Japan Computer Emergency Response Team Coordination Center

電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2017.04.13 10:01:01 +09'00'

JPCERT-PR-2017-01
発行日：2017-4-13

JPCERT/CC 活動概要 [2017 年 1 月 1 日 ～ 2017 年 3 月 31 日]

活動概要トピックス

ートピック1ー　Active Directory のセキュリティにフォーカスした実践的解説書を公開

JPCERT/CC は、高度サイバー攻撃において特に Active Directory（以下「AD」）が狙われている背景を踏まえ、AD のセキュリティに特化した「ログを活用した Active Directory に対する攻撃の検知と対策」を、2017 年 3 月 14 日に公開しました。

標的型攻撃等の高度サイバー攻撃は、国内においても、多数の事案が発生し、深刻なセキュリティ脅威となっています。AD が侵害されたことを契機に、AD のドメイン管理者アカウントが悪用され、他のサーバやコンピュータへ感染被害が拡大した事例を JPCERT/CC では多数確認しています。さらに、JPCERT/CC が報告を受けた事例を分析すると、AD の脆弱性への対応が遅れたために侵害を受けたケースや、ログが適切に保存されていないために被害状況の調査が困難なケースがありました。これらは、攻撃から AD を防御、あるいは防御を破られたことを迅速に検知して調査することによって、高度サイバー攻撃の被害を局所化するために、多くの組織で AD のログ確認や運用の改善が求められていることを示しています。

本文書は、JPCERT/CC がこれまで数多くの高度サイバー攻撃の対応支援を通して得た知見に基づき、AD への代表的な攻撃手法と検知および対策方法をセットにした実践的解説書としてまとめています。また、必要な箇所だけを拾い読みできるように構成を工夫していますので、緊急時対応時など通読する時間がとりづらい場合を含め、システム運用やインシデント対応の現場でも是非ご活用ください。

ログを活用した Active Directory に対する攻撃の検知と対策
https://www.jpcert.or.jp/research/AD.html

ートピック2ー　マルウエアの類似度によるクラスタリング結果を可視化するためのツールを公開

JPCERT/CC では、マルウエアの類似度に基いて複数のマルウエアをクラスタリングし、結果を可視化するためのツール「impfuzzy for Neo4j」を 2017 年 3 月 10 日に公開しました。

近年では部分的な改変などにより大量のマルウエアが作成されていることから、その改変の度合いを把握し、分析すべきマルウエアや新種のマルウエアを抽出することがマルウエア分析において重要な作業となっています。

今回公開した「impfuzzy for Neo4j」は、このマルウエア分析に関連した活動をサポートする目的で作成したツールです。組織のインシデント対応に関連するマルウエア分析や、マルウエア分析に関連した調査・研究等に幅広く活用していただくことを期待しています。

「impfuzzy for Neo4j」は、マルウエアの類似度の計算に impfuzzy という手法を使用し、その結果からマルウエア間のグラフ（ネットワーク）を作成します。さらに作成したグラフをネットワーク分析という手法を用いてクラスタリングし、結果を可視化します。可視化にはグラフデータベースである Neo4j を使用しています。

マルウエアの類似度の計算に使用している impfuzzy は、JPCERT/CC が独自に提案している実行ファイルのハッシュ値を計算する手法で、実行ファイルの Import API に基づいて fuzzy hash と呼ばれる値を計算します。impfuzzy は従来の手法と比較して、実行ファイル形式のマルウエアの分類により適した手法です。

JPCERT/CC では、impfuzzy を実装したツールとして、既に impfuzzy を計算および比較するための python モジュール「pyimpfuzzy」や、impfuzzy を使用してメモリイメージから類似のファイルを調査することが可能な「impfuzzy for volatility」を公開しています。それらのツール加え、今回の「impfuzzy for Neo4j」を利用することで、マルウエアのハッシュ値の計算から類似度の比較および可視化までの一連のマルウエア分析業務のそれぞれで impfuzzy を活用していただくことが可能となりました。

なお、今回公開した「impfuzzy for Neo4j」を含む impfuzzy 関連のツールの公開は、ソフトウエア開発プロジェクトのための共有ウェブサービスの GitHub で行っています。

impfuzzy とネットワーク分析を用いたマルウエアのクラスタリング ~impfuzzy for Neo4j~(2017-03-10)
https://www.jpcert.or.jp/magazine/acreport-impfuzzy_neo4.html

JPCERTCC/aa-tools GitHub - impfuzzy
https://github.com/JPCERTCC/aa-tools/tree/master/impfuzzy/

ートピック3ー　制御システムセキュリティカンファレンス 2017 を開催

2 月 21 日に制御システムセキュリティカンファレンス 2017 を「将来のインシデントに備えて」をテーマに東京で開催しました。

約 270 名の方にご来場いただき、その内訳は、アセットオーナが 32%、制御システムの機器ベンダが 25%、システムベンダが 16%、エンジニアリング会社が 11%、研究者が 7%でした。本カンファレンスの初回と比べると、8 年前は制御システムのベンダの限られた方々の関心にとどまっていましたが、その後、アセットオーナを中心に参加者数が約 4 倍に増えるなど、制御システムのセキュリティ強化に向けた業界内の力強い潮流が感じられます。

また、今回は初の試みとして、一部の講演を公募により選定してプログラムを構成しましたが、さまざまな立場の関係者の方から発表のご提案をいただくことができました。

制御システムセキュリティカンファレンス 2017（プログラム）
https://www.jpcert.or.jp/event/ics-conference2017.html

制御システムセキュリティカンファレンス 2017（講演資料）
https://www.jpcert.or.jp/present/#year2017

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」）に関する報告は、報告件数ベースで 4095 件、インシデント件数ベースでは 4856 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 3077 件でした。前四半期の 2883 件と比較して 7%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/2017/IR_Report20170413.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 707 件で、前四半期の 521 件から 36%増加しました。また、前年度同期（645 件）との比較では、10%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	本四半期合計（割合）
国内ブランド	56	42	85	183(26%)
国外ブランド	111	161	152	424(64%)
ブランド不明 (注 5)	24	43	33	100(14%)
全ブランド合計	191	246	270	707(100%)

（注 2）「ブランド不明」は、報告されたフィッシングサイトが停止していた等の理由により、JPCERT/CC がブランドを確認することができなかったサイトの件数を示します。

国内ブランドのフィッシングサイトでは、国内通信事業者の Web メールのログイン画面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。これらのフィッシングサイトの大半は、海外の IP アドレスで稼働しており、侵入されたとみられる海外の Web サイトや、海外のホスティングサービス上に作成されていました。特に、ロシアの特定のホスティングサービスが継続して使用されていました。

1 月以降、日本マイクロソフトを装ったフィッシングメールが継続して確認されています。フィッシングメールの内容は、オフィスソフトのプロダクトキーが不正にコピーされているため検証作業を行う必要があるとして、メール内のリンクから認証を行うよう誘導するものでした。リンクの誘導先は、Microsoft アカウントの情報を窃取するフィッシングサイトで、ホスト名には共通して support、security、microsoft などの文字列が含まれていました。

フィッシングサイトの調整先の割合は、国内が 27%、国外が 73%であり、前四半期（国内 38%、国外 62%）に比べ、国内で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、967 件でした。前四半期の 688 件から 41%増加しています。

アクセスするとフォントのアップデートを促すポップアップが表示されるように改ざんされたとみられる Web サイトに関する報告が 1 月ごろから複数寄せられています。ポップアップ上のボタンを押すと EXE ファイルがダウンロードされ、EXE ファイルを実行するとランサムウエアに感染することを確認しています。ポップアップを表示する不正なスクリプトは、アクセス元のリファラ、ユーザエージェントが特定のものであり、且つアクセス元 IP アドレスからの初回のアクセス時にのみ、ページに埋め込まれるようになっていました。

2 月初めごろ、WordPress の REST API の脆弱性を悪用した攻撃が大規模に行われ、攻撃によって改ざんされたと見られる国内サイトが非常に多く確認されました。改ざんの内容は、海外のハッカーグループが

ページ上にメッセージを埋め込むものでした。

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、11 件でした。前四半期の 15 件から 27%減少しています。本四半期は、対応を依頼した組織はありませんでした。

2 月から 3 月にかけて、標的型攻撃と見られるなりすましメールに関する報告が複数寄せられています。確認したメールには、ZIP ファイルが添付されているか、ZIP ファイルをダウンロードするリンクが存在し、いずれの場合も ZIP ファイルには拡張子が.lnk のショートカットファイルが含まれていました。このショートカットファイルが開かれると、PowerShell コマンドで追加のファイルがダウンロード、実行される仕組みになっていました。ダウンロードされるファイルは攻撃によって異なり、PowerShell スクリプトや EXE ファイルなどが見られました。

PowerShell スクリプトがダウンロードされる事例では、.lnk ファイルを実行すると、最初に短縮 URL へのアクセスが行われ、リダイレクト先から画像ファイルに偽装した PowerShell スクリプトがダウンロードされるようになっていました。ダウンロードされた PowerShell スクリプトを実行すると、ダミーの文書が表示される裏でマルウエアが実行され、ChChes と呼ばれる、HTTP で C&C サーバと通信を行うマルウエア（HTTP ボット）に感染することを確認しました。同様の攻撃に関与した複数の C&C サーバが確認されており、さまざまなドメイン名が使われていましたが、それらのドメインの登録情報には類似性が見られました。

ショートカットファイルが添付される標的型攻撃メールは、以前から継続して確認されていますが、ショートカットファイルを実行することでダウンロードされるファイルや感染するマルウエアの種類は、時期によって違いが見られます。2015 年 11 月から 2016 年 6 月にかけて確認された標的型攻撃メールでは、添付ファイルに含まれる.lnk ファイルを実行すると、マルウエア（ダウンローダ）に感染し、このマルウエアが画像に見せかけたファイルをダウンロードした後にデコードし実行することで、Asruex と呼ばれる HTTP ボットに感染させる仕組みになっていました。

マルウエア ChChes と PowerShell を悪用して感染を広げる事例の詳細については、下記をご参照ください。

Cookie ヘッダーを用いて C&C サーバとやりとりするマルウエア ChChes(2017-01-26)
https://www.jpcert.or.jp/magazine/acreport-ChChes.html

PowerSploit を悪用して感染するマルウエア(2017-02-10)
https://www.jpcert.or.jp/magazine/acreport-ChChes_ps1.html

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、国内の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、併せて脆弱性やウイルス検体の検証等も必要に応じて行っています。さらに、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 33,000 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

