Japan Computer Emergency Response Team Coordination Center

JPCERT/CC®

JPCERT-PR-2014-04
発行日 : 2014-10-09

JPCERT/CC 活動概要 [2014 年 7 月 1 日 ～ 2014 年 9 月 30 日]

活動概要トピックス

ー トピック1ー　STOP!パスワード使い回し!キャンペーン

JPCERT/CC では、パスワードリスト攻撃による不正ログインの被害が後を絶たないことから、複数のサービスにおいて同じパスワードを使い回すリスクを認識してもらえるよう、独立行政法人情報処理推進機構(IPA)と共同で、インターネットサービス利用者に向けて「STOP!!パスワード使い回し!!パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ」を行いました。また、パスワードリスト攻撃による被害の軽減を図るためには、サービス提供事業者における対策の実施もさることながら、サービス利用者による適切なアカウント管理も必要となるため、ID とパスワードを用いてサービス利用者の認証を行っているサービス提供事業者などの協力を得て、サービス利用者へのパスワード使い回しを控えるように広く呼びかけるためのキャンペーンを開始しました。2014 年 10 月 9 日現在、本キャンペーンへの協力事業者は 20 社を超えています。

2014 年 8 月に IPA が発表した「オンライン本人認証方式の実態調査」報告書によると、利用者が金銭に関連したサービスサイト(インターネットバンキングやネットショッピングなど)と同一のパスワードを使い回している人の割合は約 4 分の 1(25.4%)となっており、パスワードを使い回している理由で最も多いのは「(パスワードを同一にしないと)パスワードを忘れてしまうから」で、64.1%を占めています。このような状況の下、JPCERT/CC においてパスワードリスト攻撃の被害にあった企業数を公表情報をもとにまとめたところ、2013 年から現在まで継続して攻撃被害が公表されています。オンラインサービスを安全に利用するためには、利用者においてもパスワードの使い回しのリスクを認識し、適切な管理を心掛ける必要があります。

オンラインサービス利用者を守るために、攻撃実態の把握やそれに基づく対策の実施、利用者への注意喚起といった活動が関連業界によって続けられていますが、JPCERT/CC も、サービス提供事業者や関係機関と連携し、パスワードの使い回しを避けるための適切な管理方法や、不正なログインに気付く、または防止するための機能の利用等の対策を公開し、被害の拡大防止に努めています。

STOP!! パスワード使い回し!!パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ
https://www.jpcert.or.jp/pr/2014/pr140004.html#1

「STOP!パスワード使い回し!」キャンペーンにご賛同いただける企業の募集
https://www.jpcert.or.jp/pr/2014/pr140005.html

ー トピック2ー　脆弱性を識別する CVE 番号の新体系による採番の公表

米国 MITRE 社が管理運営する脆弱性の識別子 CVE (Common Vulnerabilities and Exposures)番号の体系が、本年 1 月 1 日から年間 1 万件を超える脆弱性にも対応できるよう拡張され、数字 4 桁で不足する場合には漸次桁数を増やす方式が採用されることになりました。 CVE を参照している組織等において固定長の CVE 番号を前提とした機械処理をしている場合には、誤動作する可能性があるため、米国 MITRE 社は、2014 年 1 月 15 日、CVE の Web サイト上で新番号体系による運用を開始している旨の Notification を公表、7 月 15 日には、CVE 番号体系変更の Reminder Notification を公表しました。そして、2014 年 9 月 17 日、CNA をはじめとする CVE 利用者や脆弱性情報を参照するエンドユーザに対し、この CVE 番号の新体系を広く周知すべく、改めてプレスリリースを発行しました。これに合わせ、CNA(CVE Numbering Authority, CVE 採番機関)である JPCERT/CC からも本新体系による採番について公表しました。

脆弱性を識別する CVE 番号の新体系による採番のお知らせ
https://www.jpcert.or.jp/pr/2014/pr140006.html

米国 MITRE 社プレスリリース
Leading Software Vendors and Cybersecurity Organizations Among Early Adopters of MITRE's New Vulnerability Naming Format
https://www.mitre.org/news/press-releases/leading-software-vendors-and-cybersecurity-organizations-among-early-adopters-of

CVE 新番号体系対応組織・機関一覧
Declarations of CVE-ID Syntax Compliance(MITRE 社)
https://cve.mitre.org/cve/identifiers/compliant_organizations.html

ー トピック3ー　Android セキュアコーディングセミナーをインド Delhi と Bangalore で開催

JPCERT/CC は、CERT-IN(インドの national CERT)および Data Security Council of India (DSCI)と協力し、9 月 10 日にインドの首都デリー、12 日には IT 企業が集まる南部バンガロールにおいて、Android セキュアコーディングセミナーを実施しました。
日本企業のソフトウエア開発拠点の一つとなっているインドにおいて、現地のソフトウエア開発者を対象に Android セキュアコーディングに関するノウハウを提供することは、現地のセキュリティ啓発に資するのみならず、日本のソフトウエアセキュリティ向上にも資するものと期待しています。

セミナーは、Android アプリの脆弱性に関する「講義」と、講義内容について理解を深めるための「演習」からなる 1 日コースとして実施しました。現地の大手ソフトウェアベンダーや外資系 IT 企業、金融機関に所属する Android プログラマや開発マネージャ、セキュリティ研究者の方に参加いただき、終始レベルの高い活発な質疑が行われ、受講者の問題意識の高さを感じられました。

Android Secure Coding
http://www.slideshare.net/jpcert_securecoding/all-for-attendee

ートピック4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。現代社会は情報通信システムに大きく依存しており、インシデントへの対処がうまくいかなければ、深刻な社会問題が引き起こされたり、影響がグローバルに拡散したりする恐れもあります。

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、2014 年6 月に加藤 孝浩様(トッパン・フォームズ株式会社ICT 事業部Web ビジネス本部業務推進部長)、モルスナー ミヒャエル様(株式会社カスペルスキー情報セキュリティラボ 所長)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/2014/PR20140703-priz.html

本活動は、経済産業省より委託を受け、「平成２６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、「2.5.セキュアコーディング啓発活動」、「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」および「12.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 4638 件、インシデント件数ベースでは 4388 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 2125 件でした。前四半期の 2134 件と比較して 0.4%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/2014/IR_Report20141009.pdf

1.1.1. インシデントの傾向

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 417 件で、前四半期の 509 件から 18%減少しました。また、前年度同期(469 件)との比較では、11%の減少となりました。

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	99	26	14	139(33%)
国外ブランド	73	63	53	189(45%)
ブランド不明	49	16	24	89(21%)
月別合計	221	105	91	417(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。

国内金融機関を装ったフィッシングサイトは、発生時期にかたよりがあり、7 月と 9 月後半には、不正にファイルを設置されたと見られる海外のサイトから、国内通信事業者の IP アドレスが割り当てられたフィッシングサイトに誘導される例を多数確認しましたが、8 月から 9 月前半にかけては、わずかな報告があるのみでした。

7 月から 8 月にかけて、国内オンラインゲームサービスを装ったフィッシングサイトの報告が多く寄せられていましたが、9 月以降は報告が大幅に減少しました。

また、国内通信事業者の Web メールサービスを装ったフィッシングサイトの報告を複数受領しています。このようなフィッシングサイトは、Web メールの認証情報を窃取し、スパムメールやフィッシングメールを送信することを目的としていると考えられます。

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%であり、前四半期(国内 55%、国外 45%)に比べ、国内への調整が増加しています。

本四半期に報告が寄せられた Web サイト改ざんの件数は、968 件でした。前四半期の 1123 件から 14%減少しています。

8 月末ごろから、不正な JavaScript が埋め込まれた Web ページに関する報告が多く寄せられています。不正な JavaScript には、以前から確認されている改ざんと同様に、script タグに 6 桁の 16 進数を含むコメントタグがついているという特徴がありました。JavaScript から誘導される先の URL には複数のパターンがあるため、異なる種類の改ざんが複数発生している可能性が考えられます。最終的に誘導される先のサイトでは、PC のアプリケーションの脆弱性を攻撃されて、マルウエアのダウンロードおよび実行が行われることを確認しています。

JPCERT/CC では、Web サイト改ざんが継続的に発生している現状を受けて、8 月に注意喚起「ウェブサイトの改ざん回避のために早急な対策を」を発行しました。

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 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)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：10 件　https://www.jpcert.or.jp/at/

2014-07-09　2014 年 7 月 Microsoft セキュリティ情報 (緊急 2 件含) に関する注意喚起
2014-07-09　Adobe Flash Player の脆弱性 (APSB14-17) に関する注意喚起
2014-07-16　2014 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
2014-08-13　2014 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
2014-08-13　Adobe Flash Player の脆弱性 (APSB14-18) に関する注意喚起
2014-08-13　Adobe Reader および Acrobat の脆弱性 (APSB14-19) に関する注意喚起
2014-09-10　2014 年 9 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起
2014-09-10　Adobe Flash Player の脆弱性 (APSB14-21) に関する注意喚起
2014-09-17　Adobe Reader および Acrobat の脆弱性 (APSB14-20) に関する注意喚起
2014-09-25　GNU bash の脆弱性に関する注意喚起

なお、JPCERT/CC に月平均 400 件程度の Web サイト改ざんの報告が寄せられる状況に鑑み、Web サイト改ざんの危険性を広く知らせるため、IPA(独立行政法人情報処理推進機構)と共同で情報発信を行いました。Web サイト改ざんの代表的な手口として、「サーバソフトウエアに残存する脆弱性を狙った Web サイト改ざん」、「Web サイトの管理端末への侵入による Web サイト改ざん」などを取り上げ、それぞれの対策と共に紹介し、Web サイト運営者および管理者に対して点検と注意を呼びかけました。

1.2.1.2. その他

1.2.1.2.1. パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ

パスワードリスト攻撃による不正ログインの被害が後を絶たないことから、複数のサービスにおいて同じパスワードを使い回すリスクを認識してもらえるよう、独立行政法人情報処理推進機構（IPA）と共同で、インターネットサービス利用者に向けて「STOP!!パスワード使い回し!!パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ」を行いました。

STOP!! パスワード使い回し!!パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ
https://www.jpcert.or.jp/pr/2014/pr140004.html#1

