Japan Computer Emergency Response Team Coordination Center

JPCERT/CC®

JPCERT-PR-2014-02
発行日：2014-04-15

JPCERT/CC 活動概要 [2014 年 1 月 1 日 ～ 2014 年 3 月 31 日]

活動概要トピックス

―トピック 1―　2013 年度のインシデント報告件数は 29,191 件、JPCERT/CC が調整を行った件数は 8,717 件に　～2013 年度インシデント対応支援統計～

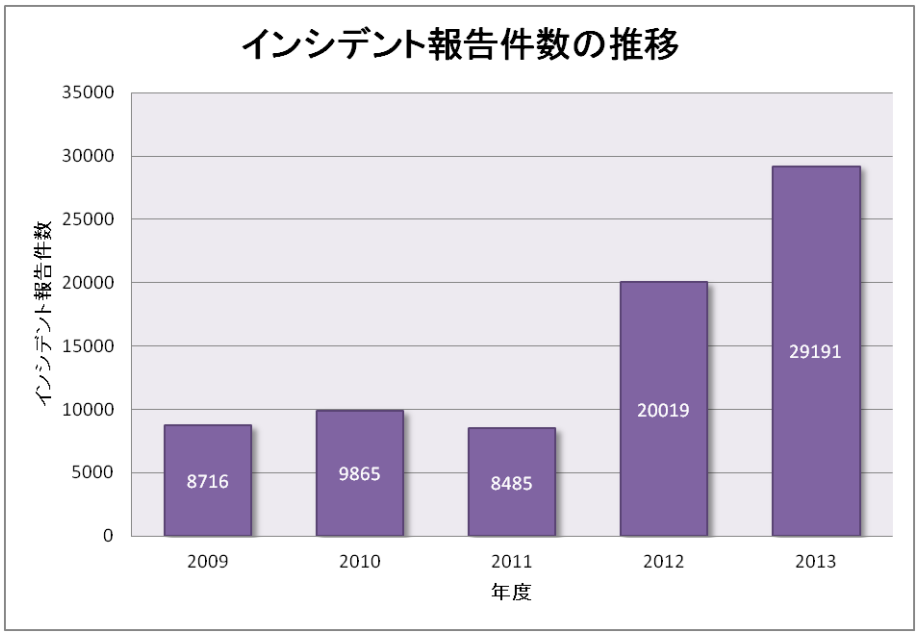
JPCERT/CC が 2013 年度(2013 年 4 月 1 日から 2014 年 3 月 31 日まで)に受け付けたインシデントの報告件数は 29,191 件となり、昨年度の 20,019 件と比べて約 46%増加しました。

また、報告に関わるインシデント件数は 26,687 件で、昨年度の 20,083 件から約 33%増加しました。このインシデント件数のうち、Web サイト改ざんの件数は 7,726 件に上り、昨年度の 2,856 件と比べ、約 2.7 倍に増加しました。2013 年度は、サイトの閲覧者をマルウエア配付サイト等へ誘導することを目的とする不正なプログラムを埋め込む Web サイト改ざんに加え、閲覧者のうちの特定のグループに属する者のみを狙う標的型攻撃のためにされた Web 改ざんの報告も見受けられました。フィッシングサイトのインシデント件数は 1,914 件と、昨年度の 1,474 件に比べて 30%増加しており、日本国内ユーザをターゲットにした国内事業者を装ったフィッシングサイトは、311 件から 719 件（前年度比 2.31 倍）に増加しました。

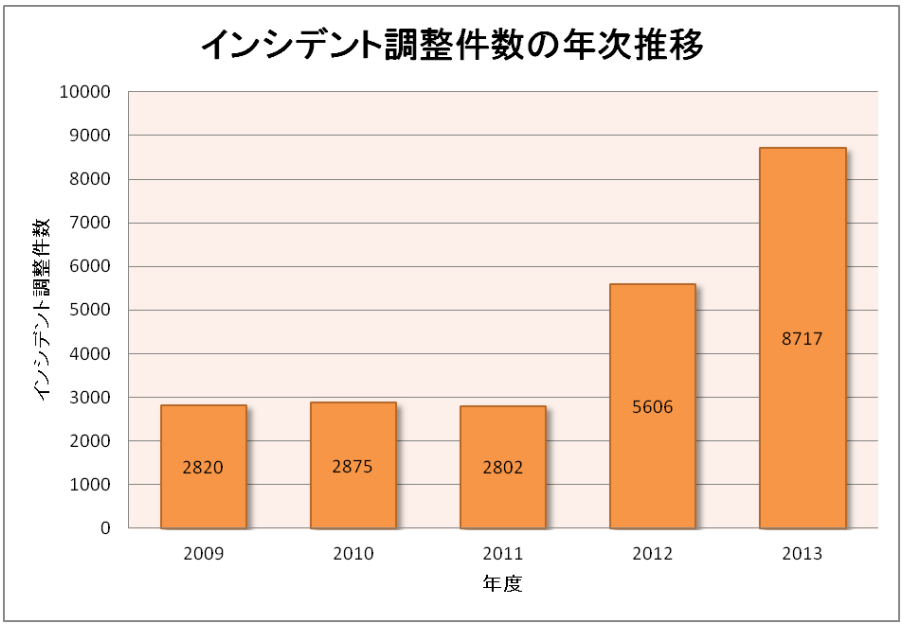
なお、受け付けたインシデントに対応するため、国内外の関連サイトと調整を行った件数は、8717 件でした。

【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。
【注 2】「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。
【注 3】「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。JPCERT/CC に寄せられるインシデント報告の中には、インシデントには既に対応済みであるが日本国内のインシデントの発生状況の把握に資する情報として情報提供のために御報告をいただいているものや、セキュリティベンダ等が自ら行うインシデントへの対応に併せて JPCERT/CC にも情報提供をいただいているもの（JPCERT/CC による調整等の対応依頼を含まないもの）が含まれているため、調整件数は、報告件数に比して少なくなっています。

2013 年度を含む過去 5 年分の報告件数および調整件数の推移は、次のとおりです。



[図 1 報告件数の推移]



[図 2 調整件数の推移]

―トピック 2― インターネットバンキングの情報を窃取するマルウエアに関する技術情報の公開や解析支援ツール”Citadel Decryptor”の提供

JPCERT/CC では、インターネットバンキングの情報を窃取する機能を持つマルウエアである Citadel について詳細な解析を行い、本四半期には、その技術情報を複数の関係組織と共有しました。また、その技術情報をより多くの組織で活用していただくことを目的に、2 月 17 日から 2 日間の日程で開催された日本発の情報セキュリティ国際会議である「CODE BLUE」で発表しました。

さらに、JPCERT/CC では、Citadel の解析作業の効率化のために内部で開発・利用していたツール("Citadel Decryptor")を、インシデントに迅速に対処することが求められる企業等の解析の現場でもご利用いただけるよう、提供しています。

"Citadel Decryptor" は、これまで Citadel の解析作業において手間がかかっていたファイルやレジストリに暗号化して保存されているデータの復号を簡単に行うツールで、本四半期までに 9 つの組織に“Citadel Decryptor”を提供しました。

JPCERT/CC は、このように、実際のインシデント対応に必要な解析技術をコミュニティ全体で共有していくことが、円滑なインシデント対応を可能にし、セキュリティの向上につながると考えています。

―トピック 3―　APCERT 年次会合 2014 および TSUBAME ワークショップの開催―JPCERT/CC は引き続き APCERT のチェアに

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、3 月 18 日から 21 日の日程で、台北で開催され、JPCERT/CC を含む 21 の加盟チームが参加しました。本年の APCERT 年次総会は、“Preparing for a Better Future – The role of CSIRT Community”というテーマで開催され、APCERT が目指す「safe, clean and reliable」なサイバースペースの構築に向けた第一歩として、サイバーセキュリティに関する比較可能で堅牢な定量評価の仕組みの必要性がチーム間で意識共有されました。

APCERT 年次総会では、運営委員会(Steering Committee)のメンバの一部とともに、APCERT 議長チーム/副議長の改選が行われ、JPCERT/CC は議長チーム(4 期目、任期は 2015 年まで)に再選されました。JPCERT/CC は、引き続き APCERT の代表としてさまざまな活動をリードすることとなりました。

また、年次総会に併せ、APCERT のワーキンググループ活動の一つである「TSUBAME ネットワークモニタリングプロジェクト」（アジア太平洋地域を中心とするインターネット上にセンサーを配置し、ワームの感染活動や弱点探索を目的としたスキャンなどのセキュリティ上の脅威となるトラフィックの観測を連携して行い、参加チームが共同でデータの分析を行うプロジェクト）のワークショップも開催しました。このワークショップでは、TSUBAME プロジェクトメンバを対象に、本年度 JPCERT/CC が観測した主な事象に関する報告や、TSUBAME で蓄積したデータから脅威を発見するハンズオン演習、香港およびスリランカのチームによる TSUBAME 活用方法の紹介が行われました。

本活動は、経済産業省より委託を受け、「平成２５年度情報セキュリティ対策推進事業」として実施したものです。
ただし、「9.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」、「6.国際連携活動関連」、「11.講演活動一覧」、「12. 開催セミナー等一覧」及び「13.協力、後援一覧」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 4898 件、インシデント件数ベースでは 4529 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 1989 件でした。前四半期の 2135 件と比較して 7%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_Report20140116.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 557 件で、前四半期の 601 件から 7%減少しました。また、前年度同期(474 件)との比較では、18%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	1 月	2 月	3 月	国内外別合計（割合）
国内ブランド	75	70	84	229(41%)
国外ブランド	64	70	53	187(25%)
ブランド不明	57	31	53	141(32%)
月別合計	196	171	190	557(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。

2014 年 2 月半ばに、検索エンジンの検索連動型広告を使用して国内金融機関を装ったフィッシングサイトに誘導する手法が確認されました。不正な広告は広告欄の最上位に表示され、金融機関の正規サイトの URL を記載しているため、画面上の表示を見ただけではフィッシングサイトへ誘導するものとは分からないようになっていました。フィッシングの被害を防ぐためには、パスワードなど機微な情報の入力に先立って URL が正規サイトのものであるか確認するなどの基本的な対策に加え、金融機関が提供している場合にはワンタイムパスワードサービスやフィッシング対策ソフトウエアを利用するなどの対策が重要です。