2017-02-13　jpcert.or.jp に類似するドメインに関するお知らせ
2017-03-14　研究・調査レポート「ログを活用した Active Directory に対する攻撃の検知と対策」を公開

1.2.1.2. 注意喚起

深刻かつ影響範囲の広い脆弱性等について、次のような注意喚起情報を発行しました。

発行件数：17 件（うち 5 件更新） https://www.jpcert.or.jp/at/

2017-01-11 Adobe Reader および Acrobat の脆弱性 (APSB17-01) に関する注意喚起 (公開)
2017-01-11 Adobe Flash Player の脆弱性 (APSB17-02) に関する注意喚起 (公開)
2017-01-11 2017 年 1 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起 (公開)
2017-01-12 ISC BIND 9 に対する複数の脆弱性に関する注意喚起 (公開)
2017-01-13 ISC BIND 9 に対する複数の脆弱性に関する注意喚起 (更新)
2017-01-18 2017 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)
2017-02-06 WordPress の脆弱性に関する注意喚起 (公開)
2017-02-09 ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2017-3135) に関する注意喚起 (公開)
2017-02-15 Adobe Flash Player の脆弱性 (APSB17-04) に関する注意喚起 (公開)
2017-02-22 Adobe Flash Player の脆弱性 (APSB17-04) に関する注意喚起 (更新)
2017-03-08 SKYSEA Client View の脆弱性 (CVE-2016-7836) に関する注意喚起 (更新)
2017-03-09 Apache Struts 2 の脆弱性 (S2-045) に関する注意喚起 (公開)
2017-03-15 Adobe Flash Player の脆弱性 (APSB17-07) に関する注意喚起 (公開)
2017-03-15 2017 年 3 月 Microsoft セキュリティ情報 (緊急 9 件含) に関する注意喚起 (公開)
2017-03-17 Apache Struts 2 の脆弱性 (S2-045) に関する注意喚起 (更新)
2017-03-21 Apache Struts 2 の脆弱性 (S2-045) に関する注意喚起 (更新)
2017-03-30 USB ストレージに保存されたデータを窃取するサイバー攻撃に関する注意喚起 (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：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。

2017-01-12 担当者が選ぶ 2016 年重大ニュース
2017-01-18 Windows Vista のサポート期間について
2017-01-25 「Mirai」またはその亜種のボットによるものと見られるアクセスの急増
2017-02-01 サイバーセキュリティ月間
2017-02-08 IPA が「情報セキュリティ 10 大脅威 2017」の順位を発表

2017-02-15　JNSA が「中小企業の情報セキュリティ対策ガイドライン」に対応する製品・サービス検索ページを公開
2017-02-22　警察庁が「情報セキュリティ対策ビデオ」を公開
2017-03-01　JIPDEC が「JIPDEC 経営読本 情報管理はマネーです」を公開
2017-03-08　CRYPTREC が「SHA-1 の安全性低下について」を公開
2017-03-15　JIPDEC が中小企業の改正個人情報保護法への対応状況についてのアンケート結果を公開
2017-03-23　US-CERT が「HTTPS Interception Weakens TLS Security」公開
2017-03-29　警察庁が「平成 28 年におけるサイバー空間の脅威の情勢等について」を公開

1.2.1.4. 早期警戒情報

JPCERT/CC では、国民の生活や社会経済活動を支えるインフラ、サービスおよびプロダクト等を提供している組織の情報セキュリティ関連部署もしくは組織内 CSIRT に向けて、セキュリティ上の深刻な影響をもたらす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。

【Active Directory のセキュリティに特化した実践的解説書の公開】
JPCERT/CC は、運用やインシデント対応の現場で活用されることを目的として、Active Directory（以下「AD」）への攻撃を効果的に検知するためのログの確認ポイントや、AD に対する代表的な攻撃手法とその予防策、攻撃抑止や被害軽減のための緊急対処法などをまとめた実践的解説書「ログを活用した Active Directory に対する攻撃の検知と対策」を公開しました。
JPCERT/CC では、高度サイバー攻撃の対応支援を実施した被害組織の多くで AD 環境が侵害され、ドメイン管理者アカウントが悪用されていることを確認しています。それらの組織の一部は、AD の脆弱性が放置されていたり、ログが十分な期間保存されていなかったりしたケースもあり、脅威が高まっているにも関わらず、AD のセキュリティ対策やログ確認の重要性が認識されていない傾向にあります。
また、AD の攻撃の対策や検知についてさまざまなドキュメントが公開されていますが、代表的な攻撃手法と検知および対策方法をセットにして整理した日本語のドキュメントは見られないため、運用現場で活用することを目的とした、より実践的なドキュメントが必要と考え、本書をまとめました。
本書では、これまで数多くの高度サイバー攻撃の対応支援を通して得た知見に加えて、近年確認されている新しい攻撃手法についての検証結果などを踏まえ、確認事項や対策の優先度を設定し、状況に応じてやるべき内容を明示しています。また、複数の国内組織を対象にアンケートを実施し、AD のログの保管や運用状況などを調査しました。その結果、多くの組織が AD のログを取得しているものの、ログ分析のノウハウや人的リソースが不足しているなどの理由で、取得したログを確認できていないなどの実態も明ら

かになりました。本書にはこれらの実態調査による数値的根拠も示しています。

ログを活用した Active Directory に対する攻撃の検知と対策
https://www.jpcert.or.jp/research/AD.html

【WordPress REST API の脆弱性に関する情報発信】
WordPress の REST API の脆弱性を狙った攻撃に関する注意喚起を 2017 年 2 月 6 日に公開しました。JPCERT/CC にて本脆弱性に関する実証コードの検証を行った結果、この脆弱性を悪用することで、遠隔の第三者が認証を受けずに WordPress の Web コンテンツを改ざんできることを確認しました。攻撃の実証コードが複数の Web サイトに公開され容易に実行できる状態にあったこともあり、本脆弱性を悪用した攻撃が発生し、社会的な問題として大きく取り上げられました。JPCERT/CC でも多数の改ざん報告を受けており、注意喚起として早期の対策を呼びかけました。

【Apache Struts 2 の脆弱性に関する情報発信】
Apache Struts 2 の脆弱性を狙った攻撃に関する注意喚起を 2017 年 3 月 9 日に公開しました。この脆弱性は、Apache Struts 2 に標準で組み込まれているパーサである Jakarta Multipart parser や、JakartaStreamMultiPartRequest 等におけるエラーメッセージの処理に起因します。
Apache Struts 2 を使用するアプリケーション（Struts アプリケーション）に対して、この脆弱性を悪用すべく細工した HTTP リクエストを送信されると、Struts アプリケーションを実行しているサーバにおいて任意のコードを遠隔の第三者に実行される可能性があります。3 月 9 日に Apache Struts 2 のアップデートバージョンが公開されたことを受け、一般に広く呼びかけるために注意喚起を公開しました。
JPCERT/CC では、本脆弱性を悪用した攻撃の報告が多数寄せられているほか、Jakarta Multipart parser の代替として挙げられていた JakartaStreamMultiPartRequest についても、本脆弱性の影響を受け、攻撃が可能であることを確認したため、3 月 17 日に注意喚起を更新しました。その後、3 月 21 日に Jakarta Multipart parser と JakartaStreamMultiPartRequest の修正用プラグインが公式にリリースされたため、再度、注意喚起を更新し対策を呼びかけました。

1.3. インターネット定点観測

JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを収集する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把握に努めています。

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。2017 年 3 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、海外諸国のナショナル CSIRT 等に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

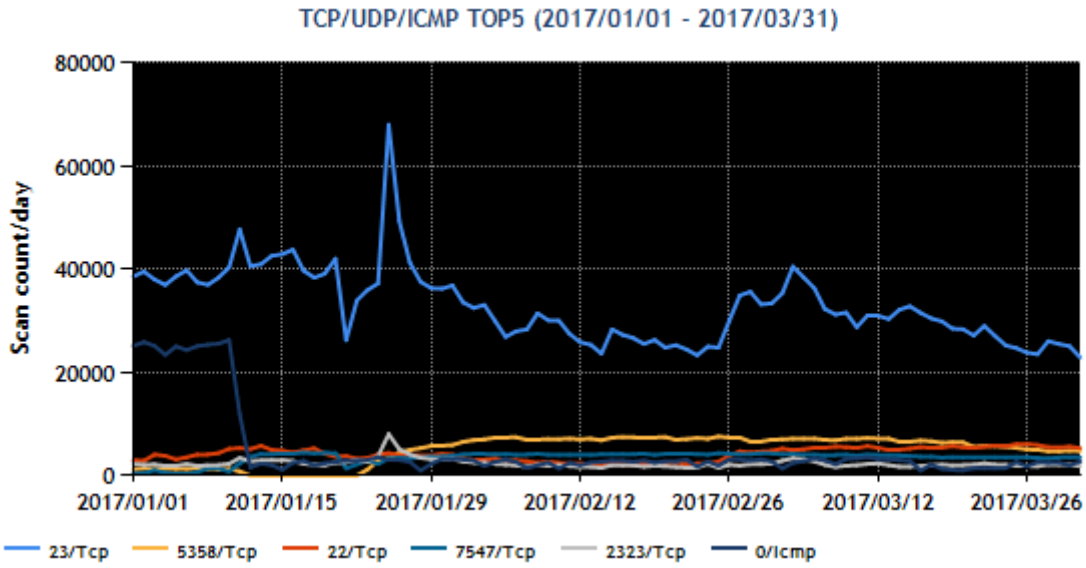
JPCERT/CC は、TSUBAME で収集したデータを宛先ポート番号や送信元地域ごとに分類して統計分析し、既知の脆弱性情報やマルウエア、攻撃ツール等との関連を考察することで、攻撃活動や準備活動の捕捉に努めています。

主に日本企業のシステム管理者等の方々に、自組織の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 10 月から 12 月分のレポートを 2017 年 2 月 9 日に公開しました。

