JPCERT/CC®

Japan Computer Emergency Response Team Coordination Center

電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2016.01.14 10:04:11 +09'00'

JPCERT-PR-2015-05
発行日 : 2016-01-14

JPCERT/CC 活動概要 [2015 年 10 月 1 日 ～ 2015 年 12 月 31 日]

活動概要トピックス

ートピック1ー　高度サイバー攻撃への対策のための文書を公開

JPCERT/CC では、高度サイバー攻撃への効果的な対策を進めていただくために、2015 年 11 月 17 日に「高度サイバー攻撃への対処におけるログの活用と分析方法」を公開するとともに、公開中の CSIRT マテリアル(構想・構築・運用）の内容を一部見直し更新しました。
「高度サイバー攻撃」は、国内においても多数の事案が表面化しており、多くの組織にとって新たなセキュリティ脅威となっています。高度サイバー攻撃は、従来型の攻撃のように防御・検出だけで完全に防ぐことが難しいため、気づかないうちに攻撃を受けて侵入されていることも想定した上で、いかに早く異常に気づき対処できるかが対策の成否の分かれ目となります。

既存の機器のログ採取機能を適切に設定し、採取されたログを適切なタイミングでチェックすることにより、比較的すみやかに、しかも大きな追加投資なしに異常に気付くことができます。しかしながら、そのための方法をまとめた文書がこれまで無く、ログ機能を十分に活用できていないケースも多くみられました。

こうした状況の改善に向けた一助を目指し、高度サイバー攻撃への備えと効果的な対処の観点から、一般的に利用される機器に、攻撃者の活動の痕跡をログとして残すための考え方、それらのログから痕跡を見つけ出す方法などをまとめたガイドが、2015 年 11 月 17 日に公開した「高度サイバー攻撃への対処におけるログの活用と分析方法」です。

また、「CSIRT マテリアル(構想・構築・運用)」は、2008 年の公開以来、組織内 CSIRT を構築するためのバイブルとしてご利用いただいてきた文書です。高度サイバー攻撃によるインシデントは、「現場＝システム管理者」だけで対応できる問題ではありません。また、一組織にとどまらず他組織や関連組織を含めた対応が必要になる場合もあり、経営層の積極的な関与に裏打ちされた組織内 CSIRT の役割が極めて重要です。

このような時代背景の変化を織り込んで、既存の「CSIRT マテリアル」の構想・構築・運用フェーズ資料をそれぞれ更新し公開しました。

今回の更新では、高度サイバー攻撃（APT（先進的で(Advanced)執拗な(Persistent)、脅威(Threat)の増加）への脅威について記載し、組織全体のリスク評価の実施と許容度の設定、CSIRT 間の情報共有・連携、CSIRT の役割や必要な CSIRT 要員のスキル等を高度サイバー攻撃に関する先進的な戦術等を従来の CSIRT マテリアルに追記する形式で更新しました。

高度サイバー攻撃への対処におけるログの活用と分析方法
https://www.jpcert.or.jp/research/apt-loganalysis.html

CSIRT マテリアル(構想・構築・運用)
https://www.jpcert.or.jp/csirt_material/

ートピック2ー　標的型攻撃に使われるマルウエアに対する、検知ツールと分析スクリプトを公開

JPCERT/CC 分析センターは、標的型攻撃に使用されるマルウエアを分析するためのツールを 2015 年 10 月 28 日に公開しました。

JPCERT/CC ではインシデント報告等をもとに、標的型攻撃に関するインシデント対応を支援する活動を行なっており、関連して標的型攻撃に関する技術的な調査や関連するマルウエアの分析を行っています。今回公開したツールもこの活動に関連して作成されたもので、インシデント対応や調査等に広く役立てていただくことを目的として公開しました。

今回公開したツールは「apt17scan.py」と「emdivi_string_decryptor.py」の 2 種類で、いずれも日本の組織を標的とした攻撃グループが使用するマルウエアの分析に使用可能なツールです。

「apt17scan.py」は、メモリイメージを探索することで、特定の攻撃グループが使用している複数のマルウエアを検知し、検知したマルウエアの設定情報を抽出するためのツールで、メモリフォレンジックツールである The Volatility Framework の Plugin として実現されています。
一方「emdivi_string_decryptor.py」は、遠隔操作マルウエア Emdivi 内の暗号化された文字列を復号するためのツールで、逆アセンブラ IDA 用の IDAPython スクリプトとして実現されています。

ツールについては、2015 年 10 月 28 日に開催された CODE BLUE 2015 における JPCERT/CC の講演「日本の組織をターゲットにした攻撃キャンペーンの詳細」でも紹介し、ツールの公開に合わせて、それぞれのツールを紹介する「分析センターだより」の公開も行いました。

なお、ツールの公開は、ソフトウエア開発プロジェクトのための共有ウェブサービスの GitHub で行っています。

JPCERTCC/aa-tools・GitHub
https://github.com/JPCERTCC/aa-tools

標的型攻撃に使われるマルウエアを検知する Volatility Plugin(2015-10-28)
https://www.jpcert.or.jp/magazine/acreport-aptscan.html

ートピック3ー　JVN にて共通脆弱性評価システム CVSS v3 による脆弱性評価を開始

JPCERT/CC は、JVN において CVSS　v3 に基づく脆弱性評価結果の公表を 2015 年 12 月 1 日より開始しました。

ソフトウェア製品に作り込まれる脆弱性は、その原因や種類、再現性、攻撃者がインターネット経由で悪用できるか否かなど、複数の要素を総合的に判断することで、その深刻度を表現することができますが、今日、その深刻度を表現する仕組みとして、CVSS と呼ばれる方式が一般的に用いられています。

CVSS の管理団体である FIRST は、CVSS の改訂を行い、現在普及している CVSS v2 の次期バージョンとなる v3 を 2015 年 6 月に正式に発行しました。これを受けて JPCERT/CC は、12 月 1 日より JVN で公開する脆弱性アドバイザリにおいて、CVSS v2 と CVSS v3 の両方の評価値を掲載しています。

CVSS v3 では、システム全体ではなく脆弱性の存在するコンポーネントに注目した影響の評価が可能になるほか、脆弱性の悪用の難易度をより細分化された項目に基づいて評価できるようになるため、現実の脅威に即して脆弱性の評価を行うためのツールとして期待されています。

JPCERT/CC は、他組織に先んじて CVSS v3 の運用を開始することで、国内組織における CVSS v3 の採用を推進してまいります。

CVSS v3 を使った脆弱性評価の詳細については、本活動概要の次の項目をご参照ください。

2.1.5. CVSS v3 による脆弱性評価を開始

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」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 3440 件、インシデント件数ベースでは 3169 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 2053 件でした。前四半期の 2058 件と比較して 0.3%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 474 件で、前四半期の 522 件から 9%減少しました。また、前年度同期(406 件)との比較では、17%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	10 月	11 月	12 月	国内外別合計（割合）
国内ブランド	30	35	59	124(26%)
国外ブランド	93	88	69	250(53%)
ブランド不明(注 2)	40	30	30	100(21%)
月別合計	163	153	158	474(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では、異なるブランドを装っていてもドメインや IP アドレスに共通点が見られるものがあり、特定の攻撃者グループが複数のブランドを標的としてフィッシングを行っている可能性が考えられます。10 月から継続的に確認されている複数ブランドのフィッシングは、TLD が.com であり、香港のホスティングサービスが多く使用されていました。また、11 月末以降に確認された別の複数ブランドのフィッシングでは、韓国やアメリカのホスティングサービスが多く使用され、URL には.help、.ren、.link などの gTLD 配下で、正規サイトを装ったサブドメインを取得して使用されていました。

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も多く寄せられており、フィッシングサイトの多くは侵入されたと見られる海外の Web サイト上に設置されていました。一方で、本四半期の国内オンラインゲームを装ったフィッシングサイトは、10 月の後半と 12 月の半ばに確認されたのみで、非常に少数でした。

フィッシングサイトの調整先の割合は、国内が 46%、国外が 54%であり、前四半期(国内 48%、国外 52%)に比べ、海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、826 件でした。前四半期の 592 件から 40%増加しています。

本四半期は、改ざんされた Web サイトにアクセスした際に、セキュリティ製品がランサムウエアのダウンロードを検知したという報告が複数寄せられました。body タグの直後やページの最上部に難読化されたコードが埋め込まれた Web サイトの改ざんが特に多く、WordPress、Joomla、Drupal などの CMS を使用して構築されたサイトが改ざんされている傾向が見られました。改ざんされたサイトにアクセスすると、不正なコードによって攻撃サイトに誘導され、Adobe Flash Player や Internet Explorer などの脆弱性を悪用した攻撃によって、マルウエアのダウンロード、実行が行われることを確認しています。

改ざんされた Web サイトの管理者からサイトのコンテンツを提供していただき調査したところ、CMS の

デフォルトのファイルに//istart や//iend などの文字列を含む不正なコードが埋め込まれていました。改ざんされた原因としては、CMS および CMS のテーマ、プラグインの脆弱性を悪用する攻撃や、管理用のパスワードの窃取などが考えられます。

1.1.1.3. その他

本四半期に報告が寄せられた標的型攻撃に分類されるインシデントの件数は、12 件でした。前四半期の 59 件から 80%減少しています。本四半期には、11 組織（延べ数）に対して連絡を行いました。

標的型攻撃が本年度の前半には非常に多く確認されましたが、本四半期はわずかが確認されたのみでした。攻撃者の活動が停止している可能性もありますが、攻撃されている組織が気づいていない可能性も考えられます。警戒を怠ることなく、標的型攻撃に備えて十分に対策ができているか、次の点を中心とした点検を推奨します。

- PC がマルウエアに感染し、攻撃者の侵入を招くことを防ぐために、PC の OS、アプリケーションを常に最新の状態にアップデートしているか。
- 攻撃者がネットワークへの侵入後に Active Directory サーバの脆弱性を攻撃しても耐えられるよう、サーバのセキュリティアップデートを確実に適用しているか。
- ネットワーク内で横断的に侵害が行われることを防ぐため、Active Directory のドメインに参加している PC で管理者権限が適切に運用され、パスワードの共有や使いまわしが行われていないか。
- 文書ファイルに偽装したマルウエアを添付した、なりすましメールに対抗するため、不審な送信元からのメールをブロックし、添付ファイルの種類を制限する等しているか。