前四半期に引き続き、国内通信事業者が動的に割り当てる IP アドレスを持った、国内および海外のオンラインゲームサービスと国内金融機関を装ったフィッシングサイトに関する報告を非常に多く受領しました。国内金融機関を装ったフィッシングサイトは 1 月末から 2 月後半にかけて確認されない期間がありましたが、2 月末以降には、前四半期にも見られた海外の Web サイトから誘導されるフィッシング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 43%、国外が 57%であり、前四半期(国内 43%、国外 57%)と同じ割合になっています。

本四半期に報告が寄せられた Web サイト改ざんの件数は、1501 件でした。前四半期の 1604 件から 6%減少しています。

2014 年 2 月後半に国内の複数の Web サイトが改ざんされ、Internet Explorer の当時未修正だった脆弱性(CVE-2014-0322)を攻撃する不正なファイルが設置されていました。改ざんされた Web サイトは、埋め込まれた iframe や JavaScript によって、脆弱性を攻撃する swf ファイルや jar ファイルなどに利用者を誘導して、閲覧した PC をマルウエアに感染させる仕組みになっていました。攻撃によって感染するマルウエアを分析した結果、海外のサーバへの端末情報の送信や、攻撃者がマルウエアへの命令に使用していたと考えられる国内ブログサービスの特定のページにアクセスして、何らかの情報を取得するなどの挙動を確認することができました。

一方で、不正な iframe や JavaScript がページに挿入された Web サイトに関する報告も大量に受領しています。

Web サイト改ざん等のインシデントを認知された場合は、JPCERT/CC にご報告ください。JPCERT/CC では、当該案件に関して攻撃元への対応依頼等の必要な調整を行うとともに、同様の被害の拡大を抑えるため、攻撃方法の変化や対策を分析し、随時、注意喚起等の情報発信を行います。

インシデントによる被害拡大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 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：12 件　https://www.jpcert.or.jp/at/

2014-01-15　2014 年 1 月 Microsoft セキュリティ情報に関する注意喚起 (公開)
2014-01-15　Adobe Flash Player の脆弱性 (APSB14-02) に関する注意喚起 (公開)
2014-01-15　Adobe Reader 及び Acrobat の脆弱性 (APSB14-01) に関する注意喚起 (公開)
2014-01-15　2014 年 1 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)
2014-01-15　ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起 (公開)
2014-02-05　Adobe Flash Player の脆弱性 (APSB14-04) に関する注意喚起 (公開)
2014-02-10　Apache Commons FileUpload および Apache Tomcat の脆弱性に関する注意喚起 (公開)
2014-02-12　2014 年 2 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)
2014-02-20　2014 年 2 月 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起 (公開)

2014-02-21　Adobe Flash Player の脆弱性 (APSB14-07) に関する注意喚起 (公開)
2014-03-12　2014 年 3 月 Microsoft セキュリティ情報 (緊急 2 件含) に関する注意喚起 (公開)
2014-03-25　2014 年 3 月 Microsoft Word の未修正の脆弱性に関する注意喚起 (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 42 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。

2014-01-08　IME のクラウド関連機能に関するセキュリティ上の注意
2014-01-16　NTP サーバのアクセス制限機能を活用しましょう
2014-01-22　マイクロソフト MD5 ハッシュの利用制限プログラム配信について
2014-01-29　情報セキュリティ月間
2014-02-05　Web サイト運用体制を確認する
2014-02-13　ISC BIND 9.6-ESV サポート終了
2014-02-19　Internet Week 2013 のプレゼンテーション資料公開
2014-02-26　ISC BIND 10 初期開発プロジェクト終了
2014-03-05　Hong Kong Security Watch Report
2014-03-12　Phishing Activity Trends Report, 3rd Quarter 2013
2014-03-19　IPA、2014 年版 情報セキュリティ 10 大脅威を公開
2014-03-26　Technical Guidance for Handling the New CVE-ID Syntax

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。

【歴史認識に関連するサイバー攻撃への対応】
特定の歴史上の出来事等が起きた日、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活発化します。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 等と連携して、攻撃準備活動等について特に注意深く情報収集を行っています。

本四半期では、韓国が「3.1 節」として祝う 3 月 1 日が特異日に当たりました。2010 年には、この日に「2 ちゃんねる」に対する大規模な DDoS 攻撃が行われ、一部のサーバがサービス不能状態になるなどの影響が発生しました。2011 年以降は大規模な攻撃はありませんでしたが、2014 年 2 月下旬に韓国のサイトにおいて、「2010 年と同等の攻撃を行う」といった呼びかけがなされたことを受け、JPCERT/CC では、KrCERT/CC(KISA)との非常連絡態勢を整えてモニタリング情報を共有するなど、サイバー攻撃発生に備えた対応態勢をとりました。併せて、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・分析態勢を強化しました。本件では、予告されていた攻撃は確認されず、深刻な被害は発生しなかったと見受けられます。

【ntpd の monlist 機能を使った DDoS 攻撃に関する調査】
本四半期、NTP サーバまたは NTP 機能を提供するネットワーク機器等を悪用したと思われる DDoS 攻撃が発生しました。NTP Project が提供する ntpd の一部のバージョンには、NTP サーバの状態を問い合わせる機能(monlist)が実装されており、同機能はトラフィック増幅器として遠隔から DDoS 攻撃に使用される可能性があることがセキュリティ研究者によって指摘されています。

JPCERT/CC では、ntpd の monlist 機能を使った DDoS 攻撃に関するインシデント報告を受け、JPCERT/CC が運用するインターネット定点観測システム(TSUBAME)において NTP サーバを探索するパケットが増加していることから、「ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起」を発行し広く注意を呼びかけました。

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

JPCERT/CC は TSUBAME の構築と、さまざまな地域に広く観測用センサーを設置し、各地域の CSIRT と共同で分析をするためのプロジェクト(TSUBAME プロジェクト)の事務局を担当しており、システムや

センサーの定常稼働に努めています。2014 年 3 月末時点で、観測用センサーをアジア・太平洋地域の 23 地域に設置しています。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 URL をご参照ください。

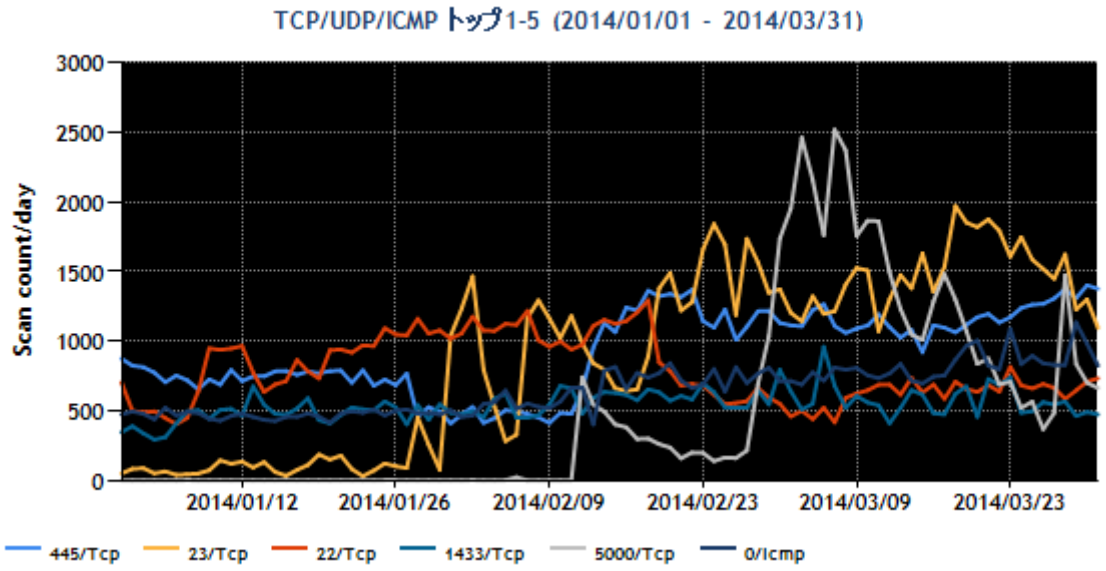
TSUBAME(インターネット定点観測システム)
https://www.jpcert.or.jp/tsubame/index.html

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。

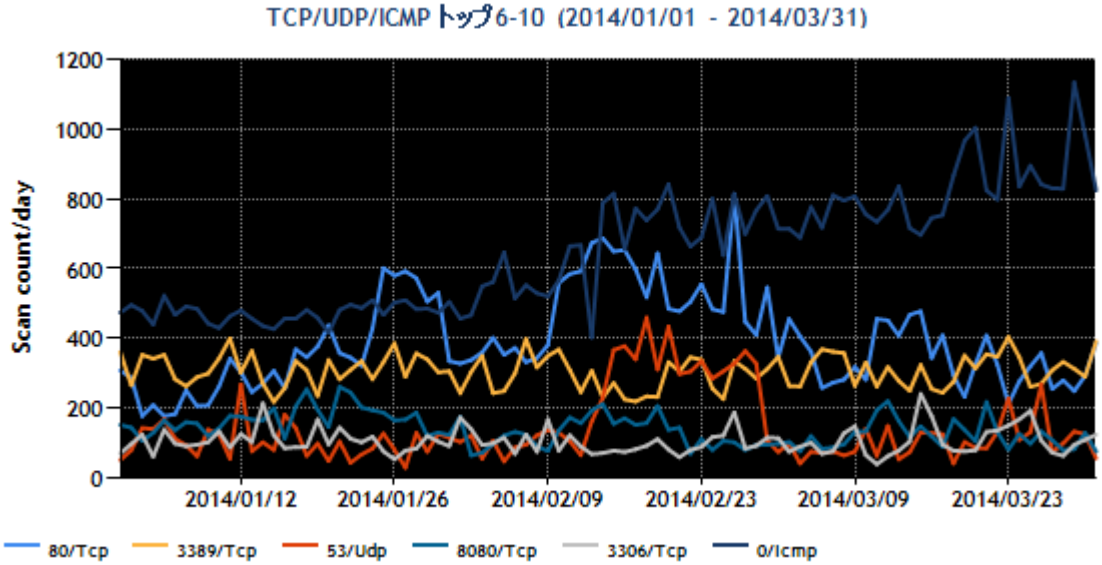
また、主に日本企業のシステム管理者等の方々に、自ネットワークに届いた意図しないパケットと比較してもらうことを目的とし、日本国内のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。