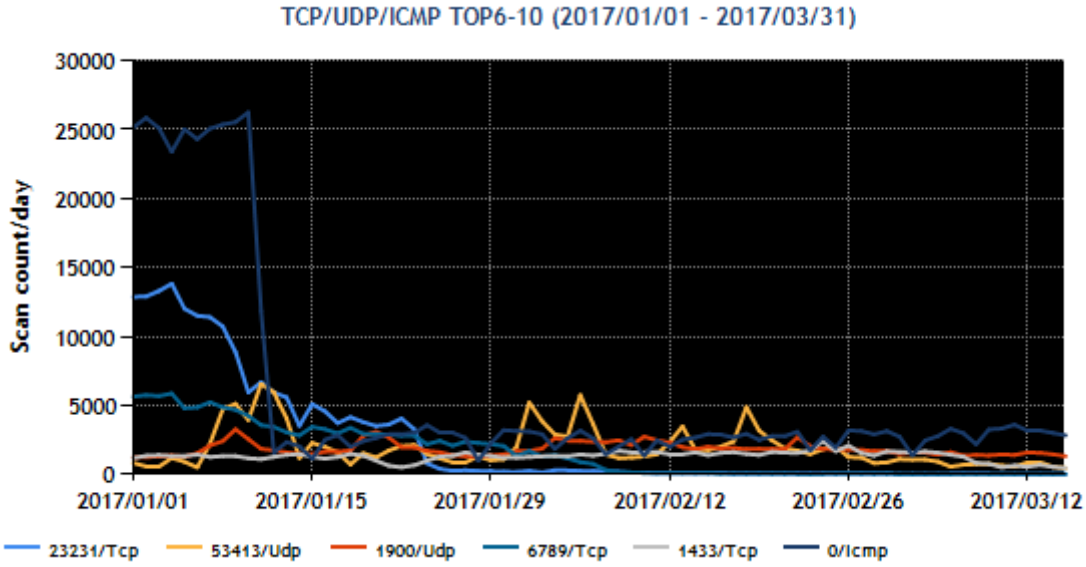
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート（2016 年 10～12 月）
https://www.jpcert.or.jp/tsubame/report/report201610-12.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 1～5 位および 6～10 位を、［図 1-1］と［図 1-2］に示します。

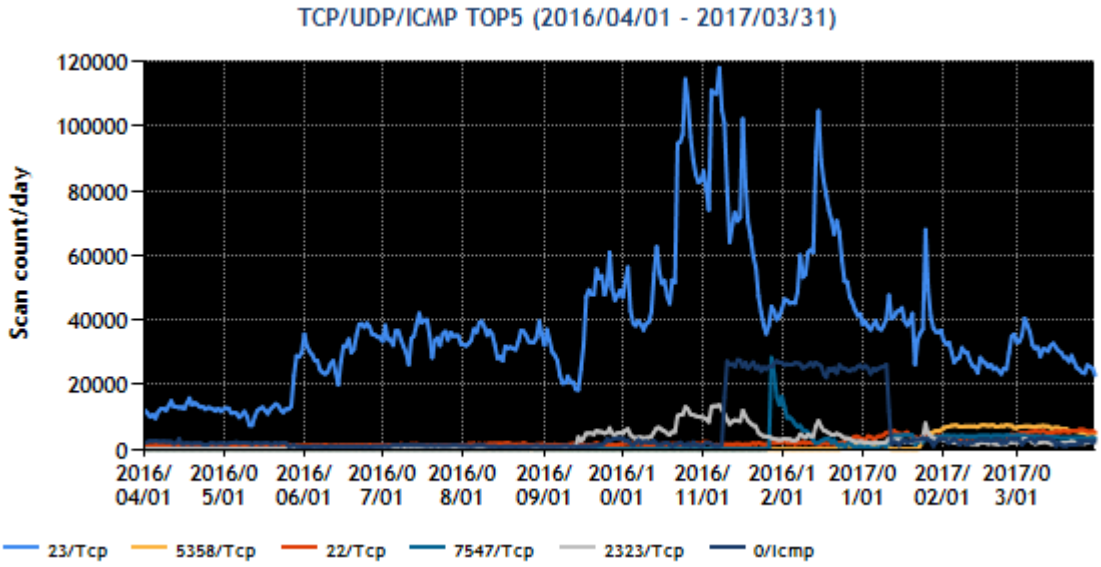


［図 1-1 宛先ポート別グラフ トップ 1-5（2017 年 1 月 1 日-3 月 31 日）］

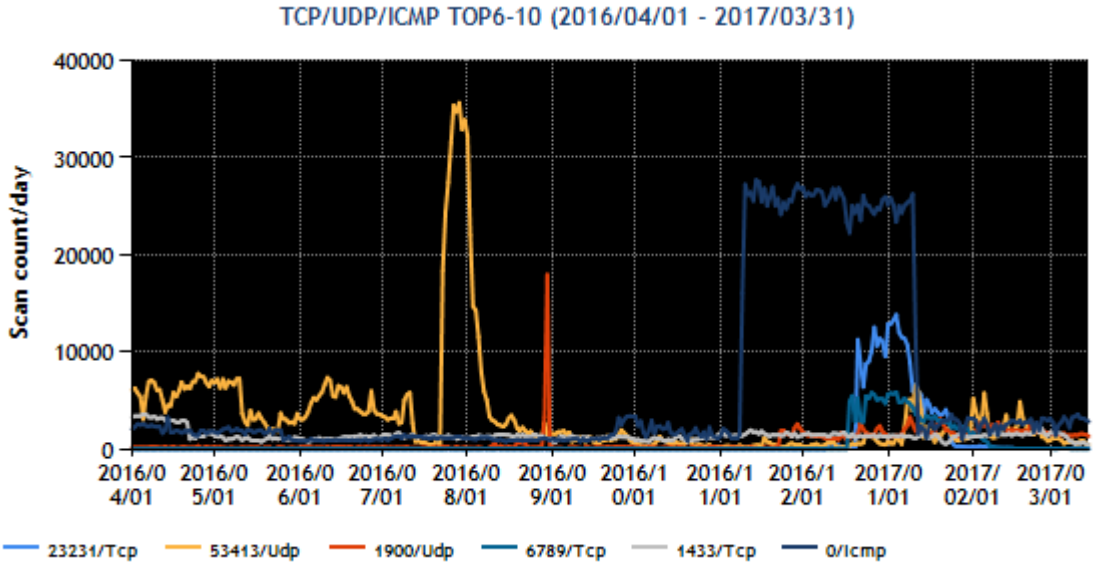


［図 1-2 宛先ポート別グラフ トップ 6-10（2017 年 1 月 1 日-3 月 31 日)］

また、過去 1 年間（2016 年 4 月 1 日-2017 年 3 月 31 日）における、宛先ポート別パケット数の上位 1～5 位および 6～10 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（2016 年 4 月 1 日-2017 年 3 月 31 日)］



［図 1-4 宛先ポート別グラフ トップ 6-10（2016 年 4 月 1 日-2017 年 3 月 31 日）］

本四半期は、23/TCP、5358/TCP 宛のパケットが多く観測されました。監視カメラやルータ NAS など専用機器を対象としたマルウエア（Mirai 等）の活動がこれまでも活発でしたが、前四半期から少しずつ対象とする機器や攻撃手法が変化してきています。パケットの送信元を調査したところ、専用機器が送信元となっている事例が含まれていました。Mirai 等のマルウエアの挙動の変化により、感染する機器の種類が拡大し、それらの機器から大量の探索パケットが送信されたのではないかと考えられます。その他、遠隔操作のための SSH サーバ等のサービスをスキャンする活動と見られるパケットも、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) 国内外の機器を主な対象とした探索活動についての対応
複数の日本国内外の IP アドレスを送信元とする、23/TCP、2323/TCP、5358/TCP, 7547/TCP,23231/TCP 等のポート宛てのパケットが前四半期に引き続き多数観測されました。これらの Port に対するパケットは、Mirai 等のマルウエアの感染と関連していると考えられます。当該マルウエアに感染した場合、さらなる拡大を目的として、前述した Port に対して探索パケットが送信されます。送信元 IP アドレスを調査したところ、マルウエアに感染した複数のベンダの機器が見つかりました。その中には、これまで感染例を確認していなかった新たな機器も含まれており、マルウエア感染が拡大している可能性が示唆されます。JPCERT/CC では、マルウエア感染が拡大しないよう、国内外にわたる機器の製造ベンダと送信元 IP アドレスの管理者に対し情報を提供して適切な対処を求めました。

(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
本四半期では、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

数観測されました。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、DNS 権威サーバに過剰な負荷をかけることを目的とした DDoS 攻撃の余波と推測されます。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 エラーパケットについて、国内の送信元 IP アドレスの管理者に対して調査を依頼したところ、「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」等の回答を得ています。

1.3.3. TSUBAME トレーニングの実施

本四半期は、香港の CSIRT（GovCERT-HK, HKCERT）向けに、次の要領で TSUBAME トレーニングを実施しました。

日時：2017 年 2 月 24 日（金）
場所：中華人民共和国香港特別行政区
参加人数：27 名（GovCERT-HK, HKCERT のメンバが参加）
トレーニングの内容：
- TSUBAME プロジェクトの概要
- 機器や機器を対象とした探索活動の現状
- 演習
- 意見交換

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「ソフトウエア製品等の脆弱性関連情報に関する取扱規程（平成 29 年経済産業省告示第 19 号。以下「本規程」）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。本規程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、本規程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」）に従って、対象となる脆弱性に関係する製品開発者の特定、脆弱性関連情報の適切な窓口への連絡、開発者による脆弱性の検証等の対応や脆弱性情報の公表スケジュール等に関する調整を行い、原則として、調整した公表日に JVN を通じて脆弱性情報等を一般に公表しています。JPCERT/CC は、脆弱性情報の分析結果や脆弱性情報の取り扱い状況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。

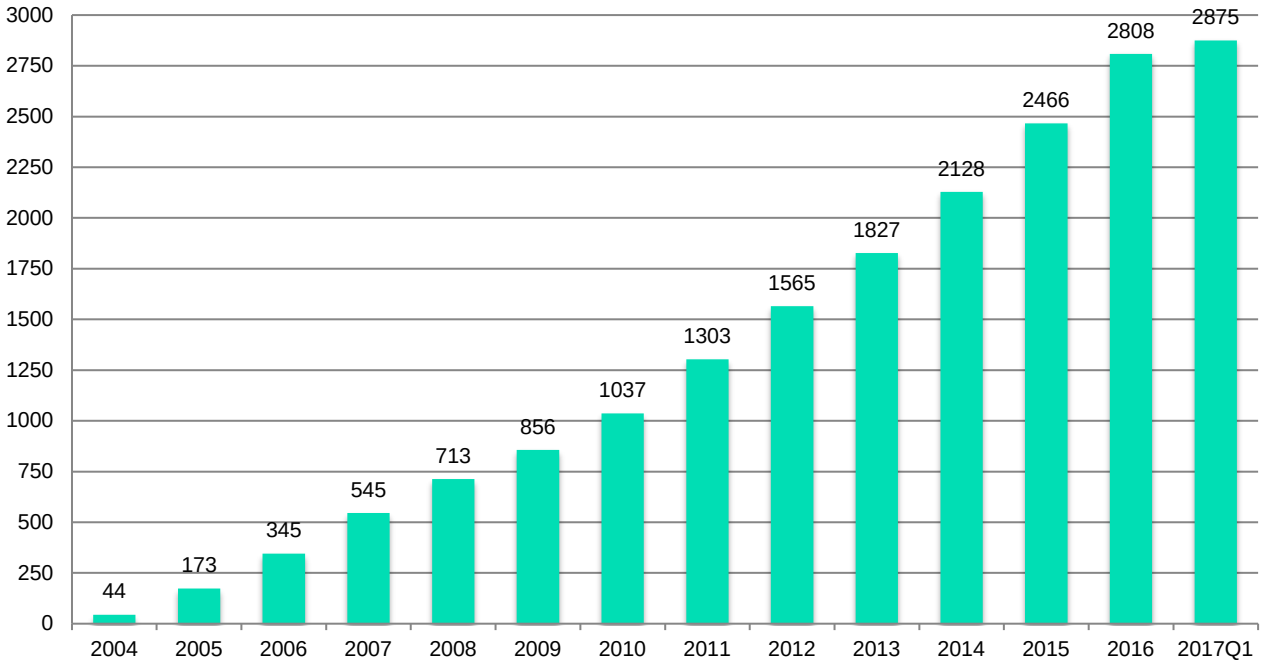
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

