JPCERT/CC®

JPCERT-PR-2016-01
発行日：2016-04-14

JPCERT/CC 活動概要 [2016 年 1 月 1 日 ～ 2016 年 3 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(APT)への備えと対応ガイド ～企業や組織に薦める一連のプロセスについて」を公開

JPCERT/CC は、高度サイバー攻撃(APT)の被害を防ぎ最小限に抑えるための対処法をガイドする「高度サイバー攻撃(APT)への備えと対応ガイド ～企業や組織に薦める一連のプロセスについて」を 2016 年 3 月 31 日に公開しました。本ガイドは、米国マンディアント社および米国ロッキード・マーティン社から提供された、高度サイバー攻撃(APT)への対応に関する豊富な専門知識と経験にもとづいた情報を、JPCERT/CC の連携先や支援先の組織に、高度サイバー攻撃(APT)に対処するためのベストプラクティスとして、米国デルタリスク社が、2013 年 7 月に第 1 版を作成し、さらに、SANS/CSC「Top20 Critical Security Controls」と NIST のサイバーセキュリティフレームワークからの基本的対策を参考に改訂した第 2 版(2015 年 3 月に再構成)の Web 版として公開したものです。

本ガイドは、まず APT 攻撃の定義と侵攻モデルを概説し、APT 攻撃の被害を防止ないし軽減するための事前準備と対処プロセスを説明しております。

JPCERT/CC が 2010 年に行った高度サイバー攻撃(APT)に関する実態調査では、社内で攻撃者による活動が行われていても、長期間にわたってその兆候を検知できなかった事例が多くみられました。異常検出後も、ログの保持や保全状況が不適切で、十分な調査ができないケースが少なからずありました。また、基本的な情報セキュリティ対策を実施していても、高度サイバー攻撃(APT)の被害に合った組織もありました。

このように従来とは異なった観点が求められている、高度サイバー攻撃(APT)への効果的な対策のために参考となる実用的なガイドとなっております。

高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて
https://www.jpcert.or.jp/research/apt-guide.html

ートピック2ー　制御システムセキュリティ啓発活動 ～制御システムセキュリティカンファレンス 2016 を開催

2 月 17 日に制御システムセキュリティカンファレンス 2016 を東京で開催しました。
今回で 8 回目となる本カンファレンスでは、北村経夫経済産業省政務官による開会挨拶に続き、「制御システムセキュリティ最前線」をテーマに、最新の制御システムセキュリティに関する情報や、制御システム利用業界や組織におけるセキュリティ強化への取組について、大学等の研究機関から重要インフラ事業者まで、さまざまな分野の方に講演をいただきました。当日は満席となる 300 名の方にご来場いただきました。参加者も、本カンファレンスを始めた 7 年前は制御システムベンダーが大多数でしたが、今回は、制御システムのアセットオーナが約 30%、制御システムベンダが約 30%、制御システムのエンジニアリング会社が約 15%となりました。

制御システムセキュリティカンファレンス 2016(プログラム)
https://www.jpcert.or.jp/event/ics-conference2016.html

制御システムセキュリティカンファレンス 2016(講演資料)
https://www.jpcert.or.jp/present/#ics-conference2016

ートピック3ー　第 12 回 APCERT 合同サイバー演習

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。

12 回目となる今回の合同サイバー演習は「進化するサイバー脅威と金融詐欺」をテーマに実施されました。インターネットバンキングの利用者を標的としたマルウエアによる被害は、日本だけでなく香港やシンガポールなど他の APCERT 加盟国・経済地域でも広く報告されています。また、スリランカにおいてもなりすましメール等を用いた金融詐欺の被害が広まっています。こうした状況を踏まえて、テーマが設定され、演習シナリオが作成されました。参加組織はシナリオを通して、関係する組織への通知やマルウエアやログの分析など、インシデント対応の手順と技術を確認しました。本演習には、APCERT 加盟組織のうち 20 経済地域から 26 チーム、および OIC-CERT (The Organisation of Islamic Cooperation – Computer Emergency Response Teams) から 6 チームが参加しました。これは過去最多の参加組織数となり、APCERT における各チームのサイバー脅威に対する危機感の強さと、近年さらに深まっている OIC-CERT との連携を表すイベントとなりました。

JPCERT/CC は、APCERT 事務局並びに演習運営委員会(Drill Organising Committee)のメンバとして、シナリオの議論や運営において主導的な役割を果たしました。また、プレーヤー(演習者)として参画するとともに、コントローラ (Exercise Control: 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。APCERT Drill 2016 についての詳細は、次の Web ページをご参照ください。

APCERT Drill 2016 - An Emerging Cyber Threat and Financial Fraud

http://www.apcert.org/documents/pdf/APCERTDrill2016PressRelease.pdf

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 4587 件、インシデント件数ベースでは 4143 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 2955 件でした。前四半期の 2053 件と比較して 44%増加しています。「調整」とは、フィッシングサイトが設置されているサイトや、改ざんにより JavaScript が埋め込まれているサイト、ウイルス等のマルウエアが設置されたサイト、「scan」のアクセス元等の管理者等に対し、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/2016/IR_Report20160414.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 645 件で、前四半期の 474 件から 36%増加しました。また、前年度同期(466 件)との比較では、38%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	48	96	45	189(29%)
国外ブランド	75	95	100	270(42%)
ブランド不明(注 2)	67	76	43	186(29%)
月別合計	190	267	188	645(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。

1 月末から 3 月前半にかけて、特定の国内金融機関を装ったフィッシングサイトが多く確認されました。この事例のフィッシングメールには、中国の複数の Web サイトの "/images"ディレクトリに不正に設置されたページが記載されており、このページから転送されるフィッシングサイトは香港や中国の IP アドレスのホストが使用されていました。

また同時期に、別の国内金融機関の類似ドメインを使用したフィッシングサイトも多数確認しています。これらのフィッシングサイトでは、正規サイトを装った.com ドメインを使用し、韓国の IP アドレスのホストが使用されていました。

オンラインゲームを装ったフィッシングサイトは、3 月半ば以降は多くの報告が寄せられています。特定のゲームを装ったフィッシングサイトが約 60URL 確認されましたが、ユニークな IP アドレスの数は 6 つのみで、すべて香港の通信事業者のものでした。また、これらのフィッシングサイト　では、無料で登録できる.cc のドメインを使用しているという特徴が見られました。

フィッシングサイトの調整先の割合は、国内が 35%、国外が 65%であり、前四半期(国内 46%、国外 54%)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、1268 件でした。前四半期の 826 件から 54%増加しています。

前四半期に引き続き、CMS を使用した Web サイトが改ざんされている例が非常に多く確認されました。

改ざんされた Web サイトに仕掛けられた不正な JavaScript によって誘導されたサイトで、Internet Explorer、Adobe Flash Player、Silverlight などのアプリケーションの脆弱性が攻撃され、その攻撃によってマルウエアがダウンロード、実行されます。攻撃される Silverlight の脆弱性は、2016 年 1 月に修正された比較的新しい脆弱性(CVE-2016-0034)であることを確認しています。

誘導先サイトからダウンロードされるマルウエアには、金銭を要求して復号するために PC 上のファイルを暗号化するランサムウエアや、アカウントなどの情報を窃取するものなどがあることを確認しています。

1.1.1.3. その他

標的型攻撃に分類されるインシデントの件数は、6 件でした。前四半期の 12 件から 50%減少しています。本四半期は、4 組織（延べ数）に対応を依頼しました。

本四半期は、標的型攻撃のインフラとして使用された国内 IP アドレスや、特定の国内組織を標的とした攻撃に使用された可能性があるマルウエアの情報などを複数の海外セキュリティ組織から受領しました。JPCERT/CC は、提供された情報をもとに、関連する国内組織に事実関係の調査を依頼しました。

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 32,000 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：1 件　https://www.jpcert.or.jp/update/2016.html

2016-01-22　注意喚起「ネットワークに接続されたシステム・機器の設定には注意を」

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：19 件（うち 4 件更新）　https://www.jpcert.or.jp/at/

2016-01-04　Adobe Flash Player の脆弱性 (APSB16-01) に関する注意喚起 (公開)
2016-01-06　Adobe Flash Player の脆弱性 (APSB16-01) に関する注意喚起 (更新)
2016-01-12　DNS ゾーン転送の設定不備による情報流出の危険性に関する注意喚起 (公開)
2016-01-13　Adobe Reader および Acrobat の脆弱性 (APSB16-02) に関する注意喚起 (公開)
2016-01-13　2016 年 1 月 Microsoft セキュリティ情報 (緊急 6 件含) に関する注意喚起 (公開)
2016-01-20　2016 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)
2016-01-20　ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2015-8704) に関する注意喚起 (公開)
2016-02-10　2016 年 2 月 Microsoft セキュリティ情報 (緊急 6 件含) に関する注意喚起 (公開)
2016-02-10　Adobe Flash Player の脆弱性 (APSB16-04) に関する注意喚起 (公開)
2016-02-17　glibc ライブラリの脆弱性 (CVE-2015-7547) に関する注意喚起 (公開)
2016-02-19　glibc ライブラリの脆弱性 (CVE-2015-7547) に関する注意喚起 (更新)
2016-03-02　OpenSSL の複数の脆弱性に関する注意喚起 (公開)
2016-03-03　OpenSSL の複数の脆弱性に関する注意喚起 (更新)
2016-03-09　2016 年 3 月 Microsoft セキュリティ情報 (緊急 5 件含) に関する注意喚起 (公開)
2016-03-09　Adobe Reader および Acrobat の脆弱性 (APSB16-09) に関する注意喚起 (公開)
2016-03-10　ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2016-1286) に関する注意喚起 (公開)
2016-03-11　Adobe Flash Player の脆弱性 (APSB16-08) に関する注意喚起 (公開)
2016-03-11　2016 年 3 月 Microsoft セキュリティ情報 (緊急 5 件含) に関する注意喚起 (更新)
2016-03-24　Oracle Java SE の脆弱性 (CVE-2016-0636) に関する注意喚起 (公開)