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

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。

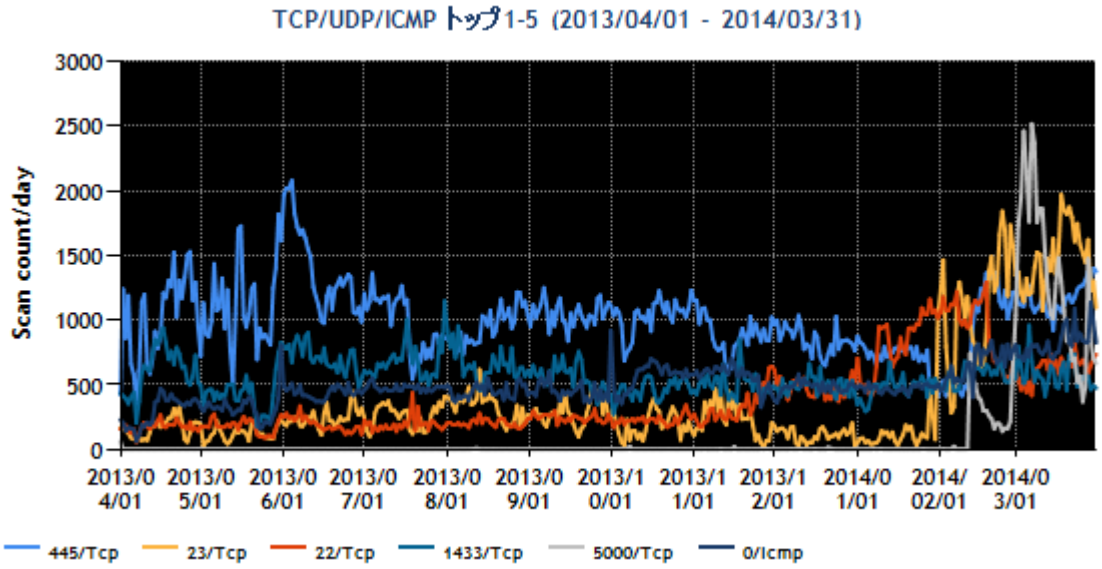


[図 1-1 宛先ポート別グラフ トップ 1-5(2014 年 1 月 1 日-3 月 31 日)]

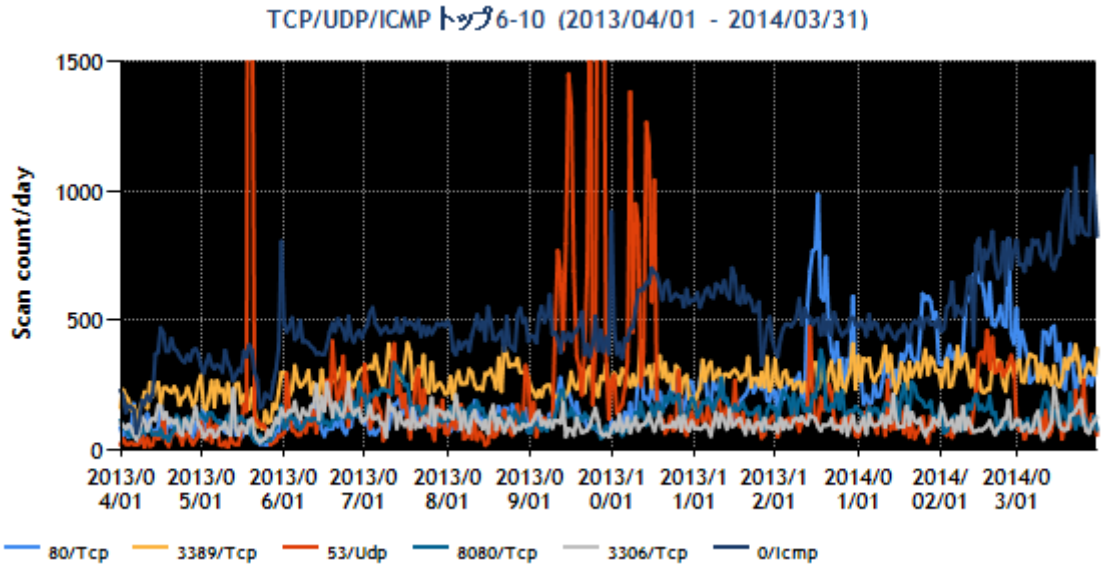


[図 1-2 宛先ポート別グラフ トップ 6-10(2014 年 1 月 1 日-3 月 31 日)]

また、過去 1 年間(2013 年 4 月 1 日～2014 年 3 月 31 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 4 月 1 日-2014 年 3 月 31 日)]



[図 1-4 宛先ポート別グラフ トップ 6-10 (2013 年 4 月 1 日-2014 年 3 月 31 日)]

2 月頃から 5000/TCP と 23/TCP 宛のパケットが急増しています。日本の IP アドレスから発信されたパケットも観測されています。これは、国外製のネットワークカメラなどによるスキャン活動と見られます。JPCERT/CC では、開発元地域の National CSIRT と連携し、ベンダに対応を依頼しました。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、日々観測情報の分析を行っており、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。

日本国内の組織に割り当てられた IP アドレスから送信された、SSH サーバ宛ての特徴的なパケットが本四半期も観測されました。JPCERT/CC は、当該 IP アドレスの管理者に情報を提供し、SSH サーバを探索するスキャンや辞書攻撃等を行う不審なツールがインストールされていないか調査を依頼しました。その後、当該管理者から「当該サーバには何者かによる侵入の痕跡があり、サーバ上に SSH サーバを探索するためのツールや操作ツールが設置されて遠隔から操作可能な状態になっており、命令を受けてスキャンを行っていたことを確認したため、必要な対応を行った」との連絡をいただきました。

1.3.3. TSUBAME トレーニングの実施

本四半期には、TSUBAME プロジェクトに参加している ID-SIRTII/CC およびインドネシア国内の大学(ACADEMIC CSIRT)向けに、次の要領で、TSUBAME トレーニング(TSUBAME システムの機能の説明と TSUBAME の情報を活用した分析方法の紹介、TSUBAME センサーの設置や運用方法の説明など)を実施しました。

日時：2014 年 3 月 5 日 (水)～2014 年 3 月 7 日 (金)
場所：インドネシア ジャカルタ (ID-SIRTII/CC 会議室)
参加人数：36 名(ID-SIRTII/CC 10 名、ACADEMIC CSIRT 26 名)
内容：
- 3 月 5 日
  - TSUBAME システムの概要
  - TSUBAME センサーセットアップと運用について
  - TSUBAME システムの機能説明
    - TSUBAME portal サイトの使い方、TSUBAME Web サイトの使い方
- 3 月 6 日
  - TSUBAME システムを活用した分析事例の紹介
    - 23/TCP (Telnet)、8443/TCP (Plesk Panel)、5060/UDP (SIP)、3389/TCP (RDP)、123/UDP (NTP)、53/UDP (DNS), 1900/UDP・5000/TCP (UPnP)
- 3 月 7 日
  - 全体の質疑応答、参加者へのトレーニングに関するヒアリング
  - Academic CSIRT の今後の展開についてのヒアリング
  - トレーニング修了証書授与

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

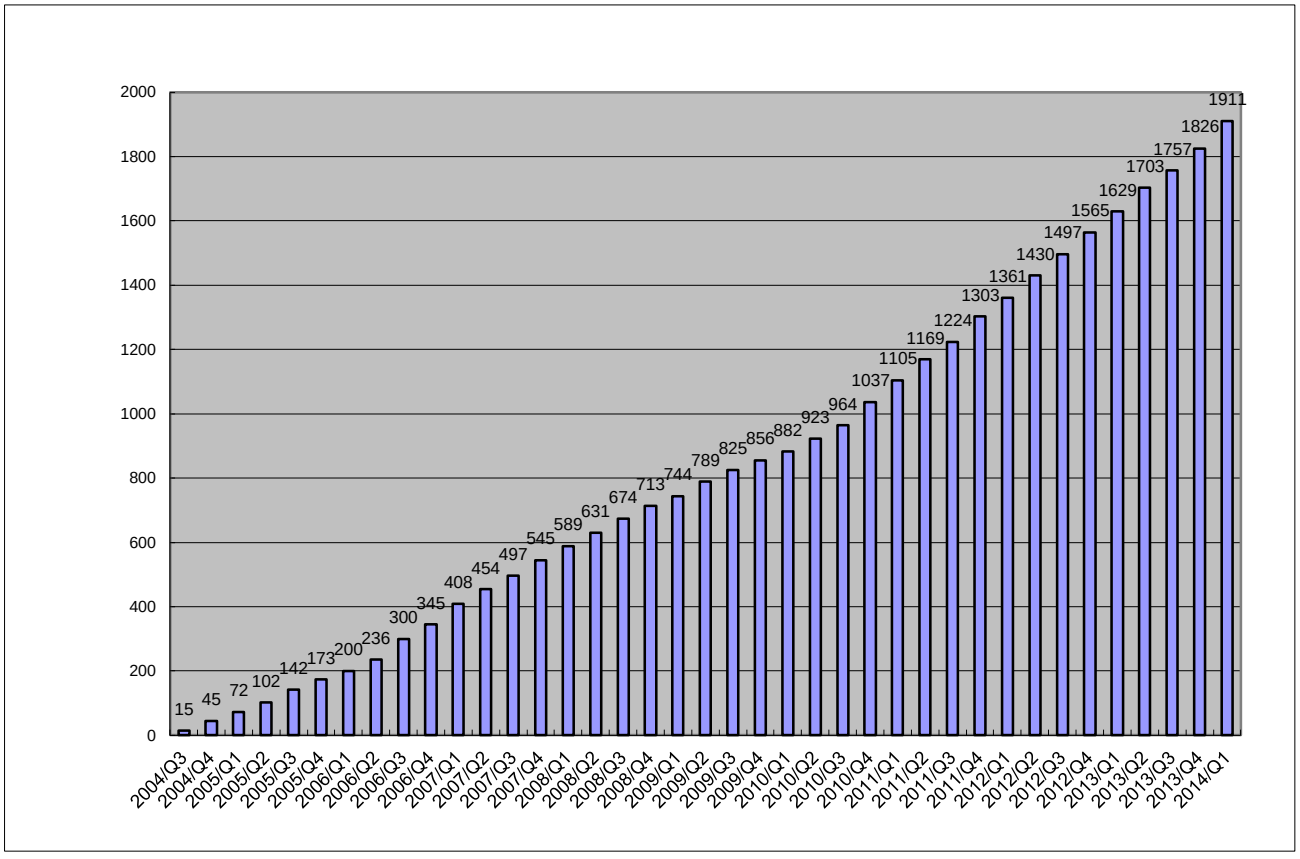
JPCERT/CC は、経済産業省告示「ソフトウエア等脆弱性情報取扱基準」(以下「本基準」といいます。)に基づいて製品開発者とのコーディネーションを行う「調整機関」に指定されており、本基準を踏まえて取りまとめられた「情報セキュリティ早期警戒パートナーシップガイドライン」に従って、対象となる脆弱性に関係する製品開発者の特定、脆弱性関連情報の適切な連絡、開発者による脆弱性の検証等の対応や脆弱性情報の公表スケジュール等に関する調整を行い、原則として、調整した公表日に JVN を通じて脆弱性情報等を一般に公表しています。JVN で公表している脆弱性情報は、本基準に従って国内で届け出られた脆弱性に関するもの(「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 CERT-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、これには特別に、原典の識別子と対応した「JVNTA」に続く 2 桁数字－3 桁数字の形式の識別子(例えば、JVNTA12-345)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 85 件(累計 1911 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 URL 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 32 件(累計 851 件)で、累計の推移は[図 2-2]に示すとおりです。32 件のうち、21 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でした。

