JPCERT/CC®

JPCERT-PR-2015-04
発行日 : 2015-10-08

JPCERT/CC 活動概要 [2015 年 7 月 1 日 ～ 2015 年 9 月 30 日]

活動概要トピックス

ートピック1ー　APCERT 年次総会 2015 、サイバーグリーンおよび TSUBAME ワークショップの開催～2016 年 APCERT 年次総会ホストは JPCERT/CC～

アジア太平洋地域の CSIRT コミュニティである APCERT の年次総会が、9 月 6 日から 10 日の日程でクアラルンプールにて開催され、APCERT の主要メンバであるオペレーショナルメンバ（全 28 チーム）から JPCERT/CC を含む 26 チームが参加しました。”Bridging the World – Go Cyber Green”をテーマに掲げ、初の試みとして、イスラム諸国のコンピュータ緊急対応チームである OIC-CERT (The Organization of the Islamic Cooperation – Computer Emergency Response Team) の年次総会と同時開催されました。APCERT が目指す”safe, clean and reliable cyber space”のビジョンに向けて、アジア太平洋地域の枠を超え、サイバーグリーンや TSUBAME 等のプロジェクトを通して OIC-CERT の加盟チームとも連携を強化していくことがチーム間で合意されました。
APCERT 年次総会では、APCERT 議長チーム/副議長の改選が行われ、JPCERT/CC は 4 期(4 年)連続して務めた議長チームの任期を満了し、CERT Australia が新たな議長チームとして選出されました。また、運営委員会(Steering Committee)および事務局の改選も行われ、JPCERT/CC は引き続き運営委員会および事務局に再選されました。JPCERT/CC は、引き続き APCERT の主要メンバとして様々な活動をリードして参ります。
さらに APCERT 運営委員会では、来年度の APCERT 年次総会の開催について協議され、JPCERT/CC がホストチームに選出されました。JPCERT/CC は、APCERT 年次総会 2016 の日本開催に向けて準備を進めて参ります。

また、年次総会に併せ、JPCERT/CC が主導するサイバーグリーンおよび TSUBAME プロジェクトのワークショップを開催しました。各プロジェクトの概要およびワークショップの詳細については、本活動概要の次の項目をご参照ください。

4.2.1.4.　サイバーグリーンワークショップの開催 (9 月 6 日)
4.2.1.5.　TSUBAME WORKSHOP 2015 の開催 (9 月 8 日)

ートピック2ー　連絡不能開発者の製品に関する脆弱性情報の公表を開始

JPCERT/CC は、ソフトウエア製品等の脆弱性情報について製品開発者との調整を行い、原則として JVN

を通じて脆弱性情報等を一般に公表する活動を 2004 年 7 月から行っています。調整に際して、連絡が取れない製品開発者もあり、2011 年度からは、JVN 上で「連絡不能開発者一覧」として公表して広く連絡の手掛かりを求めることになりました。それでも連絡が取れない場合があり、当該製品の利用者が脆弱性の存在を知らされることなく使い続けるリスクに晒されることを避けるため、十分な審議手続きを経たうえで脆弱性情報を公表するように、2014 年 5 月に脆弱性情報取扱基準等が改正されました。この新ルールに依った初めてのものとして 9 月 3 日に 2 件の脆弱性情報を公表しました。同様に製品開発者と連絡が取れていない脆弱性情報が 10 年間余りの取扱業務の中で少なからず累積してきています。JPCERT/CC は IPA と連携して、製品開発者の協力が得られない状況下で情報を公表するために必要な慎重さと時機を逸しない迅速さを両立させつつ、脆弱性取扱制度の実効性を高めるために努めてまいります。

2015-09-03　連絡不能開発者の製品に関する脆弱性情報の公表を開始
https://www.jpcert.or.jp/press/2015/20150903-vuladj.pdf

ートピック3ー　サイバーセキュリティ対策活動への協力者に感謝状贈呈

JPCERT/CC は、わが国におけるサイバー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。)の被害の最小化を目的に、インシデントへの対応支援活動、インシデントを未然に防止するための早期警戒活動、マルウエア分析、ソフトウエア製品等の脆弱性に関する調整活動などを行っていますが、これらの活動を円滑かつ効果的に進めるためには、皆様からの情報提供や様々なご協力が欠かせません。

JPCERT/CC では、サイバーセキュリティ対策活動に対する皆様からの御好意と御力添えに深く思いをいたし、特に顕著なご貢献をいただいた方に感謝状を贈呈する制度を設けています。本年度の対象者として、脆弱性情報を JVN 上で広くお知らせする活動を通して、製品利用者のサイバー攻撃による被害の抑止、IT 利用の安全性の確保にご協力をいただいたサイボウズ株式会社　Cy-SIRT　様、制御システムセキュリティ分野における先進的な活動をもって脆弱性情報ハンドリングのスキームにご協力いただいた横河電機株式会社 YOKOGAWA PSIRT 様に対して 2015 年 8 月に感謝状と記念の盾を贈呈致しました。

サイバーセキュリティ対策活動への協力者に感謝状贈呈
https://www.jpcert.or.jp/press/priz/2015/PR20150820-priz.html

ートピック4ー　日本シーサート協議会の加盟会員が 100 組織となる

JPCERT/CC が事務局を務めている日本シーサート協議会(英文名：Nippon CSIRT Association、以下「NCA」といいます。)は、日本で活動する CSIRT 間の情報共有および連携を図るとともに、組織内

JPCERT CC®
CSIRT の構築を促進、支援することを目的に、日本国内で活動する、有志の民間および企業内 CSIRT から構成された会員組織です。
組織を狙ったサイバー攻撃の巧妙化・複雑化により、複数の CSIRT が連携して迅速な対応をすることが求められる状況となり、組織内 CSIRT 構築とともに NCA への加盟も増加し、本四半期末において、NCA に加盟した国内 CSIRT は 100 組織となりました。
加盟組織数は今後も増加する見込みであり、加盟組織は各 CSIRT 間の連携強化に取り組んでいます。

日本シーサート協議会(英文名：Nippon CSIRT Association、略称：NCA)：
国内のシーサート(CSIRT：Computer Security Incident Response Team)組織が互いに協調し、連携して共通の問題を解決する場として、平成 19 年 3 月 28 日、有志の民間および企業内 CSIRT によりに設立されました。
JPCERT/CC は、設立発起人として設立に協力、会員として参加しているほか、NCA 事務局を担当しています。日本シーサート協議会の詳細は、次の URL をご参照ください。

日本シーサート協議会(NCA)
http://www.nca.gr.jp/

本活動は、経済産業省より委託を受け、「平成２７年度サイバー攻撃等国際連携対応調整事業」として実施したものです。
ただし、「7.フィッシング対策協議会の会員組織向け活動」に記載の活動については、この限りではありません。また、「4.国際連携活動関連」、「9.主な講演活動一覧」、「10. 主な執筆一覧」、「11. 協力、後援一覧」「12.JPCERT/CC 感謝状贈呈」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 4128 件、インシデント件数ベースでは 3748 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、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も 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 2058 件でした。前四半期の 2593 件と比較して 21%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等に対し、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、インターネット利用組織における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することを目的として活動しています。国際的な調整・支援が必要となるインシデントについては、日本における窓口組織として、国内や国外(海外の CSIRT 等)の関係機関との調整活動を行なっています。

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/2015/IR_Report20151008.pdf

1.1.1. インシデントの傾向

1.1.1.1. フィッシングサイト

本四半期に報告をいただいたフィッシングサイトの件数は 522 件で、前四半期の 491 件から 6%増加しました。また、前年度同期(417 件)との比較では、25%の増加となりました。

本四半期のフィッシングサイトの報告件数を、装っていたブランドが国内か国外かで分けた内訳を添えて[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	7 月	8 月	9 月	国内外別合計（割合）
国内ブランド	51	32	30	113(22%)
国外ブランド	96	97	75	268(51%)
ブランド不明(注 2)	42	44	55	141(27%)
月別合計	189	173	160	522(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等の理由により、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。

国内金融機関および国内オンラインゲームを装ったフィッシングサイトを調べると、大量に作成された.com ドメインが使用されており、大半のドメインに香港の IP アドレスが割り当てられていました。金融機関のフィッシングでは標的のブランド名に似せた文字列を含むドメイン名が、オンラインゲームのフィッシングでは無作為に作られた文字列のドメイン名が多く使用されていました。また、xyz、top、space のような比較的新しい gTLD を使用したフィッシングサイトを確認しています。

国内ブランドを装ったフィッシングサイトが使用していた IP アドレスの国別内訳を見ると、43.1%が香港、28.5%がアメリカの IP アドレスであり、あわせて 7 割以上を占めていました。

フィッシングサイトの調整先の割合は、国内が 48%、国外が 52%であり、前四半期(国内 52%、国外 48%)に比べ、国外への調整が増加しています。

1.1.1.2. Web サイト改ざん

本四半期に報告が寄せられた Web サイト改ざんの件数は、592 件でした。前四半期の 649 件から 9%減少しています。

7 月に Adobe Flash Player の脆弱性が複数公開されました。それから間もなくして、国内 Web サイトが改ざんされ、それらの脆弱性を悪用した攻撃サイトに誘導していた事例を JPCERT/CC でも確認しました。その後も、同じ攻撃目的で改ざんされた国内 Web サイトの報告を多数受領し、複数の改ざんパターンがあることを特定しています。

また、改ざんされた国内 Web サイトにアクセスすることにより、国内組織を標的とした攻撃に使用されたマルウエア Emdivi がダウンロードされる事例が本四半期には確認されました。改ざんされたサイトでは、正規の js ファイルに不正なコードが埋め込まれており、それによって、同サイト上に不正に設置され、上記の脆弱性を悪用する swf ファイルを読み込ませるページに誘導される仕組みになっていました。

9 月上旬ごろから、Web サイトに埋め込まれた広告によってマルウエア配布サイトに誘導されたと推測されるインシデントの報告を受領しています。報告をもとに Web サイト上の広告を定期的に取得して観測したところ、広告に埋め込まれる js ファイルが、不定期に不正なコードが混ざったものになっていることを確認しました。

1.1.1.3. その他

JPCERT/CC では、国内組織を標的とした高度な攻撃に関して、使用されたマルウエア、C&C サーバなどの調査、被害組織への調査協力を行うなどの活動に取り組んでいます。

本四半期は、標的型攻撃に関する連絡を 67 組織に行っています。そのうち 52 組織への連絡は Emdivi と呼ばれる遠隔操作マルウエアに関連したものでした。また、Emdivi の対応の他に、PlugX とよばれる遠隔操作マルウエアや、アクセスした端末の情報を収集する ScanBox とよばれる JavaScript のツールなどに関連して、被害組織やインフラとして使用されていたサーバを管理する組織へ連絡を行いました。

JPCERT/CC では、引き続き、被害組織への対応支援、調査協力を行うとともに、被害の可能性のある組織への連絡、調査協力などの活動を通じて被害拡大防止の活動に取り組んで参ります。

1.1.2. インシデントに関する情報提供のお願い

Web サイト改ざん等のインシデントを認知された場合は、JPCERT/CC にご報告ください。JPCERT/CC では、当該案件に関して攻撃に関与してしまう結果となった機器等の管理者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およ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 サイト改ざん等のサイバー攻撃に関する情報を収集し、分析しています。これらのさまざま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等も併せて行い、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」 (限定配付) 等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 31,000 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) 等を通じて、本四半期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等について、次のような注意喚起情報を発行しました。