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、本規程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、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」）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や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 67 件（累計 2,875 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/



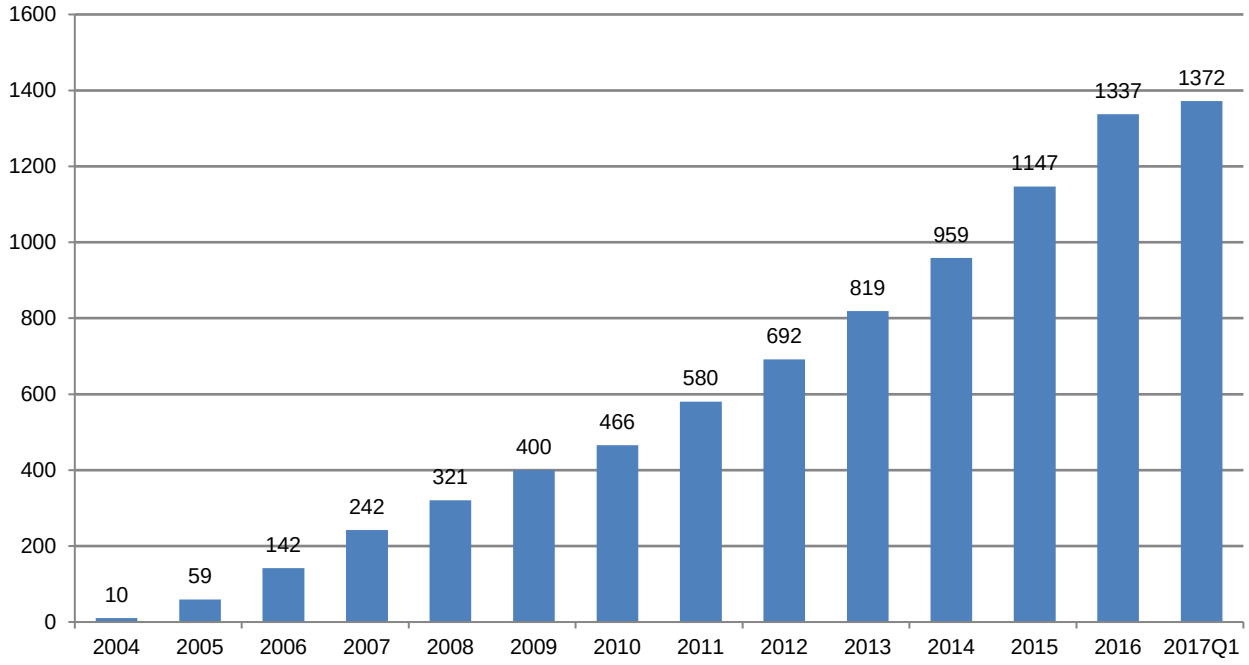
［図 2-1　JVN 公表累積件数］

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 35 件（累計 1,372 件）で、累計の推移は［図 2-2］に示すとおりです。35 件のうち、27 件が国内製品開発者の製品、7 件が海外の製品開発者の製品、1 件が国内外の複数の製品開発者の製品に関連したものでした。また、27 件の国内製品開発者の製品のうち、3 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、Windows アプリケーション、CMS、ウェブアプリケーション、モバイルアプリケーション（Android アプリケーション、iOS アプリケーション、スマホアプリケーション）の脆弱性情報が多く、それに続いて無線 LAN ルータ等の組込み系製品、グループウエア等の脆弱性情報が多くありました。

［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
Windows アプリケーション	7
CMS	5
ウェブアプリケーション	4
Android アプリケーション	3
組込み系	2
グループウエア	2
スマホアプリケーション	2
iOS アプリケーション	1
アンチウイルス製品	1
ウェブアプリケーションフレームワーク	1
エディタ	1
管理ソフトウエア	1
情報共有サービス	1
脆弱性検査ツール	1
ファイル暗号化ソフトウエア	1
プラグイン	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］

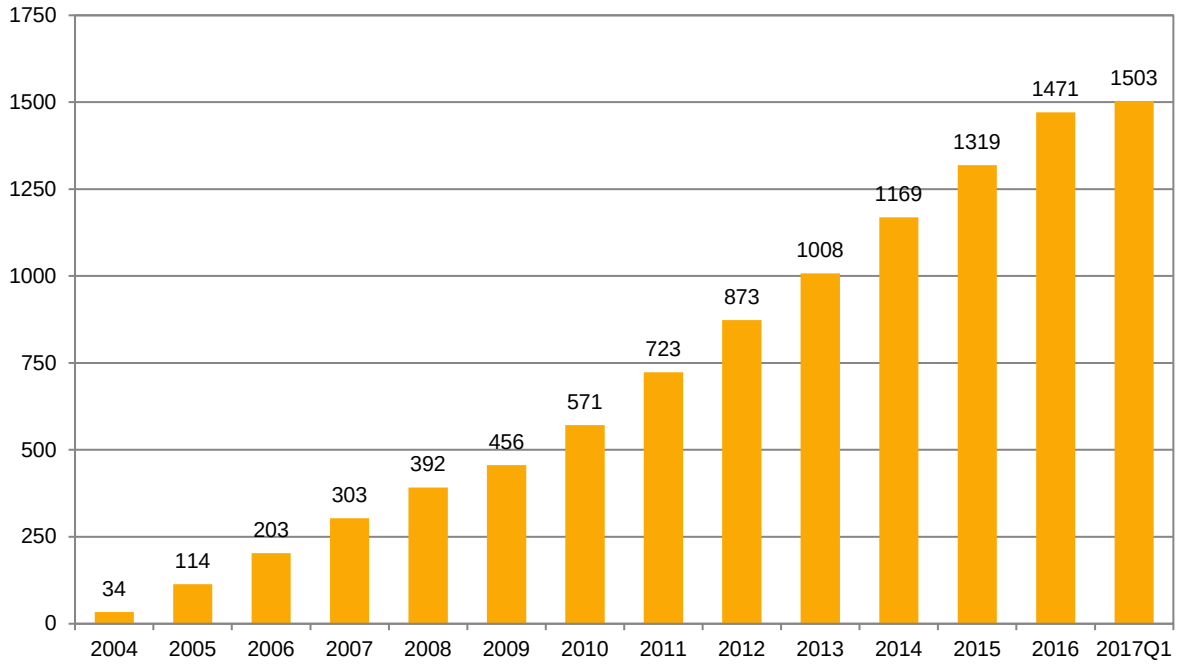
本四半期に公表した国際取扱脆弱性情報は 32 件（累計 1,503 件）で、累計の推移は［図 2-3］に示すとおりです。この 32 件には、HTTPS 通信監視機器によるセキュリティ強度低下の問題に関する注意喚起（Technical Alert）1 件が含まれます。

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。2016 年を通して、非常に多くの組込系製品に関する脆弱性情報を公表しており、本四半期においても 4 件のルータ機器等を含む組込系製品の脆弱性情報を公表しました。また、国内製品開発者と同様に、海外製品開発者からも、自社製品の脆弱性対応に関する事前通知等が JPCERT/CC に報告される事例が徐々に増えており、本四半期においては 6 件の自社製品における脆弱性情報の通知を受け、JVN にて公表しました。

［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
macOS アプリケーション	4
組込系	4
Windows アプリケーション	3
サーバ製品	3
ライブラリ	3
DNS	2
iOS アプリケーション	2
マルチプラットフォームアプリケーション	2
CMS	1

SDK	1
Windows OS	1
ウェブアプリケーションフレームワーク	1
ウェブサービス	1
ウェブサーブレットコンテナ	1
オンライン会議システム	1
スマホアプリケーション	1
アンチウィルスソフトウエア	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

本規程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、連絡の手掛かりを広く求めています。これまでに 251 件（製品開発者数で 164 件）を公表し、45 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り扱いにおける「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 1 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 206 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かけています。

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 NCSC、フィンランドの CERT-FI、オランダの NCSC-NL 等の海外の調整機関と協力関係を結び連携して、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 との連携を 2013 年末に正式に開始し、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ており、新たな分野での国際的活動が定着したと言えます。

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 50 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

