JPCERT-PR-2016-02
発行日 : 2016-07-14

JPCERT/CC 活動概要 [2016 年 4 月 1 日 ～ 2016 年 6 月 30 日]

活動概要トピックス

ートピック1ー　FIRST 理事 JPCERT/CC スタッフが再選

JPCERT/CC は、CSIRT の国際団体である FIRST に 1998 年に加盟して以来、同団体の活動に積極的に参加しています。その一環として、同団体の運営にも JPCERT/CC の複数のメンバが理事として貢献してきました。2014 年 6 月からは国際部マネージャ 小宮山 功一朗が理事（FIRST Board of Directors のメンバ）を務めてきており任期満了を迎えていましたが、6 月 16 日に開催された FIRST 年次総会における理事改選選挙で再選され、更に 2 年間にわたり理事を務めることになりました。小宮山の再選は、カンファレンス担当理事としての実績や、アフリカ・アジア地域での CSIRT 構築支援の実績に代表される、これまでの貢献を会員が高く評価していることを反映したものと見られます。
JPCERT/CC の国際貢献として 2009 年に始めたアフリカにおける CSIRT 構築支援も、アフリカ地域ではもちろんのこと、国際的な CSIRT コミュニティにおいても成果が広く認知されています。この活動に関しては、AfricaCERT 功労賞が 6 月に、元理事の山口 英、小宮山、および法人としての JPCERT/CC に対して授与されました。
FIRST 理事の再任と AfricaCERT 功労賞の受賞について小宮山は「今後も FIRST という国際組織と CSIRT コミュニティの活動の効果をより高めるために、そのネットワークをアフリカやそれ以外の地域に広げていきたい。」と述べています。

FIRST.Org, Inc., Board of Directors（FIRST.Org 理事紹介）
https://www.first.org/about/organization/directors

JPCERT/CC、山口 英氏、国際部シニアアナリスト 小宮山 功一朗が AfricaCERT Meritorious Service Award を受賞
https://www.jpcert.or.jp/press/priz/2016/PR20160617_africacert-award.html

ートピック2ー　「2015 年度 CSIRT 構築および運用における実態調査」を公開

JPCERT/CC では昨年度、日本シーサート協議会（NCA）に加盟している CSIRT を対象としたアンケート調査とインタビューにより、CSIRT の組織体制やメンバ構成、ポリシー整備などを調査し、CSIRT を構築する時に参考としていただけるような報告書にまとめ、6 月に公表しました。

深刻化しているサイバー攻撃に対する備えの一つとして、セキュリティインシデントの発生時に、組織が効果的に対処する際の要となる組織体制である CSIRT が注目されています。ところが、CSIRT は、母体となる組織文化や集められる要員の技術的背景などによってさまざまな形態があります。本報告書では、国内のさまざまな CSIRT の実態を紹介することにより、新たに CSIRT を構築しようとしている方々だけではなく、既に CSIRT を運用している組織が次の段階に向けて検討する際にも役立てていただくことを期待しています。CSIRT の構築や活動の改善の参考資料としてご活用ください。

2015 年度 CSIRT 構築および運用における実態調査
https://www.jpcert.or.jp/research/2015_CSIRT-survey.html

ートピック3ー　攻撃者の行動によって残る痕跡を調査するための文書を公開

JPCERT/CC では、攻撃者がネットワークに侵入した後に利用する可能性が高いツール、コマンドを調査し、それらを実行した際にどのような痕跡が Windows OS 上に残るのかを検証し、「インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書」というタイトルの報告書にまとめて 2016 年 6 月 28 日に公開しました。

近年のサイバー攻撃では、マルウエアに感染したマシンを侵入の起点として、他のマシンへの感染拡大や、内部サーバへの侵入など、組織内の至るところを侵害する事例が多く確認されています。こうした事案においては調査対象ポイントが多数になるため、それらを重大な事象を見落とすことなく迅速に調査して、できる限り正確に被害の全体像を掌握し、善後策の立案に必要な事実を収集するための手立てが求められています。

一方、攻撃対象であるネットワークの構成は組織によってさまざまですが、攻撃の手口には一定のパターンが存在し、共通したツールがしばしば使用されます。

そこで、実際の攻撃に使われることが多いツールの実行時にどのようなログが残るのか、またどのような設定をすれば十分な情報を含むログを取得できるようになるのかを JPCERT/CC の経験に基づいて調査し、報告書にまとめました。インシデント調査において、必ずしも専門家でなくても活用できる資料になっていますので、是非ご活用ください。

なお、本報告書に関連した「分析センターだより」も、併せてご一読下さい。

インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書
https://www.jpcert.or.jp/research/ir_research.html

分析センターだより「攻撃者の行動によって残る痕跡を調査(2016-06-28) 」
https://www.jpcert.or.jp/magazine/acreport-ir_research.html

ートピック4ー　　OWASP の Web アプリケーションのセキュリティ要件を邦訳して公開

JPCERT/CC では、脆弱性を未然に防ぐ取り組みとして、これまでにもセキュアな製品開発のためのガイドやコーディング規約、脆弱性の事例解説資料等を公開してきました。今四半期は、OWASP（Open Web Application Security Project）が策定した Web アプリケーションのセキュリティ要件 OWASP ASVS（Application Security Verification Standard）の第 3 版を日本語に翻訳し、公開しました。

OWASP ASVS は、Web アプリケーションのセキュリティに関する検証要件を標準化したドキュメントです。2008 年に策定が始まり、その後も版を重ね、国内外の Web アプリ開発者や脆弱性診断を行うセキュリティベンダ等に広く利用されてきました。

第 3 版では、認証やセッション管理、アクセス制御等、19 の大項目ごとに、セキュアな Web アプリケーションに求められるセキュリティ要件がまとめられており、巻末の附属書には PCI-DSS v3.0 と ASVS 3.0 との対応表が含まれています。

JPCERT/CC が開発者と調整した脆弱性の中では、Web アプリケーションやインターネットに繋がる組込み機器の Web インターフェイスに関する割合が高く、今四半期においても、JVN で公表した脆弱性の半数以上を Web アプリケーションに関する脆弱性が占めました。ASVS の最新版 v3.0.1 の日本語版の公開をきっかけに、国内の Web アプリケーションコミュニティにおいて ASVS がより多くの方々に活用され、脆弱性の低減につながることを期待しています。

OWASP アプリケーションセキュリティ検証標準
https://www.jpcert.or.jp/securecoding/materials-owaspasvs.html

ートピック5ー　　サイバーセキュリティ対策活動への協力者に感謝状贈呈

JPCERT/CC は、国内のサイバーセキュリティインシデント（以下「インシデント」といいます。）の被害を低減するために、インシデントへの対応支援活動、インシデントを未然に防ぐための早期警戒活動、マルウエア分析、ソフトウエア製品等の脆弱性に関する調整活動などを行っています。これらの活動を円滑かつ効果的に進めるためには、皆様からの情報提供やさまざまなご協力が欠かせません。

JPCERT/CC では、サイバーセキュリティ対策活動に対する皆様からの御好意と御力添えに深く思いをいたし、特に顕著なご貢献をいただいた方に感謝状を贈呈する制度を設けています。本年度の対象者として、昨今国内でも大きな被害が発生しているランサムウエアやバンキングトロージャンへ誘導する Web 改ざんをはじめ、攻撃の変化や全体像の把握につながるさまざまな情報を提供いただいた東芝インフォメーションシステムズ株式会社　柏村 卓哉 様に 2016 年 6 月 30 日に感謝状と記念の盾を贈呈いたしました。

サイバーセキュリティ対策活動への協力者に感謝状贈呈
https://www.jpcert.or.jp/press/priz/2016/PR20160707-priz.html

本活動は、経済産業省より委託を受け、「平成 28 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」、「10. 主な執筆活動」、「11. 協力、後援」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 4686 件、インシデント件数ベースでは 3791 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 2559 件でした。前四半期の 2955 件と比較して 13%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/2016/IR_Report20160714.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 642 件で、前四半期の 645 件から 0.5%減少しました。また、前年度同期（491 件）との比較では、31%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	4 月	5 月	6 月	国内外別合計（割合）
国内ブランド	44	38	44	126(20%)
国外ブランド	115	108	89	312(49%)
ブランド不明(注 2)	46	55	103	204(32%)
月別合計	205	201	236	642(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。

本四半期は、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に関する報告が多く寄せられました。国内通信事業者を装ったフィッシングサイトの多くは、侵入されたとみられる海外の Web サイトに設置されていました。異なる通信事業者のブランドを装った複数の Web ページを収容したフィッシングサイトを確認しており、国内通信事業者が提供する Web メールのアカウント窃取を目的とした攻撃が活発になっている可能性があります。

国内金融機関を装ったフィッシングサイトは、4 月から 5 月後半にかけては継続的に確認していましたが、6 月後半までのおよそ 1 か月間は、新規の IP アドレスのフィッシングサイトが確認されておらず、攻撃が減少してきている傾向が見られました。

国内オンラインゲームを装ったフィッシングサイトは、4 月から 6 月前半までは 1 つのブランドのみ確認されていましたが、6 月半ばに別のブランドが複数確認されるようになりました。いずれのフィッシングサイトも、前四半期にも確認された、無料で登録できる.cc のドメインを使用していました。

フィッシングサイトの調整先の割合は、国内が 30%、国外が 70%であり、前四半期（国内 35%、国外 65%）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、1065 件でした。前四半期の 1268 件から 16%減少しています。

前四半期に多く確認された、特定のブラウザでアクセスした場合のみ、不正な JavaScript を表示する仕組みの改ざんも見られましたが、その他に、”jquery.min.php”という文字列を含む URL に誘導する JavaScript が、head タグ内の末尾に埋め込まれる改ざんが多く確認されました。改ざんされたサイトの多くは CMS を使用しており、CMS のテーマやプラグインの脆弱性を使用した攻撃や、管理画面の認証を破られたことによって侵入され、改ざんされた可能性があります。

また、通信販売を利用して商品を購入する際に、検索エンジンサイトで商品を検索すると不審な通信販売サイトが表示される事例が数多く確認されました。この不審な通信販売サイトは、第三者の正規 Web サイトを改ざんして作成されており、その正規サイトを調査すると正規サイトと関係のない様々な商品を販売する通信販売のページを模したサイトが大量に表示されることを確認しました。対象サイトの URL に直接アクセスした場合は、関連するキーワードが埋め込まれた正規のページが表示されるのに対し、検索エンジンサイトの URL をリファラに指定してアクセスした場合には、iframe タグによって不審な通信販売サイトのページを読み込ませるようになっていました。

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、15 件でした。前四半期の 6 件から 150%増加しています。本四半期は、延べ 2 組織に対応を依頼しました。

Web ページにアクセスした PC の環境情報を収集する、Scanbox とよばれる攻撃フレームワークの情報送信先に対して、国内組織の IP アドレスから通信が行われていることを 5 月初めごろ確認しました。調査したところ、アクセスのリファラ情報から、組織内部で使用するネットワーク装置の Web UI が改ざんされ、Scanbox のコードが埋め込まれた可能性があることが分かりました。

