JPCERT/CC

Japan Computer Emergency Response Team Coordination Center

JPCERT-PR-2016-03
発行日：2016-10-12

JPCERT/CC 活動概要 [2016 年 7 月 1 日 ～ 2016 年 9 月 30 日]

活動概要トピックス

ートピック1ー　Windows の新しいセキュリティ機能の効果を検証して分析センターだよりで紹介

JPCERT/CC では、最近の Windows OS に実装されたセキュリティ機能のうち、システムから隔離した環境（サンドボックス）でアプリケーションを動作させる「AppContainer」、アカウント情報を保護する「LSA の保護モード」および「Credential Guard」の機能に着目し、実際の攻撃に用いられた検体を使って検証を行い、分析センターだより「脆弱性を攻撃された Web ブラウザにおける AppContainer の防御効果」および「Windows の新セキュリティ機能を検証する:LSA の保護モードと Credential Guard」で紹介しました。

Microsoft 社は、高度化する最近のサイバー攻撃に対する防御手段として Windows OS にさまざまな新しいセキュリティ機能を追加・実装しています。そうしたセキュリティ機能のうち、アプリケーションをシステムから隔離した環境で動作させファイルアクセスや他プロセスへのアクセスを制限する機能である「AppContainer」、ドメイン端末のアカウント情報を保護する機能である「LSA の保護モード」および「Credential Guard」について、JPCERT/CC が調査した標的型攻撃事案などで使用された攻撃ツールや検体などを用いて、実際の攻撃に近い形で検証を行いました。また、セキュリティ機能の有効性を損なわないための注意点も記載しています。高度化するサイバー攻撃への対抗手段を検討する際の参考資料として本検証結果をぜひご活用ください。

脆弱性を攻撃された Web ブラウザにおける AppContainer の防御効果 (2016-07-20)
https://www.jpcert.or.jp/magazine/acreport-AppContainer.html

Windows の新セキュリティ機能を検証する:LSA の保護モードと Credential Guard (2016-09-07)
https://www.jpcert.or.jp/magazine/acreport-lsa_protect.html

「分析センターだより」では、JPCERT/CC の分析センターの分析技術者が日々の業務によって得られた情報や知見、および個別の事案に直結した調査結果を個人の視点からまとめ、マルウエアアナリストや情報セキュリティの専門家の皆様と共有するために不定期に発行しています。

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 3137 件、インシデント件数ベースでは 2801 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 2122 件でした。前四半期の 2559 件と比較して 17%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 467 件で、前四半期の 642 件から 27%減少しました。また、前年度同期（522 件）との比較では、11%の減少となりました。

本四半期のフィッシングサイトの報告件数を、装っていたブランドが国内か国外かで分けた内訳を添えて［表 1-1］に示します。

［表 1-1 フィッシングサイトの国内・国外ブランド別の件数］

フィッシングサイト	7 月	8 月	9 月	国内外別合計（割合）
国内ブランド	30	43	33	106(23%)
国外ブランド	94	73	76	243(52%)
ブランド不明(注 2)	42	31	45	118(25%)
月別合計	166	147	154	467(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。

前四半期に引き続き、国内通信事業者の Web メールを装ったフィッシングサイトに関する報告が多数寄せられています。これらのフィッシングサイトでは、海外の Web サイトに不正に侵入して設置されたものや、無料 Web サイトサービスを使用して設置されたものがありました。無料 Web サイトサービスは、大学の Web メールを装ったフィッシングサイトでも使用されており、メールの認証情報を窃取しようとする攻撃者に悪用される傾向があります。

金融機関を装ったフィッシングでは、複数のクレジットカードのブランドを装ったフィッシングサイトの報告が寄せられています。これらのフィッシングサイトでは、無料で登録できる.cc ドメインや.online ドメインを使用しているという特徴が見られました。

国内オンラインゲームを装ったフィッシングサイトでは、無料で登録できる.cc ドメインのサブドメインを正規サイトに似せた多数の URL が作成されており、香港、中国の特定のホスティング事業者の IP アドレスが割り当てられていました。

フィッシングサイトの調整先の割合は、国内が 25%、国外が 75%であり、前四半期（国内 30%、国外 70%）に比べ、国外と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、554 件でした。前四半期の 1065 件から 48%減少しています。

前四半期に引き続き、”jquery.min.php”という文字列を含む URL に誘導する、不正な JavaScript が埋め込まれる改ざんが多く確認されました。改ざんの被害を受けたサイトとの調整において、サイト管理者の方から、改ざんされた PHP ファイルや、改ざんされた原因の調査結果を提供していただいた事例があり、この事例では、CMS への攻撃によって、攻撃者がコードの実行に使用するバックドアの設置や、PHP ファイルの改ざんが行われたことが分かりました。

改ざんの被害を受けたサイトは CMS を使用している Web サイトが多く、CMS およびそのテーマやプラグインを対象としたスキャンが広範囲に行われていることから推測すると、JPCERT/CC が認知している以上に多数の Web サイトで改ざんが発生している可能性があります。Web サイトの管理に CMS を使用している場合は、最新のバージョンにアップデートし、不要なテーマやプラグインを削除するなどの対策を実施することが推奨されます。

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、10 件でした。前四半期の 15 件から 33%減少しています。本四半期は、延べ 2 組織に対応を依頼しました。

7 月下旬以降、複数の国内組織から、特定の攻撃グループの標的型攻撃によるものと見られるマルウエア感染の報告が寄せられました。

これらの被害組織から、マルウエア感染端末で発見されたファイルの提供を受け分析したところ、HTTP を使用して攻撃者のサーバと通信し遠隔操作を行う HTTP ボットに分類されるマルウエアや、攻撃者が情報収集に使用したと見られるツールなどが確認されました。また、被害組織から提供されたプロキシサーバのログを調査したところ、HTTP ボットに感染した端末と攻撃者のサーバとの通信には、暗号化された文字列が含まれており、復号すると、攻撃者が感染端末を遠隔操作して情報を収集するためのコマンドを実行した結果などが含まれていることが分かりました。

この一連の攻撃では、被害組織のネットワーク上で、一台の感染端末を踏み台にして多数の端末にマルウエア感染を広げていました。これらのマルウエアは、ひとつの被害組織のなかでも感染端末ごとに通信先が設定されており、攻撃者からの指令を伝達する C2 サーバが多数確認されました。また、マルウエアの通信先には、不正に侵入された国内の Web サーバが多く使用されていました。通信先として悪用されたサーバ上には、攻撃者とボットとのやり取りを仲介する PHP スクリプトが設置されており、この PHP スクリプトによって、攻撃者からボットへの命令の送信やボットから送信されたデータの保存、サーバ上に保存されたデータの取得・削除といった操作ができるようになっていました。

その他にも、なりすましメールによって、遠隔操作を行うマルウエア PlugX や、複数の機能を持つボットのダウンロードおよび実行を行う拡張子を偽装したマルウエアが送りつけられるといった報告が寄せられました。

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：2 件　https://www.jpcert.or.jp/update/2016.html

2016-08-01　STOP!! パスワード使い回し!!キャンペーン 2016
　　そのパスワードを知っているのは、本当にあなただけですか？
2016-08-24　注意喚起「サイバー攻撃に備えて Web サイトの定期的な点検を」

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：11 件（うち 0 件更新）　https://www.jpcert.or.jp/at/

2016-07-13　2016 年 7 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)
2016-07-13　Adobe Flash Player の脆弱性 (APSB16-25) に関する注意喚起 (公開)
2016-07-13　Adobe Reader および Acrobat の脆弱性 (APSB16-26) に関する注意喚起 (公開)
2016-07-19　CGI 等を利用する Web サーバの脆弱性 (CVE-2016-5385 等) に関する注意喚起 (公開)