2.2. 日本国内の脆弱性情報流通体制の整備

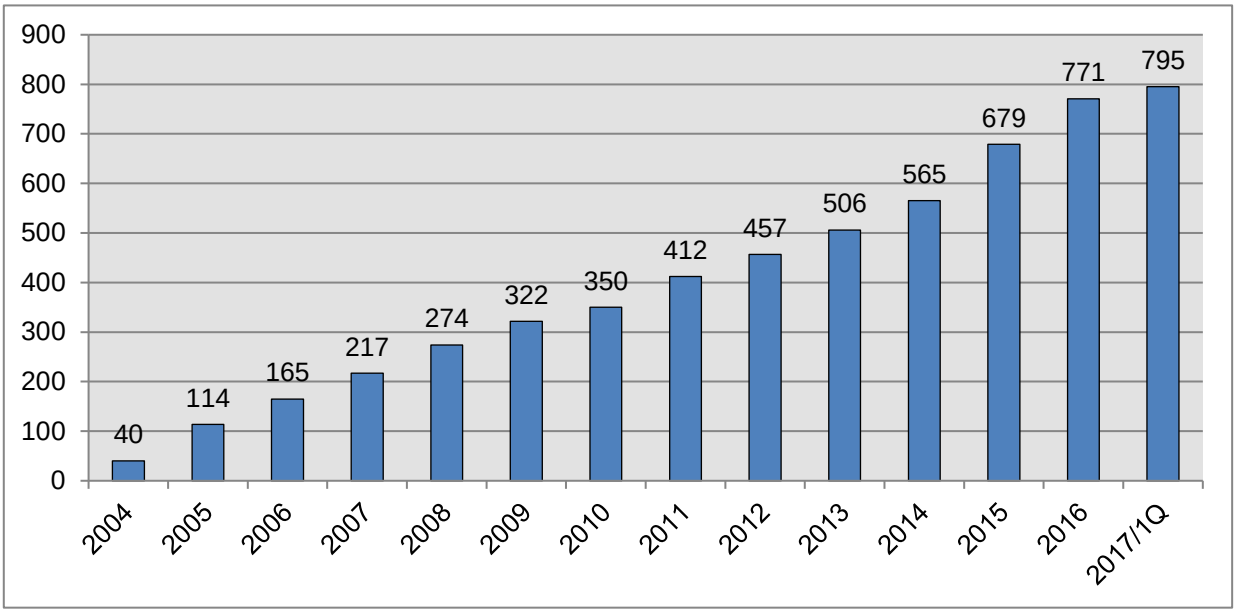
JPCERT/CC では、本規程に従って、日本国内の脆弱性情報流通体制を整備しています。
詳細については、次の Web ページをご参照ください。

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

本規程では、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、2017 年 3 月 31 日現在で 795 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、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 2017 年 3 月 9 日にミーティングを開催し、脆弱性の取り扱い状況と事例紹介、脆弱性情報流通に関連する告示や法制度の動向、海外カンファレンス等で発表された脆弱性対応事例などを紹介するとともに、共通脆弱性評価システム（CVSS）の評価方法に関するワークショップを実施し、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. 講演活動

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 2 件の講演を行いました。

講演日時: 1 月 28 日
講演タイトル: 脆弱性を作りこまない安全なソフトウェア開発のためのコーディング標準 SEI CERT コーディングスタンダードのご紹介
イベント名: オープンソースカンファレンス 2017 Osaka

CMU/SEI（カーネギーメロン大学/ソフトウエアエンジニアリング研究所）の CERT division が公開している SEI CERT コーディングスタンダードは、脆弱性を作りこまない安全なソフトウエア開発にフォー

カスしたコーディング標準です。JPCERT/CC ではこのスタンダードの C 言語版と Java 言語版の日本語化を行い、開発者への普及を推進しています。この講演では、SEI CERT コーディングスタンダードの現状と今後の展望を紹介しました。

講演日時: 3 月 2 日
講演タイトル: Evolving vulnerability coordination in Japan
イベント名: Raleigh 2017 FIRST Technical Colloquium

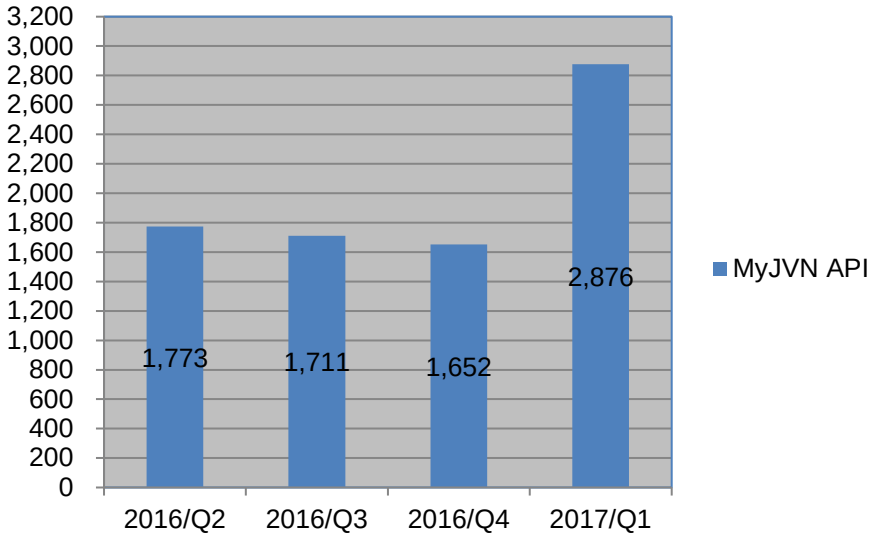
3 月 2 日からの 2 日間、米ノースカロライナ州で Raleigh 2017 FIRST Technical Colloquium が開催されました。
FIRST 加盟組織のうち、すでに PSIRT（Product-SIRT、顧客に製品を提供している組織において製品に関する脆弱性やインシデントへの対応を目的として活動する CSIRT）を設置している組織やこれから PSIRT を設置しようとする組織が主に集まり、脆弱性の取り扱いに関するさまざまな情報交換を行いました。
JPCERT/CC は、日本国内の脆弱性対応状況やこれまで行ってきた脆弱性情報ハンドリングの経験について、事例を交えて紹介しました。また、参加者との意見交換や他のセッションへの参加をとおして情報収集を行いました。

2.4. VRDA フィードによる脆弱性情報の配信

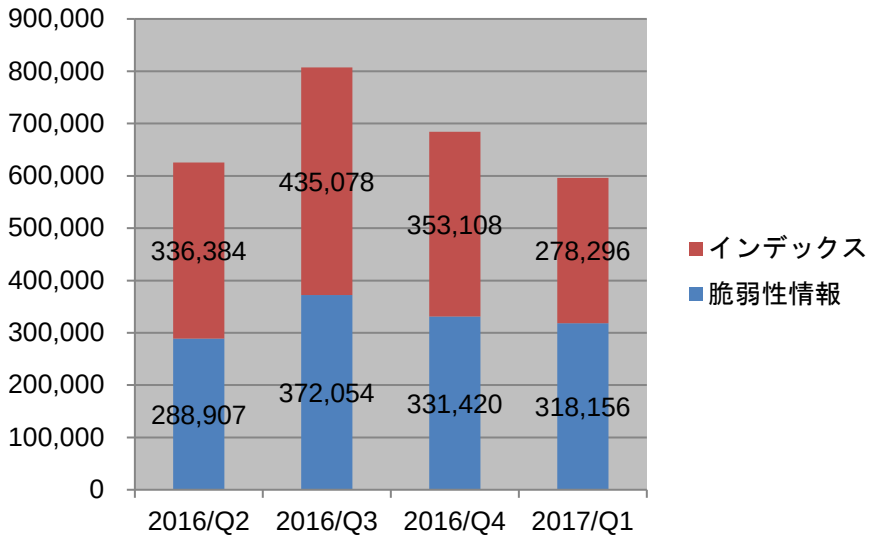
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。
VRDA フィードについての詳しい情報は、次の Web ページをご参照ください。

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 フィード配信件数を［図 2-6］に、VRDA フィードの利用傾向を［図 2-7］と［図 2-8］に示します。［図 2-7］では、VRDA フィードインデックス（Atom フィード）と、脆弱性情報（脆弱性の詳細情報）の利用数を示します。VRDA フィードインデックスは、個別の脆弱性情報のタイトルと脆弱性の影響を受ける製品の識別子（CPE）を含みます。［図 2-8］では、HTML と XML の 2 つのデータ形式で提供している脆弱性情報について、データ形式別の利用割合を示しています。

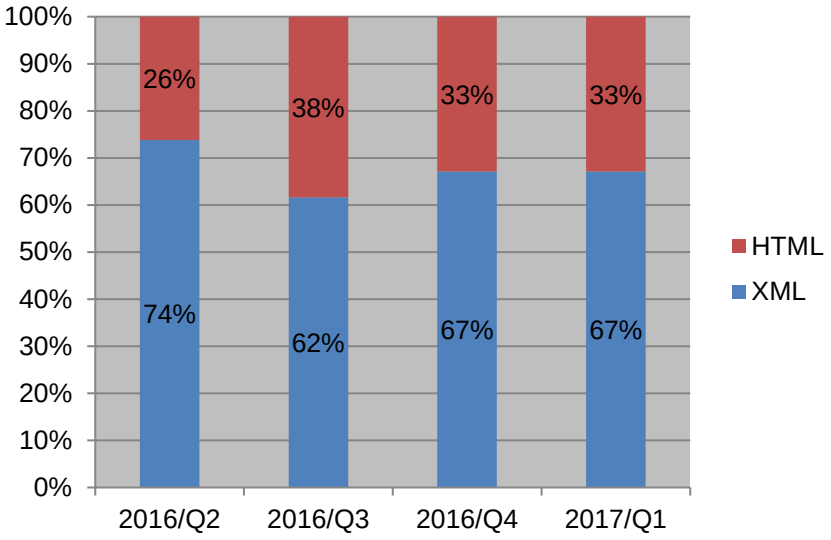


［図 2-6 VRDA フィード配信件数］



［図 2-7 VRDA フィード利用件数］

［図 2-7］に示したように、インデックスの利用数については、前四半期と比較し、約 21%減少しました。脆弱性情報の利用数についても、約 4%減少しました。



［図 2-8 脆弱性情報のデータ形式別利用割合］

［図 2-8］に示したように、本四半期の脆弱性情報のデータ形式別利用傾向については、前四半期と比較し、目立った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。本四半期で収集・分析した情報は 432 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 1 件でした。

2017/01/10 【参考情報】トルコでサイバー攻撃により停電が発生との報道

また、海外での事例や、標準化動向などを 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。

2017-01-10 制御システムセキュリティニュースレター 2016-0012
2017-02-06 制御システムセキュリティニュースレター 2017-0001
2017-03-07 制御システムセキュリティニュースレター 2017-0002

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 646 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（8IP アドレス）は、海外 CSIRT からの報告で、もう 1 件（58IP アドレス）は国内の研究者からの報告でした。いずれも、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して注意を促して欲しいとの報告でした。また、JPCERT/CC では 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。
以上に関する本四半期の情報提供は 6 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提供

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、申込み制）や J-CLICS（制御システムセキュリティ自己評価ツール、フリーダウンロード）を提供しています。本四半期は、日本版 SSAT に関して 13 件の利用申し込みがあり、直接配付件数の累計は、日本版 SSAT が 229 件となりました。