さらに、攻撃の早期発見や、原因の調査ができるように、PC およびサーバのイベントログや、プロキシ、ファイアウォール、DNS クエリなどのログが適切に取得できているかについても、ご確認ください。

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っています。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. JPCERT/CC からのお知らせ

JPCERT/CC で収集したセキュリティ関連情報のうち、各組織のセキュリティ対策に有用であると判断した情報をまとめ、次のようなお知らせとして発行しました。

発行件数：3 件　https://www.jpcert.or.jp/update/2015.html

2015-10-28　注意喚起「SNS やクラウドサービスで連携されるアカウント情報には細心の注意を」 (公開)
2015-11-17　高度サイバー攻撃への対処におけるログの活用と分析方法(公開)
2015-12-17　冬期の長期休暇に備えて(公開)

1.2.1.2. 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（うち 2 件更新）　https://www.jpcert.or.jp/at/

2015-10-14　2015 年 10 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起 (公開)
2015-10-14　Adobe Reader および Acrobat の脆弱性 (APSB15-24) に関する注意喚起 (公開)
2015-10-14　Adobe Flash Player の脆弱性 (APSB15-25) に関する注意喚起 (公開)
2015-10-19　Adobe Flash Player の脆弱性 (APSB15-27) に関する注意喚起 (公開)
2015-10-20　Adobe Flash Player の脆弱性 (APSB15-25) に関する注意喚起 (更新)
2015-10-20　Adobe Flash Player の脆弱性 (APSB15-27) に関する注意喚起 (更新)
2015-10-21　2015 年 10 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)
2015-11-11　2015 年 11 月 Microsoft セキュリティ情報 (緊急 4 件含) にする注意喚起 (公開)
2015-11-11　Adobe Flash Player の脆弱性 (APSB15-28) に関する注意喚起 (公開)
2015-12-09　2015 年 12 月 Microsoft セキュリティ情報 (緊急 8 件含) にする注意喚起 (公開)
2015-12-09　Adobe Flash Player の脆弱性 (APSB15-32) に関する注意喚起 (公開)

2015-12-16　ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2015-8000) に関する注意喚起

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：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 77 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。

2015-10-07　10 月は「サイバーセキュリティ国際キャンペーン」
2015-10-15　JPNIC 管理下の逆引きゾーンへ DNSSEC 導入
2015-10-21　日本版 「STOP. THINK. CONNECT. 立ち止まって、考えて、ネットを楽しむためのクイズ」公開
2015-10-28　NICT が暗号プロトコルのセキュリティ評価結果を公開
2015-11-05　IPA が「情報セキュリティ対策ベンチマーク バージョン 4.4」と「診断の基礎データの統計情報」を公開
2015-11-11　マイクロソフトが SHA-1 廃止に向けた FAQ を公開
2015-11-18　無線 / 有線 LAN ルータを使用する際はデフォルトのパスワードの変更を
2015-11-26　SecurityDay 2015 開催のお知らせ
2015-12-02　JPCERT/CC が「CSIRT マテリアル」を更新
2015-12-09　JAIPA が「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン（第４版）」を公開
2015-12-16　内閣サイバーセキュリティセンター (NISC) が重要インフラにおける分野横断的演習を実施
2015-12-24　警察庁、「IoT 機器を標的とした攻撃の観測について」を公開

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。

【Commmons Collections ライブラリの脆弱性】
Apache Software Foundation が提供する Commons Collections ライブラリの脆弱性と、その脆弱性を使用して WebSphere 等のアプリケーションサーバを攻撃する手法を 2015 年 11 月 6 日（米国時間）にセキュリティ研究者が公開しました。オブジェクトのデシリアライズ処理において、任意のコードが実行できる脆弱性であり、JPCERT/CC の追試でも、Commons Collections ライブラリを使用したアプリケーションサーバに細工したオブジェクトを送り付けて、サーバ上で任意のコードが実行できることを確認しました。Commons Collections ライブラリは、アプリケーションサーバ以外の Java アプリケーションでも幅広く使用されています。JPCERT/CC では、脆弱性の深刻度が高いと判断し、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、2015 年 11 月 12 日に早期警戒情報を発行しました。

【「高度サイバー攻撃への対処におけるログの活用と分析方法」の公開】
組織を標的とした「高度サイバー攻撃」は、国内においても多くの組織で表面化しており、新たなセキュリティ脅威となっています。高度サイバー攻撃への対策は、侵入前の防御・検出をめざす従来型の手法では攻撃を完全に防ぐことが難しいため、攻撃を受けて内部に侵入された場合に、いかに早く異常に気づき対処できるかが成否の分かれ目となります。高度サイバー攻撃への対策を検討される際の参考となるよう、JPCERT/CC では、2015 年 11 月 17 日に「高度サイバー攻撃への対処におけるログの活用と分析方法」を公開しました。この文書は、高度サイバー攻撃への備えと効果的な対処の観点から、攻撃者の活動の痕跡をログとして残すための設定方法と、ログから痕跡を見つけ出す分析方法などを、一般的に利用されるネットワーク機器を前提として記載しています。

高度サイバー攻撃への対処におけるログの活用と分析方法
https://www.jpcert.or.jp/research/apt-loganalysis.html

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 12 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、プロジェクトへの参加を呼びかけています。

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

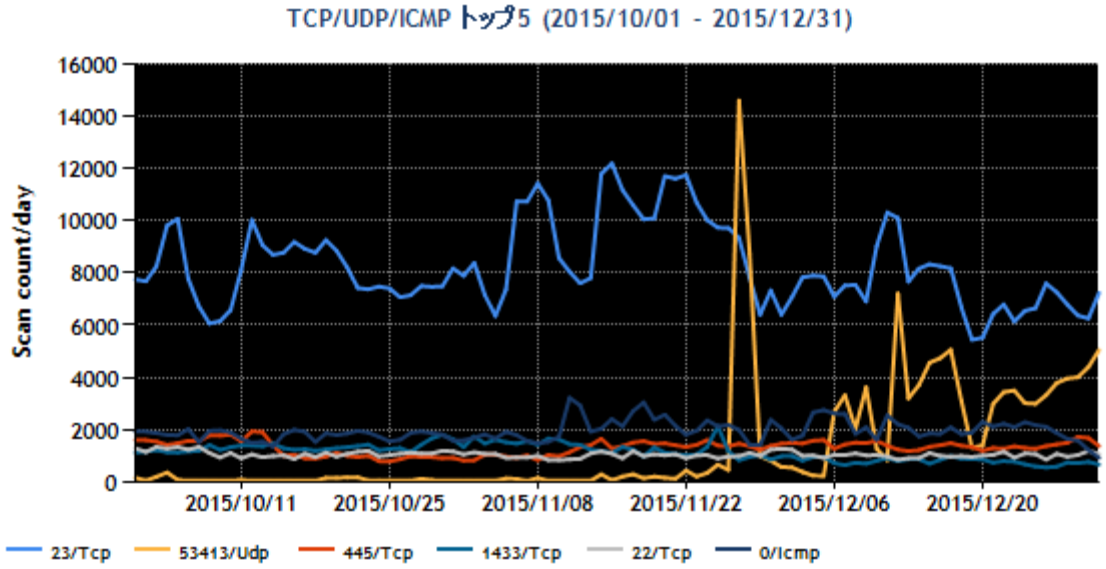
JPCERT/CC は、TSUBAME で収集したデータを宛先ポート番号や送信元地域ごとに分類して統計分析し、既知の脆弱性情報やマルウエア、攻撃ツール等との関連を考察することで、攻撃活動や準備活動の捕捉に努めています。

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 7 月から 9 月分のレポートを 2015 年 10 月 29 日に公開しました。

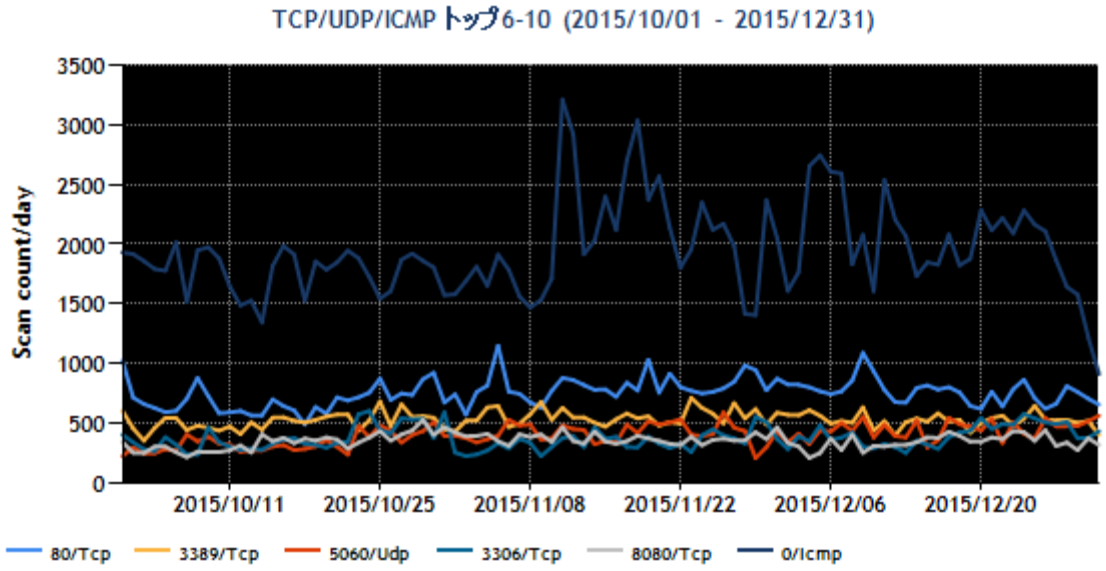
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

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/report201507-09.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。