2016-07-20　2016 年 7 月 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起 (公開)
2016-08-10　2016 年 8 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)
2016-09-14　Adobe Flash Player の脆弱性 (APSB16-29) に関する注意喚起 (公開)
2016-09-14　2016 年 9 月 Microsoft セキュリティ情報 (緊急 7 件含) に関する注意喚起 (公開)
2016-09-27　Web サイトで使用されるソフトウエアの脆弱性を悪用した攻撃に関する注意喚起 (公開)
2016-09-28　ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2016-2776) に関する注意喚起 (公開)
2016-09-28　OpenSSL の脆弱性 (CVE-2016-6309) 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 13 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。

2016-07-06　「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」公開
2016-07-13　総務省と経済産業省が「IoT セキュリティガイドライン」公開
2016-07-21　IPA が「ウイルス感染したという警告でアプリのインストールを誘導する手口が急増」を公開
2016-07-27　CGI 等を利用するウェブサーバの脆弱性 (httpoxy) を標的としたアクセス
2016-08-03　NISC と IPA がスマートフォンアプリの使用に関する注意事項を公開
2016-08-10　STOP!! パスワード使い回し!!　そのパスワードを知っているのは、本当にあなただけですか？
2016-08-17　FIRST、奨励金プログラムを「Suguru Yamaguchi Fellowship Program」に改名
2016-08-24　総務省が「Wi-Fi 提供者向け セキュリティ対策の手引き(平成 28 年 8 月版)」公開
2016-08-31　NISC が「安全な IoT システムのためのセキュリティに関する一般的枠組」公開
2016-09-07　銀行をかたるフィッシングサイトに注意
2016-09-14　警察庁が「平成 28 年上半期におけるインターネットバンキングに係る不正送金事犯の発生状況等について」公開
2016-09-23　JSSEC が「Android アプリのセキュア設計・セキュアコーディングガイド 2016 年 9 月 1 日版」を公開
2016-09-28　CEATEC JAPAN 2016 開催

1.2.1.4. 早期警戒情報

JPCERT/CC では、国民の生活や社会経済活動を支えるインフラ、サービスおよびプロダクト等を提供している組織の情報セキュリティ関連部署もしくは組織内 CSIRT に向けて、それらの組織やサービス提供先に深刻なセキュリティ上の問題を惹起する可能性のある脅威情報やその分析結果、対策方法に関する情報等を「早期警戒情報」として提供しています。

早期警戒情報の提供について
https://www.jpcert.or.jp/wwinfo/

1.2.2. 情報収集・分析・提供（早期警戒活動）事例

本四半期における情報収集・分析・提供（早期警戒活動）の事例を紹介します。

【日本に対するサイバー攻撃への対応】
日本の年中行事や記念日、日本が関わる歴史上の出来事に起因する、いわゆるサイバー攻撃の特異日には、日本の政府関係組織等に向けた反日的なサイバー攻撃が多く発生する傾向にあります。本四半期は、とりわけ特異日が集中する時期にあたるため、JPCERT/CC では、国内の関係組織や国外の National CERT と連携して、特に注意深く情報収集を行いました。また、攻撃に備えた対応体制をとるとともに、8 月 24 日に注意喚起「サイバー攻撃に備えて Web サイトの定期的な点検を」を公開しました。
2015 年 8 月下旬には、日本に対するサイバー攻撃の呼びかけや攻撃予告が確認されましたが、大規模な攻撃に繋がる動きは確認されませんでした。また、DDoS 攻撃の影響と思われる Web サイトの応答時間の悪化は一部で確認されましたが、深刻な被害はおおむね発生しませんでした。また、特異日に関連する Web サイト改ざんの被害も確認されませんでした。JPCERT/CC では、特異日周辺でみられた状況を分析し、重要インフラ企業や組織内 CSIRT にレポートを配信しました。

【CGI によって動作する Web サーバの基盤の脆弱性に関する情報発信】
CGI は Web サーバ上で動的にプログラムを動作させる仕組みです。CGI によって起動する複数の Web サーバの基盤に脆弱性が報告されました。この基盤を使用している Web サーバが、遠隔の第三者が送信した Proxy ヘッダを含むリクエストを受信した場合に、サーバの環境変数 HTTP_PROXY に意図しない値が設定される可能性があります。その結果、Web アプリケーションがプロキシサーバを使用する際に、不正なホストへ中継されて、中間者攻撃などが行われる恐れがあります。この脆弱性をもつ Web サーバの基盤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 7 月 19 日に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 9 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

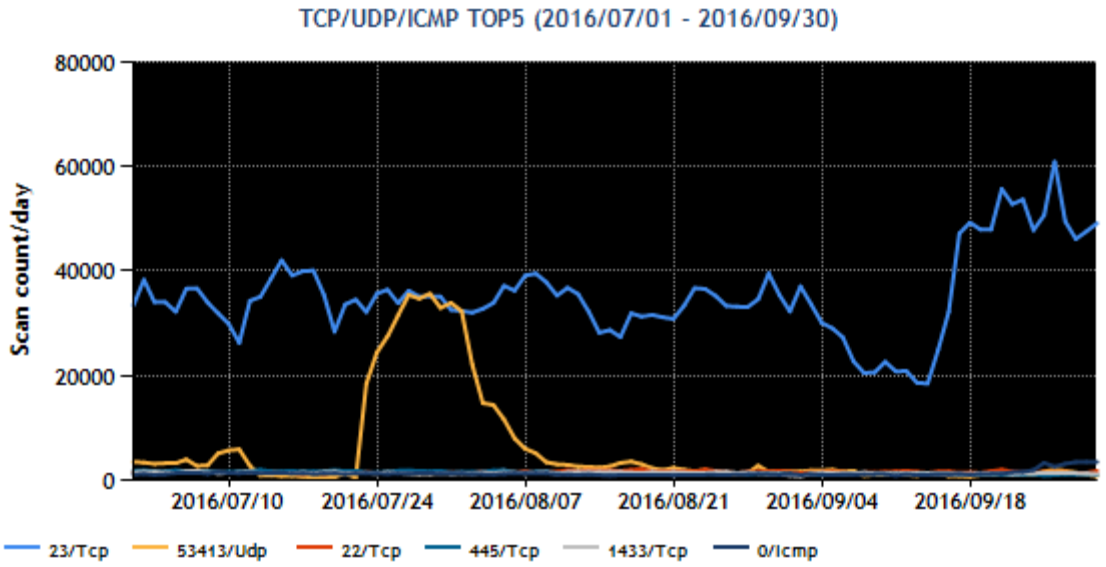
JPCERT/CC は、TSUBAME で収集したデータを宛先ポート番号や送信元地域ごとに分類して統計分析し、既知の脆弱性情報やマルウエア、攻撃ツール等との関連を考察することで、攻撃活動や準備活動の捕捉に努めています。

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 4 月から 6 月分のレポートを 2016 年 8 月 24 日に公開しました。

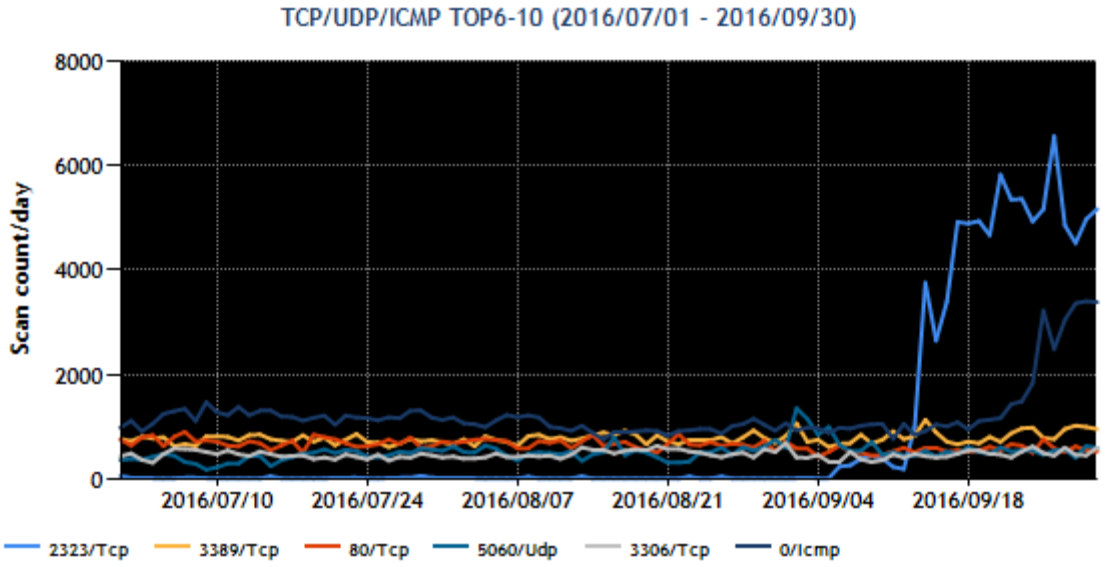
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート（2016 年 4～6 月）
https://www.jpcert.or.jp/tsubame/report/report201604-06.html