また、5 月半ばには、海外のセキュリティ組織から、マルウエアが感染端末から収集した情報を送信する先となっている、海外の C&C サーバと通信を行っていた国内 IP アドレスの情報を受領しました。

JPCERT/CC は、入手した情報をもとに、関連する国内組織に対して、該当する通信が発生していないか、事実関係を調査するよう依頼しました。

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

2016-04-20　長期休暇に備えて 2016/04
https://www.jpcert.or.jp/pr/2016/pr160002.html

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 7 件更新）　https://www.jpcert.or.jp/at/

2016-04-08　Adobe Flash Player の脆弱性 (APSB16-10) に関する注意喚起 (公開)
2016-04-13　Adobe Flash Player の脆弱性 (APSB16-10) に関する注意喚起 (更新)
2016-04-13　2016 年 4 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)
2016-04-20　2016 年 4 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)
2016-04-26　ケータイキット for Movable Type の脆弱性 (CVE-2016-1204) に関する注意喚起 (公開)
2016-04-28　Apache Struts 2 の脆弱性 (S2-032) に関する注意喚起 (公開)
2016-05-06　ケータイキット for Movable Type の脆弱性 (CVE-2016-1204) に関する注意喚起 (更新)
2016-05-06　ImageMagick の脆弱性 (CVE-2016-3714) に関する注意喚起 (公開)
2016-05-09　ImageMagick の脆弱性 (CVE-2016-3714) に関する注意喚起 (更新)
2016-05-11　2016 年 5 月 Microsoft セキュリティ情報 (緊急 8 件含) に関する注意喚起 (公開)
2016-05-11　Adobe Reader および Acrobat の脆弱性 (APSB16-14) に関する注意喚起 (公開)
2016-05-13　Adobe Flash Player の脆弱性 (APSB16-15) に関する注意喚起 (公開)
2016-05-16　2016 年 5 月 Microsoft セキュリティ情報 (緊急 8 件含) に関する注意喚起 (更新)
2016-05-16　Adobe Flash Player の脆弱性 (APSB16-15) に関する注意喚起 (更新)
2016-06-15　2016 年 6 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)

2016-06-17　Adobe Flash Player の脆弱性 (APSB16-18) に関する注意喚起 (公開)
2016-06-20　2016 年 6 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)
2016-06-20　Apache Struts 2 の脆弱性 (S2-037) に関する注意喚起 (公開)
2016-06-21　Apache Struts 2 の脆弱性 (S2-037) に関する注意喚起 (更新)

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 12 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。

2016-04-06　「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」公開
2016-04-13　Microsoft SQL Server 2005 および Windows Home Server 2011 サポート終了
2016-04-20　ランサムウェア感染を狙った攻撃が急増
2016-04-27　デジタル・フォレンジック研究会が「証拠保全ガイドライン第５版」公開
2016-05-11　Apache Struts 2 の脆弱性を標的としたアクセスが増加
2016-05-18　SAP 製品に対する攻撃について
2016-05-25　JPRS によるゾーン転送の設定状況調査の実施と調査対象からの除外 (オプトアウト) の受け付けについて
2016-06-01　WPAD と名前衝突の問題について
2016-06-08　IPA が改訂版「増加するインターネット接続機器の不適切な情報公開とその対策」公開
2016-06-15　CCDS が「製品分野別セキュリティガイドライン第１版」を公開
2016-06-22　NICT と IPA が「CRYPTREC Report 2015」を公開
2016-06-29　JNSA が「コンシューマ向け IoT セキュリティガイド」公開

1.2.1.4. 早期警戒情報

JPCERT/CC では、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。

【「国内組織における CSIRT 構築と運用に関する調査報告書」の公開】
標的型攻撃など昨今のサイバーセキュリティに関する状況の変化は、国内の多くの組織において CSIRT（Computer Security Incident Response Team）を構築する必要性を高めていると考えられています。JPCERT/CC では、さまざまな組織の CSIRT 構築事例が、新たに、あるいは困難に抗しつつ CSIRT を構築・運用している方々に大いに参考となるのではないかと考え、2015 年度に「CSIRT 構築および運用における実態調査」として、CSIRT の構築・運用を行っている 66 の CSIRT に対してアンケートを実施し、CSIRT の多様な実像について定量的な評価を行いました。さらに、各業界を牽引している主な CSIRT にインタビューを行い、各組織の課題や取り組み状況などの定性的な評価も併せて試みました。これらの調査結果を 6 月 29 日に「2015 年度 CSIRT 構築および運用における実態調査」と題して公開しました。

2015 年度 CSIRT 構築および運用における実態調査
https://www.jpcert.or.jp/research/2015_CSIRT-survey.html

【Web アプリケーション関連の脆弱性に関する情報発信】
ケータイキット for Movable Type と、Apache Struts 2、ImageMagick の脆弱性を狙った攻撃に関する注意喚起をそれぞれ発行しました。これらの脆弱性を悪用することで、遠隔の第三者であっても Web アプリケーションやそのフレームワークを不正に終了させたり、任意のコードを実行させたりすることができます。これらの Web アプリケーション関連の脆弱性を悪用する攻撃が継続的に発生していることから、JPCERT/CC では、本脆弱性を悪用した攻撃と対策について検証を行うとともに、ソフトウエア側で迅速に脆弱性を除く対策が難しいケースに対処するために利用される WAF（Web Application Firewall）による対策の有効性について検証を行い、レポートを発行しました。

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 5 月には GovCERT.HK（香港）が新たに参加し 2016 年 6 月末時点で、観測用センサーは 21 地域 26 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

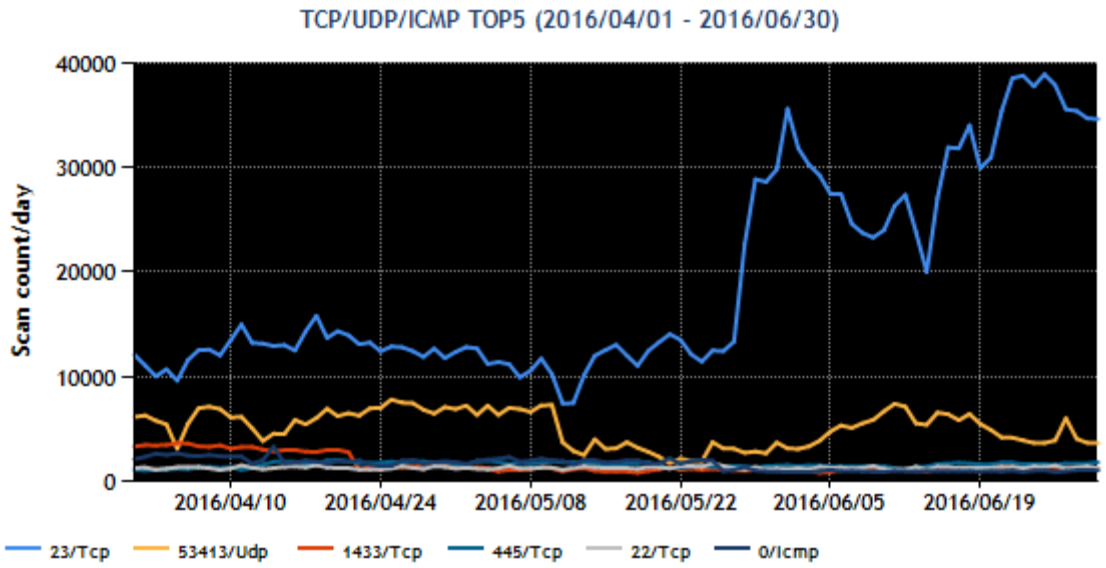
JPCERT/CC は、TSUBAME で収集したデータを宛先ポート番号や送信元地域ごとに分類して統計分析し、既知の脆弱性情報やマルウエア、攻撃ツール等との関連を考察することで、攻撃活動や準備活動の捕捉に努めています。

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、2016 年 1 月から 3 月分のレポートを 2016 年 5 月 26 日に公開しました。

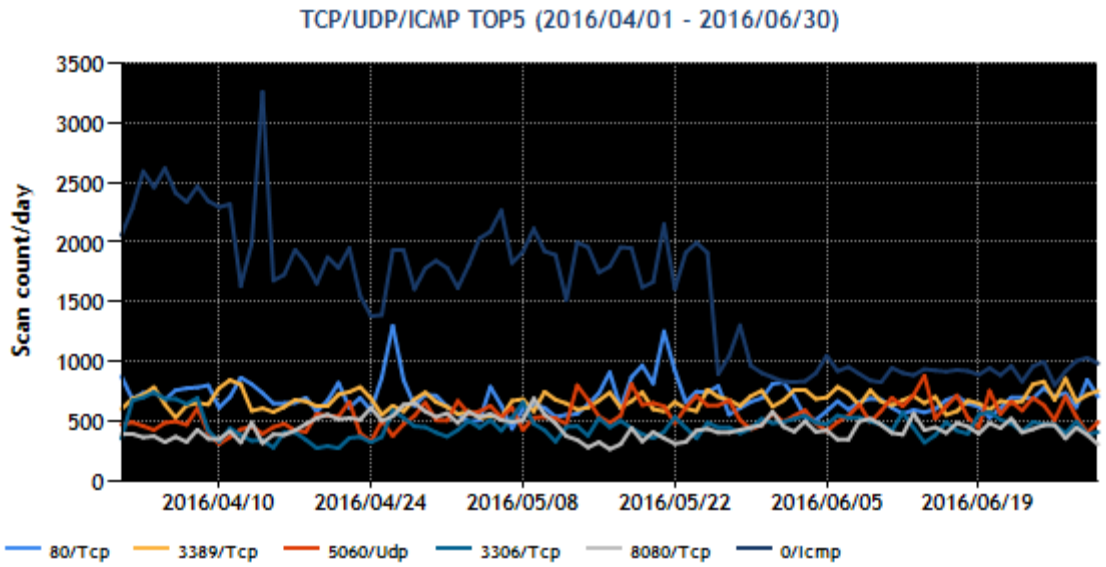
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート（2015 年 1～3 月）
https://www.jpcert.or.jp/tsubame/report/report20161-3.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。