1.2.1.2.2. 「STOP!パスワード使い回し!」キャンペーン

パスワードリスト攻撃による被害の軽減を図るためには、サービス提供事業者における対策の実施もさることながら、サービス利用者による適切なアカウント管理も必要となるため、JPCERT/CC は、ID とパスワードを用いてサービス利用者の認証を行っているサービス提供事業者などの協力を得て、サービス利用者へのパスワード使い回しを控えるように広く呼びかけるためのキャンペーンを開始しました。
キャンペーン期間は、2014 年 9 月 17 日から 11 月末までを予定しており、10 月 9 日現在、本キャンペーンへの協力事業者は 20 社を超えています。

「STOP!パスワード使い回し!」キャンペーンにご賛同いただける企業の募集
https://www.jpcert.or.jp/pr/2014/pr140005.html

1.2.1.3. 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 60 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。

2014-07-02　PHP のアップデートを確認しましょう
2014-07-09　DNS Summer Days 2014
2014-07-16　JNSA セキュリティ被害調査 WG 2012 年報告書公開
2014-07-24　フィッシング対策協議会の公開ドキュメント
2014-07-30　オープンリゾルバを悪用した攻撃活動について
2014-08-06　EMET 5.0 正式リリース
2014-08-13　POS システムを狙うマルウエア
2014-08-20　PHP 5.3 サポート終了
2014-08-27　SECCON 2014 開催
2014-09-03　IPA テクニカルウォッチ「ウェブサイト改ざんの脅威と対策」が公開
2014-09-10　Pre-loaded Public Key Pinning
2014-09-18　Public Key Pinning Extension for HTTP
2014-09-25　「STOP!パスワード使い回し!」キャンペーンにご賛同いただける企業の募集

1.2.1.4.　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内 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。

【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、攻撃に対する事前対策を促す早期警戒情報の提供を行いました。
2014 年 8 月中下旬および、2014 年 9 月上旬には、一部 Web サイトなどで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確認されず、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。一方、Web 改ざんの被害は一定数確認され、JPCERT/CC では、これらのサイトの管理者に対して状況の確認依頼を行うと共に、攻撃に関する情報提供や、問題解決の支援を行いました。

1.2.3. enPiT-Security (SecCap)リスクマネジメント演習における教材の開発と演習実施

JPCERT/CC は enPiT-Security (SecCap)における演習科目のひとつであるリスクマネジメント演習の講義の一部を担当しました。enPiT-Security (SecCap)は、文部科学省の「情報技術人材育成のための実践教育ネットワーク形成事業」において昨年度から開始されている「分野・地域を越えた実践的情報教育協働ネットワーク」（通称 enPiT）のセキュリティ分野プロジェクトです。
本年度のリスクマネジメント演習は 5 大学院から 18 名の受講生を迎えて開催されました。JPCERT/CC が担当した演習では、マルウエア感染を起点とした仮想インシデントに対して、感染元となった Web サイトの調査と検体の解析を行う一連のプロセスを実習していただきました。
JPCERT/CC は、リスクマネジメント演習の中でインシデント対応における実務能力に関する部分を担当しました。実際のインシデント対応では、知識と実務能力の双方が必要です。知識だけでは戦略立案はできても、実施段階で頓挫しかねません。効果的な実施には実務能力が不可欠なのです。このような観点から、実習を通じてインシデント対応を学び、実務能力を身につける契機となるような教材の開発も、JPCERT/CC の重要な役割であると考えています。

enPiT-Security (SecCap)
http://www.seccap.jp/

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。2014 年 9 月末時点で、観測用センサーはアジア・太平洋地域の 24 地域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

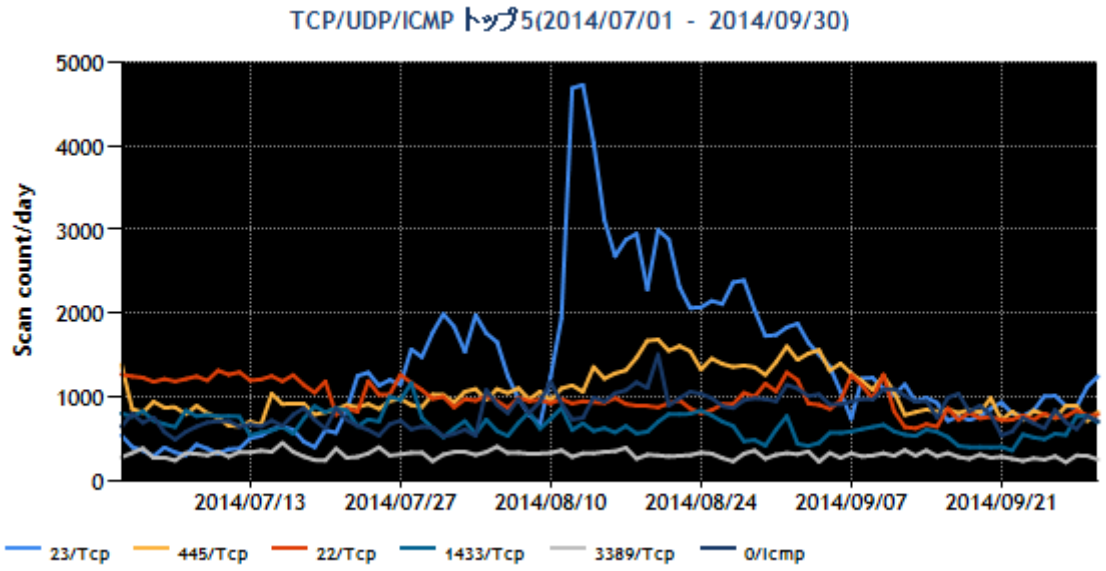
JPCERT/CC は、TSUBAME で収集したデータを宛先ポート番号や送信元地域ごとに分類して統計分析し、既知の脆弱性情報やマルウエア、攻撃ツール等との関連を考察することで、攻撃活動や準備活動の

捕捉に努めています。

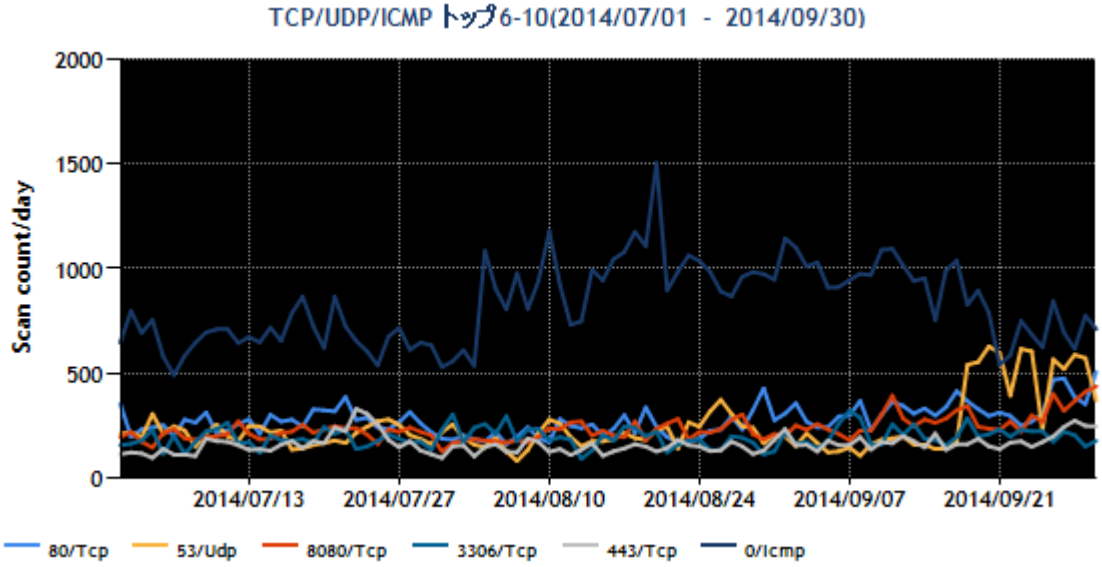
主に日本企業のシステム管理者等の方々に、自ネットワークに届くパケットの傾向と比較していただけるよう、日本国内のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2014 年 1 月から 3 月分のレポートを 4 月 21 日に公開しました。

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(2014 年 4～6 月)
https://www.jpcert.or.jp/tsubame/report/report201404-06.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。

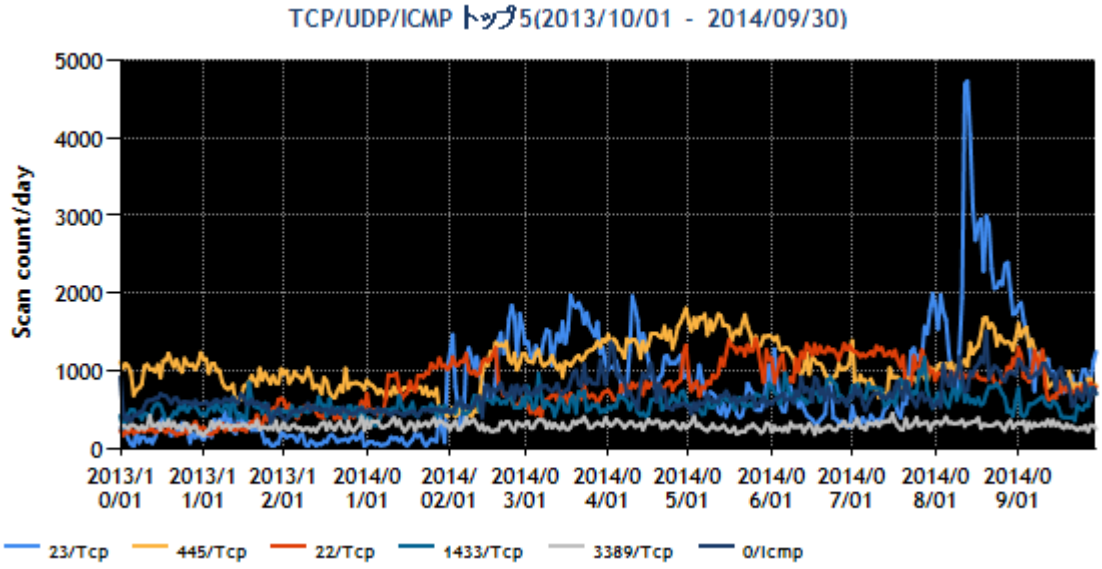


[図 1-1　宛先ポート別グラフ　トップ 1-5 (2014 年 7 月 1 日-9 月 30 日)]