本四半期には、海外 OSS 製品の開発者が脆弱性関連情報のハンドリング中に誤って脆弱性関連情報を公のメーリングリストに流すというアクシデントが発生しました。製品開発者側で急遽アドバイザリを公表したため、JPCERT/CC においても製品開発者および発見者と調整の協議を行い、短時間のうちに本

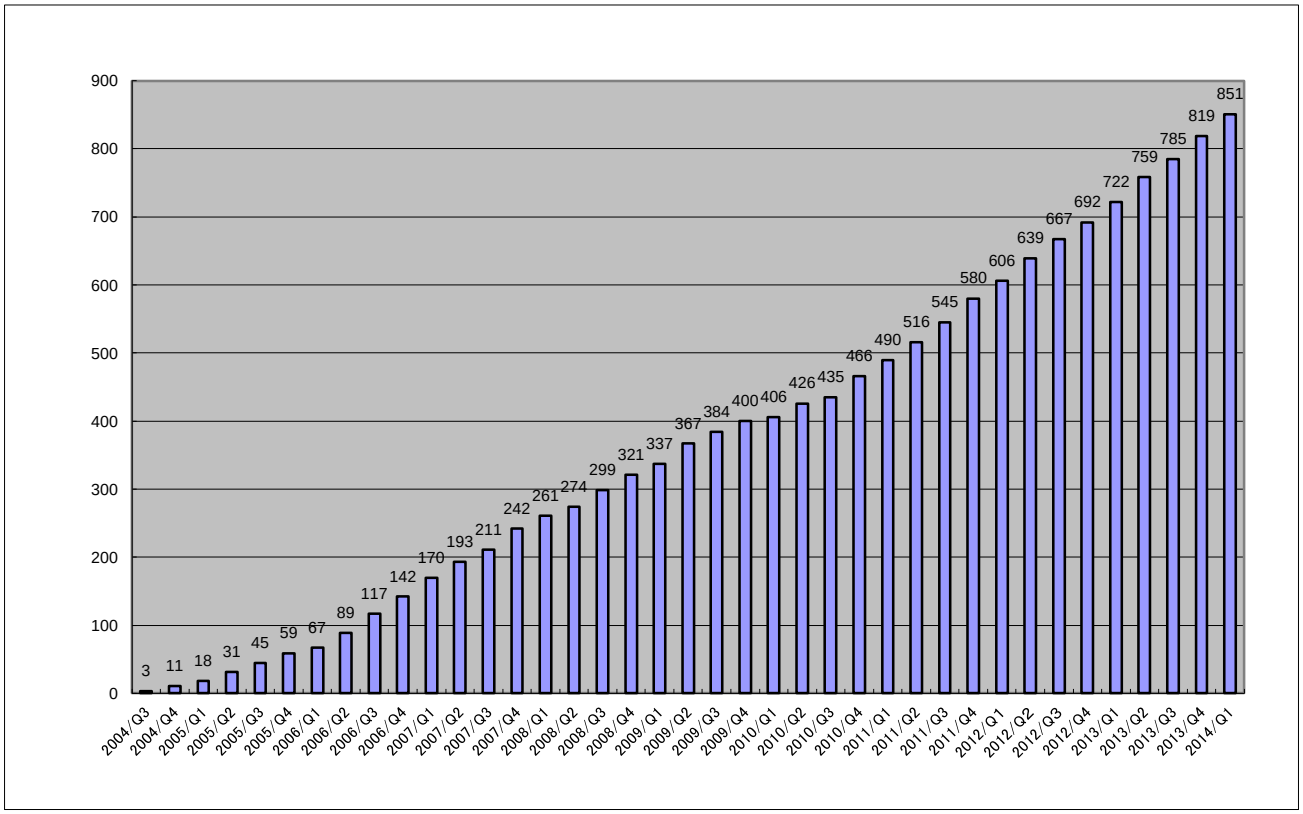
脆弱性情報を公表しました。不測の事態の中で国内外の関係者との迅速な調整ができた背景には、情報セキュリティ早期警戒パートナーシップの海外製品開発者への浸透があると考えられます。

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 6 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 19%を占めるまでに増加しています。

Android およびその関連製品をはじめとするモバイル関連製品の脆弱性情報の届出は 2012 年度から増加傾向にあり、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 12 件、Android 向け Web ブラウザに関する脆弱性情報が 2 件と、全体の約 44%を占めるに至りました。

モバイル関連以外の製品で、公表件数が多かった脆弱性情報は、グループウェア製品に関するものが 6 件、OSS 製品に関するものが 4 件、E コマース製品に関するものが 2 件、CAD 製品に関するものが 2 件でした。

JPCERT/CC は、今後も引き続き国内外の関係者との調整を行い、脆弱性問題への速やかな対応の促進に努めてまいります。

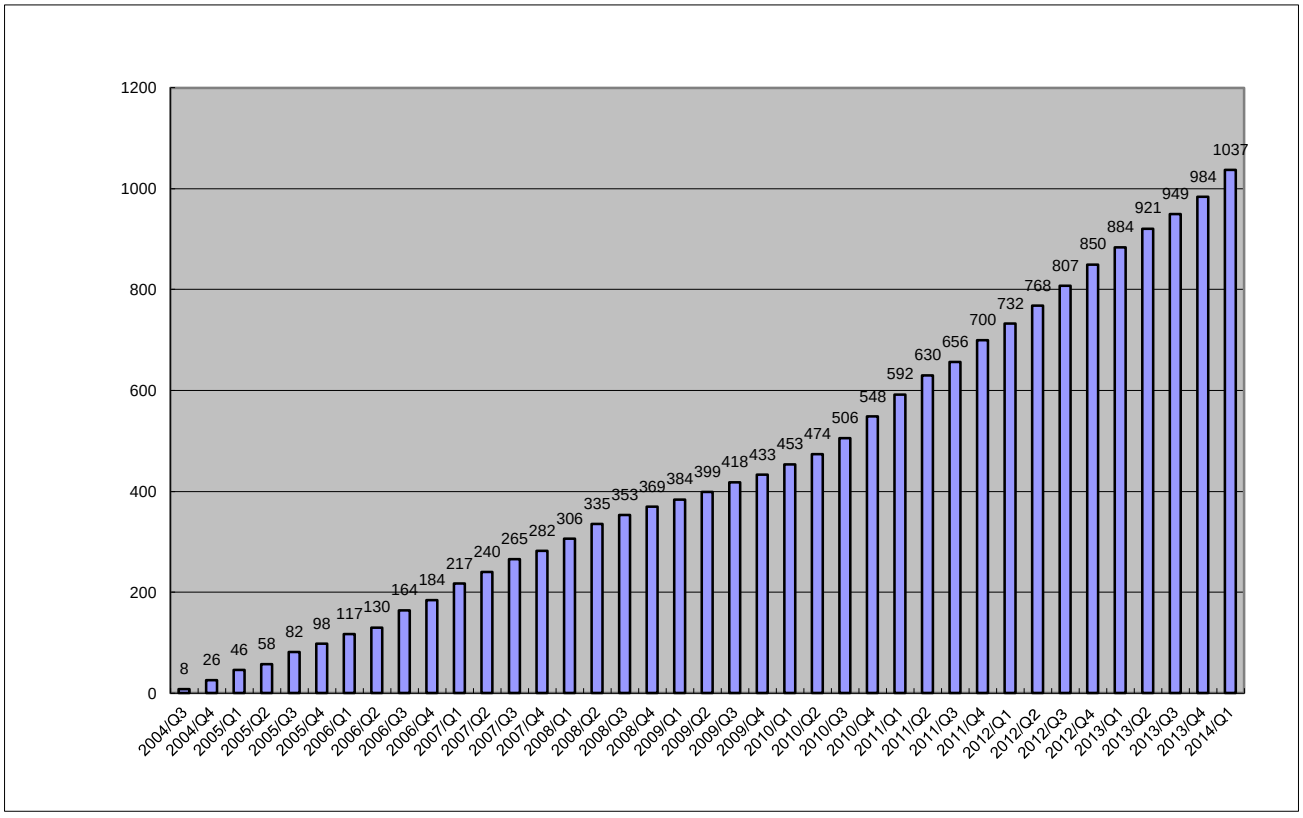


[図 2-2 公表を行った国内取扱脆弱性情報の累積件数]

本四半期に公表した国際取扱脆弱性情報は 53 件(累計 1037 件)で、累計の推移は[図 2-3]に示すとおりです。このうち US-CERT の脆弱性注意喚起(JVNTA から始まる識別子を付して公表したもの)の 1 件は、Microsoft の OS 製品に関するサポート終了の注意喚起でした。