本四半期に TSUBAME で観測された宛先ポート別パケット数の上位 1 位～5 位および 6 位～10 位を、［図 1-1］と［図 1-2］に示します。

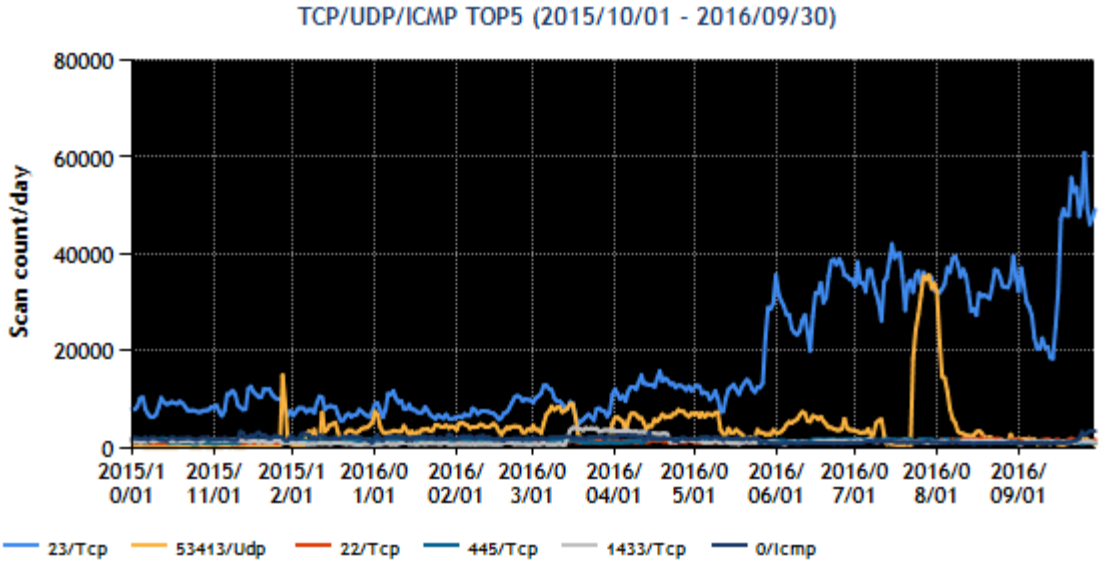


［図 1-1 宛先ポート別グラフ トップ 1-5（2016 年 7 月 1 日-9 月 30 日）］

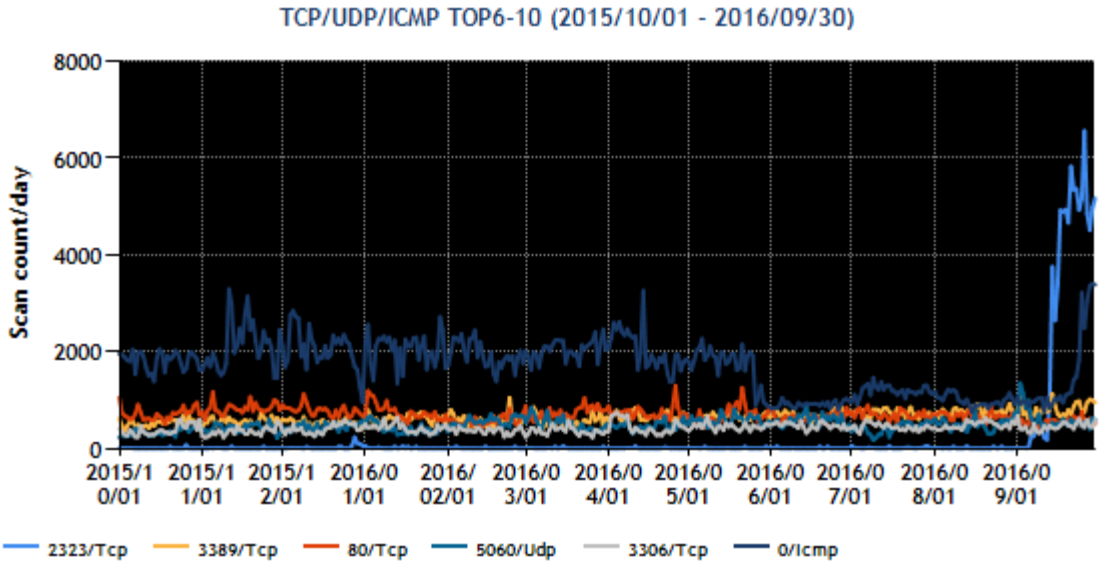


［図 1-2 宛先ポート別グラフ トップ 6-10（2016 年 7 月 1 日-9 月 30 日）］

また、過去 1 年間（2015 年 10 月 1 日-2016 年 9 月 30 日）における、宛先ポート別パケット数の上位 1 位～5 位および 6 位～10 位を［図 1-3］と［図 1-4］に示します。



［図 1-3 宛先ポート別グラフ トップ 1-5（2015 年 10 月 1 日-2016 年 9 月 30 日）］



［図 1-4 宛先ポート別グラフ トップ 6-10（2015 年 10 月 1 日-2016 年 9 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 宛パケット数は 7 月 23 日から 8 月 10 日にかけて急増しました。観測したパケットには、認証とマルウエアのダウンロードを目的としていると思われるパケットが含まれていました。送信元はインターネットに接続された CCTV やルータなどの専用機器であり、これらの専用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されます。

その他、Windows や Windows 上で動作するサービスへのスキャン活動や、SSH サーバ等の遠隔操作のためのサービスへ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ました。

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。主な事例を次に掲げます。

(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ました。JPCERT/CC では、過去の事例から Telnet ポートの探索や Telnet ポートに対する攻撃を行うマルウエアと、23/ TCP 宛のパケット数増加の関連性を疑い、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、マルウエアに感染した複数の国内ベンダ製の機器であることが判明しました。当該機器ベンダの一社に観測したログ情報の一部を共有した結果、機器の設定などを見直すなど対策が行われたようで、そのベンダ製の機器からのパケットが観測されなくなりました。また、他のベンダの機器については管理者に情報を提供して善処を求めました。