3.5 制御システムセキュリティアセスメントサービス開始

JPCERT/CC は、日本国内の制御システムセキュリティの実態把握と利用組織におけるセキュリティの向上を目的として、制御システムセキュリティアセスメントサービスを開始しました。
本四半期においては、実施に向けた調整と事前説明を前四半期に行った 3 組織に対して、サイトアセスメントを実施しました。さらに実施組織を増やすために、前四半期に JPCERT/CC の Web ページで行った一般向けの募集のフォローアップとして、説明会を開催しました。これにより、新たに 4 組織より応募がありました（4 組織のうち 1 組織に関しては本四半期中にサイトアセスメントを実施、他の 3 組織は 4 月以降に実施予定）。

また、先行する 3 組織に対して実施したアセスメントにより得られた知見（発見事項や実施組織からのフィードバック）は、匿名化をした上で後述の制御システムセキュリティカンファレンス 2017 において発表しました。今後もこのような知見は、制御システム利用者に広くお伝えしていく予定です。

3.6 制御システムセキュリティカンファレンス 2017 開催

2 月 21 日（火）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 2017 を開催し、約 260 名の方にご来場いただきました。今回で 9 回目となる本カンファレンスでは、将来の脅威に備えたセキュリティ対策をアセットオーナに考えていただくトリガーになるように「将来のインシデントに備えて」をテーマに［表 3-1］のようなプログラム構成とし、講演者の方々から制御システムセキュリティへの取り組みについて講演いただきました。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 2017
https://www.jpcert.or.jp/event/ics-conference2017.html

制御システムセキュリティカンファレンス 2017 においての講演資料
https://www.jpcert.or.jp/present/#year2017

［図 3-1 制御システムセキュリティカンファレンス 2017 講演風景］

［表 3-1 制御システムセキュリティカンファレンス・プログラム構成］

(1)「IoT で 2030 年の製造業はどうなる？」 一般社団法人 日本電機工業会 スマートマニュファクチャリング特別委員会 松隈 隆志
(2)「制御システムセキュリティ動向～2016 年度を振り返る～」 JPCERT/CC 顧問 宮地 利雄
(3)「制御システムのためのモデルベースセキュリティ技術」 技術研究組合 制御システムセキュリティセンター 顧問 電気通信大学 i-パワードエネルギー・システム研究センター 澤田 賢治
(4)「製造システムのセキュリティ確保に向けたパナソニックでの取り組み」 パナソニック株式会社 藤井 俊郎
(5)「建物設備システムリファレンスガイドと WG 活動の紹介」 特定非営利活動法人 日本データセンター協会 粕谷 貴司
(6)「CSMS 構築・運用の進め方と CSMS 認証取得による期待効果」 ジェイティ エンジニアリング株式会社 福田 敏博
(7)「制御システムのサイバー&物理セキュリティ」 綜合警備保障株式会社 佐藤 将史
(8)「制御システムセキュリティアセスメントについて」 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. JICA 情報セキュリティ能力向上研修における CSIRT 運用支援（2 月 3 日）

JPCERT/CC は、インドネシア、カンボジア、パプアニューギニア、ベトナム、ラオスの 5 ヶ国の National CSIRT や関係組織の IT 担当者 10 名を対象に、独立行政法人国際協力機構（JICA）が開催した「情報セキュリティ能力向上研修」の実施に協力し、研修生を JPCERT/CC に招いて JPCERT/CC の活動、重要インフラ防護や標的型攻撃への取り組み、最新のインシデント動向等について講義し、National CSIRT としての活動状況について理解を深めていただきました。

4.1.2. ASEAN 諸国への CSIRT 運用支援（2 月 14 日）

JPCERT/CC は、一般財団法人 海外産業人材育成協会（HIDA）が実施した「2016 年度 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（ENIS）」の 2 月 14 日の講義枠において、

ASEAN 8 ヶ国（インドネシア、カンボジア、タイ、フィリピン、ベトナム、マレーシア、ラオス、ミャンマー）の重要インフラ事業者や政策担当者 22 名に向けて、重要インフラ防御および制御システムセキュリティに対する JPCERT/CC の取り組みについて説明しました。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セキュリティ対策の状況が共有されました。

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 との連携を強化するための活動を行っています。また、APCERT（4.2.1.参照）や FIRST（4.2.2.参照）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、2003 年 2 月の APCERT 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 APCERT の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

Steering Committee は、APRICOT 2017 の開催にあわせてホーチミンで、1 月 18 日に電話会議を、また 2 月 25 日に会議をそれぞれ行い、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 メンバとしてこれらの会議に参加すると同時に、事務局として会議運営をサポートしました。

4.2.1.2. APCERT メンバとしての会議出席

2 月 20 日から 3 月 2 日にかけてホーチミンにて、アジア太平洋地域におけるインターネット運用技術者に向けた国際会合である APRICOT 2017 が開催され、その一環として 2 月 26 日に FIRST Technical Colloquium（TC）が実施されました。この FIRST TC で JPCERT/CC は開発中の有害サイト確認システムについて紹介し、改ざんサイトへの対応を向上すべく、関係者と意見交換を行いました。また、APCERT メンバとして FIRST TC の運営をサポートしました。APRICOT 2017 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。

APRICOT 2017
https://2017.apricot.net/

Ho Chi Minh City 2017 FIRST Technical Colloquium
https://2016.apricot.net/program#sessions/first-tc

4.2.1.3. APCERT サイバー演習（APCERT Drill）2017 への参加（3 月 22 日）

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 CSIRT 間の連携の強化ならびに APCERT 加盟組織がサイバー攻撃に迅速に対応できる能力の向上を目的として、毎年実施されています。

13 回目となる今回のサイバー演習は「DDoS 攻撃の新たな脅威の出現」をテーマに実施されました。IoT 機器の脆弱性を悪用し攻撃の踏み台とすることで、ボットネットを形成し、大規模な DDoS 攻撃を仕掛ける Mirai マルウエアなど、IoT 機器を利用した新たな脅威が広まっています。こうした状況を踏まえ、今回のテーマが設定され、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、関係する組織とのインシデント情報のやり取りやマルウエアおよびログの分析など、インシデント対応の手順を確認しました。本演習には、APCERT 加盟組織のうち 18 経済地域から 23 チーム、および OIC-CERT（The Organisation of Islamic Cooperation - Computer Emergency Response Teams）からエジプト、ナイジェリア、パキスタン、モロッコの 4 チームが参加しました。

JPCERT/CC は、APCERT 事務局なら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）として参加するとともに、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ました。APCERT Drill 2017 についての詳細は、次の Web ページをご参照ください。

APCERT Drill 2017 - Emergence of a New DDoS Threat
http://www.apcert.org/documents/pdf/APCERTDrill2017PressRelease.pdf

4.2.2 FIRST（Forum of Incident Response and Security Teams）

JPCERT/CC は、FIRST の活動に 1998 年の加盟以来、積極的に参加しています。現在は JPCERT/CC の国際部マネージャー 小宮山功一朗が FIRST の理事を務めています。本四半期は 1 月 25 日から 27 日にかけてバレンシア（スペイン）で開催された理事会に出席し、組織運営に関わる議論に参画しました。また、シンポジウム担当理事として 1 月 24 日に同じくバレンシアで行われた FIRST Regional Symposium for Europe の準備調整を行いました。本シンポジウムは、欧州の CSIRT コミュニティである TF-CSIRT の会合と同時開催されたもので、最新のインシデント動向や対応事例、脅威情報共有の取り組みや分析ツールの活用等について、各国の関連組織が講演しました。
FIRST と理事ならびに FIRST Regional Symposium for Europe 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

FIRST Regional Symposium for Europe
https://www.first.org/events/symposium/valencia2017

4.2.2.1 Raleigh 2017 FIRST Technical Colloquium への参加（3 月 2 日 - 3 日）

3 月 2 日から 3 日にかけて米ノースカロライナ州のローリーで開催された Raleigh 2017 FIRST Technical Colloquium に参加し、責任ある脆弱性情報開示に関して講演を行うとともに、製品の脆弱性に対応する PSIRT（製品セキュリティインシデント対応チーム）と活動の取り組みや課題について情報共有を行いました。Raleigh 2017 FIRST Technical Colloquium の詳細については、本活動概要の「2.3.1.講演活動」をご参照ください。

4.2.3 国際 CSIRT 間連携に係る国内外カンファレンス等への参加

4.2.3.1 JAIPA クラウド部会への参加（2 月 1 日）

JPCERT/CC は、インターネット環境の健全性と利用に伴うリスクを各国／地域間で比較できる定量的な評価指標（グリーンインデックス）を用いてセキュリティ対策の実効性を確認し、健全なサイバー空間を効率的に実現することを目的とするプロジェクト「サイバーグリーン」を主導しています。
このようなセキュリティ対策を実行していくためには、実際にネットワークを管理しているサービスプロバイダ（ISP）の皆様との協力が必要不可欠です。そのため、2 月 1 日に、ISP の団体の一つである一般社団法人日本インターネットプロバイダー協会（JAIPA）のクラウド部会で本プロジェクトの概要を説明するとともに、グリーンインデックスについて意見交換を行いました。現在開発中のグリーンインデックスは ccTLD 別および AS 番号別に算出しています。後者は ISP 別に算出することとほぼ同義であるため、ISP の皆様とそのメリットとデメリット等を議論しました。指標値があまりよくない場合には ISP の営業上の問題になる可能性があると指摘を受けた一方で、リスク要因の除去はいずれにしてもやるべきことであり ISP 側の取り組みが指標の改善に反映されれば営業上も社会貢献上も有意義であるとの声が上がりました。今後も適切なタイミングで意見交換を行うことで、このような指標の公開についてコミュニティの理解を得ていく所存です。サイバーグリーンについての詳細は、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
サイバーグリーン情報サイト
http://www.cybergreen.net/
サイバーグリーン統計サイト
http://stats.cybergreen.net/

4.2.4 海外 CSIRT 等の来訪および往訪

4.2.4.1 CERT-FR 往訪（1 月 24 日）

CERT-FR（フランスコンピュータ緊急対応チーム）を往訪し、相互に協力している AfricaCERT（アフリカコンピュータ緊急対応チーム）への CSIRT 構築支援および運用支援活動について意見交換を行い、今後も活動を通して密な連携を維持していくことを確認しました。

4.2.4.2 AusCERT 来訪（3 月 9 日）

AusCERT（オーストラリアコンピュータ緊急対応チーム）が来訪し、AusCERT および JPCERT/CC の活動状況等について情報を共有しました。また、今後も APCERT の活動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して行っています。本四半期は次の記事をブログに掲載しました。

2016 in Review: Top Cyber Security Trends in Japan（1 月 25 日）
http://blog.jpcert.or.jp/2017/01/2016-in-review-top-cyber-security-trends-in-japan.html