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 79 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。

2016-01-06　担当者が選ぶ 2015 年重大ニュース
2016-01-14　Internet Explorer のバージョンアップを
2016-01-20　NoSQL データベース「Redis」を標的としたアクセスが増加
2016-01-27　サイバーセキュリティ月間
2016-02-03　NISC が「我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針」を決定
2016-02-10　「CSIRT 人材セミナー」開催
2016-02-17　経済産業省が「秘密情報の保護ハンドブック～企業価値向上に向けて～」公開
2016-02-24　IPA が「情報セキュリティ 10 大脅威 2016」を発表
2016-03-02　Ruby 2.0.0 公式サポート終了
2016-03-09　経済産業省が「情報セキュリティ管理基準（平成 28 年改正版）」公開
2016-03-16　IPA が「2015 年度 中小企業における情報セキュリティ対策に関する実態調査 報告書」を公開
2016-03-24　警察庁が「HTTP ステータスコードを偽装する C2 サーバの観測について」を公開
2016-03-30　「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」公表

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。

【ネットワークに接続されたシステム・機器の設定に対する注意】
昨今、Internet of Things (IoT) の普及により、さまざまな機器がインターネットに接続されるようになりました。その中で、ネットワークカメラ (ネットワーク機能を備えた Web カメラなど)、複合機、データベースシステムなどの機器が、インターネットを経由して遠隔の第三者から意図せずアクセスされる事例が報じられています。JPCERT/CC でも、SHODAN などの Web サービスにおいて、インターネットからアクセス可能な状態になっているシステム・機器が、国内に多数存在していることを確認しました。

システム・機器がインターネットに接続されている場合、たとえ脆弱性がなくても、認証の設定やネットワークの設定に不備が存在すると、カメラに映し出された映像、データベースや複合機に格納された情報などが第三者に窃取されてしまう危険性があります。第三者から意図しないアクセスを受けることで、利用者が被害に遭う危険性があると JPCERT/CC では判断し、2016 年 1 月 22 日に注意喚起「ネットワークに接続されたシステム・機器の設定には注意を」のお知らせを Web サイトに掲載しました。

【glibc ライブラリの脆弱性 (CVE-2015-7547) に対する注意】
Linux などの OS にて広く利用されている glibc ライブラリにおいて、send_dg() および send_vc() の処理に起因するバッファオーバーフローの脆弱性 (CVE-2015-7547) が報告されました。JPCERT/CC の追試においても、本脆弱性による影響が再現することを確認しています。glibc ライブラリがサーバ等の OS に広く利用されているだけでなく、脆弱性の影響範囲が広範に及ぶことから、JPCERT/CC では危険性が高いと判断し、2016 年 2 月 19 日「glibc ライブラリの脆弱性 (CVE-2015-7547) に関する注意喚起」を公開しました。

1.3. インターネット定点観測

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

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

JPCERT/CC は、さまざまな地域に設置された観測用センサーを含むインターネット定点観測システム TSUBAME を構築運用するとともに、観測されたデータを各地域の CSIRT と共同で分析をするためのプロジェクトである TSUBAME プロジェクトの事務局を担当しています。2016 年 3 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。

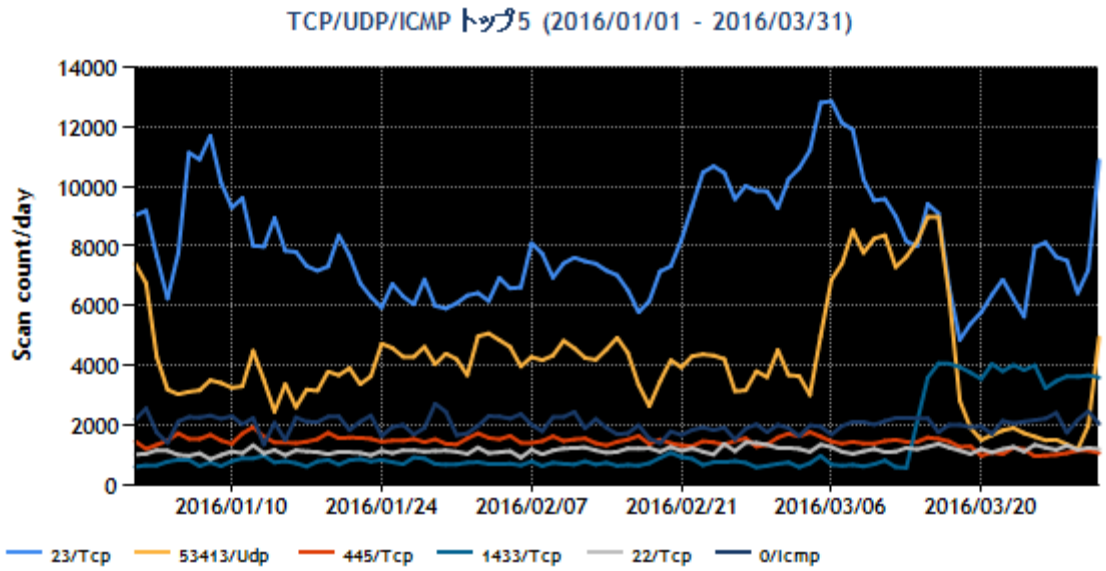
主に日本企業のシステム管理者等の方々に、自ネットワークに届くパケットの傾向と比較していただけるよう、日本国内のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に

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 10 月から 12 月分のレポートを 2016 年 2 月 4 日に公開しました。

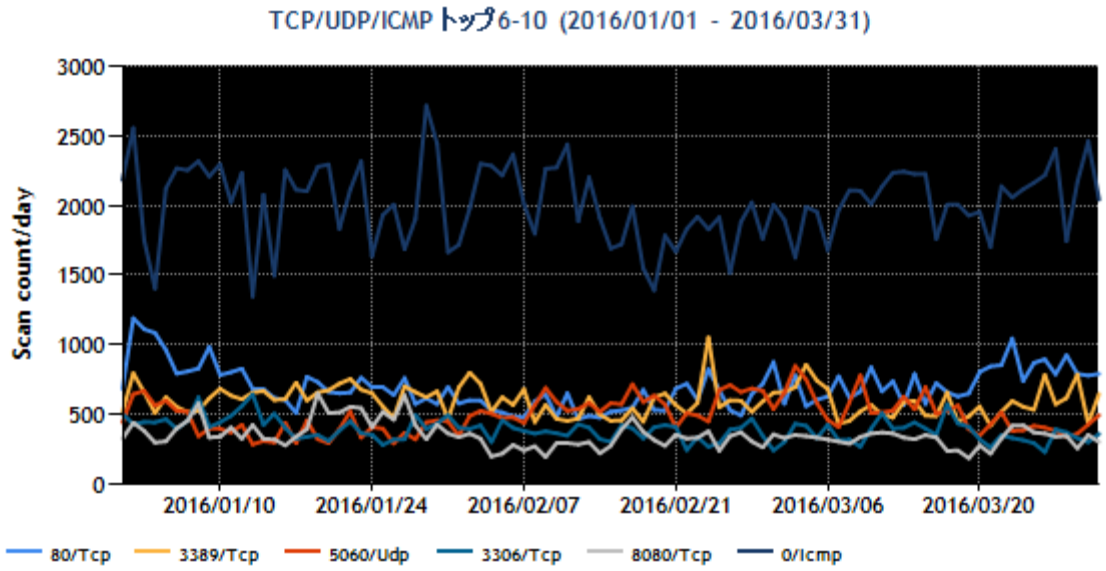
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート(2015 年 10～12 月)
https://www.jpcert.or.jp/tsubame/report/report201510-12.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。