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。

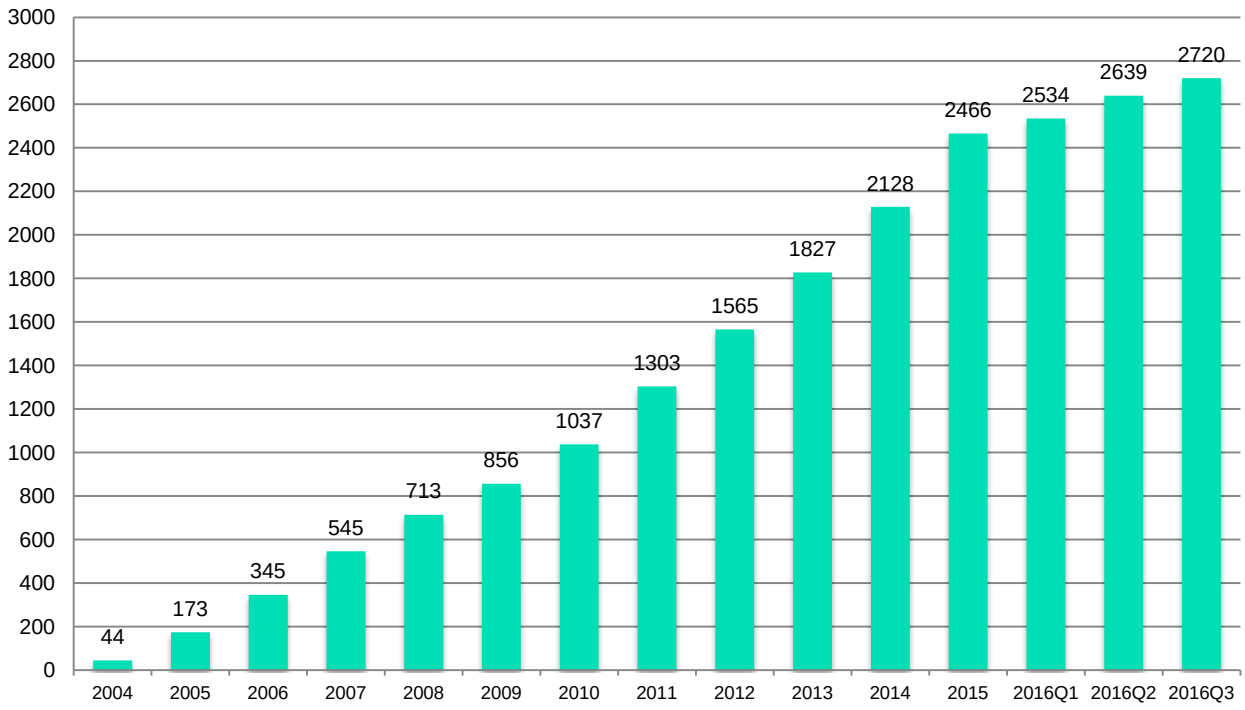
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

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 81 件（累計 2,720 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］

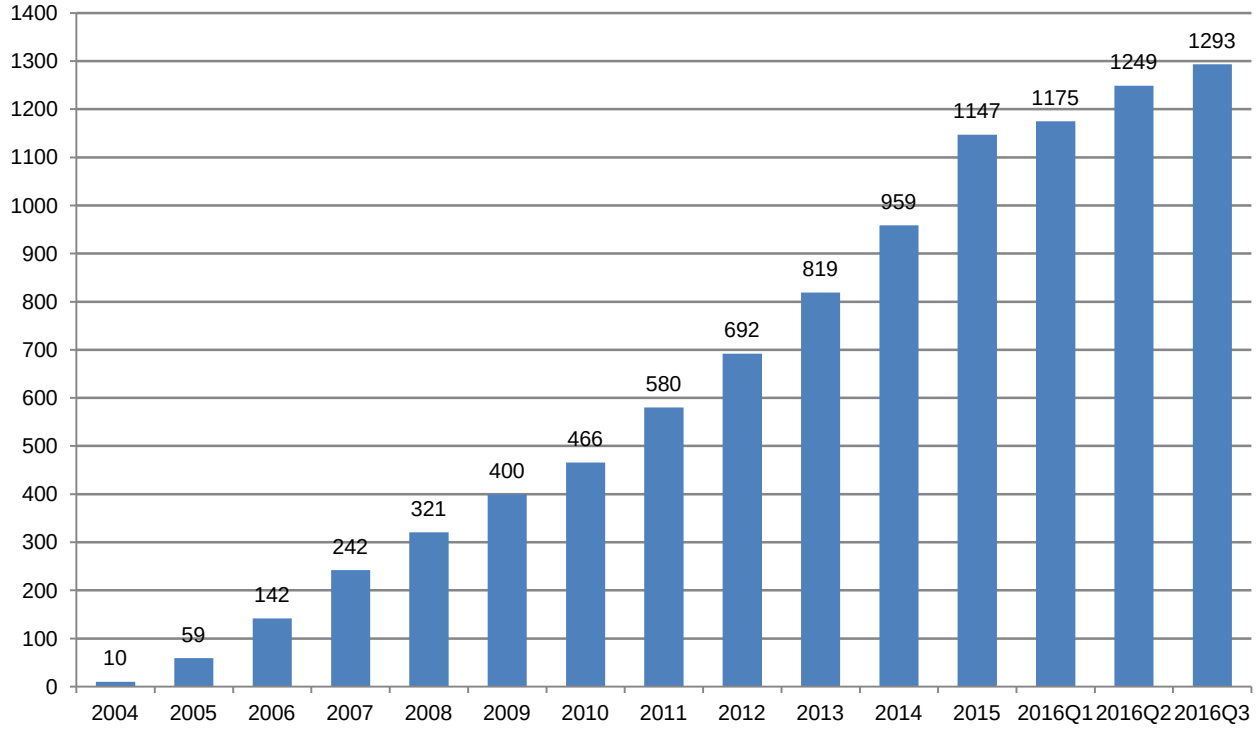
本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 44 件（累計 1,293 件）で、累計の推移は［図 2-2］に示すとおりです。44 件のうち、27 件が国内製品開発者の製品、15 件が海外の

製品開発者の製品、2 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、27 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、グループウエア、Web アプリ、Android アプリ、Windows アプリ、妥規模データ処理ソフトウエア、CMS、プラグイン等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	9
Web アプリ	6
Android アプリ	5
Windows アプリ	4
大規模データ処理ソフトウェア	4
CMS	3
プラグイン	3
Android OS	2
組込系	2
CRM	1
Mac OS アプリ	1
ウェブアプリケーションフレームワーク	1
サーバ製品	1
スマホアプリ	1
ライブラリ	1



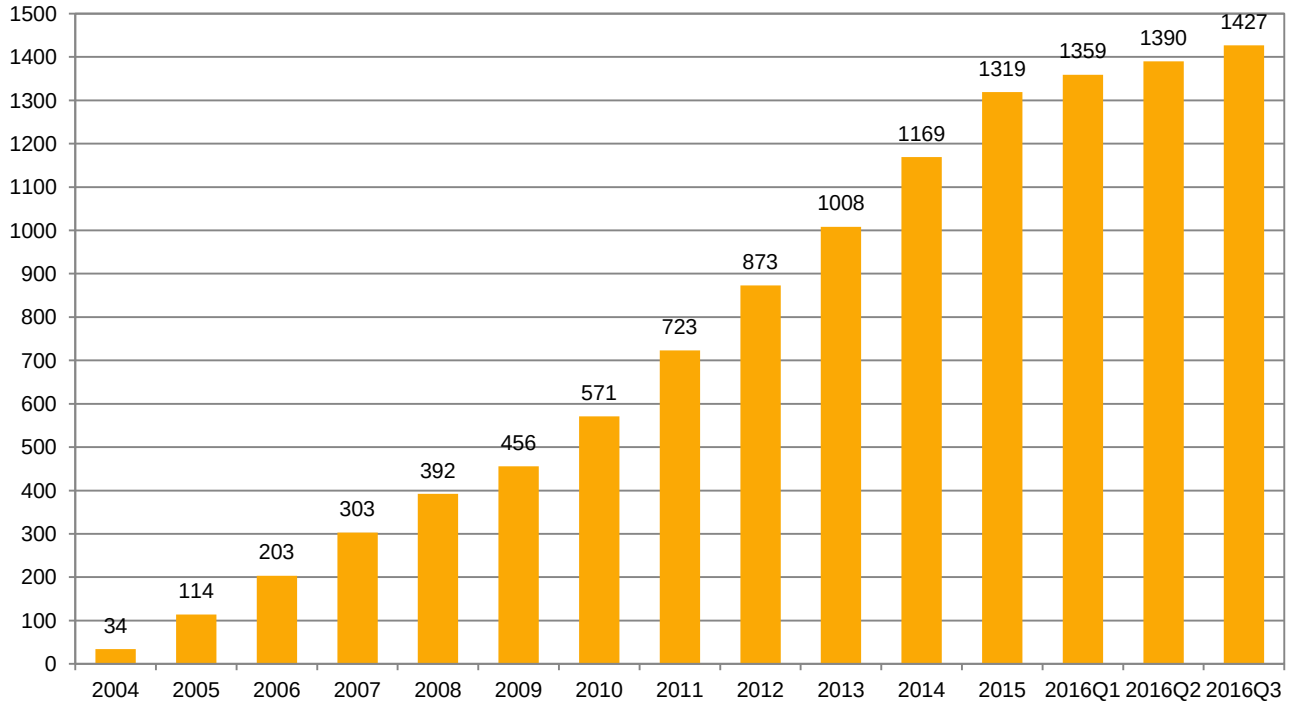
［図 2-2 公表を行った国内取扱脆弱性情報の累積件数］

本四半期に公表した国際取扱脆弱性情報は 37 件（累計 1,427 件）で、累計の推移は［図 2-3］に示すとおりです。また 37 件のうち 1 件は、特定製品に関する注意喚起（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。全四半期に引き続き、本四半期においても組込系製品に関する脆弱性情報を多数公開しました。組込系製品の中でも特に医療関連製品に関するものが多くありました。