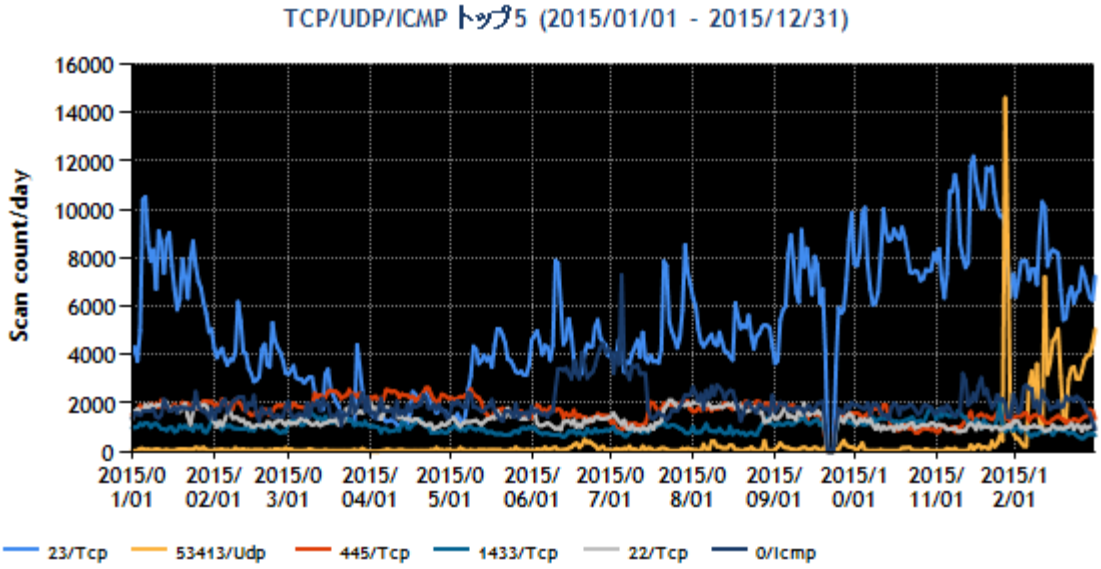


[図 1-1 宛先ポート別グラフ トップ 1-5 (2015 年 10 月 1 日-12 月 31 日)]

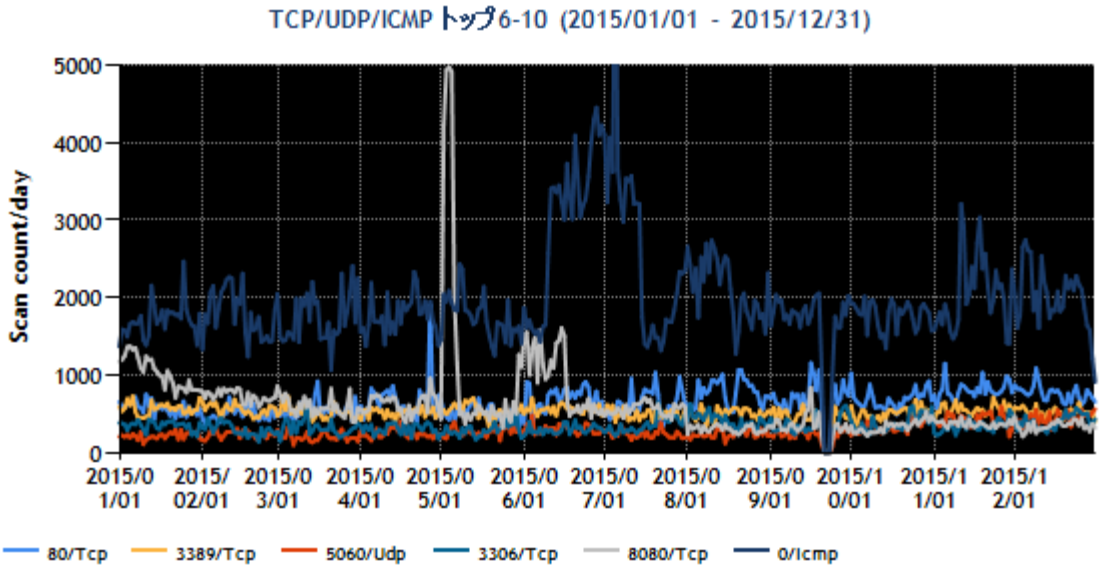


[図 1-2 宛先ポート別グラフ トップ 6-10 (2015 年 10 月 1 日-12 月 31 日)]

また、過去 1 年間 (2015 年 1 月 1 日-2015 年 12 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。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 1-3 宛先ポート別グラフ トップ 1-5 (2015 年 1 月 1 日-2015 年 12 月 31 日)]



[図 1-4 宛先ポート別グラフ トップ 6-10 (2015 年 1 月 1 日-2015 年 12 月 31 日)]

本四半期は、前四半期に引き続き 23/Tcp 宛へのパケット数が高い水準にあります。また、11 月 27 日、28 日に突発的に主に中国を送信元とする 53413/Udp 宛へのパケットが増加し、その後再び 12 月上旬から増加し続けています。観測したパケットを分析した結果、これは 53413/Udp を標準ポートとして使用する Netis/Netcore 社製のルータ製品を探索する目的のパケットと推測しています。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) 445/TCP 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、ファイル共有などのための Windows のダイレクトホスティング SMB サービスが使用するポート (445/TCP) 宛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、Conficker などのマルウエアへの感染や不審なツールが設置されていないかなど調査を依頼したところ、ある管理者から「当該 IP アドレスの機器が Conficker に感染していることが判明したため駆除を行った」との回答を得ました。

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。

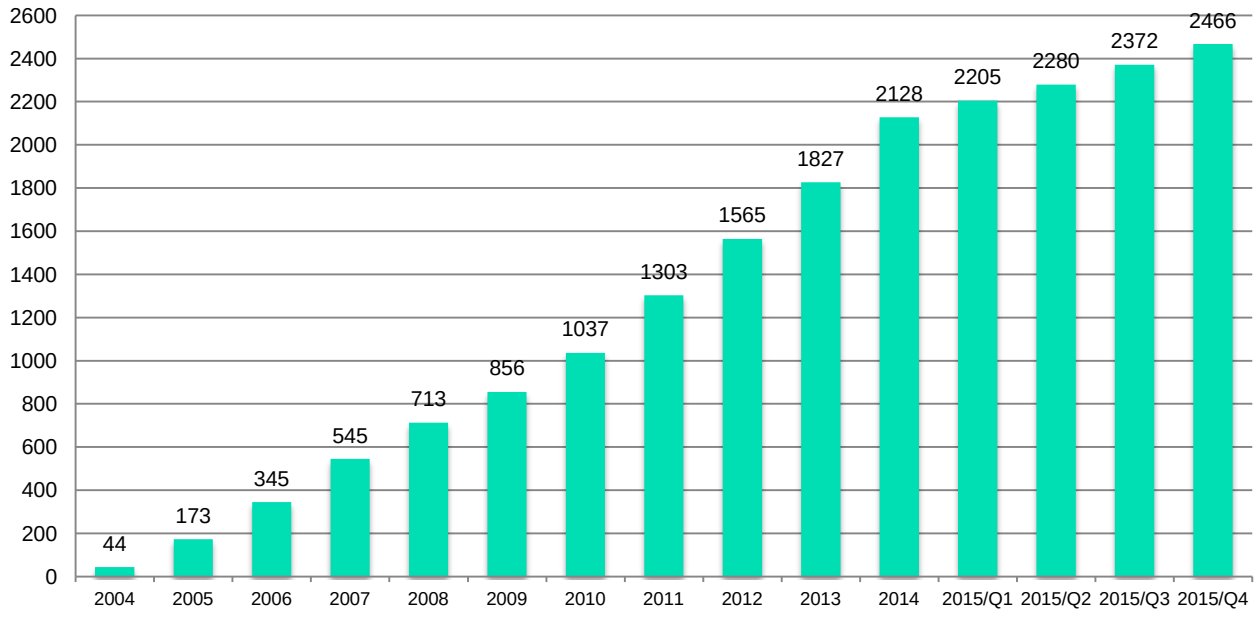
独立行政法人情報処理推進機構(IPA) 脆弱性対策
http://www.ipa.go.jp/security/vuln/

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 94 件(累計 2,466 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/



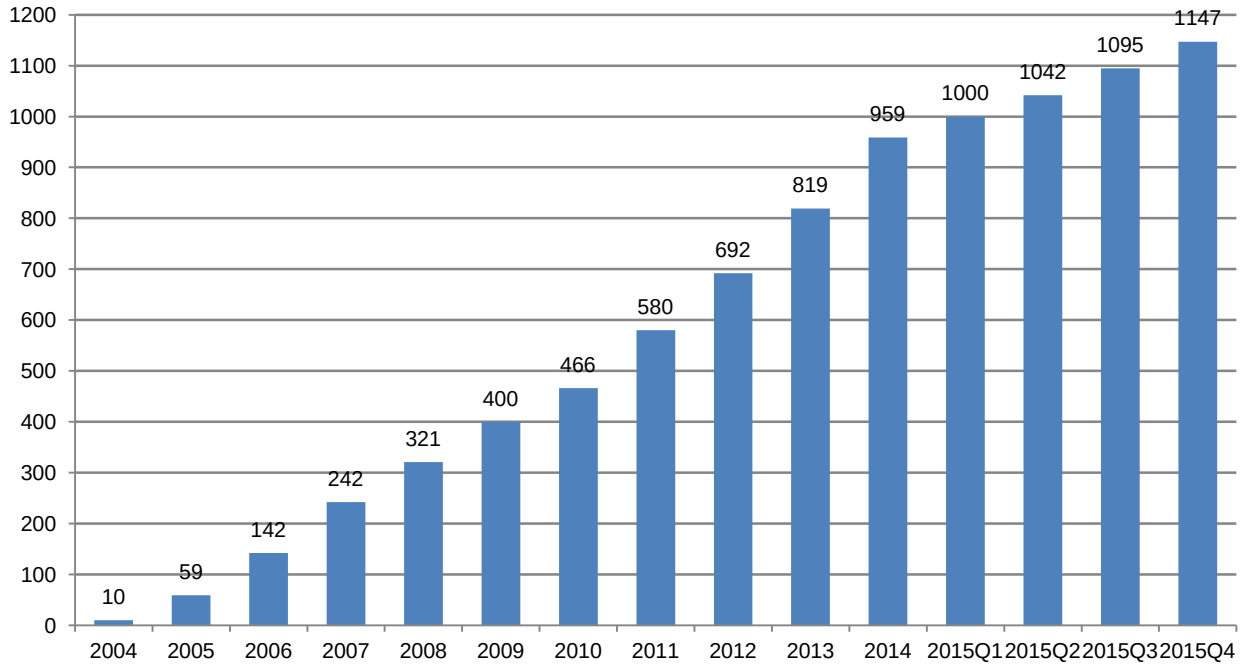
[図 2-1　JVN 公表累積件数]

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 52 件(累計 1,147 件)で、累計の推移は[図 2-2]に示すとおりです。52 件のうち、25 件が国内製品開発者の製品、26 件が海外の製品開発者の製品、1 件が複数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 2 件公表しました。