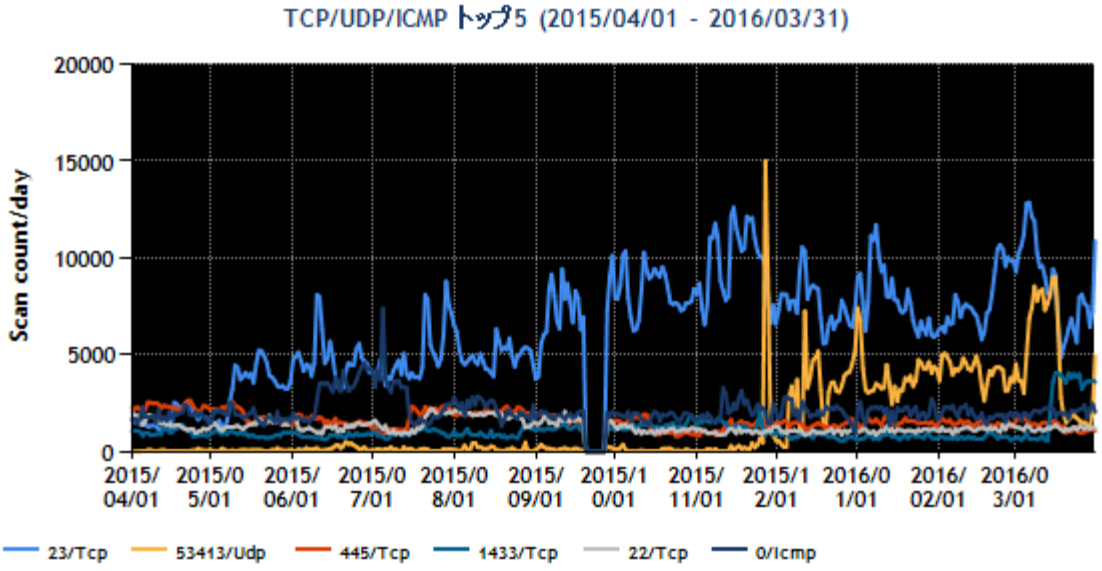


[図 1-1 宛先ポート別グラフ トップ 1-5 (2016 年 1 月 1 日-3 月 31 日)]

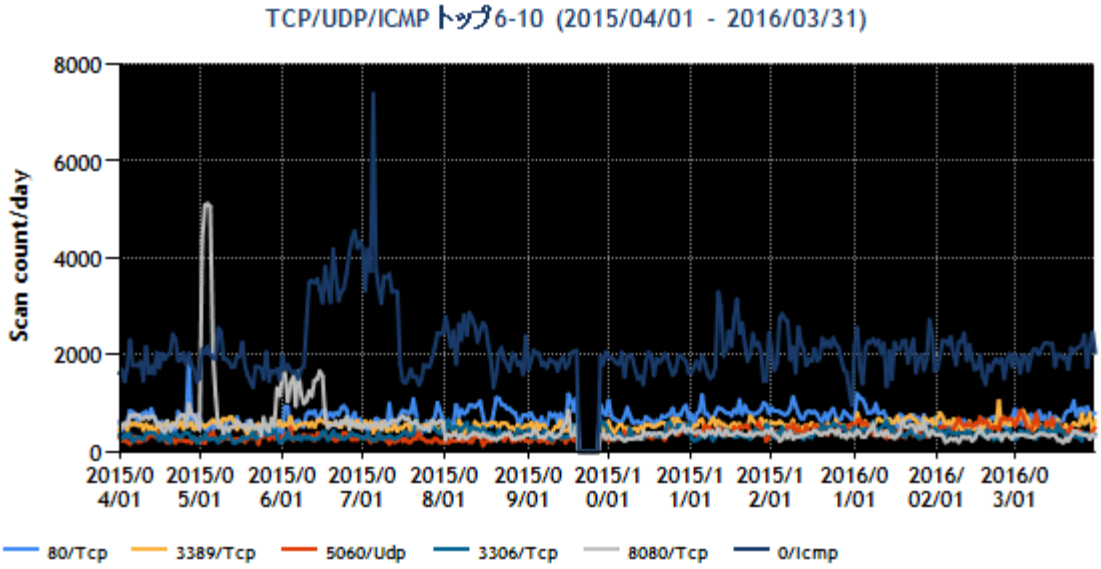


[図 1-2 宛先ポート別グラフ トップ 6-10 (2016 年 1 月 1 日-3 月 31 日)]

また、過去 1 年間 (2015 年 4 月 1 日-2016 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。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 4 月 1 日-2016 年 3 月 31 日)]



[図 1-4 宛先ポート別グラフ トップ 6-10 (2015 年 4 月 1 日-2016 年 3 月 31 日)]

本四半期は、前四半期に引き続き 23/Tcp 宛と、前四半期に増加した 53413/Udp 宛へのパケット数が高い水準にあります。3 月 14 日から、主に国外地域を送信元とした 1433/Tcp 宛のパケットが増加しています。マイクロソフト社の SQLServer を対象とした探索と考えていますが、原因はわかっていません。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) 国内の 23/TCP ポートを探索するサーバについての対応
複数の日本国内の IP アドレスを送信元とする、Telnet(23/TCP)ポート宛てのパケットが 1 月ごろよりしばしば TSUBAME で観測されました。JPCERT/CC では、過去の事例から Telnet ポートの探索や攻撃を行うマルウエアとの関連性を疑い、送信元 IP アドレスにどのような機器が接続されているかを確認しました。その結果、国内ベンダー製の機器が接続されていることが判明し、本事象に関する情報提供や推測される事象に関する分析結果などを当該機器ベンダーと共有し、今後の対応方法を相談しました。
JPCERT/CC では､該当パケットの送信元 IP アドレスの管理者にも情報を提供して善処を求めています。

(2) 韓国からの 23/TCP ポートを探索する送信元についての対応
定点観測を行っている組織間で情報交換を実施している定点観測友の会において、上述の(1)と同様 Telnet(23/TCP)ポート宛てへのパケットが、韓国の特定の ISP から特に多く送信されているという情報が共有されました。TSUBAME でも同様の傾向が観測されており、TSUBAME プロジェクトに参加している韓国の KrCERT/CC に照会し調査を依頼しました。

(3) 国内のオープンリゾルバが DNS 水責め攻撃の踏み台となっている問題への対応

国内外の多数の IP アドレスから DNS のクエリーに対するリプライパケットを TSUBAME で受信しています。受信したパケットを分析したところ、存在しないランダムなホスト名を含んだ名前解決要求パケットに対する応答パケットであることが分かりました。これは、DNS 水責め攻撃のために、オープンリゾルバに対して第三者が TSUBAME のセンサーの IP アドレスを詐称して送信した名前解決要求パケットに対する応答パケットと考えられます。

オープンリゾルバは、DNS 水責め攻撃だけでなく、リフレクション攻撃にも悪用されるので、除去することが求められています。1 月下旬に複数の事業者が DDoS 攻撃を受けたとの報道がありましたが、その攻撃では複数のプロトコルが使用され、国内のオープンリゾルバを悪用したリフレクション攻撃も含まれていたと JPCERT/CC は推測しています。

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て善処を求めました。その結果、インターネットに接続された組込 Linux ボードがオープンリゾルバとなっていた事例や、機器ベンダーが対策情報として公開しているフィルタルールの設定等をしないまま運用されていた事例が見つかりました。

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

2.1.1. 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

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扱状況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。

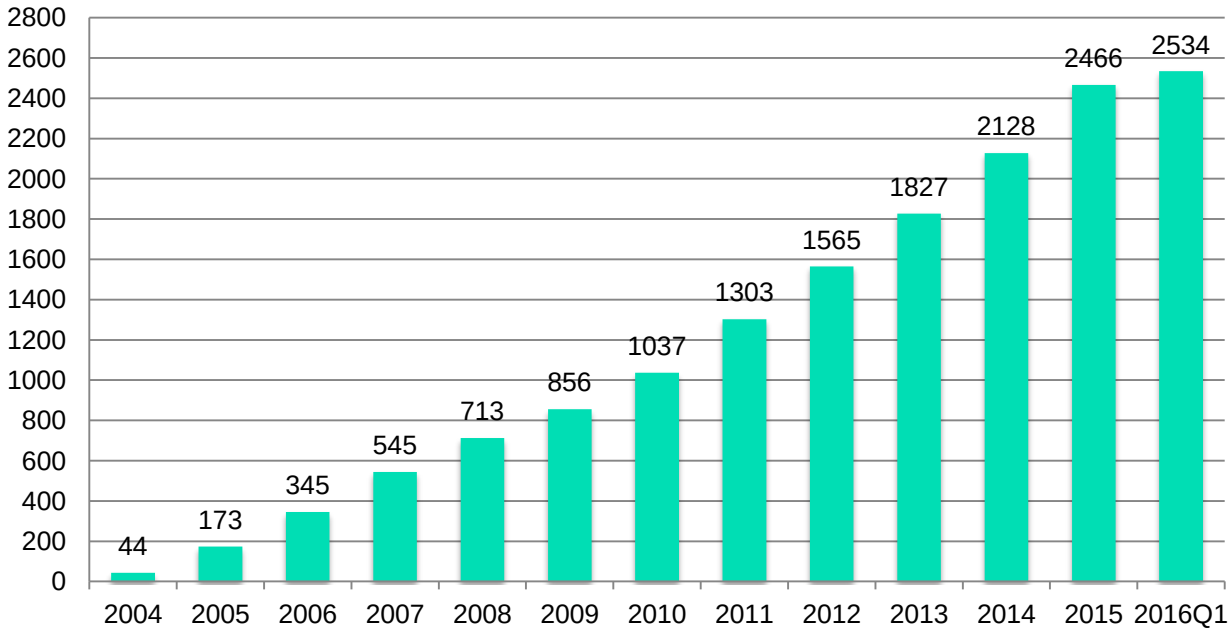
独立行政法人情報処理推進機構(IPA) 脆弱性対策
http://www.ipa.go.jp/security/vuln/

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 68 件(累計 2,534 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]