［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	6
Web アプリ	5
Windows アプリ	5
Mac OS アプリ	4
ライブラリ	4
DNS	2
iOS	2
Web サーバ	2
ネットワーク製品	2
Android アプリ	1
SDK	1
制御系	1
その他	2



［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 247 件（製品開発者数で 162 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 5 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 205 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2014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、2014年11月より、公表判定委員会が定期的に開催されており、その審議により、これまでに2案件を公表し、その他に、公表すべきと判定されている5案件の公表準備を進めています。

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 13 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。JPCERT/CC は、本四半期に JVN で公表したもののうち国内で届出られた脆弱性情報に 60 個の 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. 脆弱性関連情報の取扱に関する講演活動

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：9 月 26 日
講演タイトル: 脆弱性情報はこうしてやってくる
イベント名：Vuls 祭り #1

脆弱性スキャンツール Vuls は、サーバに対して既知の脆弱性が存在するかどうかを探索するためのツールです。Vuls では、脆弱性情報として NVD や JVN が公開している情報を使っています。システム管理者を中心とする Vuls ユーザ向けに、脆弱性情報が JVN で公開されるまでにどのような活動が行われているかを簡単に解説しました。Vuls および Vuls 祭りに関する詳細は次の Web ページを参照ください。

Vuls 祭り #1
http://vuls-jp.connpass.com/event/38391/
http://www.slideshare.net/jpcert_securecoding/ss-66412794 (講演資料)
vuls: VULnerability Scanner
https://github.com/future-architect/vuls

2.2. 日本国内の脆弱性情報流通体制の整備

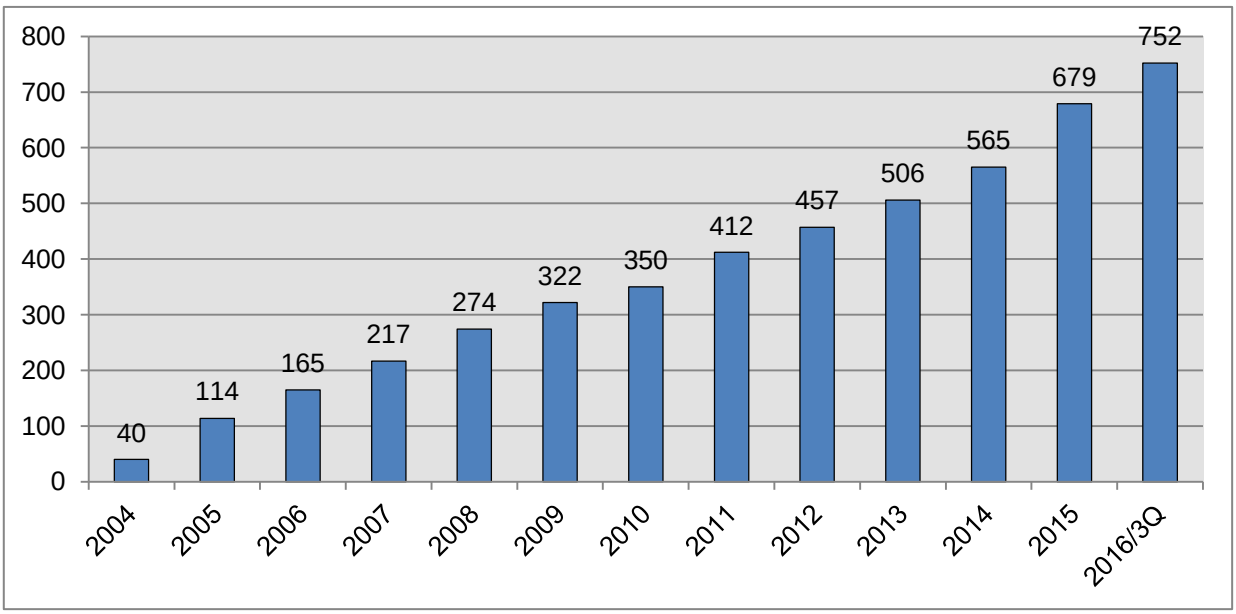
JPCERT/CC では、本基準に従って、日本国内の脆弱性情報流通体制を整備しています。
詳細については、次の Web ページをご参照ください。

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)
https://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 9 月 30 日現在で 752 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. 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（6 件）

- PRE00-C. 関数形式マクロよりもインライン関数やスタティック関数を使う
- PRE01-C. マクロ内の引数名は括弧で囲む
- PRE02-C. マクロ置換リストは括弧で囲む
- PRE03-C. ポインタ型でない型をエンコードするには define よりも typedef を選ぶ

- DCL05-C. typedef による型定義ではポインタ型を避ける
- EXP20-C. 成功、真偽、等価を判定するには明示的な検査を行う

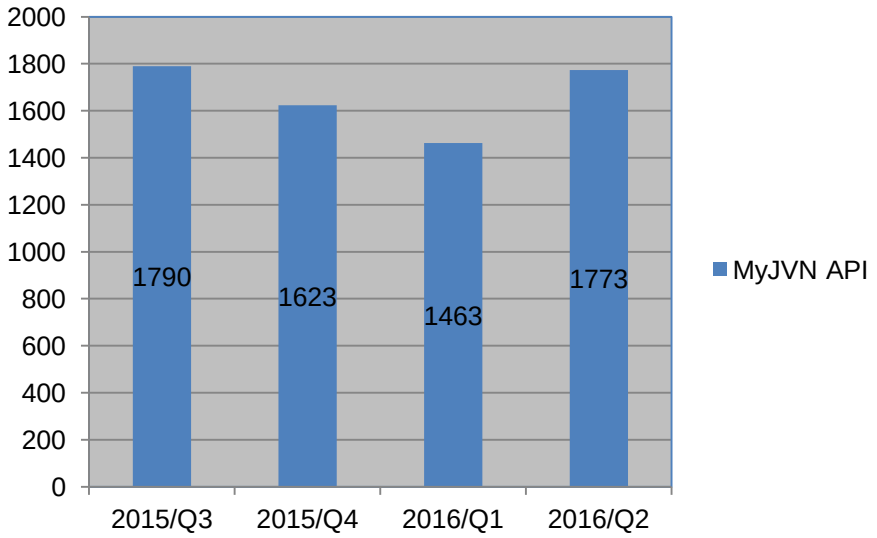
CERT C コーディングスタンダード
https://www.jpcert.or.jp/sc-rules/