発行件数：17 件（うち 2 件更新） https://www.jpcert.or.jp/at/

2015-07-09 Adobe Flash Player の脆弱性 (APSB15-16) に関する注意喚起 (公開)
2015-07-13 2015 年 7 月 Adobe Flash Player の未修正の脆弱性に関する注意喚起 (公開)
2015-07-14 Cisco 社製セキュリティアプライアンスソフトウェアの脆弱性に関する注意喚起 (公開)
2015-07-15 2015 年 7 月 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)
2015-07-15 Adobe Reader および Acrobat の脆弱性 (APSB15-15) に関する注意喚起 (公開)
2015-07-15 Adobe Flash Player の脆弱性 (APSB15-18) に関する注意喚起 (公開)
2015-07-15 2015 年 7 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起 (公開)
2015-07-15 2015 年 7 月 Adobe Flash Player の未修正の脆弱性に関する注意喚起 (更新)
2015-07-16 Adobe Flash Player の脆弱性 (APSB15-18) に関する注意喚起 (更新)
2015-07-21 マイクロソフト セキュリティ情報 (MS15-078) に関する注意喚起 (公開)
2015-07-29 ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2015-5477) に関する注意喚起 (公開)
2015-08-12 2015 年 8 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起 (公開)
2015-08-12 Adobe Flash Player の脆弱性 (APSB15-19) に関する注意喚起 (公開)
2015-08-19 マイクロソフト セキュリティ情報 (MS15-093) に関する注意喚起 (公開)
2015-09-03 ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2015-5986) に関する注意喚起 (公開)
2015-09-09 2015 年 9 月 Microsoft セキュリティ情報 (緊急 5 含) に関する注意喚起 (公開)
2015-09-24 Adobe Flash Player の脆弱性 (APSB15-23) に関する注意喚起 (公開)

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 Weekly Report として発行しています。このレポートには、「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 74 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。

2015-07-01　APCERT Annual Report 2014 公開
2015-07-08　IETF が「Deprecating Secure Sockets Layer Version 3.0」を公開
2015-07-15　PHP 5.5 系最後のリリース
2015-07-23　Windows Server 2003 サポート終了
2015-07-29　DNS Summer Days 2015 開催、および資料公開
2015-08-05　総務省が「ウェブサービスに関する ID・パスワードの管理・運用実態調査結果」を公開
2015-08-12　MS14-025 への対策確認の呼びかけ
2015-08-19　データベース・セキュリティ・コンソーシアム「DB 内部不正対策ガイドライン」を公開
2015-08-26　「サイバーセキュリティ 2015（案）」コメント募集
2015-09-02　組織外にある DNS サーバへのアクセスを制御する
2015-09-09　警察庁「平成 27 年上半期のインターネットバンキングに係る不正送金事犯の発生状況等について」公開
2015-09-16　フィッシング対策協議会「フィッシングレポート 2015 ― 進む対策、利用者としてできること ―」を公開
2015-09-30　SiSOC Tokyo 発足セミナ開催

1.2.1.3. 早期警戒情報

JPCERT/CC では、国民の生活や社会経済活動を支えるインフラ、サービスおよびプロダクト等を提供している組織の情報セキュリティ関連部署もしくは組織 CSIRT に向けて、それらの組織やサービス提供先に深刻なセキュリティ上の問題を惹起する可能性のある脅威情報やその分析結果、対策方法に関する情報等を「早期警戒情報」として提供しています。

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。

【セキュリティ関連企業から流失した未修正の脆弱性を利用した攻撃への対応】
2015 年 7 月、イタリアのセキュリティ関連企業から、未修正の脆弱性や検証コードを含む情報が流出した事件がありました。流出した情報のうち、Adobe Flash Player に関する未修正の脆弱性 (CVE-2015-5199, CVE-2015-5122, CVE-2015-5123) や Windows に関する未修正の脆弱性 (CVE-2015-2426) については、検証コード

も含まれていたため、攻撃者が悪用することが容易な状況でした。流出した検証コードを利用した標的型攻撃などを JPCERT/CC でも確認したので、被害の未然防止や軽減のため、当該脆弱性に関する注意喚起を発行しました。

【日本に対するサイバー攻撃への対応】
歴史上の出来事等に起因する、いわゆるサイバー攻撃の特異日には、日本の政府関係組織等に向けた反日
的なサイバー攻撃が多く発生する傾向にあります。JPCERT/CC では、そうした特異日の前後には、関係
する各国の National CSIRT と連携して、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 つの特異日がありました。昨年は大規模なサイバー攻撃には繋がらなかったものの、攻撃予告や、一定数の Web サイト改ざんが確認されており、本年も攻撃に備えた対応体制をとると共に、Web サイトへの攻撃に対する注意喚起を、7 月 14 日に 情報処理推進機構 (IPA) と共同で提供を行いました。2015 年 9 月上旬には、日本に対するサイバー攻撃の呼びかけは確認されたものの、大規模な攻撃に繋がる動きは確認されませんでした。DDoS 攻撃の影響と思われる Web サイトの応答時間の悪化は一部で確認されたものの、おおむね深刻な被害は発生しなかったように見受けられます。また、特異日に関連する Web サイト改ざんの被害も確認されませんでした。JPCERT/CC では、攻撃に関して収集した情報を、重要インフラ企業や組織内 CSIRT に向けて提供しました。

1.3. インターネット定点観測

JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを収集するインターネット定点観測システム TSUBAME を構築し、運用しています。TSUBAME から得られる情報を、既に公開されている脆弱性情報やマルウエア、攻撃ツールの情報などと対比して分析することで、攻撃活動や攻撃の準備活動等の状況を把握することに努めています。

1.3.1. インターネット定点観測システム TSUBAME の運用、および観測データの活用

JPCERT/CC は、さまざまな地域に設置された観測用センサーを含むインターネット定点観測システム TSUBAME を構築運用するとともに、観測されたデータを各地域の CSIRT と共同で分析をするためのプロジェクトである TSUBAME プロジェクトの事務局を担当しています。2015 年 8 月には maCERT（モロッコ）、MNCERT/CC(モンゴル) が新たに参加し、2015 年 9 月末時点で、観測用センサーは 21 地域 25 組織に設置されています。今後も設置地域を拡大し、より充実したセンサー網の構築と共同分析の高度化を進めるべく関係機関と交渉を続けています。

TSUBAME プロジェクトの目的等詳細については、次の Web ページをご参照ください。

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

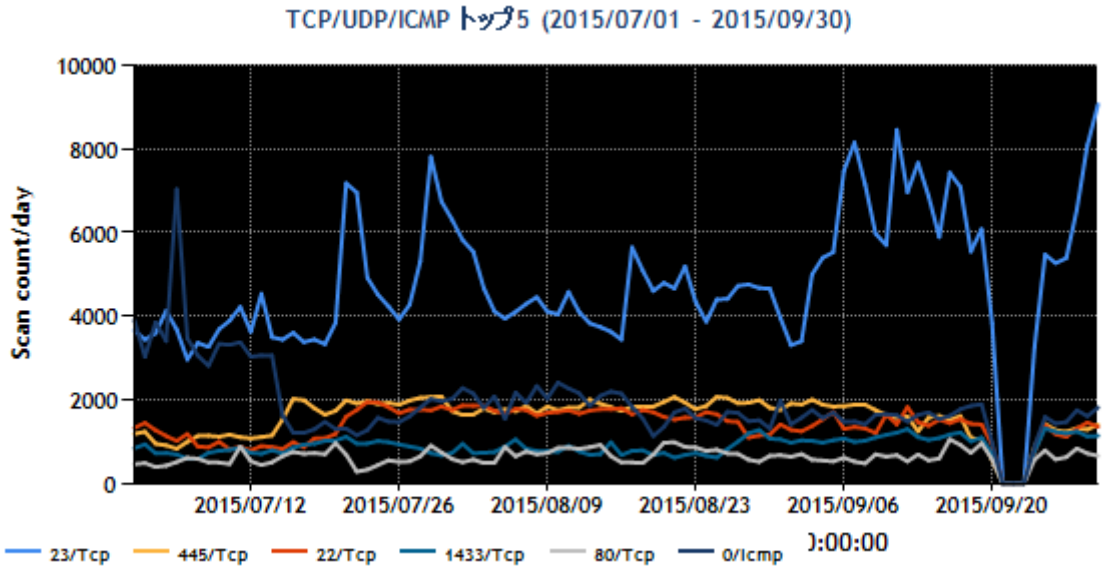
JPCERT/CC は、TSUBAME で収集したデータを宛先ポート番号や送信元地域ごとに分類して統計分析し、既知の脆弱性情報やマルウエア、攻撃ツール等との関連を考察することで、攻撃活動や準備活動の捕捉に努めています。

主に日本企業のシステム管理者等の方々に、自ネットワークに届くパケットの傾向と比較していただけるよう、日本国内のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2015 年 4 月から 6 月分のレポートを 2015 年 7 月 29 日に公開しました。

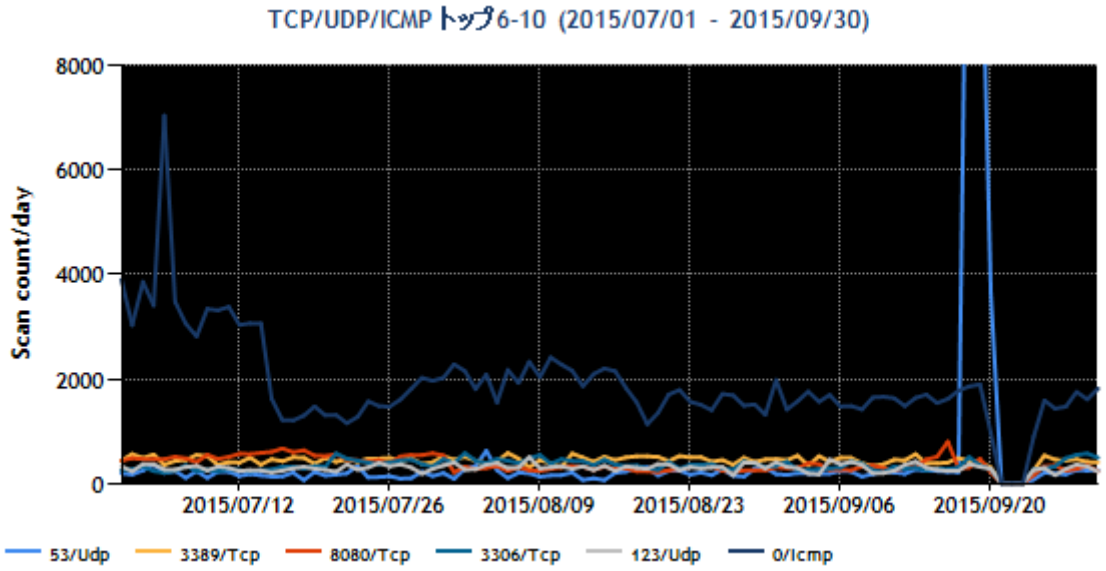
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート(2015 年 4～6 月)
https://www.jpcert.or.jp/tsubame/report/report201504-06.html

本四半期に TSUBAME で観測された宛先ポート別パケット数の上位 1 位～5 位および 6 位～10 位を、[図 1-1]と[図 1-2]に示します。なお、2015 年 9 月 20 日 14 時 50 分から 9 月 24 日 9 時 20 分にかけて、インターネット定点観測システムの収容施設の設備に問題が発生し、当該システムの一部に障害が発生しました。このため障害期間の観測データが欠落しています。

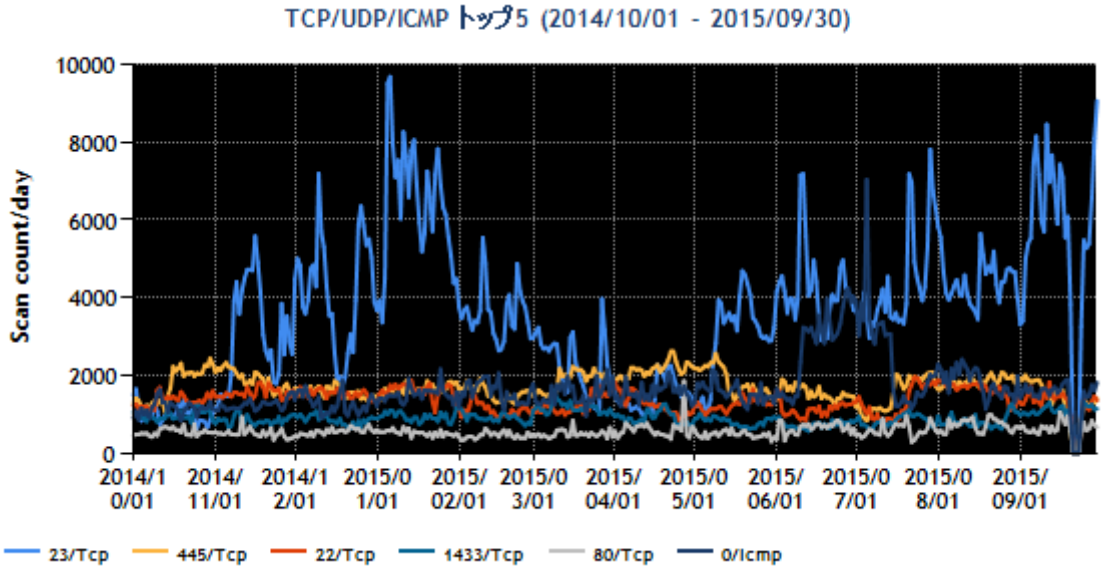


[図 1-1 宛先ポート別グラフ トップ 1-5 (2015 年 7 月 1 日-9 月 30 日)]