本四半期に公表した脆弱性情報の件数の、影響を受けた製品のカテゴリ別の内訳は、表 2-1 のとおりでした。本四半期の特徴としては、組込系製品、コンテンツ管理システム(CMS)、ウェブアプリケーション、グループウエアの脆弱性情報の公開が多かったと言えます。

製品分類	件数
組込系製品	8
コンテンツ管理システム(CMS)	8
ウェブアプリケーション	7
グループウエア	6
Android アプリ	2
Android 向け SDK	2
iOS アプリ	2
掲示板	2
ライブラリ	2
Flash	1
iOS 向け SDK	1
JavaScript ライブラリ	1
MacOS	1
SDK	1
Windows アプリケーション	1
アーカイバー	1
アンチウイルス製品	1
ウェブアプリケーションフレームワーク	1
スマホアプリ	1
制御系製品	1
セキュリティアプライアンス製品	1
プログラミング言語	1

[表 2-1 公表を行った国内取扱脆弱性情報の件数の製品カテゴリ別内訳]



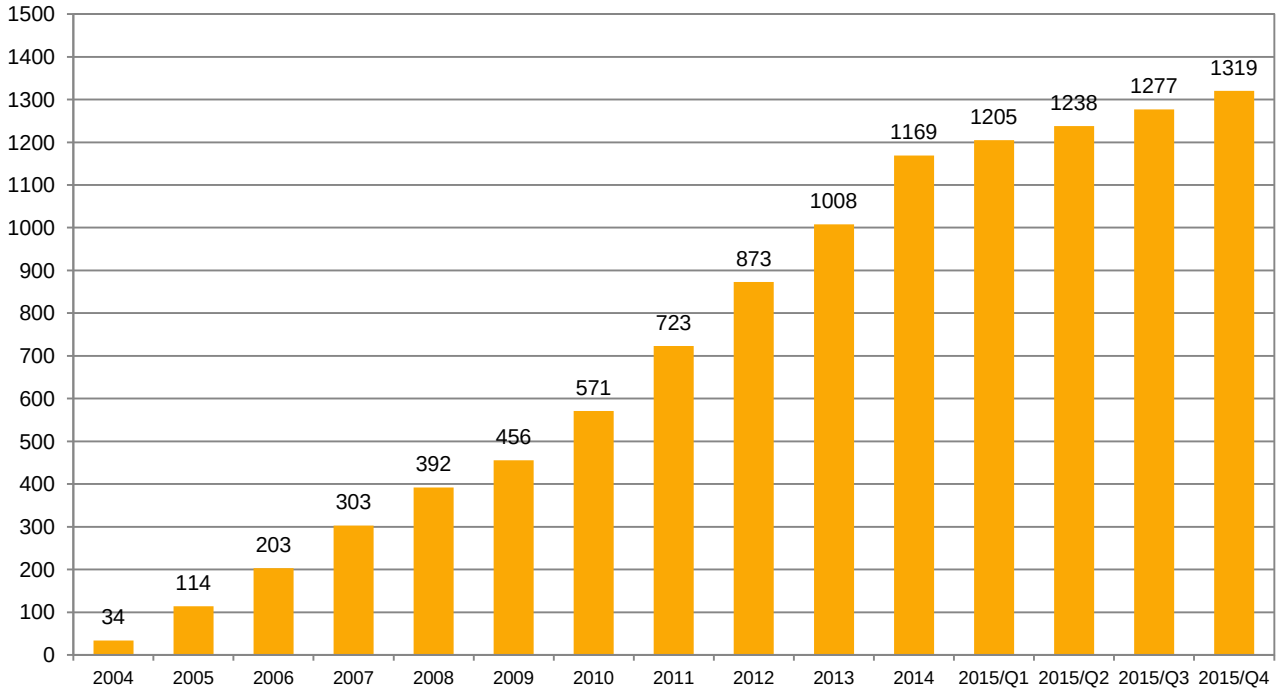
[図 2-2 公表を行った国内取扱脆弱性情報の累積件数]

本四半期に公表した国際取扱脆弱性情報は 42 件(累計 1,319 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情報の件数の、影響を受けた製品のカテゴリ別内訳は、表 2-2 のとおりでした。本四半期の特徴としては、組込系製品に関する脆弱性情報の公開が多かったことです。この理由は、CERT/CC での組込系ルータ機器における独自調査で、複数製品に脆弱性が見つかったことが要因の一つとしてあげられます。

製品分類	件数
組込系製品	15
ウェブアプリケーション	7
Windows アプリケーション	6
Apple 製品	3
ライブラリ	3
DNS	2
Android アプリ	1
制御系製品	1
プロトコル	1
モバイルアプリ	1
仮想化用ソフトウェア	1
統合管理ソリューション	1

[表 2-2 公表を行った国際取扱脆弱性情報の件数の製品カテゴリ別内訳]



[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上げています。

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ありませんでしたが、前四半期に公表した 12 件の連絡不能開発者情報に製品およびバージョン情報を追加掲載し、更新を行いました。
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。本四半期には、11月に第三回公表判定委員会を開催し、6件の連絡不能開発者案件の脆弱性情報の公開可否について審議を行いました。

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 11 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。

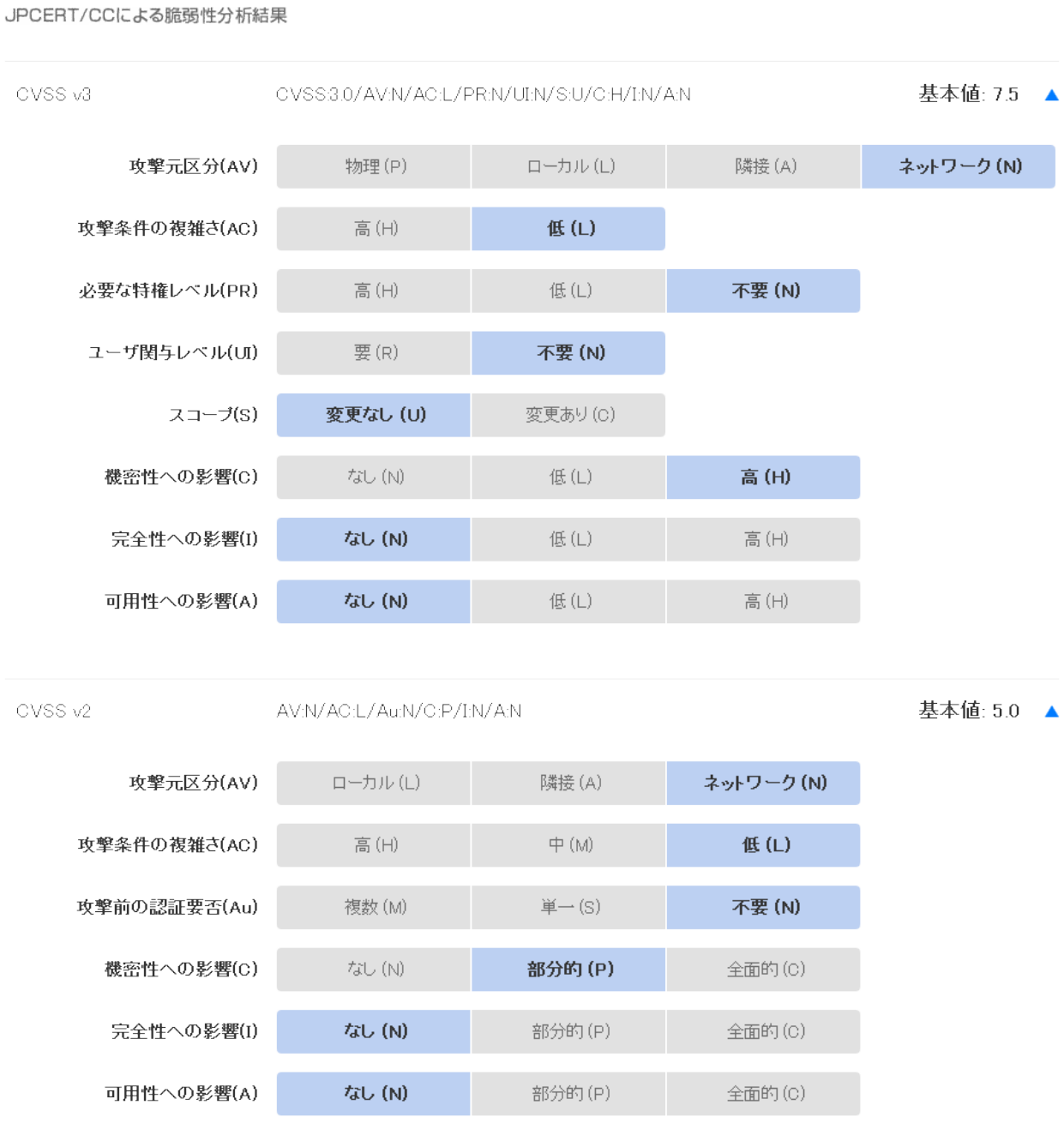
CNA および CVE に関する詳細は、次の Web ページをご参照ください。

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

2.1.5. CVSS v3 による脆弱性評価を開始

2015 年 12 月 1 日以降 JVN において公表する脆弱性情報について、共通脆弱性評価システム CVSS v3http://www.jpcert.or.jp/press/2015/20151201-CVSSv3.html - 1 による脆弱性評価の付記を始めました。
CVSS (Common Vulnerability Scoring System)は、脆弱性の影響と深刻度を表現する標準化された方式として、FIRST (The Forum of Incident Response and Security Teams) によって策定され、多くの脆弱性アドバイザリ発行機関が採用しています。これまでは CVSS v2 が使われてきましたが、 CVSS v3 の規格が 2015 年 6 月 10 日に発行されました。
CVSS v3 では、記述の柔軟性と一貫性の向上をはかるとともに、セキュリティ技術の変遷にも配慮して、脆弱性が悪用された時の影響範囲が直接に攻撃されたシステムに留まるかどうかを表す 「スコープ」のような評価項目が追加され、また、攻撃による機密性・完全性への影響を評価する項目においては、重要な情報に対する副次的な影響を含めて評価するように変更されています。
他の脆弱性アドバイザリ発行機関にさきがけて JVN では CVSS v3 を採用し、当面は CVSS v2 と CVSS v3 の双方による脆弱性の深刻度を評価していきます。

評価分析値は脆弱性アドバイザリ中で図 2-4 のように表示されます。



[図 2-4 JVN における CVSS v3 と CVSS v2 の併記例]