2.4. VRDA フィードによる脆弱性情報の配信

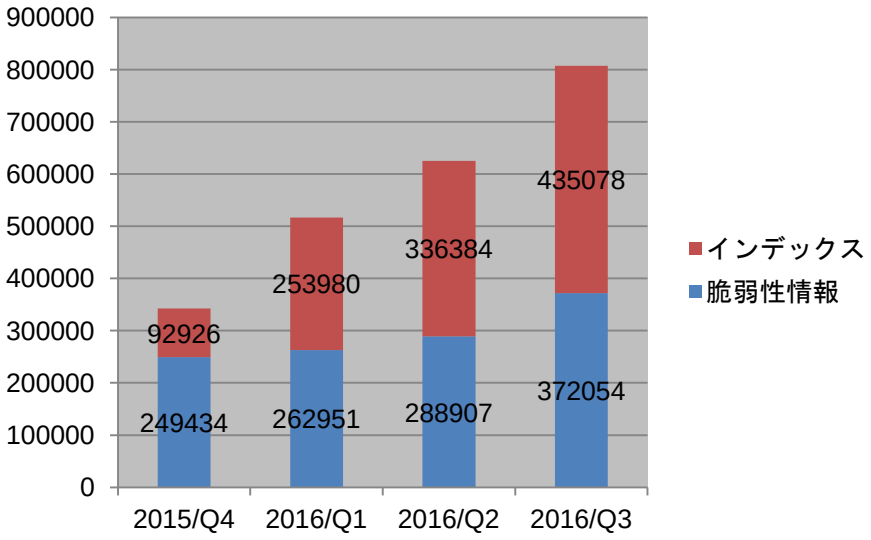
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページをご参照ください。

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 2-5］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。

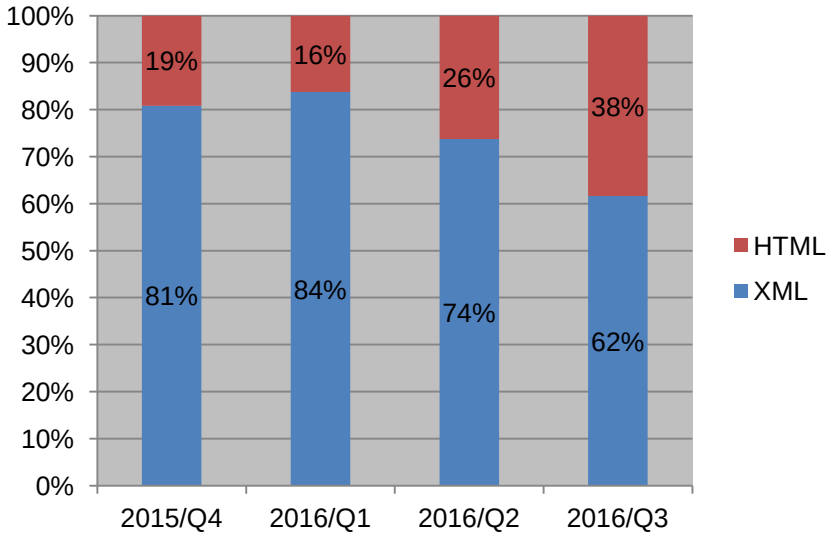


［図 2-5 VRDA フィード配信件数］



［図 2-6 VRDA フィード利用件数］

［図 2-6］に示したように、インデックスおよび脆弱性情報の利用数は、前四半期と比較し、それぞれ約 1.3 倍に増加しました。



［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、前四半期から引き続き HTML 形式の利用割合が増加しました。

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 426 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 5 件（うち、3 件が個社向けの情報提供）でした。

- 2016/07/11　【参考情報】 制御システムに対するランサムウエアの脅威について
- 2016/07/14　【参考情報】Cisco 社製セキュリティアプライアンスソフトウェアの脆弱性に関する注意喚起
- 2016/07/15　【参考情報】電力会社を狙うサイバー攻撃に国家の影(個社向け)
- 2016/08/16　【参考情報】キーレスエントリーシステムの脆弱性について(個社向け)
- 2016/09/30　【参考情報】American Auto-Matrix 社のビル管理用製品の脆弱性情報について(個社向け)

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

2016-07-08　制御システムセキュリティニュースレター 2016-0006
2016-08-10　制御システムセキュリティニュースレター 2016-0007
2016-09-03　制御システムセキュリティニュースレター 2016-0008

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 572 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。
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 6 件でした。そのうち 1 件は BASEC（ビルオートメーションシステム用のインターネット・ノード検索システム）で公開されている情報をもとに分析しました。

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 5 件、J-CLICS に関して 11 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 208 件、J-CLICS が 322 件となりました。

3.5 SICE Annual Conference 参加

JPCERT/CC では、制御システムにおける最近の脅威やセキュリティ対策の必要性を広く伝えるため、SICE（計測自動制御学会）に論文を投稿し、SICE Annual Conference において講演およびパネラーとしてパネルディスカッションに参加しました。
論文では、インターネットからアクセス可能な制御システムの存在とその危険性を取り上げ、近年汎用化が進む制御システムにおいて、適切なセキュリティ設定なしにインターネットからアクセス可能な機器があることを説明しました。さらにそれらの機器に迫る脅威と、脅威に対する JPCERT/CC の取り組みを紹介しました。聴衆からは、制御システムに関する脆弱性やインシデント報告数が増えているのはなぜか、サイバーインシデントの発生確率を数値化できると、ユーザにセキュリティ啓発をしやすい、といった質問やコメントがありました。
パネルディスカッションでは、インターネットからアクセス可能な制御システムを容易に検索できることや、具体的な脅威について述べ、セキュリティ対策の必要性をアピールしました。SHODAN 等のインターネット・ノード検索システムで接続された機器のベンダ名や型番が見えてしまっている実例に驚かれている制御システム関係者もいました。

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ベトナムへの専門家派遣（8 月 15 日 - 19 日）

JPCERT/CC はベトナムのセキュリティ関連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。VNCERT（ベトナムコンピュータ緊急対応チーム）および現地の大手アンチウィルスソフトウエアベンダ等を訪問し、ベトナムで流行しているマルウエアやインシデント状況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事業「平成 28 年度　技術協力活用型・新興国市場開拓事業」の一環として実施している「ASEAN 重要インフラ防護情報セキュリティ強化支援研修 ベトナム／ホーチミン、ハノイ海外研修」の 8 月 15 日、19 日の講義枠において、ベトナムを含めた 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組み等についての講義を行いました。直前にベトナム航空関連施設へのサイバー攻撃があったこともあり、サイバーへの関心が高まっており、ベトナムを中心に多数のセキュリティ関係者が参加されました。

［図 4-1　研修参加者との集合写真］

4.1.2. MNSEC 2016 への参加（9 月 28 日-9 月 29 日）

モンゴルの CSIRT 構築支援の一環として、MNCERT/CC（モンゴルサイバー緊急対応チームコーディネーションセンター）が 9 月 28 日から 29 日にウランバートルで開催した MNSEC 2016 に参加し、講演を行いました。JPCERT/CC の活動、日本における最新のインシデント動向や早期警戒の取組み、および攻撃の解析手法等について紹介しました。参加者は、モンゴル国内の政府関係者、民間企業、通信事業者、金融機関、学術系組織、および海外のセキュリティ関連組織等から約 200 名が集い、モンゴル国内におけるインシデント動向や課題に関して活発な意見交換を行いました。また、主催者の MNCERT/CC や National Data Center 等の関係組織との打合せを行い、今後も一層の連携強化を図ることを確認しました。

4.2 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 8 月 18 日、9 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。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 の理事を務めており、本四半期は組織運営に関わる議論に参画しました。FIRST および理事の詳細については、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. Bali 2016 FIRST Technical Colloquium への参加（9 月 29 日 - 30 日）

JPCERT/CC は、9 月 29 日から 30 日にインドネシアのバリで開催された FIRST Technical Colloquium（TC）に参加し、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等を行いました。Bali 2016 FIRST TC の詳細については、次の Web ページをご参照ください。

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. 第四回 日中韓 サイバーセキュリティインシデント対応年次会合（8 月 31 日 - 9 月 1 日）

日中韓の National CSIRT（JPCERT/CC、CNCERT/CC、KrCERT/CC）による「日中韓 サイバーセキュリティインシデント対応年次会合」が 8 月 31 日から 9 月 1 日に中国の昆明で開催されました。本会合は、2011 年 12 月に三者が締結した覚書（MOU）に基づき毎年開催されています。
本会合では、前会合以降の実績を振り返り、日中韓に影響を及ぼす重大なサイバーセキュリティインシデントにおいて、適切なインシデント対応が行われたことを確認しました。また、最近のインシデント動向や対応等に関する技術的な情報交換を行いました。今年は脆弱性ハンドリングについて各国の取り組みや、今後 5 年間の連携活動について協議し、サイバーセキュリティに関する課題解決のため、これまでに培った連携をさらに強化することで合意しました。