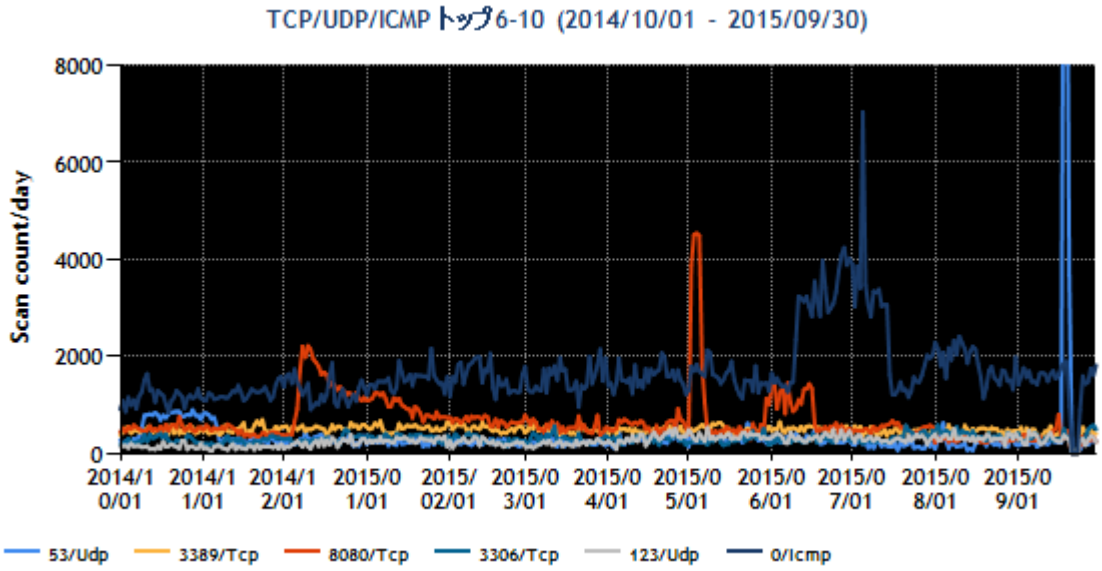


[図 1-2 宛先ポート別グラフ トップ 6-10 (2015 年 7 月 1 日-9 月 30 日)]

また、過去 1 年間 (2014 年 10 月 1 日-2015 年 9 月 30 日) における、宛先ポート別パケット数の上位 1 位～5 位および 6 位～10 位を[図 1-3]と[図 1-4]に示します。



[図 1-3 宛先ポート別グラフ トップ 1-5 (2014 年 10 月 1 日-2015 年 9 月 30 日)]



[図 1-4 宛先ポート別グラフ トップ 6-10 (2014 年 10 月 1 日-2015 年 9 月 30 日)]

前四半期に増加した 8888/Tcp、37564/Tcp、8118/Tcp 宛へのパケットは、増加以前の水準まで減少しました。23/Tcp 宛へのパケット数は、5 月に増加し、以降その水準を維持しています。その他、順位に変動はありますが、Windows や Windows 上で動作するサービスへのスキャン活動と見られるパケットや、SSH サーバ等遠隔操作のためにサーバ側が待ち受けているポートのスキャン活動と見られるパケットも、これまでと同様に多く観測されています。

1.3.2. TSUBAME 観測データに基づいたインシデント対応事例

JPCERT/CC では、日々TSUBAME の観測情報を分析し、不審な動きが認められた場合に、必要に応じて送信元 IP アドレスの管理者に連絡する等の対処をしています。

(1) RDP (Remote Desktop Protocol) が使用するポートを探索するサーバについての対応

日本国内の企業や大学の IP アドレスを送信元とする、RDP (Remote Desktop Protocol) が使用するポートへのパケットを多数観測しています。JPCERT/CC では、該当パケットの送信元 IP アドレスの管理者に情報を提供し、マルウエアなどに感染し、不審なツールが設置されていないかなど調査を依頼しました。その後、該当 IP アドレスから同様のパケットは観測されなくなったことから、ツールの除去等の対処が行われ、その後の被害拡大の抑止につながったと考えられます。

1.3.3. TSUBAME WORKSHOP 2015 の開催（2015 年 9 月 8 日）

2015 年 9 月の APCERT 年次会合において TSUBAME Workshop 2015 を開催しました。今回の APCERT 年次会合は、イスラム諸国のコンピュータ緊急対応チームである OIC-CERT の年次会合と合同開催され

ましたので、TSUBAME Workshop 2015 には、TSUBAME プロジェクトメンバだけでなく、OIC-CERT 側の参加者で同プロジェクトに関心を寄せる方々も加わり、例年の 2 倍近く約 60 名が参加しました。TSUBAME Workshop 2015 では、JPCERT/CC からの報告とハンズオン演習を実施し、このうち報告では、本年度 JPCERT/CC が観測したパケットを分析した結果、Shellshock の脆弱性が残る多くの組込み製品や、SCADA、OpenResolver などを探索する活動を捕捉した事例を紹介し、ハンズオン演習では、TSUBAME で蓄積したデータから、パケット数の推移をもとに傾向の変化を見極め、自地域のインシデント対応を行うための方法を習得していただきました。

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]と共同運営)を通じて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、脆弱性を作り込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. 脆弱性関連情報の取扱状況 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

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」(平成 26 年経済産業省告示第 10 号。以下「本基準」といいます。)に基づ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」に指定されています。本基準の受付機関に指定されている IPA から届出情報の転送を受け、本基準を踏まえて取りまとめられた「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(以下「パートナーシップガイドライン」といいます。)に従って、対象となる脆弱性に関係する製品開発者の特定、脆弱性関連情報の適切な窓口への連絡、開発者による脆弱性の検証等の対応や脆弱性情報の公表スケジュール等に関する調整を行い、原則として、調整した公表日に JVN を通じて脆弱性情報等を一般に公表しています。JPCERT/CC は、脆弱性情報の分析結果や脆弱性情報の取り扱い状況等の情報交換を行う等、IPA と緊密な連携を行っています。なお、脆弱性関連情報に関する四半期ごとの届出状況については、次の Web ページをご参照ください。

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/

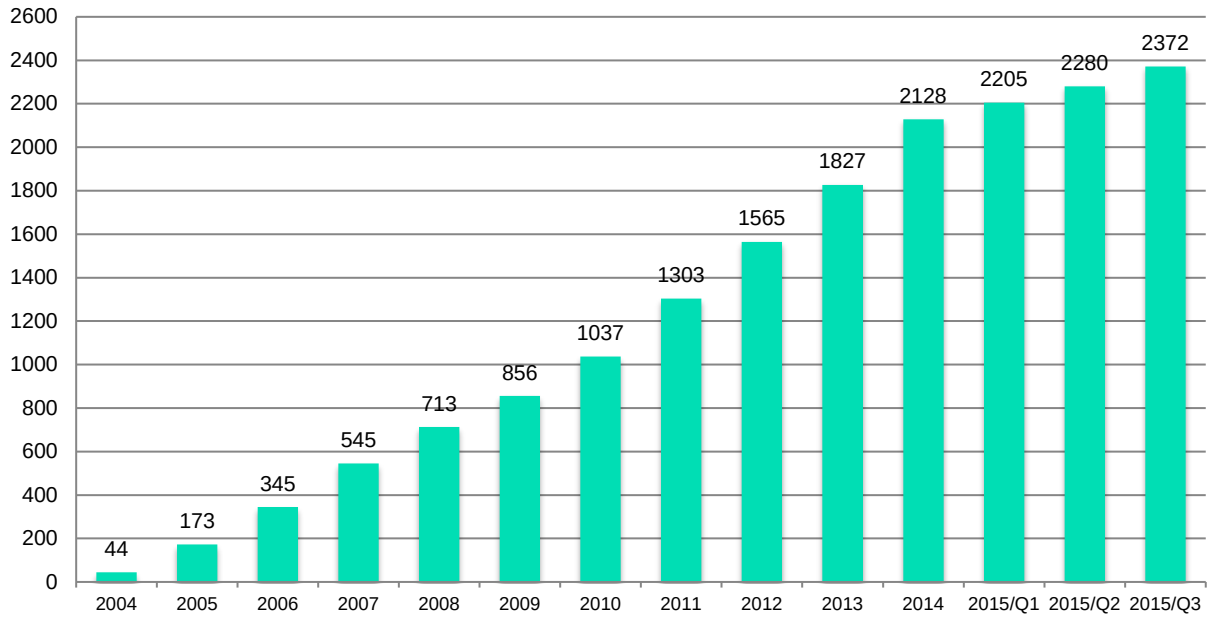
2.1.2. Japan Vulnerability Notes(JVN)において公表した脆弱性情報および対応状況

JVN で公表している脆弱性情報は、本基準に従って国内で届け出られた脆弱性に関するもの(「JVN#」に続く 8 桁の数字の形式の識別子[例えば、JVN#12345678 等]を付与。以下「国内取扱脆弱性情報」といいます。)と、それ以外の脆弱性に関するもの(「JVNVU#」に続く 8 桁の数字の形式の識別子[例えば、JVNVU#12345678 等]を付与。以下「国際取扱脆弱性情報」といいます。)の 2 種類に分類されます。国

際取扱脆弱性情報には、CERT/CC や NCSC-FI といった海外の調整機関に届け出られ国際調整が行われた脆弱性情報、海外の製品開発者から JPCERT/CC に直接届け出られた自社製品の脆弱性情報等が含まれます。なお、国際取扱脆弱性情報には、US-CERT からの脆弱性注意喚起の邦訳を含めていますが、これには「JVNTA」に続く 8 桁数字の形式の識別子(例えば、JVNTA#12345678)を使っています。

本四半期に JVN において公表した脆弱性情報は 92 件(累計 2,372 件)で、累計の推移は[図 2-1]に示すとおりです。本四半期に公表された個々の脆弱性情報に関しては、次の Web ページをご参照ください。

JVN(Japan Vulnerability Notes)
https://jvn.jp/

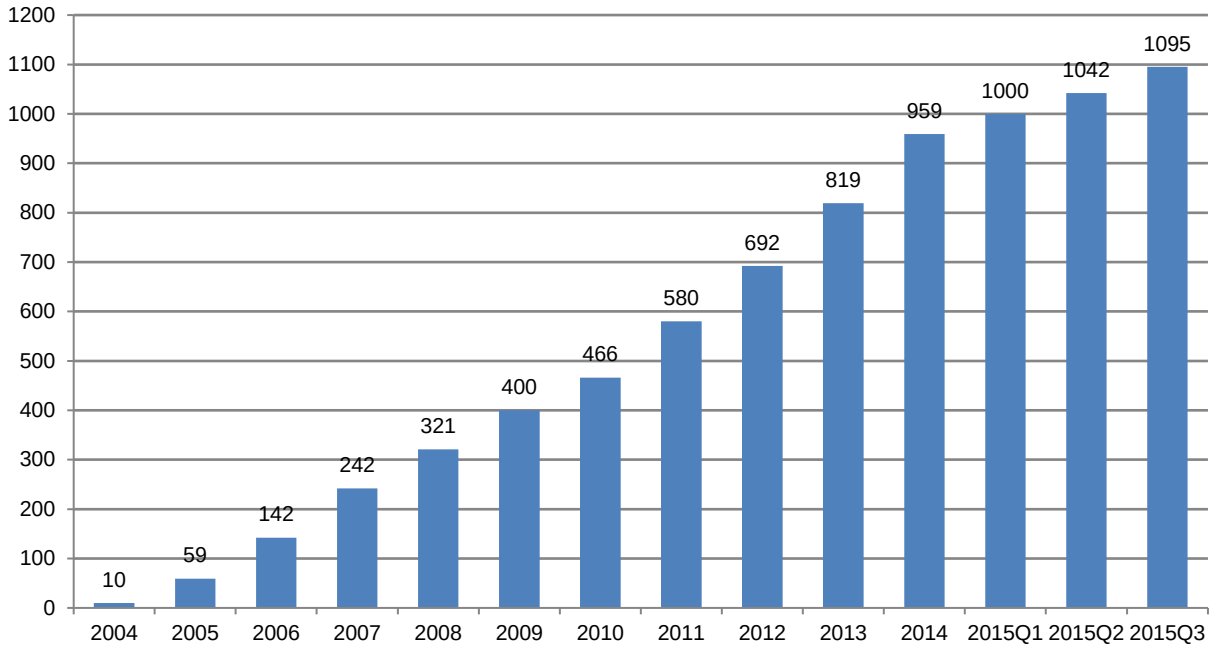


[図 2-1　JVN 公表累積件数]