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。

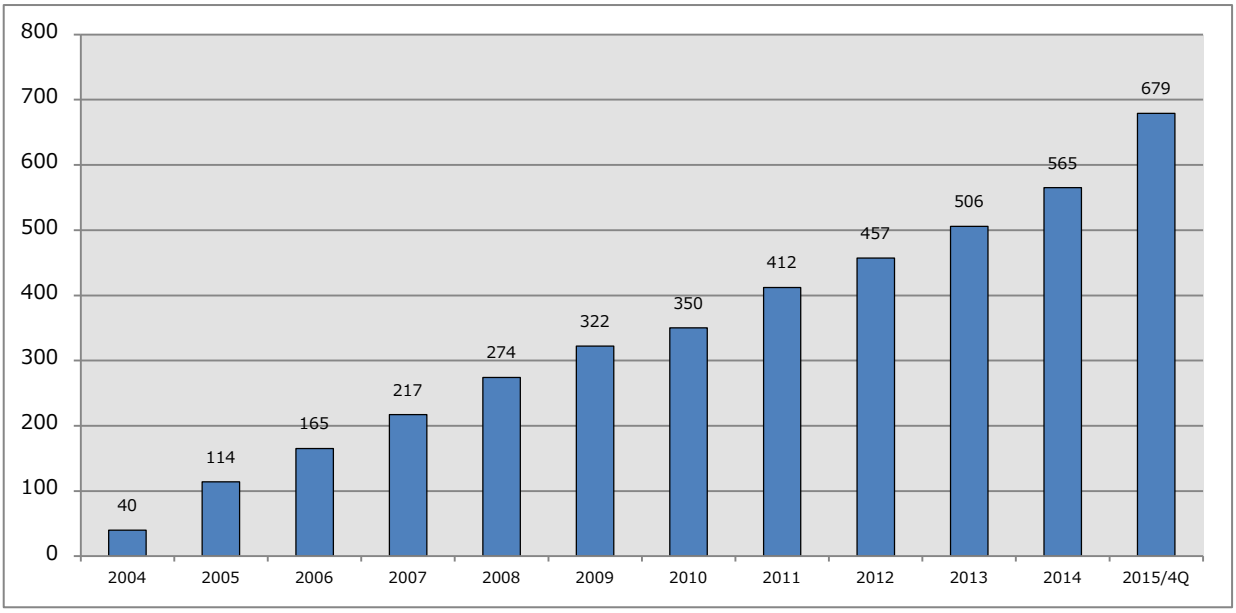
脆弱性情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
脆弱性情報コーディネーション概要
https://www.jpcert.or.jp/vh/

「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 12 月 31 日現在で 679 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]

2.2.2. 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います。

本四半期は 2015 年 11 月 10 日にミーティングを開催し、最近の脆弱性の動向や事例分析、製品開発者による脆弱性報奨金制度の事例、脆弱性報告者や脆弱性情報を収集する利用者の立場からの意見など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]

2.3. 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 4 件の講演を行いました。

講演タイトル: セキュアプログラミング Web アプリケーション
講演月日：10 月 17 日
イベント名：東京電機大学 国際化サイバーセキュリティ学特別コース(CySec)
「セキュアシステム設計・開発」

CISO や上級セキュリティエンジニア人材の育成を目指して、東京電機大学で今年度から開講されることになった「国際化サイバーセキュリティ学特別コース」を構成している「セキュアシステム設計・開発」科目の中の「セキュアプログラミング: Web アプリケーション」の講師を、JPCERT/CC の解析チームがソフトウエア開発者向け啓発活動の一環として、担当しました。Web アプリケーションの脆弱性とその対策の習得を目的として、クロスサイトスクリプティング、SQL インジェクション、クロスサイトリクエストフォージェリといった脆弱性について、講師による解説を行うとともに、IPA が公開している脆弱性体験学習ツール AppGoat による実習を行いました。

講演タイトル: [CON4844] Case Studies and Lessons Learned from Certificate Validation Vulnerabilities

講演月日：10 月 29 日
イベント名：JavaOne 2015

JavaOne 2015 カンファレンスが米国サンフランシスコで開催され、解析チームの戸田が参加するとともに講演を行いました。今回の講演は、昨年 11 月の KOF2014 や今年 4 月の Java Day Tokyo 2015 における SSL/TLS 証明書検証に関する脆弱性事例解説の講演内容をアップデートしたものです。

講演タイトル：制御システム用ソフトウェアの脆弱性にみる対策に有効な CERT C コーディングルール
講演月日：11 月 24 日
イベント名：QAC User's Meeting 2015

解析チームの久保が、ソースコード解析ツール QAC のユーザミーティングにおける基調講演者の一人として招聘され、昨年度(2014 年度)公開した調査レポート「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」の主要部分を紹介する講演を行いました。

講演タイトル：OWASP ドキュメントの翻訳 – ASVS, Cheat Sheet ドキュメント
講演月日：12 月 21 日
イベント名：OWASP Night/WAS Night 2015 Year End

12 月 21 日に開催された OWASP(注 1) Japan チャプターのミーティングで、解析チームの戸田が「OWASP ドキュメントの翻訳」と題して講演し、OWASP が公開している ASVS (Application Security Verification Standard) および Cheat Sheet シリーズドキュメント(英語)の日本語翻訳作業を開始したことを紹介しました。また、今年度中に翻訳作業を完了して 2016 年 4 月までに公開予定である点、今後、元ドキュメントの更新に合わせて翻訳ドキュメントの更新作業を皆さんの手で続けてほしい点を呼びかけました。

(注 1) OWASP (Open Web Application Security Project) は、Web 技術をはじめとするソフトウエアのセキュリティに関する情報共有と普及啓発を目的とした団体です。

2.3.1. 「クロスサイトリクエストフォージェリ(CSRF)とその対策」資料公開

Web アプリケーションにおける典型的な脆弱性のひとつ、CSRF(クロスサイトリクエストフォージェリ)の仕組みとその対策に関する資料を公開しました。この資料では、CSRF の仕組みや対策の考え方を解説するとともに、CSRF 対策の実装を支援する CSRF 対策ライブラリについても紹介しています。CSRF 脆弱性に対する理解を深め、よりセキュアな Web アプリケーション開発を行う一助として、自習用や勉強会資料としてご活用ください。

クロスサイトリクエストフォージェリ(CSRF)とその対策
https://www.jpcert.or.jp/securecoding/materials-csrf.html

2.3.2. 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。
本四半期に邦訳を追加したルールは次のとおりです。

新規追加 (2 件)

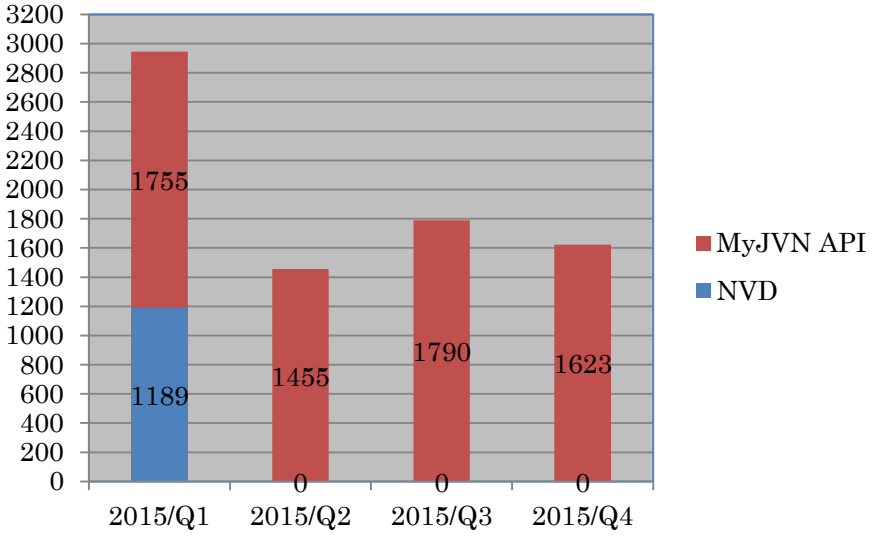
- SER12-J. 信頼できないクラスの復元はしない
- SER13-J. デシリアライズするデータは悪質なものという前提で処理する

2.4. VRDA フィードによる脆弱性の配信

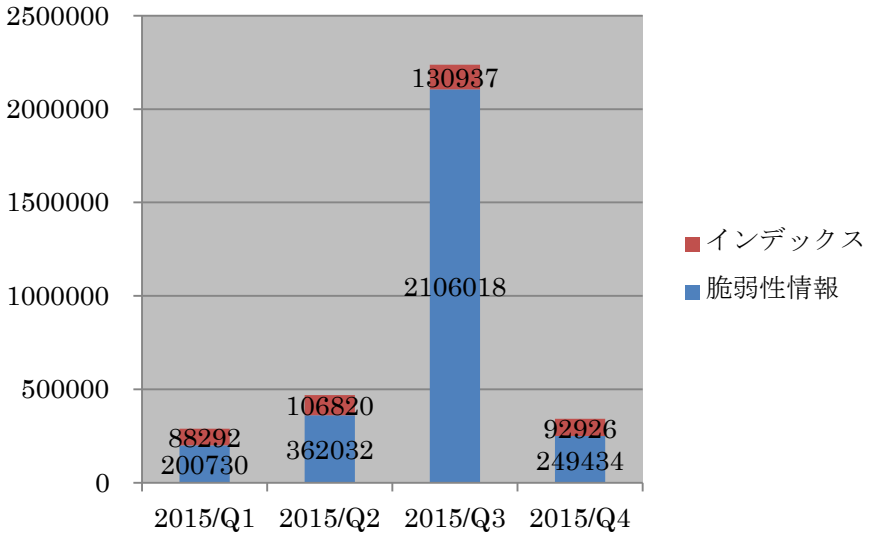
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST(National Institute of Standards and Technology)の NVD(National Vulnerability Database)を外部データソースとして利用した、VRDA(Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。
VRDA フィードについての詳しい情報は、次の 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 2-6]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 2-8]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 2-8]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。
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、2015 年第二四半期からは、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。