4.2.3.2. CODEBALI 2016 への参加（9 月 28 日）

Id-SIRTII/CC 主催で 9 月 28 日にインドネシアのバリ島で開催された CODEBALI 2016 に参加し、おもにインドネシアの学生や若い世代の参加者に向けて、インドネシアおよびアジア太平洋地域におけるインターネットセキュリティのますますの重要性について、日本のセキュリティ動向を交えて講演しました。CODEBALI 2016 についての詳細は、次の Web ページをご参照ください。

CODEBALI 2016
http://www.codebali.net/

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. ACID への参加（9 月 27 日）

JPCERT/CC は、シンガポールの National CSIRT である SingCERT が主導し、ASEAN（東南アジア諸国連合）各国の CSIRT が合同で実施したサイバーインシデント演習である ACID (ASEAN CERTs Incident Drill) に参加しました。本演習は、国境を越えて発生するサイバーセキュリティインシデントに備え、ASEAN 加盟国および周辺各国の CSIRT 間の連携の強化を目的に毎年実施されていて、今回が 11 回目になります。今年はランサムウエアの発生を想定した演習が行われました。

4.2.4. 海外 CSIRT 等の来訪および往訪

4.2.4.1. CERT Australia の来訪（8 月 3 日）

CERT Australia が来訪し、CERT Australia および JPCERT/CC の活動状況、オーストラリアのサイバーセキュリティ戦略や関連組織の体制等について情報共有を行いました。また、今後も脅威情報の共有を通して一層の連携強化を図ることを確認しました。

4.2.4.2. シンガポール CSA (Cyber Security Agency) の来訪（9 月 8 日）

SingCERT の母体組織である CSA が来訪し、CSA および JPCERT/CC の活動状況やシンガポール、日本における国内 CSIRT の体制等について情報共有を行いました。また、今後もサイバーグリーンプロジェクト等を通して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。

Japan Vulnerability Notes (JVN) Site Update (7 月 8 日)
http://blog.jpcert.or.jp/2016/07/japan-vulnerability-notes-jvn-site-update.html

Workshop and Training in Botswana (7 月 29 日)
http://blog.jpcert.or.jp/2016/07/workshop-and-training-in-botswana.html

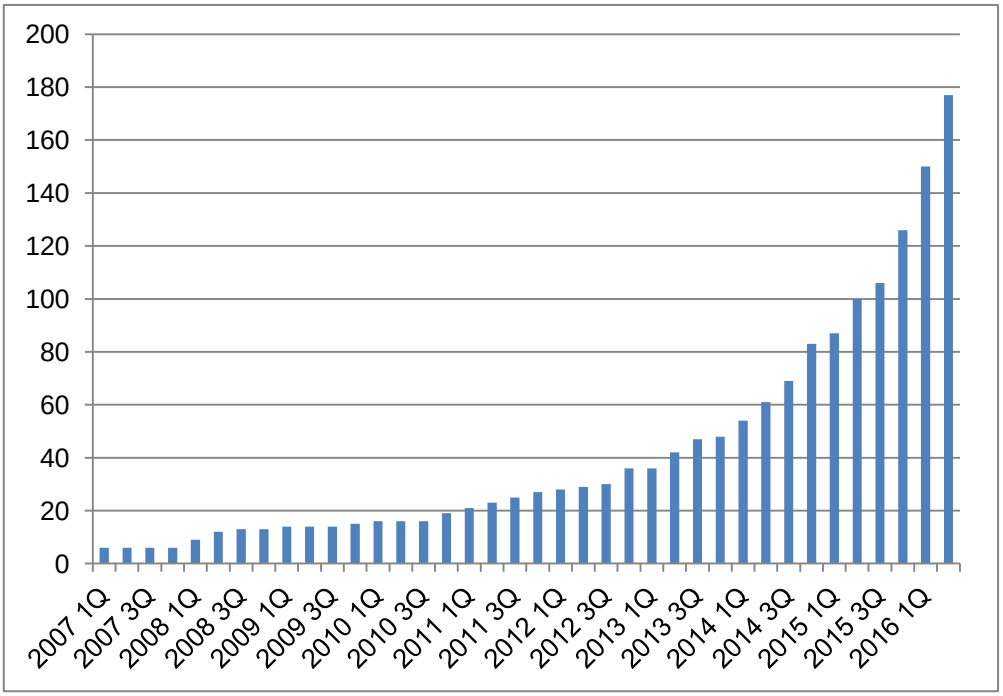
AppContainer’s Protecting Effects on Vulnerability-Exploited Web Browsers (8 月 29 日)
http://blog.jpcert.or.jp/2016/08/appcontainers-p-d296.html

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、イオンクレジットサービス株式会社（シーサート名称は ACS-CSIRT。他の会員についても同様にシーサート名称を括弧書き）、株式会社産業経済新聞社（SANKEI-CSIRT）、トランスコスモス株式会社（transcosmos-CSIRT）、ソネット株式会社（So-net SIRT）、

三菱 UFJ リース株式会社（MUL-CSIRT）、株式会社アテナ（ATENA-SIRT）、三菱自動車工業株式会社（MMC-CERT）、ソニー銀行株式会社（ソニー銀行 CSIRT）、日本郵便株式会社（JPPost CSIRT）、学校法人　東京電機大学（TDU-CSIRT）、株式会社かんぽ生命保険（JPLife CSIRT）、エヌシーアイ株式会社（NCI-SIRT)、株式会社　豊通シスコム（TSYS-CSIRT）、伊藤忠テクノソリューションズ株式会社（CTC-SIRT)、マクニカネットワークス株式会社（Macnica-CIRT）、日本郵政株式会社（JPHoldings CSIRT）、セコムトラストシステムズ株式会社（SECOM-CSIRT）、新日鉄住金ソリューションズ株式会社 （NSSOL-CSIRT）、第一フロンティア生命保険株式会社（DFL-CSIRT）、TIS 株式会社（TIS-CSIRT）、一般社団法人共同通信社（KYODO-CSIRT）、住友電気工業株式会社（SEI-CSIRT）、株式会社竹中工務店 （TAKENAKA-SIRT）、東京センチュリーリース株式会社（TC-CSIRT）、富士通エフ・アイ・ピー株式会社（FIP-CSIRT）、クックパッド株式会社（Cookpad CSIRT）、株式会社　証券保管振替機構（JASDEC-CSIRT）の 27 組織が新規に加盟しました。本四半期末時点で 177 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］

日本シーサート協議会 地区活動タスクフォース

近年、加盟に関する問合せが増加していること、加盟前から他組織のシーサートのメンバと顔を合わせ信頼関係を構築することが加盟後の情報収集に重要なことから、2016 年 2 月より、加盟希望組織向け説明会を開催しています。

日本シーサート協議会では、こうした既存組織と新規加盟組織および加盟予定組織がお互いに“顔の見えるシーサート”となることを目指し、そのための場を提供しています。

加盟希望組織向け説明会 開催概要（2016 年 2 月～7 月）

説明会で使った NCA の紹介資料につきましては、次の Web ページを参照してください。

http://www.nca.gr.jp/2016/ws-tokyo/index.html

第 1 回
日時：2016 年 2 月 2 日（火）15:30 - 17:30
場所：株式会社ディー・エヌ・エー（東京都渋谷区）
参加者数：約 30 名

第 2 回
日時：2016 年 3 月 1 日（火）5:30 - 17:30
場所：JPCERT/CC（東京都千代田区）
参加者数：約 20 名

第 3 回
日時：2016 年 5 月 17 日（火）13:00 - 15:00
場所：株式会社日立製作所（東京都品川区）
参加者数：約 20 名

第 4 回
日時：2016 年 7 月 6 日（水）14:00 - 16:00
場所：サイバーディフェンス研究所（東京都中央区）
参加者数：約 25 名

また、8 月 24 日（水）には、「第 11 回総会 & 第 14 回シーサートワーキンググループ会」を次の要領で開催し、運営規約の改定を行いました。また、運営委員の選挙を行い、6 名の立候補者から 5 名の運営委員を改選しました。
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、各ワーキンググループの開催報告や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 22 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 11 回総会 & 第 14 回シーサートワーキンググループ会
2016 年 8 月 24 日（水）10:00-17:30
会場：TDU-CSIRT（東京電機大学）
参加人数：250 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 12 件発信しました。