Anti-analysis technique for PE Analysis Tools - INT Spoofing -（1 月 30 日）
http://blog.jpcert.or.jp/2017/01/anti-analysis-t-24b9.html

ChChes - Malware that Communicates with C&C Servers Using Cookie Headers（2 月 15 日）
http://blog.jpcert.or.jp/2017/02/chches-malware--93d6.html

PlugX + Poison Ivy = PlugIvy? - PlugX Integrating Poison Ivy's Code -（2 月 21 日）
http://blog.jpcert.or.jp/2017/02/plugx-poison-iv-919a.html

Malware Leveraging PowerSploit（3 月 1 日）
http://blog.jpcert.or.jp/2017/03/malware-leveraging-powersploit.html

Malware Clustering using impfuzzy and Network Analysis - impfuzzy for Neo4j -（3 月 23 日）
http://blog.jpcert.or.jp/2017/03/malware-clustering-using-impfuzzy-and-network-analysis---impfuzzy-for-neo4j-.html

Board game on Cyber Security for Awareness Raising（3 月 28 日）
http://blog.jpcert.or.jp/2017/03/board-game-on-cyber-security-for-awareness-raising.html

5. 日本シーサート協議会（NCA）事務局運営

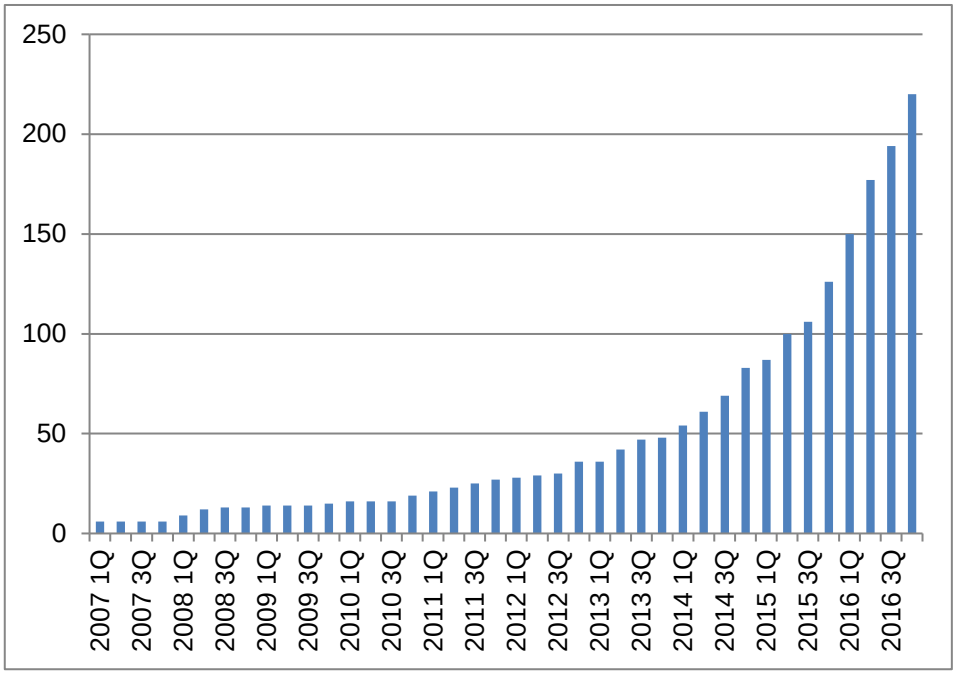
5.1 概況

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。

本四半期には、次の 26 組織（括弧内はシーサート名称）が新規に NCA に加盟しました。

マネックス証券株式会社 (Monex-CSIRT)
株式会社アシックス (ASICS-CSIRT)
アクサ生命保険株式会社 (AXA Japan CSIRT)
電源開発株式会社 (J-POWER CSIRT)
東日本旅客鉄道株式会社 (JRE-CSIRT)
国立大学法人千葉大学 (C-csirt)
NTT コムウェア株式会社 (CW-CSIRT)
アカマイ・テクノロジーズ合同会社 (AkamaiJP-SIRT)
三井住友カード株式会社 (SMCC-CSIRT)
学校法人近畿大学 (KINDAI-CSIRT)
大東建託株式会社 (DK-SIRT)
株式会社　SIG (SIG CSIRT)
ピー・シー・エー株式会社 (PCA-CSIRT)
九州通信ネットワーク株式会社 (QTNet-CSIRT)
株式会社大林組 (OBAYASHI-CSIRT)
アイフル株式会社 (AIFUL-CSIRT)
株式会社 D2C (D2C-CSIRT)
日本たばこ産業株式会社 (JT CSIRT)
ニュートン・コンサルティング株式会社 (NCiSIRT)
株式会社ソリトンシステムズ (Soliton-CSIRT)
国立大学法人　東京工業大学 (東工大 CERT)
ソフトバンク・テクノロジー株式会社　(SBT CSIRT)
株式会社　電通国際情報サービス　(ISID-CSIRT)
株式会社　読売新聞東京本社　(YOMIURI-SIRT)
京阪ホールディングス株式会社　(KEIHAN-SIRT)
商船三井システムズ株式会社　(MOL-CSIRT)

本四半期末時点で 220 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］

5.2 第 12 回臨時総会＆第 16 回シーサートワーキンググループ会

第 12 回臨時総会＆第 16 回シーサートワーキンググループ会を次のとおり開催いたしました。

日時：2017 年 3 月 22 日
場所：THE GRAND HALL 品川グランドセントラルタワー3 階

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協議会への加盟を前提に組織内シーサートの構築を検討している方々が参加する会合です。会合では、5 つのワーキンググループの開催報告や、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 15 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。
臨時総会においては、「運営規約の承認について」と「監事の承認について」の 2 件の議案が承認されました。

5.3 日本シーサート協議会　運営委員会

3 回の運営委員会を開催いたしました。

第 116 回運営委員会
日時：2017 年 1 月 18 日（水）16:00 - 18:00
場所：日本電信電話株式会社

第 117 回運営委員会
日時：2017 年 2 月 22 日（水）16:00 - 18:00
場所：沖電気工業株式会社

第 118 回運営委員会
日時：2017 年 3 月 29 日（水）16:00 - 18:00
場所：三井物産セキュアディレクション株式会社

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

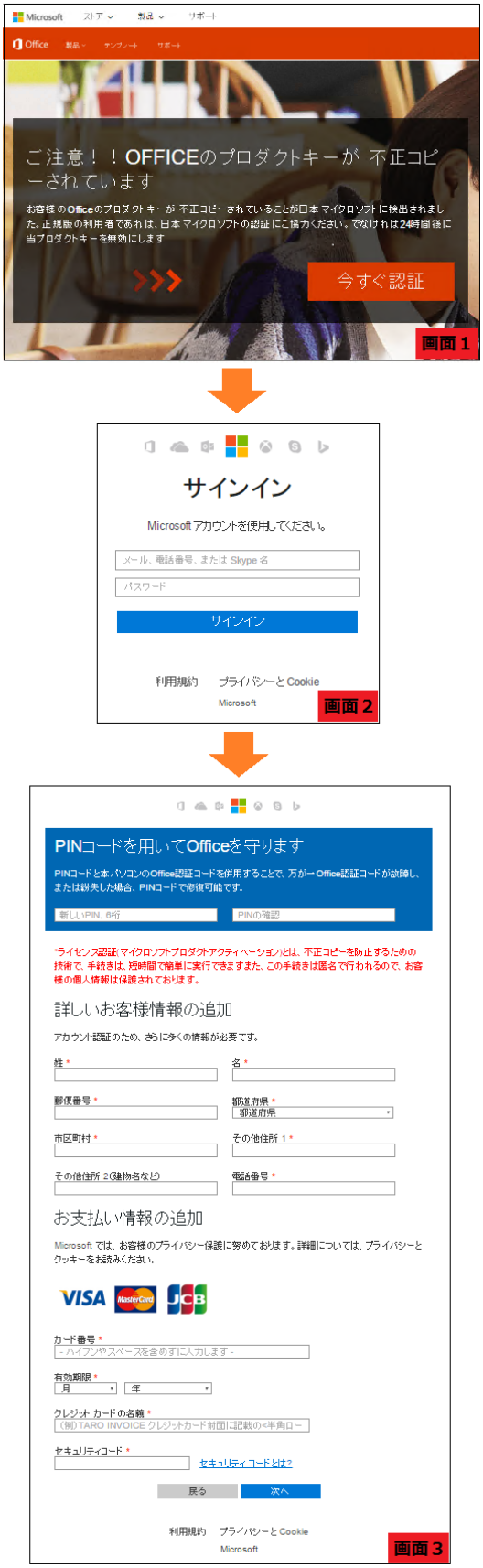
JPCERT/CC は、フィッシング対策協議会（以下「協議会」）の事務局を担当しており、経済産業省からの委託により、協議会における各ワーキンググループ活動の運営や、協議会名での一般消費者からのフィッシングに関する報告・問合せの受付、報告に基づいたフィッシングサイトに関する注意喚起等の活動を行っています。

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 23 件発信しました。

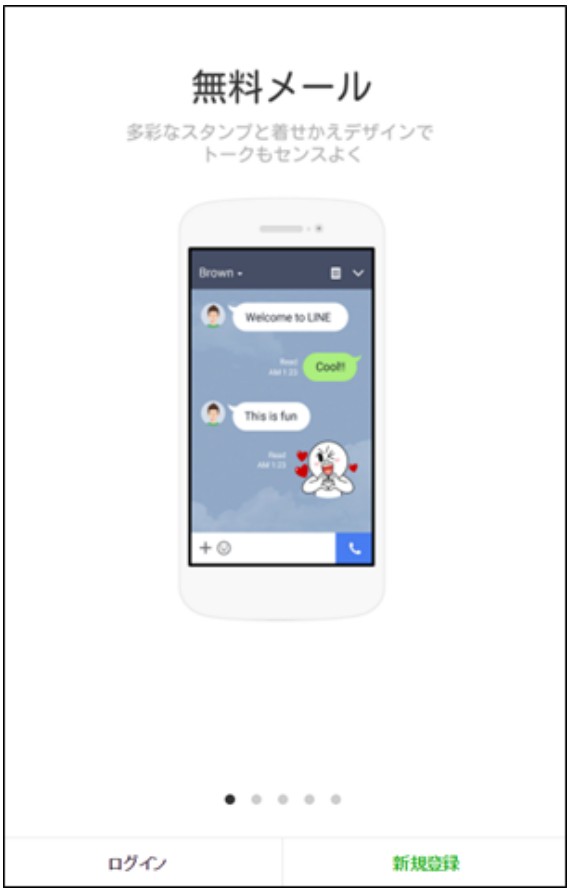
本四半期は、マイクロソフトをかたるフィッシング事案が初めて報告されました。マイクロソフトのアカウント ID とパスワードおよびクレジットカード情報の入力を促すフィッシングサイトが用意され、そこにアクセスするよう促す「オフィスソフトのプロダクトキーが違法にコピーされた」という内容のフィッシングメールが送信されていることが確認されました。マイクロソフトのサービスはユーザ数が非常に多いため、フィッシング対策協議会の緊急情報で注意を促しました。また、以前からあった、LINE をかたるフィッシングは、本四半期においても引き続き報告が寄せられました。協議会では、名前をかたられた各事業者に、メール本文やサイトの URL 等の関連情報を提供しました。