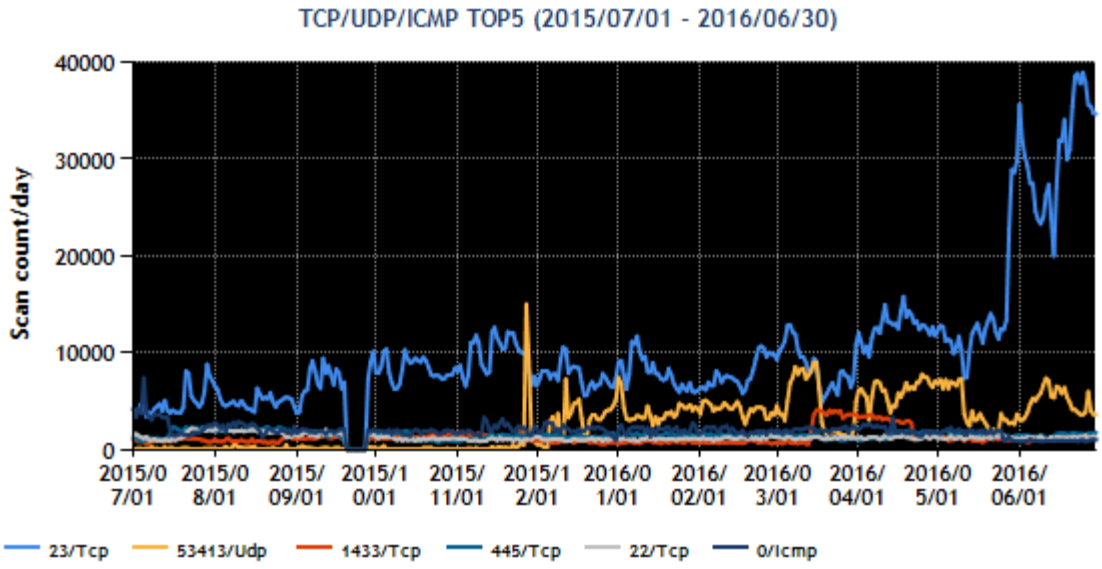


［図 1-1 宛先ポート別グラフ トップ 1-5（2016 年 4 月 1 日-6 月 30 日)］

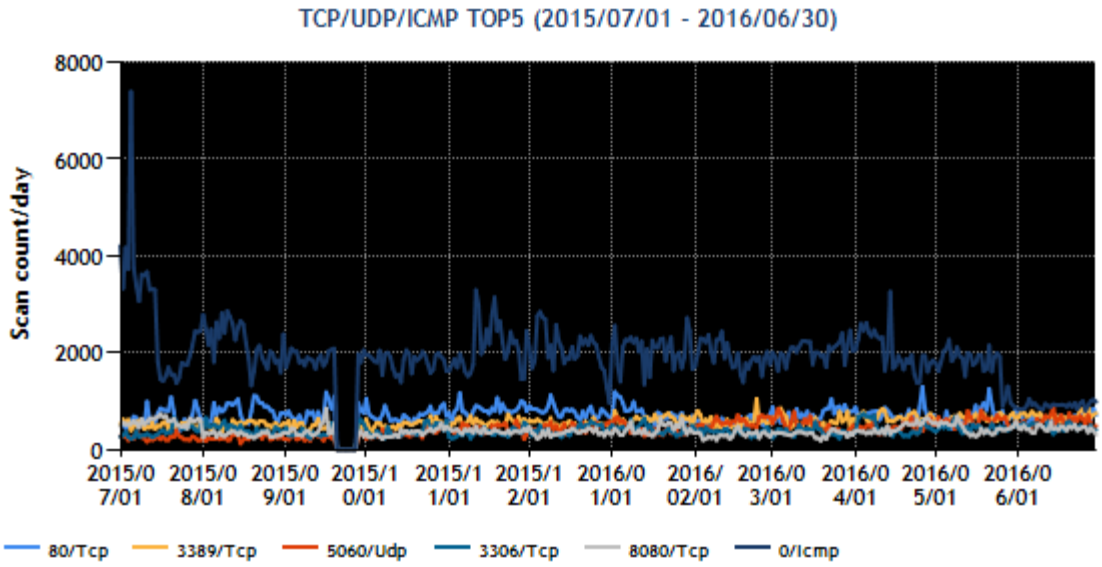


［図 1-2 宛先ポート別グラフ トップ 6-10（2016 年 4 月 1 日-6 月 30 日)］

また、過去 1 年間（2015 年 7 月 1 日-2016 年 6 月 30 日）における、宛先ポート別パケット数の上位 1 位～5 位および 6 位～10 位を［図 1-3］と［図 1-4］に示します。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 7 月 1 日-2016 年 6 月 30 日)］



［図 1-4 宛先ポート別グラフ トップ 6-10（2015 年 7 月 1 日-2016 年 6 月 30 日）］

本四半期に観測されたパケット数が多かったのは、23/Tcp 宛パケットと 53413/Udp 宛パケットでした。53413/Udp 宛パケットは前四半期に増加し、そのままの状態が続きました。23/Tcp 宛パケットは、前四半期も数多く観測されていましたが、5 月 28 日からさらに増加しました。その多くの送信元は海外でした。一部の送信元 IP アドレスについて調査した結果、急増したパケットの送信元 IP アドレスでは、CCTV / Web カメラが接続されていることが分かりました。インターネットに接続された機器が、感染の拡大などを目的にパケットを盛んに送信していると推測しています。
その他、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、順位に変動はありますが、これまで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、不審なパケットが見つかった場合に、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) 国内外の 23/TCP ポートを探索するサーバについての対応
本四半期も、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前四半期から継続して観測されています。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調べました。その結果、新たに複数のベンダ製の機器がマルウエアに感染していることが判明しました。JPCERT/CC では、当該機器の国内外の製造ベンダと送信元 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。

(2) DDoS 攻撃に使用されうるオープンリゾルバとなっている機器についての対応
本四半期も、前四半期に引き続き、DNS 応答パケットおよび DNS サービスのポートの不達を示す ICMP エラーパケットが多数観測されています。それらのパケットの送信元 IP アドレスのうち国内のものを調

査したところ、インターネット側からの DNS のリクエストに応答するオープンリゾルバが見つかりました。観測されたパケットは、攻撃者が DNS 権威サーバに過剰な負荷を課す DDoS 攻撃の余波と推測されます。JPCERT/CC が、TSUBAME で観測した DNS 応答パケットおよび DNS サービスのポートの不達を示す ICMP エラーパケットを調査し、その送信元となっている国内の IP アドレスの管理者に対して調査を依頼したところ、多くの管理者から「DNS サーバやネットワーク機器の設定が不適切でオープンリゾルバになっていたことを確認し、必要な対応を行った」等の回答を得ました。

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

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/

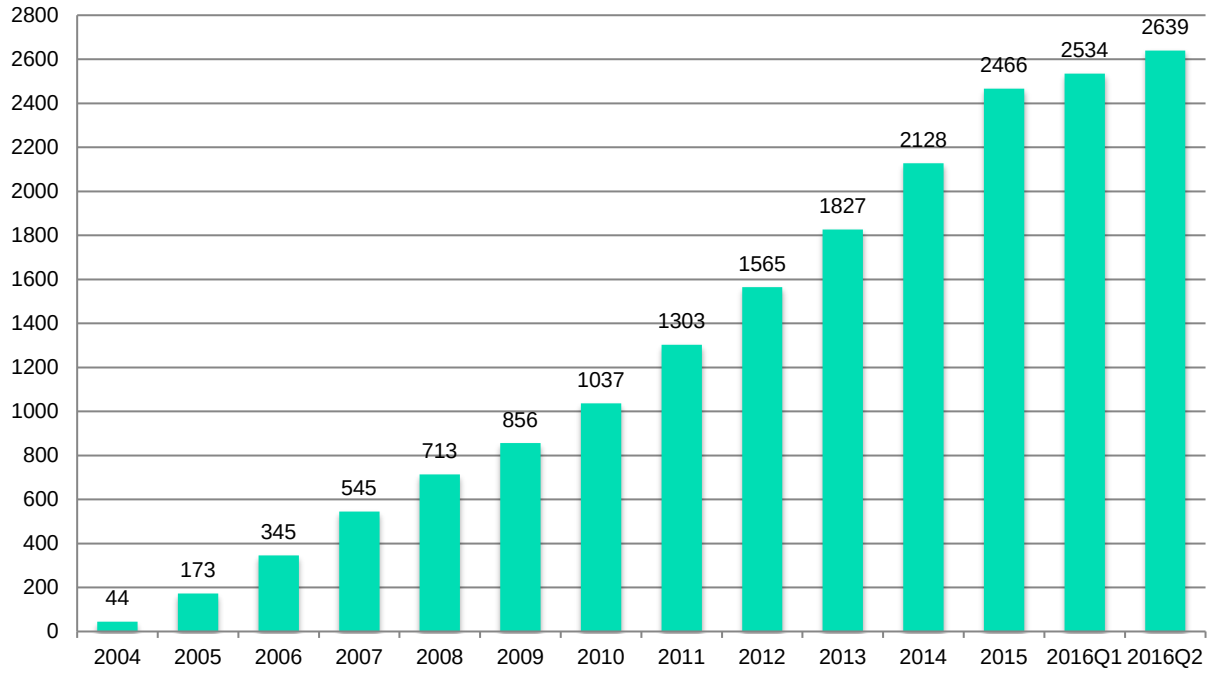
2.1.2. Japan Vulnerability Notes(JVN)において公表した脆弱性情報および対応状況

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 105 件（累計 2,639 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/



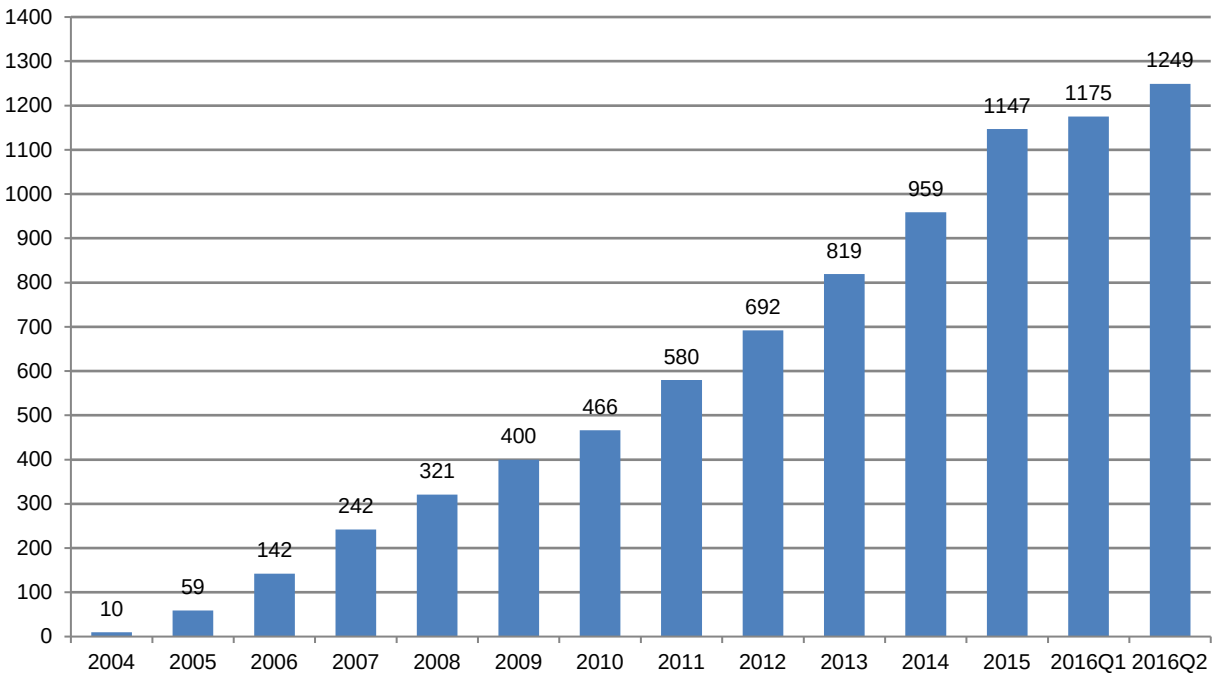
［図 2-1　JVN 公表累積件数］

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 74 件（累計 1,249 件）で、累計の推移は［図 2-2］に示すとおりです。74 件のうち、58 件が国内製品開発者の製品、9 件が海外の製品開発者の製品、7 件が国内外含む複数の製品開発者の製品に関連したものでした。また、58 件のうち 13 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についての、影響を受けた製品のカテゴリ別の件数の内訳は、表 2-1 のとおりでした。本四半期は、組込系製品、グループウエア、スマートフォンアプリ、プラグイン、CMS、ウェブアプリケーション、ウェブアプリケーションフレームワーク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
組込系	13
グループウエア	9
スマートフォンアプリ	7
プラグイン	7
CMS	6
ウェブアプリケーション	6
ウェブアプリケーションフレームワーク	6
Android アプリ	3
SDK	3
アンチウイルス製品	3
フォームメール	2
ライブラリ	2
ActiveX	1
CGI	1
データベース	1
iOS アプリ	1
SNS 構築ソフトウエア	1
サーバ製品	1
認証ソフトウエア	1