本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 53 件(累計 1095 件)で、累計の推移は[図 2-2]に示すとおりです。53 件のうち、42 件が国内製品開発者の製品、11 件が海外の製品開発者の製品に関連したものでした。また、前四半期に引き続き本四半期も、自社製品届出による脆弱性情報を 1 件公表しました。

本四半期に公表した脆弱性情報を、影響を受けた製品のカテゴリで分類すると、Android アプリに関するものが 9 件、掲示板ソフトウエアに関するものが 5 件、SNS に関するものが 3 件、Web アプリケーションフレームワークに関するものが 3 件、施設予約管理ソフトウエアに関するものが 3 件、ネットワークモニタリングソフトウエアに関するものが 3 件、プラグインに関するものが 3 件、アクセス解析ツールに関するものが 2 件、グループウエアに関するものが 2 件、コンテンツ管理システム(CMS)に関す

るものが 2 件、iOS 向けアプリに関するものが 2 件、PHP スクリプトに関するものが 2 件、請求書作成ソフトウエアに関するものが 2 件、それ以外では、ActiveX、Microsoft Office、PHP、SNS 構築ソフトウエア、暗号化ソフトウエア、組込系ルータ、組込系プリンタ、サーバ関連製品、スクリプトエンジン、文書管理システム(DMS)、メール配信システム、等がそれぞれ 1 件ずつあり、そのカテゴリは多岐に及びました。



[図 2-2 公表を行った国内取扱脆弱性情報の累積件数]

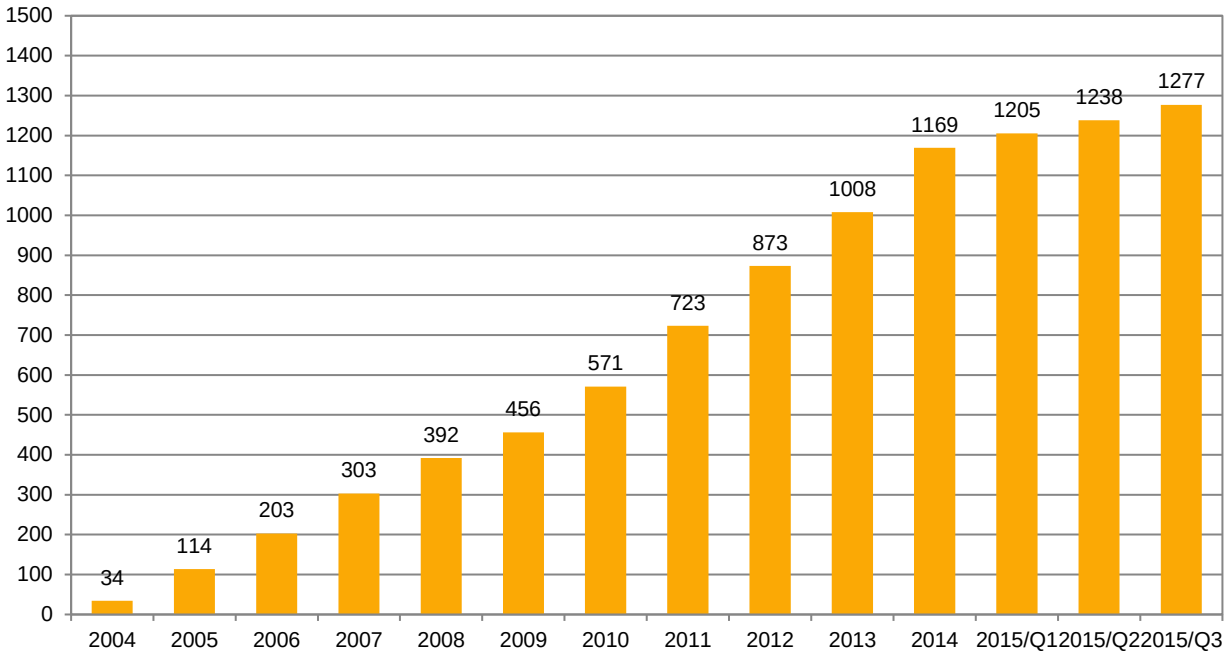
本四半期に公表した国際取扱脆弱性情報は 39 件(累計 1277 件)で、累計の推移は[図 2-3]に示すとおりです。

本四半期に公表した脆弱性で特筆すべきものが二つありました。一つは、対策が無いいわゆるゼロデイの脆弱性情報を 4 件公開したことです。この 4 件の内訳は、Adobe Flash Player が 2 件、Microsoft のモジュールに関するものが 1 件、そして複数製品に影響がある Android 向けメディア再生サービスである Stagefright に関するものが 1 件でした。いずれも一般に広く使われている製品であることから、速やかに注意喚起を促し、各製品開発者より対策が提供されるまでの間、回避策等で脆弱性の影響を軽減する必要があるものでした。二つめは、ルータ、デジタルビデオレコーダ、無線 LAN やルータといったいわゆる組込系製品における脆弱性の公開が 13 件と、これまでになく多かったことです。またそれら組込系製品の中には、自動車に搭載する製品も含まれていました。これは、組込系製品の新たな分野における脆弱性に対し、研究員や発見者が注目していた結果ではないかと推測されます。

本四半期に公表した脆弱性情報の製品カテゴリ別内訳を多い順に挙げると、組込系製品に関するものが 13 件、ウェブブラウザ用メディアプレイヤーが 4 件、サーバ関連製品が 3 件、ネットワーク管理ソフトウエアが 2 件、データベース製品が 2 件、Android 向けメディア再生サービス、BIOS 実装、

OpenSSL、制御系製品、企業向け管理ソリューション製品、教育機関向け管理ソリューション製品、ストレージ製品、セキュリティ対策製品、フォント用モジュール、プラグイン、プロトコル、ヘルプデスク向け管理システム、指紋認証入退室管理システム等がそれぞれ 1 件ずつあり、取り扱い製品は多岐に及びました。
また自社製品に関する届出は、ISC から 3 件、Apple から 2 件、OpenSSL Project から 1 件、横河電機から 1 件ありました。

本四半期においては、既に公開済みの Flash Player に関する個別脆弱性情報とは別に、改めて JVN Technical Alert(注意喚起)として、「2015/07/15　JVNTA#97243368: Adobe Flash Player および Microsoft Windows の脆弱性」を JVN にて公開し、ユーザへアップデート等の適切な対策を講じるよう促しました。



[図 2-3　国際取扱脆弱性情報の公表累積件数]

2.1.3. 連絡不能開発者とそれに対する対応の状況等

本基準に基づいて報告された脆弱性について、製品開発者と連絡が取れない場合には、2011 年度以降、当該製品開発者名を JVN 上で「連絡不能開発者一覧」として公表し、広く連絡の手掛かりを求めています。これまでに 217 件(製品開発者数は 145 件)を公表し、40 件(製品開発者の数は 24 件)の調整を再開することができ、脆弱性関連情報の取扱いにおける「滞留」の解消に一定の効果を挙げています。

本四半期に新たに連絡不能開発者一覧に掲載した案数は 12 件(製品開発者の数は 10 件)でした。本四半期末日時点で、合計 177 件の連絡不能開発者案件を引き続き掲載し、継続して製品開発者や関係者から

の連絡および情報提供を呼び掛けています。

こうした呼びかけによっても製品開発者と連絡が取れないケースについて、利用者保護の観点から脆弱性情報を公表する手続きを定めた、本規準およびパートナーシップガイドラインが昨年5月に改正され、公表判定委員会の第一回目が2014年第4四半期に、第二回目が2015年5月にそれぞれ開催されました。これを受けて本四半期には、第二回公表判定委員会において公表が妥当と判断された2件の脆弱性情報を9月3日に公表しました。開催された制度に基づく初の脆弱性情報の公表であり、併せてプレスリリースも公表しました。プレスリリースの詳細は、次のWebページをご参照ください。

2015-09-03　連絡不能開発者の製品に関する脆弱性情報の公表を開始
https://www.jpcert.or.jp/press/2015/20150903-vuladj.pdf

2.1.4. 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、脆弱性情報の円滑な国際的流通のための脆弱性情報ハンドリングを行っている米国の CERT/CC、英国の CPNI、フィンランドの CERT-FI 等の海外の調整機関と協力関係を結び、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通知および対応状況の集約、脆弱性情報の公表時期の設定等の調整活動を連携して行っています。さらに Android 関連製品や OSS 製品の脆弱性の増加につれて、それらの製品開発者が存在するアジア圏の調整機関、特に韓国 KrCERT/CC や中国 CNCERT/CC、台湾 TWNCERT との連携も増えており、国際連携活動の幅が一層広がっています。また、米国 ICS-CERT との連携も、2013 年末より活発化しており、本四半期までに合計 9 件の制御システム用製品の脆弱性情報を公表しました。新たな分野での国際的活動が定着しつつあると言えます。
JPCERT/CC は、日本における脆弱性ハンドリングのコンタクトポイントとして、脆弱性情報ハンドリングにおける国際的活動を引き続き推進してまいります。

JVN 英語版サイト(https://jvn.jp/en)上の脆弱性情報も、日本語版とほぼ同時に公表しており、脆弱性情報の信頼できるソースとして、海外のセキュリティ関連組織等からも注目されています。

また、JPCERT/CC は、CNA（CVE Numbering Authorities）として認定されています。本四半期は、JVN で公表したもののうち、国内で届出られた脆弱性情報 52 件に、JPCERT/CC が CVE 番号を付与しました。2008 年以降においては、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（全体の 1 割弱）を除いて、JVN 上で公表する脆弱性のほぼすべてに 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 Web ページをご参照ください。

News & Events　“JPCERT/CC Becomes CVE Numbering Authority”
https://cve.mitre.org/news/archives/2010_news.html#jun232010a

CVE Numbering Authorities
https://cve.mitre.org/cve/cna.html
About CVE
https://cve.mitre.org/about/index.html