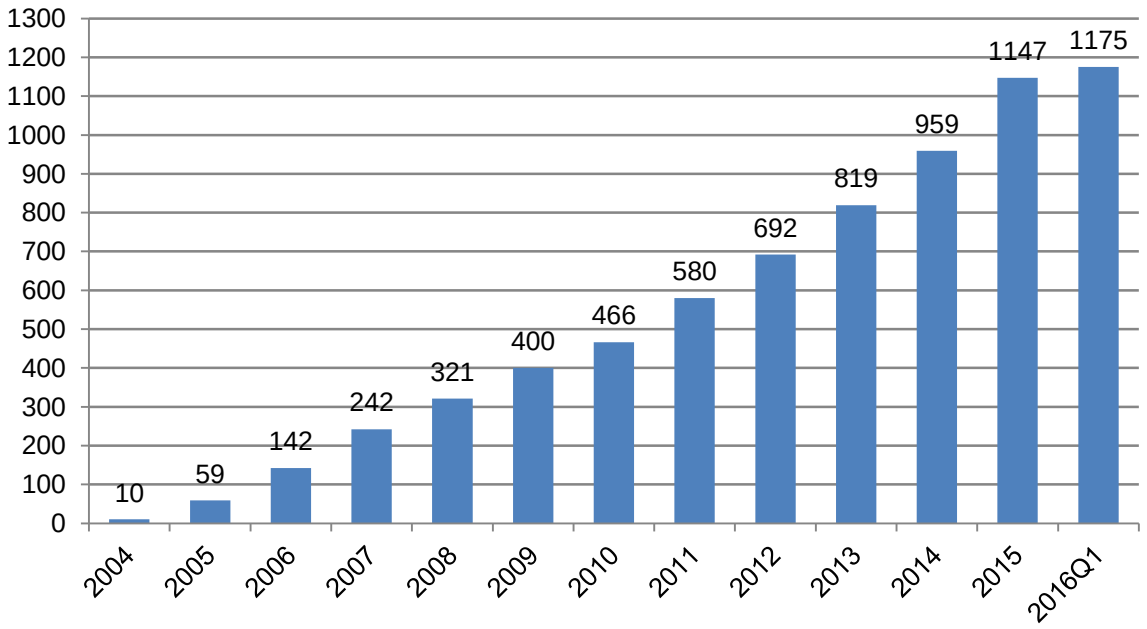
本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 28 件(累計 1,175 件)で、累計の推移は[図 2-2]に示すとおりです。28 件のうち、25 件が国内製品開発者の製品、3 件が海外の製品開発者の製品に関連したものでした。また、7 件が自社製品届出による脆弱性情報でした。

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。本四半期は、グループウエア、組込系製品、Windows または iOS 上のアプリケーションの脆弱性情

報が数多くありました。

[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]

製品分類	件数
グループウエア	7
組込系製品	7
iOS アプリ	2
ウェブアプリケーション	2
CGI	1
Windows アプリケーション	1
ウェブサイト構築ソフトウエア	1
ウェブブラウザ	1
コンテンツ管理システム(CMS)	1
サーバ製品	1
プラグイン	1
マルチプラットフォームアプリケーション	1
ライブラリ	1



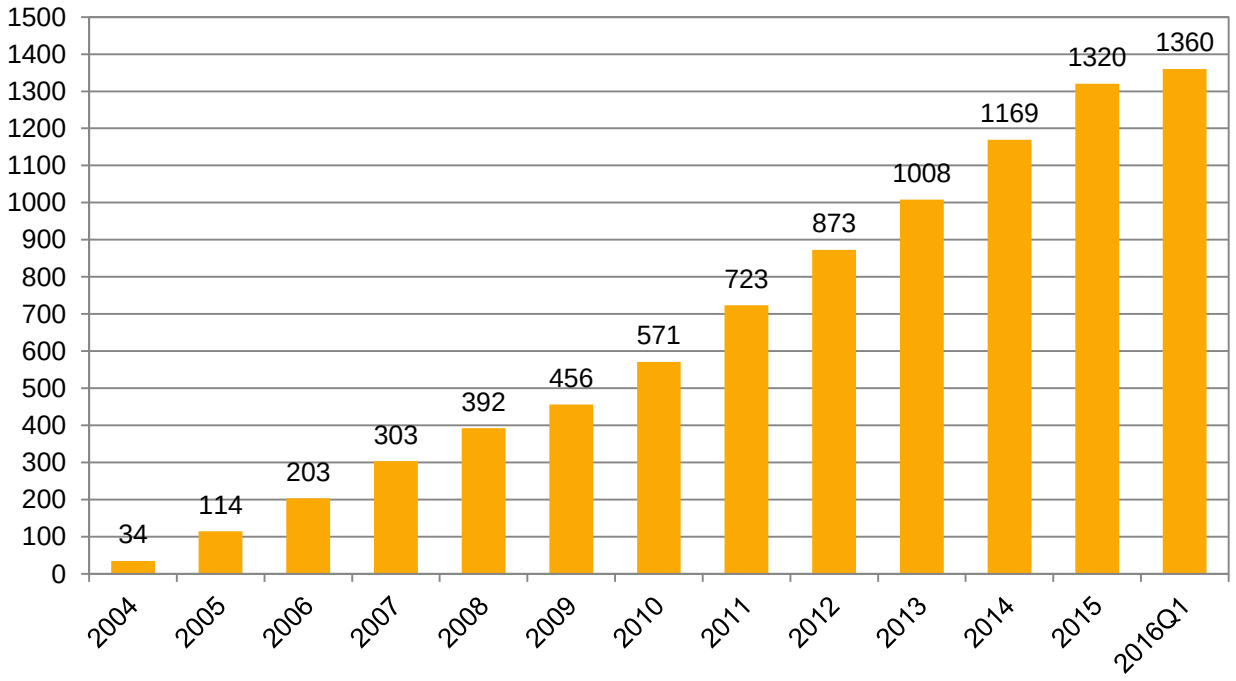
「[図 2-2 公表を行った国内取扱脆弱性情報の累積件数]

本四半期に公表した国際取扱脆弱性情報は 40 件(累計 1,360 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。本四半期も、前四半期から引き続き、組込系製品に関する脆弱性情報を多数公開しました。この要因の一つとしては、組込みルータ機器に対する CERT/CC の独自調査で、複数製品に脆弱性が見つかったことがあげられます。

[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]

製品分類	件数
組込系	10
DNS	4
プロトコル	4
ライブラリ	4
MacOS アプリケーション	2
ウェブサービス	2
AndroidOS	1
Linux ディストリビューション	1
Windows アプリケーション	1
ウェブアプリケーション	1
ウェブサーブレットコンテナ	1
ウェブサイト	1
ウェブブラウザ	1
音声映像記録、変換、配信ソフトウエア	1
航海データ記録装置	1
デバイス	1
マルチファイル変換ソリューション	1
ライセンス管理ソフトウエア	1
統合管理ソリューション	1
統合ネットワーク管理ソフトウエア	1



[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 229 件(製品開発者数で 152 件)を公表し、41 件(製品開発者数で 25 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 12 件を連絡不能開発者一覧に掲載しました。
本四半期末日時点で、合計 188 件の連絡不能開発者案件を掲載しており、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、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、利用者保護の観点から脆弱性情報を公表する手続きが定められました。この規定に従って、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。さらに、前四半期11月に開催された第三回公表判定委員会において、5件が審議され、5件すべてについて公表すべきと判定されました。それを受け、本四半期には、JVNでの公表に向けて準備を進めました。

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 28 件に、JPCERT/CC が CVE 番号を付与しました。2008 年以降においては、MITRE やその他の組織への確認や照合を必要とする特殊なケース（全体の 1 割弱）を除いて、JVN 上で公表する脆弱性のほぼすべてに CVE 番号が付与されています。

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

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

2.2. 日本国内の脆弱性情報流通体制の整備

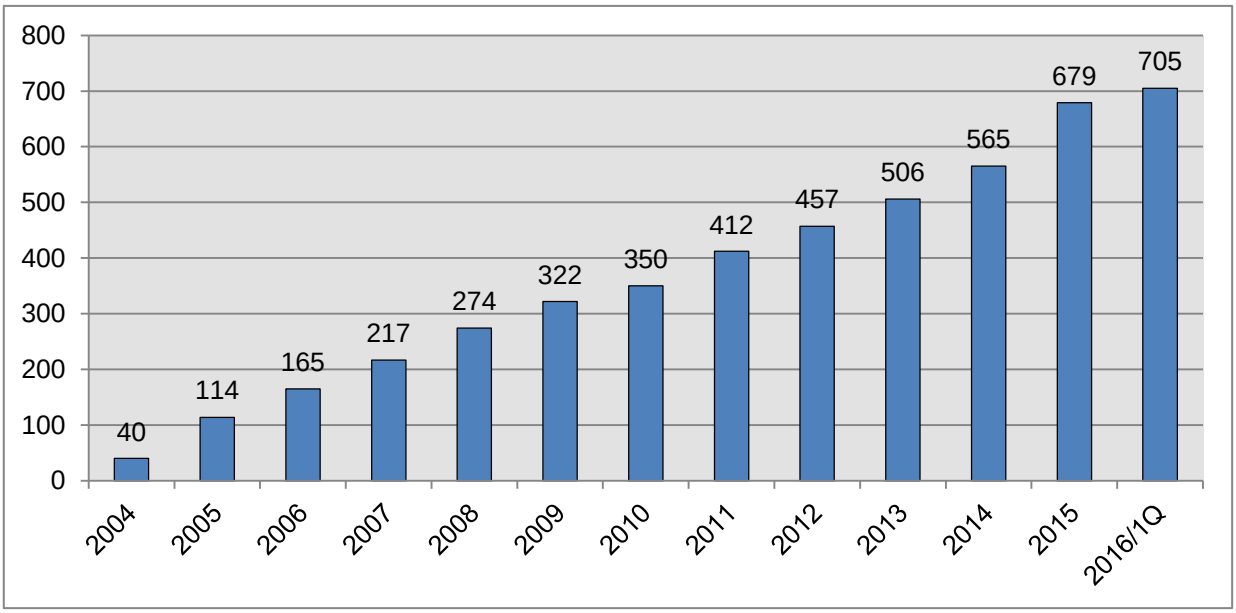
JPCERT/CC では、本基準に従って、日本国内の脆弱性情報流通体制を整備しています。
詳細については、次の Web ページをご参照ください。

