 (理事,分析センター長) :
「最近の事例に見るサイバー攻撃の傾向とこれからの取り組み」
チェック・ポイント 脅威対策ロードショー Japan 春, 2012 年 4 月 24 日
(3) 早貸 淳子 (常務理事) :
「進化するインシデントレスポンスー攻撃の変質への対応、新たな領域への対応」
第 16 回サイバー犯罪に関する白浜シンポジウム, 2012 年 5 月 24 日

(4) 真鍋 敬士 (理事,分析センター長) :
「最近の事例に見るサイバー攻撃の傾向とこれからの取り組み」
チェック・ポイント 脅威対策ロードショー in 大阪, 2012 年 5 月 25 日
(5) 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) :
「情報セキュリティ対策研修：基本と対策」
公立大学法人高崎経済大学 情報セキュリティ研修, 2012 年 6 月 27 日

10. 執筆一覧

(1) 熊谷 裕志(情報流通対策グループ 情報システムセキュリティアナリスト) :
「Android のここに注意！セキュリティ対策のツボ」
日経 BP 日経ソフトウエア 6 月号,2012 年 4 月 24 日
(2) 山田 秀和(情報流通対策グループ 制御システムセキュリティ 情報セキュリティアナリスト) :
「制御システム(装置)における脆弱性と今後の取り組み」
月刊計装 6 月号,2012 年 5 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) :
「日本近期網路攻擊概述」
資安人雜誌 86 期 June 2012, 2012 年 6 月
(4) 宮地 利雄 (理事) :
「組織・企業の制御システムを守る」
電気学会誌 第 132 巻 6 号 特集「サイバー攻撃から組織・システムを守れ」, 2012 年 6 月
(5) 熊谷 裕志(情報流通対策グループ 情報システムセキュリティアナリスト) :
「スマートフォンアプリへのブラウザ機能の実装に潜む危険—WebView クラスの問題について」
翔泳社 CodeZine,2012 年 6 月 25 日

11. 開催セミナー等一覧

(1) Java および Android セキュアコーディングセミナー
※本セミナーの詳細は、「2-5-1」をご参照ください。
(2) Java セキュアコーディングセミナー
※本セミナーの詳細は、「2-5-2」をご参照ください。
(3) 企業向けセキュアコーディングセミナー
※本セミナーの詳細は、「2-5-6」をご参照ください。

12. 後援一覧

(1) IAF フォーラム 2012

(主催：IAF（Industrial Automation Forum）)

2012 年 6 月 27 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