また、CERT/CC が公表した脆弱性情報は 52 件あり、このうち ntp の脆弱性と、Microsoft Internet Explorer の脆弱性については、公表の時点で攻撃にも使われている特に深刻度が高いものでした。この他、モバイルルータ等の小型デバイス製品が 7 件、企業向けネットワーク機器およびサーバ製品が 11 件(うち、DELL 製品が 3 件)、NAS 関連製品が 5 件、OSS 製品が 2 件ありました。さらに、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 7 件ありました。本四半期に公表した国際取扱脆弱性情報の特徴としては、ネットワーク機器関連製品(個人向けと企業向けの双方を含む。)の脆弱性情報が多く、全体の 40%を占めました。

なお、横河電機製の制御システムに関する脆弱性情報の公表が 1 件ありましたが、これは制御システムの脆弱性情報ハンドリングにおいて JPCERT/CC が ICS-CERT と連携して開発者との調整を行い、公表に至った初めてのケースとなりました。



[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

本基準に基づいて脆弱性が報告されたものの、しかるべき呼び掛けをしても調査と対策をしていただくべき製品開発者に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 152 件(製品開発者数としては 92 件)を公表し、21 件(製品開発者の数としては 14 件)の調整が再開でき、脆弱性関連情報の取り扱いにおける「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 131 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。

こうした対応によってもなお製品開発者への連絡が取れない脆弱性に関し、再現性を確認できた場合には、利用者のリスクを低減するため、脆弱性情報を JVN で公表するための手順や手続き等の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、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。2011 年より増加傾向にある Android 関連の脆弱性の調整活動の中では、Android 関連製品を開発している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。

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、CVE 採番機関)として認定されています。本四半期は、JVN 上で公表した脆弱性情報のうち 33 件に CVE 識別子が付与されており、そのうち 31 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 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/archives/2010_news.html#jun232010a
CVE Numbering Authorities
https://cve.mitre.org/cve/cna.html
About CVE
https://cve.mitre.org/about/index.html

2.4. 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 URL をご参照ください。

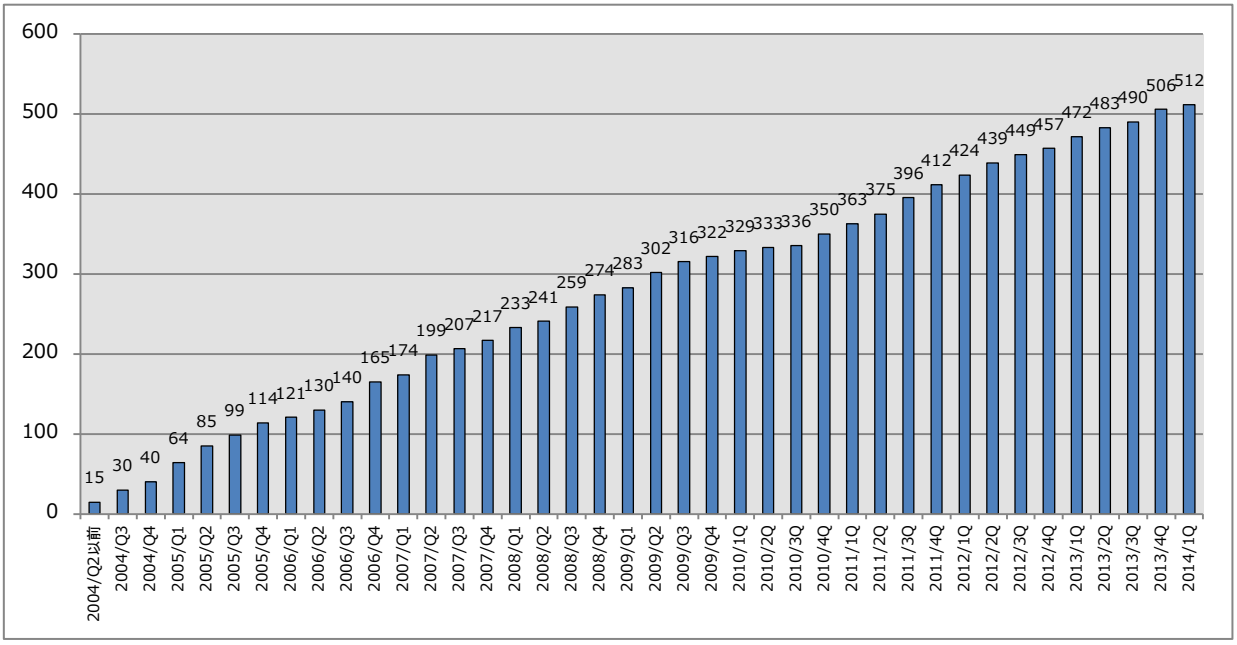
独立行政法人情報処理推進機構(IPA) 脆弱性対策
http://www.ipa.go.jp/security/vuln/

2.4.2. 日本国内製品開発者との連携

本基準では、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 3 月 31 日現在で 512 となっています。

登録等の詳細については、次の URL 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]

2.4.3. 製品開発者との定期ミーティングの実施

JPCERT/CC では、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報ハンドリング業務に関する製品開発者との意見交換、また製品開発者間の情報交換を目的として、脆弱性情報ハンドリングにご協力いただいている製品開発者の皆さまとのミーティングを定期的に開催しております。

本四半期は2014年3月7日にミーティングを開催し、脆弱性情報ハンドリングに関する活動状況の報告、海外における脆弱性やセキュリティに関する動向および技術情報等を紹介するとともに、それらに関する製品開発者との意見交換、脆弱性情報ハンドリング業務における課題等についてのディスカッションを行いました。

[図 2-5 製品開発者との定期ミーティングの様子]

2.5. セキュアコーディング啓発活動

2.5.1. Android セキュアコーディングルールを作成中

前四半期に続き、Android アプリの脆弱性と脆弱性の原因となるコーディング上のアンチパターンに関する調査・研究を行いました。セキュアな Android アプリ開発に役立てていただくため、調査の過程で得られた知見をコーディングルール化する作業を進めています。本四半期は下に示したルールを新たに 1 件追加しました。

The CERT Oracle Secure Coding Standard for Java
50. Android (DRD)
https://www.securecoding.cert.org/confluence/x/H4ClBg

追加したルール：
DRD015-J. Consider privacy concerns when using Geolocation API
https://www.securecoding.cert.org/confluence/x/G4DkBw

これでルールは合計 9 件となり、各ルールでは、脆弱なコード(アンチパターン)とその修正例とともに、JVN 等で公開されている関連する事例や、参考文献、関連する Java セキュアコーディングルール等も紹介しています。セキュアな Android アプリ開発の方法に関する情報源の一つとして活用していただければ幸いです。

今後も新たなルールを追加していくとともに、公開済みのルールも随時アップデートしていく予定です。ルールの内容に関するコメントや改善案については Wiki に直接コメントするか、もしくは、secure-coding@jpcert.or.jp にお送りください。ルールの改善に活用させていただきます。

2.5.2. Android セキュアコーディングに関する SEI テクニカルレポートが公開される

カーネギーメロン大学ソフトウェア工学研究所(SEI)の Secure Coding Initiative では Mobile SCALe と呼ばれるモバイルアプリのセキュリティと静的解析に関する研究プロジェクトが進められており、JPCERT/CC もこのプロジェクトに参加して Android ルール開発等を担当しています。先般、このプロジェクトの成果としてテクニカルレポート"Mobile SCALe: Rules and Analysis for Secure Java and Android Coding"が公開されました。

Mobile SCALe: Rules and Analysis for Secure Java and Android Coding
http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=69225

テクニカルレポートでは、Mobile SCALe プロジェクトのメンバが作成に携わった書籍『Java Coding Guidelines: 75 Recommendations for Reliable and Secure Programs』、および、Android セキュアコーディングルール、Android アプリ解析ツールの開発の 3 つのトピックスが報告されています。

2.5.3. 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 6 回「動的メモリ管理に関する脆弱性」(公開： 1 月 23 日、執筆：戸田 洋三)
http://www.atmarkit.co.jp/ait/articles/1401/23/news002.html

2.5.4. Android アプリ解析ツールの機能拡張用プラグインを開発するためのチュートリアルを作成中

JPCERT/CC の脆弱性解析チームでは、Android アプリを解析するために Android アプリ解析ツール「JEB」を使用しています。その際の解析業務の負担を減らし効率化を図るために、JEB の機能を拡張するプラグインに関する調査／研究を行っており、プラグイン開発に役立てていただくために、その過程で得られた知見をまとめてチュートリアルを作成する作業を進めています。