脆弱性情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
脆弱性情報コーディネーション概要
https://www.jpcert.or.jp/vh/
「情報セキュリティ早期警戒パートナーシップ」の運用を開始
https://www.jpcert.or.jp/press/2004/0708.txt
情報セキュリティ早期警戒パートナーシップガイドライン(2015 年版)
https://www.jpcert.or.jp/vh/partnership_guideline2015.pdf
JPCERT/CC 脆弱性情報取扱いガイドライン
https://www.jpcert.or.jp/vh/vul-guideline2014.pdf

2.2.1. 日本国内製品開発者との連携

本基準では、脆弱性情報を提供する先となる製品開発者のリストを作成し、各製品開発者の連絡先情報を整備することが、調整機関である JPCERT/CC に求められています。JPCERT/CC では、製品開発者の皆さまに製品開発者リストへの登録をお願いしています。製品開発者の登録数は、[図 2-4]に示すとおり、2016 年 3 月 31 日現在で 705 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 2016 年 3 月 28 日にミーティングを開催し、国内外の脆弱性情報取扱制度やその周辺事情についての動向などを紹介や、脆弱性評価指標（CVSS）に関するワークショップを実施するとともに、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

2.3.1. セキュアコーディングに関する講演活動

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

本四半期は、次の 1 件の講演を行いました。

講演月日：2 月 18 日
講演タイトル: Issues, Lessons learned through the eyes of JPCERT/CC on the vulnerability handling framework in Japan
イベント名：FIRST Technical Colloquium at Raleigh, North Carolina

今回の TC (FIRST Technical Colloquium) は、IBM PSIRT がホストして行われたもので、ソフトウエアベンダの product CSIRT が集まりディスカッションを行う初めての TC となりました。JPCERT/CC からは、日本におけるこれまでの活動と課題について紹介しました。

2.3.2. 「Android プラットフォームの URLConnection クラスに HTTP ヘッダインジェクションの脆弱性」資料公開

2015 年 9 月に公開した脆弱性 JVN#21612597 (Apache Cordova プラグイン cordova-plugin-file-transfer における HTTP ヘッダインジェクションの脆弱性)の根本原因が Android Platform における Java 標準 API 実装の URLConnection クラスにあるとの追加情報が同脆弱性を報告した西村宗晃氏から寄せられました。JPCERT/CC では、この報告を受けて、Android Platform のソースコード解析および検証コードを用いた動作検証を行い、その結果を JVNVU#99757346 (Android Platform の URLConnection クラス

に HTTP ヘッダインジェクションの脆弱性)として公開するとともに、新たな試みとして、解析結果の詳細資料を Slideshare を通じて公開しました(http://www.slideshare.net/jpcert_securecoding/android-platform-urlconnection-http)。

2.3.3. OWASP ASVS (Application Security Verification Standard) および Cheat Sheet シリーズ文書の日本語訳作成

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米国の団体 OWASP が公開している文書 ASVS (Application Security Verification Standard) および Cheat Sheet シリーズ文書の日本語訳を行いました。4 月以降、JPCERT/CC の Web サイトにおいて公開するとともに、OWASP の ASVS プロジェクトおよび Cheat Sheet プロジェクトへのフィードバックを行う予定です。

2.3.4. セキュアコーディング出張セミナ

JPCERT/CC では、ソフトウエア製品等の開発を行う企業・組織を対象に、セキュアコーディングに関する出張セミナ(有償)の実施を承っています。本四半期は、国内ベンダ 3 社に対して、C/C++、Java、および CSRF とその対策に関するセキュアコーディングセミナを実施しました。

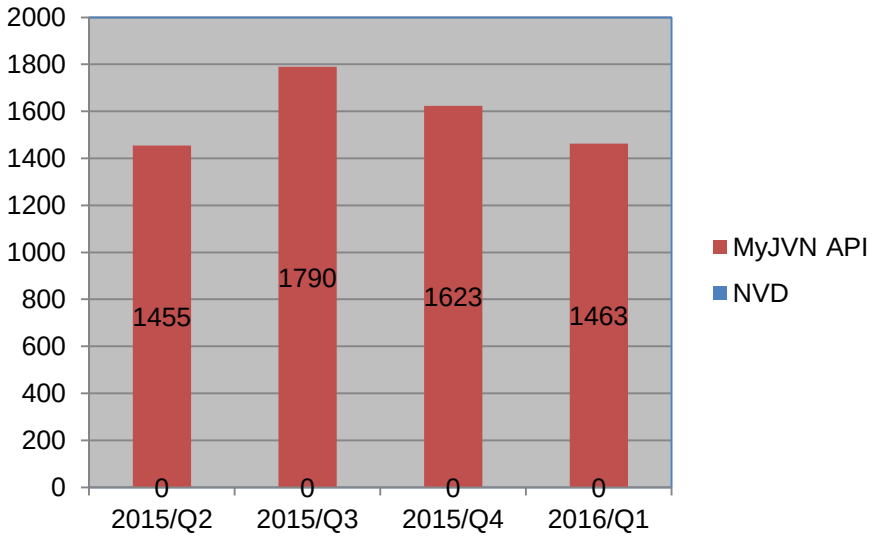
- 出張セミナのご依頼、お問い合わせは、secure-coding@jpcert.or.jp までご連絡ください。

2.4. VRDA フィードによる脆弱性情報の配信

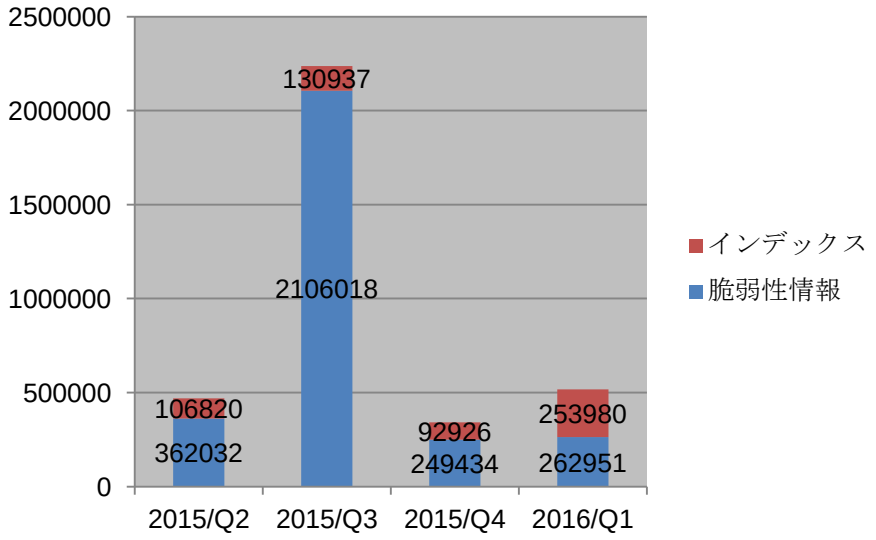
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST(National Institute of Standards and Technology)の NVD(National Vulnerability Database)を外部データソースとして利用した、VRDA(Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web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

VRDA フィード 脆弱性脅威分析用情報の定型データ配信
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 2-7]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、約 2.7 倍に増加しました。一方、脆弱性情報の利用数については、大きな変化は見られませんでした。

[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、前四半期と比較し、大きな変化は見られませんでした。

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 265 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 0 件でした。

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、制御システムセキュリティ情報共有コミュニティに登録いただいている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

2016-01-07　制御システムセキュリティニュースレター 2015-0012
2016-02-08　制御システムセキュリティニュースレター 2016-0001
2016-03-04　制御システムセキュリティニュースレター 2016-0002

制御システムセキュリティ情報共有コミュニティには、現在 590 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 2 件でした。1 件目の報告はインターネットからアクセスできる制御システム関連機器に関するもので、602 件の IP アドレスが記載されていました。このうち ISP 管理のものを除く 15 件の IP アドレスについて調査を行い、外部から不正に操作される可能性がある 3 件に対して危険性を伝えました。2 件目の報告も同様にインターネットからアクセスできる制御システム関連機器に関するもので、2 件の IP アドレスが記載されていました。2 件の IP アドレスは、ISP が管理しているアドレスではなかったので調査し、ともに不正に操作される可能性があったので、調査結果をそれぞれの管理者に伝えました。
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、以前と比べて格段に制御システム機器を見つけやすくなっています。そのため、こうしたサービスを発端と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、5 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 6 件、J-CLICS に関して 23 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 191 件、J-CLICS が 292 件となりました。

3.5 海外セミナー参加報告会の開催

2016 年 03 月 09 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、最近に米国で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「S4x16」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 24 名の方にご参加いただきました。