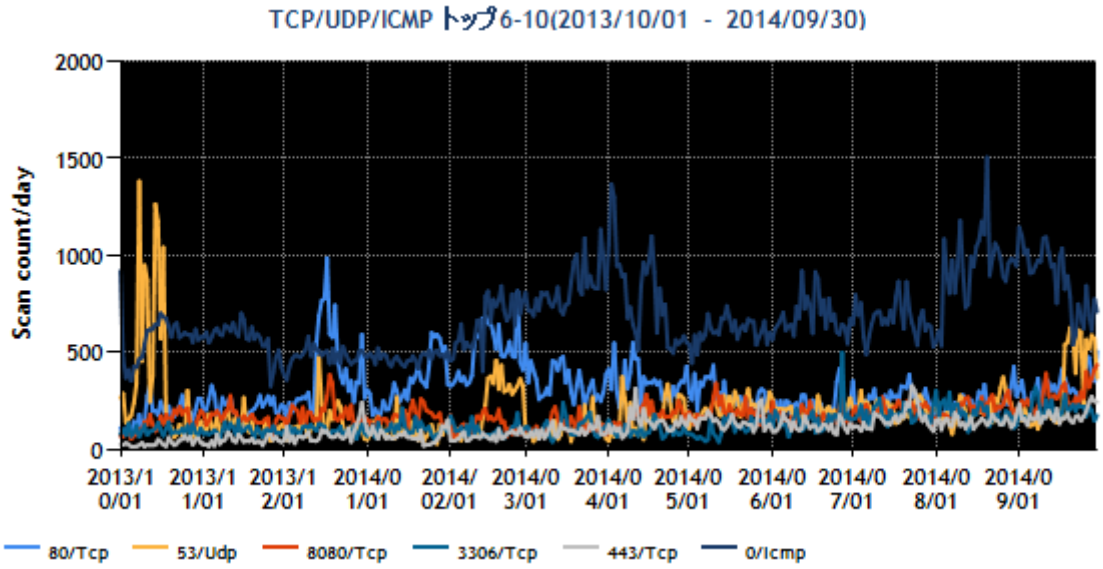


[図 1-2　宛先ポート別グラフ　トップ 6-10(2014 年 7 月 1 日-9 月 30 日)]

また、過去 1 年間(2013 年 10 月 1 日～2014 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 (2013 年 10 月 1 日-2014 年 9 月 30 日)]



[図 1-4　宛先ポート別グラフ　トップ 6-10 (2013 年 10 月 1 日-2014 年 9 月 30 日)]

2014 年 8 月 12 日に 23/TCP 宛のパケットが急増し、日を追って少しずつ減少しましたが本四半期末まで多い状態が続いています。今回の急増は、前四半期で紹介した外国製ネットワークカメラに加え、主に国外で広く利用されているブロードバンドルータなどがマルウエアに感染して頻繁なスキャン活動を行ったことが原因と見られます。本事象については、製品ベンダがある地域の National CSIRT にも情報を共有しています。その他、順位に変動はありますが、Windows や Windows 上で動作するソフトウエア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 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は、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。

DNS 応答パケットおよび、DNS サービスのポート不達を示す ICMP エラーパケットが、本四半期もセンサー上で継続して多数観測されました。これらの観測されたパケットは、実際には存在しない FQDN をオープンリゾルバ経由で多数問い合わせることにより DNS 権威サーバに過剰な負荷を課そうとする攻撃において、攻撃者が応答パケットを受け取らずにすませるために詐称した送信元が，たまたまセンサーの IP アドレスだったために観測されたパケットであると推測されています。すなわち、攻撃者がオープンリゾルバだと思って利用したノードが，実際にはオープンリゾルバでなかった場合には ICMP エラーが、本当にオープンリゾルバであった場合には「名前解決できなかった」旨の応答がセンサーに届いていると見られます。この考え方に基づく分析で、日本国内だけでも毎日 10 数件近くのオープンリゾルバが新たに見つかっています。JPCERT/CC は、この情報を DNS サーバの管理者に提供し、DNS サーバやネットワーク機器がオープンリゾルバとなっていないか調査を依頼しまし、多くの管理者から「当該サーバの設定が不適切でオープンリゾルバであったことを確認し、必要な対応を行った」等の返事を

得ています。

1.3.3. TSUBAME トレーニングの実施

本四半期は、Sri Lanka CERT|CC (スリランカ民主社会主義共和国の National CSIRT) 向けに、次の要領で TSUBAME トレーニングを実施しました。

日時：2014 年 9 月 30 日 (火)
場所：スリランカ民主社会主義共和国 コロンボ (Sri Lanka CERT|CC 会議室)
参加人数：10 名(Sri Lanka CERT|CC のメンバが参加)

トレーニングの内容：
- TSUBAME プロジェクトの概要
- TSUBAME システム、センサーの機能の説明
- TSUBAME システムから得られた情報の活用方法の紹介など

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

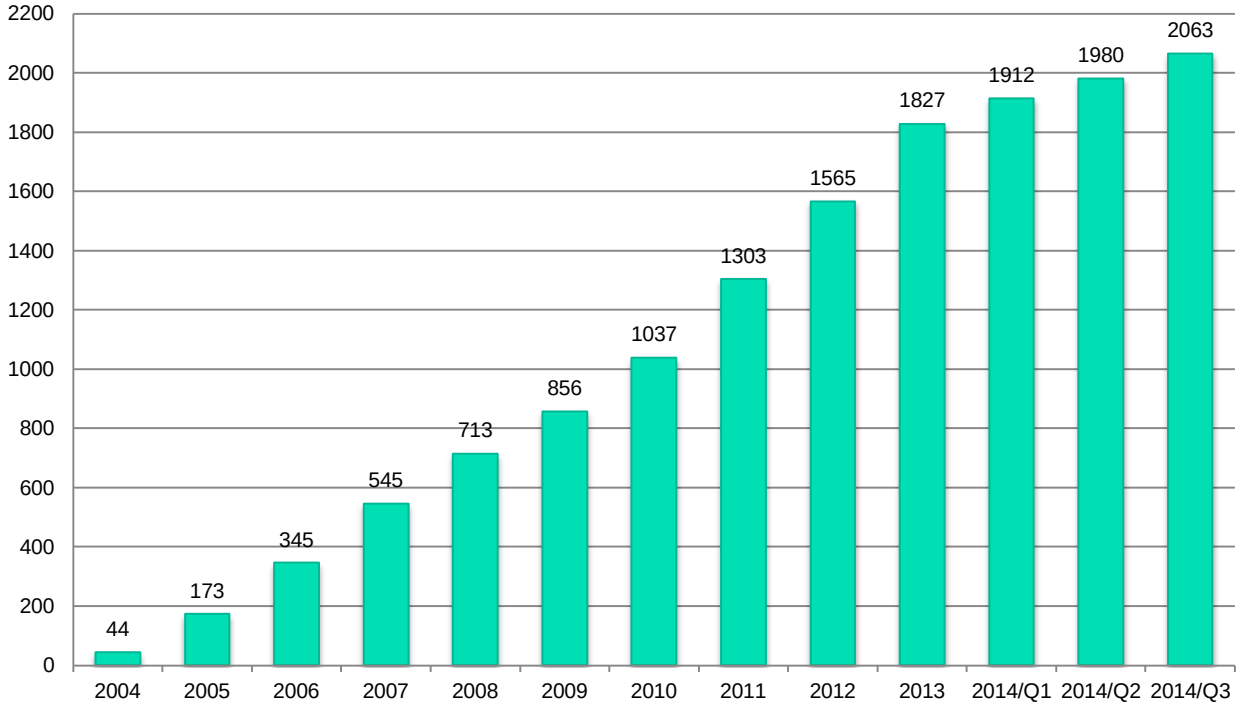
JPCERT/CC は、経済産業省告示「ソフトウエア等脆弱性情報取扱基準」(平成 26 年経済産業省告示 第 110 号。以下「本基準」といいます。)に基づいて製品開発者とのコーディネーションを行う「調整機関」に指定されており、本基準を踏まえて取りまとめられた「情報セキュリティ早期警戒パートナーシップガイドライン(以下「パートナーシップガイドライン」といいます。)に従って、対象となる脆弱性に関係する製品開発者の特定、脆弱性関連情報の適切な窓口への連絡、開発者による脆弱性の検証等の対応や脆弱性情報の公表スケジュール等に関する調整を行い、原則として、調整した公表日に JVN を通じて脆弱性情報等を一般に公表しています。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 83 件(累計 2063 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]

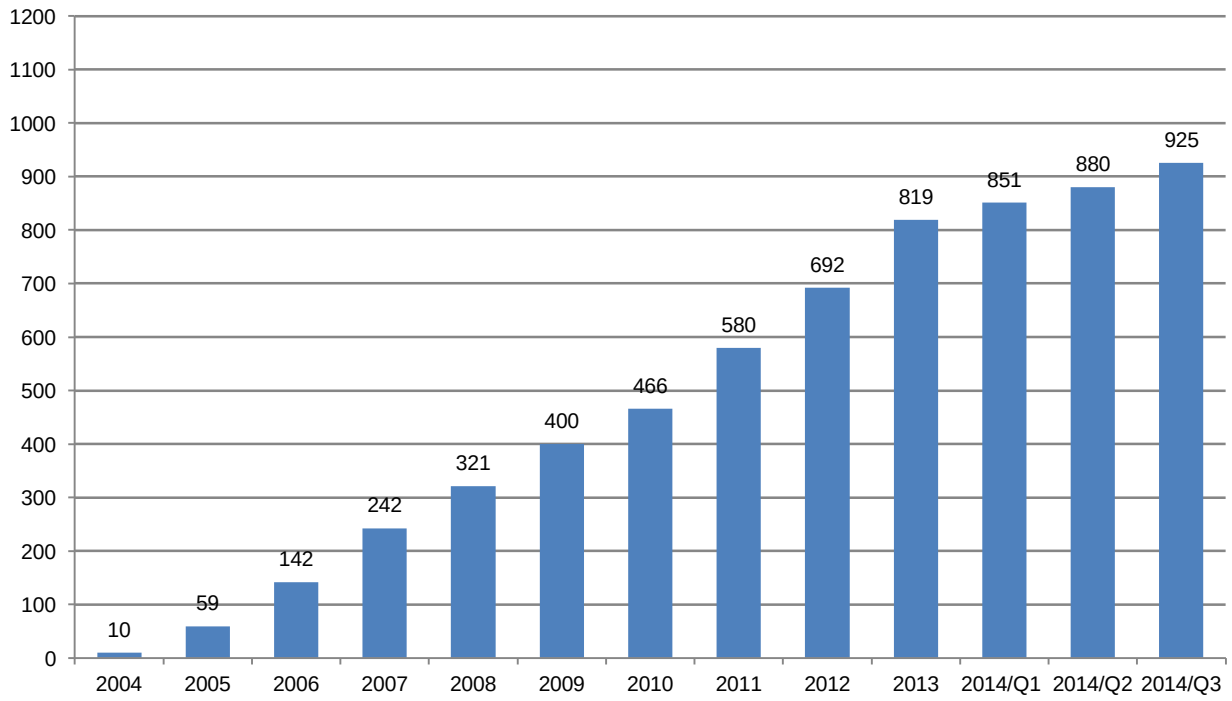
本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 45 件(累計 925 件)で、累計の推移は[図 2-2]に示すとおりです。45 件のうち、26 件が国内製品開発者の製品、19 件が海外の製品開発者の製品でした。