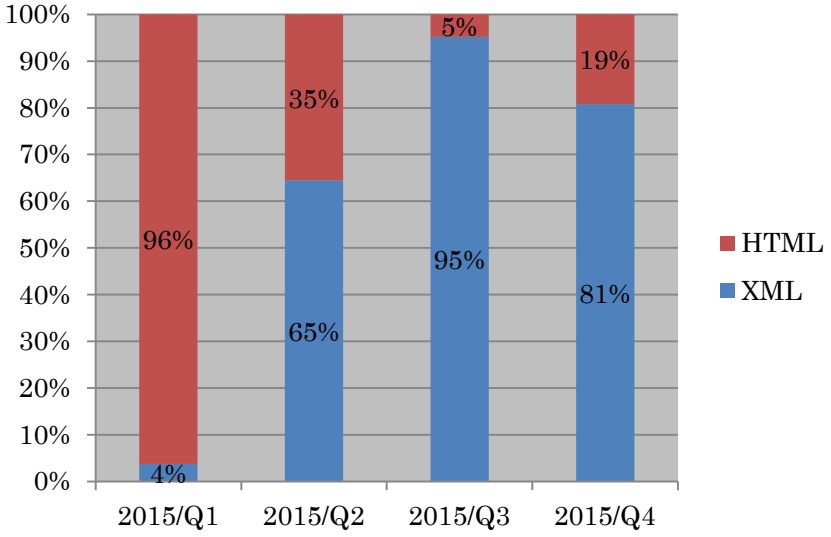


[図 2-6 VRDA フィード配信件数]



[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、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、前四半期の約 12%に減少しました。



[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、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 形式の利用割合が高い傾向に変化は有りませんが、前四半期と比較し、HTML 形式の利用割合が、約 4 倍に増加しました。

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 284 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 1 件でした。

発行件数：1 件
2015-12-25 [参考情報] Juniper Networks 社の ScreenOS に複数の脆弱性

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

2015-10-15　制御システムセキュリティニュースレター 2015-0009
2015-11-06　制御システムセキュリティニュースレター 2015-0010
2015-12-11　制御システムセキュリティニュースレター 2015-0011

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 509 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 1 件でした。本報告はインターネットに接続された制御システム関連機器に関するもので、IP アドレスが 602 件列挙されていました。このうち直接連絡が可能な 15 の IP アドレスについて調査を行い、外部からアクセスできる状態で、かつ将来的なインシデントにつながる可能性がある 1 件(3IP)に対して情報提供しました。
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、制御システム機器や関連プロトコルに関連するインシデントが起きるリスクが高まっていると考え、「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、7 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)を配付しています。本四半期は、日本版 SSAT に関して 7 件、J-CLICS に関して 17 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 185 件、J-CLICS が 269 件となりました。

3.5 海外セミナー参加報告会の開催

2015 年 12 月 10 日、「海外カンファレンス参加報告会」と題したセミナーを開催いたしました。本セミナーでは、最近にスウェーデンと米国でそれぞれ開催された制御システムセキュリティに関するカンファレンスの「4SICS」と「ICS Cyber Security Conference 2015」において注目された講演や技術動向をまとめて、背景にある問題意識を交えながら報告いたしました。セミナーには、制御システム関連のアセットオーナーやベンダの方を中心に 21 名の方にご参加いただきました。

4. 国際連携活動関連

4.1 海外 CSIRT 構築支援および運用支援活動

海外の National CSIRT(Computer Security Incident Response Team)等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. 経済産業省の委託事業によるインドネシアへの専門家派遣 (11 月 11 日-13 日)

JPCERT/CC はインドネシアの重要インフラ企業のサイバーセキュリティ対策状況の調査を行いました。現地の大手 ISP やコングロマリットを訪問し、現在講じているサイバーセキュリティ対策や今後の課題等についてヒアリングを行いました。

また、現地滞在中に開催された、一般財団法人 海外産業人材育成協会 (HIDA) が経済産業省からの委託を受けて実施している「平成 27 年度貿易投資促進事業」の採択案件「ASEAN 重要インフラ関係者の情報セキュリティ強化支援事業 インドネシア／ジャカルタ海外研修」の 11 月 12 日の講義枠において、インドネシアを含めた ASEAN の重要インフラ事業者や政策担当者に向けて、日本のサイバー攻撃動向や制御システムセキュリティへの取り組み等についての講義を行いました。

4.1.2. アフリカ CSIRT 構築支援 (11 月 29 日-12 月 2 日)

JPCERT/CC は、アフリカの CSIRT 構築支援の一環として、コンゴ共和国のポワント・ノワールにて開催された AFRINIC-23 で、Web 改ざん等のインシデントレスポンスに関する一日半の CSIRT トレーニングを 11 月 29 日から 30 日にかけて行いました。コンゴ共和国やその近隣のコンゴ民主共和国、アンゴラ等から約 25 名が参加しました。本トレーニングは、アフリカ諸国の CSIRT コミュニティであり、アジア地域との連携を促進する AfricaCERT が、AFRINIC-23 のプログラムの一つとして開催した「AfricaCERT Workshop」の一部として行われました。JPCERT/CC は同様のトレーニングを 2010 年春からほぼ半年ごとに実施しています。

[図 4-1 トレーニングの様子]

また、AfricaCERT Workshop では、AfricaCERT の活動状況や今後の活動計画、アフリカにおけるサイバーセキュリティ動向について発表があり、参加各国からはそれぞれの活動報告がありました。JPCERT/CC は APCERT の活動状況等を共有し、今後の連携の可能性について意見交換を行いました。

AFRINIC-23 および AfricaCERT の詳細については、次の Web ページをご参照ください。

AFRINIC-23
https://meeting.afrinic.net/afrinic-23/

AfricaCERT
http://www.africacert.org/home/

情報セキュリティに関する制度や技術が発展段階にある国・地域等からのサイバー攻撃も、日本のインターネットユーザにとって脅威となります。アフリカ地域に起因するインシデントが、今後の急速なインターネット普及に伴って増え、その一部は日本にも影響を及ぼすと懸念されます。JPCERT/CC は、そのような緊急事態にも迅速かつ円滑な対応ができるよう、同地域との連携強化の基盤づくりに努めています。

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 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)

2003 年 2 月の APCERT 発足時から継続して JPCERT/CC は Steering Committee (運営委員会) のメンバに選出されており、事務局も継続して担当しています。APCERT の詳細および APCERT における JPCERT/CC の役割については、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 11 月 20 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 Steering Committee メンバとして本会議に参加すると同時に、事務局としてのサポートを行いました。

4.2.2 FIRST (Forum of Incident Response and Security Teams)

JPCERT/CC は、1998 年の加盟以来 FIRST でも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、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 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
https://www.first.org/

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

4.2.2.1 Seoul 2015 FIRST Technical Colloquium への参加 (11 月 17 日-18 日)

JPCERT/CC は、11 月 17 日から 18 日に韓国のソウルで開催された FIRST Technical Colloquium に参加し、日中韓の CSIRT 連携について講演を行いました。また、JPCERT/CC の国際部シニアアナリスト 小宮山功一朗が、FIRST 理事として本イベントのオープニングスピーチを行いました。さらに、FIRST 理事の活動の一環として 2016 年にソウルにて開催予定の FIRST 年次会合に向けた準備をローカルホストの韓国 KrCERT/CC と行いました。

Seoul 2015 FIRST Technical Colloquium についての詳細は、次の Web ページをご参照ください。

Seoul 2015 FIRST Technical Colloquium
https://www.first.org/events/colloquia/seoul2015

4.2.3 海外カンファレンス等への参加

4.2.3.1 ルーマニア CERT-Ro 年次会合での講演 (10 月 5 日-6 日)

ルーマニアの National CSIRT の第 5 回年次会合が 10 月 5 日から 6 日にブカレストで開催され、JPCERT/CC 職員が参加して講演を行いました。同会合への参加は去年に続き 2 回目となり、JPCERT/CC の活動や日本のインシデント動向等を、ルーマニアの産学官の関係者等約 30 名に向けて紹介しました。

また、去年の同会合への参加をきっかけに JPCERT/CC が推進する IT 予防接種を CERT-Ro に提供しており、CERT-Ro がルーマニア国内にて IT 予防接種を実施した旨や、今後も継続して国内関係者に対して広めていきたい意向について確認し、引き続き連携することで合意しました。

4.2.3.2 第 2 回 NAPCI (Northeast Asia Peace and Cooperation Initiative) Forum 2015 での講演 (10 月 27 日-29 日)

10 月 27 日-29 日に韓国のソウルにて開催された第 2 回 NAPCI Forum 2015 に参加し、北東アジアの国々が集う本フォーラムにおいて、地域の共同プロジェクトの一つとしてサイバーグリーンの取組みについて講演を行いました。講演では、堅牢で継続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を訴え、サイバーグリーン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呼びかけました。

サイバーグリーンの詳細は、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

4.2.3.3 GFCE (Global Forum on Cyber Expertise) International Kickoff Meeting での講演 (11 月 2 日-3 日)

11 月 2 日-3 日にオランダのハーグにて開催された GFCE International Kickoff Meeting に参加し、サイバーグリーンについて講演を行いました。GFCE は、今年 4 月にハーグで開催された GCCS (Global Conference on CyberSpace) 2015 にて、サイバーキャパシティビルディングを推進するためのプラットフォームとして創設されました。本会議は、GFCE の第一回目の会議として、キャパシティビルディングの様々な取組みや GFCE の今後の方向性について協議する目的で開催されました。

JPCERT/CC は GCCS 2015 のオープニングセッションでサイバーグリーンの取組みを紹介したことに続き、本会議にてサイバーグリーンの構想をあらためて紹介するとともに、評価指標に関するフィードバック等を呼びかけました。

GFCE および GFCE International Kickoff Meeting の詳細は、次の Web ページをご参照ください。

GFCE

https://www.thegfce.com/

4.2.4 海外 CSIRT 等の来訪および往訪

4.2.4.1 JTEC による APT 研修の研修員来訪(10 月 28 日)

一般財団法人 海外通信・放送コンサルティング協力 (JTEC) が APT (Asia-Pacific Telecommunity：アジア太平洋電気通信共同体) から受託して実施している「サイバーセキュリティー情報の共有化およびアジア太平洋地域における相互連携の取組み」の研修コースを受講中の 15 名（アフガニスタン、バングラデシュ、ブータン、カンボジア、クック諸島、インド、ラオス、モルディブ、ネパール、パキスタン、パラオ、フィリピン、スリランカ、タイ、ベトナム）の来訪を受け、JPCERT/CC が講義を行いました。CSIRT の役割や JPCERT/CC の活動、日本におけるインシデント動向、TSUBAME やサイバーグリーンのプロジェクトについて紹介した後、活発な質疑が行われ、日本および各国におけるインターネットセキュリティ対策の状況が共有されました。