本四半期は、銀行をかたるフィッシングが頻繁に発生しており、以前は「こんにちは」から始まるフィッシングメールが、メール文中の日本語に違和感が少なくなったフィッシングメールが送られるようになりましたので、フィッシングサイトへ誘導されるユーザが多くなる可能性を危惧し、フィッシング対策協議会の緊急情報で注意を促しました。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、初めてのＶプリカ（Visa プリペイドカード）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 9 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 5 件、クレジットカード会社をかたるフィッシング関連が 1 件、その他が 3 件でした。それぞれの例として、［図 6-1］に福岡銀行をかたるフィッシング (2016/08/19)、［図 6-2］に V プリカ（Visa プリペイドカード）をかたるフィッシング (2016/07/21)、［図 6-3］に Amazon をかたるフィッシング (2016/09/13)の注意喚起を示します。

［図 6-1］福岡銀行をかたるフィッシング (2016/08/19)

https://www.antiphishing.jp/news/alert/fukuokabank_20160819.html

［図 6-2］V プリカ（Visa プリペイドカード）をかたるフィッシング（2016/07/21)

https://www.antiphishing.jp/news/alert/lifecard_20160721.html

［図 6-3］Amazon をかたるフィッシング (2016/09/13)
https://www.antiphishing.jp/news/alert/amazon_20160913.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 23 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
「フィッシング対策ガイドライン全体説明」
フィッシング対策ガイドライン実践セミナー 2016 , 2016 年 8 月 10 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 7 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201607.html
フィッシング対策協議会 2016 年 8 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201608.html
フィッシング対策協議会 2016 年 9 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201609.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 40 回運営委員会
日時：2016 年 7 月 15 日 16:00 - 18:00
場所：GMO グローバルサイン株式会社

フィッシング対策協議会 第 41 回運営委員会
日時：2016 年 8 月 19 日 10:00 - 12:00
場所：ソースネクスト株式会社

フィッシング対策協議会 第 42 回運営委員会
日時：2016 年 9 月 9 日 16:00 - 18:00
場所：NTT コミュニケーションズ株式会社

7.2 フィッシング対策ガイドライン実践セミナー 2016 開催

フィッシング対策ガイドライン実践セミナー 2016 を次のとおり開催しました。

フィッシング対策ガイドライン実践セミナー 2016
日時：2016 年 8 月 10 日 14:00 - 17:00
場所：日立システムズ　ソリューションスクエア東京
東京都品川区大崎 1-2-1 大崎フロントタワー

7.3 ガイドラインの改訂版を公開

警察庁の発表によれば平成 27 年にはフィッシング詐欺の被害額が 30 億円を超えました。被害の抑制のための対策を利用者に呼びかけるため、フィッシング対策協議会では、利用者向け啓発教材として「利用者向けフィッシング詐欺対策ガイドライン」 およびインターネットバンキング利用者の情報を盗み取り、利用者の口座から不正に送金する被害が急増していることを受けて「インターネットバンキングの不正送金被害にあわないためのガイドライン」作成しています。これらのガイドラインについて、事例内容などを追記・変更しました。

改訂したガイドラインは以下の 2 つです。

インターネットバンキングの不正送金被害にあわないためのガイドライン
https://www.antiphishing.jp/report/pdf/internetbanking_guideline.pdf

利用者向けフィッシング詐欺対策ガイドライン
http://www.antiphishing.jp/report/pdf/consumer_antiphishing_guideline.pdf

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 2 四半期（4 月～6 月）］（2016 年 7 月 21 日）
https://www.jpcert.or.jp/press/2016/vulnREPORT_2016q2.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 4 月～6 月（2016 年 8 月 25 日）
https://www.jpcert.or.jp/tsubame/report/report201604-06.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2016Q1.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 2 件の記事を公開しました。

(1) 脆弱性を攻撃された Web ブラウザにおける AppContainer の防御効果(2016-07-20)

Web ブラウザの脆弱性を悪用してマルウエアに感染させようとする攻撃は度々確認されています。このような攻撃に対する防御に活用できる仕組みとして、Windows 8 から導入されたサンドボックス「AppContainer」があります。この AppContainer が実際の攻撃に対してどのような効果を発揮するのかを検証しました。

脆弱性を攻撃された Web ブラウザにおける AppContainer の防御効果(2016-07-20)
https://www.jpcert.or.jp/magazine/acreport-AppContainer.html

(2) Windows の新セキュリティ機能を検証する:LSA の保護モードと Credential Guard(2016-09-07)

ほとんどの標的型攻撃では、マルウエアに感染して侵入される端末は 1 台にとどまらず、横断的に他の端末そして重要なサーバも侵入されていきます。その準備として行われる情報窃取への防御を強化

するための機能として、Windows 8.1 等では LSA の保護モードが、Windows 10 Enterprise では Credential Guard が導入されました。これら新機能の効果を検証するとともに、その効果を損なわないために注意すべき点について解説しました。

Windows の新セキュリティ機能を検証する:LSA の保護モードと Credential Guard(2016-09-07)
https://www.jpcert.or.jp/magazine/acreport-lsa_protect.html

9. 主な講演活動

(1) 真鍋 敬士(理事・最高技術責任者) ：
「インシデントに備えた体制作りと CSIRT の役割」
FireEye Cyber Defense LIVE Tokyo 2016,2016 年 07 月 12 日

(2) 竹田 春樹(分析センター　マネージャー) ：
「サイバー攻撃の最新動向～対応のための備えについて～」
ネクストセキュリティ 重要インフラ情報セキュリティ対策セミナー, 2016 年 07 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　兼 早期警戒グループ担当部門長）：
「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・アイ標的型攻撃対策セミナー（名古屋）,2016 年 07 月 22 日

(4) 洞田 慎一(早期警戒グループ マネージャー)：
「高度サイバー攻撃への備えと対応」
核融合科学研究所 情報セキュリティ講習会, 2016 年 07 月 22 日

(5) 朝長 秀誠（分析センター リーダー）：
「JPCERT/CC とサイバー攻撃対応」
警察大学校　職員研修, 2016 年 07 月 26 日

(6) 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について」
MKI Internet Technical day 2016, 2016 年 08 月 02 日

(7) 鹿野 恵祐(早期警戒グループ　リーダー)：
「つながった機器」と「インシデント」
サイエンティフィック・システム研究会システム技術分科会, 2016 年 08 月 23 日

(8) 竹田 春樹(分析センター　マネージャー) ：
「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・アイ標的型攻撃対策セミナー（東京）,2016 年 09 月 02 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について」
日経 BP 情報セキュリティ戦略セミナー,2016 年 09 月 15 日

10. 主な執筆活動

(1) 佐藤 祐輔（エンタープライズサポートグループ リーダー）：
「高度サイバー攻撃（APT）への備えと対応ガイド」の紹介と利活用のポイント
一般社団法人行政情報システム研究所「行政&情報システム」8 月号,2016 年 08 月 10 日

(2) 佐藤 祐輔（エンタープライズサポートグループ リーダー）：
公開資料「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」の概要
計装・8 月号,2016 年 08 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) RSA Conference Asia Pacific & Japan 2016
主　催：RSA Security LLC
開催日：2016年07月20日～22日

(2) JAIPA Cloud Conference2016
主　催：一般社団法人 日本インターネットプロバイダー協会 クラウド部会
開催日：2016年07月20日

(3) 第6回 日韓情報セキュリティシンポジウム会
主　催：特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)、韓国知識情報保安産業協(KISIA)
開催日：2016年07月28日

(4) 第12回IPAひろげよう情報モラル・セキュリティコンクール2016
主　催：独立行政法人情報処理推進機構(IPA)
開催日：2016年04月01日～11月30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