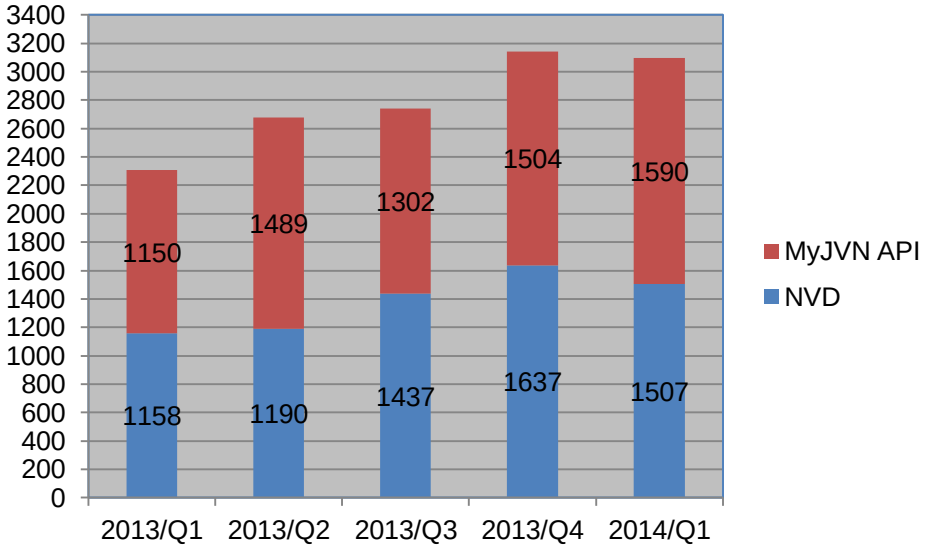
作成したチュートリアルとプラグインは、順次公開する予定です。

2.6. VRDA フィードによる脆弱性情報の配信

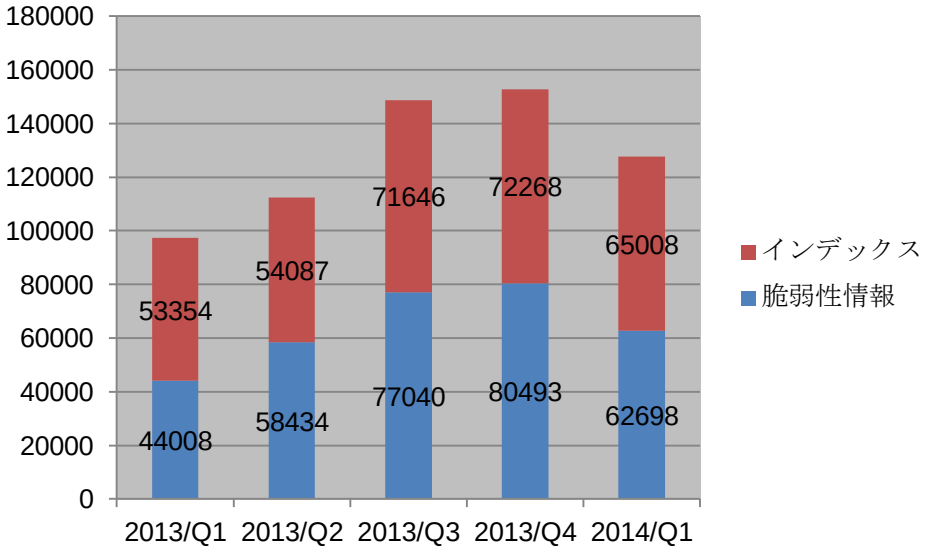
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST(National Institute of Standards and Technology)の NVD(National Vulnerability Database)を外部データソースとして利用した、VRDA(Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の URL 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 2-6]に、VRDA フィードの利用傾向を[図 2-7]と[図 2-8]に示します。[図 2-7]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 2-8]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。

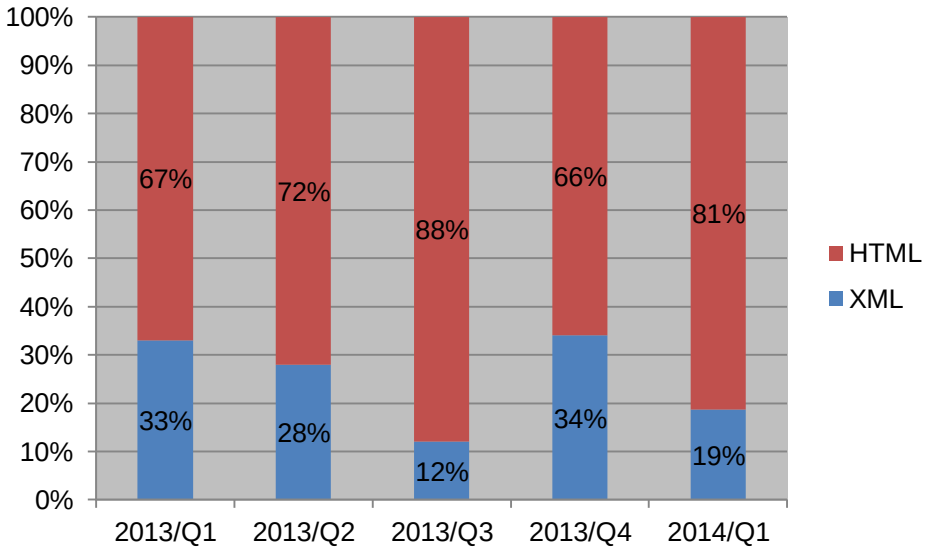


[図 2-6 VRDA フィード配信件数]



[図 2-7 VRDA フィード利用件数]

[図 2-7] 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、約 10%減少しました。脆弱性情報の利用数についても 20%以上前四半期と比較して減少しました。



[図 2-8 脆弱性情報のデータ形式別利用割合]

[図 2-8] 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、前四半期に大きく増加した XML 形式の利用割合が 19%に減少しました。

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。分析対象はウイルスやボット等のマルウエアに限らず、攻撃に使われるツールをはじめとするプログラムや攻撃手法等(アーティファクト)にまで及び、それら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。

また、JPCERT/CC は、アーティファクト分析で得た知見を国内外で対策活動を行う組織と共有することが重要であると考えています。JPCERT/CC が取り扱った個別のインシデントの情報を第三者に開示することはありませんが、調査・分析により判明した攻撃手法やその調査・分析のために使った技術情報等を、適切に活用していただける組織と共有する活動も行っています。

3.1. インターネットバンキングの情報を窃取するマルウエア Citadel の技術情報共有

JPCERT/CC では、インターネットバンキングの情報を窃取する機能を持つマルウエアである Citadel について詳細な解析を実施し、その技術情報を複数の関係組織と共有しました。さらに、その技術情報をより多くの組織で活用していただくことを目的に、2 月 17 日から 2 日間の日程で開催された日本発の情報セキュリティ国際会議である「CODE BLUE」にて発表しました。このように、実際のインシデント対応に必要な解析技術をコミュニティ全体で共有していくことが、円滑なインシデント対応を可能にし、セキュリティの向上につながると考えています。

CODE BLUE
http://www.codeblue.jp/

3.2. 攻撃に関連するサイトの情報を共有する取組

マルウエアの通信先や改ざんされた Web サイトで誘導される先等の、攻撃に関連するサイトに関する情報を収集して共有することは、インシデントへの対策や調査・解析を行う上で非常に有用です。今日、そのようなサイトの情報を収集する取組が複数あり、インシデント対応における重要な調査ツールとしての位置付けを確立しつつあります。

JPCERT/CC では、アーティファクト分析等で判明した攻撃に関連するサイトの情報として、FQDN とその名前解決で得られた情報を蓄積し、インシデントの影響を受ける可能性のある組織に対して提供しています。JPCERT/CC は、CSIRT との連携活動の中でこの取組を進めるために、攻撃に関連する FQDN の情報を収集・蓄積・共有するシステム「FIT(FQDN Indicator Tracker)」の開発を行い、連携組織に対して Web サービスとして提供する準備を進めてきました。本四半期においては、3 月 21 日に開催された APCERT Public Conference 2014 で FIT について発表を行いました。FIT で共有された情報が、インシデントの早期発見や被害の極小化に役立てられるよう、普及を図っていきたいと考えています。

APCERT Public Conference 2014
http://www.twncert.org.tw/apcert2014/

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し、JPCERT/CC からのお知らせとともにまとめ、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 4 回(2 月 3 日、3 月 4 日、3 月 13 日、3 月 31 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 358 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 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. 制御システム関連のインシデント対応および情報収集分析活動

本四半期に制御システムに関連するとして報告されたインシデントの件数は 2 件でした。

また、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 562 件でした。これらの中から、国内の制御システム関係者にとって新しく、有益であると考えられる情報を厳選した上でニュースレターの形で配信しました。

さらに、一般社団法人日本ガス協会が実施したサイバー攻撃対応演習に、プレーヤー、演習進行役、有識者として参加し、演習遂行の支援を行うとともに、演習に参加したガス事業者の方々とインシデントレスポンスについての意見交換を行い、相互理解を深めました。

4.3. 関連団体との連携

定期的に開催されている 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)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。

4.4. 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、JPCERT/CC に対して、日本語版 SSAT に関しては 2 件、J-CLICS に関しては 11 件の利用申込みがありました。直接配布件数の累計は、日本語版 SSAT が 157 件、J-CLICS が 191 件となりました。

4.5. 制御システムベンダにおける脆弱性取扱の社内体制整備促進

昨年 10 月より「制御システムベンダにおける脆弱性取扱の社内体制整備促進検討会」を開始しました。全 7 回を終了し、制御システムベンダで脆弱性対応を行う場合に考えられる「必要な機能」「機能を担う体制の在り方」「実現に関わる課題」等を中心に検討会を行い、発見された脆弱性に対する情報流通の体制を社内で整備するため、社内関係組織や会社幹部への説明などで必要となることを想定した各種の資料を作成しました。

4.6. 制御システムセキュリティカンファレンス 2014 開催

制御システムセキュリティカンファレンス 2014 を 2 月 5 日(水)に東京(品川)で開催し、264 名の方にご来場いただきました。今回で 6 回目となる本カンファレンスでは、「アウェアネスからアクションへ」をテーマに講演者の方々から制御システムセキュリティへの取組について講演いただき、今後のセキュリテ

ィ改善活動に繋がるような情報交換に役立つプログラム構成としました。プログラム等の詳細については、次の URL をご参照ください。

制御システムセキュリティカンファレンス 2014
https://www.jpcert.or.jp/event/ics-conference2014.html

制御システムセキュリティカンファレンス 2014 においての講演資料
https://www.jpcert.or.jp/present/#year2014

4.7. 講演活動

2014 年 1 月から 3 月にかけて、一般社団法人日本ガス協会の実施する情報セキュリティ・保安通信説明会にて「制御システムセキュリティ」と題する発表を行いました。また、2014 年 2 月 25 日に東京で開催された@IT Security Live UP!において「他人事ですまない危うい現実 ― 制御システム・セキュリティ」と題した講演を行いました。

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

ISO/IEC JTC-1/SC27 の WG3 において進められてきた、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)の 2 つの国際標準の策定作業に参加してきました。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、外側からは見えない活動等を含む、ベンダ内部での対応を規定しています。

「脆弱性情報の開示」については、国際標準最終草案(FDIS：Final draft of International Standard)が国際投票で承認され、2 月に国際標準として発行されました。「脆弱性取扱手順」については、既に 2013 年 11 月に国際標準として発行されており、2008 年 4 月から始まった脆弱性の取扱に関する ISO/IEC JTC-1/SC27 における標準化作業はすべて完了しました。JPCERT/CC では SC27 国際会議への参加ならびに日本の標準化組織である情報規格調査会を通じて、これらの標準がわ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と整合したものとなるよう努めてきました。