4.2.4.2 スリランカ TechCERT の来訪 (11 月 2 日)

スリランカの TechCERT より Gihan Dias 氏が来訪し、TechCERT および JPCERT/CC の活動状況や、スリランカ、日本において発生しているインシデントの動向等について情報を共有しました。また、セキュアコーディングトレーニング等を通した今後の連携について協議しました。

4.2.4.3 米国 US-CERT との年次会合、第 11 回日米重要インフラ防護フォーラムでの講演 (12 月 1 日-4 日)

JPCERT/CC は、US-CERT、ICS-CERT、CS&C 等のインシデント対応で協力関係にある米国の組織との年次会合を 12 月 1 日にワシントン D.C.で行いました。各組織の活動状況や、日米におけるインシデント動向およびインシデント対応における連携等について情報共有および意見交換を行い、今後も密な連携を維持していくことを確認しました。

また、12 月 3 日および 4 日に開催された、第 11 回日米重要インフラ防護フォーラムに参加し、講演を行いました。昨年に引き続いて、サイバーグリーンの構想をあらためて紹介するとともに、インターネットの健全性とリスクの指標（サイバーグリーンインデックス）に関するフィードバック等を呼びかけました。

4.2.4.4 シンガポール CSA (Cyber Security Agency) 等の来訪 (12 月 3 日)

SingCERT の母体組織である CSA の Ng Hoo Ming 氏 他 6 名が来訪し、CSA および JPCERT/CC の活動状況やシンガポール、日本において発生しているインシデントの動向等について情報共有を行い、今後も TSUBAME やサイバーグリーンのプロジェクトを通して一層の連携強化を図ることを確認しました。

4.2.4.5 台湾 TWCERT/CC 等の来訪 (12 月 10 日)

TWCERT/CC の母体組織である台湾行政院資通安全辦公室の Hsiu-Chin Hsiao 氏 他、TWCERT/CC や TWNCERT 関係者 8 名が来訪し、TWCERT/CC や TWNCERT および JPCERT/CC の活動状況や、台湾、日本において発生しているインシデントの動向およびインシデント対応における連携等について情報共有と意見交換を行い、今後も密な連携を維持していくことを確認しました。

4.3 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)を通して、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 の活動等について英文による情報発信を継続的に行っています。本四半期は次の記事をブログに掲載しました。

APCERT Annual General Meeting and Conference 2015 in Kuala Lumpur (10 月 13 日)
http://blog.jpcert.or.jp/2015/10/apcert-annual-general-meeting-and-conference-2015-in-kuala-lumpur.html

The 5th CERT-RO Annual International Conference in Bucharest and Latest Cyber Security Trends in Romania (10 月 21 日)
http://blog.jpcert.or.jp/2015/10/the-5th-cert-ro-annual-international-conference-in-bucharest-and-latest-cyber-security-trends-in-romania.html

Emdivi and the Rise of Targeted Attacks in Japan (11 月 6 日)
http://blog.jpcert.or.jp/2015/11/emdivi-and-the-rise-of-targeted-attacks-in-japan.html

A Volatility Plugin Created for Detecting Malware Used in Targeted Attacks (11 月 9 日)
http://blog.jpcert.or.jp/2015/11/a-volatility-plugin-created-for-detecting-malware-used-in-targeted-attacks.html

Decrypting Strings in Emdivi (11 月 19 日)
http://blog.jpcert.or.jp/2015/11/decrypting-strings-in-emdivi.html

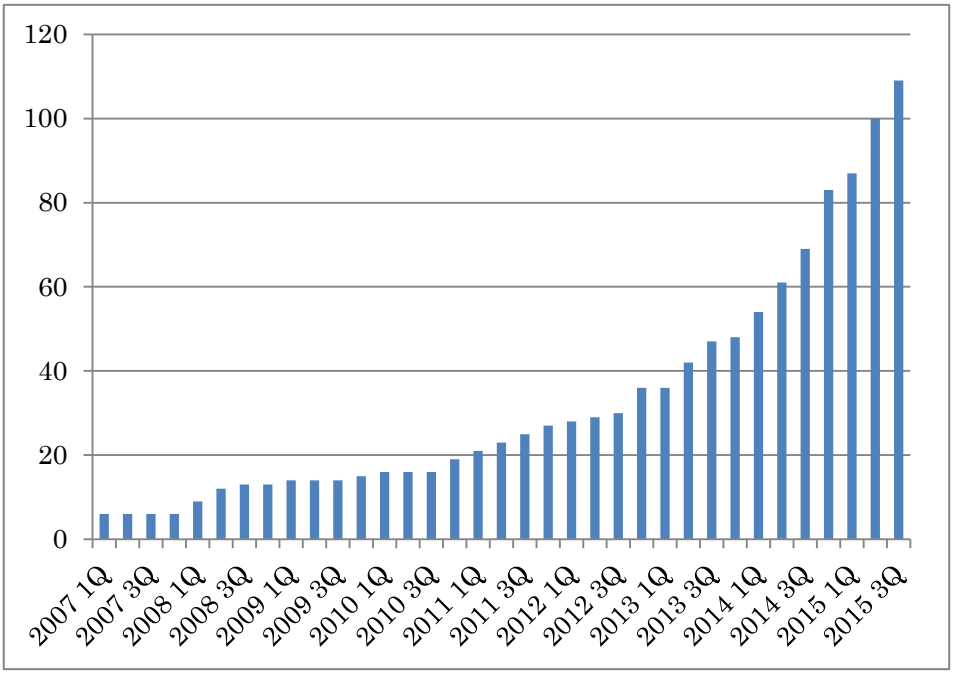
Malware Analysis Training Course at Security Camp Japan 2015 (12 月 21 日)
http://blog.jpcert.or.jp/2015/12/malware-analysis-training-course-at-security-camp-japan-2015.html

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。

本四半期における会員組織の異動では、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)、中部電力株式会社 (HAMA-CSIRT)、キヤノン電子株式会社 (Canon-Elec-CSIRT)、アフラック (AHIRU)、三菱電機株式会社 (MELCO-CSIRT)、農林中央金庫 (NB-CSIRT)と、協力会員として国立研究開発法人情報通信研究機構 (NICT-CSIRT)を含む 11 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]

本四半期における活動では、「第 11 回シーサートワーキンググループ会」を次の要領で開催いたしました。シーサートワーキンググループ会は、日本シーサート協議会の会員、およびこれから組織内にシーサートを構築し、日本シーサート協議会への加盟を検討している方々が参加する会合です。会合では、インシデント対応に関する勉強会やディスカッション、組織内シーサートの構築や運用に関する課題認識や意見の交換等が行われます。

第 11 回シーサートワーキンググループ会
　2015 年 12 月 8 日 (火) 14:00-17:40
　会場：株式会社日立製作所（HIRT）
　参加人数：179 名

この会合では、新しく加盟した 14 チームが自組織のシーサートチームの紹介を、加盟組織が講演しました。

加盟組織の増加とともに、12 の各ワーキンググループでも引き続き登録者が増え、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一層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

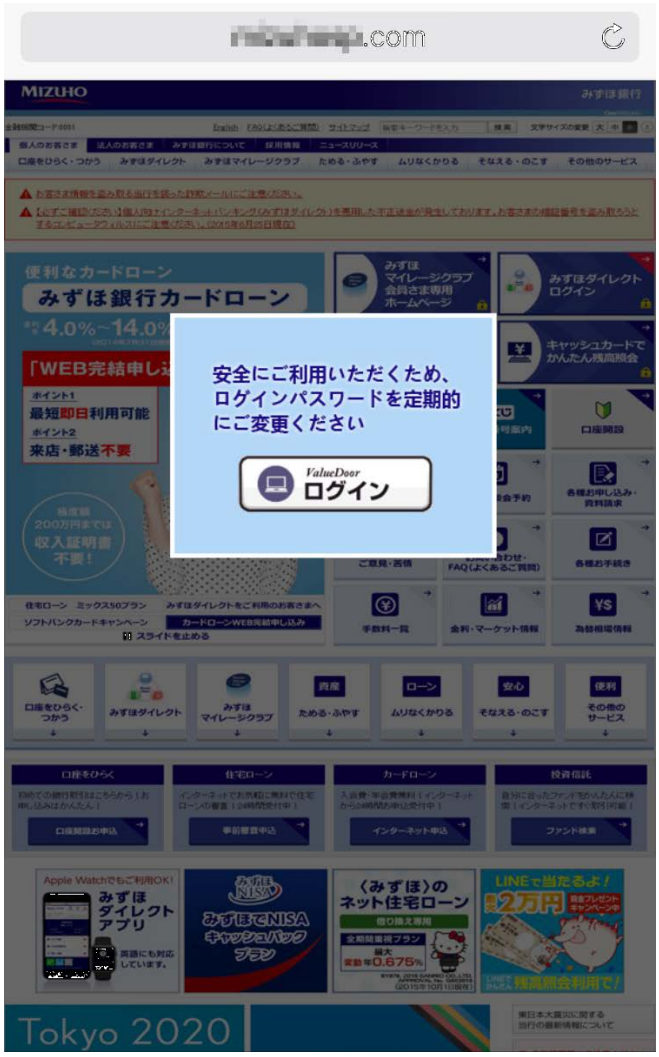
JPCERT/CC は、フィッシング対策協議会(以下「協議会」といいます。)の事務局を担当しており、経済産業省からの委託により、協議会における各ワーキンググループ活動の運営や、協議会名での一般消費者からのフィッシングに関する報告・問合せの受付、報告に基づいたフィッシングサイトに関する注意喚起等の活動を行っています。

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 13 件発信しました。

本年度当初に始まった、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。また、以前からあったオンラインゲームサイトをかたるフィッシングは、本四半期においても継続的に報告されました。なお、本四半期においては、Apple 社をかたるフィッシングのサイトの報告が多数寄せられました。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、合計 14 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。その内訳は、金融機関をかたるフィッシング関連が 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を扱った[図 6-1]の「みずほ銀行をかたるフィッシング (2015/10/28)」等の 10 件、通信事業者をかたるフィッシング関連が [図 6-2]の「J:com をかたるフィッシング (2015/10/20)」の 1 件、その他が[図 6-3]の「Apple をかたるフィッシング (2015/10/02)」等の 3 件でした。