2.2. 日本国内の脆弱性情報流通体制の整備

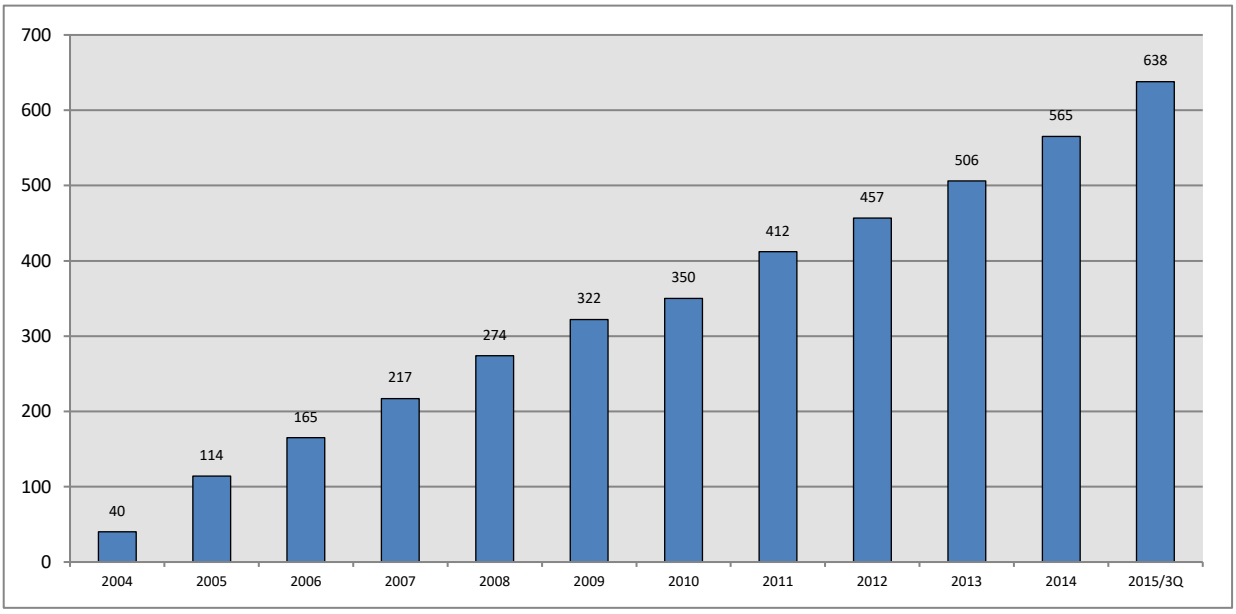
JPCERT/CC では、本基準に従って、日本国内の脆弱性情報流通体制を整備しています。
詳細については、次の Web ページをご参照ください。

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(2015 年版)
https://www.jpcert.or.jp/vh/partnership_guideline2015.pdf
JPCERT/CC 脆弱性情報取扱いガイドライン
https://www.jpcert.or.jp/vh/vul-guideline2014.pdf

2.2.1. 日本国内製品開発者との連携

本基準では、脆弱性情報を提供する先となる製品開発者のリストを作成し、各製品開発者の連絡先情報を整備することが、調整機関である JPCERT/CC に求められています。JPCERT/CC では、製品開発者の皆さま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 2-4]に示すとおり、2015 年 9 月 30 日現在で 638 となっています。
登録等の詳細については、次の Web ページをご参照ください。

JPCERT コーディネーションセンター製品開発者リスト登録規約
https://www.jpcert.or.jp/vh/agreement.pdf



[図 2-4 累計製品開発者登録数]

2.3. 脆弱性の低減方策の研究・開発および普及啓発セキュアコーディングに関する講演活動

情報流通対策グループの脆弱性解析チームでは、脆弱なソフトウエアの解析等を通じて得られた、脆弱性やその対策方法に関する知見を、広く一般のソフトウエア開発者の方々に伝えるための活動を行っています。
本四半期は、次の 1 件の講演を行いました。

PHP/Java/Android Secure Coding Seminar
タイの首都バンコクにて 7 月 15 日からの 3 日間で、ThaiCERT 主催によるセキュアコーディングセミナが開催され、JPCERT/CC の久保正樹と戸田洋三が講師を努めました。このセミナは、1 日目 PHP、2 日目 Java、3 日目 Android という構成で各言語環境におけるセキュアコーディングを学ぶもので、1 日目の PHP は ThaiCERT のスタッフ、2 日目の Java は戸田、3 日目の Android は久保がそれぞれ講義を担当しました。

[図 2-5　Java セミナの様子]

[図 2-6 Android セミナの様子]

Java、Android ともに約 40 名が参加し、各 1 日コースのレクチャおよびハンズオンに熱心に取り組んでいただきました。

2.3.2. ハイブリッドアプリケーションフレームワーク「Apache Cordova」の脆弱性に関する調査報告書

HTML5 や Javascript といったウェブ関連技術を使用してアプリケーションを開発する、ハイブリッドアプリケーションフレームワーク Apache Cordova を利用したアプリケーション開発の際に作りこまれ得る脆弱性に関して調査した結果をまとめた報告資料を、GitHub のリポジトリの形で公開しました。

「Apache Cordova」を使ったハイブリッドアプリケーションの脆弱性に関する調査報告書
https://github.com/JPCERTCC/cordova/

また、この調査から得られた知見を論文にまとめ、第 14 回情報科学技術フォーラム(FIT2015)にて発表しました。

RL-003: ハイブリッドアプリケーションの脆弱性に関する分析
https://www.ipsj.or.jp/event/fit/fit2015/FIT2015_web_program/data/html/abstract/RL-003.html

2.3.3. 日本シーサート協議会　シーサート課題検討 SWG 主催の PGP 講習会に講師を派遣

日本シーサート協議会 (NCA: Nippon CSIRT Association) のシーサート課題検討 SWG では、9 月 15 日(火)に PGP 講習会を開催しました。脆弱性解析チームの戸田洋三が、この講習会の講師を務めました。この講習会は、新たにシーサートの活動に関わるスタッフを対象とし、PGP ツールの役割や初歩的な使い方についてハンズオンを交えて学ぶことを目的としています。

2.3.4. CERT コーディングスタンダードのルールを更新中

JPCERT/CC では､CMU/SEI のセキュアコーディングプロジェクトが提供する CERT C Coding Standard および CERT Oracle Coding Standard for Java を邦訳して提供しています。これは C 言語や Java 言語におけるセキュアコーディングを実践するためのルール集で、その内容は日々更新されています。
本四半期に邦訳を更新したルールは次のとおりです。

内容の更新(1 件)

- IDS00-J. SQL インジェクションを防ぐ

2.3.5. セキュアコーディング出張セミナ

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(有償)の実施を承っています。本四半期は、国内メーカー1 社に対して、C/C++および Java アプリ開発におけるセキュアコーディングセミナを実施しました。

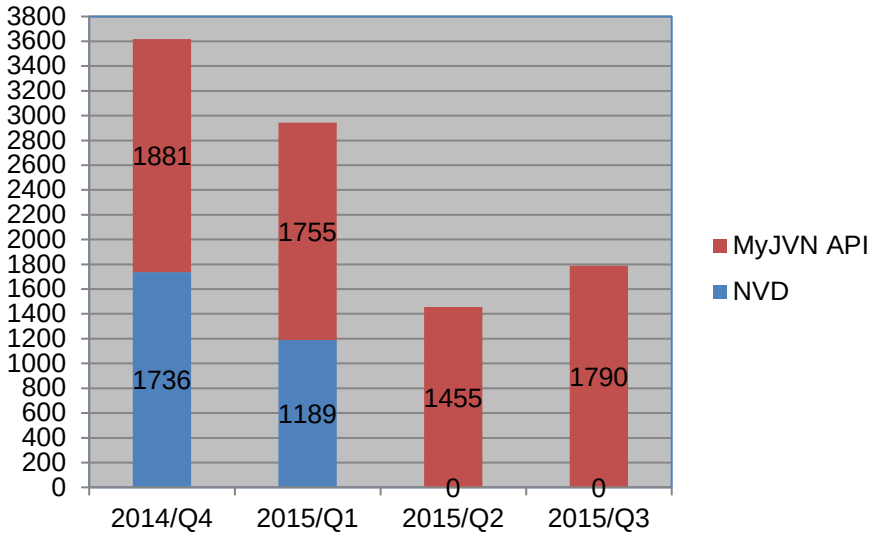
※出張セミナのご依頼、お問い合わせは、secure-coding@jpcert.or.jp までご連絡ください。

2.4. VRDA フィードによる脆弱性情報の配信

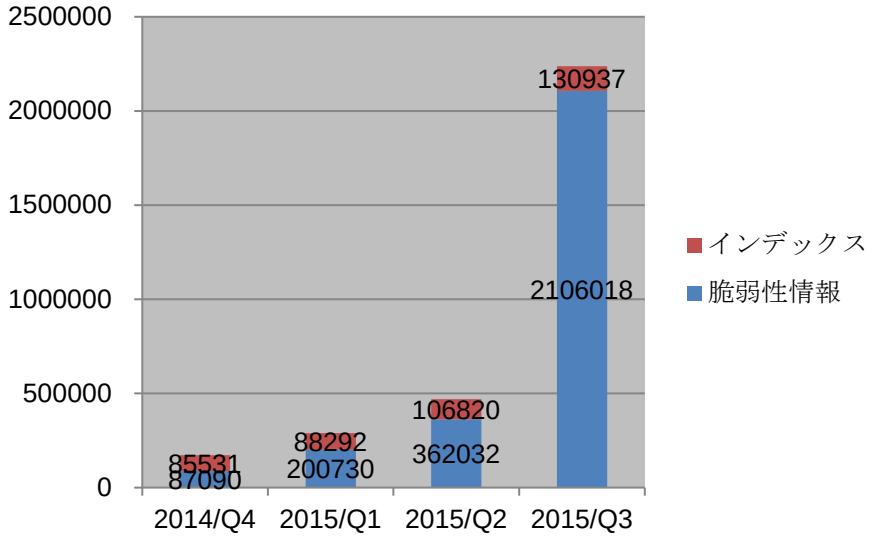
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST(National Institute of Standards and Technology)の NVD(National Vulnerability Database)を外部データソースとして利用した、VRDA(Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページをご参照ください。

VRDA フィード 脆弱性脅威分析用情報の定型データ配信

四半期ごとに配信した VRDA フィード配信件数のデータソース別の内訳を[図 2-7]に、VRDA フィードの利用傾向を[図 2-8]と[図 2-9]に示します。[図 2-8]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 2-9]では、HTML と XML の 2 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。
なお、NVD から得られる脆弱性情報は、IPA が運用する MyJVN API からも取得可能であるため、本四半期からは、MyJVN API のみを VRDA フィードのデータソースとして配信することになりました。



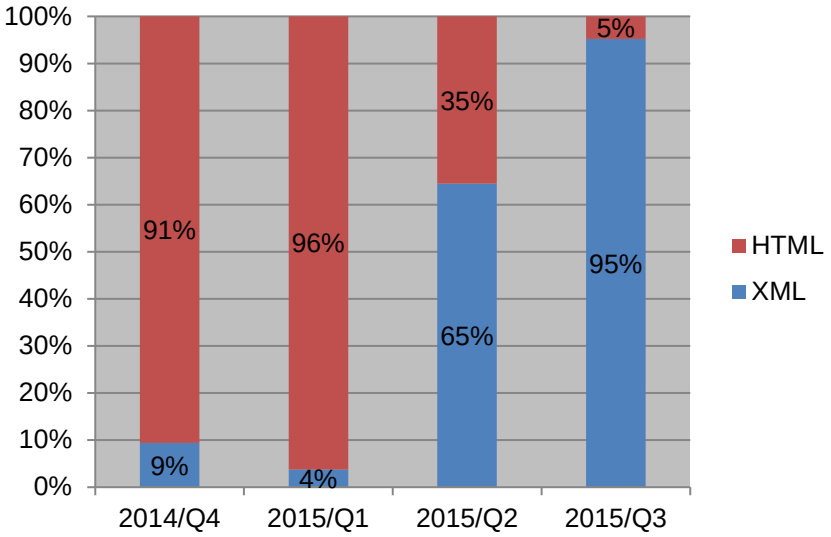
[図 2-7 VRDA フィード配信件数]



[図 2-8 VRDA フィード利用件数]

[図 2-8] に示したように、インデックスの利用数については、前四半期と比較し、大きな変化は見られ

ませんでした。一方、脆弱性情報の利用数については、前四半期と比較し、約 5.8 倍に増加しました。



[図 2-9 脆弱性情報のデータ形式別利用割合]

[図 2-9] に示したように、本四半期の脆弱性情報のデータ形式別利用傾向については、XML 形式の利用割合が 9 割以上となりました。

3. 制御システムセキュリティ強化に向けた活動

3.1 情報収集分析

JPCERT/CC では、制御システムにおけるセキュリティインシデントに関わる事例や標準化活動の動向、その他セキュリティ技術動向に関するニュースや情報等を収集・分析し、必要に応じて国内組織等に情報提供を行っています。本四半期の情報収集分析活動の中で収集し分析した情報は 419 件でした。このうち、国内の制御システム関係者に影響があり、注目しておくべき事案を「参考情報」として、制御システムセキュリティ情報共有コミュニティ(注 1)に提供しました。