3.6 制御システムセキュリティカンファレンス 2016 開催

2 月 17 日(水)に東京(品川)で、制御システムセキュリティカンファレンス 2016 を開催し、300 名の方にご来場いただきました。今回で 8 回目となる本カンファレンスでは、「制御システムセキュリティ最前線」をテーマに[表 3-1]のようなプログラムで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 Web ページをご参照ください。

制御システムセキュリティカンファレンス 2016
https://www.jpcert.or.jp/event/ics-conference2016.html

制御システムセキュリティカンファレンス 2016 においての講演資料
https://www.jpcert.or.jp/present/#year2016

[図 3-1 制御システムセキュリティカンファレンス 2016 講演風景]

[表 3-1 講演内容]

(1)「制御システムセキュリティ動向～2015 年度を振り返る～」 JPCERT/CC 顧問 宮地 利雄
(2)「制御システムセキュリティの対策技術紹介～ホワイトリストスイッチ、サイバー攻撃早期認識支援技術～」 技術研究組合 制御システムセキュリティセンター　細川 嵩
(3)「制御システムセキュリティ演習から見えてきたこと　－　早期警戒網整備と ICS-CSIRT 育成－」 国立大学法人名古屋工業大学 教授　越島 一郎
(4)「都市ガス業界における制御系システムのセキュリティ確保の取組みについてーサイバー演習の紹介を中心にー」 一般社団法人　日本ガス協会　谷 吉智
(5)「制御システムセキュリティへの取組み」 住友化学株式会社　大谷 和史
(6)「制御システムセキュリティへの取り組みについて」 中部電力株式会社 浜岡原子力発電所 藤田 達雄
(7)「制御システムセキュリティの重要性」 JPCERT/CC 落合 一郎

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. ASEAN 諸国への CSIRT 運用支援 (2 月 16 日)

JPCERT/CC は、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事業「平成 27 年度 貿易投資促進事業」の一環として実施した「ASEAN 地域の重要インフラ関係者に対する情報セキュリティ強化支援研修」の 2 月 16 日の講義枠において、ASEAN 諸国の重要インフラ事業者や政策担当者に向けて、重要インフラ防御や制御システムセキュリティへの JPCERT/CC の取組み等について講義を行いました。

4.1.2. インドネシア、カンボジア、ラオス、ミャンマー、ベトナム、東ティモールへの CSIRT 運用支援(3 月 3 日- 4 日)

独立行政法人 国際協力機構 (JICA) が「情報セキュリティ能力向上プロジェクト」の一環としてインドネシア ID-SIRTII/CC とともに 3 月 3 日、4 日にバリで開催した「CSIRT マネージャ向け研修」に JPCERT/CC 職員が調査団員として派遣されました。インドネシア、カンボジア、ラオス、ミャンマー、ベトナム、東ティモールの 6 ヶ国の National CSIRT および関係組織のマネージャ層に対して、"Future Role of National CSIRT"をテーマに、National CSIRT に求められる活動や役割について、JPCERT/CC での取組みを例にとり講演しました。また JICA やインドネシアの関係者とともに今後の ASEAN 諸国での CSIRT 構築支援計画等について協議しました。JICA の「情報セキュリティ能力向上プロジェクト」の詳細については、次の Web ページをご参照ください。

JICA 情報セキュリティ能力向上プロジェクト
http://www.jica.go.jp/project/indonesia/014/index.html

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状況の共有を目的として、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 1 月 20 日に電話会議を、また 2 月 22 日から 23 日に APRICOT 2016 の開催にあわせてオークランドで会議を行い、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

(1) Auckland 2016 FIRST Technical Colloquium (2 月 21 日)

JPCERT/CC は、2 月 15 日から 26 日にオークランドで開催された APRICOT 2016 のプログラムの一環として、21 日に行われた FIRST Technical Colloquium (TC) において、サイバーグリーンプロジェクトについて講演を行いました。講演では、サイバーグリーンの構想を紹介するとともに、本プロジェクトを通したサイバー空間のクリーンアップ活動への協力、およびリスクの評価指標に関するフィードバックを呼びかけました。なお、本イベントは FIRST が主催し、APNIC および APCERT が協力して開催され、APCERT Steering Committee に属する組織や関係組織のメンバを講師として、サイバーセキュリティに係る技術動向や各種取組みが紹介されました。サイバーグリーンおよび FIRST TC についての詳細は、次の Web ページをご参照ください。

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

Auckland 2016 FIRST Technical Colloquium
https://2016.apricot.net/program#sessions/first-tc

(2) ASEAN 地域フォーラム (ASEAN Regional Forum: ARF) サイバー空間の信頼醸成措置に係るワークショップでの講演 (3 月 2 日-3 日)

JPCERT/CC は、3 月 2 日から 3 日にクアラルンプールで開催された ASEAN 地域フォーラム (ARF) の信頼醸成措置に係るワークショップにおいて APCERT を代表して登壇し、APCERT における POC (Point Of Contact：連絡窓口) の体制について紹介しました。また、JPCERT/CC として、CSIRT 間の連携がどのように信頼醸成措置に貢献し得るかについて講演し、CSIRT の活動や役割について外交政策担当者等に向けてアピールしました。
ASEAN 地域フォーラムは、政治・安全保障問題に関する対話と協力を通じ、アジア太平洋地域の安全保障環境を向上させることを目的としたフォーラムです。

4.2.1.3. APCERT 合同サイバー演習 (APCERT Drill) 2016 への参加 (3 月 16 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。

12 回目となる今回の合同サイバー演習は「進化するサイバー脅威と金融詐欺」をテーマに実施されました。インターネットバンキングの利用者を標的としたマルウエアによる被害は、日本だけでなく香港やシンガポールなど他の APCERT 加盟国・経済地域でも広く報告されています。また、スリランカにおいてもなりすましメール等を用いた金融詐欺の被害が広まっています。こうした状況を踏まえて、テーマが設定され、演習シナリオが作成されました。参加組織はシナリオを通して、関係する組織への通知やマルウエアやログの分析など、インシデント対応の手順と技術を確認しました。本演習には、APCERT 加盟組織のうち 20 経済地域から 26 チーム、および OIC-CERT (The Organisation of Islamic Cooperation – Computer Emergency Response Teams) からエジプト、モロッコ、ナイジェリア、オマーン、パキスタン、チュニジアの 6 チームが参加しました。これは過去最多の参加組織数となり、APCERT における各チームのサイバー脅威に対する危機感の強さと、近年さらに深まっている OIC-CERT との連携を表すイベントとなりました。

JPCERT/CC は、APCERT 事務局並びに演習運営委員会(Drill Organising Committee)のメンバとして、シナリオの議論や運営において主導的な役割を果たしました。また、プレーヤー（演習者）として参画するとともに、コントローラ (Exercise Control: 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。APCERT Drill 2016 についての詳細は、次の Web ページをご参照ください。

APCERT Drill 2016 - An Emerging Cyber Threat and Financial Fraud
http://www.apcert.org/documents/pdf/APCERTDrill2016PressRelease.pdf

4.2.2 FIRST (Forum of Incident Response and Security Teams)

JPCERT/CC は、1998 年の加盟以来 FIRST の活動に積極的に参加しています。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 1 月 25 日から 27 日にプラハ、3 月 14 日から 17 日にプエルトリコで開催された Board of Directors 会合に出席し、組織運営に関わる議論に参画しました。
特に今四半期は、2016 年 6 月にソウルで開催が予定されている FIRST カンファレンス/年次総会の担当理事として、予算案の策定、スポンサー募集、ローカルホストとの調整、基調講演選定、プログラム策定、講演者との調整等、多岐にわたる任務をつとめました。

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 G7 エネルギー大臣会合電力分野におけるサイバーセキュリティワークショップへの参加 (3 月 8 日)

3 月 8 日に東京で開催された G7 エネルギー大臣会合電力分野におけるサイバーセキュリティワークショップに JPCERT/CC の国際部シニアアナリスト 小宮山功一朗が FIRST 理事として参加し、電力・エネルギー分野でのサイバーセキュリティ対応について、FIRST の活動や取組みを紹介しました。

4.2.3 国際 CSIRT 間連携に係る海外カンファレンス等への参加

4.2.3.1 FIRST/TF-CSIRT Technical Colloquium (TC)での講演 (1 月 25 日- 27 日)

JPCERT/CC は、1 月 25 日から 27 日にプラハで開催された FIRST/TF-CSIRT TC に参加し、サイバーグリーンの取組みについて講演しました。TF-CSIRT は欧州内の CSIRT 間協力を促進するために設立されたタスクフォースであり、本イベントに参加した欧州の CSIRT 等に向けて、インターネット全体の健全性とリスクを各国／地域間で比較可能にする評価指標を打ち立て、その指標を用いてより効率的に健全なサイバー空間を実現することを目的とした、JPCERT/CC が主導するサイバーグリーンの取組みを紹介しました。また、サイバーグリーンの活動への参加を呼びかけ、リスク評価指標の適否に対する意見を求めました。サイバーグリーンおよび FIRST/TF-CSIRT TC についての詳細は、次の Web ページをご参照ください。

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

Auckland 2016 FIRST Technical Colloquium
https://www.terena.org/activities/tf-csirt/meeting47/