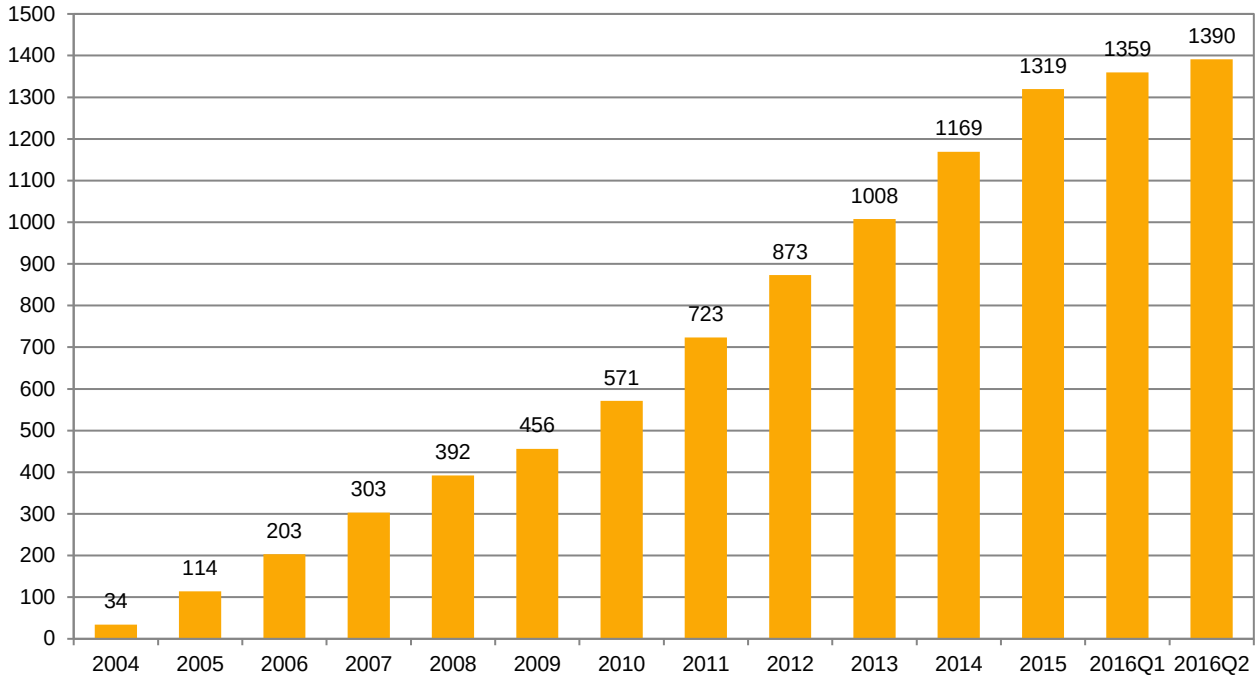
［図 2-2 公表を行った国内取扱脆弱性情報の累積件数］

本四半期に公表した国際取扱脆弱性情報は 31 件（累計 1,390 件）で、累計の推移は［図 2-3］に示すとおりです。また 31 件のうち 3 件は、特定製品やプロトコルに関する注意喚起（Technical Alert）でした。

本四半期に公表した脆弱性情報の、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、米国の CERT/CC の独自調査で、複数の組込みルータ機器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	5
ライブラリ	3
MacOS アプリケーション	2
UNIX	2
メディアプレイヤー	2
3D ネットワーク　レンダリング管理ソフトウエア	1
CMS	1
ERP	1
PBX	1
Windows	1
Windows アプリケーション	1
アプライアンス	1
ウェブアプリケーション	1
ウェブアプリケーションフレームワーク	1
運用管理ソフトウエア	1
アンチウイルス製品	1
データバックアップソフトウエア	1
統合開発環境	1
パスワード管理ソフトウエア	1
プラグイン	1
プロトコル	1
プロトコル実装	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 242 件（製品開発者数で 160 件）を公表し、42 件（製品開発者数で 27 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 13 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 200 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伴い、それらの製品開発者が存在するアジア圏の調整機関、特に韓国の KrCERT/CC や中国の CNCERT/CC、台湾の 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、米国の 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 67 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

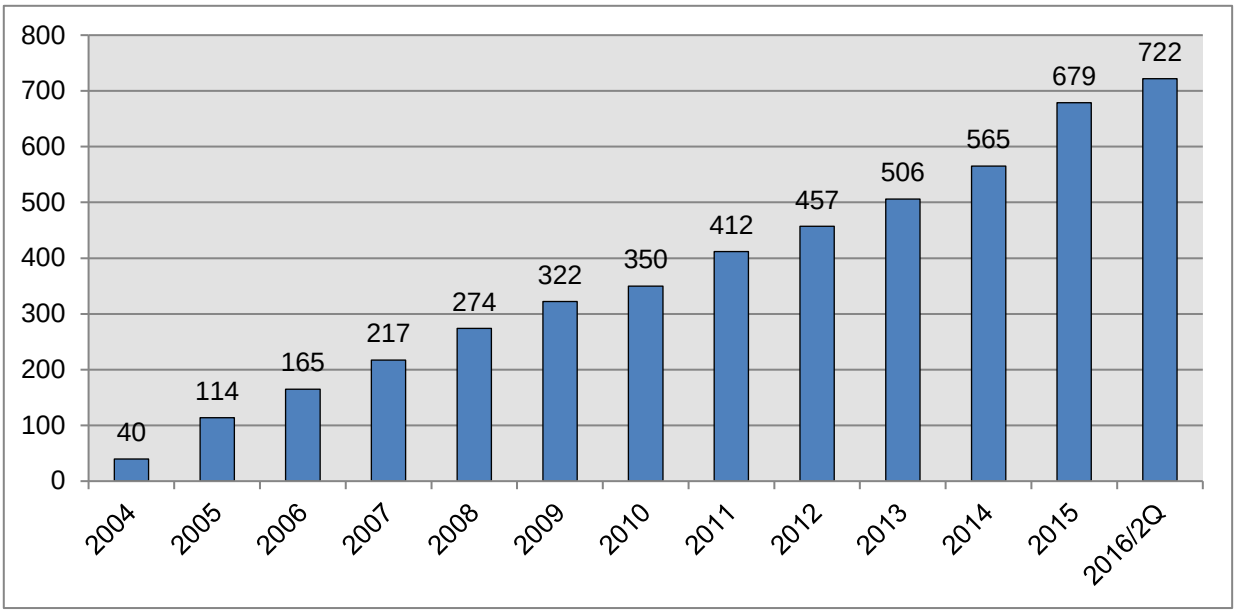
JPCERT/CC では、本基準に従って、日本国内の脆弱性情報流通体制を整備しています。
詳細については、次の Web ページをご参照ください。

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ガイドライン(2016 年版)
http://www.jpcert.or.jp/vh/partnership_guideline2016.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 6 月 30 日現在で 722 となっています。
登録等の詳細については、次の Web ページをご参照ください。

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



[図 2-4 累計製品開発者登録数]

2.3. 脆弱性の低減方策の研究・開発および普及啓発

2.3.1. セキュアコーディングに関する講演活動

JPCERT/CC の情報流通対策グループでは、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。

講演日：6 月 18 日
講演タイトル: OWASP ASVS と Cheat Sheet（日本語版）のご紹介
イベント名：オープンソースカンファレンス 2016 Hokkaido

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行っている米国の団体 OWASP（Open Web Application Security Project）が公開していて、今四半期に JPCERT/CC が日

本語訳して公表した文書 ASVS （Application Security Verification Standard）および Cheat Sheet シリーズ文書（次項 1.2.2 参照）について、文書が作られた目的や内容を紹介しました。

OWASP（Open Web Application Security Project）
https://www.owasp.org/index.php/Main_Page

2.3.2. OWASP アプリケーションセキュリティ検証標準 3.0.1 を公開

JPCERT/CC では、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、「OWASP アプリケーションセキュリティ検証標準 3.0.1」として JPCERT/CC の Web サイトで公開しました。ASVS については、GitHub の JPCERT/CC リポジトリを通じていただいた、OWASP の活動に参加している日本の方々からのコメントを反映し、同サイトで公開しました。今後、Cheat Sheet シリーズ文書の日本語訳も同様に追加していく予定です。

2.3.3. CERT コーディングスタンダードのルールを更新

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

内容の更新（1 件）

- EXP30-C. 副作用が発生する式の評価順序に依存しない

2.3.4. セキュアコーディング出張セミナ

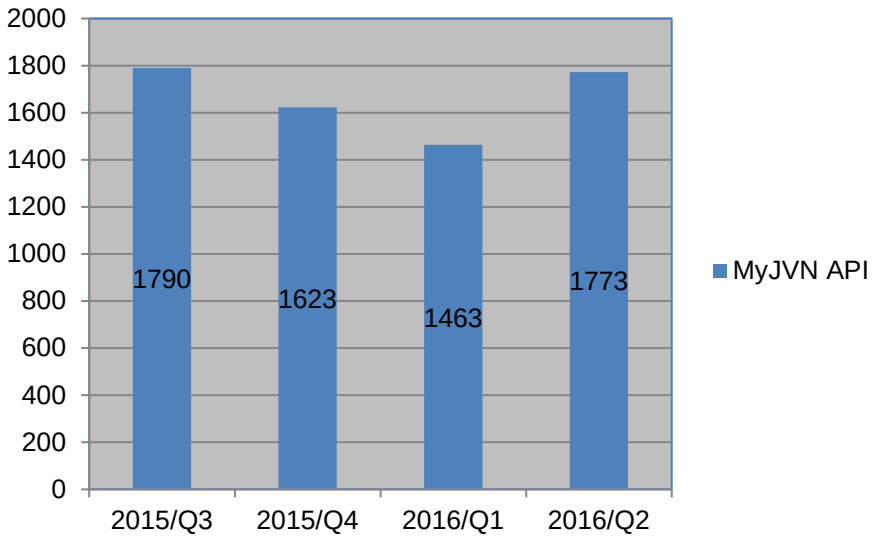
JPCERT/CC では、ソフトウエア製品等の開発を行う企業・組織を対象に、セキュアコーディングに関する出張セミナ（有償）の実施を承っています。本四半期は、国内ベンダ 1 社に対して、C/C++ セキュアコーディングセミナを実施しました。