5.2. インシデント管理の国際標準化活動への参加

現在 ISO/IEC JTC-1/SC27 の WG4 では、情報セキュリティインシデント管理に関する国際標準 27035:2011 を下記の 3 つの標準からなるマルチパート標準へと改訂する作業が進められています。

27035-1. インシデント管理の原理(Principles of Incident Management)
27035-2. インシデント対応の計画と準備のためのガイドライン(Guidelines to Plan and Prepare for

Incident Response)

27035-3. 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)

JPCERT/CC は 27035:2011 の策定段階からこの標準化活動に関わっています。

本四半期は、2014 年 4 月に香港で開催される SC27 国際会議に先立ち、各パートの 4th Working Draft に対する日本のコメントを作成し、SC27 事務局に提出しました。

日本からは、27035-1 に 14 件、27035-2 に 15 件、27035-3 については 8 件のコメントを提出しています。日本以外の国ではスウェーデン、英国、米国、中国からコメントが寄せられているほか、SC27 とリエゾン関係にある FIRST(Forum of Incident Response and Security Teams)からもコメントが提出されています。

提出したコメントの処理については、次回の香港会議に日本の代表団の一員として参加し、各国の代表と議論を行う予定です。

JPCERT/CC では、インシデントの管理と対応に関連した 3 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における活動を通じて、引き続き、この国際標準がわが国の CSIRT の取組と整合性の取れたものとなるよう努めていく所存です。

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。

本四半期の活動は、メールでの問合せへの対応及び次年度に向けた計画立案が中心でした。

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等、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. 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 URL をご参照ください。

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

6.2.1.1 APCERT Steering Committee 会議の実施

Steering Committee は 1 月 15 日、2 月 12 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を行いました。JPCERT/CC は議長チームおよび事務局として、本会議の主導およびサポートを行いました。

6.2.1.2. APCERT 合同サイバー演習 (APCERT Drill 2014) に参加 (2014 年 2 月 19 日)

APCERT は、サイバー攻撃への即時対応能力を確認するため、合同サイバー演習を実施しました。本演習は、アジア太平洋地域で発生し、国境を越えて広範囲に影響を及ぼすインシデントへの対応における各経済地域 CSIRT 間の連携の強化を目的として、毎年実施されています。

9 回目となる今回の合同サイバー演習のテーマは「サイバー攻撃への地域連携による対処」でした。APCERT の加盟チームのみならず、イスラム諸国会議機構に加盟する CSIRT の集まりである OIC-CERT からエジプト、パキスタン、ナイジェリア、欧州からドイツのチームも加わって、21 の経済地域から計 24 チームが参加しました。

JPCERT/CC は、この演習にプレーヤー(演習者)として参画するとともに、ExCon と呼ばれる演習の進行調整役も務め、スムーズな演習の実施を支えました。

6.2.1.3. APCERT 年次総会 2014 への参加(2014 年 3 月 18 日-21 日)

アジア太平洋地域の CSIRT コミュニティである APCERT の年次総会が台北で開催され、JPCERT/CC を含む 21 の加盟チームが参加しました。会合の概要は、次のとおりです。

1) 日程：
3/18(火) 終日：APCERT 運営委員会(SC Meeting) / APCERT ワーキンググループ会合
3/19(水) 終日：各種ワークショップ
3/20(木) 午前：APCERT 年次総会(Annual General Conference)
午後：APCERT カンファレンス(Closed Session)
3/21(金) 終日：APCERT カンファレンス(Open Session)
2) 場所：Le Meridien Hotel Taipei, Howard Civil Service International House Taipei
3) 概要
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・研究活動などを共有することを目的に、毎年開催されています。今年は“Preparing for a

Better Future – The role of CSIRT Community”というテーマで開催され、APCERT が目指す「safe, clean and reliable」なサイバースペースの構築に向けた第一歩として、サイバーセキュリティに関する比較可能で堅牢な定量評価の仕組みの必要性がチーム間で意識共有されました。

APCERT カンファレンスにおいては各チームの取組の紹介やモバイルセキュリティ、クラウドセキュリティ、ビッグデータ、標的型攻撃等に関する専門家の講演が行われました。

APCERT 年次総会では、運営委員会(Steering Committee)のメンバの一部とともに、APCERT 議長チーム/副議長の改選が行われ、JPCERT/CC は議長チーム(4 期目、任期は 2015 年まで)に再選されました。JPCERT/CC は、引き続き APCERT の代表としてさまざまな活動をリードすることとなりました。

[図 6-1 APCERT 年次総会集合写真]

6.2.1.4. APCERT を代表しての会議出席

・APRICOT 2014

JPCERT/CC は 2 月 18 日から 28 日に開催された APRICOT 2014(以下「APRICOT」といいます。)に 24 日から参加しました。26 日に設けられた APCERT による特別セッション枠において、APCERT 議長として「サイバースペースのリスク削減アプローチ」をテーマとしたワークショップの議論を主導しました。また、DNS オープンリゾルバ問題への JPCERT/CC の取組について、ワークショップ内で発表を行いました。APRICOT についての詳細は、次の URL をご参照ください。

APRICOT 2014
https://2014.apricot.net/

・Cyber Intelligence Asia

JPCERT/CC は APCERT を代表して Cyber Intelligence Asia 2014(以下「Cyber Intelligence Asia」といいます。)に参加し、加盟各チーム間の協力関係およびサイバースペースのクリーンアップ活動、アジア太平洋のサイバー脅威動向について講演を行いました。Cyber Intelligence Asia についての詳細は、次の URL をご参照ください。

Cyber Intelligence Asia 2014
http://www.intelligence-sec.com/events/cyber-intelligence-asia-2014

・ASEAN Regional Forum

JPCERT/CC は 3 月 25 日から 26 日に開催された ASEAN Regional Forum(以下「ARF」といいます。)の Cyber Confidence Building Measures(CBM) Workshop において、APCERT を代表して APCERT のチーム間連携、インシデント対応における連携状況等に関する講演を行いました。ARF についての詳細は、次の URL をご参照ください。

ASEAN REGIONAL FORUM
http://aseanregionalforum.asean.org/

本会合では ARF 参加国の代表によるサイバー空間での信頼醸成措置の実現に向けた議論が行われました。会議では APCERT による技術情報や脅威情報を共有する仕組みを強化することが、信頼醸成の手段の一つとして有効であるという認識が多くの参加者に共有されました。

[図 6-2 ARF での講演の模様]

6.2.2. TSUBAME ネットワークモニタリングワークショップの開催(2014 年 3 月 19 日)

「TSUBAME ネットワークモニタリングプロジェクト」は、APCERT のワーキンググループ活動の一つとして位置づけられており、アジア太平洋地域における連携した定点観測のために、各地域のインターネ

ット上にセンサーを配置し、ワームの感染活動や弱点探索を目的としたスキャンなどのセキュリティ上の脅威となるトラフィックの観測を行っています。JPCERT/CC は、このプロジェクトの提案組織として、運営を主導しています。APCERT 年次総会の会期中、15 名の参加を得て、本プロジェクトのワークショップを開催しました。

ワークショップでは、TSUBAME プロジェクトメンバを対象に、今年度 JPCERT/CC が観測した主な事象に関する報告や、TSUBAME により蓄積したデータから脅威を発見するハンズオン演習を行いました。また、香港、スリランカのチームよりゲストスピーカを迎え、それぞれのチームの TSUBAME 活用方法の紹介を行いました。さらに、プロジェクトメンバ間で今後のプロジェクトの方向性について意見交換を行い、センサーの設置地域や設置数の拡大や、モニタリング結果の共有の強化等を確認しました。

6.2.3. FIRST (Forum of Incident Response and Security Teams)

JPCERT/CC は FIRST に加盟しており、JPCERT/CC の理事 山口英は FIRST の Steering Committee のメンバを務めています。本四半期は、組織運営に関わる議論に参画しました。FIRST および Steering Committee の詳細については、次の URL をご参照ください。

FIRST
http://www.first.org/

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

6.2.4. オープンリゾルバ確認サイト公開

JPCERT/CC は、前四半期に公開したオープンリゾルバ確認サイトの英語版サイトを本四半期に公開しました。本サイトにアクセスすると、当該 PC およびそれが接続されているネットワーク機器に設定されている DNS サーバがオープンリゾルバとなっているかを確認することができます。英語版サイトの公開やサイト構築のノウハウの提供を通じて、協力関係にある各国 CSIRT が国ごとにローカライズしたオープンリゾルバ対策を進めることを支援し、オープンリゾルバを悪用した DDoS 攻撃を低減させる取組の多言語化、より広い範囲への浸透を図っていきます。

オープンリゾルバ確認サイト
http://www.openresolver.jp/

Open DNS Resolver Check Site
http://www.openresolver.jp/en/

6.2.5. 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。本四半期の活動は次のとおりです。

2 月 6 日に日立製作所で開催された「HIRT(Hitachi Incident Response Team)オープンミーティング」にて、「中国のセキュリティ事情～DarKnight(中国黒客の夜明け)～」を題目とし、中国のハッカー、情報セキュリティの傾向について紹介しました。

2 月 17、18、19 日に来日した台湾國家實驗研究院高速網路與計算中心の「電腦機房 異地備援機制」(コンピュータ施設災害リモートバックアップ)調査研究プロジェクトに関して、電気通信事業者のデータセンター訪問を支援し、また Honeynet project 日本分会との会合も設定しました。

6.3. その他の活動

6.3.1. 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。本四半期は以下に関してブログにエントリーを掲載しました。

ICS SECURITY CONFERENCE 2014
http://blog.jpcert.or.jp/2014/03/ics-security-conference-2014.html

JPCERT/CC at “CODE BLUE”
http://blog.jpcert.or.jp/2014/03/jpcertcc-at-cod-ac8c.html