4.2.4 海外 CSIRT 等の来訪および往訪

4.2.4.1 JICA 情報セキュリティ東京研修の研修員来訪 (2 月 3 日)

JICA 東京国際センターで「情報セキュリティ政策能力向上コース」を受講中の研修生 9 名（インドネシア、ラオス、マレーシア、ミャンマー、ベトナムの政府系組織の IT 担当者等）が JPCERT/CC を来訪しました。JPCERT/CC の事業紹介、インシデント動向、重要インフラ防護に向けた取組みや日本国内における民間 CSIRT の取組み等について講義しました。講義後に研修生との意見交換が行われ、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 シンガポール IDA の来訪 (3 月 11 日)

シンガポールの IDA (Infocomm Development Authority of Singapore:情報通信開発庁) から 3 名が来訪し、IDA および JPCERT/CC の活動状況やシンガポール、日本における情報セキュリティに関する組織・機関の体制、両国で発生しているインシデント動向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。

Windows Commands Abused by Attackers (1 月 26 日)
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html

Banking Trojan “Citadel” Returns (2 月 19 日)
http://blog.jpcert.or.jp/2016/02/banking-trojan--27d6.html

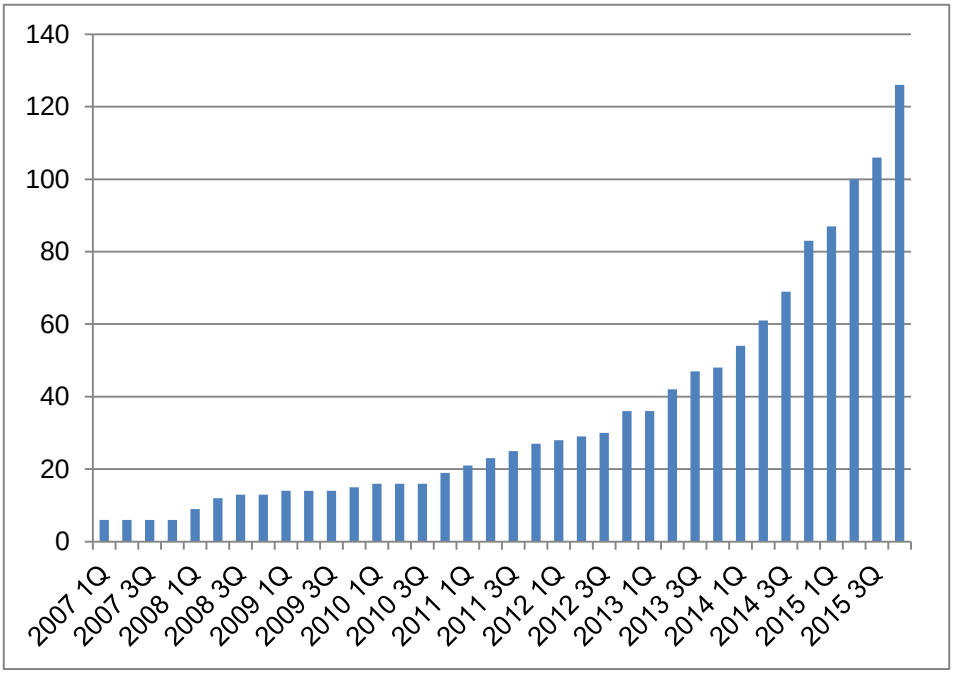
Experience in MNSEC 2015, Ulaanbaatar (3 月 29 日)
http://blog.jpcert.or.jp/2016/03/experience-in-mnsec-2015-ulaanbaatar.html

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、丸紅 IT ソリューションズ株式会社 (シーサート名称は M-CSIRT。他の会員についても同様)、株式会社セプテーニ・ホールディングス (Sep-CIRT)、東京電力株式会社 (TEPCO-SIRT)、株式会社 日本経済新聞社 (NIKKEI-SIRT)、株式会社 商工組合中央金庫 (Shochu-SIRT)、株式会社 セブン銀行 (7BK-CSIRT)、株式会社 大崎コンピュータエンヂニアリング (OCE-CSIRT)、東京ガス株式会社 (TG CSIRT)、三井物産株式会社 (MBK-CSI)、株式会社セブン&アイ・ホールディングス (7&i CSIRT)、住信 SBI ネット銀行株式会社 (SSNB-CSIRT)、住友ゴム工業株式会社 (SRIG-SIRT)、株式会社オービックビジネスコンサルタント (OBC-SIRT)、JFE ホールディングス株式会社 (JFE-SIRT)、アイレット株式会社 (CLP-CSIRT)、三井化学株式会社 (MC-SIRT)、日本ビジネスシステムズ株式会社 (JBS-CIRT)、株式会社ブリヂストン (Bridgestone CSIRT)、キヤノンマーケティングジ

ャパン株式会社 (Canon MJ-CSIRT)、ネットワンシステムズ株式会社 (NetOne-CSIRT)の 20 組織が新規に加盟しました。本四半期末時点で 1 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 12 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した。この会合では、新しく加盟した 15 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。

第 12 回シーサートワーキンググループ会

2016 年 3 月 18 日 (金) 14:00-17:40

会場：株式会社日立製作所（HIRT）

参加人数：188 名

また、2 月 17 日～19 日には「TRANSITS Workshop NCA Japan」を開催しました。TRANSITS は、CSIRT の設立の促進、既存の CSIRT の対応能力向上を目的として、ヨーロッパで開発された教育プログラムに基づいた教育訓練コースです。JPCERT/CC は TRANSITS マテリアルの翻訳等を担当しました。「TRANSITS Workshop NCA Japan」の詳細については、次の URL をご参照ください。

TRANSITS Workshop NCA Japan

http://www.nca.gr.jp/2016/transits/index.html

さらに、2 月 23 日(火)には「CSIRT 人材セミナー ～サイバーセキュリティを担う人材とは～」を開催しました。本セミナーは、日本が直面しているセキュリティ人材の確保や育成といった課題に対して、企業がどのように取り組むべきかを、人材採用の担当者や育成を担当している方に学んでいただくためのセミナーです。詳しくは次の URL をご参照ください。

CSIRT 人材セミナー ～サイバーセキュリティを担う人材とは～
http://www.nca.gr.jp/2016/pr-seminar/index.html

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。

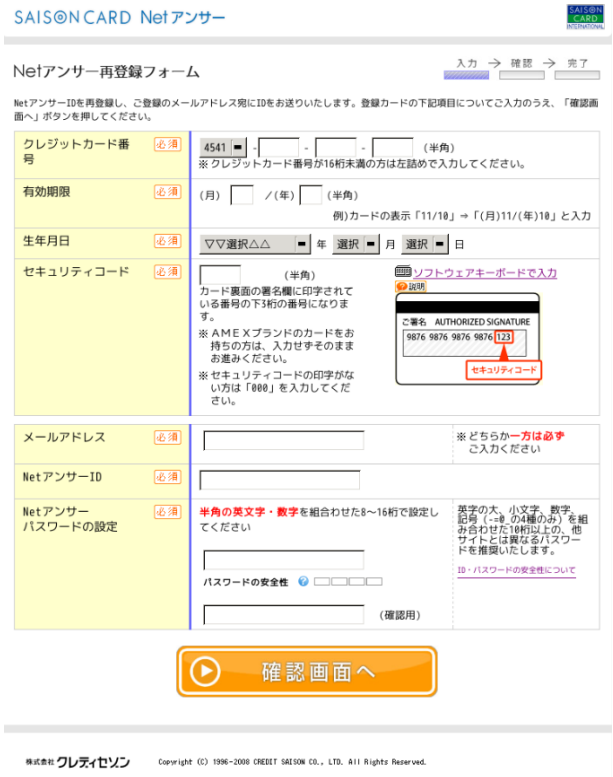
6.1 情報収集/発信の実績

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 25 件発信しました。

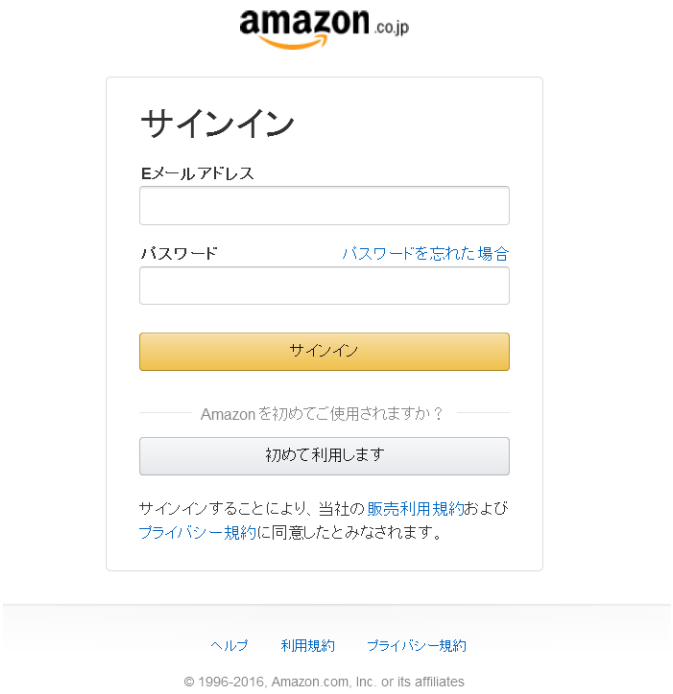
本年度初頭に始まった、銀行のフィッシングサイトへの、SMS (ショートメッセージサービス) を使った誘導が、本四半期に入ってからも引き続き確認されました。また、以前からあった、クレジットカード会社をかたるフィッシングは、本四半期においても継続的に報告されました。なお、本四半期においては、Amazon をかたるフィッシングのサイトの報告が寄せられました。協議会では、名前をかたられた各事業者に、メール本文やサイトの URL 等の関連情報を提供しました。