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 8 件公表しました。これは本四半期で公表した全脆弱性情報の約 18%にあたります。

Android およびその関連製品の脆弱性情報の届出は、2012 年度から目立っており、これまで毎四半期ごとに複数件の公表を行っています。本四半期には、JVN 上での公表ベースで、Android 向けアプリケー

ションに関する脆弱性情報が 8 件あり、全体の約 18%を占めました。国内取扱脆弱性情報以外でも、複数の Android アプリに存在する脆弱性 JVNVU#90369988 が米国 CERT/CC から公表されました。Android アプリにおける脆弱性の発見は、まだ今後も続きそうです。

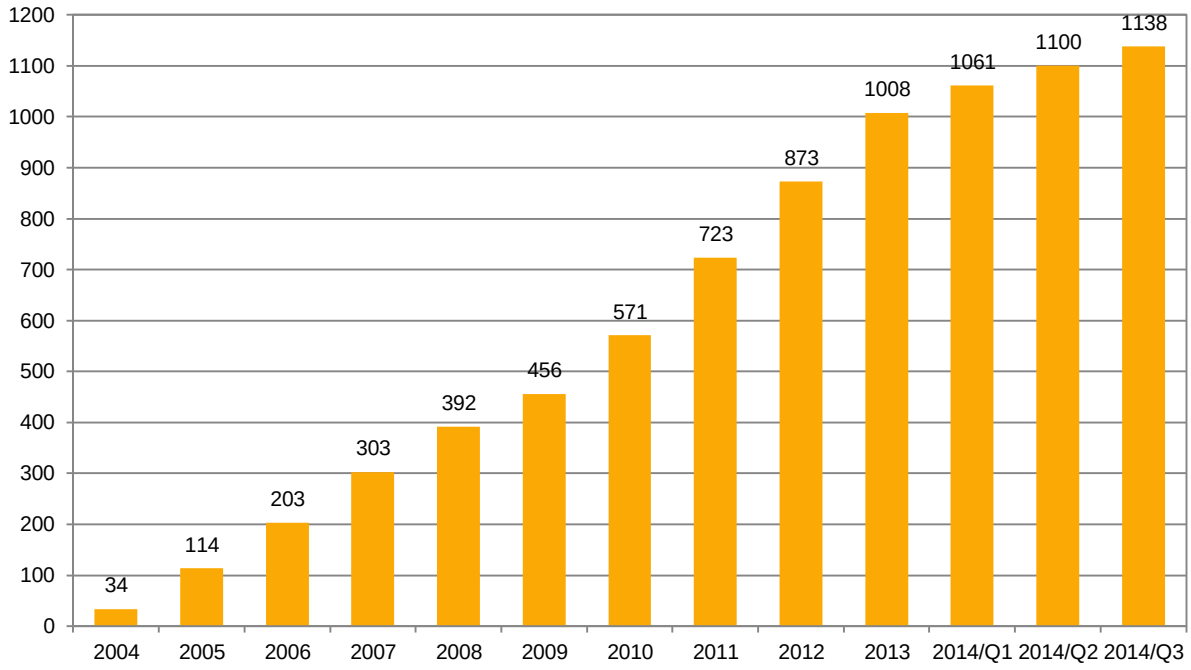
Android 関連製品以外で公表された脆弱性情報の内訳は、グループウェア製品に関するものが 6 件、ウェブアルバム関連製品が 5 件、組込系ネットワーク関連機器が 4 件、オープンソースソフトウエア製品が 2 件、ブログ関連製品が 2 件となりました。またそれ以外の製品では、メディアプレイヤー、証券取引システム、サーバ監視システム、制御関連製品など比較的多様な製品の脆弱性情報も公開しました。



[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 38 件(累計 1138 件)で、累計の推移は[図 2-3]に示すとおりです。本四半期は 4 件と JPCERT/CC が調整に関与したものが多くありました。このうち 2 件は、米国 The Industrial Control Systems Cyber Emergency Response Team (以下「ICS-CERT」といいます。)が届出を受け、JPCERT/CC へ国際展開され、JPCERT/CC が日本の製品開発者との調整を経て公開に至った制御系製品に関するものでした。この他、フィンランド NISCC(旧 CERT-IF)が届出を受け、米国 CERT/CC および JPCERT/CC へ国際展開され、各国 CERT が自国の製品開発者との調整を行い公開に至った OpenSSL の脆弱性が 1 件、米国 CERT/CC が届出を受け、JPCERT/CC へ国際展開され、日本の製品開発者との調整を経て公開に至った Unified Extensible Firmware Interface (UEFI)の脆弱性が 1 件ずつありました。なお、9 月 26 日に世界的に問題視された Bash の脆弱性に関して、JPCERT/CC では、同日に JVNVU#97219505「GNU Bash に OS コマンドインジェクションの脆弱性」として公開しました。この公開は米国 CERT/CC が公開した VU#252743 に基づく JVN での公開となり、事前の国際展開および調整がないものでしたが、影響範囲が大きいことから、JVN での公開と同時に複数の製品開発者に展開し調整を行いました。

例年この期は、8 月に米国ラスベガスで開催される Black Hat Conference あるいは DEFCON を契機に、研究者による脆弱性情報の発表、製品開発者による対策情報の公開等が多くなる傾向にあります。本四半期においてもその影響を受け、7 件の通信衛星関連製品の脆弱性情報を公開しました。この他、公表された脆弱性情報の中で多かったものとしては、ネットワーク関連製品が 5 件、企業向け管理製品(電源管理、顧客管理、企業管理などソリューション系製品を指します。)などの脆弱性情報を 3 件公開しました。また Apple による自社製品に関する脆弱性情報の届出によるものが 3 件ありました。



[図 2-3　国際取扱脆弱性情報の公表累積件数]

2.2.　連絡不能開発者とそれに対する対応の状況等

本基準に基づいて脆弱性が報告されたものの、調査と対策を期待して呼び掛けても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」として公表しています。これまでに 173 件(製品開発者数としては 107 件)を公表し、22 件(製品開発者の数としては 15 件)の調整が再開でき、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製品開発者名は 8 件でした。本四半期末日時点で、合計 151 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。

なお、2013 年度の「情報システム等の脆弱性情報の取扱いに関する研究会」において検討された結果をも踏まえ、本年5 月14 日に本基準が改正され、所定の努力を尽くしても製品開発者と連絡が取れないケースについて、中立的な委員会での審議を経て脆弱性情報公表できることとされました。この改正を受け、

パートナーシップガイドラインが改訂され、5 月30 日に公表されました。 これにあわせ JPCERT/CC では、「JPCERT/CC 脆弱性関連情報取扱いガイドライン」を改訂し、同日に公表しました。
このガイドライン改訂により、脆弱性関連情報の一般公表に関する取扱いや、連絡不能等の理由により製品開発者と調整ができない脆弱性案件の取扱いが変更されています。その他、脆弱性情報の一般公表を取りやめる場合についての記述や、製品開発者が顧客等の製品利用者に対し脆弱性情報を一般公表の前に通知する場合についての記述なども追加されています。本基準、パートナーシップガイドライン、JPCERT/CC 脆弱性関連情報取扱いガイドラインを参照されるにあたっては、内容が最新の改訂版に更新されていることをご確認ください。
各種ガイドライン等の最新版は、次の Web ページで御確認いただくことが可能です。
https://www.jpcert.or.jp/vh/top.html

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、脆弱性情報の円滑な国際的流通のため、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 製品の脆弱性の調整活動の中では、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、前四半期においては 2 件、本四半期においても 2 件と合計 4 件の脆弱性情報の公開を行い、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（National CERT）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に対し、45 件に CVE 番号が付与されており、そのうち 42 件は JPCERT/CC が採番しました。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

なお、1999 年の運用開始以来、CVE 番号の構文が「CVE-<西暦年号>-<4 桁の数字>」と定められていたため、1 年間に付与できる CVE には上限がありました。一方で、世界中で発見される脆弱性は年々増加の一途をたどっており、やがて 1 万件を超えて CVE 番号を付与できない事態になることが懸念される事態に至っていました。CVE を管理・運営している Primary CNA である米国 MITRE 社では、2013 年に CVE 番号体系の変更に対応するための調査、関連組織や利用者へのヒアリングやアンケート等を実施し、約 1 年間をかけて番号体系の変更を検討しました。その結果、数字 4 桁で不足する場合には漸次桁数を増やす方式が採用されることになり、本年 1 月 1 日より実施されています。JPCERT/CC も CNA のひとつとして、この番号体系に準じた運用を開始しています。

新しい CVE 番号体系でも、年間の初期に付与される CVE 番号は以前とまったく変わりませんが、1 万件目以降については、CVE 番号を固定長として取り扱う処理系では 2000 年問題と同様の混乱を生じます。そうした混乱を避けるため、米国 MITRE 社はまず、年初の 2014 年 1 月 15 日に CVE のウェブサイト上で新番号体系での運用が開始している旨の Notification を掲載しました。次に 7 月 15 日に、CVE 番号体系変更の Reminder Notification を掲載しました。米国 MITRE 社は、更に CNA をはじめとする CVE 利用者や脆弱性情報を参照するエンドユーザに至るまで、この CVE 番号体系を改めて広く周知すべく、9 月 18 日に MITRE プレスリリースを発行しました。JPCERT/CC でも日本のユーザに CVE 番号体系の変更を周知すべく、米国 MITRE 社と連携して、9 月 24 日にプレスリリースを発行しました。両組織からのプレスリリースについては、次の Web ページをご参照ください。

Leading Software Vendors and Cybersecurity Organizations Among Early Adopters of MITRE's New Vulnerability Naming Format
https://www.mitre.org/news/press-releases/leading-software-vendors-and-cybersecurity-organizations-among-early-adopters-of