- 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。

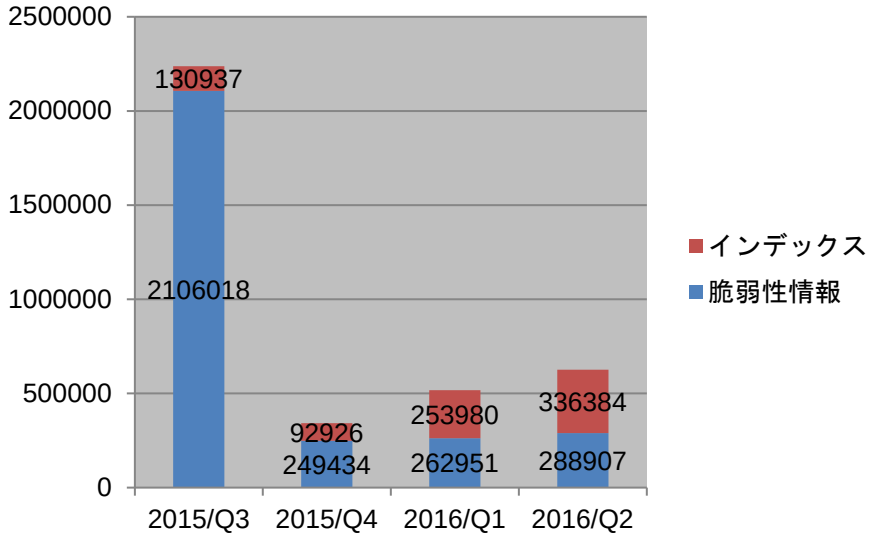
2.4. VRDA フィードによる脆弱性情報の配信

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 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。

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 2-5］に、VRDA フィードの利用傾向を［図 2-6］と［図 2-7］に示します。［図 2-6］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 2-7］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。

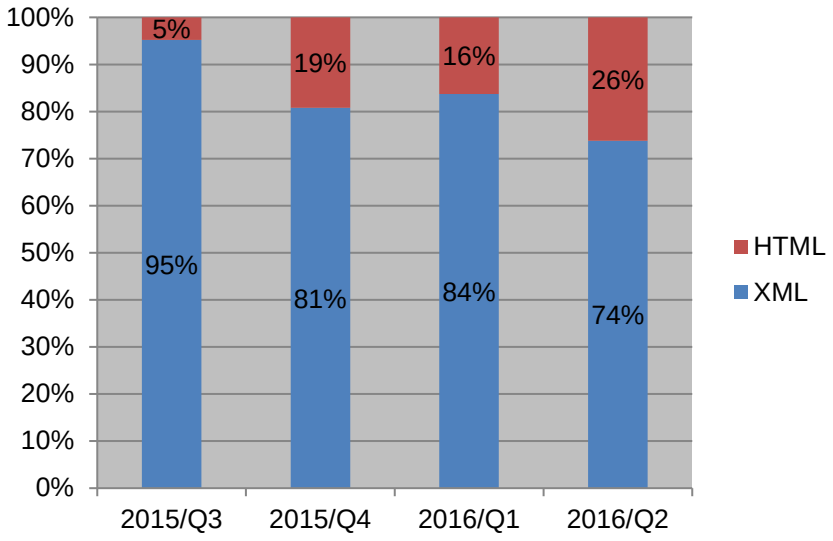


［図 2-5 VRDA フィード配信件数］



［図 2-6 VRDA フィード利用件数］

［図 2-6］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 1.3 倍に増加しました。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。



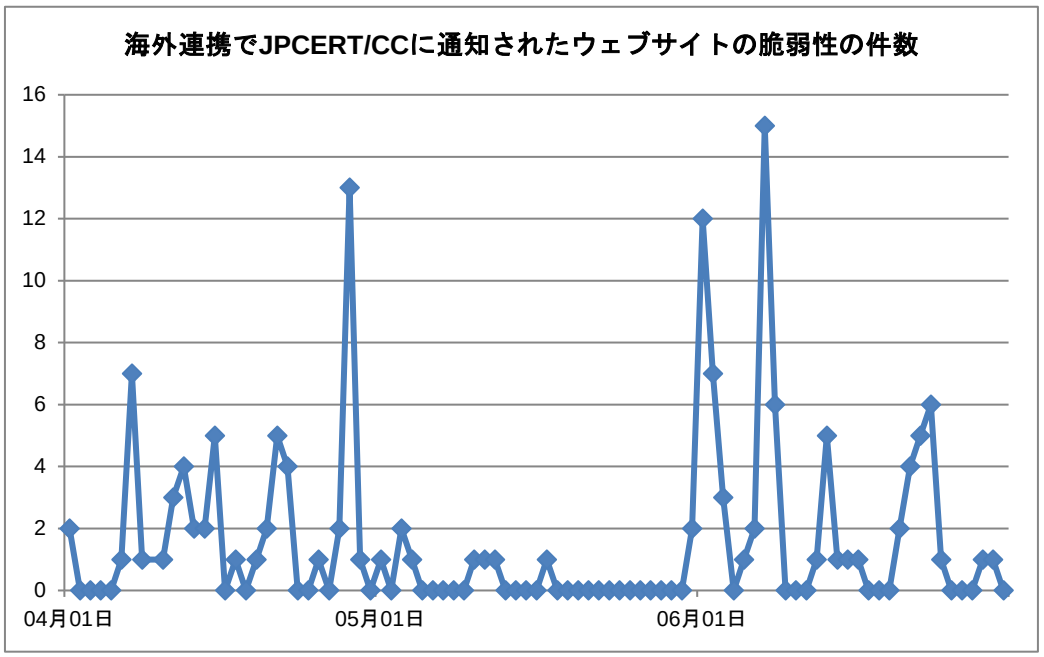
［図 2-7 脆弱性情報のデータ形式別利用割合］

［図 2-7］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、HTML 形式の利用割合が 10%増加しました。

2.5. 海外 CSIRT 等から JPCERT/CC に通知されたウェブサイトの脆弱性情報

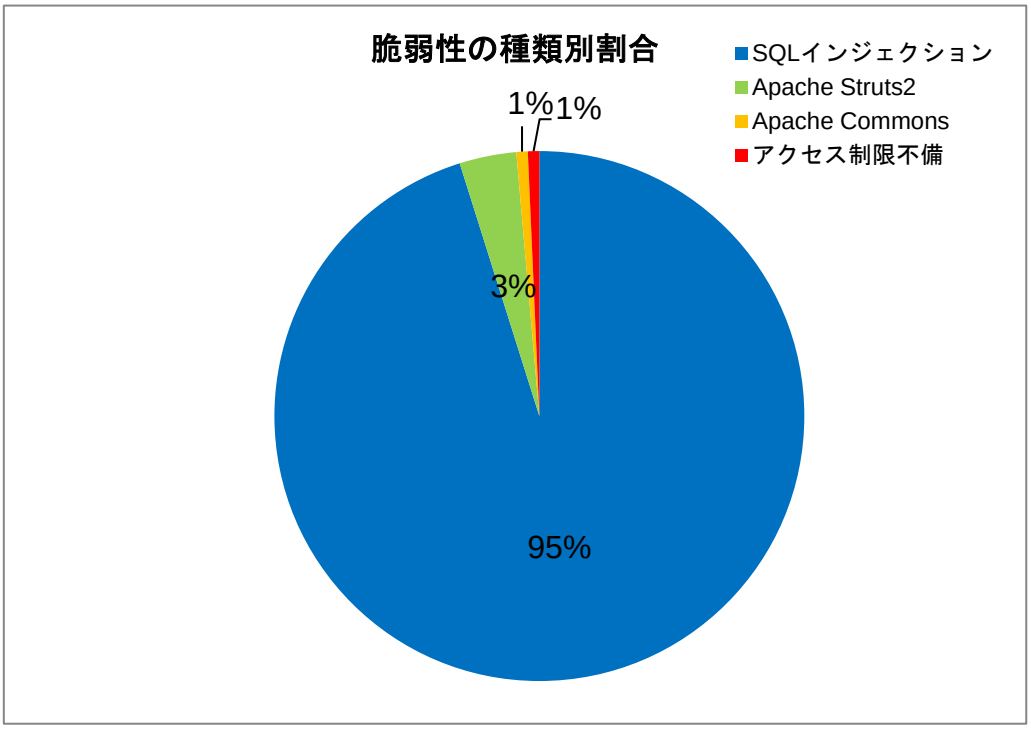
経済産業省告示「ソフトウエア等脆弱性情報取扱基準」では、Web サイトの脆弱性を見つけた場合には IPA に報告を行い、IPA が Web サイトの運営者に是正措置をはたらきかける調整を行うように定めています。ところが、最近になって、海外のセキュリティ関連組織から日本国内の Web サイトの脆弱性に関する情報がもたらされる機会が増えてきました。

JPCERT/CC では、こうした Web サイトの脆弱性情報を各 Web サイトの運営者にお知らせする活動を IPA とも調整を図りつつ展開しています。本四半期には、米国 US-CERT や中国の CNCERT/CC、脆弱性情報ポータルサイトから JPCERT/CC に 143 件のウェブサイトの脆弱性情報の報告があり、関連組織と連携して対応しました。



［図 2-8 JPCERT/CC に通知された日本のウェブサイトの脆弱性の件数］

このうち SQL インジェクションの脆弱性は 136 件、Apache Struts2 の脆弱性（CVE-2013-2251）は 5 件、Apache Commons の脆弱性（CVE-2015-7051）は 1 件、アクセス制御不備が 1 件でした。



［図 2-9 通知された脆弱性の種類別割合］

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 192 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

2016-04-08　制御システムセキュリティニュースレター 2016-0003
2016-05-10　制御システムセキュリティニュースレター 2016-0004
2016-06-03　制御システムセキュリティニュースレター 2016-0005

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 640 名の方にご登録いただいています。今後も内容の充実を図っていく予定です。参加資格や申込み方法については、次の Web ページをご参照ください。

制御システムセキュリティ情報共有コミュニティ
https://www.jpcert.or.jp/ics/ics-community.html

3.2 制御システム関連のインシデント対応

本四半期における制御システムに関連するインシデントの報告件数は 0 件でした。前四半期に報告のあった、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 602 件の IP アドレスが記載されたリストのうち ISP 管理の 587 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 19 件に対して危険性を伝えました。
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等のインターネット上の公開情報を分析し、外部から不正にアクセスされる危険性のある制御システム等を保有する国内の組織に対して情報を提供しています。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はありませんでした。一方、制御システムではないものの、SHODAN において VNC ポートがインターネットから接続でき、