また、合計 12 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 7 件、クレジットカード会社をかたるフィッシング関連が 2 件、その他が 3 件でした。それぞれに関連したものとして、 [図 6-1]に三井住友銀行をかたるフィッシング (2016/01/22)を、[図 6-2]にセゾン Net アンサーをかたるフィッシング (2016/01/19)を、[図 6-3]に Amazon をかたるフィッシング (2016/02/01)を例示します。

[図 6-1] 三井住友銀行をかたるフィッシング (2016/01/22)
https://www.antiphishing.jp/news/alert/smbc_20160122.html



[図 6-2] セゾン Net アンサーをかたるフィッシング (2016/01/19)
https://www.antiphishing.jp/news/alert/saison_20160119.html



[図 6-3] Amazon をかたるフィッシング (2016/02/01)
https://www.antiphishing.jp/news/alert/amazon_20160201.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. フィッシングサイ 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 22 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。

6.3. 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。

駒場一民「フィッシングの現状と対策 2016」
神奈川県クレジットカード犯罪対策連絡協議会 2016 年 2 月 4 日

6.4. 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 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 2016 年 1 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201601.html
フィッシング対策協議会 2016 年 2 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201602.html
フィッシング対策協議会 2016 年 3 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201603.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 34 回運営委員会
日時：2016 年 1 月 15 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

フィッシング対策協議会 第 35 回運営委員会
日時：2016 年 2 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 36 回運営委員会
日時：2016 年 3 月 11 日 16:00 - 18:00
場所：トレンドマイクロ株式会社

7.2 フィッシング対策協議会が東京メトロ全駅で 「STOP. THINK. CONNECT.」 キャンペーンポスターを掲出

2 月 1 日から 3 月 18 日までの 「サイバーセキュリティ月間」 にあわせて、東京地下鉄株式会社 (東京メトロ)、独立行政法人 情報処理推進機構 (IPA) と協力し、サイバー空間における安全習慣を呼びかける「STOP. THINK. CONNECT.」 ポスターを作成し、2 月 22 日～28 日まで東京メトロにおける 160 の駅に掲示しました。

フィッシング対策協議会が東京メトロ全駅で 「STOP. THINK. CONNECT.」 キャンペーンポスターを掲出
https://www.antiphishing.jp/news/info/_stc_metroposter.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、この制度の運用に関連した本四半期の活動実績と、同期間中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 4 四半期(10 月～12 月)]
(2016 年 1 月 27 日)
https://www.jpcert.or.jp/press/2016/vulnREPORT_2015q4.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 10 月～12 月
(2016 年 2 月 4 日)
https://www.jpcert.or.jp/tsubame/report/report201510-12.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 2 件の記事を公開しました。

(1) 帰ってきたバンキングトロイ Citadel(2016-01-05)

2015 年 11 月末に Drive-by-Download 経由で Citadel に感染させようとする事例で見られた、バージョンアップした Citadel の変化の内容と、バージョンアップした Citadel に対応した復号ツールについて紹介しました。

帰ってきたバンキングトロイ Citadel(2016-01-05)
https://www.jpcert.or.jp/magazine/acreport-citadel.html

(2) 改ざんの標的となる CMS 内の PHP ファイル(2016-02-25)

CMS を構成している一部の PHP ファイルが改ざんされ、その影響で Web サイトが生成するコンテンツの改ざんが生じた複数の調査事例から、標的となっていた CMS を構成するファイルの改ざん内容や攻撃の仕組みについて紹介しました。

改ざんの標的となる CMS 内の PHP ファイル(2016-02-25)
https://www.jpcert.or.jp/magazine/acreport-cms.html

8.4 産業用制御システム(ICS)ガイドセキュリティ　SCADA、DCS、PLC、その他の制御システムの設定

米国国立標準技術研究所（NIST）が 2015 年 5 月に公開した「NIST SP800-82 Rev.2」を翻訳し、日英対訳資料「産業用制御システム(ICS)ガイドセキュリティ　SCADA、DCS、PLC、その他の制御システムの設定」として公開しました。本資料は、SCADA システム、分散制御システム (DCS)、プログラマブル論理制御装置 (PLC)その他の制御システム設定を含む産業用制御システム（ICS）の保全方法に関するガイダンスです。産業用制御システム（ICS）独自の性能・信頼性・安全性要件について、概要や典型的なシステムトポロジー、脅威と脆弱性を解説し、リスクを減らすためのセキュリティ対策を紹介したものです。

産業用制御システム(ICS)ガイドセキュリティ　SCADA、DCS、PLC、その他の制御システムの設定 (2016 年 3 月 14 日)
https://www.jpcert.or.jp/ics/information02.html#NISTSP800-82

8.5 「高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて」

昨今のサイバーインシデント事例の報道の増加に伴って、「標的型攻撃」と呼ばれる概念を含む APT の脅威と対策の重要性について理解が浸透してきています。こうした現状を鑑み、昨今の脅威に対抗するための具体的な対策をご検討いただくために、国内企業と組織に向けて、高度サイバー攻撃(APT)を妨害し情報資産を防御するための具体的な対応と活動目標の参考としてご利用いただくための資料として「高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて」を公開しました。本資料は、高度サイバー攻撃に対する企業や組織の備えについて「APT の定義と活動モデル」、「APT 対応のための事前準備」、「インシデント対応プロセス」の 3 部構成にまとめたものです。

高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて
(2016 年 3 月 31 日)
https://www.jpcert.or.jp/research/apt-guide.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) :
「高度サイバー攻撃の最新動向と対応体制について」
株式会社シー・アイ・シー 社内セキュリティセミナー,2016 年 01 月 29 日
(2) 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」
@IT セキュリティセミナー 標的型攻撃、「被害端末はどれ？」「影響範囲は？」企業を脅かすセキュリティインシデントに立ち向かうには, 2016 年 02 月 03 日
(3) 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最新動向と対応体制について」
第二地方銀行協会 サイバーセキュリティセミナー, 2016 年 02 月 15 日
(4) 宮地 利雄(顧問) :
「制御システムセキュリティの現在と展望 2016 この 1 年間を振り返って」
制御システムセキュリティカンファレンス 2016, 2016 年 02 月 17 日
(5) 落合 一郎(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) :
「制御システムセキュリティの重要性」
制御システムセキュリティカンファレンス 2016, 2016 年 02 月 17 日
(6) 久保 啓司(インシデントレスポンスグループ マネージャ) :
「JPCERT/CC の見たサイバー攻撃の現状（標的型攻撃を中心に）」
日本マイクロソフト株式会社 ラウンドテーブル, 2016 年 02 月 24 日
(7) 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) :
「セキュリティ脅威の最新動向と対策～経営目線のプロアクティブなセキュリティ対策～」
公益財団法人とくしま産業振興機構 中小企業向けセキュリティセミナー, 2016 年 02 月 26 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) :
「IoT 時代における高度サイバー攻撃」
ISP&クラウド事業者の集い in 神戸, 2016 年 02 月 26 日
(9) 満永 拓邦(早期警戒グループ 技術アドバイザー) :
「サイバー攻撃への備えと対応体制の必要性」
平成 27 年度文部科学省セキュリティセミナー, 2016 年 03 月 04 日
(10) 落合 一郎(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) :
「S4x16 報告」
海外カンファレンス参加報告会, 2016 年 03 月 09 日
(11) 有村 浩一(常務理事) :
「2015 年におけるサイバー攻撃・インシデントの傾向について」
日経 BP セキュリティ＆ガバナンス 東京 2016, 2016 年 03 月 11 日
(12) 村上 晃(経営企画室 兼 エンタープライズサポートグループ 部門長) :
「CSIRT 構築の事例と勘所を知る～"百社百様"ひとつとして同じものはない」
ITmedia エンタープライズソリューションセミナー, 2016 年 03 月 18 日
(13) 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) :
「セキュリティリスクに対応した CSIRT 構築の勘所～PoC(Point Of Contact)の重要性と連携の勧め」
日経 BP セキュリティ対策チーム（CSIRT）の構築・運営テクニック, 2016 年 03 月 23 日

10. 主な執筆一覧

(1)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) :
「新聞、通信社に対する高度サイバー攻撃と必要な備えとは」
日本新聞協会『新聞技術』235 号,2016 年 03 月 25 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) JSSECスマートフォン セキュリティ・シンポジウム2016
主催：一般社団法人日本スマートフォンセキュリティ協会(JSSEC)
開催日：2016年03月09日(水)
(2) サイバーセキュリティイニシアティブ2016「サイバーセキュリティ対策を経営戦略の中核に 」
主　催：IT Fourum&RoundTable事務局
開催日：2016年03月16日(水)

12. セミナー開催

本四半期は、次の行事を開催しました。

(1) 制御システムセキュリティカンファレンス 2016

主　催：経済産業省、JPCERT コーディネーションセンター(JPCERT/CC)

開催日：2016 年 02 月 17 日(水)

(2) 海外カンファレンス参加報告会

主　催：JPCERT コーディネーションセンター(JPCERT/CC)

開催日：2016 年 03 月 09 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