Organizations Compliant with the New CVE-ID Syntax
https://cve.mitre.org/cve/identifiers/compliant_organizations.html

脆弱性を識別する CVE 番号の新体系による採番のお知らせ
https://www.jpcert.or.jp/pr/2014/pr140006.html

CVE-ID Syntax Change
https://cve.mitre.org/cve/identifiers/syntaxchange.html

January 15, 2014
New CVE-ID Format in Effect as of January 1, 2014
https://cve.mitre.org/news/index.html#jan152014_New_CVE-ID_Format_in_Effect_as_of_January_1_2014

July 15, 2014

Reminder to Update Products, Services, and Processes to the New CVE-ID Numbering Format

https://cve.mitre.org/news/index.html#july292014_Reminder_to_Update_Products,_Services,_and_Processes_to_the_New_CVE-ID_Numbering_Format

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 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(2014 年版)
https://www.jpcert.or.jp/vh/partnership_guide2014.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

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り扱い状況等の情報交換を行う等、緊密な連携を行っています。なお、本基準における IPA の活動および四半期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/

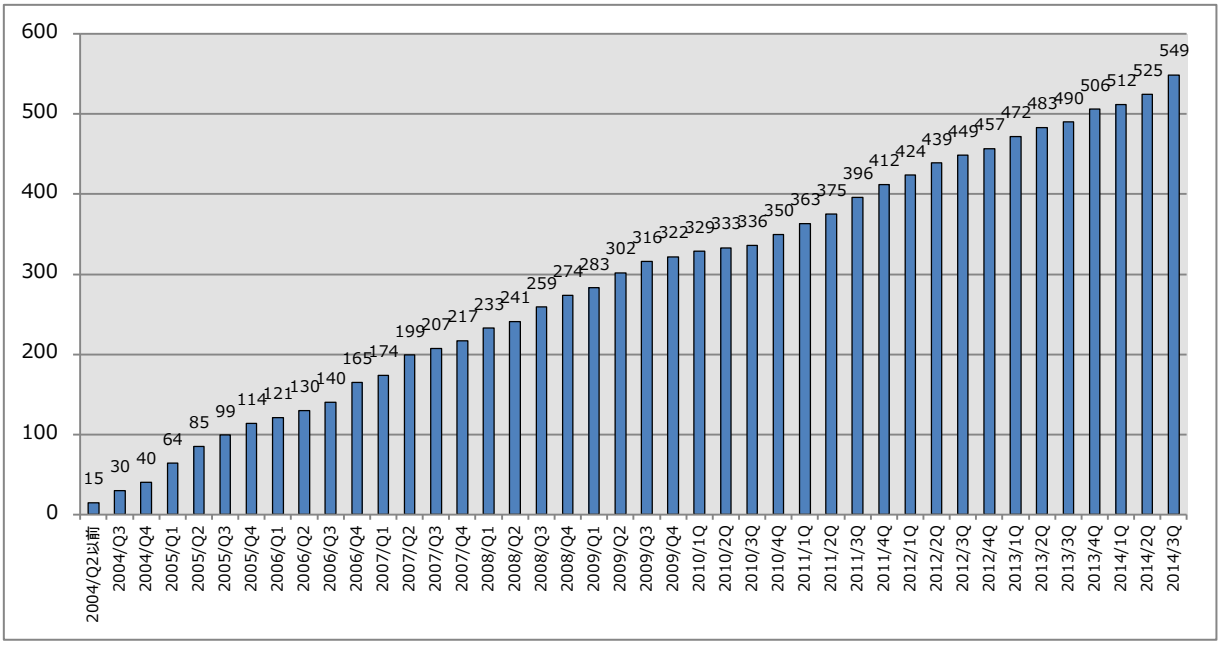
2.4.2. 日本国内製品開発者との連携

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、

2014 年 9 月 30 日現在で 549 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



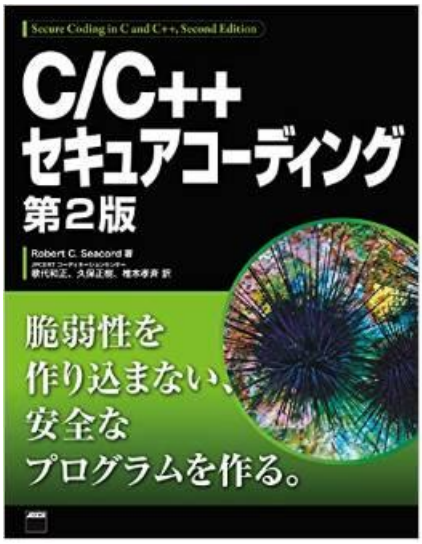
[図 2-4　累計製品開発者登録数]

2.5.　セキュアコーディング啓発活動

2.5.1.　「C/C++セキュアコーディング 第 2 版」を出版

JPCERT/CC では、久保正樹と椎木孝斉、代表理事の歌代和正の 3 名が翻訳を担当し「C/C++ セキュアコーディング第 2 版」を出版しました。2006 年に本書の初版を出版していましたが、2013 年に原書が “Secure Coding in C and C++, 2nd Edition”として改訂されたことを受けて、翻訳しなおして第 2 版としました。

第 2 版では、各章の内容が大幅に改訂されるとともに、並行処理に関する章が新たに追加されています。ソフトウエア開発に携わるプログラマや、プロジェクトマネージャ、コードレビュー担当者、品質管理担当者、教育担当者、その他ソフトウエアセキュリティに関心のある皆様にご一読いただき、セキュリティ向上に役立てていただけることを期待しています。



[図 2-5　「C/C++ セキュアコーディング 第 2 版」]

著者：Robert C. Seacord
翻訳：歌代和正、久保正樹、椎木孝斉
発行：株式会社 KADOKAWA
発売：2014 年 9 月 17 日
　　552 ページ
定価：4,104 円 (本体 3,800 円)
http://ascii.asciimw.jp/books/books/detail/978-4-04-891987-6.shtml

2.5.2. 「Android セキュアコーディングセミナー in Delhi & Bangalore」 を実施

9 月 10 日にインドの首都デリー、12 日には IT 企業が集まる南部バンガロールにおいて、Android セキュアコーディングセミナーを実施しました。
セミナーは、Android アプリの脆弱性に関する「講義」と、講義内容について理解を深めるための「演習」からなる 1 日コースとして実施しました。現地の大手ソフトウェアベンダーや外資系 IT 企業、金融機関に所属する Android プログラマや開発マネージャ、セキュリティ研究者の方に参加いただき、終始レベルの高い活発な質疑が行われ、受講者の問題意識の高さを感じました。

[図 2-6　バンガロールの受講者と共に]

日本の企業が販売･利用する製品に組み込まれるソフトウエアの開発やプログラミングの外注先となっている企業等が多く存在するインドにおいて、現地のソフトウエア開発者を対象に Android セキュアコーディングに関するノウハウを提供することは、現地のセキュリティ啓発に資するのみならず、日本のソフトウエアセキュリティ向上にも資するものと期待しています。
本セミナーの企画・開催は、CERT-IN(インドの national CERT)および Data Security Council of India (DSCI)と協力して行っており、受講者から高い評価を得るとともに、これらの組織との一層の連携強化に資するものとなりました。
セミナーの資料(英語)は次の Web ページで公開されています。

Android Secure Coding
http://www.slideshare.net/jpcert_securecoding/all-for-attendee

2.5.3.　JEB Plugin 開発チュートリアルを公開

JPCERT/CC の脆弱性解析チームでは、Android アプリの脆弱性解析のために、Android アプリ解析ツール「JEB」を使用しています。本ツールをより多くの Android アプリ開発者の方々にご利用いただけるように、7 月 28 日に、JEB の機能を拡張するプラグインの開発に関するチュートリアル資料を公開しました。

JEB Plugin 開発チュートリアル
https://www.jpcert.or.jp/research/jebplugin.html

JEB はリリースされて間もないということもあり、一般公開されているプラグインの数が少なくドキュメントも殆どありません。本資料は、JEB のプラグインを自由に定義して使いこなせるようになるためのチ

ュートリアルとして、JEB が提供する API や DEX ファイルの構造を、例題を通して分かりやすく説明しています。

2.5.4. 月刊「計装」に調査レポートを掲載

前四半期に公開した調査報告書「制御システム用ソフトウエアの脆弱性対策に有効な CERT C コーディングルールの調査」の前半部分が、月刊「計装」9 月号(2014. Vol.57 No.9)、10 月号(2014. Vol57 No.10)の巻末に参考資料として掲載されました。

2.5.5. セキュアコーディング関連記事を連載中

各種 Web マガジンにおいてセキュアコーディング関連の連載を担当しています。本四半期は、次の記事を執筆しました。

@IT 連載「もいちど知りたい、セキュアコーディングの基本」
第 7 回「動的メモリ管理に関する脆弱性 (その 2)」(公開： 7 月 7 日、執筆：戸田 洋三)
http://www.atmarkit.co.jp/ait/articles/1407/04/news006.html

2.5.6. CERT C コーディングスタンダードのルールを最新版にアップデート中

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 の内容を日本語で提供しています。これは C 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。

本四半期に更新されたルールは次の通りです。

新規追加(4 件)
- FIO21-C. 一時ファイルを共有ディレクトリに作成しない
- FIO22-C. プロセスを生成する前にファイルをクローズする
- FIO47-C. 書式指定文字列を正しく使う
- MEM36-C. realloc() 関数呼び出しでオブジェクトのアラインメントを変更しない

削除(2 件)
- FIO00-C. (FIO47-C. に移動)
- FIO43-C. (FIO21-C. に移動)

内容の更新(28 件)
- ERR33-C. 標準ライブラリ関数のエラーを検出し対処する
- EXP33-C. 初期化されていないメモリからの読み込みを行わない
- EXP34-C. null ポインタを参照しない
- FIO02-C. 汚染された情報源から取得したパス名は正規化する
- FIO03-C. fopen() やファイル作成時の動作について勝手な想定をしない