(注 1) JPCERT/CC が運営するコミュニティで、制御システム関係者を中心に構成されています。

本四半期に提供した参考情報は次の 2 件でした。

発行件数：2 件

2015-07-14 [参考情報] Cisco 社製セキュリティアプライアンスソフトウェアの脆弱性に関する注意喚起

2015-08-10 [参考情報]Switches Get Stitches(Black Hat 2015)について

また、海外での事例や、標準化動向などは JPCERT/CC からのお知らせとともに、制御システム関係者向けに月刊ニュースレターとして配信しています。本四半期は計 3 件を配信しました。

発行件数：3 件

2015-07-06　制御システムセキュリティニュースレター 2015-0006
2015-08-07　制御システムセキュリティニュースレター 2015-0007
2015-09-04　制御システムセキュリティニュースレター 2015-0008

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 490 名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 Web ページをご参照ください。

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

3.2 制御システム関連のインシデント対応

本四半期における制御システムに関連するインシデントの報告件数は 0 件でした。
また、SHODAN をはじめとするインターネット・ノード検索システムにおいて制御システム機器や関連プロトコルに対応した機能拡張が進み、攻撃されるリスクが高まっていることへの対策として、「インターネット・ノード検索システム」等のインターネット上の公開情報を分析し、国内の制御システム等で外部から悪用される危険性のあるシステムの保有組織に対して情報を提供しました。こうした危険性のあるシステムに関する本四半期の情報提供件数は、4 件でした。
本対応の過程において、管理画面に認証がかかっておらず、外部から悪用される危険性のある複合機が多数検出されたことから、同複合機の保有組織に対して情報を提供しました。こうした危険性のある複合機に関する本四半期の情報提供数は 40 件でした。

3.3 関連団体との連携

SICE(計測自動制御学会)と JEITA(電子情報技術産業協会)、JEMIMA(日本電気計測器工業会)が定期的に開催している合同セキュリティ検討 WG(ワーキンググループ)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。

3.4 制御システム向けセキュリティ自己評価ツールの配付情報

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を目的として、簡便なセキュリティ自己評価ツールである日本版 SSAT(SCADA Self Assessment Tool)や J-CLICS(制御システムセキュリティ自己評価ツール)の配付を行っています。本四半期は、日本版 SSAT に関して 6 件、J-CLICS に関して 14 件の利用申込みがありました。直接配付件数の累計は、日本版 SSAT が 178 件、J-CLICS が 252 件となりました。

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

4.1.1. MNSEC 2015 への参加 (9 月 29 日-30 日)

モンゴルの CSIRT 構築支援の一環として、MNCERT/CC（モンゴルサイバー緊急対応チームコーディネーションセンター）が 9 月 29 日から 30 日にウランバートルで開催した MNSEC 2015 に参加し、講演を行いました。29 日は JPCERT/CC の活動、早期警戒の取組みや日本における最新のインシデント動向について紹介し、30 日は脆弱性を悪用した攻撃の解析手法等について講演しました。参加者は、モンゴル国内の政府関係者、民間企業、通信事業者、金融機関、学術系組織等から約 200 名が集い、モンゴル国内におけるインシデント動向や課題に関して活発な意見交換を行いました。また、主催者の MNCERT/CC と個別の打合せを行い、今後も一層の連携強化を図ることを確認しました。

4.2 国際 CSIRT 間連携

インシデント対応に関する海外の National CSIRT との連携強化、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の取組みの実施状況等に関する情報収集を目的として、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等、多国間の CSIRT との連携の枠組みにも積極的に参画しています。

4.2.1 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(運営委員)のメンバに選出されており、事務局も担当しています。2011 年 3 月からは、議長チーム(現在 4 期目)としてさまざまな活動をリードしています。JPCERT/CC の APCERT における役割および APCERT の詳細については、次の Web ページをご参照ください。

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

4.2.1.1. APCERT Steering Committee 会議の実施

Steering Committee では 7 月 29 日、8 月 19 日に電話会議を行い、今後の APCERT の運営方針等につい

て議論しました。JPCERT/CC は議長チームおよび事務局として、これらの会議を主導およびサポートしました。

4.2.1.2. APCERT オンライントレーニングの実施 (6 月 3 日)

APCERT では APCERT 加盟組織向けのオンライントレーニングを実施しています。6 月 3 日に実施されたトレーニングでは JPCERT/CC が講師を務め「脆弱性情報ハンドリング―ハンドリングの流れと脆弱性情報の活用方法 (Vulnerability Handling – What goes on and how to use information that comes out of it)」と題して、脆弱性情報の収集方法、ハンドリング事例、脆弱性情報データベース等について説明しました。

4.2.1.3. APCERT 年次総会 2015 への参加 (9 月 6 日-10 日)

アジア太平洋地域の CSIRT コミュニティである APCERT の年次総会がマレーシアのクアラルンプールで開催され、APCERT の主要メンバであるオペレーショナルメンバ（全 28 チーム）から JPCERT/CC を含む 26 チームが参加しました。 APCERT 年次総会は、各経済地域における最近のインターネットセキュリティ動向、インシデント対応の事例、調査・研究活動等を共有することを目的に、毎年開催されています。今回は”Bridging the World – Go Cyber Green”をテーマに掲げました。また、本年次総会は、イスラム諸国のコンピュータ緊急対応チームである OIC-CERT (The Organization of the Islamic Cooperation – Computer Emergency Response Team) の年次総会と初めて同時開催されました。概要は次のとおりです。

1) 日程：
   9/6(日) 午前：サイバーグリーンを含む各種ワークショップ
   午後：APCERT ワーキンググループ会合
   9/7(月) 午前：APCERT 運営委員会 (SC Meeting)
   午後：APCERT 年次総会 (Annual General Conference)
   9/8(火) 午前：TSUBAME ワークショップ
   午後：APCERT、OIC-CERT 合同机上演習
   9/9(水) 午前：APCERT カンファレンス (Closed Session)
   午後：APCERT、OIC-CERT 合同運営委員会
   9/10(木) 終日：APCERT、OIC-CERT カンファレンス (Open Session)
2) 場所：The Royale Chulan, Kuala Lumpur, Malaysia
3) 主な決定事項等：

APCERT が目指す”safe, clean and reliable cyber space”のビジョンの実現に向けて、アジア太平洋地域の枠を越え、OIC-CERT の加盟チームともサイバーグリーンや TSUBAME 等のプロジェクトを通して連携を強化していくことがチーム間で合意されました。

APCERT カンファレンスにおいては、インシデントや脆弱性への対応事例、サイバー脅威動向、IoT、クラウドセキュリティ、モバイルセキュリティ、サイバーリスクに関する比較可能で堅牢な定量評価の仕組み等に関する講演が行われました。

APCERT 運営委員会では、来年度の APCERT 年次総会の開催について協議され、JPCERT/CC がホストチームに選出されました。

また、APCERT 年次総会では、APCERT 議長チームおよび副議長チームの改選が行われました。JPCERT/CC は 4 期 (4 年) 連続して務めた議長チームの任期を満了し、CERT Australia が新たな議長チームとして選出されました。また、運営委員会 (Steering Committee) および事務局の改選も行われ、JPCERT/CC は引き続き運営委員会および事務局に再選されました。JPCERT/CC は、引き続き APCERT の主要メンバとして様々な活動をリードして参ります。

[図 4-1 APCERT 年次総会集合写真]

APCERT 年次総会についての詳細は、次の Web ページをご参照ください。

APCERT and OIC-CERT AGM & Annual Conference 2015
http://csm-ace.my/apcert-oiccert2015/

4.2.1.4. サイバーグリーンワークショップの開催 (9 月 6 日)

「サイバーグリーン」は、インターネット全体の健全性とリスクを各国／地域間で比較可能にする評価指標を打ち立て、その指標を用いてより効率的に健全なサイバー空間を実現することを目的とした、

JPCERT/CC が主導する取組みです。APCERT 年次総会の会期中に本プロジェクトのワークショップを開催し、APCERT や OIC-CERT の加盟チームを含む約 100 名が参加しました。ワークショップでは、サイバーグリーンにおける評価指標の概念や詳細、蓄積したデータの活用方法等について紹介し、評価指標のさらなる改善に向けた意見交換を行いました。

なお、APCERT は、サイバーグリーンのワーキンググループを新たに立ち上げて、アジア太平洋地域におけるサイバー空間の健全性向上に向けた取組みを進めることを今回の年次総会で決定するとともに、この分野でも OIC-CERT と連携していく方針を確認しました。JPCERT/CC は、このプロジェクトの提案組織として、ワーキンググループの活動を全面的に支えて参ります。サイバーグリーンについての詳細は、次の Web ページをご参照ください。

実証実験：サイバーグリーンプロジェクト(Cyber Green Project)
https://www.jpcert.or.jp/research/cybergreen.html

4.2.1.5. TSUBAME WORKSHOP 2015 の開催 (9 月 8 日)

JPCERT/CC が主導する「TSUBAME プロジェクト」は、APCERT の中ではワーキンググループの一つとして位置づけられた活動です。JPCERT/CC は APCERT 年次総会の会期中に本プロジェクトのワークショップを開催しました。TSUBAME WORKSHOP 2015 の詳細については、本活動概要の次の項目をご参照ください。

1.3.3 TSUBAME WORKSHOP 2015 の開催（2015 年 9 月 8 日）

4.3 FIRST (Forum of Incident Response and Security Teams)

JPCERT/CC は 1998 年の FIRST 加盟以来、積極的に活動に参加しています。現在は JPCERT/CC の国際部シニアアナリスト 小宮山功一朗が FIRST の Board of Directors のメンバを務めており、8 月 31 日から 9 月 2 日にアイルランドのダブリンにて開催された Board of Directors 会合に出席しました。FIRST および Board of Directors の詳細については、次の Web ページをご参照ください。

FIRST
http://www.first.org/

FIRST.Org,Inc., Board of Directors
http://www.first.org/about/organization/directors

4.3.1. FIRST Accra Regional Symposium への参加 (9 月 28 日-10 月 1 日)

9 月 28 日から 10 月 1 日にガーナの首都アクラで開催された FIRST Accra Regional Symposium において、FIRST の Board of Directors のメンバとして同機関の活動に貢献している JPCERT/CC の国際部シニアアナリスト 小宮山功一朗が、JPCERT/CC が推進している国際的に比較可能なサイバーセキュリティ評価指標の策定に関する「サイバーグリーン」の取組みについて多数の参加者に紹介しました。
また、9 月 28 日と 29 日はシンポジウムの参加者に向けて 2 日間の CSIRT トレーニングを行い、アフリカの CSIRT 構築支援活動に貢献しました。FIRST Accra Regional Symposium およびサイバーグリーンについての詳細は、次の Web ページをご参照ください。

Accra Regional Symposium
https://www.first.org/events/symposium/accra2015

実証実験：サイバーグリーンプロジェクト(Cyber Green Project)
https://www.jpcert.or.jp/research/cybergreen.html

4.4 第三回 日中韓 サイバーセキュリティインシデント対応年次会合 (8 月 24 日-25 日)

2011 年 12 月に日中韓の各 National CSIRT (JPCERT/CC、CNCERT/CC、KrCERT/CC) が締結した覚書 (MOU) で定められている、三者による「日中韓 サイバーセキュリティインシデント対応年次会合」が 8 月 24 日、25 日に東京で開催されました。本年次会合は、一昨年の上海での第一回会合、昨年のソウルでの第二回会合に続くものです。
本会合では、日中韓三ヵ国に影響を及ぼす重大なサイバーセキュリティインシデント対応における連携について、前会合以降における実績を評価項目に従ってレビューし、適切なインシデント対応が行われたことを確認しました。また、最近のインシデント動向や対応等に関する技術的な情報交換を行いました。
三者はこれまでに培った連携関係をさらに強化すべく、重大なインシデントに関する事後の評価を引き続き行うとともに、それぞれの組織のインシデント対応等に係るキャパシティについて情報共有を深めること、年次会合以外でも機会を捉えてインシデント動向や対応に関する情報交換を図ること、また、マルウエアのクリーンアップを含む国際サイバー空間の健全性向上に貢献すべく、各種インディケータ情報や、比較可能なサイバーリスクの計測情報およびサイバーリスクへの対応活動の共有を促進していくことを合意しました。