[図 6-1] みずほ銀行をかたるフィッシング (2015/10/28)

https://www.antiphishing.jp/news/alert/mizuho_20151028.html

[図 6-2] J:com をかたるフィッシング (2015/10/20)
https://www.antiphishing.jp/news/alert/jcom_20151020.html

[図 6-3] Apple をかたるフィッシング (2015/10/02)
https://www.antiphishing.jp/news/alert/apple_20151002.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、すべてについてサイトの停止を確認しました。

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 10 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201510.html
フィッシング対策協議会 2015 年 11 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201511.html
フィッシング対策協議会 2015 年 12 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201512.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 31 回運営委員会
日時：2015 年 10 月 16 日 16:00 - 18:00
場所：トッパン・フォームズ株式会社

フィッシング対策協議会 第 32 回運営委員会
日時：2015 年 11 月 13 日 16:00 - 18:00
場所：トッパン・フォームズ株式会社

フィッシング対策協議会 第 33 回運営委員会
日時：2015 年 12 月 11 日 16:00 - 18:00
場所：GMO グローバルサイン株式会社

7.2 フィッシング対策セミナー2015 開催

フィッシング対策セミナー2015 を次のとおり開催しました。

フィッシング対策セミナー2015
日時：2015 年 11 月 20 日 13:00 - 18:00
場所：大崎ブライトコアホール

7.3 日本版 「STOP. THINK. CONNECT. 立ち止まって、考えて、ネットを楽しむためのクイズ」 を公開

日本版「STOP. THINK. CONNECT. 立ち止まって、考えて、ネットを楽しむためのクイズ」は、中学生程度の年齢を対象の中心に定め、サイバー空間の安全習慣を知ってもらうための学習資料として公開いたしました。

日本版 「STOP. THINK. CONNECT. 立ち止まって、考えて、ネットを楽しむためのクイズ」
https://www.antiphishing.jp/news/info/stc_jpn_online_safety_quiz.html

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 7 月 1 日から 2015 年 9 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 3 四半期(7 月～9 月)]
(2015 年 10 月 27 日)
https://www.jpcert.or.jp/press/2015/vulnREPORT_2015q3.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 7 月～9 月
(2015 年 10 月 28 日)
https://www.jpcert.or.jp/tsubame/report/report201507-09.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 3 件の記事を公開しました。

(1) 標的型攻撃に使われるマルウエアを検知する Volatility Plugin(2015-10-28)
マルウエアを検知し、検知されたマルウエアの設定情報を抽出するために JPCERT/CC が作成したツール「apt17scan.py」について紹介しました。また、このツールをソフトウエア開発プロジェクトのための共有ウェブサービス GitHub で公開しました。

標的型攻撃に使われるマルウエアを検知する Volatility Plugin(2015-10-28)
https://www.jpcert.or.jp/magazine/acreport-aptscan.html
JPCERTCC/aa-tools・GitHub
https://github.com/JPCERTCC/aa-tools

(2) Emdivi が持つ暗号化された文字列の復号(2015-10-28)
遠隔操作マルウェア Emdivi を分析するために JPCERT/CC が作成した IDAPython スクリプト「emdivi_string_decryptor.py」について紹介しました。また、このスクリプト等をソフトウエア開発プロジェクトのための共有ウェブサービスの GitHub で公開しました。

Emdivi が持つ暗号化された文字列の復号(2015-10-28)
https://www.jpcert.or.jp/magazine/acreport-emdivi.html
JPCERTCC/aa-tools・GitHub
https://github.com/JPCERTCC/aa-tools

(3) 攻撃者が悪用する Windows コマンド(2015-12-02)
侵入した Windows OS 上で攻撃者が使用する Windows コマンドを明らかにし、攻撃者は使うがユーザはほとんど使わない Windows コマンドの実行を抑止ないし監視することで、攻撃を防止ないし検知する方法を紹介しました。

攻撃者が悪用する Windows コマンド(2015-12-02)
https://www.jpcert.or.jp/magazine/acreport-wincommand.html

8.4 高度サイバー攻撃への対処におけるログの活用と分析方法

JPCERT/CC では、高度サイバー攻撃に関する様々な調査研究を行ってきました。その一つとして、複数のサーバや機器等に 記録される特徴的なログを適切に採取し分析することにより、侵入や攻撃の影響範囲を捉えられる可能性があることがわかりました。本書は、高度サイバー攻撃への備えと効果的な対処の観点から、一般的に利用される機器に、攻撃者の活動の痕跡をログとして残すための考え方、それらのログから痕跡を見つけ出す方法などをまとめたものです。また、本書の内容を抽出したプレゼンテーション資料も公開しました。

高度サイバー攻撃への対処におけるログの活用と分析方法
https://www.jpcert.or.jp/research/APT-loganalysis_Report_20151117.pdf
ログを活用した高度サイバー攻撃の早期発見と分析（プレゼンテーション資料）
https://www.jpcert.or.jp/research/APT-loganalysis_Presen_20151117.pdf

9. 主な講演活動一覧

(1) 真鍋 敬士(理事・分析センター長) ：
「高度化するサイバー攻撃、その時企業で何が起こっているのか？」
日経ビジネスイノベーションフォーラム,2015 年 10 月 2 日
(2) 竹田 春樹(分析センター　リーダ) ：
「サイバー攻撃の最新動向について」
情報セキュリティワークショップ in 越後湯沢 2015, 2015 年 10 月 10 日
(3) 久保 正樹(情報流通対策グループ マネージャ), 佐藤 裕二(情報流通対策グループ リードアナリスト) , 戸田 洋三(情報流通対策グループ リードアナリスト) :
「セキュアプログラミング Web アプリケーション」
東京電機大学 国際化サイバーセキュリティ学特別コース(CySec)「セキュアシステム設計・開発」, 2015 年 10 月 17 日
(4) 朝長 秀誠(分析センター), 中村 祐(分析センター) :
「日本の組織をターゲットにした攻撃キャンペーンの詳細」
CODE BLUE 2015, 2015 年 10 月 28 日
(5) 戸田 洋三(情報流通対策グループ リードアナリスト) :
「[CON4844] Case Studies and Lessons Learned from Certificate Validation Vulnerabilities」
JavaOne 2015, 2015 年 10 月 29 日
(6) 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) :
「FISC 安全対策基準にみる高度サイバー攻撃」
FISC セミナー, 2015 年 11 月 4 日
(7) 久保 正樹(情報流通対策グループ マネージャ) ：
「標的型攻撃インシデント対応の中で見た現実」
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) :
「経営におけるセキュリティのインパクト ～基本的な用語解説を交えながら～」

水野 哲也(早期警戒グループ 情報セキュリティアナリスト) :
「ログを活用した標的型攻撃の早期発見と分析」
Internet Week 2015, 2015 年 11 月 17 日～20 日

(8) 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) :
「FISC 安全対策基準にみる高度サイバー攻撃」
金融情報システムセンター FISC セミナー, 2015 年 11 月 4 日

(9) 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脅威とその分析」
富士通エフ・アイ・ピー株式会社 社内セミナー, 2015 年 11 月 19 日

(10) 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) :
「学術機関におけるサイバー攻撃の脅威と対策」
総合研究大学院大学 学内セミナー, 2015 年 11 月 20 日

(11) 有村 浩一(常務理事) :
「サイバーセキュリティ対策の強化に向けた提言」
日本経済団体連合会 情報通信委員会, 2015 年 11 月 24 日

(12) 久保 正樹(情報流通対策グループ マネージャ) :
「制御システム用ソフトウェアの脆弱性にみる対策に有効な CERT C コーディングルール」
QAC User's Meeting 2015, 2015 年 11 月 24 日

(13) 満永 拓邦(早期警戒グループ 技術アドバイザー) :
「2015 年サイバーセキュリティ動向」
株式会社バンダイナムコエンターテインメント 情報セキュリティ講演会, 2015 年 12 月 1 日

(14) 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) :
「IoT 時代と高度サイバー攻撃」
第 7 回 TCG JRF 公開セキュリティーワークショップ, 2015 年 12 月 2 日

(15) 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) :
「変化するサイバー攻撃への対応～その防御策を検討するためのポイント~」
企業情報化協会 第 10 回期グループ CIO 交流会議, 2015 年 12 月 2 日

(16) 満永 拓邦(早期警戒グループ 技術アドバイザー) :
「セキュリティインシデントの傾向から読み解く！マイナンバー等重要情報の取扱い」
株式会社ナノオプト・メディア 今からはじめるマイナンバー対策セミナー, 2015 年 12 月 8 日

(17) 満永 拓邦(早期警戒グループ 技術アドバイザー) :
「標的型攻撃から重要な情報資産を守るためのベストプラクティス」
日経 BP 情報セキュリティ戦略セミナー, 2015 年 12 月 9 日

(18) 久保 啓司(インシデントレスポンスグループ マネージャ) :
「標的型攻撃時代のインシデントレスポンス」
SB クリエイティブ株式会社 インシデント・レスポンス～標的型攻撃・サイバー犯罪時代の事故前提社会への備え, 2015 年 12 月 11 日

10. 主な執筆一覧

(1)宮地 利雄(技術顧問)：
「制御システムセキュリティの傾向」
月刊計装 12 月号,2015 年 11 月 10 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) Email Security Conference 2015/ID Management Conference 2015
主　催：ナノ・オプトメディア
開催日：2015年10月09日(金),10月16日(金)
(2) 第12回(東京)、13回(大阪)迷惑メール対策カンファレンス
主催：IA Japan
開催日：2015年10月09日(金),10月16日(金)
(3) CODE BLUE2015
主　催：CODE BLUE実行委員会
開催日：2015年10月27日(火)～10月28日(水)
(4) InternetWeek2015
主　催：日本ネットワークインフォメーションセンター
開催日：2015年11月17日(火)～11月20日(金)
(5) 今からはじめるマイナンバー対策セミナー
主　催：ナノ・オプトメディア
開催日：2015年12月8日(火)
(6) 第12回デジタル・フォレンジック・コミュニティ2015
主　催：特定非営利活動法人デジタル・フォレンジック研究会
開催日：2015年12月14日(月)～12月15日(火)

12. セミナー開催

本四半期は、次の行事を開催しました。

(1) SecurityDay 2015
主　催：SecurityDay 運営委員会
・JPCERT コーディネーションセンター(JPCERT/CC)
・日本インターネットプロバイダー協会 (JAIPA)
・日本データ通信協会 (Telecom-ISAC Japan)
・日本ネットワークセキュリティ協会 (JNSA)
開催日：2015 年 12 月 16 日(水)

■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