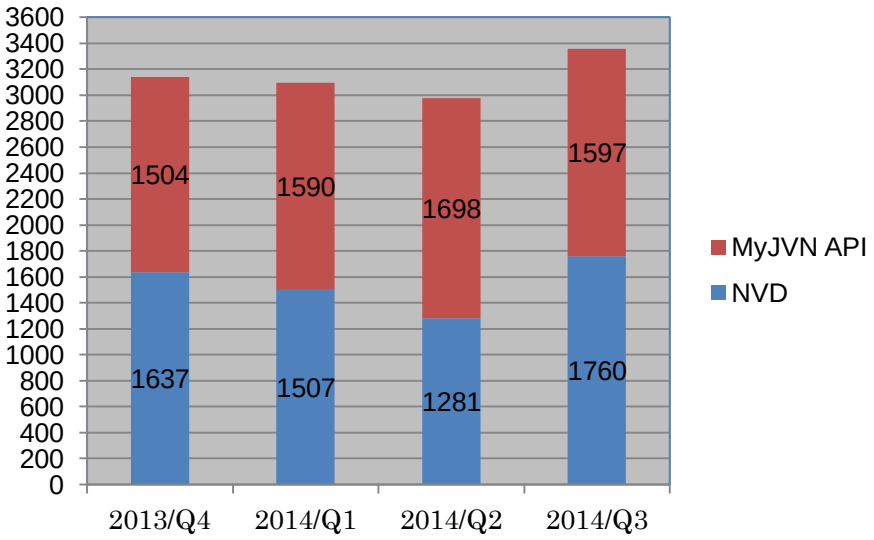
- FIO15-C. ファイル操作はセキュアディレクトリで行う
- FIO30-C. ユーザからの入力を使って書式指定文字列を組み立てない
- FIO32-C. 通常ファイルに対してのみ行われるべき操作をデバイスファイルに対して行わ
- FIO34-C. ファイルから読み込んだ文字と EOF や WEOF を区別する
- INT34-C. 負のビット数のシフトやオペランドのビット数以上のシフトを行わない
- MEM09-C. メモリ割り当て関数がメモリを初期化すると仮定しない
- MSC00-C. 高い警告レベルでのコンパイルで警告が出ないようにする
- MSC06-C. コンパイラの最適化に注意する
- MSC14-C. 必要もなくコードをプラットフォーム依存にしない
- MSC31-C. 関数の返り値は必ず適切な型と比較する
- POS01-C. ファイルを操作するときにはリンクかどうかを確認する
- POS35-C. シンボリックリンクの存在をチェックするときには競合状態を避ける
- PRE00-C. 関数形式マクロよりもインライン関数やスタティック関数を使う
- PRE01-C. マクロ内の引数名は括弧で囲む
- PRE02-C. マクロ置換リストは括弧で囲む
- PRE03-C. 型をエンコードするには define よりも typedef を選ぶ
- PRE04-C. 標準ヘッダファイル名を再利用しない
- PRE05-C. 字句の結合や文字列化を行う際のマクロ置換動作をよく理解する
- PRE06-C. ヘッダファイルはインクルードガードで囲む
- PRE07-C. "??" の繰り返しは避ける
- STR31-C. 文字データと null 終端文字を格納するために十分な領域を確保する
- STR32-C. 文字列を引数にとるライブラリ関数に null 終端されていない文字配列を渡さ
- STR35-C. 長さに制限のないデータを固定長配列へコピーしない

2.6. VRDA フィードによる脆弱性情報の配信

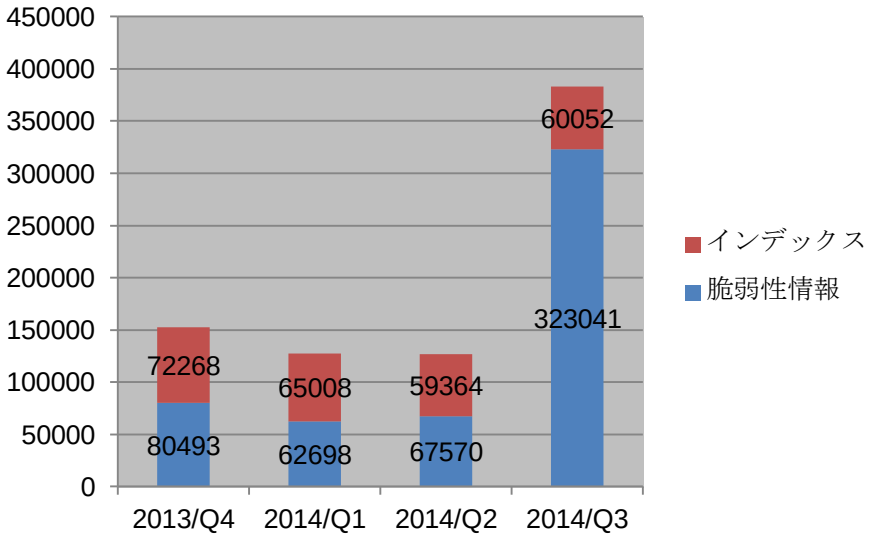
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST(National Institute of Standards and Technology)の NVD(National Vulnerability Database)を外部データソースとして利用した、VRDA(Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web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

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。

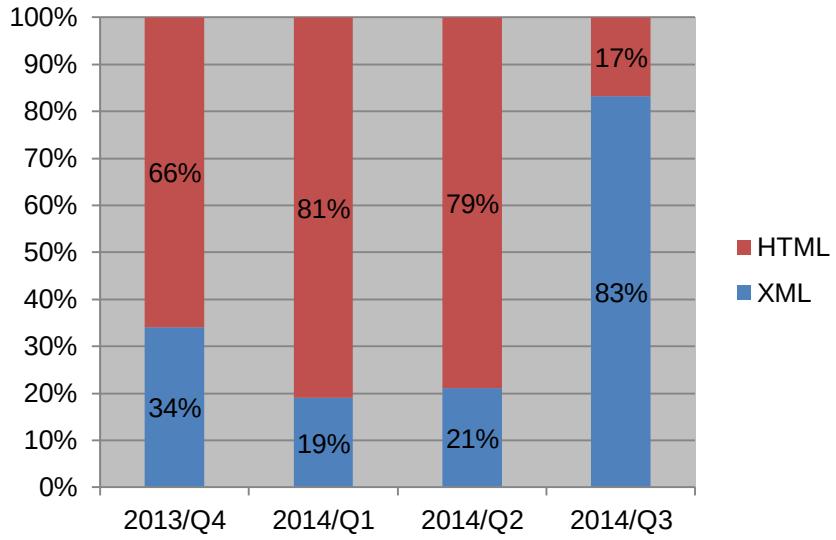


[図 2-7　VRDA フィード配信件数]



[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。脆弱性情報の利用数については、前四半期と比較し、約 4.8 倍増加しました。



[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、脆弱性情報のデータ形式別利用傾向については、本四半期において、HTML 形式と XML 形式の利用割合が逆転しました。

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 553 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*)に提供いたしました。

*)　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る。

本四半期に提供した参考情報は次の 3 件でした。

- 2014/09/01　[参考情報] DNP3 プロトコルの脆弱性に関する情報共有
- 2014/09/26　[参考情報] GNU bash の脆弱性に関する情報共有
- 2014/09/30　[参考情報] GNU bash の脆弱性に関する情報共有(続報)

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 回配信しました。

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 380 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

本四半期に報告された制御システムに関連するインシデントの件数は 0 件でした。
今期より、「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てしまう危険性のあるシステムの保有組織に対する情報提供を開始しました。悪用されてしまう危険性のあるシステムに対する今期の情報提供件数は、6 件でした。

3.3. 関連団体との連携

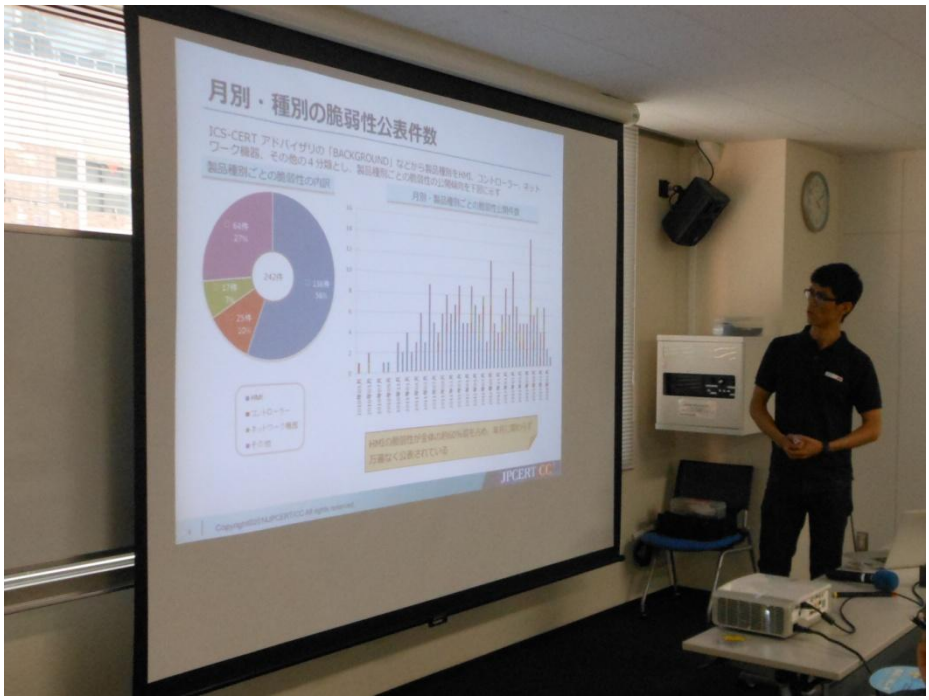
SICE (計測自動制御学会)と JEITA(電子情報技術産業協会)、JEMIMA(日本電気計測器工業会)が定期的に開催している合同セキュリティ検討 WG(ワーキンググループ)に参加し、制御システムのセキュリティに関して専門家の方々と意見交換を行いました。

3.4. 制御システム向けツールの配布情報

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)の配布を行っています。本四半期は、日本版 SSAT に関して 1 件、J-CLICS に関して 8 件の利用申込みがありました。直接配布件数の累計は、日本版 SSAT が 160 件、J-CLICS が 211 件となりました。

3.5. 制御システム開発者向けセキュアコーディングセミナーの開催

2014 年 7 月 25 日、千代田プラットフォームスクエアにて「制御システムの脆弱性その傾向と対策～CERT C コーディングルールの活用に向けて～」と題した技術セミナーを開催いたしました。本セミナーでは、**「制御システムセキュリティの現状と CSSC の取り組み」と題した特別講演に続き、**過去に実際に発見された制御システム関連の脆弱性の具体事例と、脆弱性を調査することで明らかになった対策に有効な 22 のセキュアコーディングルールについて解説しました(図 3-1 参照)。セミナーには、主に制御システムを開発する国内ベンダの技術者を中心に 26 名(定員:30 名)の方にご参加いただきました。