4.5 CGI.br 20 周年カンファレンスへの参加 (9 月 17 日-18 日)

CGI.br (Comitê Gestor da Internet no Brasil、英語名：The Brazilian Internet Steering Committee) は、ブラジル国内のインターネットサービス関係者を取りまとめる、今年で創立 20 周年を迎える団体です。その一連の記念カンファレンスの一環として、9 月 17 日から 18 日に開催された 4th Brazilian CSIRTs Forum で JPCERT/CC は基調講演を行いました。講演では、継続性、耐久性のあるセキュリティ対策の基盤とし

て、インターネットエコシステムの健全性向上の取組みの重要性について訴えるとともに、サイバーグリーンの取組みについて紹介し、プロジェクトへの参加を呼びかけました。CGI.br 20 周年カンファレンスおよびサイバーグリーンについての詳細は、次の Web ページをご参照ください。

CGI.br 20 周年カンファレンス
http://cgi.br/20anos/en/

実証実験：サイバーグリーンプロジェクト(Cyber Green Project)
https://www.jpcert.or.jp/research/cybergreen.html

4.6 Code Bali 2015 国際サイバーセキュリティシンポジウムへの参加 (9 月 21 日-22 日)

9 月 21 日から 23 日にインドネシアのバリ島で開催された Code Bali 2015 国際サイバーセキュリティシンポジウムに参加し、JPCERT/CC は「サイバーグリーン」の取組みについて講演しました。講演では、おもにインドネシアの学術機関や IT 関連組織に向けてサイバーグリーンの必要性を訴えるとともに、評価指標や活用方法へのフィードバックを呼びかけました。また、インドネシアの CSIRT である ID-SIRTII/CC やインドネシアにおける TSUBAME プロジェクト参加メンバと意見交換を行い、Cyber Green を通したサイバー空間のクリーンアップ活動への協力を依頼しました。
Code Bali 2015 国際サイバーセキュリティシンポジウムおよびサイバーグリーンについての詳細は、次の Web ページをご参照ください。

CODEBALI
http://www.codebali.net/

実証実験：サイバーグリーンプロジェクト(Cyber Green Project)
https://www.jpcert.or.jp/research/cybergreen.html

4.7 その他の活動ブログや Twitter を通した情報発信

英語ブログ(http://blog.jpcert.or.jp/)や Twitter(@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英文による情報発信を行っています。本四半期は次の記事をブログに掲載しました。

Protected Mode in Internet Explorer (7 月 1 日)
http://blog.jpcert.or.jp/2015/07/protected-mode-in-internet-explorer.html

The 27th FIRST Annual Conference in Berlin (7 月 10 日)
http://blog.jpcert.or.jp/2015/07/the-27th-first-annual-conference-in-berlin.html

PoisonIvy adapts to communicate through Authentication Proxies (7 月 23 日)
http://blog.jpcert.or.jp/2015/07/poisonivy-adapts-to-communicate-through-authentication-proxies.html

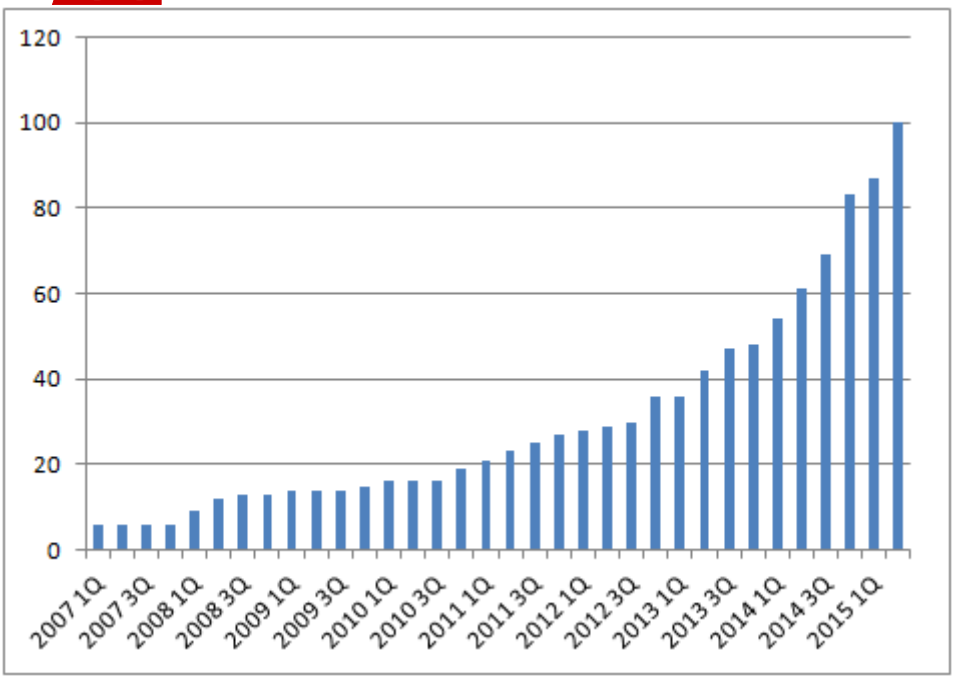
Enhanced Protected Mode in Internet Explorer (8 月 28 日)
http://blog.jpcert.or.jp/2015/08/enhanced-protected-mode-in-internet-explorer.html

VPN Servers Altered by Attacker Leading to Scanbox, a Reconnaissance Framework (9 月 30 日)
http://blog.jpcert.or.jp/2015/09/vpn-servers-altered-by-attacker-leading-to-scanbox-a-reconnaissance-framework.html

5. 日本シーサート協議会(NCA)事務局運営

日本シーサート協議会(NCA：Nippon CSIRT Association)は、国内のシーサート(CSIRT：Computer Security Incident Response Team)組織が互いに協調し、連携して共通の問題を解決する場として設立されました。その事務局として、JPCERT/CC は、NCA の Web サイトの管理や更新を通じた広報活動、協議会の問合せ窓口やメーリングリストを含む会員情報の管理、加盟のためのガイダンスの実施および手続きの運用を担当するとともに、自らも会員として協議会の活動に参加しています。

本四半期においては、株式会社ブロードバンドセキュリティ (B2SIRT)、グローバルセキュリティエキスパート株式会社 (GSX-CSIRT)、AGS 株式会社 (AGS-CSIRT)、さくらインターネット株式会社 (SAKURA.CSIRT)、ソニー生命保険株式会社 (SL-CSIRT)、株式会社ケイ・オプティコム (K-OPT CSIRT)、株式会社 ＮＴＴドコモ (DOCOMO-CSIRT)、スカパーＪＳＡＴ株式会社 (SJ-CSIRT)、株式会社東芝 (TOSHIBA-CSIRT)、住友セメントシステム開発株式会社 (SUMITEM-CSIRT)、NTT コミュニケーションズ株式会社 (NTT Com-SIRT)、オリンパス株式会社 (OLYMPUS-CIRT)、トッパン・フォームズ株式会社 (TF-CIRT)、株式会社バンダイナムコエンターテインメント (BNESIRT)、株式会社大和総研ホールディングス (DIR-CSIRT)の 13 組織が新規に加盟しました。本四半期末時点で 100 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 5-1]のとおりです。



[図 5-1　日本シーサート協議会 加盟組織数の推移]

8 月に「第 10 回総会&第 16 回ワーキンググループ会」を開催いたしました。

2015 年 8 月 28 日 (金) 14:00-17:30
会場：大成建設株式会社 52 階
参加人数：163 名

大成建設株式会社にて第 10 回総会を執り行い、運営規約の改定や運営委員の選挙を行いました。また第 16 回ワーキンググループ会が併催され、新しく加盟した 6 チームが自組織のシーサートチームの紹介を、加盟組織が「事例から学ぶ標的型攻撃～他社から学ぶいますぐできる対策～」について講演を行いました。

本四半期末現在ついに 100 組織が加盟いたしました。引き続き各ワーキンググループでも登録者が増え、活発な活動が行われることになりそうです。また、今後の課題として、会員数の増加に伴って増加する事務局業務の効率化を検討する必要があります。

日本シーサート協議会の活動の詳細については、次の Web ページをご参照ください。

日本シーサート協議会
http://www.nca.gr.jp/

6. フィッシング対策協議会事務局の運営

JPCERT/CC は、フィッシング対策協議会(以下「協議会」といいます。)の事務局を担当しており、経済産業省からの委託により、協議会における各ワーキンググループ活動の運営や、協議会名での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、報告に基づいたフィッシングサイトに関する注意喚起等の活動を行っています。

6.1 情報収集/発信の実績

本四半期は、協議会 Web サイトや会員向けメーリングリストを通じて、フィッシングに関するニュースや緊急情報を 18 件発信しました。

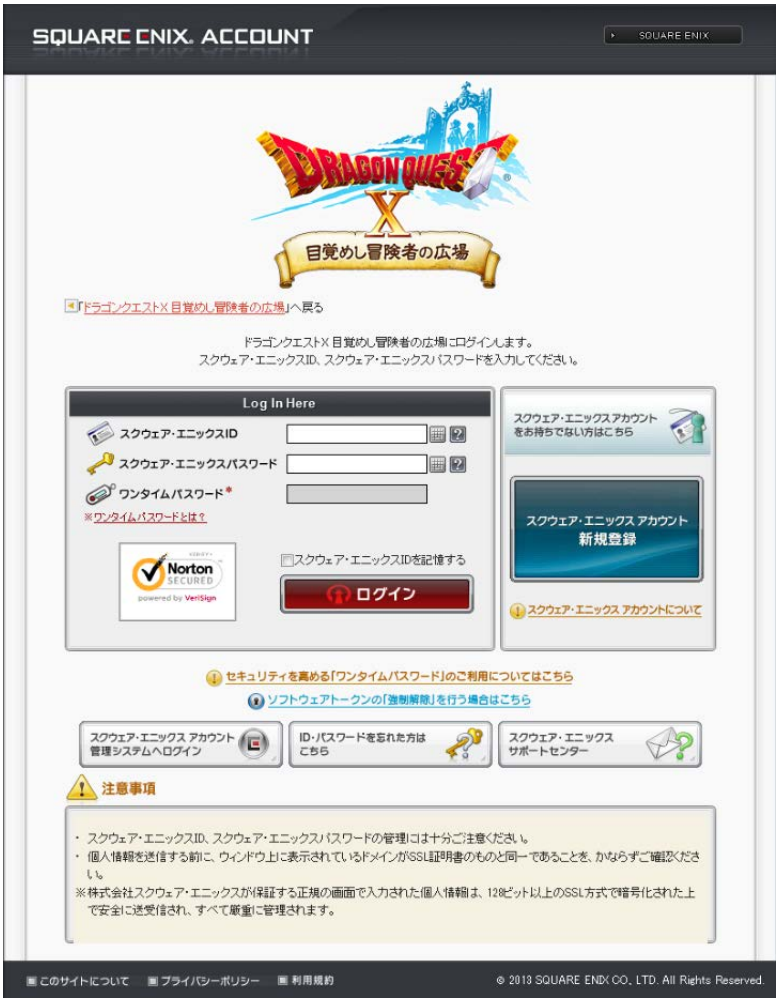
2015 年 5 月に確認され始めた、銀行のフィッシングサイトへの SMS (ショートメッセージサービス) を使った誘導が、本四半期に入ってからも引き続き確認されました。以前からあったオンラインゲームをかたるフィッシングは、本四半期においても継続的に多数報告されました。金融機関や通信事業者をかたる新たなフィッシングのサイトの報告も寄せられました。協議会では、名前をかたられた各事業者に、メール本文やサイトの URL 等の関連情報を提供しました。