パスワードなしでログインが可能なシステムを調査し、24 件の IP アドレスの管理者に対して危険性を伝えました。
さらに、国外で同じ状態下のシステムの IP アドレスをまとめた SHODAN とは別の海外サイトが開設され、その中に日本の IP アドレスが 68 件含まれていました。これらについて調査し、制御システムに関連する 1 件の IP アドレスの管理者に危険性を伝えました。残りの 67 件については調査中です。

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 11 件、J-CLICS に関して 18 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 202 件、J-CLICS が 313 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 04 月 27 日、「第 4 回 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しました。本セミナーでは、海外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「Kaspersky Security Analyst Summit 2016」（スペインで開催）と「RSA Conference 2016」（米国で開催）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やベンダの方を中心に 36 名の申し込みがあり、当日は 26 名の方にご参加いただきました。

［第 4 回 海外カンファレンス報告会］

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. アフリカ CSIRT 構築支援 （6 月 1 日-10 日）

情報セキュリティに関する制度や技術が成長段階にある国・地域等からのサイバー攻撃は日本のインターネットユーザの脅威の一つとなっています。JPCERT/CC では、2010 年から、急速なインターネット普及が予想されるアフリカ地域に起因するインシデントの増加に備え、事態が発生した際に迅速かつ円滑な対応ができるよう、同地域の育成と連携の基盤づくりを目的に、CSIRT の構築・運営とそれらを支える人材の育成に取り組んできました。

本四半期には、ボツワナ共和国の首都ハボロネで開催された Africa Internet Summit（AIS）'16 にアフリカ CSIRT 構築支援の一環として参加しました。AIS は AfNOG、AFRINIC が主催する、アフリカのインターネットの発展に携わる産官学を対象としたイベントで、アフリカの ICT における技術動向や政策等に関して、国際コミュニティとの交流を通し、現状や課題について協議することを目的に 2013 年から毎年開催されています。今年は 5 月 29 日から 6 月 10 日まで開催され、366 名が参加者しました。JPCERT/CC は、AfNOG のメンバである AfricaCERT から依頼を受けて、情報技術の向上を目的としたワークショップにおいて 6 月 1 日から 2 日にかけてマルウエア解析トレーニングを行いました。また、同 6 月 2 日に JPCERT/CC が主導するサイバーグリーンのワークショップを行い、インターネット全体の健全性とリスクを各国および地域間で比較できる評価指標を打ち立て、その指標を用いて、より効率的で健全なサイバー空間の実現を目的としたサイバーグリーンへの参加を呼びかけました。JPCERT/CC が関与したトレーニングおよびワークショップには、ボツワナ共和国や南アフリカ、ケニヤ等から約 28 名が参加しました。

［図 4-1　マルウエア解析トレーニング参加者との集合写真］

また、6 月 3 日には JPCERT/CC 元理事の山口 英氏、国際部シニアアナリストの小宮山 功一朗、および法人としての JPCERT/CC に対して AfricaCERT から AfricaCERT Meritorious Service Award（AfricaCERT 功労賞）が授与されました。これは、アフリカ地域における CSIRT の構築と運営に対する支援、および人材育成への取組みにおける功績を顕彰したものです。

［図 4-2　受賞の風景］

［図 4-3　AfricaCERT 功労賞］

AIS’16 および AfricaCERT、サイバーグリーンの詳細については、次の Web ページをご参照ください。

Africa Internet Summit ’16

https://internetsummitafrica.org/

AfricaCERT

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

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 国際 CSIRT 間連携

インシデント対応における連携強化、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り組み状況の共有を目的として、海外の National CSIRT との国際連携を強化するための活動を行っています。また、APCERT や FIRST で主導的な役割を担う等、多国間の CSIRT 連携の枠組みにも積極的に参加しています。

4.2.1 APCERT（Asia Pacific Computer Emergency Response Team）

JPCERT/CC は、APCERT において 2003 年 2 月の発足時から継続して Steering Committee（運営委員会）のメンバに選出されており、継続して事務局を担当しています。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

APCERT Steering Committee は 4 月 19 日、6 月 24 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、事務局としてサポートを行いました。

4.2.2 FIRST（Forum of Incident Response and Security Teams）

JPCERT/CC は、FIRST の活動にも 1998 年の加盟以来、積極的に参加しています。2014 年からは国際部シニアアナリストの小宮山功一朗が FIRST の理事を務めてきました。本四半期は、6 月にソウルで開催された第 28 回 FIRST 年次会合の担当理事として、会合準備および開催に係るさまざまな活動をしました。今年の FIRST 年次総会で任期が満了しましたが、6 月 16 日に実施された理事改選選挙で再選され、さらに 2 年間にわたり理事を務めることになりました。今後も引き続きさまざまな FIRST の活動をリードしてまいります。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 28th Annual FIRST Conference Seoul への参加（6 月 12 日-17 日）

第 28 回 FIRST 年次会合が 6 月 12 日から 17 日までソウルで開催されました。本会合は、サイバーインシデントの予防、対応、技術分析等に関する最新動向の情報交換およびインシデント対応チームの連携強化を目的に毎年開催されています。今年は "Getting to the Soul of Incident Response"のテーマの下に多種多様なトピックが取り上げられ、67 の国と地域から 670 名が参加しました。

JPCERT/CC は、6 月 15 日と 17 日にそれぞれ "Approach and Outcome of 'AOKI' – DNS Sinkhole by JPCERT/CC"および"Detecting Lateral Movement in APTs – Analysis Approach on Windows Event Log" と題する講演を行い、JPCERT/CC が運用する DNS シンクホールへの取り組みや、APT 攻撃による内部ネットワークの感染拡大を検知する手法としての Windows イベントログの分析について紹介しました。また、6 月 15 日にはサイバーグリーンの BOF セッションを開き、サイバーグリーンのリスク評価指標やポータルに関するアップデートを紹介し、リスク評価指標を向上させるための意見を求めました。

さらに、この機会を利用し、世界各国の National CSIRT や製品ベンダの CSIRT 等と個別に意見を交換するとともに、脆弱性ハンドリングや制御システムセキュリティ等に関する SIG（Special Interest Group）、またアジア太平洋地域の National CSIRT の集いに参加し、各分野の活動について情報を共有しました。このような会合への参加を通した、各地域間の情報共有の促進や信頼関係の醸成によって、国際間でのインシデント対応調整がより円滑に進められるよう今後も活動してまいります。第 28 回 FIRST 年次会合についての詳細は、次の Web ページをご参照ください。

28th Annual FIRST Conference Seoul
https://www.first.org/conference/2016

4.2.2.2 National CSIRT Meeting（NatCSIRT）2016 への参加（6 月 17 日-18 日）

第 28 回 FIRST 年次会合後に引き続き、米国 CERT/CC が主催する National CSIRT Meeting（NatCSIRT）2016 がソウルで開催されました。本会合は、世界各国の National CSIRT が一堂に会し、国を代表するインシデント対応チームとしての活動計画や課題を共有し、開発ツールや共同プロジェクト、調査研究等に関して発表や議論することを目的に毎年開催されており、今年で 11 回目を迎えました。今回は過去最多の 46 の国と地域から 102 名が参加しました。JPCERT/CC は、NatCSIRT の場でもサイバーグリーンのリスク評価指標やポータルのアップデートを紹介し、リスク評価指標を向上させるための意見を求めました。NatCSIRT についての詳細は、次の Web ページをご参照ください。

NatCSIRT 2016
https://www.cert.org/natcsirt/

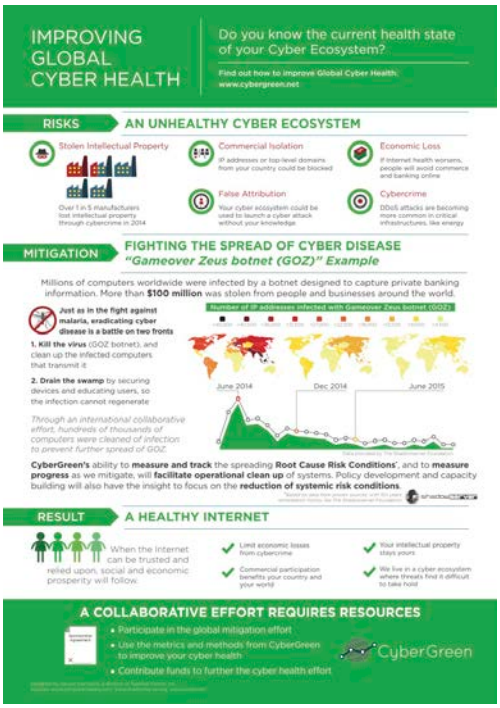
4.2.3 国際 CSIRT 間連携に係る海外カンファレンス等への参加

4.2.3.1 28th TRANSITS I Training Workshop への参加（4 月 13 日-4 月 14 日）

JPCERT/CC は、4 月 13 日から 14 日にオランダのエグモント・アーン・ゼーで開催された TRANSITS I Training Workshop に参加しました。TRANSITS は、欧州の教育研究振興のための会員組織 GÉANT が主導する CSIRT トレーニングで、CSIRT としての組織体制や、技術、運用、法制度、組織構成等、複数の側面から CSIRT の総合的な理解を深めることを目的に開催されています。日本では、日本シーサート協議会が CSIRT の設立促進および対応能力向上を目的に、日本向けに編成した TRANSITS トレーニングを開催しています。JPCERT/CC は、欧州のトレーニングマテリアルを日本でのトレーニングに生かせるよう取り組んでいます。

4.2.3.2 G7 香川・高松情報通信大臣会合におけるサイバーグリーンの紹介（4 月 29 日-30 日）

先進国首脳会議 G7 の香川･高松情報通信大臣会合が 4 月 29 日から 30 日の二日間にわたり開催されました。本会合では 4 つのセッションが行われ、そのうち「情報の自由な流通とサイバーセキュリティ」のセッションにおいて、JPCERT/CC が主導するサイバーグリーンの取り組みが紹介されました。本会合のためにサイバーグリーンについて分かりやすく説明したパンフレット（図 4-4 参照）を作成して配布し、情報提供サイト https://www.cybergreen.net/ のデザインも一新しました。



［図 4-4　サイバーグリーン説明パンフレット］

本会合では、国際機関も含めた相互の連携・協力を図ることを目的に、G7 各国の具体的な取り組みを集めた協調行動集が、G7 の成果文書の一つである「共同宣言」の附属書として策定されました。その中で、G7 各国が連携の拡大を模索することが奨励される活動の一つとして「日本は、ボットと脆弱なネットワークサーバの除去、およびサイバー攻撃に対して強靭かつクリーンなサイバー空間の形成のためにサイバ

ーリスクを分析する、リスクベースの共通指標を開発し利用することを目標とするグローバルな連携のイニシアティブである、サイバーグリーンプロジェクトにおける連携を歓迎する」旨が明記されました。G7 香川・高松情報通信大臣会合についての詳細は、次の Web ページをご参照ください。