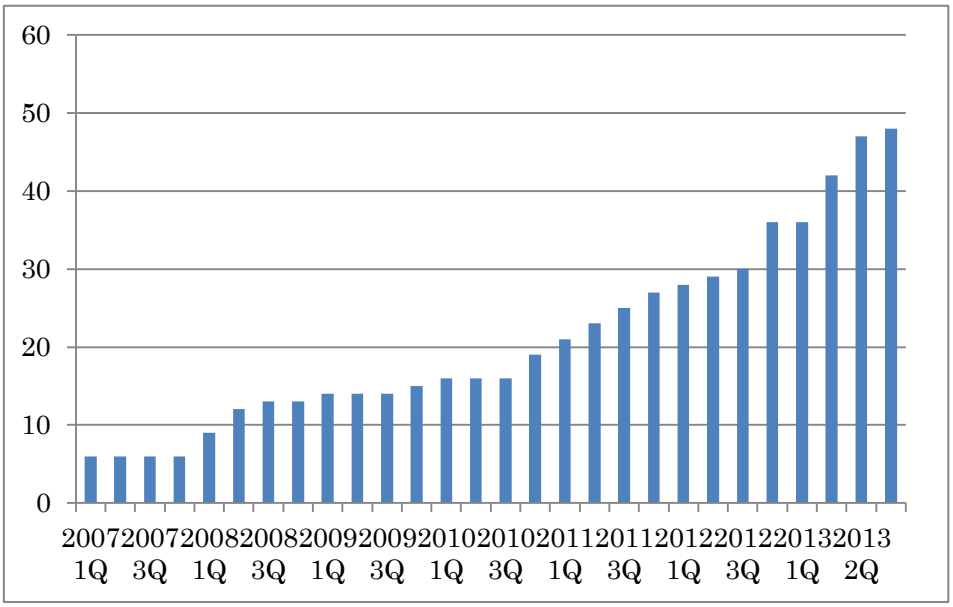
JPCERT/CC 英語ブログ：http://blog.jpcert.or.jp/

7. 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、Web サイトを通じた広報活動、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、富士ゼロックス株式会社(FujiXerox-SIRT)の 1 組織が新規に加盟しました。本四半

期末時点で 48 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 7-1]のとおりです。



[図 7-1　日本シーサート協議会 加盟組織数の推移]

3 月に富士通クラウド CERT にて「13 回ワーキンググループ会」を開催し、各ワーキンググループおよび会員チームからの活動報告が行われました。

日本シーサート協議会の活動の詳細については、次の 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/

8.　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等の活動を行っています。

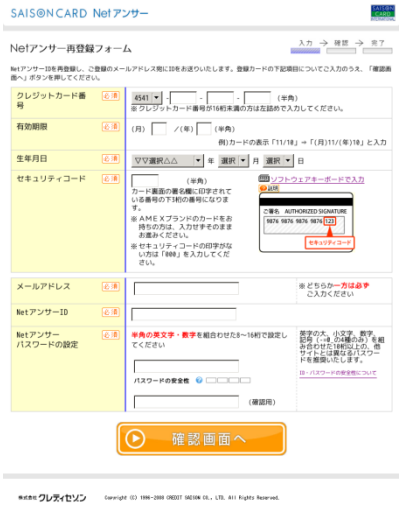
8.1.　情報収集/発信の実績

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 7 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、Web メ

ールサービス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、フィッシング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 8-1]の「セゾン Net アンサーをかたるフィッシング（2014/02/06）」や[図 8-2]の「ゆうちょ銀行をかたるフィッシング(2014/02/20)」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 8-1　セゾン Net アンサーをかたるフィッシング（2014/02/06）
https://www.antiphishing.jp/news/alert/saison20140206.html]

[図 8-2　ゆうちょ銀行をかたるフィッシング(2014/02/20)
https://www.antiphishing.jp/news/alert/20140220jpbank.html]

8.2.　フィッシングサイト URL 情報の提供

協議会では、フィッシング対策ツールバーやウイルス対策ソフト等を提供している協議会員の事業者と、フィッシングに関する研究を行っている協議会員の学術機関に対し、協議会に報告されたフィッシングサ

イトの URL を集めたリストを、日に数回提供しています。この活動は、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に活用していただくことや、関連研究の促進を目的としています。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 19 組織でした。今後と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い、提供先を順次拡大していく予定です。

8.3. 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掛けるため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。

瀬古敏智「2013 年のセキュリティ脅威を振り返って」
愛知県クレジットカード犯罪対策連絡協議会 2014 年 2 月 12 日

山本健太郎「フィッシング詐欺の現状と対策について」
埼玉県クレジットカード犯罪対策連絡協議会 2014 年 2 月 13 日

8.4. 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、毎月の活動報告等を公開しています。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 2014 年 1 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201401.html
フィッシング対策協議会 2013 年 2 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201402.html
フィッシング対策協議会 2013 年 3 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201403.html

9. 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。

9.1. 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 10 回運営委員会
日時：2014 年 1 月 23 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 11 回運営委員会
日時：2014 年 2 月 24 日 16:00 - 18:00
場所：ネットスター株式会社

フィッシング対策協議会 第 12 回運営委員会
日時：2014 年 3 月 14 日 16:00 - 18:00
場所：ネットスター株式会社

10. 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。

10.1. 制御システムセキュリティカンファレンス 2014 講演資料

2014 年 2 月 5 日にコクヨホール(東京都港区)にて開催した、「制御システムセキュリティカンファレンス 2014」の講演資料を公開しました。

カンファレンスについては、「4. 開催セミナー等一覧」をご参照ください。

制御システムセキュリティカンファレンス 2014 においての講演資料
(2014 年 2 月 20 日公開)
https://www.jpcert.or.jp/present/

11. 講演活動一覧

(1) 松本 悦宜(早期警戒グループ 情報分析ライン 情報セキュリティアナリスト) :
「Web アプリケーション開発における HTML5 のセキュリティ」
OWASP AppSec APAC 2014 in Tokyo,2014 年 3 月 20 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 情報セキュリティアナリスト) :
「最新の情報セキュリティ脅威動向と対策と対応について」
セプターカウンシル情報収集 WG ワークショップ,2014 年 3 月 13 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) :
「高度化する脅威に対抗！ JAIPA クラウド部会と JPCERT/CC が作った情報共有体制」
JAIPA CLOUD CONFERENCE 2014,2014 年 3 月 12 日

(4) 有村 浩一(常務理事)：
「情報セキュリティの脅威の動向～2013 年を振り返る～」
電力業界におけるセキュリティ担当会議,2014 年 2 月 28 日

(5) 宮地 利雄(理事/顧問)：
「他人事ですまない危うい現実――制御システム・セキュリティ」
@IT Security Live UP!,2014 年 2 月 25 日

(6) 重森友行(早期警戒グループ 情報セキュリティアナリスト)：
「HTML5 Security & Headers - X-Crawling-Response-Header -」
CODE BLUE,2014 年 2 月 18 日

(7) 中津留 勇(分析センター)：
「Fight Against Citadel in Japan」
CODE BLUE,2014 年 2 月 18 日

(8) 満永 拓邦(早期警戒グループ 情報分析ライン リーダー 情報セキュリティアナリスト)：
「最近のセキュリティ動向」
神奈川県クレジットカード犯罪対策連絡協議会第 18 回定例会,2014 年 2 月 17 日

(9) 満永 拓邦(早期警戒グループ 情報分析ライン リーダー 情報セキュリティアナリスト)：
「情報セキュリティを取り巻く現状」
Windows XP サポート終了に関する記者会見(日本マイクロソフト),2014 年 2 月 13 日

(10) 山本 健太郎(フィッシング対策協議会)：
「フィッシング詐欺の現状と対策について」
埼玉県クレジットカード犯罪対策連絡協議会平成 25 年度定例会,2014 年 2 月 13 日

(11) 瀬古 敏智(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)：
「2013 年のセキュリティ脅威を振り返って」
愛知県クレジットカード犯罪対策連絡協議会第 23 回定例会,2014 年 2 月 12 日

(12) 真鍋 敬士(理事,分析センター長)：
「2020 年のサイバーセキュリティ～東京五輪開催へ向けた安全・安心な IT～」パネリスト
IPA サイバーセキュリティシンポジウム 2014,2014 年 2 月 12 日

(13) 有村 浩一(常務理事)
「情報セキュリティの脅威の動向～2013 年を振り返る～」
情報セキュリティ対策に関する説明会(日本民間放送連盟),2014 年 2 月 7 日

(14) 林 永熙(制御システムセキュリティ対策グループ 情報セキュリティアナリスト)：
「中国のセキュリティ事情～DarKnight(中国黒客の夜明け)～」
Hitachi Incident Response Team オープンミーティング,2014 年 2 月 6 日

(15) 小宮山 功一朗(国際部 兼 エンタープライズサポートグループ マネージャー)：
「報告 1（サイバー空間)」に関してコメント
公開シンポジウム「グローバル・コモンズ（サイバー空間、宇宙、北極海）における
日米同盟の新しい課題」,2014 年 1 月 31 日

(16) 松本 悦宜(早期警戒グループ 情報分析ライン 情報セキュリティアナリスト)：
「今から始める HTML5 セキュリティ」
第 44 回 HTML5 とか勉強会,2014-01-29

12. 執筆一覧

(1) 戸田 洋三(情報流通対策グループ リードアナリスト):
もいちど知りたい、セキュアコーディングの基本（6）
「動的メモリ管理に関する脆弱性」
アイティメディア ＠IT,2014 年 1 月 23 日

13. 開催セミナー等一覧

(1) 企業向けセキュアコーディングセミナー

JPCERT/CC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。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、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セミナーも提供しています。

本四半期は、国内メーカー1社に対して、「Javaセキュアコーディングセミナー」を実施しました。

(2) 制御システムセキュリティカンファレンス 2014

制御システムのセキュリティ向上に向けて、課題と最新の技術動向を関係業界の皆さまにご理解いただくために、第6回となる「制御システムセキュリティカンファレンス 2014」を開催しました。

・主　　催：経済産業省
　　JPCERT/CC
・開催日時：2014年2月5日 10:00～16:00
・参加人数：264名

この行事の詳細については、次のURL をご参照ください。
https://www.jpcert.or.jp/event/ics-conference2014.html

当日の講演資料については、次のURLをご参照ください。
https://www.jpcert.or.jp/present/

14. 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) OWASP AppSec APAC 2014 in Tokyo

主　催：OWASP

開催日：2014年3月17日(月)～20日(木)

(2) 情報セキュリティシンポジウム道後2014

主　催：情報セキュリティシンポジウム道後2014実行委員会

開催日：2014年2月27日(木)、28日(金)

(3) CODE BLUE

主　催：CODE BLUE実行委員会

開催日：2014年2月17日(月)、18日(火)

■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