また、合計 18 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、ライセンス更新をかたるフィッシング関連が 5 件、SNS サービスをかたるフィッシング関連が 3 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、オンラインゲームをかたるフィッシング関連が 1 件、その他が 7 件でした。それぞれの例として、[図 6-1]にマイクロソフトをかたるフィッシング(2017/01/12)、［図 6-2］LINE をかたるフィッシング (2017/01/10)、［図 6-3］に MyJCB をかたるフィッシング(2017/02/20)の注意喚起を示します。



［図 6-1］マイクロソフトをかたるフィッシング（2017/01/12）

https://www.antiphishing.jp/news/alert/microsoft_20170112.html



［図 6-2］LINE をかたるフィッシング (2017/01/10)

https://www.antiphishing.jp/news/alert/line_20170110.html

［図 6-3］MyJCB をかたるフィッシング (2017/02/20)
https://www.antiphishing.jp/news/alert/jcb_20170220.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
「フィッシングの現状と対策 2016」」
北海道クレジットカード犯罪対策連絡協議会 , 2017 年 1 月 20 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 2017 年 1 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201701.html
フィッシング対策協議会 2017 年 2 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201702.html
フィッシング対策協議会 2017 年 3 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201703.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 46 回運営委員会
日時：2017 年 1 月 13 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 47 回運営委員会
日時：2017 年 2 月 10 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 48 回運営委員会＆合宿検討会
日時：2017 年 3 月 10 日 15:00 - 16:00
場所：マホロバ・マインズ三浦

7.2 フィッシング対策勉強会 第 2 回会合

フィッシング対策セミナー 2016 を次のとおり開催しました。

フィッシング対策勉強会 第 2 回会合
日時：2017 年 3 月 9 日 13:00 - 15:00
場所：JPCERT/CC 大会議室
講演内容：講演 1: オンライン認証と FIDO の動向
講演者 1：ヤフー株式会社 Yahoo! JAPAN 研究所 山口 修司 様

講演 2：サイバー犯罪対策の為に取り組んでいる 10 のこと
講演者 2：LINE 株式会社 セキュリティ室
アプリケーションセキュリティチーム マネージャー 市原 尚久 様

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、ソフトウエア製品等の脆弱性関連情報に関する取扱規程（平成 29 年経済産業省告示 第 19 号）等に基づき、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前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 3 四半期（10 月～12 月）］（2017 年 1 月 25 日）
https://www.jpcert.or.jp/press/2016/vulnREPORT_2016q4.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して収集するインターネット定点観測システム「TSUBAME」を構築・運用しています。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、収集したデータを分析することで、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 10～12 月)
（2017 年 2 月 9 日）
https://www.jpcert.or.jp/tsubame/report/report201610-12.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2016Q3.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収集または報告いただいた情報をもとに、攻撃に用いられた手法やその影響を把握するため、アーティファクトの調査・分析を行っています。また、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) Poison Ivy のコードを取り込んだマルウエア PlugX(2017-01-12)

PlugX は、標的型攻撃に用いられる、C&C サーバから受信した命令にしたがって動作するマルウエアです。PlugX は機能追加が繰り返され、現在でもたびたび攻撃に使われています。本記事では 2016 年 4 月以降に確認された PlugX の構造に関わる変更について紹介しました。

Poison Ivy のコードを取り込んだマルウエア PlugX(2017-01-12)
https://www.jpcert.or.jp/magazine/acreport-plugx2.html

(2) Cookie ヘッダーを用いて C&C サーバとやりとりするマルウエア ChChes(2017-01-26)

2016 年 10 月以降に標的型メールへの添付が確認されるようになった、ChChes と呼ばれるマルウエアについて紹介しました。ChChes は HTTP のリクエストヘッダ内の Cookie フィールドの値を用いて C&C サーバへリクエストを行い、コマンドやモジュールを受信するマルウエアです。本記事では、ChChes が行う通信と、ChChes が C&C サーバから受信するモジュールやコマンドの構成と機能について解説しました。

Cookie ヘッダーを用いて C&C サーバとやりとりするマルウエア ChChes(2017-01-26)
https://www.jpcert.or.jp/magazine/acreport-ChChes.html

(3) PowerSploit を悪用して感染するマルウエア(2017-02-10)

マルウエア ChChes が PowerShell を悪用して感染を広げる事例を紹介しました。本記事では、ショートカットファイルを悪用した PowerShell スクリプトを用いた感染の流れや GitHub で公開されているペネトレーション試験ツールである PowerSploit をカスタマイズして作成された PowerShell スクリプトについて解説しました。

PowerSploit を悪用して感染するマルウエア(2017-02-10)
https://www.jpcert.or.jp/magazine/acreport-ChChes_ps1.html

(4) impfuzzy とネットワーク分析を用いたマルウエアのクラスタリング~impfuzzy forNeo4j~(2017-03-10)

マルウエア分析では、大量のマルウエアをすばやく分類し、分析するべき新種のマルウエアを抽出することが求められます。本記事では、マルウエア分類を支援するために JPCERT/CC が開発し公開したツール impfuzzy forNeo4j について紹介しました。このツールは、先に JPCERT/CC が開発し公表している impfuzzy を用いてマルウエア相互間の類似度を計算し、その結果を「Neo4j」を使ってクラスター図として可視化します。

impfuzzy とネットワーク分析を用いたマルウエアのクラスタリング ~impfuzzy for Neo4j~(2017-03-10)
https://www.jpcert.or.jp/magazine/acreport-impfuzzy_neo4.html

8.4 研究・調査レポート「ログを活用した Active Directory に対する攻撃の検知と対策」

標的型攻撃を受けた際に、局所的な被害に止められるか、広範囲の侵害を許してしまうかの分け目となることが多いのが、Active Directory を巡る攻防です。Active Directory に対する攻撃を凌ぎ、標的型攻撃の被害を最小限に抑えていただくために、代表的な攻撃手法とその検知方法や攻撃の影響を抑止または軽減する対策方法などを実践的な解説書としてまとめ、さらに、解説書のエッセンスを講演資料に仕立てて、本四半期に解説書と講演資料をともに公開しました。
詳細は、「1.1.2. 情報収集・分析・提供（早期警戒活動事例）【「ログを活用した Active Directory に対する攻撃の検知と対策」の公開】」をご参照ください。

ログを活用した Active Directory に対する攻撃の検知と対策（2017-03-14）
https://www.jpcert.or.jp/research/AD_report_20170314.pdf
ログを活用した Active Directory に対する攻撃の検知と対策［プレゼンテーション資料版］（2017-03-14）
https://www.jpcert.or.jp/research/AD_presen_20170314.pdf

9. 主な講演活動

(1) 佐々木 勇人（早期警戒グループ 情報セキュリティアナリスト）、 輿石 隆（早期警戒グループ 情報セキュリティアナリスト） ：
「情報セキュリティ研修【基礎編】【応用編】」
茨城県神栖市役所職員研修,2017 年 1 月 20 日、2 月 10 日
(2) 真鍋 敬士（理事・最高技術責任者）：
「サイバー脅威にさらされる企業に期待される取り組み」
日経 BP 社 経営課題解決シンポジウム セキュリティ Special , 2017 年 1 月 30 日

(3) 洞田 慎一（早期警戒グループ マネージャー）：
「研究機関におけるサイバー攻撃の脅威と対策」
公益財団法人高輝度光科学研究センター講演, 2017 年 2 月 10 日

(4) 椎木 孝斉（分析センター 分析センター長）：
「ビジネスを加速するサイバーセキュリティ戦略」
Microsoft Security Forum パネル , 2017 年 2 月 14 日

(5) 洞田 慎一（早期警戒グループ マネージャー）：
「公共機関等における CSRIT 構築と運用について」
総合研究大学院大学講演, 2017 年 2 月 17 日

(6) 中村 祐（分析センター 情報セキュリティアナリスト）：
「JPCERT/CC とサイバー攻撃対応」
警察大学校 サイバー捜査研修課「サイバー犯罪（応用）第 5 期）講演, 2017 年 2 月 21 日

(7) 阿部 真吾（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）：
「最近の脅威事例と JPCERT/CC の取り組み」
神奈川県産業技術センター IoT プロジェクトフォーラム, 2017 年 3 月 24 日

10. 主な執筆活動

(1) 青木 亘（早期警戒グループ 情報セキュリティアナリスト）：
「情報セキュリティの動向」
Impress R&D「インターネット白書 2017」,
2017 年 2 月 1 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) SecurityDays2017（福岡・名古屋・東京・大阪）
主　催：株式会社ナノオプト・メディア
開催日：2017年1月30日（福岡）、2月23日（名古屋）、3月8日（東京）、3月16日（大阪）

(2) 重要インフラサイバーセキュリティコンファレンス
主　催：重要インフラサイバーセキュリティコンファレンス実行委員会、株式会社インプレス
開催日：2017年2月8日

(3) IPAサイバーセキュリティシンポジウム2017
主　催：独立行政法人情報処理推進機構（IPA）
開催日：2017年2月8日

(4) JSSEC セキュリティフォーラム 2017
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：2017年2月8日

(5) S/MIME普及シンポジウム2017

主　催：一般財団法人日本情報経済社会推進協会（JIPDEC）

開催日：2017年2月27日

(6) CSMSセミナー ー重要インフラのサイバーセキュリティ戦略と制御システムセキュリティについてー

主　催：一般財団法人日本情報経済社会推進協会（JIPDEC）

開催日：2017年3月10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/
■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
■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

■PGP 公開鍵について　：https://www.jpcert.or.jp/jpcert-pgp.html

本文書を引用、転載する際には JPCERT/CC 広報 (pr@jpcert.or.jp) 宛にご連絡をお願いします。最新情報については JPCERT/CC の Web サイトをご参照ください。
■JPCERT コーディネーションセンター(JPCERT/CC)
https://www.jpcert.or.jp/