また、金融機関をかたるフィッシングに関しては SMS (ショートメッセージサービス) を使った銀行のフィッシングサイトとして[図 6-1]の「ジャパンネット銀行をかたるフィッシング(2015/07/06)」を含む 2 件、オンラインゲームをかたるフィッシングに関しては [図 6-2]の「[更新] スクウェア・エニックス（ドラゴンクエスト X）をかたるフィッシング（2015/07/09）」をかたるフィッシングの 1 件、通信事業者をかたるフィッシングに関して [図 6-3]の「OCN をかたるフィッシング (2015/07/17)」の 1 件、その他 5 件の合計 9 件の緊急情報を協議会の Web 上で公開し、広く注意を喚起しました。

ジャパンネット銀行をかたるフィッシングサイト

[図 6-1] ジャパンネット銀行をかたるフィッシング(2015/07/06)
https://www.antiphishing.jp/news/alert/jnb20150706.html

さらに、これら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、JPCERT/CC のインシデント対応支援活動を通じて行い、すべてについて停止を確認しました。



[図 6-2] [更新] スクウェア・エニックス（ドラゴンクエスト X）をかたるフィッシング（2015/07/09）

[図 6-3] OCN をかたるフィッシング (2015/07/17)
https://www.antiphishing.jp/news/alert/ocn20150717.html

6.2 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、毎月の活動報告等を公開しています。詳細については、次の Web ページをご参照ください。

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 2015 年 7 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201507.html
フィッシング対策協議会 2015 年 8 月 フィッシング報告状況

https://www.antiphishing.jp/report/monthly/201508.html
フィッシング対策協議会 2015 年 9 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201509.html

7. フィッシング対策協議会の会員組織向け活動

フィッシング対策協議会では、経済産業省から委託された活動以外に、会費による会員組織向けの活動を、運営委員会の決定に基づいて行っています。

7.1 運営委員会開催

本四半期においては、フィッシング対策協議会の活動の企画・運営方針の決定等を行う運営委員会を次のとおり開催しました。

フィッシング対策協議会 第 28 回運営委員会
日時：2015 年 7 月 17 日 16:00 - 18:00
場所：NTT コミュニケーションズ株式会社

フィッシング対策協議会 第 29 回運営委員会
日時：2015 年 8 月 14 日 16:00 - 18:00
場所：トレンドマイクロ株式会社

フィッシング対策協議会 第 30 回運営委員会
日時：2015 年 9 月 11 日 16:00 - 18:00
場所：日立システムズ株式会社

7.2 フィッシング対策ガイドライン実践セミナ 2015 開催

フィッシング対策ガイドライン実践セミナ開催を次のとおり開催しました。

フィッシング対策ガイドライン実践セミナ 2015
日時：2015 年 8 月 19 日 14:00 - 17:00
場所：日立システムズ　ソリューションスクエア東京

7.3 フィッシング対策ガイドラインの改訂について

平成 26 年に公表したフィッシング対策ガイドラインについて、読みやすさの向上、脅威の現状や新しい対策技術の反映等を目的として、昨年度、フィッシング対策協議会内に 「ガイドライン策定ワーキング

グループ」 を設置し、フィッシング対策ガイドラインを改訂いたしました。

フィッシング対策ガイドライン
https://www.antiphishing.jp/report/pdf/antiphishing_guide.pdf

7.4 フィッシングレポート 2015 の掲載 ～ 進む対策、利用者としてできること ～

2015 年度のフィッシング対策協議会のガイドライン策定ワーキンググループにおいて、フィッシングの被害状況、フィッシングの攻撃サイドの技術・手法などをとりまとめたフィッシングレポートを公開しました。

フィッシングレポート 2015
https://www.antiphishing.jp/report/pdf/phishing_report_2015.pdf

8. 公開資料

JPCERT/CC が本四半期に公開した調査・研究の報告書や論文、セミナ資料は次のとおりです。

8.1 脆弱性関連情報に関する活動報告レポート

IPA と JPCERT/CC は、ソフトウエア等脆弱性関連情報取扱基準（平成 26 年改正：平成 26 年経済産業省告示 第 110 号）に基づき、2004 年 7 月からそれぞれ受付機関および調整機関として脆弱性関連情報流通制度の一端を担っています。
本レポートは、2015 年 4 月 1 日から 2015 年 6 月 30 日までの活動実績と、本四半期に届出ないし公表された脆弱性に関する注目すべき動向についてまとめたものです。

ソフトウェア等の脆弱性関連情報に関する活動報告レポート[2015 年第 2 四半期(4 月～6 月)]
(2015 年 07 月 23 日)
https://www.jpcert.or.jp/press/2015/vulnREPORT_2015q2.pdf

8.2 インターネット定点観測レポート

JPCERT/CC では、インターネット上に複数のセンサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集するインターネット定点観測システム「TSUBAME」を構築・運用をしています。収集したデータを、脆弱性情報、マルウエアや攻撃ツールの情報などを参考に分析することで、攻撃活動やその準備活動の捕捉に努めています。
本レポートは、インターネット定点観測の結果を四半期ごとにまとめたものです。

インターネット定点観測レポート 2015 年 4 月～6 月
(2015 年 07 月 29 日)
https://www.jpcert.or.jp/tsubame/report/report201504-06.html

8.3 分析センターだより

JPCERT/CC では、インシデントに関連して報告いただいた情報や収集した情報を調査し、インシデントをもたらした攻撃の手法やその影響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。分析技術の普及や技術者の育成にも努めており、その一環として日々のアーティファクト分析業務の中で感じたこと、発見したことを「分析センターだより」として発信しています。本四半期においては次の 4 件の記事を公開しました。

(1)認証プロキシに対応した PoisonIvy(2015-07-31)
最近の複数の攻撃事例において確認した、マルウエア PoisonIvy における通信機能の拡張について紹介しました。

認証プロキシに対応した PoisonIvy(2015-07-31)
https://www.jpcert.or.jp/magazine/acreport-poisonivy.html

(2) Internet Explorer の拡張保護モード(2015-08-07)
Internet Explorer10、11 で実現されている、保護モードをさらに強化した拡張保護モード(Enhanced Protected Mode)によるマルウエア被害の防止効果について紹介しました。

Internet Explorer の拡張保護モード(2015-08-07)
https://www.jpcert.or.jp/magazine/acreport-ie2.html

(3) 改ざんされた VPN サーバから攻撃ツール Scanbox に誘導(2015-08-20)
2015 年 5 月頃発生を確認した、VPN サーバを改ざんしたうえで Scanbox と呼ばれる攻撃ツールに誘導し、アクセスした端末の情報を収集しようとする攻撃について紹介しました。

改ざんされた VPN サーバから攻撃ツール Scanbox に誘導(2015-08-20)
https://www.jpcert.or.jp/magazine/acreport-scanbox.html

(4) セキュリティ・キャンプ全国大会 2015 でのマルウエア分析講義(2015-09-10)
学生を対象としたセキュリティ・キャンプ全国大会 2015 におけるマルウエア分析の講義内容について紹介しました。

セキュリティ・キャンプ全国大会 2015 でのマルウエア分析講義(2015-09-10)
https://www.jpcert.or.jp/magazine/acreport-seccamp.html

9. 主な講演活動一覧

(1) 久保 正樹(情報流通対策グループマネージャ), 戸田 洋三(情報流通対策グループ 脆弱性解析チーム リードアナリスト)

「Java Secure Coding」,「Android Secure Coding」

ThaiCERT PHP/Java/Android Secure Coding Seminar(タイ),2015 年 7 月 15 日～7 月 17 日

(2) 洞田 慎一(早期警戒グループ情報セキュリティアナリスト) :

「高度サイバー攻撃の現状とその対策」

福島県ネットワーク・セキュリティ連絡協議会総会,2015 年 7 月 17 日

(3) 村上 晃(経営企画室 兼 エンタープライズサポートグループ 部門長) :

「強い CSIRT 構築は経営目線で～インシデント対応だけではない CSIRT 構築の勘所～」

日経コンピュータ,日経コミュニケーション サイバー攻撃に屈しない企業の砦「強い CSIRT」構築・運用セミナ,2015 年 7 月 17 日

(4) 満永 拓邦(早期警戒グループ マネージャ) :

「標的型攻撃の脅威 実態を知り対策を考える」

ITpro、ITpro Active 標的型攻撃への対策 ―最新トレンドと事例を知り、攻めの IT 経営へ―

2015 年 8 月 4 日

(5) 中津留 勇(分析センター) :

「Understanding Malware」

セキュリティ・キャンプ全国大会 2015 マルウエア分析講義,2015 年 8 月 13～14 日

(6) 村上 晃(経営企画室 兼 エンタープライズサポートグループ 部門長) :

「CSIRT 構築の事例と勘所を知る～“百社百様”ひとつとして同じものはない～」

第 32 回 ITmedia エグゼクティブセミナ,2015 年 9 月 9 日

(7) 藤本 万里子(早期警戒グループ情報セキュリティアナリスト) :

「標的型攻撃などのサイバー攻撃への備えと対応」

2015 中小企業情報化促進セミナ,2015 年 9 月 14 日

(8) 山本 健太郎(エンタープライズサポート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・インシデントの傾向と JPCERT/CC の活動」

日本金融監査協会 特別企画セミナ サイバー・セキュリティと IT ガバナンス,2015 年 9 月 15 日

(9) 戸田 洋三(情報流通対策グループ 脆弱性解析チーム リードアナリスト)

「PGP 初級編」

日本シーサート協議会 シーサート課題検討 SWG, 2015 年 9 月 15 日

(10) 満永 拓邦(早期警戒グループ マネージャ) :

「新たな脅威 実態を知り対策を考える」

日経 BP 情報セキュリティ Summit 2015,2015 年 9 月 17 日

10. 主な執筆一覧

(1)満永 拓邦(早期警戒グループ マネージャ)：
「STOP!パスワード使い回し! - パスワードリスト攻撃をご存じですか？」
マイナビニュース,2015 年 08 月 11 日
(2)中谷 昌幸(制御システムセキュリティ対策グループ マネージャ)：
「産業用制御システムのセキュリティについて」
東京海上日動リスクコンサルティング リスクマネジメント最前線,2015 年 09 月 07 日
(3)小林 裕士(インシデントレスポンスグループ情報セキュリティアナリスト)：
「STOP!パスワード使い回し! - 特集最終回、JPCERT が振り返る"対策法"」
マイナビニュース,2015 年 09 月 30 日

11. 協力、後援一覧

本四半期は、次の行事の開催に協力または後援をしました。

(1) Asia Pacific & Japan 2015
主　催：RSA Conference
開催日：2015年7月22日(水)～7月24日(金)
(2) S/MIME普及シンポジウム2015
主催：一般財団法人日本情報経済社会推進協会
開催日：2015年9月4日(金)
(3) 第11回IPAひろげよう情報モラル・セキュリティコンクール2015
主　催：独立行政法人情報処理推進機構(IPA)
募集期間：2015年4月1日(水)～9月7日(月)

12. JPCERT/CC 感謝状贈呈

JPCERT/CC では、サイバーセキュリティ対策活動に対する皆様からの御好意と御力添えに深く思いをいたし、特に顕著なご貢献をいただいた方を毎年選んで感謝状を贈呈する制度を設けています。
第 2 回となる本年は、サイバー攻撃による被害の抑止と IT 利用の安全性の確保に向けた、脆弱性情報を JVN 上で広くお知らせする活動にご協力をいただいたサイボウズ株式会社 Cy-SIRT 様と、制御システムセキュリティ分野における模範的な脆弱性対処の実践を通じて脆弱性情報ハンドリングのスキームの推進にご協力いただいた横河電機株式会社 YOKOGAWA PSIRT 様に対して、感謝状と記念の盾を 2015 年 8 月に贈呈致しました。

サイバーセキュリティ対策活動への協力者に感謝状贈呈
https://www.jpcert.or.jp/press/priz/2015/PR20150820-priz.html

■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
■制御システムに関するインシデントの対応依頼、情報のご提供
icsr-ir@jpcert.or.jp
https://www.jpcert.or.jp/ics/ics-form.html
PGP Fingerprint ： B3C2 A91C AE92 50A9 BBB2 24FF B313 E0E1 0DDE 98C1
■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 ：icsr@jpcert.or.jp
■セキュアコーディングセミナのお問い合わせ ：seminar-secure@jpcert.or.jp
■公開資料、講演依頼、資料使用、その他のお問い合わせ：pr@jpcert.or.jp