[図 3- 1　講演風景]

3.6.　参考資料「制御システム用製品の開発ベンダにおける脆弱性対応について」の公開

2014 年 5 月に「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」が改訂され、対象となるソフトウエア製品に制御システムが含まれることが明記されたことを受け、制御システム製品開発ベンダにおける脆弱性対応のための資料として、「参考資料：制御システム用製品の開発ベンダにおける脆弱性対応について」を公開しました。本資料は、制御システム用製品を提供しているベンダが自社製品の脆弱性情報を適切に取り扱うために必要な機能と体制の整備等についてまとめています。

参考資料「制御システム用製品の開発ベンダにおける脆弱性対応について」
https://www.jpcert.or.jp/ics/information05.html

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)等のインシデント対応調整能力の向上を図るため、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。

4.1.1.　モンゴル CSIRT 構築支援等(2014 年 9 月 4 日-7 日)

モンゴル CSIRT 構築支援の一環で、MNCERT/CC が主催した MNSEC 2014 Information Security Training and Seminar に 2 名の講師派遣を行いました。9 月 5 日は、約 100 名以上の聴衆が集まる中、JPCERT/CC

の活動紹介、日本のセキュリティ事情、APCERT の組織概要、また最新のインシデント動向について講演を行いました。9 月 6 日は、政府組織やインフラ関係のセキュリティ従事者約 40 名に対して、ネットワークフォレンジックのハンズオン研修を行いました。

[図 4-1　ハンズオン研修の模様]

4.1.2.　インドネシアの CSIRT 構築支援活動(2014 年 8 月 4 日)

インドネシアの CSIRT の構築・運用支援活動として、独立行政法人国際協力機構（JICA）から依頼を受け、インドネシア通信省職員 2 名に対して、CSIRT の人材育成や JPCERT/CC の重要インフラ保護に向けての取り組みなどの講義を行いました。また、JICA やインドネシアの関係者とともに今後のインドネシアでの CSIRT 構築支援計画について協議しました。

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 連携の取組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、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(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 は、7 月 17 日に電話会議を、また 9 月 15～16 日には APNIC 38 会合の開催にあわせオーストラリア・ブリスベンでの会議を行い、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、これらの会議の主導およびサポートを行いました。

4.2.1.2. APCERT を代表しての会議出席

- IGF 2014 Istanbul

  トルコのイスタンブールで 9 月 1 日から 5 日まで開催された The Internet Governance Forum (IGF) 2014 において、JPCERT/CC は APCERT を代表して登壇し、インターネットガバナンスに携わる関係者に対して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の必要性を訴えるとともに、サイバー分野での官民連携、APCERT の取組み等の紹介／報告を行いました。

  IGF 2014 Istanbul 公式ページ
  http://www.igf2014.org.tr/

- APNIC 38

  JPCERT/CC はオーストラリア・ブリスベンで開かれた APNIC 38 会合に出席し、APNIC Security Track では APCERT を代表して活動の最新状況について講演を行いました。

  APNIC 38 公式ページ
  https://conference.apnic.net/38/home

4.2.2. 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 19 日-21 日に米国のサンディエゴで開催された 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/

4.2.3. 第ニ回 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 (2014 年 8 月 21 日-22 日)

日中韓の National CSIRT (JPCERT/CC、CNCERT/CC、KrCERT/CC)が、2011 年 12 月に締結した覚書(MOU)で定めている、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 21 日、22 日に韓国・ソウルで開催されました。本年次会合は、昨年の上海での第一回会合に続くものです。日中韓 3 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、第一回会合以降の実績のレビューを行うとともに、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。
本会合では、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適切に行うとともに、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を再確認すること、また、三者は国際サイバー空間の健全性向上に貢献すべく、比較可能なサイバーリスク計測を行うための情報共有プロトコル、メトリックス、標準等の整備を行うことが合意されました。

4.2.4. ACID: ASEAN 及び周辺各国の CSIRT による合同サイバーインシデント演習への参加(9 月 24 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 9 度目になります。今年は企業に対する情報（サイバー）スパイの発生を想定した演習が行われました。

4.2.5. 日本・イスラエル・ビジネスフォーラム 参加 (2014 年 7 月 6 日)

JPCERT/CC は、日イスラエル政府高官や企業関係者等が参加する「日本・イスラエル・ビジネスフォーラム」に参加しました。両国企業が一堂に会する初めての本格的なフォーラムであり、イスラエルのサイバーセキュリティへの取組みに関する情報収集と、関係者との人脈形成、今後の連携に向けた情報交換を行いました。

4.2.6. インド CERT-In のオフィスを訪問 (2014 年 9 月 9 日)

JPCERT/CC は、インドの National CSIRT である CERT-In のオフィスを訪問し、今後の両者の連携について会合を持ちました。会合では、CERT-In、JPCERT/CC それぞれの活動状況を紹介し、また標的型攻撃への対応や、DNS オープンリゾルバ問題への対応について協議し、今後も密な連携を維持することを確認しました。

4.2.7. 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。

AfricaCERT Training in Djibouti
http://blog.jpcert.or.jp/2014/07/africacert-training-in-djibouti.html

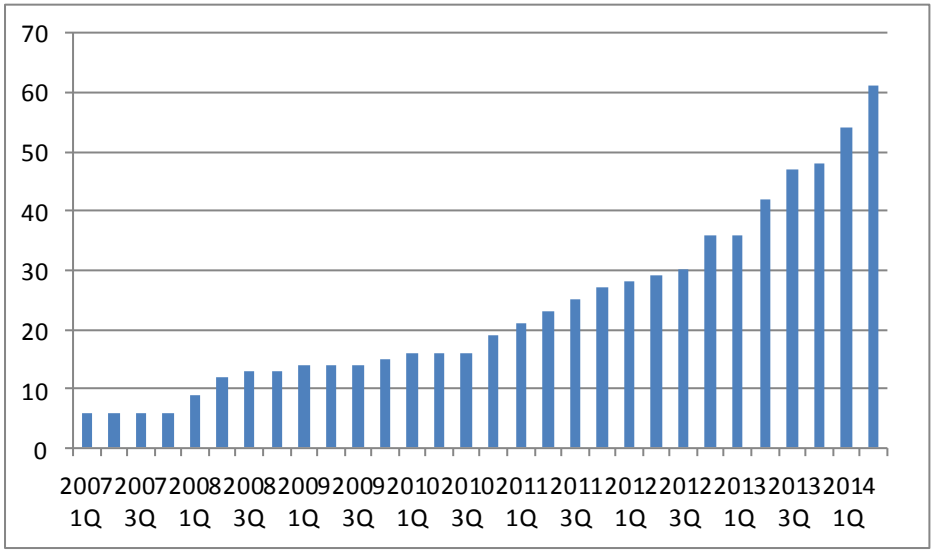
English Version of HTML5 Investigation Report Now Available
http://blog.jpcert.or.jp/2014/08/english-version-of-html5-investigation-report-now-available.html

The 26th FIRST Annual Conference in Boston
http://blog.jpcert.or.jp/2014/08/the-26th-first-annual-conference-in-boston.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主催の会議およびイベントに参加しています。

本四半期においては、株式会社ゆうちょ銀行 (JPBank CSIRT) 、株式会社 FFRI (FFRI) 、東京海上日動システムズ株式会社(TMNS-CSIRT)、株式会社インテック(intec-SIRT) 、株式会社インフォメーション・ディベロプメント(iD-SIRT)、ヤマトホールディングス株式会社(YAMATO-CSIRT)、株式会社 三越伊勢丹システム・ソリューションズ(MI-CSIRT)の 7 組織が新規に加盟しました。本四半期末時点で 61 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 8 回総会を開催いたしました。

2014 年 8 月 21 日(木)　14:00～18:00
会場：株式会社日立製作所　講堂
参加人数：161 名

総会において事務局指定の審議が行われ、今年度も引き続き JPCERT/CC が事務局を担当することが承認されました。また、年次活動報告や新規加盟組織の紹介などが行われました。また、総会後に行われた運営委員会では、株式会社日立製作所　Hitachi Incident Response Team　寺田真敏氏が運営委員長に選任されました。

日本シーサート協議会の活動の詳細については、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

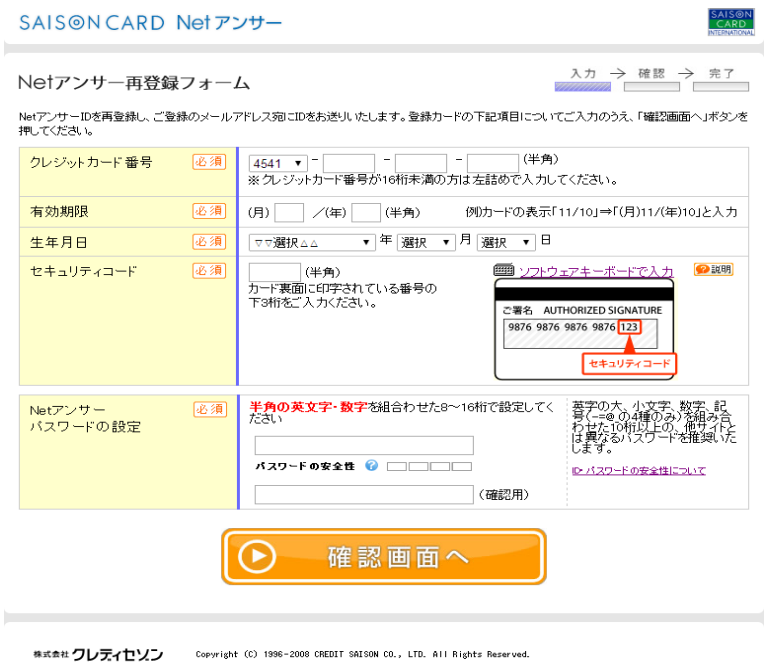
JPCERT/CC は、フィッシング対策協議会(本章において「協議会」といいます。)の事務局を担当しており、経済産業省からの委託により、協議会における各ワーキンググループ活動の運営や、協議会名での一般消費者からのフィッシングに関する報告・問合せの受付、報告に基づくフィッシングサイトに関する注意喚起、等の活動を行っています。

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 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 14 件発信しました。

本四半期は、金融機関をかたるフィッシングやオンラインゲーム事業者をかたるフィッシングの報告を多数受けました。協議会では、名前をかたられた事業者に、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[図 6-1]の「セゾン Net アンサーをかたるフィッシング(2014/08/11)」、Web メールサービスをかたるフィッシングに関しては[図 6-2]の「ODN をかたるフィッシング(2014/07/14)」を、緊急情報として協議会の Web 上で公開し、広く注意を喚起しました。