林大臣が G7 香川・高松情報通信大臣会合に出席しました
http://www.meti.go.jp/press/2016/05/20160502001/20160502001.html
G7 香川・高松情報通信大臣会合の開催結果
http://www.soumu.go.jp/menu_news/s-news/01tsushin06_02000083.html
G7 協調行動集（仮訳）
http://www.meti.go.jp/press/2016/05/20160502001/20160502001-6.pdf

4.2.3.3 米国大使館 Cyber Security Conference への参加（5 月 17 日）

5 月 17 日に慶應義塾大学三田キャンパスで、米国務省および米国大使館・商務部の主催による Cyber Security Conference が開催されました。JPCERT/CC は本カンファレンスに参加し、サイバーグリーンの構想と取り組みについて講演し、政府関係者やセキュリティ関連企業等の参加者に向けて、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を呼びかけました。

4.2.3.4 CNCERT/CC 年次会合への参加（5 月 24 日-26 日）

JPCERT/CC は、5 月 24 日から 26 日に中国の成都で開催された CNCERT/CC 年次会合に参加し、中国でのインシデント動向や脅威動向に関する情報を収集しました。また、サイバーグリーンの取組みについて講演し、政府関係者やセキュリティ関連企業等の参加者に向けて、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を呼びかけました。さらに、中国と協力して対応している案件等について、関連組織と意見交換を行いました。

4.2.3.5 GFCE（Global Forum on Cyber Expertise）年次会合への参加（6 月 1 日-2 日）

JPCERT/CC は、6 月 1 日から 2 日にワシントン D.C.で開催された第一回 GFCE 年次会合に参加しました。本会合にて、サイバーグリーンが GFCE のイニシアティブとして新たに採択されることが決定しました。GFCE は、2015 年 4 月にハーグで開催された GCCS（Global Conference on CyberSpace: サイバー空間に関する国際会議）2015 にて、サイバーに関する機能強化を支援、推進するためのプラットフォームとして創設されたものです。GFCE 年次会合についての詳細は、次の Web ページをご参照ください。

GFCE members share results at first Annual Meeting
http://www.thegfce.com/

4.2.4 海外 CSIRT 等の来訪および往訪

4.2.4.1 ミャンマーmmCERT の来訪（6 月 20 日）

独立行政法人 国際協力機構（JICA）による研修の一環として、ミャンマーの mmCERT およびその管轄組織である運輸通信省の NCSC（National Cyber Security Center）から 1 名ずつ、計 2 名が JPCERT/CC を来訪しました。JPCERT/CC は、National CSIRT に求められる活動や役割について、JPCERT/CC での取り組みを例に講義を行い、日本シーサート協議会をはじめとした日本国内における民間 CSIRT の状況や、APCERT や FIRST 等を通じた CSIRT 間の国際連携の取り組みについて紹介しました。さらに、ミャンマーの情報セキュリティに関する体制や法整備等について情報収集と意見交換を行い、今後も一層の連携強化を図ることを確認しました。

4.3 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。

PHP Files in CMS, Targeted for Alteration (4 月 8 日)
http://blog.jpcert.or.jp/2016/04/php-files-in-cms-targeted-for-alteration.html

Some coordinated vulnerability disclosures in April 2016 (5 月 6 日)
http://blog.jpcert.or.jp/2016/05/some-coordinated-vulnerability-disclosures-in-april-2016.html

Workshop and Training in Congo (5 月 23 日)
http://blog.jpcert.or.jp/2016/05/workshop-and-training-in-congo.html

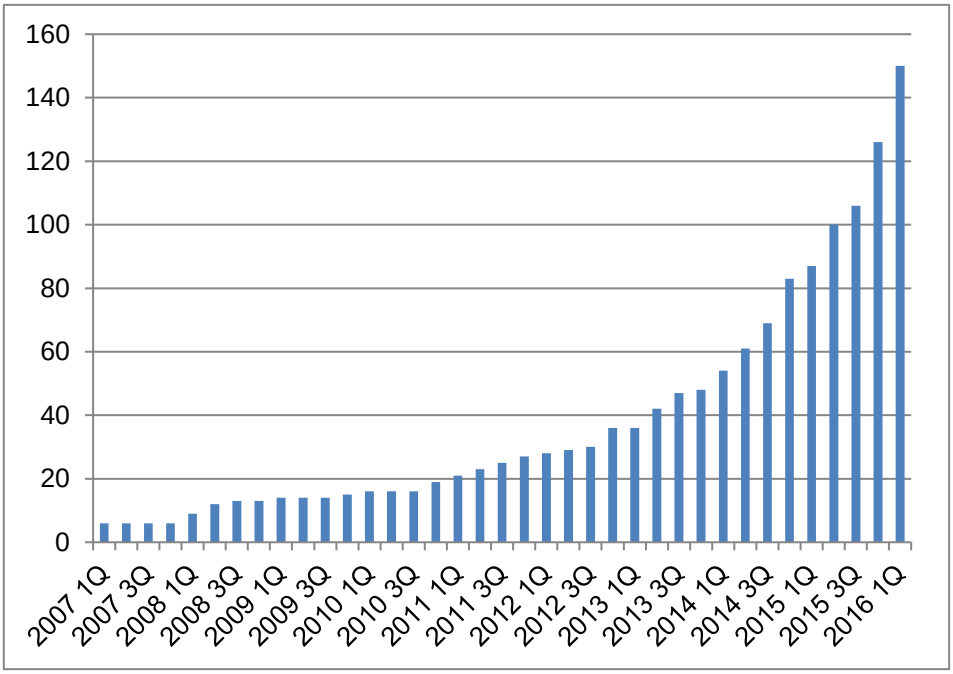
Decoding Obfuscated Strings in Adwind (5 月 25 日)
http://blog.jpcert.or.jp/2016/05/decoding-obfuscated-strings-in-adwind.html

Classifying Malware using Import API and Fuzzy Hashing – impfuzzy – (5 月 25 日)
http://blog.jpcert.or.jp/2016/05/classifying-mal-a988.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、JB サービス株式会社（シーサート名称は SMAC。他の会員についても同様にシーサート名称を括弧書き）、大日本印刷株式会社（DNP-CSIRT）、株式会社　住友倉庫（SWC-CSIRT）、テンプホールディングス株式会社（TEMP-SIRT）、株式会社静岡銀行（SHIZUGIN-CSIRT）、鹿島建設株式会社（K-SIRT）、アメリカンホーム医療・損害保険株式会社（AHA-CSIRT）、株式会社バンダイナムコホールディングス（BN-CSIRT）、城北信用金庫（JOHOKU-CSIRT）、株式会社シーイーシー（CEC-SIRT）、京王電鉄株式会社（KEIO-SIRT）、コニカミノルタ株式会社（KM-CSIRT）、株式会社ティーエムホールディングス（KTC-SIRT）、三菱原子燃料株式会社（MNF-CSIRT）、株式会社 IHI（IHI-CSIRT）、総合メディカル株式会社（SOGO SIRT）、株式会社シマンテック（START）、Sansan 株式会社（Sansan-CSIRT）、三井住友トラスト・パナソニックファイナンス株式会社（SuMiTPFC-CSIRT）、フォーティネットジャパン株式会社（FortiGuard）、京セラコミュニケーションシステム株式会社（KCCS-CSIRT）、富士フイルム株式会社（FF-CSIRT）、株式会社　ジャックス（JACCS-CSIRT）、エイベックス・グループ・ホールディングス株式会社（avex-sec）の 24 組織が新規に加盟しました。本四半期末時点で 150 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］

5 月 23 日（月）には「日本シーサート協議会　第 2 回連携ワークショップ（大阪）～ 脆弱性ハンドリングとインシデントハンドリングへの対応 ～」を開催しました。本ワークショップは、日本シーサート協議会に加盟している組織を対象にしており、外部からの報告や通知を受けた場合の 「脆弱性ハンドリング」と、具体的なハンドリング事例を交えた「インシデントハンドリング」についての勉強会です。

日本シーサート協議会　第 2 回連携ワークショップ（大阪）開催報告
～ 脆弱性ハンドリングとインシデントハンドリングへの対応 ～
http://www.nca.gr.jp/2016/coop-ws/index.html

また、6 月 21 日（火）には、「第 13 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。また、新しく加盟した 31 チームが自組織のシーサートチームの概要を紹介しました。

第 13 回シーサートワーキンググループ会
2016 年 6 月 21 日（火）10:00-18:00
会場：株式会社日立製作所（HIRT）
参加人数：219 名

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 11 件発信しました。

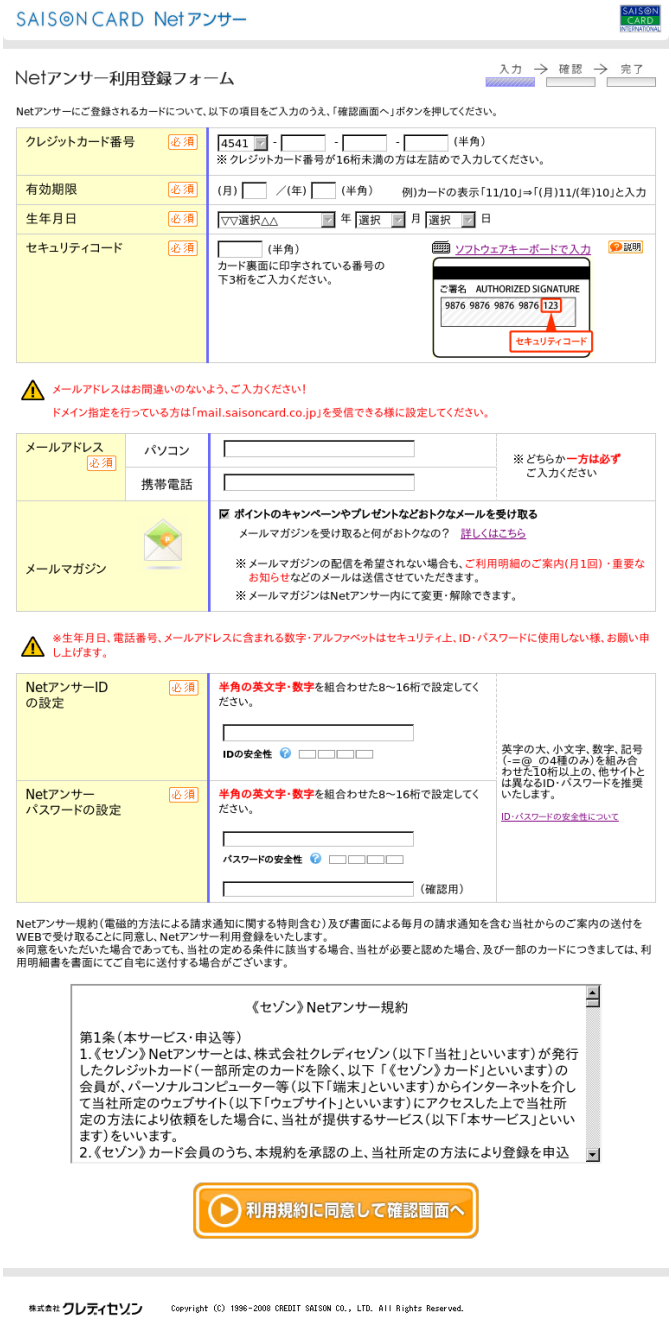
昨年 12 月から頻繁に発生している、SMS（ショートメッセージサービス）を使った銀行のフィッシングサイトへの誘導が、本四半期に入ってからも引き続き確認されました。また、以前からあった、クレジットカード会社をかたるフィッシングは、本四半期においても継続的に報告されました。なお、本四半期においては、2016 年に入ってから初めての Apple をかたるフィッシングのサイトの報告が寄せられました。協議会では、名前をかたられた各事業者に、メール本文やサイトの URL 等の関連情報を提供しました。

また、合計 7 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 1 件、クレジットカード会社をかたるフィッシング関連が 4 件、その他が 2 件でした。それぞれの例として、［図 6-1］にゆうちょ銀行をかたるフィッシング（2016/04/12）、［図 6-2］に OMC Plus をかたるフィッシング（2016/05/23）、［図 6-3］に Apple をかたるフィッシング

（2016/05/20）の注意喚起を示します。

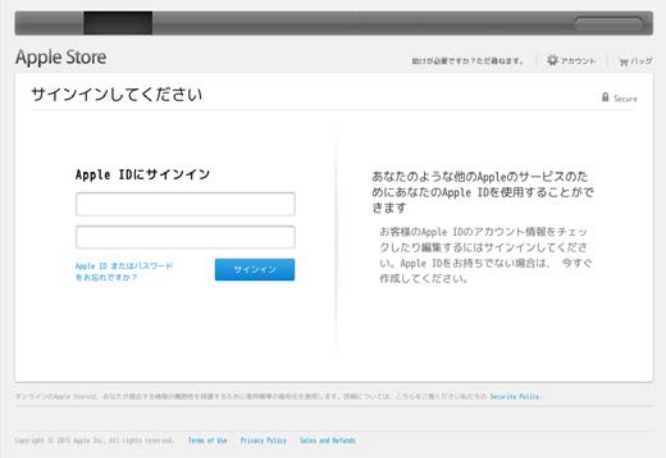
［図 6-1］ゆうちょ銀行をかたるフィッシング（2016/04/12）

https://www.antiphishing.jp/news/alert/yuucho_20160412.html



［図 6-2］OMC Plus をかたるフィッシング（2016/05/23）

https://www.antiphishing.jp/news/alert/omc_plus_20160523.html



［図 6-3］Apple をかたるフィッシング（2016/05/20）
https://www.antiphishing.jp/news/alert/apple_20160520.html

これらの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、全てのサイトの停止を確認しました。

6.2. フィッシングサイト URL 情報の提供

協議会員のうち、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事業者と、フィッシングに関する研究を行っている学術機関に対し、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、日に数回の頻度で提供しています。この URL 情報の提供は、各社の製品のブラックリストへの追加等、ユーザ保護に向けた取り組みに活用していただくことや、研究教育機関における関連研究の促進を目的としています。本四半期末の時点における情報提供先は 24 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の講演活動を行っています。本四半期は次の講演を行いました。

駒場 一民
「Phishing Trend in Japan and the Counteraction taken as the Council of Anti-Phishing Japan」
APWG Symposium on Electronic Crime Research , 2016 年 6 月 1 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 4 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201604.html
フィッシング対策協議会 2016 年 5 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201605.html
フィッシング対策協議会 2016 年 6 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201606.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 37 回運営委員会
日時：2016 年 4 月 15 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 38 回運営委員会
日時：2016 年 5 月 17 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 39 回運営委員会
日時：2016 年 6 月 10 日 16:00 - 18:00
場所：トッパン・フォームズ株式会社

7.2 「フィッシングレポート 2016 ～ 世界に広がるフィッシング対策の輪 ～」 公開

昨年度開催された、フィッシング対策協議会のガイドライン策定ワーキンググループにおいて、フィッシングの被害状況、フィッシングの攻撃技術・手法などをとりまとめた 「フィッシングレポート 2016 ～ 世界に広がるフィッシング対策の輪 ～」 を公開しました。

本レポートは、2015 年度のフィッシング対策協議会のガイドライン策定ワーキンググループにおける、フィッシングの被害状況、フィッシングの攻撃サイドの技術・手法などをまとめています。

フィッシングレポート 2016 - 世界に広がるフィッシング対策の輪 -
https://www.antiphishing.jp/report/pdf/phishing_report_2016.pdf

7.3 フィッシング対策ガイドラインの改訂

フィッシング対策協議会のガイドライン策定ワーキンググループでは、サービス事業者や利用者におけるフィッシング対策など各要件の内容の見直し、読みやすさの向上を目的として、年ごとにフィッシング対策ガイドラインを改訂しています。2015 年に公表したガイドラインに脅威の現状や新しい対策技術の反映し、2016 年 5 月 27 日に「フィッシング対策ガイドライン 2016 年度版」を公開しました。

フィッシング対策ガイドライン 2016 年度版
https://www.antiphishing.jp/report/pdf/antiphishing_guide.pdf

7.4 フィッシング対策協議会総会開催

フィッシング対策協議会年次総会を次のとおり開催しました。

フィッシング対策協議会 2016 年度総会
日時：2016 年 6 月 24 日 14:00 - 16:00
場所：エッサム神田 1 号館 5 階会議室

8. 公開資料

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

8.1 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［2016 年第 1 四半期（1 月～3 月）］（2016 年 4 月 27 日）
https://www.jpcert.or.jp/press/2016/vulnREPORT_2016q1.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 2016 年 1 月～3 月
（2016 年 5 月 26 日）
https://www.jpcert.or.jp/tsubame/report/report201601-03.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2015Q4.pdf

8.3 分析センターだより

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

(1) Adwind が持つ難読化された文字列の解読（2016-04-25）

2015 年後半から 2016 年にかけて、Adwind と呼ばれる遠隔操作マルウエアを用いた攻撃が世界的に増えました。分析センターは、Adwind が持つ難読化された文字列の解読を効率的に行うためのツール「adwind_string_decoder.py」を作成し公開しました。

Adwind が持つ難読化された文字列の解読（2016-04-25）
https://www.jpcert.or.jp/magazine/acreport-adwind.html

(2) Import API と Fuzzy Hashing でマルウエアを分類する ～impfuzzy～（2016-05-09）

マルウエア検体の調査は、既知のマルウエアかどうかを判別することから始めます。データベース化された多数の既知のマルウエアの中から調査検体と似たものを高速に見つけ出すための新たな手法 impfuzzy を提案し、impfuzzy を計算、比較する Python モジュール pyimpfuzzy を公開しました。

Import API と Fuzzy Hashing でマルウエアを分類する ～impfuzzy～（2016-05-09）
https://www.jpcert.or.jp/magazine/acreport-impfuzzy.html

(3) ショートカットファイルから感染するマルウエア Asruex（2016-06-23）

2015 年 10 月頃から宛先の組織を絞り込んで不正なショートカットファイルが送信されています。このファイルを開くと、Asruex と呼ばれるマルウエアに感染します。この Asruex は、リモートから操作する機能を持ったマルウエアで、攻撃者はターゲットにした組織に侵入を試みていると考えられます。JPCERT/CC が調査した Asruex の詳細を解説しました。

ショートカットファイルから感染するマルウエア Asruex（2016-06-23）
https://www.jpcert.or.jp/magazine/acreport-asruex.html

(4) 攻撃者の行動によって残る痕跡を調査（2016-06-28）

攻撃者がネットワーク内に侵入後に利用する可能性が高いツール、コマンドについて、それらを実行した際にどのような痕跡が Windows OS 上に残るのかを検証し、インシデントの初期調査を行う担当者に利用いただける参照用資料としてまとめた「インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書」を紹介しました。

攻撃者の行動によって残る痕跡を調査（2016-06-28）
https://www.jpcert.or.jp/magazine/acreport-ir_research.html

8.4 OWASP アプリケーションセキュリティ検証標準 3.0.1 邦訳資料

セキュアな Web アプリケーションに求められる要件とそのセキュリティ検証を行うための標準として OWASP（Open Web Application Security Project）において策定された OWASP Application Security Verification Standard （ASVS:アプリケーションセキュリティ検証標準）3.0.1 を翻訳し、公開しました。本資料は、アプリケーションの設計、開発、脆弱性診断などにおいて必要となるセキュリティ要件の標準を確立することを目指し、アーキテクチャ、認証、セッション管理、アクセス制御など、アプリケーションに必要とされるセキュリティ要件を総計 19 のカテゴリに分類してまとめています。アプリケーション開発を発注する企業、開発業者、セキュリティ診断サービス提供者など、複数の関係者がセキュリティ要件に関する認識を合せるなど、セキュアなアプリケーション開発にご活用いただけます。

OWASP アプリケーションセキュリティ検証標準 3.0.1
https://www.jpcert.or.jp/securecoding/materials-owaspasvs.html

8.5 インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書

近年の標的型攻撃におけるインシデント調査で見つかった、多くの攻撃者が使用するツールを選び出し、それらツールが実行された時にサーバやクライアントにどのようなログが残るのか、またどのような設定をすれば十分な情報を含むログを取得できるようになるのかを調査し、報告書にまとめて公開しました。

インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書
（2016 年 6 月 28 日）
https://www.jpcert.or.jp/ research/ir_research.html

8.6 2015 年度 CSIRT 構築および運用における実態調査

日本シーサート協議会（NCA）に加盟している CSIRT と業界の中で際立った活動を行っている CSIRT を対象に、組織体制やメンバ構成、ポリシーなど CSIRT の構築時に定義しておくべき項目について、アンケート調査およびインタビューによって調査しました。CSIRT の構築や活動の改善に参考資料として活用いただけるよう調査報告書にまとめ公開しました。

2015 年度 CSIRT 構築および運用における実態調査
（2016 年 6 月 29 日）
https://www.jpcert.or.jp/research/2015_CSIRT-survey.html

9. 主な講演活動

(1) 竹田 春樹（分析センター　マネージャ）：
「サイバー攻撃の最新動向と対応・対策を行う上での備えと対応」
日経 BP 情報セキュリティ戦略セミナー,2016 年 05 月 31 日
(2) 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）：
「サイバー攻撃の最新動向と対応」
デジタルアーツ/ファイア・アイ 高度標的型攻撃対策セミナー, 2016 年 06 月 15 日
(3) 村上 晃（経営企画室 兼 エンタープライズサポートグループ 部門長）：
「サイバー攻撃の最新動向と対応体制」
北関東 IBM ユーザー研究会　2016 総会, 2016 年 06 月 21 日

10. 主な執筆活動

(1)洞田 慎一（早期警戒グループ マネージャ）：
「メディアに対するサイバー攻撃とその対策 2015 年の事例から」
日本民間放送連盟「月刊民放」5 月号,2016 年 05 月 01 日

11. 協力、後援

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) Interop Tokyo2016
主催：Inlerop Tokyo実行委員会
開催日：2016年06月08日～10日

(2) Hardening Project2016
主　催：内閣府沖縄総合事務局
開催日：2016年06月04日～05日

(3) RSA Capture The Flag
主　催：EMCジャパン株式会社 RSA事業本部
開催日：2016年06月29日

■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