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 6-1　セゾン Net アンサーをかたるフィッシング(2014/08/11)
https://www.antiphishing.jp/news/alert/saison20140811.html]

[図 6-2　ODN をかたるフィッシング(2014/07/14)
https://www.antiphishing.jp/news/alert/odn0714.html

6.2.　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掛けるための講演活動を行っています。本四半期は次の講演を行いました。

山本健太郎「フィッシングの現状 狙われる金融機関」警察大学校　2014 年 8 月 1 日

6.3.　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　2014 年 7 月　フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201407.html
フィッシング対策協議会　2014 年 8 月　フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201408.html
フィッシング対策協議会　2014 年 9 月　フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201409.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. フィッシング対策ガイドライン実践セミナーの開催

フィッシング対策協議会では、「フィッシング対策ガイドライン」を協議会の Web サイトで公開しています。さらに、「フィッシング対策ガイドライン」を事業者の皆様に詳しく解説する場として、「フィッシング対策ガイドライン実践セミナー2014」を開催し、主に銀行やクレジットカード会社などの金融機関の方々にご参加いただきました。セミナーでは、ライフカード株式会社より「クレジットカード会社のインシデント事例紹介」、トレンドマイクロ株式会社より「ネットバンキング被害の対策も STOP. THINK. CONNECT.」、株式会社ジャックスより「フィッシング詐欺被害対応フローの活用方法」、フィッシング対策協議会から「フィッシング詐欺の現状」の講演が行われました。

フィッシング対策セミナー2014
開催日程：2014 年 9 月 2 日（火）14:00-17:00
会場：株式会社日立システムズ　ソリューションスクエア東京
参加人数：26 名

7.2. 運営委員会開催

本四半期においては、次のとおり、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開催しました。

フィッシング対策協議会 第 16 回運営委員会
日時：2014 年 7 月 18 日 16:00 - 18:00
場所：株式会社ジャックス

フィッシング対策協議会 第 17 回運営委員会
日時：2014 年 8 月 22 日 16:00 - 18:00
場所：株式会社日立システムズ

フィッシング対策協議会 第 18 回運営委員会
日時：2014 年 9 月 19 日 16:00 - 18:00
場所：アルプス システム インテグレーション株式会社

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、セミナー資料は次のとおりです。

8.1. 参考資料「制御システム用製品の開発ベンダにおける脆弱性対応について」

制御システム用製品を扱うベンダが適切に脆弱性関連情報を取り扱うために必要な機能や体制を確立するアプローチ等について、主要ベンダを交えた検討会での議論を経てまとめたもので、制御システム用製品ベンダの皆様が自社製品の脆弱性の取扱いについて検討される際にご活用いただける資料です。

参考資料「制御システム用製品の開発ベンダにおける脆弱性対応について」
(2014 年 8 月 11 日公開)
https://www.jpcert.or.jp/ics/information05.html

8.2. IPv6 セキュリティテスト手順書および検証済み製品リスト(2014/08/01)

「IPv6 セキュリティテスト手順書」に従って IPv6 対応機器ベンダが検証した結果をリスト化した「IPv6 セキュリティテスト検証済み製品リスト(2014/08/01)」を公開しました。これは、IPv6 対応機器の購入を検討されている企業や組織のシステム担当者の方に、機器選定時の参考資料としてご利用いただくことを目的としています。

IPv6 セキュリティテスト検証済み製品リスト
(2014 年 8 月 01 日公開)
https://www.jpcert.or.jp/research/ipv6product_list.html

8.3. HTML5 を利用した Web アプリケーションのセキュリティ問題に関する調査報告書(英語版)

本資料は、HTML5 を利用して安全な Web アプリケーションを開発するための技術ガイドのベースとなる体系的な資料を海外にも広く提供する目的で、2013 年 10 月 30 日に公開した調査報告書を英訳したものです。この報告書は、HTML5 に関連して懸念されるセキュリティ問題を抽出して検討を加え、それぞれに可能な限りの検証を行ったうえで、まとめられています。

Investigation Report Regarding Security Issues of Web Applications Using HTML5
(2014 年 7 月 30 日公開)
https://www.jpcert.or.jp/research/html5.html

8.4. JEB Plugin 開発チュートリアルとソースコードサンプル

本資料は、JEB のプラグインを自由に定義して使いこなせるようになるよう、JEB が提供している API や DEX ファイルの構造を、全 4 回のチュートリアル形式で例題を交えて分かりやすく説明したものです。

また、これらチュートリアルに併せて、ソースコードサンプルも公開しました。

第 0 回　JEB Plugin 開発チュートリアル
第 1 回　－JEB Plugin とは－構造、UI からの情報取得と設定方法を修得する
第 2 回　－DEX ファイルの構造を理解する－JEB Plugin から DEX ファイルを扱う方法を修得する
第 3 回　－バイトコードについての理解－JEB Plugin からバイトコードを扱う方法を修得する
第 4 回　－JEB Plugin から AST を扱う－

JEB Plugin 開発チュートリアル
(2014 年 7 月 28 日公開)
https://www.jpcert.or.jp/research/jebplugin.html

8.5. 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（現行版は平成 26 年経済産業省告示 第 110 号）に基づき、2004 年 7 月から受付機関(IPA)や調整機関(JPCERT/CC)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、2014 年 4 月 1 日から 2014 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[2014 年第 2 四半期(4 月～6 月)]
(2014 年 7 月 24 日)
https://www.jpcert.or.jp/press/2014/vulnREPORT_2014q2.pdf

8.6. Oracle Java 標準ライブラリ AtomicReferenceArray クラスにおけるデシリアライズに関する脆弱性

Java 言語で書かれたアプリケーションの脆弱性事例に関する解説資料であり、セキュアコーディングを学ぶための教材として活用していただくことを目的としてまとめました。
本資料は、AtomicReferenceArray クラスの脆弱性「CVE-2012-0507」について解説したものです。

Oracle Java 標準ライブラリ AtomicReferenceArray クラスにおけるデシリアライズに関する脆弱性
(2014 年 7 月 22 日)
https://www.jpcert.or.jp/securecoding/2014/OracleJava-AtomicReferenceArray.pdf

8.7. 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し、宛先ポート番号や送信元地域ごとに分類して分析するインターネット定点観測を継続的に実施しています。これを、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 2014 年 4 月～6 月
(2014 年 7 月 17 日)
https://www.jpcert.or.jp/tsubame/report/report201401-03.html

9. 主な講演活動一覧

(1) 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 は百社百様、構築の勘所を知る」
「信頼される組織を目指す、CSIRT 運用の勘所」
日経コンピュータ セキュリティ組織「CSIRT」構築セミナー,2014 年 9 月 29 日
(2) 満永 拓邦(早期警戒グループ 情報分析ライン リーダー)：
「なぜ「CSIRT」が必要か？限界に来た「防御によるセキュリティ」」
日経コンピュータ セキュリティ組織「CSIRT」構築セミナー,2014 年 9 月 29 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)：
「最新のセキュリティ動向と対策～インシデントレスポンス体制の重要性と情報連携～」
ISAC 名古屋支部月例会,2014 年 9 月 27 日
(4) 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)：
「被害にあわないためのポイント」
国立大学長崎大学情報セキュリティ講習会,2014 年 9 月 19 日
(5) 宮地利雄(技術顧問)：
“Current Issues and Challenges on Cyber Security for Industrial Automation and Control Systems”
SICE Annual Conference 2014, 2014 年 9 月 11 日
(6) 有村 浩一(常務理事)：
「わが国におけるサイバー攻撃の現状とその対策について」
ガスエネルギー新聞 国内研修ツアーエネルギー自由化時代　勝つための情報セキュリティとは
2014 年 8 月 21 日
(7) 松本 悦宜(早期警戒グループ 情報セキュリティアナリスト)：
「最近のセキュリティ動向」
埼玉県クレジットカード犯罪対策連絡協議会総会,2014 年 8 月 19 日
(8) 山本 健太郎(エンタープライズサポート 情報セキュリティアナリスト)：
「フィッシングの現状」
警察大学校サイバー犯罪捜査幹部研修,2014 年 8 月 1 日
(9) 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)：
「組織における情報セキュリティインシデント対応体制（CSIRT 等）の構築～昨今の外部脅威、攻撃手法と被害の実態～」
JEITA 情報セキュリティ調査専門委員会(第 4 回会合),2014 年 7 月 31 日

(10) 竹田 春樹(分析センター リーダ) :
「不正送金だけが目的ではない!?- Banking Trojan の現状 -」
広島県クレジットカード犯罪対策連絡協議会総会,2014 年 7 月 31 日

(11) 満永 拓邦(早期警戒グループ 情報分析ライン リーダー)
「CERT/CSIRT 運用におけるシステム構築」
NECOMA プロジェクト 第 2 回大学・高等教育機関におけるサイバーセキュリティ能力向上と体制整備に関するワークショップ,2014 年 7 月 28 日

(12) 竹田 春樹(分析センター リーダ) :
「不正送金だけが目的ではない!?- Banking Trojan の現状 -」
千葉県クレジットカード犯罪対策連絡協議会総会,2014 年 7 月 2 日

10. 主な執筆一覧

(1) 竹田 春樹(分析センター リーダ)、澤田 昭浩(分析センター) :
「水飲み場型攻撃などの最近の標的型攻撃の動向と対策」
日本セキュリティ・マネジメント学会 日本セキュリティ・マネジメント学会誌 第 28 巻 第 2 号,2014 年 9 月 25 日

11. 協力、後援一覧

本四半期においてJPCERT/CCは次の行事の開催に協力または後援をしました。

(1) 第10回 IPA 「広げよう情報モラル・セキュリティコンクール」2014
主 催：独立行政法人情報処理推進機構
開催日：2014年4月1日(火) ~11月中旬

12. 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ました。第1回目として2014 年6 月に、日本CSIRT協議会の活動の活性化にご尽力いただいた加藤 孝浩様(トッパン・フォームズ株式会社ICT 事業部Web ビジネス本部業務推進部長)と、多数の有用なセキュリティ情報の報告をいただいているモルスナー ミヒャエル 様(株式会社カスペルスキー情報セキュリティラボ 所長)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/2014/PR20140703-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ーのお問い合わせ ：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：office@jpcert.or.jp